

kaspersky

Kaspersky Endpoint Security cho Windows 11.9.0

© 2024 AO Kaspersky Lab

Nội dung

[Kaspersky Endpoint Security cho Windows Help](#)

[Có gì mới](#)

[Các câu hỏi thường gặp](#)

[Kaspersky Endpoint Security cho Windows](#)

[Gói phân phối](#)

[Các yêu cầu về phần cứng và phần mềm](#)

[So sánh các tính năng ứng dụng có sẵn tùy thuộc vào loại hệ điều hành](#)

[Việc so sánh các chức năng ứng dụng phụ thuộc vào các công cụ quản lý.](#)

[Khả năng tương thích với các ứng dụng khác](#)

[Cài đặt và gỡ bỏ ứng dụng](#)

[Triển khai thông qua Kaspersky Security Center](#)

[Bản cài đặt tiêu chuẩn của ứng dụng](#)

[Tạo một gói cài đặt](#)

[Cập nhật cơ sở dữ liệu trong gói cài đặt](#)

[Tạo một tác vụ cài đặt từ xa](#)

[Cài đặt ứng dụng một cách cục bộ bằng Trình hướng dẫn](#)

[Cài đặt ứng dụng từ xa sử dụng Trình Quản lý Cấu hình Trung tâm Hệ thống](#)

[Mô tả thiết lập cài đặt của tập tin setup.ini](#)

[Thay đổi thành phần ứng dụng](#)

[Nâng cấp từ phiên bản trước của ứng dụng](#)

[Gỡ bỏ ứng dụng](#)

[Cấp giấy phép ứng dụng](#)

[Thông tin về Thỏa thuận giấy phép người dùng cuối](#)

[Thông tin về giấy phép](#)

[Thông tin về chứng chỉ giấy phép](#)

[Thông tin về gói đăng ký](#)

[Thông tin về khóa giấy phép](#)

[Thông tin về mã kích hoạt](#)

[Thông tin về tập tin khóa](#)

[So sánh chức năng ứng dụng tùy thuộc vào loại giấy phép cho máy trạm](#)

[So sánh chức năng ứng dụng tùy thuộc vào loại giấy phép cho máy chủ](#)

[Kích hoạt ứng dụng](#)

[Kích hoạt ứng dụng thông qua Kaspersky Security Center](#)

[Sử dụng Trình hướng dẫn Kích hoạt để kích hoạt ứng dụng](#)

[Xem thông tin giấy phép](#)

[Mua giấy phép](#)

[Giá hạn gói đăng ký](#)

[Cung cấp dữ liệu](#)

[Cung cấp dữ liệu theo Thỏa thuận giấy phép người dùng cuối](#)

[Cung cấp dữ liệu khi sử dụng Kaspersky Security Network](#)

[Cung cấp dữ liệu khi sử dụng giải pháp Detection and Response](#)

[Kaspersky Endpoint Detection and Response](#)

[Kaspersky Sandbox](#)

[Tuân thủ luật của Liên minh châu Âu \(GDPR\)](#)

[Bắt đầu](#)

[Thông tin về Tiện ích Quản lý Kaspersky Endpoint Security cho Windows](#)

[Các cân nhắc đặc biệt khi làm việc với các phiên bản khác nhau của tiện ích quản lý](#)

[Những lưu ý đặc biệt khi sử dụng các giao thức được mã hóa để tương tác với các dịch vụ bên ngoài](#)

[Giao diện ứng dụng](#)

[Biểu tượng ứng dụng trong khu vực thông báo trên thanh tác vụ](#)

[Giao diện ứng dụng đơn giản hóa](#)

[Cấu hình việc hiển thị giao diện ứng dụng](#)

[Bắt đầu](#)

[Quản lý chính sách](#)

[Quản lý tác vụ](#)

[Cấu hình các thiết lập cục bộ của ứng dụng](#)

[Bắt đầu và dừng Kaspersky Endpoint Security](#)

[Tạm ngưng và khôi phục tính năng bảo vệ và kiểm soát máy tính](#)

[Tạo và sử dụng một tập tin thiết lập](#)

[Khôi phục các thiết lập mặc định của ứng dụng](#)

[Quét virus của máy tính](#)

[Quét máy tính](#)

[Quét ổ đĩa di động khi chúng được kết nối với máy tính](#)

[Quét trong nền](#)

[Quét từ menu ngữ cảnh](#)

[Kiểm soát tính toàn vẹn của ứng dụng](#)

[Chỉnh sửa phạm vi quét](#)

[Chạy tác vụ quét được lên lịch](#)

[Chạy quét với dưới quyền người dùng khác](#)

[Tối ưu hóa quét](#)

[Cập nhật cơ sở dữ liệu và các mô-đun phần mềm ứng dụng](#)

[Các kịch bản cập nhật mô-đun ứng dụng và cơ sở dữ liệu](#)

[Cập nhật từ một máy chủ lưu trữ](#)

[Cập nhật từ một thư mục được chia sẻ](#)

[Cập nhật sử dụng Kaspersky Update Utility](#)

[Cập nhật trong chế độ di động](#)

[Bắt đầu và dừng một tác vụ cập nhật](#)

[Bắt đầu một tác vụ cập nhật theo quyền của một tài khoản người dùng khác](#)

[Chọn chế độ chạy tác vụ cập nhật](#)

[Bổ sung một nguồn cập nhật](#)

[Cấu hình cập nhật từ một thư mục được chia sẻ](#)

[Cập nhật mô-đun ứng dụng](#)

[Sử dụng một máy chủ proxy để cập nhật](#)

[Lần hoàn tác bản cập nhật gần nhất](#)

[Làm việc với các mối đe dọa đang hoạt động](#)

[Khử mã độc các mối đe dọa đang hoạt động trên máy trạm](#)

[Khử mã độc các mối đe dọa đang hoạt động trên máy chủ](#)

[Bật hoặc tắt Công nghệ khử mã độc nâng cao](#)

[Xử lý các mối đe dọa đang hoạt động](#)

[Bảo vệ máy tính](#)

[Bảo vệ mối đe dọa tập tin](#)

[Bật và tắt Bảo vệ mối đe dọa tập tin](#)

[Tự động tạm ngưng Bảo vệ mối đe dọa tập tin](#)

[Thay đổi hành động xử lý tập tin bị nhiễm của thành phần Bảo vệ mối đe dọa tập tin](#)

[Cấu hình phạm vi bảo vệ của thành phần Bảo vệ mối đe dọa tập tin](#)
[Sử dụng các phương thức quét](#)
[Sử dụng công nghệ quét trong hoạt động của thành phần Bảo vệ mối đe dọa tập tin](#)
[Tối ưu quét tập tin](#)
[Quét các tập tin phức hợp](#)
[Thay đổi chế độ quét](#)

[Bảo vệ mối đe dọa web](#)
[Bật và tắt Bảo vệ mối đe dọa web](#)
[Cấu hình các phương pháp phát hiện địa chỉ web độc hại](#)
[Chống lừa đảo](#)
[Tạo danh sách các địa chỉ web được tin tưởng](#)
[Xuất và nhập danh sách địa chỉ web được tin tưởng](#)

[Bảo vệ mối đe dọa thư điện tử](#)
[Bật và tắt Bảo vệ mối đe dọa thư điện tử](#)
[Thay đổi hành động xử lý các email bị nhiễm](#)
[Cấu hình phạm vi bảo vệ của thành phần Bảo vệ mối đe dọa thư điện tử](#)
[Quét các tập tin phức hợp đính kèm email](#)
[Lọc tập tin đính kèm nội dung email](#)
[Xuất và nhập phần mở rộng để lọc tập tin đính kèm](#)
[Quét email trong Microsoft Office Outlook](#)

[Bảo vệ mối đe dọa mạng](#)
[Bật và tắt Bảo vệ mối đe dọa mạng](#)
[Chặn máy tính tấn công](#)
[Cấu hình các địa chỉ được loại trừ khỏi quy tắc chặn](#)
[Xuất và nhập danh sách các loại trừ khỏi hoạt động chặn](#)
[Cấu hình bảo vệ ngăn các cuộc tấn công mạng theo loại](#)

[Tường lửa](#)
[Bật hoặc tắt Tường lửa](#)
[Thay đổi trạng thái kết nối mạng](#)
[Quản lý các quy tắc gói tin mạng](#)
[Tạo một quy tắc gói tin mạng](#)
[Bật hoặc tắt một quy tắc gói tin mạng](#)
[Thay đổi hành động của Tường lửa cho một quy tắc gói tin mạng](#)
[Thay đổi mức độ ưu tiên của một quy tắc gói tin mạng](#)
[Xuất và nhập quy tắc gói tin mạng](#)
[Quản lý các quy tắc mạng cho ứng dụng](#)
[Tạo một quy tắc mạng cho ứng dụng](#)
[Bật và tắt một quy tắc mạng cho ứng dụng](#)
[Thay đổi hành động của Tường lửa cho một quy tắc mạng cho ứng dụng](#)
[Thay đổi mức độ ưu tiên của một quy tắc mạng cho ứng dụng](#)

[Giám sát mạng](#)

[Phòng chống Tấn công BadUSB](#)
[Bật và tắt Phòng chống Tấn công BadUSB](#)
[Sử dụng Bàn phím ảo để xác thực các thiết bị USB](#)

[Bảo vệ AMSI](#)
[Bật và tắt Bảo vệ AMSI](#)
[Sử dụng Bảo vệ AMSI để quét các tập tin hỗn hợp](#)

[Phòng chống khai thác](#)

[Bật và tắt Phòng chống khai thác](#)

[Chọn một hành động để thực hiện khi phát hiện mã khai thác](#)

[Bảo vệ bộ nhớ của tiến trình hệ thống](#)

[Phát hiện hành vi](#)

[Bật và tắt Phát hiện hành vi](#)

[Chọn hành động để thực hiện khi phát hiện hoạt động của phần mềm độc hại](#)

[Bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài](#)

[Bật hoặc tắt bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài](#)

[Chọn hành động khi phát hiện nỗ lực mã hóa các thư mục được chia sẻ từ bên ngoài](#)

[Tạo một loại trừ cho tính năng bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài](#)

[Cấu hình các địa chỉ được loại trừ khỏi tính năng bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài](#)

[Xuất và nhập danh sách loại trừ từ Bật tính năng bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài](#)

[Phòng chống xâm nhập máy chủ](#)

[Bật và tắt Phòng chống xâm nhập máy chủ](#)

[Quản lý các nhóm tin tưởng ứng dụng](#)

[Thay đổi nhóm tin tưởng của một ứng dụng](#)

[Cấu hình quyền của nhóm tin tưởng](#)

[Chọn một nhóm tin tưởng cho các ứng dụng được khởi động trước Kaspersky Endpoint Security.](#)

[Chọn một nhóm tin tưởng cho các ứng dụng không xác định](#)

[Chọn một nhóm tin tưởng cho các ứng dụng được ký bằng chữ ký số](#)

[Quản lý các quyền của ứng dụng](#)

[Bảo vệ tài nguyên hệ điều hành và dữ liệu cá nhân](#)

[Xóa thông tin về các ứng dụng không sử dụng](#)

[Giám sát Phòng chống xâm nhập máy chủ](#)

[Bảo vệ quyền truy cập âm thanh và video](#)

[Công cụ khắc phục](#)

[Kaspersky Security Network](#)

[Bật và tắt sử dụng Kaspersky Security Network](#)

[Hạn chế của KSN Riêng](#)

[Bật và tắt chế độ đám mây cho các thành phần bảo vệ](#)

[Thiết lập Proxy KSN](#)

[Kiểm tra danh tiếng của một tập tin trong Kaspersky Security Network](#)

[Quét kết nối được mã hóa](#)

[Bật quét kết nối được mã hóa](#)

[Cài đặt chứng chỉ gốc được tin tưởng](#)

[Quét các kết nối được mã hóa bằng chứng chỉ không được tin tưởng](#)

[Quét các kết nối được mã hóa trong Firefox và Thunderbird](#)

[Loại trừ các kết nối khỏi tác vụ quét](#)

[Xóa sạch dữ liệu](#)

[Kiểm soát máy tính](#)

[Kiểm soát Web](#)

[Bật và tắt Kiểm soát Web](#)

[Hành động với quy tắc truy cập tài nguyên web](#)

[Bổ sung một quy tắc truy cập tài nguyên web](#)

[Gán ưu tiên cho các quy tắc truy cập tài nguyên web](#)

[Bật và tắt một quy tắc truy cập tài nguyên web](#)

[Xuất và nhập danh sách địa chỉ web được tin tưởng](#)

[Kiểm tra các quy tắc truy cập tài nguyên web](#)

[Xuất và nhập danh sách địa chỉ tài nguyên web](#)
[Giám sát hoạt động truy cập Internet của người dùng](#)
[Sửa mẫu thông điệp Kiểm soát Web](#)
[Sửa mặt nạ cho các địa chỉ tài nguyên web](#)
[Di chuyển quy tắc truy cập tài nguyên web từ phiên bản cũ của ứng dụng](#)

[Kiểm soát Thiết bị](#)

[Bật và tắt Kiểm soát thiết bị](#)
[Thông tin về quy tắc truy cập](#)
[Sửa đổi một quy tắc truy cập thiết bị](#)
[Sửa một quy tắc truy cập bus kết nối](#)
[Bổ sung một mạng Wi-Fi vào danh sách được tin tưởng](#)
[Giám sát việc sử dụng ổ đĩa di động](#)
[Thay đổi thời gian lưu vào bộ nhớ đệm](#)
[Hành động với các thiết bị được tin tưởng](#)
[Bổ sung một thiết bị vào danh sách Được Tin tưởng từ giao diện ứng dụng](#)
[Bổ sung một thiết bị vào danh sách Được Tin tưởng từ Kaspersky Security Center](#)
[Xuất và nhập danh sách các thiết bị được tin tưởng](#)
[Nhận truy cập đến một thiết bị bị chặn](#)
[Chế độ trực tuyến để cấp quyền truy cập](#)
[Chế độ ngoại tuyến để cấp quyền truy cập](#)
[Sửa mẫu thông điệp Kiểm soát thiết bị](#)
[Anti-Bridging](#)
[Bật Anti-Bridging](#)
[Thay đổi trạng thái của một quy tắc kết nối](#)
[Thay đổi mức độ ưu tiên của một quy tắc kết nối](#)

[Kiểm soát thích ứng sự cố](#)

[Bật và tắt Kiểm soát thích ứng sự cố](#)
[Bật và tắt một quy tắc Kiểm soát thích ứng sự cố](#)
[Sửa hành động được thực hiện khi một quy tắc Kiểm soát thích ứng sự cố được kích hoạt](#)
[Tạo loại trừ cho một quy tắc Kiểm soát thích ứng sự cố](#)
[Xuất và nhập các loại trừ cho quy tắc Kiểm soát thích ứng sự cố](#)
[Áp dụng bản cập nhật cho các quy tắc của Kiểm soát thích ứng sự cố](#)
[Chỉnh sửa khuôn mẫu tin nhắn Kiểm soát thích ứng sự cố](#)
[Xem các báo cáo Kiểm soát thích ứng sự cố](#)

[Kiểm soát ứng dụng](#)

[Giới hạn chức năng của Kiểm soát ứng dụng](#)
[Bật và tắt Kiểm soát ứng dụng](#)
[Chọn chế độ Kiểm soát ứng dụng](#)
[Làm việc với các quy tắc Kiểm soát ứng dụng trong giao diện ứng dụng](#)
[Thêm một Quy tắc kiểm soát ứng dụng](#)
[Bổ sung một điều kiện kích hoạt cho một quy tắc Kiểm soát ứng dụng](#)
[Thay đổi trạng thái của một quy tắc Kiểm soát ứng dụng](#)
[Quản lý các quy tắc Kiểm soát ứng dụng trong Kaspersky Security Center](#)
[Truy xuất thông tin về các ứng dụng được cài đặt trên máy tính của người dùng](#)
[Tạo danh mục ứng dụng](#)
[Bổ sung các tập tin thực thi từ thư mục Tập tin thực thi đến danh mục ứng dụng](#)
[Bổ sung các tập tin thực thi liên quan đến sự kiện vào danh mục ứng dụng](#)
[Bổ sung và sửa đổi một quy tắc Kiểm soát ứng dụng sử dụng Kaspersky Security Center](#)

[Thay đổi trạng thái của một quy tắc Kiểm soát ứng dụng qua Kaspersky Security Center](#)

[Xuất và nhập các Quy tắc kiểm soát ứng dụng](#)

[Kiểm tra các quy tắc Kiểm soát ứng dụng sử dụng Kaspersky Security Center](#)

[Xem các sự kiện từ hoạt động thử nghiệm của thành phần Kiểm soát ứng dụng](#)

[Xem báo cáo về các ứng dụng bị chặn trong chế độ kiểm tra](#)

[Xem các sự kiện từ hoạt động của thành phần Kiểm soát ứng dụng](#)

[Xem một báo cáo về các ứng dụng bị chặn](#)

[Kiểm tra các Quy tắc Kiểm soát ứng dụng](#)

[Quản lý hoạt động ứng dụng](#)

[Quy tắc tạo đại diện tên cho tập tin hoặc thư mục](#)

[Sửa mẫu thông điệp Kiểm soát ứng dụng](#)

[Biện pháp tốt nhất để triển khai danh sách các ứng dụng được phép](#)

[Cấu hình chế độ danh sách được phép cho các ứng dụng](#)

[Kiểm tra chế độ danh sách được phép](#)

[Hỗ trợ cho chế độ danh sách được phép](#)

[Giám sát cổng mạng](#)

[Bật tính năng giám sát tất cả cổng mạng](#)

[Tạo một danh sách cổng mạng bị giám sát](#)

[Tạo một danh sách ứng dụng được giám sát tất cả cổng mạng](#)

[Xuất và nhập danh sách các cổng được giám sát](#)

[Bảo vệ bằng mật khẩu](#)

[Bật Bảo vệ bằng mật khẩu](#)

[Cấp quyền truy cập cho người dùng cá nhân hoặc nhóm](#)

[Sử dụng một mật khẩu tạm thời để cấp quyền truy cập](#)

[Các khía cạnh đặc biệt của quyền truy cập được Bảo vệ bằng mật khẩu](#)

[Đặt lại mật khẩu KAdmin](#)

[Khu vực tin tưởng](#)

[Tạo một loại trừ quét](#)

[Bật và tắt một loại trừ quét](#)

[Chọn các loại đối tượng có thể được phát hiện](#)

[Sửa danh sách các ứng dụng được tin tưởng](#)

[Bật và tắt quy tắc vùng tin tưởng cho một ứng dụng trong danh sách các ứng dụng được tin tưởng](#)

[Sử dụng ổ lưu trữ chứng chỉ hệ thống được tin tưởng](#)

[Quản lý Sao lưu](#)

[Cấu hình thời gian lưu trữ tối đa cho các tập tin trong Sao lưu](#)

[Cấu hình kích cỡ tối đa của Sao lưu](#)

[Khôi phục các tập tin từ Sao lưu](#)

[Xóa bản sao lưu của tập tin khỏi Sao lưu](#)

[Dịch vụ thông báo](#)

[Cấu hình cấu hình nhật ký sự kiện](#)

[Cấu hình việc hiển thị và truyền tải thông báo](#)

[Cấu hình việc hiển thị cảnh báo về trạng thái ứng dụng trong khu vực thông báo](#)

[Nhắn tin giữa người dùng và quản trị viên](#)

[Quản lý báo cáo](#)

[Xem báo cáo](#)

[Cấu hình thời gian lưu trữ báo cáo tối đa](#)

[Cấu hình kích cỡ tối đa của tập tin báo cáo](#)

[Lưu một báo cáo ra tập tin](#)

[Xóa nội dung báo cáo](#)

[Tự bảo vệ cho Kaspersky Endpoint Security](#)

[Bật và tắt Tự bảo vệ](#)

[Bật và tắt hỗ trợ AM-PPL](#)

[Bật và tắt bảo vệ quản lý bên ngoài](#)

[Hỗ trợ các ứng dụng quản trị từ xa](#)

[Kết quả hoạt động và tính tương thích với các ứng dụng khác của Kaspersky Endpoint Security](#)

[Bật hoặc tắt chế độ tiết kiệm năng lượng](#)

[Bật hoặc tắt tính năng nhường tài nguyên cho các ứng dụng khác](#)

[Các phương pháp tốt nhất để tối ưu hóa hiệu năng của Kaspersky Endpoint Security](#)

[Mã hóa dữ liệu](#)

[Hạn chế của chức năng mã hóa](#)

[Thay đổi độ dài của khóa mã hóa \(AES56 / AES256\)](#)

[Kaspersky Disk Encryption](#)

[Các tính năng đặc biệt của mã hóa ổ SSD](#)

[Khởi chạy Kaspersky Disk Encryption](#)

[Tạo một danh sách các ổ cứng được loại trừ khỏi tác vụ mã hóa](#)

[Xuất và nhập một danh sách các ổ đĩa cứng được loại trừ khỏi tác vụ mã hóa](#)

[Bật công nghệ Single Sign-On \(SSO\)](#)

[Quản lý tài khoản Authentication Agent](#)

[Sử dụng token và thẻ thông minh với Authentication Agent](#)

[Giải mã ổ cứng](#)

[Khôi phục quyền truy cập vào ổ đĩa được bảo vệ bởi công nghệ Kaspersky Disk Encryption](#)

[Đăng nhập bằng tài khoản dịch vụ Authentication Agent](#)

[Cập nhật hệ điều hành](#)

[Loại trừ lỗi của bản cập nhật chức năng mã hóa](#)

[Chọn cấp độ truy vết Authentication Agent](#)

[Chỉnh sửa văn bản trợ giúp Authentication Agent](#)

[Xóa các đối tượng và dữ liệu còn lại sau khi kiểm tra hoạt động của Authentication Agent](#)

[Quản lý BitLocker](#)

[Khởi chạy BitLocker Drive Encryption](#)

[Giải mã ổ cứng được bảo vệ bằng BitLocker](#)

[Khôi phục quyền truy cập ổ đĩa được bảo vệ bằng BitLocker](#)

[Tạm dừng bảo vệ BitLocker để cập nhật phần mềm](#)

[Mã hóa mức độ tập tin trên các ổ đĩa máy tính cục bộ](#)

[Mã hóa các tập tin trên ổ đĩa nội bộ của máy tính](#)

[Tạo quy tắc truy cập tập tin được mã hóa cho ứng dụng](#)

[Mã hóa những tập tin được tạo hoặc sửa đổi bởi những ứng dụng cụ thể](#)

[Tạo một quy tắc giải mã](#)

[Giải mã các tập tin trên ổ đĩa nội bộ trên máy tính](#)

[Tạo các gói mã hóa](#)

[Khôi phục quyền truy cập vào các tập tin được mã hóa](#)

[Khôi phục truy cập đến dữ liệu được mã hóa sau khi hỏng hệ điều hành](#)

[Sửa mẫu thông điệp truy cập tập tin được mã hóa](#)

[Mã hóa ổ đĩa di động](#)

[Bắt đầu mã hóa ổ đĩa di động](#)

[Thêm một quy tắc mã hóa cho ổ đĩa di động](#)

[Xuất và nhập danh sách các quy tắc mã hóa cho ổ đĩa di động](#)

[Chế độ di động để truy cập các tập tin được mã hóa trên ổ đĩa di động](#)

[Giải mã ổ đĩa di động](#)

[Xem chi tiết mã hóa dữ liệu](#)

[Xem trạng thái mã hóa](#)

[Xem thống kê mã hóa trên các bảng điều khiển của Kaspersky Security Center](#)

[Xem lỗi mã hóa tập tin trên các ổ đĩa nội bộ trên máy tính](#)

[Xem báo cáo mã hóa dữ liệu](#)

[Làm việc với các thiết bị được mã hóa khi không có truy cập đến chúng](#)

[Khôi phục dữ liệu bằng cách sử dụng Tiện ích khôi phục FDERT](#)

[Tạo một đĩa cứu hộ cho hệ điều hành](#)

[Các giải pháp Detection and Response](#)

[Kaspersky Endpoint Agent](#)

[Chuyển đổi chính sách và tác vụ cho Kaspersky Endpoint Agent](#)

[Chuyển cấu hình \[KES+KEA\] sang cấu hình \[KES+built-in agent\]](#)

[Managed Detection and Response](#)

[Tích hợp với MDR](#)

[Chuyển sang từ Kaspersky Endpoint Agent](#)

[Endpoint Detection and Response](#)

[Tích hợp với Kaspersky Endpoint Detection and Response](#)

[Chuyển sang từ Kaspersky Endpoint Agent](#)

[Quét các dấu hiệu về sự xâm nhập \(tác vụ tiêu chuẩn\)](#)

[Di chuyển tập tin đến Khu vực cách ly](#)

[Lấy tập tin](#)

[Xóa tập tin](#)

[Khởi chạy tiến trình](#)

[Chấm dứt tiến trình](#)

[Phòng chống thực thi](#)

[Cách ly mạng máy tính](#)

[Phụ lục 1. Các phần mở rộng tập tin được hỗ trợ cho Phòng chống thực thi](#)

[Phụ lục 2. Các trình thông dịch tập lệnh được hỗ trợ](#)

[Phụ lục 3. Phạm vi quét IOC trong registry \(RegistryItem\)](#)

[Phụ lục 4. Các yêu cầu của tập tin IOC](#)

[Kaspersky Sandbox](#)

[Tích hợp với Kaspersky Sandbox](#)

[Chuyển sang từ Kaspersky Endpoint Agent](#)

[Thêm một chứng chỉ TLS](#)

[Thêm máy chủ Kaspersky Sandbox](#)

[Quét các dấu hiệu về sự xâm nhập \(tác vụ độc lập\)](#)

[Kaspersky Anti Targeted Attack Platform \(KATA EDR\)](#)

[Quản lý Khu vực cách ly](#)

[Cấu hình kích thước tối đa cho Khu vực cách ly](#)

[Gửi dữ liệu về các tập tin được cách ly tới Kaspersky Security Center](#)

[Kaspersky Security cho Windows Server](#)

[Cài đặt KES trên KSWs](#)

[Kích hoạt KES bằng khóa KSWs](#)

[Quản lý ứng dụng trên máy chủ Chế độ Core](#)

[Quản lý ứng dụng từ dòng lệnh](#)

[Cài đặt ứng dụng](#)

[Kích hoạt ứng dụng](#)

[Gỡ bỏ ứng dụng](#)

[Các lệnh AVP](#)

[SCAN. Quét virus](#)

[UPDATE. Cập nhật cơ sở dữ liệu và các mô-đun phần mềm ứng dụng](#)

[ROLLBACK. Làn hoàn tác bản cập nhật gần nhất](#)

[TRACES. Truy vết](#)

[START. Bắt đầu hồ sơ](#)

[STOP. Dừng một hồ sơ](#)

[STATUS. Trạng thái hồ sơ](#)

[STATISTICS. Thống kê hoạt động của hồ sơ](#)

[RESTORE. Khôi phục các tập tin từ Sao lưu](#)

[EXPORT. Xuất thiết lập ứng dụng](#)

[IMPORT. Nhập thiết lập ứng dụng](#)

[ADDKEY. Áp dụng một tập tin khóa](#)

[LICENSE. Cấp giấy phép](#)

[RENEW. Mua giấy phép](#)

[PBATESTRESET. Đặt lại kết quả kiểm tra ổ đĩa trước khi mã hóa ổ đĩa](#)

[EXIT. Thoát khỏi ứng dụng](#)

[EXITPOLICY. Tắt chính sách](#)

[STARTPOLICY. Bật chính sách](#)

[DISABLE. Tắt bảo vệ](#)

[SPYWARE. Phát hiện phần mềm gián điệp](#)

[KSN. Chuyển đổi KSN Toàn cầu/Riêng](#)

[Các lệnh KESCLI](#)

[Quét. Quét virus](#)

[GetScanState. Trạng thái hoàn thành tác vụ quét](#)

[GetLastScanTime. Xác định thời gian hoàn thành tác vụ quét](#)

[GetThreats. Nhận dữ liệu về các mối đe dọa được phát hiện](#)

[UpdateDefinitions. Cập nhật cơ sở dữ liệu và các mô-đun phần mềm ứng dụng](#)

[GetDefinitionState. Xác định thời gian hoàn thành tác vụ cập nhật](#)

[EnableRTP. Bật bảo vệ](#)

[GetRealTimeProtectionState. Trạng thái của thành phần Bảo vệ mối đe dọa tập tin](#)

[Phiên bản. Xác định phiên bản của ứng dụng](#)

[Lệnh quản lý Detection and Response](#)

[SANDBOX. Quản lý Kaspersky Sandbox](#)

[PHÒNG CHỐNG. Quản lý phòng chống thực thi](#)

[CÁCH LY. Quản lý cách ly mạng](#)

[RESTORE. Khôi phục các tập tin từ Khu vực cách ly](#)

[IOCSAN. Quét các dấu hiệu về sự xâm nhập \(IOC\)](#)

[MDRLICENSE. Kích hoạt MDR](#)

[Các mã lỗi](#)

[Phụ lục. Hồ sơ ứng dụng](#)

[Quản lý ứng dụng thông qua REST API](#)

[Cài đặt ứng dụng với REST API](#)

[Làm việc với API](#)

[Các nguồn thông tin về ứng dụng](#)

[Liên hệ với Hỗ trợ kỹ thuật](#)

[Nội dung và bộ nhớ của tập tin truy vết](#)

[Truy vết hoạt động của ứng dụng](#)

[Truy vết hiệu năng của ứng dụng](#)

[Ghi kết xuất](#)

[Bảo vệ tập tin kết xuất và tập tin dấu vết](#)

[Hạn chế và cảnh báo](#)

[Thuật ngữ](#)

[Authentication Agent](#)

[Báo động giả](#)

[Chứng nhận giấy phép](#)

[Cơ sở dữ liệu diệt virus](#)

[Cơ sở dữ liệu về các địa chỉ web độc hại](#)

[Cơ sở dữ liệu về các địa chỉ web lừa đảo](#)

[Đại diện](#)

[Dạng chuẩn hóa của địa chỉ của một tài nguyên web](#)

[Đối tượng OLE](#)

[Đơn vị cấp chứng chỉ](#)

[IOC](#)

[Khóa bổ sung](#)

[Khóa hiện hoạt](#)

[Khử mã độc](#)

[Mô-đun Nền tảng Tin tưởng](#)

[Network Agent](#)

[Nhóm quản trị](#)

[OpenIOC](#)

[Phạm vi bảo vệ](#)

[Phạm vi quét](#)

[Tác vụ](#)

[Tập tin bị nhiễm](#)

[Tập tin có thể gây nhiễm](#)

[Tập tin IOC](#)

[Tập tin nén](#)

[Trình quản lý tập tin di động](#)

[Phụ lục](#)

[Phụ lục 1. Thiết lập ứng dụng](#)

[Bảo vệ mối đe dọa tập tin](#)

[Bảo vệ mối đe dọa web](#)

[Bảo vệ mối đe dọa thư điện tử](#)

[Bảo vệ mối đe dọa mạng](#)

[Tường lửa](#)

[Phòng chống Tấn công BadUSB](#)

[Bảo vệ AMSI](#)

[Phòng chống khai thác](#)

[Phát hiện hành vi](#)

[Phòng chống xâm nhập máy chủ](#)

[Công cụ khắc phục](#)

[Kaspersky Security Network](#)

[Kiểm soát Web](#)

[Kiểm soát Thiết bị](#)
[Kiểm soát ứng dụng](#)
[Kiểm soát thích ứng sự cố](#)
[Cảm biến điểm cuối](#)
[Kaspersky Sandbox](#)
[Endpoint Detection and Response](#)
[Mã hóa toàn bộ ổ đĩa](#)
[Mã hóa mức độ tập tin](#)
[Mã hóa ổ đĩa di động](#)
[Mẫu \(mã hóa dữ liệu\)](#)
[Loại trừ](#)
[Thiết lập ứng dụng](#)
[Các báo cáo và lưu trữ](#)
[Thiết lập mạng](#)
[Giao diện](#)
[Quản lý thiết lập](#)
[Cập nhật cơ sở dữ liệu và các mô-đun phần mềm ứng dụng](#)
[Phụ lục 2. Các nhóm tin tưởng của ứng dụng](#)
[Phụ lục 3. Phần mở rộng tập tin để quét nhanh ổ đĩa di động](#)
[Phụ lục 4. Các loại tập tin cho bộ lọc đính kèm Bảo vệ mối đe dọa thư điện tử](#)
[Phụ lục 5. Thiết lập mạng để tương tác với các dịch vụ bên ngoài](#)
[Phụ lục 6. Các sự kiện ứng dụng](#)
[Thông tin về mã của bên thứ ba](#)
[Thông báo thương hiệu](#)

Kaspersky Endpoint Security cho Windows Help

🔔 Có gì mới trong 11.9.0

- [Bây giờ bạn có thể tạo tài khoản dịch vụ Authentication Agent cho Kaspersky Disk Encryption](#)
- [Cải tiến giao diện chi tiết phát hiện cho EDR Optimum](#)
- [Có gì mới trong mỗi phiên bản của Kaspersky Endpoint Security cho Windows](#)

📁 Bắt đầu

- [Triển khai Kaspersky Endpoint Security cho Windows](#)
- [Thiết lập ban đầu Kaspersky Endpoint Security cho Windows](#)
- [Cấp giấy phép cho Kaspersky Endpoint Security cho Windows](#)

🛡️ Loại bỏ các mối đe dọa

- [Trên máy trạm](#)
- [Trên máy chủ](#)
- Phản ứng khi phát hiện một Dấu hiệu về sự xâm nhập ([Cách ly mạng](#) → [Khu vực cách ly](#) → [Phòng chống thực thi](#))

🗂️ Sử dụng KES như một phần của các giải pháp khác

- [Kaspersky EDR](#)
- [Kaspersky Sandbox](#)
- [Kaspersky MDR](#)

📄 Cung cấp dữ liệu

- [Trong mục Thỏa thuận giấy phép người dùng cuối](#)
- [Khi sử dụng KSN](#)

- [GDPR](#)

Có gì mới

Bản cập nhật 11.9.0

Kaspersky Endpoint Security 11.9.0 cho Windows cung cấp các tính năng và cải tiến sau đây:

1. Bây giờ bạn có thể [tạo tài khoản dịch vụ Authentication Agent](#) khi sử dụng Kaspersky Disk Encryption. Cần có tài khoản dịch vụ để có quyền truy cập vào máy tính, như khi người dùng quên mật khẩu. Bạn cũng có thể sử dụng tài khoản dịch vụ như tài khoản dự trữ.
2. Gói phân phối Kaspersky Endpoint Agent không còn thuộc [gói phân phối ứng dụng](#). Bạn có thể sử dụng tác nhân tích hợp của Kaspersky Endpoint Security để hỗ trợ các giải pháp [Detection and Response](#). Nếu cần, bạn có thể tải xuống gói phân phối Kaspersky Endpoint Agent từ gói phân phối Kaspersky Anti Targeted Attack Platform.
3. Giao diện thông tin chi tiết phát hiện cho [Kaspersky Endpoint Detection and Response Optimum \(EDR Optimum\)](#) được cải tiến. Các tính năng Phản hồi về mối đe dọa hiện đã có chú giải công cụ. Hướng dẫn từng bước để đảm bảo khả năng bảo mật cho cơ sở hạ tầng của công ty cũng được hiển thị khi phát hiện các dấu hiệu xâm nhập.
4. Bây giờ bạn có thể kích hoạt Kaspersky Endpoint Security cho Windows bằng khóa giấy phép của Kaspersky Hybrid Cloud Security.
5. Đã thêm các sự kiện mới về [thiết lập kết nối với các miền có chứng chỉ không được tin tưởng](#) và các lỗi quét kết nối được mã hóa.

Bản cập nhật 11.8.0

Kaspersky Endpoint Security 11.8.0 cho Windows cung cấp các tính năng và cải tiến sau đây:

1. [Đã thêm tác nhân tích hợp để hỗ trợ hoạt động của giải pháp Kaspersky Endpoint Detection and Response Expert](#). *Kaspersky Endpoint Detection and Response Expert* là một giải pháp để bảo vệ cơ sở hạ tầng CNTT của doanh nghiệp trước các mối đe dọa mạng nâng cao. Chức năng của giải pháp này kết hợp tính năng tự động phát hiện các mối đe dọa với khả năng phản ứng trước các mối đe dọa này để chống lại các cuộc tấn công nâng cao, bao gồm các cuộc tấn công khai thác mới, phần mềm tống tiền, các cuộc tấn công không dùng tập tin, cũng như các phương pháp sử dụng các công cụ hệ thống hợp pháp. EDR Expert cung cấp nhiều chức năng giám sát và phản ứng trước mối đe dọa hơn EDR Optimum. Để biết thêm thông tin về giải pháp này, hãy xem [Trợ giúp của Kaspersky Endpoint Detection and Response Expert](#).
2. Giao diện [Giám sát mạng](#) đã được cải tiến. Giám sát mạng hiện hiển thị giao thức UDP ngoài giao thức TCP.
3. Tác vụ [Quét virus](#) đã được cải tiến. Nếu bạn đã khởi động lại máy tính trong quá trình quét, Kaspersky Endpoint Security sẽ tự động chạy tác vụ, tiếp tục từ thời điểm tác vụ quét bị gián đoạn.
4. Bây giờ bạn có thể đặt giới hạn cho thời gian thực thi tác vụ. Bạn có thể giới hạn thời gian thực thi cho tác vụ [Quét virus](#) và [Quét IOC](#). Sau một khoảng thời gian được quy định, Kaspersky Endpoint Security

sẽ dừng tác vụ đó. Ví dụ như để giảm thời gian thực thi tác vụ *Quét virus*, bạn có thể: [cấu hình phạm vi quét](#) hoặc [tối ưu tác vụ quét](#).

5. Các hạn chế của nền tảng máy chủ được dỡ bỏ đối với ứng dụng được cài đặt trên Windows 10 Enterprise đa phiên. Giờ đây Kaspersky Endpoint Security coi Windows 10 Enterprise đa phiên là một hệ điều hành máy trạm, không phải là hệ điều hành máy chủ. Tương ứng với điều đó, [các hạn chế của nền tảng máy chủ](#) không còn được áp dụng cho ứng dụng trên Windows 10 Enterprise đa phiên. Ứng dụng cũng sử dụng một khóa giấy phép để kích hoạt cho máy trạm thay vì khóa giấy phép cho máy chủ.

Bản cập nhật 11.7.0

Kaspersky Endpoint Security cho Windows 11.7.0 cung cấp các tính năng mới và cải tiến sau đây:

1. [Giao diện của Kaspersky Endpoint Security cho Windows](#) được cập nhật.

2. [Hỗ trợ Windows 11, Windows 10 21H2 và Windows Server 2022](#).

3. Đã thêm các thành phần mới mới:

- Đã thêm [Một tác nhân tích hợp để tích hợp với Kaspersky Sandbox](#). *Giải pháp Kaspersky Sandbox* phát hiện và tự động chặn các mối đe dọa nâng cao trên máy tính. Kaspersky Sandbox sẽ phân tích hành vi của đối tượng để phát hiện hoạt động độc hại và hoạt động đặc trưng của các cuộc tấn công có chủ đích vào cơ sở hạ tầng CNTT của tổ chức. Kaspersky Sandbox sẽ phân tích và quét các đối tượng trên các máy chủ đặc biệt chứa các ảnh máy ảo được triển khai của hệ điều hành Microsoft Windows (máy chủ Kaspersky Sandbox). Để biết chi tiết về giải pháp này, hãy tham khảo [Trợ giúp của Kaspersky Sandbox](#).

Bạn không còn cần Kaspersky Endpoint Agent để sử dụng Kaspersky Sandbox nữa. Kaspersky Endpoint Security có thể thực hiện các chức năng của Kaspersky Endpoint Agent. Để chuyển các chính sách của Kaspersky Endpoint Agent, hãy sử dụng [Trình hướng dẫn chuyển đổi](#). Bạn cần Kaspersky Security Center 13.2 để tắt tất cả các chức năng của Kaspersky Sandbox hoạt động. Để biết chi tiết về việc chuyển đổi từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security cho Windows, vui lòng tham khảo [trợ giúp của ứng dụng](#).

- [Đã thêm tác nhân tích hợp để hỗ trợ hoạt động của giải pháp Kaspersky Endpoint Detection and Response Optimum](#). *Kaspersky Endpoint Detection and Response Optimum* là một giải pháp để bảo vệ cơ sở hạ tầng CNTT của tổ chức trước các mối đe dọa mạng nâng cao. Chức năng của giải pháp này kết hợp tính năng tự động phát hiện các mối đe dọa với khả năng phản ứng trước các mối đe dọa này để chống lại các cuộc tấn công nâng cao, bao gồm các cuộc tấn công khai thác mới, phần mềm tổng tiền, các cuộc tấn công không dùng tập tin, cũng như các phương pháp sử dụng các công cụ hệ thống hợp pháp. Để biết thêm thông tin về giải pháp này, hãy xem [Trợ giúp của Kaspersky Endpoint Detection and Response Optimum](#).

Bạn không còn cần Kaspersky Endpoint Agent để sử dụng Kaspersky Endpoint Detection and Response nữa. Kaspersky Endpoint Security có thể thực hiện các chức năng của Kaspersky Endpoint Agent. Để chuyển các chính sách và tác vụ của Kaspersky Endpoint Agent, hãy sử dụng [Trình hướng dẫn chuyển đổi](#). Để sử dụng tất cả các chức năng, Kaspersky Endpoint Detection and Response Optimum cần có Kaspersky Security Center 13.2. Để biết chi tiết về việc chuyển đổi từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security cho Windows, vui lòng tham khảo [trợ giúp của ứng dụng](#).

4. Đã thêm [Trình hướng dẫn chuyển đổi](#) cho các chính sách và tác vụ của Kaspersky Endpoint Agent. Trình hướng dẫn chuyển đổi sẽ tạo các chính sách và tác vụ mới được gộp cho Kaspersky Endpoint Security cho Windows. Trình hướng dẫn cho phép chuyển Detection and Response solutions từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security. Các giải pháp của Detection and Response bao gồm Kaspersky Sandbox, Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) và Kaspersky Managed Detection and Response (MDR).

5. [Kaspersky Endpoint Agent](#) kèm theo trong gói phân phối, được cập nhật lên phiên bản 3.11.

Khi nâng cấp Kaspersky Endpoint Security, ứng dụng sẽ phát hiện phiên bản và mục đích được chỉ định của Kaspersky Endpoint Agent. Nếu Kaspersky Endpoint Agent được chỉ định cho hoạt động của Kaspersky Sandbox, Kaspersky Managed Detection and Response (MDR) và Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) thì Kaspersky Endpoint Security sẽ chuyển hoạt động của tất cả các giải pháp này sang tác nhân tích hợp của ứng dụng. Đối với Kaspersky Sandbox và EDR Optimum, ứng dụng sẽ tự động gỡ bỏ Kaspersky Endpoint Agent. Đối với MDR, bạn có thể gỡ bỏ Kaspersky Endpoint Agent theo cách thủ công. Nếu ứng dụng được chỉ định cho hoạt động của Kaspersky Endpoint Detection và Response Expert (EDR Expert) thì Kaspersky Endpoint Security sẽ nâng cấp phiên bản của Kaspersky Endpoint Agent. Để biết thêm chi tiết về ứng dụng, vui lòng tham khảo tài liệu về các giải pháp của Kaspersky hỗ trợ Kaspersky Endpoint Agent.

6. Chức năng mã hóa BitLocker được cải tiến:

- Bây giờ bạn có thể sử dụng mã PIN cải tiến với [BitLocker Drive Encryption](#). Mã PIN cải tiến cho phép sử dụng các ký tự khác ngoài ký tự số: chữ cái Latinh viết hoa và viết thường, ký tự đặc biệt và dấu cách.
- Đã thêm một tính năng để [tắt xác thực BitLocker để nâng cấp hệ điều hành hoặc cài đặt các gói cập nhật](#). Việc cài đặt các bản cập nhật có thể yêu cầu khởi động lại máy tính nhiều lần. Để cài đặt đúng cách các bản cập nhật, bạn có thể tạm thời tắt xác thực BitLocker và bật lại xác thực sau khi cài đặt các bản cập nhật.
- Bây giờ bạn có thể [đặt thời gian hết hạn cho mật khẩu hoặc mã PIN mã hóa BitLocker](#). Khi mật khẩu hoặc mã PIN hết hạn, Kaspersky Endpoint Security sẽ nhắc người dùng nhập mật khẩu mới.

7. Bây giờ bạn có thể cấu hình số lần tối đa cấp phép cho bàn phím để Phòng chống Tấn công BadUSB. Khi đạt đến [số lượt thử nhập mã cấp phép không thành công được cấu hình](#), thiết bị USB sẽ tạm thời bị khóa.

8. Chức năng Tường lửa được cải tiến:

- Bây giờ bạn có thể cấu hình một dải địa chỉ IP cho [Quy tắc gói tin Tường lửa](#). Bạn có thể nhập một dải địa chỉ theo định dạng IPv4 hoặc IPv6. Ví dụ: 192.168.1.1-192.168.1.100 hoặc 12:34::2-12:34::99.
- Bây giờ bạn có thể nhập tên DNS cho [Quy tắc gói tin Tường lửa](#) thay vì địa chỉ IP. Bạn chỉ nên sử dụng tên DNS cho các máy tính mạng LAN hoặc các dịch vụ nội bộ. Tương tác với các dịch vụ đám mây (như Microsoft Azure) và các tài nguyên Internet khác nên được xử lý bởi thành phần Kiểm soát Web.

9. Tìm kiếm [Quy tắc kiểm soát web](#) được cải tiến. Để tìm kiếm quy tắc truy cập tài nguyên web, ngoài tên của quy tắc, bạn có thể sử dụng URL của trang web, tên người dùng, danh mục nội dung hoặc kiểu dữ liệu.

10. Tác vụ [Quét virus](#) đã được cải tiến:

- Tác vụ [Quét virus](#) ở chế độ rảnh đã được cải tiến. Nếu bạn đã khởi động lại máy tính trong quá trình quét, Kaspersky Endpoint Security sẽ tự động chạy tác vụ, tiếp tục từ thời điểm tác vụ quét bị gián đoạn.
- Tác vụ [Quét virus](#) đã được tối ưu hóa. Theo mặc định, Kaspersky Endpoint Security chỉ chạy quét khi máy tính đang rảnh. Bạn có thể cấu hình thời điểm chạy tác vụ quét máy tính trong thuộc tính tác vụ.

11. Bây giờ bạn có thể hạn chế quyền truy cập của người dùng vào dữ liệu được cung cấp bởi công cụ [Giám sát hoạt động ứng dụng](#). [Giám sát hoạt động ứng dụng](#) là một công cụ được thiết kế để xem thông tin về hoạt động của các ứng dụng trên máy tính người dùng theo thời gian thực. Quản trị viên có thể ẩn công cụ Giám sát hoạt động ứng dụng khỏi người dùng trong thuộc tính chính sách ứng dụng.

12. [Đã cải tiến tính bảo mật quản lý ứng dụng thông qua REST API](#). Giờ đây Kaspersky Endpoint Security sẽ kiểm tra chữ ký của các yêu cầu được gửi qua REST API. Để quản lý chương trình, bạn cần cài đặt một chứng chỉ nhận dạng yêu cầu.

Kaspersky Endpoint Security 11.6.0 cho Windows cung cấp các tính năng và cải tiến sau đây:

1. [Hỗ trợ cho Windows 10 21H1](#). 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](#).
2. [Đã thêm thành phần Managed Detection and Response](#). Thành phần này hỗ trợ tương tác với giải pháp có tên là Managed Detection and Response của Kaspersky. Managed Detection and Response (MDR) của Kaspersky cung cấp khả năng bảo vệ liên tục trước các mối đe dọa ngày càng nhiều và chúng có khả năng vượt qua cơ chế bảo vệ tự động. Đây là giải pháp dành cho các tổ chức gặp khó khăn trong việc tìm kiếm các chuyên gia có trình độ cao hoặc có nguồn lực nội bộ hạn chế. Để biết thông tin chi tiết về cách hoạt động của giải pháp này, vui lòng tham khảo Trợ giúp của Managed Detection and Response của Kaspersky.
3. [Kaspersky Endpoint Agent](#), được kèm theo trong gói phân phối, đã được cập nhật lên phiên bản 3.10. Kaspersky Endpoint Agent 3.10 cung cấp các tính năng mới, giải quyết một số vấn đề phát sinh trước đó và tăng cường tính ổn định. Để biết thêm chi tiết về ứng dụng, vui lòng tham khảo tài liệu về các giải pháp của Kaspersky hỗ trợ Kaspersky Endpoint Agent.
4. Bây giờ ứng dụng cung cấp khả năng quản lý bảo vệ để chống lại các cuộc tấn công như Làm nghẽn mạng và Quét cổng trong [Thiết lập Bảo vệ mối đe dọa mạng](#).
5. Đã thêm phương pháp mới để tạo quy tắc mạng cho Tường lửa. Bạn có thể [thêm quy tắc gói tin](#) và [quy tắc ứng dụng](#) cho các kết nối được hiển thị trong cửa sổ [Giám sát mạng](#). Tuy nhiên, các thiết lập kết nối của quy tắc mạng sẽ được cấu hình tự động.
6. Giao diện [Giám sát mạng](#) đã được cải tiến. Đã thêm thông tin về hoạt động mạng: ID tiến trình khởi tạo hoạt động mạng; loại mạng (mạng cục bộ hay mạng Internet); cổng cục bộ. Theo mặc định, thông tin về loại mạng bị ẩn.
7. Bây giờ ứng dụng đã có khả năng tự động tạo tài khoản Authentication Agent cho người dùng Windows mới. Agent cho phép người dùng hoàn tất xác thực để truy cập vào các ổ đĩa đã được [mã hóa bằng công nghệ Kaspersky Disk Encryption](#) và nạp hệ điều hành. Ứng dụng sẽ kiểm tra thông tin về tài khoản người dùng Windows trên máy tính. Nếu Kaspersky Endpoint Security phát hiện tài khoản người dùng Windows không có tài khoản Authentication Agent, ứng dụng sẽ tạo một tài khoản mới để truy cập các ổ đĩa được mã hóa. Điều này có nghĩa rằng bạn không cần phải [thêm tài khoản Authentication Agent theo cách thủ công](#) cho các máy tính có ổ đĩa đã được mã hóa.
8. Bây giờ ứng dụng đã có khả năng giám sát quá trình mã hóa ổ đĩa trong giao diện ứng dụng trên máy tính của người dùng (Kaspersky Disk Encryption và BitLocker). Bạn có thể chạy công cụ Giám sát mã hóa từ [cửa sổ chính của ứng dụng](#).

[Bản cập nhật 11.5.0](#)






Kaspersky Endpoint Security 11.5.0 cho Windows cung cấp các tính năng và cải tiến sau đây:

1. [Hỗ trợ cho Windows 10 20H2](#). 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](#).
2. [Giao diện ứng dụng](#) được cập nhật. Ngoài ra, [biểu tượng ứng dụng trong vùng thông báo](#), thông báo của ứng dụng và các hộp thoại cũng được cập nhật.
3. Cải tiến giao diện của tiện ích web Kaspersky Endpoint Security cho các thành phần Kiểm soát ứng dụng, Kiểm soát thiết bị và Kiểm soát thích ứng sự cố.
4. Thêm chức năng để nhập và xuất danh sách các quy tắc và loại trừ theo định dạng XML. Định dạng XML cho phép bạn chỉnh sửa danh sách sau khi chúng được xuất. Bạn chỉ có thể quản lý các danh sách trong Bảng điều khiển Kaspersky Security Center. Bạn có thể xuất/nhập các danh sách sau đây:
 - [Phát hiện hành vi \(danh sách loại trừ\)](#).
 - [Bảo vệ mỗi đe dọa web \(danh sách các địa chỉ web được tin tưởng\)](#).
 - [Bảo vệ mỗi đe dọa thư điện tử \(danh sách phần mở rộng bộ lọc tập tin đính kèm\)](#).
 - [Bảo vệ mỗi đe dọa mạng \(danh sách loại trừ\)](#).
 - [Tường lửa \(danh sách các quy tắc gói tin mạng\)](#).
 - [Kiểm soát ứng dụng \(danh sách quy tắc\)](#).
 - [Kiểm soát Web \(danh sách quy tắc\)](#).
 - [Giám sát cổng mạng \(danh sách cổng và ứng dụng được Kaspersky Endpoint Security giám sát\)](#).
 - [Kaspersky Disk Encryption \(danh sách loại trừ\)](#).
 - [Mã hóa ổ đĩa di động \(danh sách quy tắc\)](#).
5. Thông tin MD5 của đối tượng đã được thêm vào [báo cáo phát hiện mỗi đe dọa](#). Trong các phiên bản trước của ứng dụng, Kaspersky Endpoint Security chỉ hiển thị giá trị SHA256 của một đối tượng.
6. Đã thêm khả năng [gán mức ưu tiên cho các quy tắc truy cập thiết bị](#) trong thiết lập Kiểm soát thiết bị. Gán mức ưu tiên cho phép cấu hình quyền truy cập của người dùng vào thiết bị linh hoạt hơn. Nếu một người dùng đã được thêm vào nhiều nhóm, Kaspersky Endpoint Security sẽ điều chỉnh quyền truy cập của thiết bị dựa trên quy tắc có mức ưu tiên cao nhất. Ví dụ: bạn có thể cấp quyền chỉ đọc cho nhóm Mọi người và cấp quyền đọc/ghi cho nhóm quản trị viên. Để làm như vậy, hãy gán mức ưu tiên bằng 0 cho nhóm quản trị viên và gán mức ưu tiên bằng 1 cho nhóm Mọi người. Bạn chỉ có thể cấu hình mức ưu tiên cho các thiết bị có hệ thống tập tin. Chúng bao gồm ổ đĩa cứng, ổ đĩa di động, ổ đĩa mềm, ổ CD/DVD và thiết bị di động (MTP).
7. Đã thêm chức năng mới:
 - [Quản lý thông báo bằng âm thanh](#).
 - Tối ưu chi phí mạng của Kaspersky Endpoint Security giới hạn lưu lượng mạng của chính nó nếu kết nối Internet bị hạn chế (ví dụ: thông qua kết nối di động).

- [Quản lý thiết lập Kaspersky Endpoint Security thông qua các ứng dụng quản trị từ xa được tin tưởng](#) (ví dụ như ứng dụng TeamViewer, LogMeIn và Remotely Anywhere). Bạn có thể sử dụng các ứng dụng quản trị từ xa để khởi động Kaspersky Endpoint Security và quản lý thiết lập trong giao diện ứng dụng.
 - [Quản lý thiết lập để quét lưu lượng bảo mật trong Firefox và Thunderbird](#). Bạn có thể chọn kho chứng chỉ sẽ được Mozilla sử dụng: kho chứng chỉ Windows hoặc kho chứng chỉ Mozilla. Chức năng này chỉ khả dụng cho các máy tính không có chính sách được áp dụng. Nếu một chính sách đang được áp dụng cho máy tính, Kaspersky Endpoint Security sẽ tự động cho phép sử dụng kho chứng chỉ Windows trong Firefox và Thunderbird.
8. Đã thêm khả năng [cấu hình chế độ quét lưu lượng bảo mật](#): luôn quét lưu lượng ngay cả khi các thành phần bảo vệ bị tắt hoặc quét lưu lượng khi các thành phần bảo vệ yêu cầu.
 9. Đã sửa đổi quy trình [xóa thông tin khỏi báo cáo](#). Một người dùng chỉ có thể xóa tất cả các báo cáo. Trong các phiên bản trước của ứng dụng, người dùng có thể chọn các thành phần ứng dụng cụ thể có thông tin bị xóa khỏi báo cáo.
 10. Đã sửa đổi quy trình [nhập tập tin cấu hình chứa thiết lập Kaspersky Endpoint Security](#) và sửa đổi quy trình [khôi phục thiết lập ứng dụng](#). Trước khi nhập hoặc khôi phục, Kaspersky Endpoint Security sẽ chỉ hiển thị cảnh báo. Trong các phiên bản trước của ứng dụng, bạn có thể xem các giá trị của thiết lập mới trước khi chúng được áp dụng.
 11. Đơn giản hóa [quy trình khôi phục quyền truy cập vào ổ đĩa đã được mã hóa bằng BitLocker](#). Sau khi hoàn tất quy trình khôi phục quyền truy cập, Kaspersky Endpoint Security sẽ nhắc người dùng đặt mật khẩu hoặc mã PIN mới. Sau khi đặt mật khẩu mới, BitLocker sẽ mã hóa ổ đĩa. Trong phiên bản trước của ứng dụng, người dùng phải đặt lại mật khẩu theo cách thủ công trong thiết lập của BitLocker.
 12. Giờ đây, người dùng có khả năng tạo [vùng tin tưởng](#) cục bộ của riêng họ cho một máy tính cụ thể. Bằng cách này, người dùng có thể tạo danh sách [loại trừ](#) cục bộ của riêng họ và các [ứng dụng được tin tưởng](#) ngoài vùng tin tưởng chung trong một chính sách. Quản trị viên có thể cho phép hoặc chặn việc sử dụng các loại trừ cục bộ hoặc các ứng dụng được tin tưởng cục bộ. Quản trị viên có thể sử dụng Kaspersky Security Center để xem, thêm, chỉnh sửa hoặc xóa các mục danh sách trong thuộc tính máy tính.
 13. Đã thêm khả năng [nhập nhận xét trong thuộc tính của ứng dụng được tin tưởng](#). Nhận xét giúp đơn giản hóa việc tìm kiếm và sắp xếp các ứng dụng được tin tưởng.
 14. [Quản lý ứng dụng thông qua REST API](#):
 - Bây giờ bạn có thể cấu hình thiết lập của phần mở rộng Bảo vệ mối đe dọa thư điện tử cho Outlook.
 - Không được phép tắt tính năng phát hiện vi rút, sâu và Trojan.

[Bản cập nhật 11.4.0](#)

Kaspersky Endpoint Security 11.4.0 cho Windows cung cấp các tính năng và cải tiến sau đây:

1. Thiết kế mới của [biểu tượng ứng dụng trong vùng thông báo của thanh tác vụ](#). Bây giờ biểu tượng  mới đã được hiển thị thay vì biểu tượng  cũ. Nếu người dùng phải thực hiện một hành động (ví dụ: khởi động lại máy tính sau khi cập nhật ứng dụng), biểu tượng này sẽ thay đổi thành . Nếu các thành phần bảo vệ của ứng dụng bị tắt hoặc bị trục trặc, biểu tượng sẽ thay đổi thành  hoặc . Nếu bạn di con trỏ chuột qua trên biểu tượng, Kaspersky Endpoint Security sẽ hiển thị mô tả sự cố về bảo vệ máy tính.
2. Kaspersky Endpoint Agent, được kèm theo trong gói phân phối, đã được cập nhật lên phiên bản 3.9. Kaspersky Endpoint Agent 3.9 hỗ trợ tích hợp với các giải pháp mới của Kaspersky. Để biết thêm chi tiết về ứng dụng, vui lòng tham khảo tài liệu về các giải pháp của Kaspersky hỗ trợ Kaspersky Endpoint Agent.
3. Thêm trạng thái *Không được giấy phép hỗ trợ* cho các thành phần Kaspersky Endpoint Security. Bạn có thể xem trạng thái của các thành phần trong danh sách thành phần trong [cửa sổ chính của ứng dụng](#).
4. Các sự kiện mới từ [Phòng chống khai thác](#) đã được thêm vào [báo cáo](#).
5. Bây giờ các ổ đĩa cho [công nghệ Kaspersky Disk Encryption](#) đã được thêm tự động vào Windows Recovery Environment (WinRE) khi bắt đầu mã hóa ổ đĩa. Phiên bản trước của Kaspersky Endpoint Security đã thêm các ổ đĩa khi cài đặt ứng dụng. Việc thêm ổ đĩa vào WinRE có thể tăng tính ổn định của ứng dụng khi khôi phục hệ điều hành trên các máy tính được bảo vệ bằng công nghệ Kaspersky Disk Encryption.

Thành phần Cảm biến điểm cuối đã bị xóa khỏi Kaspersky Endpoint Security. Bạn vẫn có thể cấu hình thiết lập Cảm biến điểm cuối trong chính sách với điều kiện Kaspersky Endpoint Security phiên bản 11.0.0 đến 11.3.0 được cài đặt trên máy tính.

Các câu hỏi thường gặp



TỔNG QUÁT

[Kaspersky Endpoint Security có thể hoạt động trên các máy tính nào?](#)

[Phiên bản gần đây nhất đã có những thay đổi gì?](#)

[Kaspersky Endpoint Security có thể hoạt động với các ứng dụng nào khác của Kaspersky?](#)

[Làm cách nào để tôi tiết kiệm tài nguyên máy tính trong quá trình hoạt động của Kaspersky Endpoint Security?](#)



TRIỂN KHAI

[Làm cách nào để tôi cài đặt Kaspersky Endpoint Security lên tất cả máy tính của một tổ chức?](#)



INTERNET

[Kaspersky Endpoint Security có quét các kết nối được mã hóa \(HTTPS\) không?](#)

[Làm cách nào để tôi cho phép người dùng chỉ được kết nối với các mạng Wi-Fi được tin tưởng?](#)

[Làm cách nào để tôi chặn mạng xã hội?](#)



NHỮNG ỨNG DỤNG

[Làm cách nào để tôi biết được những ứng dụng nào được cài đặt trên máy tính của người dùng \(kiểm kê\)?](#)

[Làm cách nào để tôi chặn hoạt động của các trò chơi máy tính?](#)

[Có thể cấu hình các thiết lập cài đặt nào trong dòng lệnh?](#)

[Làm cách nào để tôi gỡ bỏ hoàn toàn Kaspersky Endpoint Security?](#)



CẬP NHẬT

[Có những phương thức khả dụng nào để cập nhật cơ sở dữ liệu?](#)

[Tôi nên làm gì nếu có vấn đề phát sinh sau một bản cập nhật?](#)

[Làm cách nào để tôi cập nhật cơ sở dữ liệu bên ngoài mạng của doanh nghiệp?](#)

[Có thể sử dụng máy chủ proxy để cập nhật hay không?](#)



BẢO MẬT

[Kaspersky Endpoint Security quét email bằng cách nào?](#)

[Làm cách nào để tôi loại trừ một tập tin được tin tưởng ra khỏi tác vụ quét?](#)

[Làm cách nào để tôi bảo vệ một máy tính không bị nhiễm virus từ ổ đĩa flash?](#)

[Làm cách nào tôi có thể chạy tác vụ quét virus bị ẩn đối với người dùng?](#)

[Làm cách nào để tôi tạm dừng chức năng bảo vệ của Kaspersky Endpoint Security?](#)

[Làm cách nào để tôi khôi phục một tập tin bị Kaspersky Endpoint Security xóa nhầm?](#)

[Làm cách nào để tôi ngăn một người dùng gỡ bỏ Kaspersky Endpoint Security?](#)

[Làm cách nào để tôi xác minh Kiểm soát ứng dụng đã được cấu hình đúng?](#)

[Làm cách nào để tôi thêm một ứng dụng vào danh sách được tin tưởng?](#)



THIẾT BỊ

[Làm cách nào để chặn sử dụng các ổ đĩa flash?](#)

[Làm cách nào để tôi thêm một thiết bị vào danh sách được tin tưởng?](#)

[Có thể lấy quyền truy cập đến một thiết bị bị chặn không?](#)



MÃ HÓA

[Trong những điều kiện nào thì không thể mã hóa?](#)

[Làm cách nào để tôi sử dụng một mật khẩu để hạn chế truy cập đến một tập tin nén?](#)

[Có thể sử dụng thẻ thông minh và token với tính năng mã hóa hay không?](#)

[Có thể lấy quyền truy cập dữ liệu được mã hóa nếu không có kết nối với Kaspersky Security Center hay không?](#)

[Tôi nên làm gì nếu hệ điều hành của máy tính bị lỗi trong khi dữ liệu vẫn được mã hóa?](#)



HỖ TRỢ

[Tập tin báo cáo được lưu trữ ở đâu?](#)


[Làm cách nào để tôi tạo một tập tin dấu vết?](#)

[Làm cách nào để tôi cho phép ghi tập tin kết xuất?](#)

Kaspersky Endpoint Security cho Windows

Kaspersky Endpoint Security cho Windows (sau đây còn được gọi là 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.

Các công nghệ phát hiện mối đe dọa

<p> Machine learning</p> <p>Kaspersky Endpoint Security sẽ sử dụng một mô hình dựa trên máy học. Mô hình này được phát triển bởi các chuyên gia Kaspersky. Sau đó, mô hình liên tục được nạp dữ liệu về mối đe dọa từ KSN (huấn luyện mô hình).</p> <p> Cloud analysis</p> <p>Kaspersky Endpoint Security sẽ nhận dữ liệu về mối đe dọa từ Kaspersky Security Network. <i>Kaspersky Security Network (KSN)</i> 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.</p> <p> Expert analysis</p> <p>Kaspersky Endpoint Security sẽ sử dụng dữ liệu về mối đe dọa được bổ sung bởi chuyên gia phân tích virus của Kaspersky. Các chuyên gia phân tích virus sẽ đánh giá các đối tượng nếu không thể xác định danh tiếng của một đối tượng một cách tự động.</p>	<p> Behavior analysis</p> <p>Kaspersky Endpoint Security sẽ phân tích hoạt động của đối tượng theo thời gian thực.</p> <p> Automatic analysis</p> <p>Kaspersky Endpoint Security sẽ nhận dữ liệu từ hệ thống phân tích đối tượng tự động. Hệ thống sẽ xử lý tất cả các đối tượng được gửi đến Kaspersky. Sau đó, hệ thống sẽ xác định danh tiếng của đối tượng và thêm dữ liệu vào cơ sở dữ liệu chống virus. Nếu không thể xác định danh tiếng của đối tượng, hệ thống sẽ tham vấn chuyên gia phân tích virus của Kaspersky.</p> <p> Kaspersky Sandbox</p> <p>Kaspersky Endpoint Security sẽ xử lý đối tượng trên một máy ảo. Kaspersky Sandbox sẽ phân tích hành vi của đối tượng và quyết định theo danh tiếng của đối tượng đó. Công nghệ này chỉ khả dụng nếu bạn đang sử dụng giải pháp Kaspersky Sandbox.</p>
---	--

Cây lựa chọn

Mỗi loại mối đe dọa đều được xử lý bởi một thành phần chuyên dụng. Các thành phần có thể được bật hoặc tắt độc lập, và các thiết lập của chúng có thể được cấu hình.

Cây lựa chọn

Phần	Thành phần
Bảo vệ mối đe dọa thiết yếu	Bảo vệ mối đe dọa tập tin



Thành phần Bảo vệ mối đe dọa tập tin cho phép bạn ngăn chặn nguy cơ nhiễm mã độc cho hệ thống tập tin của máy tính. Theo mặc định, thành phần Bảo vệ mối đe dọa tập tin sẽ chạy thường trực trong RAM của máy tính. Thành phần này quét các tập tin trên tất cả các ổ đĩa của máy tính cũng như trên các ổ đĩa được kết nối. Thành phần này giúp bảo vệ máy tính với sự trợ giúp của cơ sở dữ liệu diệt virus, [dịch vụ đám mây của Kaspersky Security Network](#) và phân tích theo hành vi.

Bảo vệ mối đe dọa web

Thành phần Bảo vệ mối đe dọa web ngăn các bản tải xuống tập tin độc hại từ mạng Internet và cũng chặn các website độc hại và lừa đảo. Thành phần này giúp bảo vệ máy tính với sự trợ giúp của cơ sở dữ liệu diệt virus, [dịch vụ đám mây của Kaspersky Security Network](#) và phân tích theo hành vi.

Bảo vệ mối đe dọa thư điện tử

Thành phần Bảo vệ mối đe dọa thư điện tử sẽ quét các tập tin đính kèm của email đến và đi để phát hiện virus và các mối đe dọa khác. Thành phần này cũng quét các thư điện tử để tìm các liên kết độc hại và lừa đảo. Theo mặc định, thành phần Bảo vệ mối đe dọa thư điện tử sẽ chạy thường trực trong RAM của máy tính và quét tất cả các thư được nhận hoặc được gửi bằng các giao thức POP3, SMTP, IMAP hoặc NNTP hoặc ứng dụng thư khách Microsoft Office Outlook (MAPI). Thành phần này giúp bảo vệ máy tính với sự trợ giúp của cơ sở dữ liệu diệt virus, [dịch vụ đám mây của Kaspersky Security Network](#) và phân tích theo hành vi.

Bảo vệ mối đe dọa mạng

Thành phần Bảo vệ mối đe dọa mạng sẽ quét lưu lượng mạng vào để phát hiện các hoạt động tương tự với các cuộc tấn công mạng. Khi Kaspersky Endpoint Security phát hiện một nỗ lực tấn công mạng vào máy tính của người dùng, ứng dụng sẽ chặn kết nối mạng với 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 Bảo vệ mối đe dọa mạng phát hiện sẽ được cập nhật trong [bản cập nhật cơ sở dữ liệu và mô-đun ứng dụng](#).

Tường lửa

Tường lửa chặn các kết nối trái phép đến máy tính khi đang làm việc trên Internet hoặc mạng cục bộ. Tường lửa cũng kiểm soát hoạt động mạng của các ứng dụng trên máy tính. Điều này cho phép bạn bảo vệ mạng LAN công ty trước hành vi trộm danh tính và các cuộc tấn công khác. Thành phần này giúp bảo vệ máy tính với sự trợ giúp của cơ sở dữ liệu diệt virus, dịch vụ đám mây của Kaspersky Security Network và các *quy tắc mạng* được xác định trước.

Phòng chống Tấn công BadUSB

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.

Bảo vệ AMSI

Thành phần Bảo vệ AMSI được dành để hỗ trợ Antimalware Scan Interface của Microsoft. *Antimalware Scan Interface (AMSI)* cho phép các ứng dụng thuộc bên thứ ba có hỗ trợ AMSI gửi các đối tượng (ví dụ như kịch bản PowerShell) đến Kaspersky Endpoint Security để quét bổ sung và sau đó nhận kết quả từ việc quét cho các đối tượng này.

**Bảo vệ
mối đe
dọa nâng
cao**

Kaspersky Security Network



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. Nếu bạn đang tham gia vào Kaspersky Security Network, các dịch vụ KSN sẽ cung cấp cho Kaspersky Endpoint Security thông tin về danh mục và danh tiếng của các tập tin được quét, cũng như thông tin về danh tiếng của các địa chỉ trang web được quét.

Phát hiện hành vi

Thành phần Phát hiện hành vi nhận dữ liệu về hành động của các ứng dụng trên máy tính của bạn và cung cấp thông tin này đến các thành phần bảo vệ khác để cải thiện hiệu quả của chúng. Thành phần Phát hiện hành vi sử dụng Dấu hiệu dòng hành vi (BSS) cho các ứng dụng. Nếu hoạt động của ứng dụng khớp với một dấu hiệu dòng hành vi cụ thể, Kaspersky Endpoint Security sẽ thực hiện hành động phản ứng được chọn. Chức năng của Kaspersky Endpoint Security dựa trên các dấu hiệu dòng hành vi cung cấp chủ động bảo vệ cho máy tính.

Phòng chống khai thác

Thành phần Phòng chống khai thác sẽ phát hiện mã chương trình lợi dụng các lỗ hổng trên máy tính để khai thác quyền của quản trị viên hoặc thực hiện các hoạt động độc hại. Ví dụ như mã khai thác có thể sử dụng một cuộc tấn công tràn bộ đệm. Để thực hiện, mã khai thác sẽ gửi số lượng lớn dữ liệu đến một ứng dụng chứa lỗ hổng. Khi xử lý dữ liệu này, ứng dụng chứa lỗ hổng bảo mật sẽ thực thi mã độc. Kết quả của cuộc tấn công này là mã khai thác có thể tiến hành cài đặt trái phép phần mềm độc hại. Khi có một nỗ lực chạy một tập tin thực thi từ một ứng dụng có lỗ hổng bảo mật không được thực hiện bởi người dùng, Kaspersky Endpoint Security sẽ chặn việc khởi chạy tập tin đó hoặc thông báo cho người dùng.

Phòng chống xâm nhập máy chủ

Thành phần Phòng chống xâm nhập máy chủ 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 cá nhân. Thành phần này giúp bảo vệ máy tính với sự trợ giúp của cơ sở dữ liệu diệt virus và dịch vụ đám mây của Kaspersky Security Network.

Công cụ khắc phục

Công cụ khắc phục cho phép Kaspersky Endpoint Security có thể hoàn tác các hành động đã được thực hiện bởi phần mềm độc hại trong hệ điều hành.

Kiểm soát bảo mật



Kiểm soát ứng dụng

Thành phần Kiểm soát ứng dụng quản lý việc khởi động ứng dụng trên máy tính của người dùng. Điều này cho phép bạn thực hiện chính sách bảo mật của công ty khi sử dụng các ứng dụng. Thành phần Kiểm soát ứng dụng cũng làm giảm nguy cơ lây nhiễm máy tính bằng cách hạn chế quyền truy cập vào các ứng dụng.

Kiểm soát Thiết bị

Kiểm soát thiết bị quản lý quyền truy cập của người dùng đến các thiết bị được cài đặt trên máy tính hoặc kết nối với máy tính (ví dụ, ổ cứng, camera, hoặc mô-đun Wi-Fi). Việc này cho phép bạn bảo vệ máy tính khỏi bị nhiễm độc khi các thiết bị đó được kết nối, và ngăn thất thoát hoặc rò rỉ dữ liệu.

Kiểm soát Web

Kiểm soát Web quản lý quyền truy cập của người dùng đối với các tài nguyên web. Điều này giúp giảm lưu lượng và việc sử dụng không hợp lý thời gian làm việc. Khi người dùng cố mở một trang web bị hạn chế bởi thành phần Kiểm soát Web thì Kaspersky Endpoint Security sẽ chặn quyền truy cập hoặc hiển thị một cảnh báo.

Kiểm soát thích ứng sự cố

Thành phần Kiểm soát thích ứng sự cố sẽ giám sát và chặn các hành động mà các máy tính trong mạng công ty ít có khả năng thực hiện. Kiểm soát thích ứng sự cố sử dụng một bộ quy tắc để theo dõi các hành vi khác biệt (ví dụ, quy tắc *Khởi động Microsoft PowerShell từ ứng dụng văn phòng*). Các quy tắc này được tạo bởi các chuyên gia của Kaspersky dựa trên các tình huống hoạt động độc hại thông thường. Bạn có thể cấu hình cách Kiểm soát thích ứng sự cố xử lý từng quy tắc và, chẳng hạn, cho phép thực thi các kịch bản PowerShell tự động hóa một số tác vụ dòng công việc nhất định. Kaspersky Endpoint Security cập nhật ộ quy tắc cùng với các cơ sở dữ liệu ứng dụng.

Tác vụ



Quét virus

Kaspersky Endpoint Security sẽ quét máy tính để tìm virus và các mối đe dọa khác. Tác vụ Quét virus này giúp loại trừ nguy cơ phân tán phần mềm độc hại không được phát hiện bởi các thành phần bảo vệ, chẳng hạn như do cấu hình bảo mật thấp.

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. 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.

Lần hoàn tác bản cập nhật gần nhất

Kaspersky Endpoint Security sẽ khôi phục lại bản cập nhật cơ sở dữ liệu và mô-đun gần nhất. Điều này cho phép bạn hoàn tác cơ sở dữ liệu và mô-đun ứng dụng về phiên bản trước đó khi cần thiết, 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.

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.

Mã hóa dữ liệu



Mã hóa mức độ tập tin

Thành phần này cho phép tạo các quy tắc mã hóa tập tin. Bạn có thể chọn các thư mục được xác định trước để mã hóa, chọn một thư mục theo cách thủ công hoặc chọn riêng từng tập tin theo phần mở rộng.

Mã hóa toàn bộ ổ đĩa

Thành phần này cho phép mã hóa ổ đĩa cứng bằng cách sử dụng Kaspersky Disk Encryption hoặc BitLocker Drive Encryption.

Mã hóa ổ đĩa di động

Thành phần này cho phép bảo vệ dữ liệu trên các ổ đĩa di động. Bạn có thể sử dụng Mã hóa toàn bộ đĩa (FDE) hoặc Mã hóa mức độ tập tin (FLE).

Detection and Response



Endpoint Detection and Response Optimum

Tác nhân tích hợp cho giải pháp Kaspersky Endpoint Detection and Response Optimum (sau đây gọi là "EDR Optimum"). *Kaspersky Endpoint Detection and Response* là một giải pháp để bảo vệ cơ sở hạ tầng CNTT của doanh nghiệp trước các mối đe dọa mạng nâng cao. Chức năng của giải pháp này kết hợp tính năng tự động phát hiện các mối đe dọa với khả năng phản ứng trước các mối đe dọa này để chống lại các cuộc tấn công nâng cao, bao gồm các cuộc tấn công khai thác mới, phần mềm tống tiền, các cuộc tấn công không dùng tập tin, cũng như các phương pháp sử dụng các công cụ hệ thống hợp pháp. Để biết thêm thông tin về giải pháp này, hãy xem [Trợ giúp của Kaspersky Endpoint Detection and Response Optimum](#).

Endpoint Detection and Response Expert

Tác nhân tích hợp cho giải pháp Kaspersky Endpoint Detection and Response Expert (sau đây gọi là "EDR Expert"). EDR Expert cung cấp nhiều chức năng giám sát và phản ứng trước mối đe dọa hơn EDR Optimum. Để biết thêm thông tin về giải pháp này, hãy xem [Trợ giúp của Kaspersky Endpoint Detection and Response Expert](#).

Kaspersky Sandbox

Tác nhân tích hợp cho giải pháp Kaspersky Sandbox. *Giải pháp Kaspersky Sandbox* phát hiện và tự động chặn các mối đe dọa nâng cao trên máy tính. Kaspersky Sandbox sẽ phân tích hành vi của đối tượng để phát hiện hoạt động độc hại và hoạt động đặc trưng của các cuộc tấn công có chủ đích vào cơ sở hạ tầng CNTT của tổ chức. Kaspersky Sandbox sẽ phân tích và quét các đối tượng trên các máy chủ đặc biệt chứa các ảnh máy ảo được triển khai của hệ điều hành Microsoft Windows (máy chủ Kaspersky Sandbox). Để biết chi tiết về giải pháp này, hãy tham khảo [Trợ giúp của Kaspersky Sandbox](#).

Managed Detection and Response

Tác nhân tích hợp để hỗ trợ hoạt động của giải pháp Managed Detection and Response của Kaspersky. Giải pháp *Managed Detection and Response (MDR) của Kaspersky* sẽ tự động phát hiện và phân tích các sự cố bảo mật trong cơ sở hạ tầng của bạn. Để thực hiện, MDR sử dụng dữ liệu đo từ xa nhận được từ các điểm cuối và công nghệ máy học. MDR sẽ gửi dữ liệu sự cố cho các chuyên gia của Kaspersky. Sau đó, các chuyên gia có thể xử lý sự cố, ví dụ như thêm một mục mới vào Cơ sở dữ liệu chống virus. Ngoài ra, các chuyên gia có thể đưa ra các khuyến nghị về cách xử lý sự cố, ví dụ như đề xuất cách ly máy tính khỏi mạng. Để biết thông tin chi tiết về cách hoạt động của giải pháp này, vui lòng tham khảo [Trợ giúp của Managed Detection and Response của Kaspersky](#).

Chức năng dịch vụ của ứng dụng

Kaspersky Endpoint Security bao gồm một số chức năng dịch vụ. Chức năng dịch vụ được cung cấp để giữ cho ứng dụng luôn được cập nhật, 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. Bạn cũng có thể sử dụng các báo cáo để theo dõi kết quả của tác vụ được hoàn tất. Báo cáo này chứa một danh sách các sự kiện xảy ra trong hoạt động của Kaspersky Endpoint Security và mọi hoạt động được ứng dụng thực hiện. 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.
- **Sao lưu.** Nếu ứng dụng phát hiện các tập tin 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 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 mối đe dọa đang hoạt động*. Bạn có thể quét các tập tin, khôi phục các tập tin về thư mục gốc, và xóa sạch kho lưu trữ dữ liệu.
- **Thông báo.** Dịch vụ thông báo giúp người dùng theo dõi các sự kiện ảnh hưởng đến trạng thái bảo vệ của máy tính và 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 sử dụng thông tin về danh tiếng các tập tin, tài nguyên web, và phần mềm được tiếp nhận trong thời gian thực từ người dùng trên toàn thế giới.
- **Giấy phép.** 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 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 đến bộ phận Hỗ trợ kỹ thuật của Kaspersky qua cổng thông tin Kaspersky CompanyAccount hoặc gọi điện thoại đến Hỗ trợ kỹ thuật.

Gói phân phối

Bộ công cụ phân phối bao gồm các gói phân phối sau:

- **Mã hóa mạnh (AES256)**

Gói phân phối này chứa các công cụ mật mã để triển khai thuật toán mã hóa AES (Tiêu chuẩn mã hóa nâng cao) với độ dài khóa hiệu quả là 256 bit.

- **Mã hóa nhẹ (AES56)**

Gói phân phối này chứa các công cụ mật mã để triển khai thuật toán mã hóa AES với độ dài khóa hiệu quả là 56 bit.

Mỗi gói phân phối chứa các tập tin sau:

kes_win.msi	Gói cài đặt Kaspersky Endpoint Security.
setup_kes.exe	Các tập tin cần thiết cho việc cài đặt ứng dụng sử dụng bất kỳ phương thức khả dụng nào.
kes_win.kud	Các tập tin để tạo một gói cài đặt cho Kaspersky Endpoint Security .
klcfginst.msi	Gói cài đặt Tiện ích quản lý Kaspersky Endpoint Security cho Kaspersky Security Center.
bases.cab	Các tập tin trong gói cập nhật được sử dụng trong quá trình cài đặt.
cleaner.cab	Các tập tin để gỡ bỏ phần mềm không tương thích.
incompatible.txt	Tập tin chứa một danh sách các phần mềm không tương thích.
ksn_<language_ID>.txt	Tập tin trong đó bạn có thể đọc các điều khoản tham gia vào Kaspersky Security Network.
license.txt	Tập tin nơi bạn có thể đọc toàn bộ Thỏa thuận giấy phép người dùng cuối và Chính sách quyền riêng tư.
installer.ini	Tập tin chứa cấu hình nội bộ của gói phân phối.
keswin_web_plugin.zip	Tập tin nén chứa các tập tin cần thiết để cài đặt tiện ích web Kaspersky Endpoint Security .

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](#).

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 đĩa trống trên ổ đĩa cứng;
- CPU:
 - Máy trạm: 1 GHz;
 - Máy chủ: 1.4 GHz;
 - Hỗ trợ tập lệnh SSE2.
- RAM:
 - Máy trạm (x86): 1 GB;
 - Máy trạm (x64): 2 GB;
 - Máy chủ: 2 GB.

Máy trạm

Các hệ điều hành được hỗ trợ cho máy trạm:

- 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 / Pro for Workstations / Education / Enterprise / Enterprise multi-session;
- - Windows 11 Home / Pro / Pro for Workstations / 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](#).

Để biết thêm chi tiết về việc hỗ trợ cho hệ điều hành Microsoft Windows 11, vui lòng tham khảo [Kiến thức cơ bản của Hỗ trợ kỹ thuật](#).

Máy chủ

Kaspersky Endpoint Security hỗ trợ cho các thành phần cốt lõi của ứng dụng trên máy tính chạy hệ điều hành Windows dành cho máy chủ. Bạn có thể sử dụng Kaspersky Endpoint Security cho Windows thay vì Kaspersky Security cho Windows Server trên các máy chủ và cụm máy chủ trong tổ chức của bạn. Chế độ Core được hỗ trợ nhưng có những [hạn chế](#).

Các hệ điều hành được hỗ trợ cho máy chủ:

- Windows Small Business Server 2011 Essentials / Standard (64-bit);

Microsoft Small Business Server 2011 Standard (64-bit) chỉ được hỗ trợ nếu Service Pack 1 cho Microsoft Windows Server 2008 R2 được cài đặt.

- Windows MultiPoint Server 2011 (64-bit);
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 hoặc mới hơn;
- 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;
- Windows Server 2022.

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](#).

Để biết thêm chi tiết về việc hỗ trợ cho hệ điều hành Microsoft Windows Server 2022, vui lòng tham khảo [Kiến thức cơ bản của Hỗ trợ kỹ thuật](#).

Máy chủ đầu cuối

Các loại máy chủ đầu cuối được hỗ trợ:

- Microsoft Remote Desktop Services dựa trên Windows Server 2008 R2 SP1;
- Microsoft Remote Desktop Services dựa trên Windows Server 2012;
- Microsoft Remote Desktop Services dựa trên Windows Server 2012 R2;
- Microsoft Remote Desktop Services dựa trên Windows Server 2016;
- Microsoft Remote Desktop Services dựa trên Windows Server 2019.

Nền tảng ảo

Các nền tảng ảo được hỗ trợ:

- VMware Workstation 16.2.2 Pro;
- VMware ESXi 7.0 Update 3b;
- Microsoft Hyper-V Server 2019;
- Citrix Virtual Apps và Desktops 7 2112;

- Citrix Provisioning 2112;
- Citrix Hypervisor 8.2.

Kaspersky Endpoint Security hỗ trợ hoạt động với các phiên bản sau của Kaspersky Security Center:

- Kaspersky Security Center 11;
- Kaspersky Security Center 12;
- Kaspersky Security Center 12 Patch A;
- Kaspersky Security Center 12 Patch B;
- Kaspersky Security Center 13;
- Kaspersky Security Center 13.1;
- Kaspersky Security Center 13.2;
- Kaspersky Security Center 13.2.2.

So sánh các tính năng ứng dụng có sẵn tùy thuộc vào loại hệ điều hành

Nhóm tính năng Kaspersky Endpoint Security khả dụng tùy thuộc vào loại hệ điều hành: máy trạm hoặc máy chủ (xem bảng dưới đây).

So sánh các tính năng của Kaspersky Endpoint Security

Tính năng	Máy trạm	Máy chủ
Bảo vệ mỗi đe dọa nâng cao		
Kaspersky Security Network	✓	✓
Phát hiện hành vi	✓	✓
Phòng chống khai thác	✓	✓
Phòng chống xâm nhập máy chủ	✓	-
Công cụ khắc phục	✓	✓
Bảo vệ mỗi đe dọa thiết yếu		
Bảo vệ mỗi đe dọa tập tin	✓	✓
Bảo vệ mỗi đe dọa web	✓	✓
Bảo vệ mỗi đe dọa thư điện tử	✓	✓
Tường lửa	✓	✓
Bảo vệ mỗi đe dọa mạng	✓	✓
Phòng chống Tấn công BadUSB	✓	✓
Bảo vệ AMSI	✓	✓

Kiểm soát bảo mật		
Kiểm soát ứng dụng	✓	✓
Kiểm soát Thiết bị	✓	✓
Kiểm soát Web	✓	✓
Kiểm soát thích ứng sự cố	✓	-
Mã hóa dữ liệu		
Kaspersky Disk Encryption	✓	-
BitLocker Drive Encryption	✓	✓
Mã hóa mức độ tập tin	✓	-
Mã hóa ổ đĩa di động	✓	-
Detection and Response		
Endpoint Detection and Response Optimum	✓	✓
Endpoint Detection and Response Expert	✓	✓
Kaspersky Sandbox	✓	✓
Managed Detection and Response (MDR)	✓	✓

Việc so sánh các chức năng ứng dụng phụ thuộc vào các công cụ quản lý

Nhóm chức năng khả dụng trong Kaspersky Endpoint Security phụ thuộc vào các công cụ quản lý (xem bảng bên dưới).

Bạn có thể quản lý ứng dụng bằng các bảng điều khiển sau của Kaspersky Security Center:

- Bảng điều khiển quản trị. Phần đính kèm của Microsoft Management Console (MMC) được cài đặt trên máy trạm của quản trị viên.
- Bảng điều khiển web. Thành phần của Kaspersky Security Center được cài đặt trên Máy chủ quản trị. Bạn cũng có thể làm việc trên Bảng điều khiển web thông qua một trình duyệt trên bất kỳ máy tính nào có quyền truy cập đến Máy chủ quản trị.

Bạn cũng có thể quản lý ứng dụng bằng cách sử dụng Bảng điều khiển đám mây Kaspersky Security Center. *Bảng điều khiển đám mây Kaspersky Security Center* là phiên bản đám mây của Kaspersky Security Center. Điều này có nghĩa là Máy chủ quản trị và các thành phần khác của Kaspersky Security Center được cài đặt trong cơ sở hạ tầng đám mây của Kaspersky. Để biết thông tin chi tiết về quản lý ứng dụng bằng Bảng điều khiển đám mây Kaspersky Security Center, hãy tham khảo [Trợ giúp của Bảng điều khiển đám mây Kaspersky Security Center](#).

So sánh các tính năng của Kaspersky Endpoint Security

Tính năng	Kaspersky Security Center		Kaspersky Security Center
	Bảng điều khiển quản trị	Bảng điều khiển web	Bảng điều khiển đám mây

Bảo vệ mối đe dọa nâng cao			
Kaspersky Security Network	✓	✓	✓
Mạng bảo mật riêng của Kaspersky	✓	✓	-
Phát hiện hành vi	✓	✓	✓
Phòng chống khai thác	✓	✓	✓
Phòng chống xâm nhập máy chủ	✓	✓	✓
Công cụ khắc phục	✓	✓	✓
Bảo vệ mối đe dọa thiết yếu			
Bảo vệ mối đe dọa tập tin	✓	✓	✓
Bảo vệ mối đe dọa web	✓	✓	✓
Bảo vệ mối đe dọa thư điện tử	✓	✓	✓
Tường lửa	✓	✓	✓
Bảo vệ mối đe dọa mạng	✓	✓	✓
Phòng chống Tấn công BadUSB	✓	✓	✓
Bảo vệ AMSI	✓	✓	✓
Kiểm soát bảo mật			
Kiểm soát ứng dụng	✓	✓	✓
Kiểm soát Thiết bị	✓	✓	✓
Kiểm soát Web	✓	✓	✓
Kiểm soát thích ứng sự cố	✓	✓	✓
Mã hóa dữ liệu			
Kaspersky Disk Encryption	✓	✓	-
BitLocker Drive Encryption	✓	✓	✓
Mã hóa mức độ tập tin	✓	✓	-
Mã hóa ổ đĩa di động	✓	✓	-
Detection and Response			
Endpoint Detection and Response Optimum	-	✓	✓
Endpoint Detection and Response Expert	-	-	✓
Kaspersky Sandbox	-	✓	-
Managed Detection and Response (MDR)	✓	✓	✓
Tác vụ			
Thêm khóa	✓	✓	✓
Thay đổi thành phần ứng dụng	✓	✓	✓
Kho	✓	✓	✓
Cập nhật	✓	✓	✓
Hoàn tác bản cập nhật	✓	✓	✓

Quét virus	✓	✓	✓
Kiểm tra tính toàn vẹn	✓	✓	-
Xóa sạch dữ liệu	✓	✓	✓
Quản lý tài khoản Authentication Agent (Kaspersky Disk Encryption)	✓	✓	-
Quét IOC (EDR)	-	✓	✓
Di chuyển tập tin đến Khu vực cách ly (EDR)	-	✓	✓
Lấy tập tin (EDR)	-	✓	✓
Xóa tập tin (EDR)	-	✓	✓
Khởi chạy tiến trình (EDR)	-	✓	✓
Chấm dứt tiến trình (EDR)	-	✓	✓

Khả năng tương thích với các ứng dụng khác

Trước khi cài đặt, Kaspersky Endpoint Security sẽ kiểm tra máy tính để xác định sự hiện diện của các ứng dụng Kaspersky. Ứng dụng này cũng sẽ kiểm tra máy tính để tìm 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](#).

[TẢI XUỐNG TẬP TIN INCOMPATIBLE.TXT](#)

Kaspersky Endpoint Security không tương thích với các ứng dụng sau đây của Kaspersky:

- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Kaspersky Anti Targeted Attack Platform (bao gồm thành phần Cảm biến điểm cuối).
- Kaspersky Sandbox (bao gồm cả Kaspersky Endpoint Agent).
- Kaspersky Endpoint Detection and Response (bao gồm thành phần Cảm biến điểm cuối).

Nếu thành phần Tác nhân điểm cuối được cài đặt trên máy tính bằng các công cụ triển khai của các ứng dụng Kaspersky khác thì các thành phần đó sẽ tự động bị gỡ bỏ trong quá trình cài đặt Kaspersky Endpoint Security. Kaspersky Endpoint Security cũng có thể bao gồm thành phần Cảm biến điểm cuối / Kaspersky Endpoint Agent nếu bạn chọn Tác nhân điểm cuối trong danh sách các thành phần của ứng dụng.

- Kaspersky Security for Virtualization Light Agent.
- Kaspersky Fraud Prevention for Endpoint.
- Kaspersky Security cho Windows Server.
- Kaspersky Embedded Systems Security.

Nếu các ứng dụng Kaspersky từ danh sách này được cài đặt trên máy tính, Kaspersky Endpoint Security sẽ gỡ bỏ các ứng dụng này. Vui lòng chờ tiến trình này hoàn tất trước khi tiếp tục cài đặt Kaspersky Endpoint Security.

Cài đặt và gỡ bỏ ứng dụng

Bạn có thể cài đặt Kaspersky Endpoint Security trên một máy tính theo các cách sau:

- cục bộ bằng cách sử dụng [Trình hướng dẫn cài đặt](#).
- cục bộ từ [dòng lệnh](#).
- từ xa thông qua [Kaspersky Security Center](#).
- từ xa thông qua Microsoft Windows Group Policy Management Editor (để biết thêm thông tin, hãy truy cập [trang web Hỗ trợ kỹ thuật của Microsoft](#)).
- từ xa sử dụng [Trình Quản lý cấu hình trung tâm hệ thống](#).

Bạn có thể cấu hình thiết lập cài đặt ứng dụng theo một số cách. Nếu bạn sử dụng đồng thời nhiều phương thức để cấu hình thiết lập thì Kaspersky Endpoint Security sẽ áp dụng thiết lập có mức độ ưu tiên cao nhất. Kaspersky Endpoint Security sẽ sử dụng thứ tự ưu tiên sau:

1. Thiết lập nhận được từ tập tin [setup.ini](#).
2. Thiết lập nhận được từ tập tin installer.ini.
3. Thiết lập nhận được từ tập tin [dòng lệnh](#).

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).

Triển khai thông qua Kaspersky Security Center

Kaspersky Endpoint Security có thể được triển khai trên các máy tính trong một mạng doanh nghiệp bằng nhiều cách. Bạn có thể chọn tình huống triển khai phù hợp nhất cho tổ chức của mình hoặc kết hợp nhiều tình huống triển khai khác nhau cùng lúc. Kaspersky Security Center hỗ trợ các phương thức triển khai chính sau đây:

- Cài đặt ứng dụng sử dụng Trình hướng dẫn Triển khai tính năng bảo vệ.
[Phương thức cài đặt tiêu chuẩn](#) rất tiện lợi nếu bạn hài lòng với các thiết lập mặc định của Kaspersky Endpoint Security và tổ chức của bạn có một hạ tầng đơn giản, không đòi hỏi cấu hình đặc biệt.
- Cài đặt ứng dụng sử dụng tác vụ cài đặt từ xa.
Phương thức cài đặt đa năng, cho phép cấu hình các thiết lập của Kaspersky Endpoint Security và quản lý linh hoạt các tác vụ cài đặt từ xa. Việc cài đặt Kaspersky Endpoint Security bao gồm các bước sau:

1. [Tạo một gói cài đặt](#).
2. [Tạo một tác vụ cài đặt từ xa](#).

Kaspersky Security Center cũng hỗ trợ các phương thức cài đặt Kaspersky Endpoint Security khác, ví dụ như triển khai trong một ảnh hệ điều hành. Để biết thêm thông tin về các phương thức triển khai khác, hãy tham khảo [Trợ giúp của Kaspersky Security Center](#).

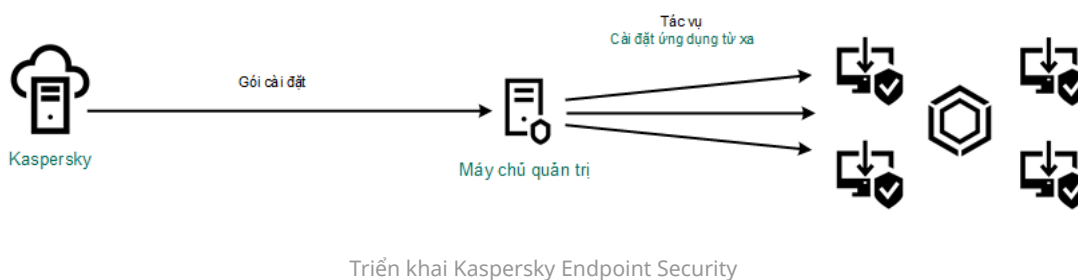
Bản cài đặt tiêu chuẩn của ứng dụng

Kaspersky Security Center cung cấp một Trình hướng dẫn Triển khai tính năng bảo vệ để cài đặt ứng dụng trên các máy tính doanh nghiệp. Trình hướng dẫn Triển khai tính năng bảo vệ bao gồm các hành động chính sau:

1. Chọn một gói cài đặt Kaspersky Endpoint Security.

Một *gói cài đặt* là một nhóm tập tin được tạo để cài đặt từ xa ứng dụng Kaspersky qua Kaspersky Security Center. Gói cài đặt chứa một khoảng thiết lập cần thiết để cài đặt ứng dụng và chạy nó ngay sau khi cài đặt. Gói cài đặt được tạo sử dụng tập tin với phần mở rộng .kpd và .kud được bao gồm trong gói phân phối ứng dụng. Gói cài đặt Kaspersky Endpoint Security có thể được sử dụng trên tất cả các phiên bản Windows và các loại cấu trúc bộ vi xử lý được hỗ trợ.

2. Tạo tác vụ *Cài đặt ứng dụng từ xa* thuộc Máy chủ quản trị Kaspersky Security Center.



[Cách chạy Trình hướng dẫn Triển khai tính năng bảo vệ trong Bảng điều khiển quản trị \(MMC\)](#)

1. Trong Bảng điều khiển quản trị, hãy vào thư mục **Administration Server** → **Additional** → **Remote installation**.

2. Nhấn vào liên kết **Deploy installation package on managed devices (workstations)**.

Thao tác này sẽ khởi chạy Trình hướng dẫn Triển khai tính năng bảo vệ. Làm theo chỉ dẫn của Trình hướng dẫn.

Các cổng TCP 139 và 445, và các cổng UDP 137 và 138 phải được mở trên một máy khách.

Bước 1. Lựa chọn một gói cài đặt

Chọn gói cài đặt Kaspersky Endpoint Security từ danh sách. Nếu danh sách không chứa gói cài đặt của Kaspersky Endpoint Security, bạn có thể tạo gói này trong Trình hướng dẫn.

Bạn có thể cấu hình [thiết lập của gói cài đặt](#) trong Kaspersky Security Center. Ví dụ, bạn có thể chọn các thành phần ứng dụng có thể được cài đặt lên một máy tính.

Network Agent cũng sẽ được cài đặt cùng với Kaspersky Endpoint Security. *Network Agent* giúp xúc tiến tương tác giữa Máy chủ quản trị và một máy khách. Nếu Network Agent đã được cài đặt trên một máy tính, nó sẽ không được cài đặt lại.

Bước 2. Chọn các thiết bị để cài đặt

Chọn các máy tính để cài đặt Kaspersky Endpoint Security. Các tùy chọn sau có thể được sử dụng:

- Gán tác vụ vào một nhóm quản trị. Trong trường hợp này, tác vụ sẽ được gán cho các máy tính được bao gồm trong một nhóm quản trị đã được tạo trước đó.
- Chọn các máy tính được Máy chủ quản trị phát hiện trong mạng – *các thiết bị chưa được gán*. Network Agent sẽ không được cài đặt trên các thiết bị chưa được gán. Trong trường hợp này, tác vụ sẽ được gán cho các thiết bị được quy định. Các thiết bị được quy định có thể bao gồm các thiết bị trong nhóm quản trị cũng như các thiết bị chưa được gán.
- Nhập vào thủ công địa chỉ của thiết bị, hoặc nhập các địa chỉ từ một danh sách. Bạn có thể quy định tên NetBIOS, địa chỉ IP, và địa chỉ IP mạng con của các thiết bị mà bạn muốn gán tác vụ.

Bước 3. Xác định thiết lập tác vụ cài đặt từ xa

Cấu hình các thiết lập ứng dụng bổ sung sau:

- **Force installation package download.** Chọn phương thức cài đặt ứng dụng:
 - **Using Network Agent.** Nếu Network Agent chưa được cài đặt trên máy tính, trước tiên, Network Agent sẽ được cài đặt sử dụng các công cụ của hệ điều hành. Sau đó, Kaspersky Endpoint Security sẽ được cài đặt bởi các công cụ của Network Agent.
 - **Using operating system resources through distribution points.** Gói cài đặt được gửi đến máy khách sử dụng tài nguyên hệ điều hành thông qua các điểm phân phối. Bạn có thể chọn

tùy chọn này nếu có ít nhất một điểm phân phối trong mạng. Để biết thêm chi tiết về các điểm phân phối, hãy tham khảo [Trợ giúp của Kaspersky Security Center](#).

- **Using operating system resources through Administration Server.** Các tập tin sẽ được gửi đến máy khách bằng tài nguyên của hệ điều hành thông qua Máy chủ quản trị. Bạn có thể chọn tùy chọn này nếu Network Agent không được cài đặt trên máy khách, nhưng máy khách kết nối đến cùng mạng lưới với Máy chủ quản trị.
- **Behavior for devices managed through other Administration Servers.** Chọn phương thức cài đặt Kaspersky Endpoint Security. Nếu mạng cài đặt nhiều hơn một Máy chủ quản trị, các Máy chủ quản trị này có thể thấy các máy khách giống nhau. Điều này có thể khiến, ví dụ, một ứng dụng được cài đặt từ xa trên một máy khách nhiều lần thông qua các Máy chủ quản trị khác nhau, hay các xung đột khác.
- **Do not re-install application if it is already installed.** Xóa hộp kiểm này nếu bạn muốn cài đặt một phiên bản cũ hơn của ứng dụng.
- **Assign Network Agent installation in Active Directory group policies.** Cài đặt thủ công Network Agent bằng tài nguyên Active Directory. Để cài đặt Network Agent, tác vụ cài đặt từ xa phải chạy với đặc quyền quản trị viên của tên miền.

Bước 4. Chọn một khóa giấy phép

Thêm một khóa vào gói cài đặt để kích hoạt ứng dụng. Bước này là không bắt buộc. Nếu Máy chủ quản trị có một khóa giấy phép có chức năng phân phối tự động, khóa đó sẽ được thêm tự động sau này. Bạn cũng có thể [kích hoạt ứng dụng](#) sau sử dụng tác vụ *Thêm khóa*.

Bước 5. Chọn thiết lập khởi động lại hệ điều hành

Chọn hành động để thực hiện nếu cần khởi động lại máy tính. Không cần khởi động lại khi cài đặt Kaspersky Endpoint Security. Chỉ cần khởi động lại nếu bạn đã 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.

Bước 6. Xóa các ứng dụng không tương thích trước khi cài đặt ứng dụng

Đọc kỹ danh sách các ứng dụng không tương thích và cho phép gỡ bỏ các ứng dụng này. Nếu các ứng dụng không tương thích được cài đặt trên một máy tính, quy trình cài đặt Kaspersky Endpoint Security sẽ kết thúc với một lỗi.

Bước 7. Chọn một tài khoản để truy cập các thiết bị

Chọn tài khoản dùng để cài đặt Network Agent sử dụng các công cụ của hệ điều hành. Trong trường hợp này, cần có quyền quản trị viên để truy cập máy tính. Bạn có thể thêm nhiều tài khoản. Nếu một tài khoản không có đủ quyền, Trình hướng dẫn Cài đặt sẽ sử dụng tài khoản tiếp theo. Nếu bạn cài đặt Kaspersky Endpoint Security sử dụng các công cụ Network Agent, bạn không phải chọn một tài khoản.

Bước 8. Bắt đầu quá trình cài đặt

Thoát Trình hướng dẫn. Nếu cần, hãy chọn hộp kiểm **Run the task after the Wizard finishes**. Bạn có thể giám sát tiến độ của tác vụ trong thuộc tính tác vụ.

Cách khởi động Trình hướng dẫn Triển khai tính năng bảo vệ trong Bảng điều khiển web và Bảng điều khiển đám mây [?](#)

Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Discovery & Deployment** → **Deployment & Assignment** → **Protection Deployment Wizard**.

Thao tác này sẽ khởi chạy Trình hướng dẫn Triển khai tính năng bảo vệ. Làm theo chỉ dẫn của Trình hướng dẫn.

Các cổng TCP 139 và 445, và các cổng UDP 137 và 138 phải được mở trên một máy khách.

Bước 1. Lựa chọn một gói cài đặt

Chọn gói cài đặt Kaspersky Endpoint Security từ danh sách. Nếu danh sách không chứa gói cài đặt của Kaspersky Endpoint Security, bạn có thể tạo gói này trong Trình hướng dẫn. Để tạo gói cài đặt, bạn không cần tìm kiếm gói phân phối và lưu gói đó vào bộ nhớ máy tính. Trong Kaspersky Security Center, bạn có thể xem danh sách các gói phân phối có trên máy chủ Kaspersky và gói cài đặt sẽ được tạo tự động. Kaspersky sẽ cập nhật danh sách sau khi phát hành các phiên bản mới của ứng dụng.

Bạn có thể cấu hình [thiết lập của gói cài đặt](#) trong Kaspersky Security Center. Ví dụ, bạn có thể chọn các thành phần ứng dụng có thể được cài đặt lên một máy tính.

Bước 2. Chọn một khóa giấy phép

Thêm một khóa vào gói cài đặt để kích hoạt ứng dụng. Bước này là không bắt buộc. Nếu Máy chủ quản trị có một khóa giấy phép có chức năng phân phối tự động, khóa đó sẽ được thêm tự động sau này. Bạn cũng có thể [kích hoạt ứng dụng](#) sau sử dụng tác vụ *Thêm khóa*.

Bước 3. Chọn một Network Agent

Chọn phiên bản Network Agent sẽ được cài đặt cùng với Kaspersky Endpoint Security. *Network Agent* giúp xúc tiến tương tác giữa Máy chủ quản trị và một máy khách. Nếu Network Agent đã được cài đặt trên một máy tính, nó sẽ không được cài đặt lại.

Bước 4. Chọn các thiết bị để cài đặt

Chọn các máy tính để cài đặt Kaspersky Endpoint Security. Các tùy chọn sau có thể được sử dụng:

- Gán tác vụ vào một nhóm quản trị. Trong trường hợp này, tác vụ sẽ được gán cho các máy tính được bao gồm trong một nhóm quản trị đã được tạo trước đó.
- Chọn các máy tính được Máy chủ quản trị phát hiện trong mạng – *các thiết bị chưa được gán*. Network Agent sẽ không được cài đặt trên các thiết bị chưa được gán. Trong trường hợp này, tác vụ sẽ được gán cho các thiết bị được quy định. Các thiết bị được quy định có thể bao gồm các thiết bị trong nhóm quản trị cũng như các thiết bị chưa được gán.
- Nhập vào thủ công địa chỉ của thiết bị, hoặc nhập các địa chỉ từ một danh sách. Bạn có thể quy định tên NetBIOS, địa chỉ IP, và địa chỉ IP mạng con của các thiết bị mà bạn muốn gán tác vụ.

Bước 5. Thiết lập cấu hình nâng cao

Cấu hình các thiết lập ứng dụng bổ sung sau:

- **Force installation package download.** Chọn phương thức cài đặt ứng dụng:
 - **Using Network Agent.** Nếu Network Agent chưa được cài đặt trên máy tính, trước tiên, Network Agent sẽ được cài đặt sử dụng các công cụ của hệ điều hành. Sau đó, Kaspersky Endpoint Security sẽ được cài đặt bởi các công cụ của Network Agent.
 - **Using operating system resources through distribution points.** Gói cài đặt được gửi đến máy khách sử dụng tài nguyên hệ điều hành thông qua các điểm phân phối. Bạn có thể chọn tùy chọn này nếu có ít nhất một điểm phân phối trong mạng. Để biết thêm chi tiết về các điểm phân phối, hãy tham khảo [Trợ giúp của Kaspersky Security Center](#).
 - **Using operating system resources through Administration Server.** Các tập tin sẽ được gửi đến máy khách bằng tài nguyên của hệ điều hành thông qua Máy chủ quản trị. Bạn có thể chọn tùy chọn này nếu Network Agent không được cài đặt trên máy khách, nhưng máy khách kết nối đến cùng mạng lưới với Máy chủ quản trị.
- **Do not re-install application if it is already installed.** Xóa hộp kiểm này nếu bạn muốn cài đặt một phiên bản cũ hơn của ứng dụng.
- **Assign package installation in Active Directory group policies.** Kaspersky Endpoint Security sẽ được cài đặt thông qua Network Agent hoặc thủ công qua Active Directory. Để cài đặt Network Agent, tác vụ cài đặt từ xa phải chạy với đặc quyền quản trị viên của tên miền.

Bước 6. Chọn thiết lập khởi động lại hệ điều hành

Chọn hành động để thực hiện nếu cần khởi động lại máy tính. Không cần khởi động lại khi cài đặt Kaspersky Endpoint Security. Chỉ cần khởi động lại nếu bạn đã 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.

Bước 7. Xóa các ứng dụng không tương thích trước khi cài đặt ứng dụng

Đọc kỹ danh sách các ứng dụng không tương thích và cho phép gỡ bỏ các ứng dụng này. Nếu các ứng dụng không tương thích được cài đặt trên một máy tính, quy trình cài đặt Kaspersky Endpoint Security sẽ kết thúc với một lỗi.

Bước 8. Gán vào một nhóm quản trị

Chọn nhóm quản trị có các máy tính sẽ được di chuyển vào khi Network Agent được cài đặt. Máy tính cần được chuyển vào một nhóm quản trị để có thể áp dụng các [chính sách](#) và [tác vụ nhóm](#). Nếu một máy tính đã nằm trong bất kỳ nhóm quản trị nào, máy tính đó sẽ không được di chuyển. Nếu bạn không chọn một nhóm quản trị, các máy tính sẽ được thêm vào nhóm **Unassigned devices**.

Bước 9. Chọn một tài khoản để truy cập các thiết bị

Chọn tài khoản dùng để cài đặt Network Agent sử dụng các công cụ của hệ điều hành. Trong trường hợp này, cần có quyền quản trị viên để truy cập máy tính. Bạn có thể thêm nhiều tài khoản. Nếu một tài khoản không có đủ quyền, Trình hướng dẫn Cài đặt sẽ sử dụng tài khoản tiếp theo. Nếu bạn cài đặt Kaspersky Endpoint Security sử dụng các công cụ Network Agent, bạn không phải chọn một tài khoản.

Bước 10. Bắt đầu cài đặt

Thoát Trình hướng dẫn. Nếu cần, hãy chọn hộp kiểm **Run the task after the Wizard finishes**. Bạn có thể giám sát tiến độ của tác vụ trong thuộc tính tác vụ.

Tạo một gói cài đặt

Một *gói cài đặt* là một nhóm tập tin được tạo để cài đặt từ xa ứng dụng Kaspersky qua Kaspersky Security Center. Gói cài đặt chứa một khoảng thiết lập cần thiết để cài đặt ứng dụng và chạy nó ngay sau khi cài đặt. Gói cài đặt được tạo sử dụng tập tin với phần mở rộng .kpd và .kud được bao gồm trong gói phân phối ứng dụng. Gói cài đặt Kaspersky Endpoint Security có thể được sử dụng trên tất cả các phiên bản Windows và các loại cấu trúc bộ vi xử lý được hỗ trợ.

[Cách tạo một gói cài đặt trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Trong Bảng điều khiển quản trị, hãy vào thư mục **Administration Server** → **Additional** → **Remote installation** → **Installation packages**.

Thao tác này sẽ mở danh sách các gói cài đặt đã được tải về Kaspersky Security Center.

2. Nhấn nút **Create installation package**.

Trình hướng dẫn Gói tin mới sẽ khởi chạy. Làm theo chỉ dẫn của Trình hướng dẫn.

Bước 1. Chọn loại gói cài đặt

Hãy chọn tùy chọn **Create an installation package for a Kaspersky application**.

Bước 2. Đặt tên cho gói cài đặt

Nhập tên của gói cài đặt, ví dụ như *Kaspersky Endpoint Security cho Windows 11.9.0*.

Bước 3. Chọn gói phân phối để cài đặt

Nhấn vào nút **Duyệt** và chọn tập tin `kes_win.kud` kèm theo [gói phân phối](#).

Nếu được yêu cầu, hãy cập nhật cơ sở dữ liệu diệt virus trong gói cài đặt bằng cách sử dụng hộp kiểm **Copy updates from repository to installation package**.

Bước 4. Thỏa thuận giấy phép người dùng cuối và Chính sách quyền riêng tư

Đọc và chấp nhận các điều khoản của Thỏa thuận giấy phép người dùng cuối và Chính sách quyền riêng tư.

Gói cài đặt sẽ được tạo và được thêm vào Kaspersky Security Center. Sử dụng gói cài đặt, bạn có thể cài đặt Kaspersky Endpoint Security trên các máy tính mạng doanh nghiệp hoặc cập nhật phiên bản ứng dụng. Trong thiết lập gói cài đặt, bạn cũng có thể chọn các thành phần ứng dụng và cấu hình thiết lập cài đặt ứng dụng (xem bảng bên dưới). Gói cài đặt chứa cơ sở dữ liệu diệt virus trong kho lưu trữ của Máy chủ quản trị. Bạn có thể [cập nhật cơ sở dữ liệu trong gói cài đặt](#) để giảm mức sử dụng lưu lượng khi cập nhật cơ sở dữ liệu sau khi cài đặt Kaspersky Endpoint Security.

[Cách tạo gói cài đặt trong Bảng điều khiển web và Bảng điều khiển đám mây](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Discovery & Deployment** → **Deployment & Assignment** → **Installation packages**.

Thao tác này sẽ mở danh sách các gói cài đặt đã được tải về Kaspersky Security Center.

2. Nhấn vào nút **Thêm**.

Trình hướng dẫn Gói tin mới sẽ khởi chạy. Làm theo chỉ dẫn của Trình hướng dẫn.

Bước 1. Chọn loại gói cài đặt

Hãy chọn tùy chọn **Create an installation package for a Kaspersky application**.

Trình hướng dẫn sẽ tạo một gói cài đặt từ gói phân phối được lưu trữ trên các máy chủ Kaspersky. Danh sách này được cập nhật tự động khi các phiên bản mới của ứng dụng được phát hành. Bạn được khuyến cáo chọn tùy chọn này để cài đặt Kaspersky Endpoint Security.

Bạn cũng có thể tạo một gói cài đặt từ một tập tin.

Bước 2. Các gói cài đặt

Chọn gói cài đặt Kaspersky Endpoint Security cho Windows. Tiến trình tạo gói cài đặt sẽ được bắt đầu. Trong quá trình tạo gói cài đặt, bạn phải chấp nhận các điều khoản của Thỏa thuận giấy phép người dùng cuối và Chính sách quyền riêng tư.

Gói cài đặt sẽ được tạo và được thêm vào Kaspersky Security Center. Sử dụng gói cài đặt, bạn có thể cài đặt Kaspersky Endpoint Security trên các máy tính mạng doanh nghiệp hoặc cập nhật phiên bản ứng dụng. Trong thiết lập gói cài đặt, bạn cũng có thể chọn các thành phần ứng dụng và cấu hình thiết lập cài đặt ứng dụng (xem bảng bên dưới). Gói cài đặt chứa cơ sở dữ liệu diệt virus trong kho lưu trữ của Máy chủ quản trị. Bạn có thể [cập nhật cơ sở dữ liệu trong gói cài đặt](#) để giảm mức sử dụng lưu lượng khi cập nhật cơ sở dữ liệu sau khi cài đặt Kaspersky Endpoint Security.

Cấu hình gói cài đặt

Phần	Mô tả
Thành phần bảo vệ	<p>Trong phần này, bạn có thể chọn các thành phần ứng dụng có thể được sử dụng. Bạn có thể thay đổi bộ thành phần ứng dụng sau này bằng cách sử dụng tác vụ <i>Thay đổi thành phần ứng dụng</i>. Thành phần Phòng chống Tấn công BadUSB, thành phần Detection and Response và các thành phần mã hóa dữ liệu không được cài đặt theo mặc định. Bạn có thể thêm các thành phần này trong thiết lập gói cài đặt.</p> <p>Nếu bạn cần cài đặt các thành phần Detection and Response thì Kaspersky Endpoint Security sẽ hỗ trợ các cấu hình sau:</p> <ul style="list-style-type: none">• Chỉ Endpoint Detection and Response Optimum• Chỉ Endpoint Detection and Response Expert• Chỉ Kaspersky Sandbox• Endpoint Detection and Response Optimum và Kaspersky Sandbox• Endpoint Detection and Response Expert và Kaspersky Sandbox.

	Kaspersky Endpoint Security sẽ xác minh việc chọn các thành phần trước khi cài đặt ứng dụng. Nếu cấu hình đã chọn của các thành phần Detection and Response không được hỗ trợ thì không thể cài đặt Kaspersky Endpoint Security.
Khóa giấy phép	Trong phần này, bạn có thể kích hoạt ứng dụng. Để kích hoạt ứng dụng, bạn phải chọn một khóa giấy phép. Trước khi thực hiện điều đó, bạn phải thêm khóa vào Máy chủ quản trị. Để biết thêm chi tiết về việc thêm khóa vào Máy chủ quản trị Kaspersky Security Center, vui lòng tham khảo Trợ giúp của Kaspersky Security Center .
Ứng dụng không tương thích	Đọc kỹ danh sách các ứng dụng không tương thích và cho phép gỡ bỏ các ứng dụng này. Nếu các ứng dụng không tương thích được cài đặt trên một máy tính, quy trình cài đặt Kaspersky Endpoint Security sẽ kết thúc với một lỗi.
Thiết lập cài đặt	<p>Thêm vị trí chương trình đến môi trường đường dẫn thay đổi %PATH%. Bạn có thể thêm đường dẫn cài đặt vào biến số %PATH% để tiện sử dụng giao diện dòng lệnh.</p> <p>Không bảo vệ quá trình 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 ứng dụng độc hại, chặn truy cập đến thư mục cài đặt của Kaspersky Endpoint Security, và chặn truy cập đến phần 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.</p> <p>Đảm bảo tương thích với Citrix PVS (điều này chỉ cần thiết khi làm việc với Citrix PVS). Bạn có thể bật hỗ trợ Citrix Provisioning Services để cài đặt Kaspersky Endpoint Security lên một máy tính ảo.</p> <p>Đường dẫn đến thư mục cài đặt chương trình. Bạn có thể thay đổi đường dẫn cài đặt của Kaspersky Endpoint Security trên một máy khách. Theo mặc định, ứng dụng được cài đặt trong thư mục %ProgramFiles%\Kaspersky Lab\Kaspersky Endpoint Security for Windows.</p> <p>Tập tin cấu hình. Bạn có thể tải lên một tập tin quy định thiết lập của Kaspersky Endpoint Security. Bạn có thể tạo một tập tin cấu hình trong giao diện cục bộ của ứng dụng.</p>

Cập nhật cơ sở dữ liệu trong gói cài đặt

Gói cài đặt chứa cơ sở dữ liệu diệt virus từ kho lưu trữ của Máy chủ quản trị được cập nhật khi gói cài đặt được tạo. Sau khi tạo gói cài đặt, bạn có thể cập nhật cơ sở dữ liệu diệt virus trong gói cài đặt. Điều này cho phép bạn giảm mức sử dụng lưu lượng khi cập nhật cơ sở dữ liệu diệt virus sau khi cài đặt Kaspersky Endpoint Security.

Để cập nhật cơ sở dữ liệu diệt virus trong kho lưu trữ của Máy chủ quản trị, hãy sử dụng tác vụ *Tải bản cập nhật về kho lưu trữ Máy chủ quản trị* của Máy chủ quản trị. Để biết thêm thông tin về việc cập nhật cơ sở dữ liệu diệt virus trong kho lưu trữ Máy chủ quản trị, vui lòng tham khảo [Trợ giúp của Kaspersky Security Center](#).

Bạn chỉ có thể cập nhật cơ sở dữ liệu trong gói cài đặt trong Bảng điều khiển quản trị và Bảng điều khiển web Kaspersky Security Center. Bạn không thể cập nhật cơ sở dữ liệu trong gói cài đặt trong Bảng điều khiển đám mây Kaspersky Security Center.

[Cách cập nhật cơ sở dữ liệu diệt virus trong gói cài đặt thông qua Bảng điều khiển quản trị \(MMC\)](#)

1. Trong Bảng điều khiển quản trị, hãy vào thư mục **Administration Server** → **Additional** → **Remote installation** → **Installation packages**.

Thao tác này sẽ mở danh sách các gói cài đặt đã được tải về Kaspersky Security Center.

2. Mở thuộc tính của gói cài đặt.

3. Trong mục **Tổng quát**, hãy chọn nút **Update databases**.

Do đó, cơ sở dữ liệu diệt virus trong gói cài đặt sẽ được cập nhật từ kho lưu trữ của Máy chủ quản trị. Tập tin bases.cab kèm theo [gói phân phối](#) sẽ được thay thế bằng thư mục bases. Các tập tin của gói cập nhật sẽ ở trong thư mục đó.

[Cách cập nhật cơ sở dữ liệu diệt virus trong gói cài đặt thông qua Bảng điều khiển web](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Discovery & Deployment** → **Deployment & Assignment** → **Installation packages**.

Việc này sẽ mở ra danh sách các gói cài đặt đã được tải về Bảng điều khiển web.

2. Nhấn vào tên của gói cài đặt Kaspersky Endpoint Security mà bạn muốn cập nhật cơ sở dữ liệu diệt virus.

Cửa sổ thuộc tính của gói cài đặt sẽ được mở ra.

3. Trên thẻ **General information**, hãy nhấn vào liên kết **Update databases**.

Do đó, cơ sở dữ liệu diệt virus trong gói cài đặt sẽ được cập nhật từ kho lưu trữ của Máy chủ quản trị. Tập tin bases.cab kèm theo [gói phân phối](#) sẽ được thay thế bằng thư mục bases. Các tập tin của gói cập nhật sẽ ở trong thư mục đó.

Tạo một tác vụ cài đặt từ xa

Tác vụ *Cài đặt ứng dụng từ xa* được thiết kế để cài đặt Kaspersky Endpoint Security từ xa. Tác vụ *Cài đặt ứng dụng từ xa* cho phép bạn triển khai [gói cài đặt của ứng dụng](#) cho tất cả các máy tính trong tổ chức. Trước khi triển khai gói cài đặt, bạn có thể [cập nhật cơ sở dữ liệu diệt virus](#) bên trong gói và chọn các thành phần ứng dụng khả dụng trong thuộc tính của gói cài đặt.

[Cách tạo tác vụ cài đặt từ xa trong Bảng điều khiển quản trị \(MMC\)](#)

1. Trong Bảng điều khiển quản trị, hãy vào thư mục **Administration Server** → **Tác vụ**.

Danh sách tác vụ sẽ mở.

2. Nhấn nút **New task**.

Trình hướng dẫn Tác vụ sẽ được bắt đầu. Làm theo chỉ dẫn của Trình hướng dẫn.

Bước 1. Chọn loại tác vụ

Chọn **Kaspersky Security Center Administration Server** → **Install application remotely**.

Bước 2. Lựa chọn một gói cài đặt

Chọn gói cài đặt Kaspersky Endpoint Security từ danh sách. Nếu danh sách không chứa gói cài đặt của Kaspersky Endpoint Security, bạn có thể tạo gói này trong Trình hướng dẫn.

Bạn có thể cấu hình [thiết lập của gói cài đặt](#) trong Kaspersky Security Center. Ví dụ, bạn có thể chọn các thành phần ứng dụng có thể được cài đặt lên một máy tính.

Network Agent cũng sẽ được cài đặt cùng với Kaspersky Endpoint Security. *Network Agent* giúp xúc tiến tương tác giữa Máy chủ quản trị và một máy khách. Nếu Network Agent đã được cài đặt trên một máy tính, nó sẽ không được cài đặt lại.

Bước 3. Bổ sung

Chọn gói cài đặt Network Agent. Phiên bản Network Agent được chọn sẽ được cài đặt cùng với Kaspersky Endpoint Security.

Bước 4. Cấu hình

Cấu hình các thiết lập ứng dụng bổ sung sau:

- **Force installation package download.** Chọn phương thức cài đặt ứng dụng:
 - **Using Network Agent.** Nếu Network Agent chưa được cài đặt trên máy tính, trước tiên, Network Agent sẽ được cài đặt sử dụng các công cụ của hệ điều hành. Sau đó, Kaspersky Endpoint Security sẽ được cài đặt bởi các công cụ của Network Agent.
 - **Using operating system resources through distribution points.** Gói cài đặt được gửi đến máy khách sử dụng tài nguyên hệ điều hành thông qua các điểm phân phối. Bạn có thể chọn tùy chọn này nếu có ít nhất một điểm phân phối trong mạng. Để biết thêm chi tiết về các điểm phân phối, hãy tham khảo [Trợ giúp của Kaspersky Security Center](#).
 - **Using operating system resources through Administration Server.** Các tập tin sẽ được gửi đến máy khách bằng tài nguyên của hệ điều hành thông qua Máy chủ quản trị. Bạn có thể chọn tùy chọn này nếu Network Agent không được cài đặt trên máy khách, nhưng máy khách kết nối đến cùng mạng lưới với Máy chủ quản trị.
- **Behavior for devices managed through other Administration Servers.** Chọn phương thức cài đặt Kaspersky Endpoint Security. Nếu mạng cài đặt nhiều hơn một Máy chủ quản trị, các Máy chủ

quản trị này có thể thấy các máy khách giống nhau. Điều này có thể khiến, ví dụ, một ứng dụng được cài đặt từ xa trên một máy khách nhiều lần thông qua các Máy chủ quản trị khác nhau, hay các xung đột khác.

- **Do not re-install application if it is already installed.** Xóa hộp kiểm này nếu bạn muốn cài đặt một phiên bản cũ hơn của ứng dụng.

Bước 5. Chọn thiết lập khởi động lại hệ điều hành

Chọn hành động để thực hiện nếu cần khởi động lại máy tính. Không cần khởi động lại khi cài đặt Kaspersky Endpoint Security. Chỉ cần khởi động lại nếu bạn đã 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.

Bước 6. Chọn các thiết bị sẽ được gán tác vụ

Chọn các máy tính để cài đặt Kaspersky Endpoint Security. Các tùy chọn sau có thể được sử dụng:

- Gán tác vụ vào một nhóm quản trị. Trong trường hợp này, tác vụ sẽ được gán cho các máy tính được bao gồm trong một nhóm quản trị đã được tạo trước đó.
- Chọn các máy tính được Máy chủ quản trị phát hiện trong mạng – *các thiết bị chưa được gán*. Network Agent sẽ không được cài đặt trên các thiết bị chưa được gán. Trong trường hợp này, tác vụ sẽ được gán cho các thiết bị được quy định. Các thiết bị được quy định có thể bao gồm các thiết bị trong nhóm quản trị cũng như các thiết bị chưa được gán.
- Nhập vào thủ công địa chỉ của thiết bị, hoặc nhập các địa chỉ từ một danh sách. Bạn có thể quy định tên NetBIOS, địa chỉ IP, và địa chỉ IP mạng con của các thiết bị mà bạn muốn gán tác vụ.

Bước 7. Chọn tài khoản để chạy tác vụ

Chọn tài khoản dùng để cài đặt Network Agent sử dụng các công cụ của hệ điều hành. Trong trường hợp này, cần có quyền quản trị viên để truy cập máy tính. Bạn có thể thêm nhiều tài khoản. Nếu một tài khoản không có đủ quyền, Trình hướng dẫn Cài đặt sẽ sử dụng tài khoản tiếp theo. Nếu bạn cài đặt Kaspersky Endpoint Security sử dụng các công cụ Network Agent, bạn không phải chọn một tài khoản.



Bước 8. Cấu hình lịch khởi chạy tác vụ

Cấu hình lịch khởi chạy một tác vụ, ví dụ như khởi chạy thủ công hoặc khi máy tính rảnh.

Bước 9. Xác định tên tác vụ

Nhập tên cho tác vụ, ví dụ như *Cài đặt Kaspersky Endpoint Security cho Windows 11.9.0*.

Bước 10. Hoàn thành tạo tác vụ

Thoát Trình hướng dẫn. Nếu cần, hãy chọn hộp kiểm **Run the task after the Wizard finishes**. Bạn có thể giám sát tiến độ của tác vụ trong thuộc tính tác vụ. Ứng dụng sẽ được cài đặt trong chế độ im lặng. Sau khi cài đặt, biểu tượng  sẽ được thêm vào khu vực thông báo của máy tính người dùng. Nếu biểu tượng nhìn giống như thế này , đảm bảo rằng bạn [đã kích hoạt ứng dụng](#).

[Cách tạo tác vụ cài đặt từ xa trong Bảng điều khiển web và Bảng điều khiển đám mây](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.

Danh sách tác vụ sẽ mở.

2. Nhấn vào nút **Thêm**.

Trình hướng dẫn Tác vụ sẽ được bắt đầu. Làm theo chỉ dẫn của Trình hướng dẫn.

Bước 1. Cấu hình thiết lập tác vụ tổng quát

Cấu hình thiết lập của tác vụ tổng quát:

1. Trong danh sách thả xuống **Ứng dụng**, chọn **Kaspersky Security Center**.
2. Trong danh sách thả xuống **Loại tác vụ**, chọn **Install application remotely**.
3. Trong trường **Task name**, nhập một mô tả ngắn gọn, ví dụ như *Cài đặt Kaspersky Endpoint Security cho người quản lý*.
4. Trong phần **Select devices to which the task will be assigned**, chọn phạm vi tác vụ.

Bước 2. Chọn máy tính để cài đặt

Ở bước này, hãy chọn các máy tính để cài đặt Kaspersky Endpoint Security theo tùy chọn phạm vi tác vụ được chọn.

Bước 3. Cấu hình một gói cài đặt

Ở bước này, hãy cấu hình gói cài đặt:

1. Chọn gói cài đặt Kaspersky Endpoint Security cho Windows (11.9.0).
2. Chọn gói cài đặt Network Agent.

Phiên bản Network Agent được chọn sẽ được cài đặt cùng với Kaspersky Endpoint Security. *Network Agent* giúp xúc tiến tương tác giữa Máy chủ quản trị và một máy khách. Nếu Network Agent đã được cài đặt trên một máy tính, nó sẽ không được cài đặt lại.

3. Trong mục **Force installation package download**, hãy chọn phương thức cài đặt ứng dụng:


- **Using Network Agent.** Nếu Network Agent chưa được cài đặt trên máy tính, trước tiên, Network Agent sẽ được cài đặt sử dụng các công cụ của hệ điều hành. Sau đó, Kaspersky Endpoint Security sẽ được cài đặt bởi các công cụ của Network Agent.
- **Using operating system resources through distribution points.** Gói cài đặt được gửi đến máy khách sử dụng tài nguyên hệ điều hành thông qua các điểm phân phối. Bạn có thể chọn tùy chọn này nếu có ít nhất một điểm phân phối trong mạng. Để biết thêm chi tiết về các điểm phân phối, hãy tham khảo [Trợ giúp của Kaspersky Security Center](#).
- **Using operating system resources through Administration Server.** Các tập tin sẽ được gửi đến máy khách bằng tài nguyên của hệ điều hành thông qua Máy chủ quản trị. Bạn có thể chọn tùy chọn này nếu Network Agent không được cài đặt trên máy khách, nhưng máy khách kết nối đến cùng mạng lưới với Máy chủ quản trị.

4. Trong trường **Maximum number of concurrent downloads**, thiết lập giới hạn về số yêu cầu tải về gói cài đặt được gửi đến Máy chủ quản trị. Giới hạn số yêu cầu sẽ ngăn mạng khỏi bị quá tải.
5. Trong trường **Maximum number of installation attempts**, thiết lập giới hạn về số nỗ lực cài đặt ứng dụng. Nếu quy trình cài đặt Kaspersky Endpoint Security kết thúc với một lỗi, tác vụ này sẽ tự động bắt đầu lại quá trình cài đặt.
6. Nếu cần, xóa hộp kiểm **Do not re-install application if it is already installed**. Nó cho phép bạn cài đặt một phiên bản cũ của ứng dụng, nếu cần.
7. Nếu cần, hãy xóa hộp kiểm **Verify operating system type before downloading**. Việc này cho phép bạn tránh tải về một gói phân phối ứng dụng nếu hệ điều hành của máy tính không đáp ứng các yêu cầu về phần mềm. Nếu bạn chắc chắn rằng hệ điều hành của máy tính đáp ứng các yêu cầu về phần mềm, bạn có thể bỏ qua bước xác minh này.
8. Nếu cần thiết, chọn hộp kiểm **Assign package installation in Active Directory group policies**. Kaspersky Endpoint Security sẽ được cài đặt thông qua Network Agent hoặc thủ công qua Active Directory. Để cài đặt Network Agent, tác vụ cài đặt từ xa phải chạy với đặc quyền quản trị viên của tên miền.
9. Nếu cần, hãy chọn hộp kiểm **Prompt users to close running applications**. Việc cài đặt Kaspersky Endpoint Security sẽ sử dụng tài nguyên máy tính. Để tiện lợi, Trình hướng dẫn Cài đặt ứng dụng sẽ nhắc bạn đóng các ứng dụng đang chạy trước khi bắt đầu việc cài đặt. Điều này tránh gây gián đoạn trong hoạt động của các ứng dụng khác và ngăn hỏng hóc có thể xảy ra cho máy tính.
10. Trong mục **Behavior for devices managed through other Administration Servers**, hãy chọn phương thức cài đặt Kaspersky Endpoint Security. Nếu mạng cài đặt nhiều hơn một Máy chủ quản trị, các Máy chủ quản trị này có thể thấy các máy khách giống nhau. Điều này có thể khiến, ví dụ, một ứng dụng được cài đặt từ xa trên một máy khách nhiều lần thông qua các Máy chủ quản trị khác nhau, hay các xung đột khác.

Bước 4. Chọn tài khoản để chạy tác vụ

Chọn tài khoản dùng để cài đặt Network Agent sử dụng các công cụ của hệ điều hành. Trong trường hợp này, cần có quyền quản trị viên để truy cập máy tính. Bạn có thể thêm nhiều tài khoản. Nếu một tài khoản không có đủ quyền, Trình hướng dẫn Cài đặt sẽ sử dụng tài khoản tiếp theo. Nếu bạn cài đặt Kaspersky Endpoint Security sử dụng các công cụ Network Agent, bạn không phải chọn một tài khoản.

Bước 5. Hoàn tất việc tạo tác vụ

Hoàn tất trình hướng dẫn bằng cách nhấn nút **Hoàn tất**. Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ. Để thực hiện một tác vụ, chọn hộp kiểm cạnh tác vụ đó và nhấn nút **Bắt đầu**. Ứng dụng sẽ được cài đặt trong chế độ im lặng. Sau khi cài đặt, biểu tượng **k** sẽ được thêm vào khu vực thông báo của máy tính người dùng. Nếu biểu tượng nhìn giống như thế này , đảm bảo rằng bạn [đã kích hoạt ứng dụng](#).

Cài đặt ứng dụng một cách cục bộ bằng Trình hướng dẫn

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.

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

1. Sao chép thư mục [gói phân phối](#) vào máy tính của người dùng.
2. Chạy setup_kes.exe.

Trình hướng dẫn cài đặt sẽ được bắt đầu.

Chuẩn bị cài đặt

Trước khi cài đặt Kaspersky Endpoint Security trên một máy tính hoặc nâng cấp ứng dụng từ một phiên bản cũ, các điều kiện sau sẽ được kiểm tra:

- Phát hiện phần mềm không tương thích được cài đặt (tập tin incompatible.txt, được kèm theo [gói phân phối](#), chứa danh sách các phần mềm không tương thích).
- 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 11.9.0 cho 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 Endpoint Security 10 Service Pack 2 Maintenance Release 4 cho Windows (bản dựng 10.3.3.304).
- Kaspersky Endpoint Security 11.1.0 cho Windows (bản dựng 11.1.0.15919).
- Kaspersky Endpoint Security 11.1.1 cho Windows (bản dựng 11.1.1.126).
- Kaspersky Endpoint Security 11.2.0 cho Windows (bản dựng 11.2.0.2254).
- Kaspersky Endpoint Security 11.2.0 cho Windows CF1 (bản dựng 11.2.0.2254).
- Kaspersky Endpoint Security 11.3.0 cho Windows (bản dựng 11.3.0.773).
- Kaspersky Endpoint Security 11.4.0 cho Windows (bản dựng 11.4.0.233).
- Kaspersky Endpoint Security 11.5.0 cho Windows (bản dựng 11.5.0.590).
- Kaspersky Endpoint Security 11.6.0 cho Windows (bản dựng 11.6.0.394).
- Kaspersky Endpoint Security 11.7.0 cho Windows (bản dựng 11.7.0.669).
- Kaspersky Endpoint Security 11.8.0 cho Windows (bản dựng 11.8.0.384).

Các thành phần Kaspersky Endpoint Security

Trong tiến trình cài đặt này, bạn có thể chọn các thành phần Kaspersky Endpoint Security mà bạn muốn cài đặt. Thành phần Bảo vệ mối đe dọa tập tin là một thành phần bắt buộc phải được 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](#).
- [Các thành phần mã hóa dữ liệu](#).
- Các thành phần Detection and Response.

Bạn có thể [thay đổi các thành phần ứng dụng khả dụng sau khi ứng dụng được cài đặt](#). Để thực hiện, bạn cần chạy lại Trình hướng dẫn cài đặt và chọn thay đổi các thành phần khả dụng.

Nếu bạn cần cài đặt các thành phần Detection and Response thì Kaspersky Endpoint Security sẽ hỗ trợ các cấu hình sau:

- Chỉ Endpoint Detection and Response Optimum
- Chỉ Endpoint Detection and Response Expert
- Chỉ Kaspersky Sandbox
- Endpoint Detection and Response Optimum và Kaspersky Sandbox
- Endpoint Detection and Response Expert và Kaspersky Sandbox.

Kaspersky Endpoint Security sẽ xác minh việc chọn các thành phần trước khi cài đặt ứng dụng. Nếu cấu hình đã chọn của các thành phần Detection and Response không được hỗ trợ thì không thể cài đặt Kaspersky Endpoint Security.

Thiết lập nâng cao

Bảo vệ tiến trình cài đặt ứng dụng. Bảo vệ quá trình cài đặt bao gồm tính năng bảo vệ chống lại nguy cơ thay thế gói phân phối bằng các ứng dụng độc hại, chặn truy cập đến thư mục cài đặt của Kaspersky Endpoint Security, và chặn truy cập đến phần 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.

Đảm bảo tương thích với Citrix PVS (điều này chỉ cần thiết khi làm việc với Citrix PVS). Bạn có thể bật hỗ trợ Citrix Provisioning Services để cài đặt Kaspersky Endpoint Security lên một máy tính ảo.

Thêm vị trí chương trình đến môi trường đường dẫn thay đổi %PATH%. Bạn có thể thêm đường dẫn cài đặt vào biến số %PATH% để tiện [sử dụng giao diện dòng lệnh](#).

Cài đặt ứng dụng từ xa sử dụng Trình Quản lý Cấu hình Trung tâm Hệ thống

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

1. Mở bảng điều khiển của Trình Quản lý Cấu hình.
2. Trong phần bên phải của bảng điều khiển, trong mục **App management**, chọn **Packages**.
3. Trong phần trên của bảng điều khiển, trong bảng kiểm soát, nhấn nút **Create package**.
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 **Package**:
 - Trong trường **Name**, nhập tên của gói cài đặt.
 - Trong trường **Source folder**, hãy chỉ định đường dẫn đến thư mục chứa gói phân phối của Kaspersky Endpoint Security.
 - b. Trong mục **Application type**, chọn **Standard program**.
 - c. Trong mục **Standard program**:
 - Trong trường **Name**, nhập tên đặc trưng cho gói cài đặt (ví dụ, tên ứng dụng bao gồm cả phiên bản).
 - Trong trường **Command line**, nhập tùy chọn cài đặt của Kaspersky Endpoint Security từ dòng lệnh.
 - Nhấn nút **Browse** để nhập đường dẫn đến tập tin thực thi của ứng dụng.
 - Đảm bảo danh sách **Run mode** có mục **Run with administrative rights** được chọn.
 - d. Trong mục **Requirements**:
 - Chọn hộp kiểm **Run another program first** 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 **Application** hoặc nhập đường dẫn đến tập tin thực thi của ứng dụng này với nút **Browse**.
 - Chọn tùy chọn **This program can run only on specified platforms** trong mục **Platform requirements** 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 **Summary**, kiểm tra tất cả các giá trị được nhập của cấu hình và nhấn **Next**.

Gói cài đặt được tạo sẽ xuất hiện trong mục **Packages** trong danh sách các gói cài đặt khả dụng.
5. Trong menu ngữ cảnh của gói cài đặt, chọn **Deploy**.
Việc này sẽ bắt đầu *Trình hướng dẫn Triển khai*.

6. Trong Trình hướng dẫn Triển khai:

a. Trong mục **General**:

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

b. Trong mục **Contains**, bổ sung các điểm phân phối (để biết thêm chi tiết, vui lòng tham khảo tài liệu trợ giúp cho Trình Quản lý Cấu hình 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 **Summary**, kiểm tra tất cả các giá trị được nhập của cấu hình và nhấn **Next**.

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.

[TẢI XUỐNG TẬP TIN SETUP.INI](#)

Tập tin setup.ini bao gồm các phần sau:

- **[Setup]** - thiết lập tổng quát cho bản cài đặt ứng dụng.
- **[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. Bảo vệ mối đe dọa 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. Thành phần Managed Detection and Response component cũng không có trong mục này. Để cài đặt thành phần này, bạn phải [kích hoạt Managed Detection and Response trong Bảng điều khiển Kaspersky Security Center](#).
- **[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=1	<p>Chấp nhận 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.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>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.</p> </div>
	PrivacyPolicy=1	<p>Chấp nhận Chính sách quyền riêng tư. Văn bản của Chính sách quyền riêng tư được bao gồm trong gói phân phối của Kaspersky Endpoint Security.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Để cài đặt ứng dụng hoặc nâng cấp ứng dụng phiên bản ứng dụng, bạn phải chấp nhận Chính sách quyền riêng tư.</p> </div>
	KSN	<p>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 khả dụng:</p> <ul style="list-style-type: none"> • 1 - đồng ý tham gia KSN. • 0 - từ chối tham gia KSN (giá trị mặc định). <p>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.</p>
	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 KAdmin được sử dụng theo mặc định.
	Mật khẩu	<p>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).</p> <p>Nếu bạn quy định một mật khẩu nhưng không quy định tên người dùng với tham số Đăng nhập, tên người dùng mặc định KAdmin sẽ được sử dụng.</p>
	PasswordArea	Quy định phạm vi của mật khẩu để truy cập Kaspersky Endpoint Security. Khi người dùng cố

		<p>gắng thực hiện một hành động có trong phạm vi này, Kaspersky Endpoint Security sẽ hỏi thông tin tài khoản của người dùng (các tham số Tên đăng nhập và Mật khẩu). Sử dụng ký tự " ; " để nhập nhiều giá trị.</p> <p>Giá trị khả dụng:</p> <ul style="list-style-type: none"> • 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	<p>Bật hoặc tắt cơ cấu bảo vệ cài đặt ứng dụng. Giá trị khả dụng:</p> <ul style="list-style-type: none"> • 1 – Cơ cấu bảo vệ cài đặt ứng dụng được bật (giá trị mặc định). • 0 – Cơ cấu bảo vệ cài đặt ứng dụng bị tắt. <p>Bảo vệ quá trình cài đặt bao gồm tính năng bảo vệ chống lại nguy cơ thay thế gói phân phối bằng các ứng dụng độc hại, chặn truy cập đến thư mục cài đặt của Kaspersky Endpoint Security, và chặn truy cập đến phần 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.</p>
	Reboot=1	<p>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.</p> <p>Không cần khởi động lại khi cài đặt Kaspersky Endpoint Security. Chỉ cần khởi động lại nếu bạn đã 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.</p>
	AddEnvironment	<p>Trong biến hệ thống %PATH%, bổ sung đường dẫn đến các tập tin thực thi trong thư mục cài đặt Kaspersky Endpoint Security. Giá trị khả dụng:</p>

		<ul style="list-style-type: none"> • 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	<p>Bật hoặc tắt tính năng bảo vệ các tiến trình Kaspersky Endpoint Security bằng công nghệ AM-PPL (Antimalware Protected Process Light). Để biết thêm chi tiết về công nghệ AM-PPL, vui lòng truy cập website Microsoft.</p> <p>Công nghệ AM-PPL có sẵn trên hệ điều hành Windows 10 phiên bản 1703 (RS2) hoặc mới hơn và Windows Server 2019.</p> <p>Giá trị khả dụng:</p> <ul style="list-style-type: none"> • 1 – Tính năng bảo vệ các tiến trình Kaspersky Endpoint Security bằng công nghệ AM-PPL được bật. • 0 – Tính năng bảo vệ các tiến trình Kaspersky Endpoint Security bằng công nghệ AM-PPL bị tắt.
	SetupReg	<p>Cho phép ghi các khóa registry từ tập tin setup.reg vào registry. SetupReg: setup.reg giá trị tham số.</p>
	EnableTraces	<p>Bật hoặc tắt truy vết ứng dụng. Sau khi Kaspersky Endpoint Security khởi chạy, ứng dụng sẽ lưu các tập tin dấu vết vào thư mục %ProgramData%\Kaspersky Lab\KES\Traces. Giá trị khả dụng:</p> <ul style="list-style-type: none"> • 1 – truy vết được bật. • 0 – truy vết bị tắt (giá trị mặc định).
	TracesLevel	<p>Cấp chi tiết dấu vết. Giá trị khả dụng:</p> <ul style="list-style-type: none"> • 100 (nghiêm trọng). Chỉ thông báo về các 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 cảnh báo. • 400 (quan trọng). Tất cả các thông báo lỗi, cảnh báo và thông tin bổ sung. • 500 (bình thường). Thông báo về tất cả các lỗi và cảnh báo, cũng như thông tin chi tiết về hoạt động của ứng dụng trong chế độ bình thường (mặc định).

		<ul style="list-style-type: none"> • 600 (thấp). Tắt cả các thông báo.
	RESTAPI	<p>Quản lý ứng dụng thông qua REST API. Để quản lý ứng dụng thông qua REST API, bạn phải chỉ định tên người dùng (tham số RESTAPI_User).</p> <p>Giá trị khả dụng:</p> <ul style="list-style-type: none"> • 1 - quản lý thông qua REST API được cho phép. • 0 - quản lý thông qua REST API bị chặn (giá trị mặc định). <p>Để quản lý ứng dụng thông qua REST API, bạn phải cho phép quản lý bằng các hệ thống quản trị. Để thực hiện, hãy đặt tham số AdminKitConnector=1. Nếu bạn quản lý ứng dụng thông qua REST API, bạn không thể quản lý ứng dụng bằng các hệ thống quản trị của Kaspersky.</p>
	RESTAPI_User	<p>Tên người dùng của tài khoản miền Windows được sử dụng để quản lý ứng dụng thông qua REST API. Quản lý ứng dụng thông qua REST API chỉ khả dụng cho người dùng này. Nhập tên người dùng theo định dạng <DOMAIN>\<Tên người dùng> (ví dụ: RESTAPI_User=COMPANY\Administrator). Bạn chỉ có thể chọn một người dùng để làm việc với REST API.</p> <p>Thêm tên người dùng là điều kiện tiên quyết để quản lý ứng dụng thông qua REST API.</p>
	RESTAPI_Port	<p>Cổng được sử dụng để quản lý ứng dụng thông qua REST API. Cổng 6782 được sử dụng theo mặc định.</p>
	RESTAPI_Certificate	<p>Chứng chỉ để xác định các yêu cầu (ví dụ: RESTAPI_Certificate=C:\cert.pem). Tương tác bảo mật của Kaspersky Endpoint Security với máy khách REST yêu cầu định cấu hình nhận dạng yêu cầu. Để thực hiện, bạn phải cài đặt chứng một chỉ và sau đó ký vào tải trọng của mỗi yêu cầu.</p>
[Components]	ALL	<p>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.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Do cách các giải pháp Detection and Response được hỗ trợ, Endpoint Detection and Response Optimum cũng như các thành phần của Kaspersky Sandbox được cài đặt trên máy tính. Thành phần Endpoint Detection and Response Expert không tương thích với cấu hình này.</p> </div>
	MailThreatProtection	<p>Bảo vệ mối đe dọa thư điện tử.</p>
	WebThreatProtection	<p>Bảo vệ mối đe dọa web.</p>
	AMSI	<p>Bảo vệ AMSI.</p>

	HostIntrusionPrevention	Phòng chống xâm nhập máy chủ.
	BehaviorDetection	Phát hiện hành vi.
	ExploitPrevention	Phòng chống khai thác.
	RemediationEngine	Công cụ khắc phục.
	Tường lửa	Tường lửa.
	NetworkThreatProtection	Bảo vệ mối đe dọa mạng.
	WebControl	Kiểm soát Web.
	DeviceControl	Kiểm soát thiết bị.
	ApplicationControl	Kiểm soát ứng dụng.
	AdaptiveAnomaliesControl	Kiểm soát thích ứng sự cố.
	FileEncryption	Thư viện Mã hóa mức độ tập tin.
	DiskEncryption	Thư viện Mã hóa toàn bộ ổ đĩa.
	BadUSBAttackPrevention	Phòng chống Tấn công BadUSB.
	EDR	Endpoint Detection and Response Optimum (EDR Optimum). Thành phần này không tương thích với thành phần EDR Expert (EDRCloud).
	EDRCloud	Endpoint Detection and Response Expert (EDR Expert). Thành phần này không tương thích với thành phần EDR Optimum (EDR).
	SB	Kaspersky Sandbox.
	AdminKitConnector	Quản lý ứng dụng bằng các hệ thống quản trị. Kaspersky Security Center là một ví dụ về hệ thống quản trị. Ngoài các hệ thống quản trị của Kaspersky, bạn có thể sử dụng các giải pháp của bên thứ ba. Kaspersky Endpoint Security cung cấp một API cho mục đích này. Giá trị khả dụng: <ul style="list-style-type: none"> • 1 - cho phép quản lý ứng dụng với sự trợ giúp của các hệ thống quản trị (giá trị mặc định). • 0 - chỉ cho phép quản lý ứng dụng qua giao diện cục bộ.
[Tasks]	ScanMyComputer	Tác vụ Quét toàn bộ. Giá trị khả dụng: <ul style="list-style-type: none"> • 1 - Tác vụ này sẽ được bao gồm trong danh sách tác vụ của Kaspersky Endpoint Security.

		<ul style="list-style-type: none"> • 0 – Tác vụ này không được bao gồm trong danh sách tác vụ của Kaspersky Endpoint Security.
	ScanCritical	<p>Tác vụ Quét khu vực quan trọng. Giá trị khả dụng:</p> <ul style="list-style-type: none"> • 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.
	Updater	<p>Tác vụ cập nhật. Giá trị khả dụng:</p> <ul style="list-style-type: none"> • 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.

Thay đổi thành phần ứng dụng

Trong quá trình cài đặt ứng dụng, bạn có thể chọn các thành phần sẽ khả dụng. Bạn có thể thay đổi các thành phần ứng dụng khả dụng theo các cách sau:

- Cục bộ bằng cách sử dụng Trình hướng dẫn cài đặt.

Các thành phần của ứng dụng được thay đổi bằng phương thức thông thường dành cho hệ điều hành Windows, thông qua Control Panel. Chạy Trình hướng dẫn cài đặt ứng dụng và chọn tùy chọn để thay đổi các thành phần ứng dụng khả dụng. Làm theo chỉ dẫn trên màn hình.

- Từ xa thông qua Kaspersky Security Center.

Tác vụ *Thay đổi thành phần ứng dụng* cho phép bạn thay đổi các thành phần của Kaspersky Endpoint Security sau khi cài đặt ứng dụng.

Vui lòng lưu ý các điểm cần nhắc đặc biệt sau đây khi thay đổi thành phần ứng dụng:

- Trên các máy tính chạy Windows Server, bạn không thể [cài đặt tất cả các thành phần của Kaspersky Endpoint Security](#) (ví dụ: thành phần Kiểm soát thích ứng sự cố sẽ không khả dụng).
- Nếu các ổ đĩa cứng trên máy tính của bạn được bảo vệ bởi [Mã hóa toàn bộ ổ đĩa \(FDE\)](#) thì bạn không thể xóa thành phần Mã hóa toàn bộ ổ đĩa. Để xóa thành phần Mã hóa toàn bộ ổ đĩa, hãy giải mã tất cả các ổ đĩa cứng của máy tính.
- Nếu máy tính có [các tập tin được mã hóa \(FLE\)](#) hoặc người dùng sử dụng [các ổ di động được mã hóa \(FDE hoặc FLE\)](#) thì bạn sẽ không thể truy cập các tập tin và ổ đĩa di động sau khi các thành phần Mã hóa dữ liệu bị xóa. Bạn có thể truy cập các tập tin và ổ đĩa di động bằng cách cài đặt lại các thành phần Mã hóa dữ liệu.

[Cách thêm hoặc xóa các thành phần ứng dụng trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Trong Bảng điều khiển quản trị, hãy vào thư mục **Administration Server** → **Tác vụ**.

Danh sách tác vụ sẽ mở.

2. Nhấn nút **New task**.

Trình hướng dẫn Tác vụ sẽ được bắt đầu. Làm theo chỉ dẫn của Trình hướng dẫn.

Bước 1. Chọn loại tác vụ

Chọn **Kaspersky Endpoint Security cho Windows (11.9.0)** → **Change application components**.

Bước 2. Thiết lập tác vụ để thay đổi các thành phần ứng dụng

Chọn các thành phần ứng dụng sẽ khả dụng trên máy tính của người dùng.

Chọn hộp kiểm **Gỡ bỏ ứng dụng không tương thích của hãng thứ ba**. Bạn có thể xem danh sách các ứng dụng không tương thích trong `incompatible.txt`, được kèm theo [gói phân phối](#). Nếu các ứng dụng không tương thích được cài đặt trên một máy tính, quy trình cài đặt Kaspersky Endpoint Security sẽ kết thúc với một lỗi.

Nếu cần, bật [bảo vệ bằng mật khẩu](#) để thực hiện tác vụ:

1. Nhấn vào **Bổ sung**.

2. Chọn hộp kiểm **Sử dụng mật khẩu để chỉnh sửa bộ thành phần ứng dụng**.

3. Nhập thông tin tài khoản người dùng của KAdmin.

Bước 3. Chọn các thiết bị sẽ được gán tác vụ

Chọn các máy tính sẽ được thực hiện tác vụ trên đó. Các tùy chọn sau có thể được sử dụng:

- Gán tác vụ vào một nhóm quản trị. Trong trường hợp này, tác vụ sẽ được gán cho các máy tính được bao gồm trong một nhóm quản trị đã được tạo trước đó.
- Chọn các máy tính được Máy chủ quản trị phát hiện trong mạng – *các thiết bị chưa được gán*. Các thiết bị được quy định có thể bao gồm các thiết bị trong nhóm quản trị cũng như các thiết bị chưa được gán.
- Nhập vào thủ công địa chỉ của thiết bị, hoặc nhập các địa chỉ từ một danh sách. Bạn có thể quy định tên NetBIOS, địa chỉ IP, và địa chỉ IP mạng con của các thiết bị mà bạn muốn gán tác vụ.

Bước 4. Cấu hình lịch khởi chạy tác vụ

Cấu hình lịch khởi chạy một tác vụ, ví dụ như khởi chạy thủ công hoặc khi máy tính rảnh.

Bước 5. Xác định tên tác vụ

Nhập tên cho tác vụ, ví dụ: *Thêm thành phần Kiểm soát ứng dụng.*

Bước 6. Hoàn tất việc tạo tác vụ

Thoát Trình hướng dẫn. Nếu cần, hãy chọn hộp kiểm **Run the task after the Wizard finishes**. Bạn có thể giám sát tiến độ của tác vụ trong thuộc tính tác vụ.

Kết quả là nhóm các thành phần Kaspersky Endpoint Security trên máy tính người dùng sẽ được thay đổi trong chế độ im lặng. Thiết lập của các thành phần khả dụng sẽ được hiển thị trong giao diện cục bộ của ứng dụng. Các thành phần chưa được bao gồm trong ứng dụng sẽ bị tắt, và không thể thiết lập cho các thành phần này.

[Cách thêm hoặc xóa các thành phần ứng dụng trong Bảng điều khiển web và Bảng điều khiển đám mây.](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.

Danh sách tác vụ sẽ mở.

2. Nhấn vào nút **Thêm**.

Trình hướng dẫn Tác vụ sẽ được bắt đầu. Làm theo chỉ dẫn của Trình hướng dẫn.

Bước 1. Cấu hình thiết lập tác vụ tổng quát

Cấu hình thiết lập của tác vụ tổng quát:

1. Trong danh sách thả xuống **Ứng dụng**, hãy chọn **Kaspersky Endpoint Security cho Windows (11.9.0)**.
2. Trong danh sách thả xuống **Loại tác vụ**, chọn **Change application components**.
3. Trong trường **Task name**, nhập một mô tả ngắn, ví dụ như *Thêm thành phần Kiểm soát ứng dụng*.
4. Trong phần **Select devices to which the task will be assigned**, chọn phạm vi tác vụ.

Bước 2. Chọn các thiết bị sẽ được gán tác vụ

Chọn các máy tính sẽ được thực hiện tác vụ trên đó. Ví dụ: chọn một nhóm quản trị riêng hoặc xây dựng một bộ.

Bước 3. Hoàn tất việc tạo tác vụ

Chọn hộp kiểm **Open task details when creation is complete** và kết thúc Trình hướng dẫn. Trong thuộc tính tác vụ, hãy chọn thẻ **Application settings** và chọn các thành phần ứng dụng sẽ khả dụng.

Nếu cần, bật [bảo vệ bằng mật khẩu](#) để thực hiện tác vụ:

1. Trong mục **Thiết lập nâng cao**, hãy chọn hộp kiểm **Sử dụng mật khẩu để chỉnh sửa bộ thành phần ứng dụng**.
2. Nhập thông tin tài khoản người dùng của KLAAdmin.

Lưu các thay đổi và chạy tác vụ.

Kết quả là nhóm các thành phần Kaspersky Endpoint Security trên máy tính người dùng sẽ được thay đổi trong chế độ im lặng. Thiết lập của các thành phần khả dụng sẽ được hiển thị trong giao diện cục bộ của ứng dụng. Các thành phần chưa được bao gồm trong ứng dụng sẽ bị tắt, và không thể thiết lập cho các thành phần này.

Nâng cấp từ phiên bản trước của ứng dụng

Khi bạn cập nhật một phiên bản cũ của ứng dụng lên một phiên bản mới hơn, hãy cân nhắc những điều sau:

- Chúng tôi khuyến nghị bạn thoát tất cả các ứng dụng đang hoạt động trước khi bắt đầu cập nhật.
- Nếu máy tính có ổ đĩa cứng được mã hóa bằng [Mã hóa toàn bộ ổ đĩa \(FDE\)](#) thì bạn cần giải mã tất cả các ổ đĩa cứng được mã hóa để nâng cấp Kaspersky Endpoint Security từ phiên bản 10 lên phiên bản 11.0.0 hoặc cao hơn.

Trước khi cập nhật, Kaspersky Endpoint Security sẽ chặn chức năng Mã hóa toàn bộ ổ đĩa. Nếu Mã hóa toàn bộ ổ đĩa không thể bị khóa, tác vụ cài đặt bản nâng cấp sẽ không thể bắt đầu. Sau khi cập nhật ứng dụng, chức năng Mã hóa toàn bộ ổ đĩa sẽ được khôi phục.

Kaspersky Endpoint Security hỗ trợ các bản cập nhật cho các phiên bản sau của ứng dụng:

- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 cho Windows (bản dựng 10.3.3.304).
- Kaspersky Endpoint Security 11.1.0 cho Windows (bản dựng 11.1.0.15919).
- Kaspersky Endpoint Security 11.1.1 cho Windows (bản dựng 11.1.1.126).
- Kaspersky Endpoint Security 11.2.0 cho Windows (bản dựng 11.2.0.2254).
- Kaspersky Endpoint Security 11.2.0 cho Windows CF1 (bản dựng 11.2.0.2254).
- Kaspersky Endpoint Security 11.3.0 cho Windows (bản dựng 11.3.0.773).
- Kaspersky Endpoint Security 11.4.0 cho Windows (bản dựng 11.4.0.233).
- Kaspersky Endpoint Security 11.5.0 cho Windows (bản dựng 11.5.0.590).
- Kaspersky Endpoint Security 11.6.0 cho Windows (bản dựng 11.6.0.394).
- Kaspersky Endpoint Security 11.7.0 cho Windows (bản dựng 11.7.0.669).
- Kaspersky Endpoint Security 11.8.0 cho Windows (bản dựng 11.8.0.384).

Khi nâng cấp Kaspersky Endpoint Security 10 Service Pack 2 cho Windows lên Kaspersky Endpoint Security 11.9.0 cho Windows, các tập tin đã được đặt trong Sao lưu hoặc Khu vực cách ly ở phiên bản trước của ứng dụng sẽ được chuyển sang Sao lưu trong phiên bản mới của ứng dụng. Đối với các phiên bản cũ hơn Kaspersky Endpoint Security 10 Service Pack 2 cho Windows, các tập tin đã được đặt trong Sao lưu hoặc Cách ly ở phiên bản cũ của ứng dụng sẽ không được chuyển sang phiên bản mới.

Kaspersky Endpoint Security có thể được cập nhật trên một máy tính theo các cách sau:

- cục bộ bằng cách sử dụng [Trình hướng dẫn cài đặt](#).
- cục bộ từ [dòng lệnh](#).
- từ xa thông qua [Kaspersky Security Center](#).

- từ xa thông qua Microsoft Windows Group Policy Management Editor (để biết thêm thông tin, hãy truy cập [trang web Hỗ trợ kỹ thuật của Microsoft](#)).
- từ xa sử dụng [Trình Quản lý cấu hình trung tâm hệ thống](#).

Nếu ứng dụng được triển khai trong mạng công ty có một nhóm các thành phần khác với nhóm mặc định, thì việc cập nhật ứng dụng qua Bảng điều khiển quản trị (MMC) sẽ khác với việc cập nhật ứng dụng qua Bảng điều khiển web và Bảng điều khiển đám mây. Khi bạn cập nhật Kaspersky Endpoint Security, hãy cân nhắc các điều sau:

- Bảng điều khiển web Kaspersky Security Center hoặc Bảng điều khiển đám mây Kaspersky Security Center.

Nếu bạn đã tạo gói cài đặt cho phiên bản mới của ứng dụng bằng nhóm thành phần mặc định thì nhóm thành phần trên máy tính của người dùng sẽ không bị thay đổi. Để sử dụng Kaspersky Endpoint Security với nhóm thành phần mặc định, bạn cần [mở thuộc tính gói cài đặt](#), thay đổi nhóm thành phần, sau đó khôi phục lại nhóm thành phần ban đầu và lưu các thay đổi.

- Bảng điều khiển quản trị Kaspersky Security Center.

Nhóm thành phần ứng dụng sau khi cập nhật sẽ khớp với nhóm thành phần trong gói cài đặt. Điều này có nghĩa là nếu phiên bản mới của ứng dụng có nhóm thành phần mặc định thì thành phần như Phòng chống Tấn công BadUSB sẽ bị xóa khỏi máy tính, vì thành phần này được loại trừ khỏi nhóm mặc định. Để tiếp tục sử dụng ứng dụng có cùng nhóm thành phần như trước khi cập nhật, hãy chọn các thành phần bắt buộc trong [thiết lập gói cài đặt](#).

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.

Gỡ bỏ ứng dụng từ xa

Bạn có thể gỡ bỏ ứng dụng từ xa thông qua tác vụ *Gỡ bỏ ứng dụng từ xa*. Khi thực hiện tác vụ này, Kaspersky Endpoint Security sẽ tải tiện ích gỡ bỏ ứng dụng về máy tính của người dùng. Sau khi hoàn tất gỡ bỏ ứng dụng, tiện ích này sẽ được xóa tự động.

[Cách gỡ bỏ ứng dụng thông qua Bảng điều khiển quản trị \(MMC\)](#)

1. Trong Bảng điều khiển quản trị, hãy vào thư mục **Administration Server** → **Tác vụ**.

Danh sách tác vụ sẽ mở.

2. Nhấn nút **New task**.

Trình hướng dẫn Tác vụ sẽ được bắt đầu. Làm theo chỉ dẫn của Trình hướng dẫn.

Bước 1. Chọn loại tác vụ

Chọn **Kaspersky Security Center Administration Server** → **Bổ sung** → **Uninstall application remotely**.

Bước 2. Chọn ứng dụng cần gỡ bỏ

Chọn **Uninstall application supported by Kaspersky Security Center**.

Bước 3. Thiết lập tác vụ để gỡ bỏ ứng dụng

Chọn **Kaspersky Endpoint Security cho Windows (11.9.0)**.

Bước 4. Gỡ bỏ thiết lập tiện ích

Cấu hình các thiết lập ứng dụng bổ sung sau:

- **Force download of the uninstallation utility.** Chọn phương thức gửi tiện ích:
 - **Using Network Agent.** Nếu Network Agent chưa được cài đặt trên máy tính, trước tiên, Network Agent sẽ được cài đặt sử dụng các công cụ của hệ điều hành. Khi đó, Kaspersky Endpoint Security sẽ được gỡ bỏ bởi các công cụ của Network Agent.
 - **Using operating system resources through Administration Server.** Tiện ích sẽ được gửi đến máy khách bằng tài nguyên của hệ điều hành thông qua Máy chủ quản trị. Bạn có thể chọn tùy chọn này nếu Network Agent không được cài đặt trên máy khách, nhưng máy khách kết nối đến cùng mạng lưới với Máy chủ quản trị.
 - **Using operating system resources through distribution points.** Tiện ích được gửi đến các máy khách sử dụng tài nguyên hệ điều hành thông qua các điểm phân phối. Bạn có thể chọn tùy chọn này nếu có ít nhất một điểm phân phối trong mạng. Để biết thêm chi tiết về các điểm phân phối, hãy tham khảo [Trợ giúp của Kaspersky Security Center](#).
- **Verify operating system type before downloading.** Xóa hộp kiểm này nếu cần. Việc này cho phép bạn tránh tải về tiện ích gỡ bỏ nếu hệ điều hành của máy tính không đáp ứng các yêu cầu về phần mềm. Nếu bạn chắc chắn rằng hệ điều hành của máy tính đáp ứng các yêu cầu về phần mềm, bạn có thể bỏ qua bước xác minh này.

Nếu hoạt động gỡ bỏ ứng dụng được [bảo vệ bằng mật khẩu](#), hãy làm như sau:

1. Chọn hộp kiểm **Use uninstallation password**.

2. Nhấn nút **Chỉnh sửa**.

3. Nhập mật khẩu của tài khoản KAdmin.

Bước 5. Chọn thiết lập khởi động lại hệ điều hành

Sau khi gỡ bỏ ứng dụng, bạn cần phải khởi động lại. Chọn hành động sẽ được thực hiện để khởi động lại máy tính.

Bước 6. Chọn các thiết bị sẽ được gán tác vụ

Chọn các máy tính sẽ được thực hiện tác vụ trên đó. Các tùy chọn sau có thể được sử dụng:

- Gán tác vụ vào một nhóm quản trị. Trong trường hợp này, tác vụ sẽ được gán cho các máy tính được bao gồm trong một nhóm quản trị đã được tạo trước đó.
- Chọn các máy tính được Máy chủ quản trị phát hiện trong mạng – *các thiết bị chưa được gán*. Các thiết bị được quy định có thể bao gồm các thiết bị trong nhóm quản trị cũng như các thiết bị chưa được gán.
- Nhập vào thủ công địa chỉ của thiết bị, hoặc nhập các địa chỉ từ một danh sách. Bạn có thể quy định tên NetBIOS, địa chỉ IP, và địa chỉ IP mạng con của các thiết bị mà bạn muốn gán tác vụ.

Bước 7. Chọn tài khoản để chạy tác vụ

Chọn tài khoản dùng để cài đặt Network Agent sử dụng các công cụ của hệ điều hành. Trong trường hợp này, cần có quyền quản trị viên để truy cập máy tính. Bạn có thể thêm nhiều tài khoản. Nếu một tài khoản không có đủ quyền, Trình hướng dẫn Cài đặt sẽ sử dụng tài khoản tiếp theo. Nếu bạn gỡ bỏ Kaspersky Endpoint Security bằng các công cụ Network Agent, bạn không phải chọn một tài khoản.

Bước 8. Cấu hình lịch khởi chạy tác vụ

Cấu hình lịch khởi chạy một tác vụ, ví dụ như khởi chạy thủ công hoặc khi máy tính rảnh.

Bước 9. Xác định tên tác vụ

Nhập tên cho tác vụ, ví dụ như *Gỡ bỏ Kaspersky Endpoint Security 11.9.0*.

Bước 10. Hoàn thành tạo tác vụ

Thoát Trình hướng dẫn. Nếu cần, hãy chọn hộp kiểm **Run the task after the Wizard finishes**. Bạn có thể giám sát tiến độ của tác vụ trong thuộc tính tác vụ.

Ứng dụng sẽ được gỡ bỏ trong chế độ im lặng.

[Cách gỡ bỏ ứng dụng thông qua Bảng điều khiển web và Bảng điều khiển đám mây](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.

Danh sách tác vụ sẽ mở.

2. Nhấn vào nút **Thêm**.

Trình hướng dẫn Tác vụ sẽ được bắt đầu. Làm theo chỉ dẫn của Trình hướng dẫn.

Bước 1. Cấu hình thiết lập tác vụ tổng quát

Cấu hình thiết lập của tác vụ tổng quát:

1. Trong danh sách thả xuống **Ứng dụng**, chọn **Kaspersky Security Center**.
2. Trong danh sách thả xuống **Loại tác vụ**, chọn **Uninstall application remotely**.
3. Trong trường **Task name**, nhập một mô tả ngắn gọn, ví dụ như *Gỡ bỏ Kaspersky Endpoint Security khỏi các máy tính của bộ phận Hỗ trợ kỹ thuật*.
4. Trong phần **Select devices to which the task will be assigned**, chọn phạm vi tác vụ.

Bước 2. Chọn các thiết bị sẽ được gán tác vụ

Chọn các máy tính sẽ được thực hiện tác vụ trên đó. Ví dụ: chọn một nhóm quản trị riêng hoặc xây dựng một bộ.

Bước 3. Cấu hình thiết lập gỡ bỏ ứng dụng

Ở bước này, hãy cấu hình thiết lập gỡ bỏ ứng dụng:

1. Chọn **Uninstall managed application**.
2. Chọn **Kaspersky Endpoint Security cho Windows (11.9.0)**.
3. **Force download of the uninstallation utility**. Chọn phương thức gửi tiện ích:
 - **Using Network Agent**. Nếu Network Agent chưa được cài đặt trên máy tính, trước tiên, Network Agent sẽ được cài đặt sử dụng các công cụ của hệ điều hành. Khi đó, Kaspersky Endpoint Security sẽ được gỡ bỏ bởi các công cụ của Network Agent.
 - **Using operating system resources through Administration Server**. Tiện ích sẽ được gửi đến máy khách bằng tài nguyên của hệ điều hành thông qua Máy chủ quản trị. Bạn có thể chọn tùy chọn này nếu Network Agent không được cài đặt trên máy khách, nhưng máy khách kết nối đến cùng mạng lưới với Máy chủ quản trị.
 - **Using operating system resources through distribution points**. Tiện ích được gửi đến các máy khách sử dụng tài nguyên hệ điều hành thông qua các điểm phân phối. Bạn có thể chọn tùy chọn này nếu có ít nhất một điểm phân phối trong mạng. Để biết thêm chi tiết về các điểm phân phối, hãy tham khảo [Trợ giúp của Kaspersky Security Center](#).
4. Trong trường **Maximum number of concurrent downloads**, hãy đặt giới hạn số lượng yêu cầu được gửi đến Máy chủ quản trị để tải về tiện ích gỡ bỏ ứng dụng. Giới hạn số yêu cầu sẽ ngăn

mạng khỏi bị quá tải.

- Trong trường hợp **Maximum number of uninstallation attempts**, hãy thiết lập giới hạn về số lượt thử gỡ cài đặt ứng dụng. Nếu quá trình gỡ bỏ Kaspersky Endpoint Security kết thúc với một lỗi, tác vụ này sẽ tự động khởi chạy lại quá trình gỡ bỏ.
- Nếu cần, hãy xóa hộp kiểm **Verify operating system type before downloading**. Việc này cho phép bạn tránh tải về tiện ích gỡ bỏ nếu hệ điều hành của máy tính không đáp ứng các yêu cầu về phần mềm. Nếu bạn chắc chắn rằng hệ điều hành của máy tính đáp ứng các yêu cầu về phần mềm, bạn có thể bỏ qua bước xác minh này.

Bước 4. Chọn tài khoản để chạy tác vụ

Chọn tài khoản dùng để cài đặt Network Agent sử dụng các công cụ của hệ điều hành. Trong trường hợp này, cần có quyền quản trị viên để truy cập máy tính. Bạn có thể thêm nhiều tài khoản. Nếu một tài khoản không có đủ quyền, Trình hướng dẫn Cài đặt sẽ sử dụng tài khoản tiếp theo. Nếu bạn gỡ bỏ Kaspersky Endpoint Security bằng các công cụ Network Agent, bạn không phải chọn một tài khoản.

Bước 5. Hoàn tất việc tạo tác vụ

Hoàn tất trình hướng dẫn bằng cách nhấn nút **Hoàn tất**. Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ.

Để thực hiện một tác vụ, chọn hộp kiểm cạnh tác vụ đó và nhấn nút **Bắt đầu**. Ứng dụng sẽ được gỡ bỏ trong chế độ im lặng. Sau khi quá trình gỡ bỏ hoàn tất, Kaspersky Endpoint Security sẽ hiển thị yêu cầu khởi động lại máy tính.

Nếu hoạt động gỡ bỏ ứng dụng được [bảo vệ bằng mật khẩu](#), hãy nhập mật khẩu của tài khoản KLAdmin vào thuộc tính của tác vụ *Gỡ bỏ ứng dụng từ xa*. Nếu không có mật khẩu, tác vụ sẽ không được thực hiện.

Để sử dụng mật khẩu của tài khoản KLAdmin trong tác vụ Gỡ bỏ ứng dụng từ xa:

- Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.
Danh sách tác vụ sẽ mở.
- Nhấn vào tác vụ **Uninstall application remotely** của Kaspersky Security Center.
Cửa sổ thuộc tính tác vụ sẽ được mở ra.
- Chọn thẻ **Application settings**.
- Chọn hộp kiểm **Use uninstallation password**.
- Nhập mật khẩu của tài khoản KLAdmin.
- Lưu các thay đổi của bạn.

Bạn cũng có thể xóa ứng dụng từ xa thông qua Microsoft Windows Group Policy Management Editor (để biết thêm thông tin, hãy truy cập [trang web Hỗ trợ kỹ thuật của Microsoft](#)).

Gỡ bỏ ứng dụng cục bộ

Bạn có thể gỡ bỏ ứng dụng trên máy bằng Trình hướng dẫn cài đặt. Kaspersky Endpoint Security được gỡ bỏ bằng phương thức thông thường dành cho hệ điều hành Windows, thông qua Control Panel. Trình hướng dẫn cài đặt sẽ được bắt đầu. Làm theo chỉ dẫn trên màn hình.

Bạn có thể chỉ định phần dữ liệu nào được ứng dụng sử dụng mà bạn muốn lưu để sử dụng sau này, trong quá trình cài đặt ứng dụng lần tới (như khi cập nhật lên phiên bản ứng dụng mới hơn). Nếu bạn không chỉ định bất cứ dữ liệu nào thì ứng dụng sẽ được gỡ bỏ hoàn toàn.

Bạn có thể lưu các dữ liệu sau:

- **Dữ liệu kích hoạt**, cho phép bạn không cần phải kích hoạt lại ứng dụng. Kaspersky Endpoint Security sẽ tự động thêm một mã khóa giấy phép nếu như thời hạn giấy phép chưa hết hạn trước khi cài đặt.
- **Tập tin sao lưu** – các tập tin được quét bởi ứng dụng và chuyển vào mục Sao lưu.

Các tập tin Sao lưu 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 dự định sử dụng các đối tượng Sao lưu sau khi gỡ bỏ ứng dụng, bạn phải khôi phục các đối tượng đó trước khi gỡ bỏ ứng dụng. Tuy nhiên, các chuyên gia Kaspersky không khuyến nghị việc khôi phục các đối tượng từ Sao lưu bởi điều đó có thể gây hại cho máy tính.

- **Thiết lập hoạt động cho 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 các tập tin và ổ đĩa được mã hóa trước khi gỡ bỏ ứng dụng. Để chắc chắn có quyền truy cập đến các tập tin và ổ đĩa được mã hóa, đảm bảo rằng bạn đã chọn chức năng mã hóa dữ liệu khi cài đặt lại Kaspersky Endpoint Security. Bạn không cần thực hiện hành động nào nữa để có quyền truy cập các tập tin và ổ đĩa được mã hóa.

Bạn cũng có thể xóa ứng dụng cục bộ bằng [dòng lệnh](#).

Cấp giấy phép ứng dụng

Mục này cung cấp thông tin về các khái niệm chung liên quan đến cấp phép sử dụng Kaspersky Endpoint Security.

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 kèm theo [gói phân phối ứng dụng](#) và cũng được đưa vào thư mục cài đặt ứng dụng %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Endpoint Security for Windows\Doc\\KES.

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.

Giấy phép trao cho bạn quyền sử dụng ứng dụng theo các điều khoản của Thỏa thuận giấy phép người dùng cuối và được nhận hỗ trợ kỹ thuật. Danh sách tính năng khả dụng 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 chỉ 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:

- Khóa giấy phép hoặc 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 (ví dụ như thời hạn kết thúc gói đăng ký và 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 hết hạn thời hạn đăng ký có giới hạn, bạn cần 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.

Khi một gói đăng ký hạn chế hết hạn, bạn có thể sẽ được cung cấp một thời gian ân hạn để gia hạn gói đăng ký, trong thời gian này ứng dụng sẽ tiếp tục hoạt động. Tình trạng sẵn có và thời hạn của thời gian ân hạn đó được quyết định bởi nhà cung cấp dịch vụ.

Để sử dụng ứng dụng Kaspersky Endpoint Security theo gói đăng ký, bạn cần áp dụng [mã kích hoạt](#) nhận được từ nhà cung cấp dịch vụ. Sau khi mã kích hoạt đã được áp dụng, khóa hiện hoạt sẽ được thêm. Khóa hiện hoạt xác định giấy phép để sử dụng ứng dụng theo gói đăng ký. Bạn không thể kích hoạt ứng dụng theo gói đăng ký bằng [tập tin khóa](#). Nhà cung cấp dịch vụ chỉ có thể cung cấp mã kích hoạt. Bạn không thể thêm khóa dự trữ theo gói đăng ký.

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 khóa giấy phép

Khóa giấy phép là một chuỗi các bit mà bạn có thể sử dụng để kích hoạt và sau đó sử dụng ứng dụng theo các điều khoản của Thỏa thuận giấy phép người dùng cuối.

Một [chứng chỉ giấy phép](#) không được cung cấp cho khóa được thêm theo diện gói đăng ký.

Bạn có thể thêm khóa giấy phép cho ứng dụng bằng cách áp dụng tập tin khóa hoặc nhập mã kích hoạt.

Khóa có thể bị chặn bởi Kaspersky nếu các điều khoản của Thỏa thuận giấy phép người dùng cuối bị vi phạm. Nếu khóa đó đã bị chặn, bạn cần thêm một khóa khác để có thể tiếp tục sử dụng ứng dụng.

Có hai loại khóa: hiện hoạt và dự trữ.

Khóa hiện 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 hiện hoạt. Ứng dụng không thể có nhiều hơn một khóa hiện hoạt.

Khóa dự trữ là khóa chứng chỉ quyền sử dụng ứng dụng của người dùng, nhưng hiện không được sử dụng. Khi khóa hiện hoạt hết hạn sử dụng, một khóa dự trữ sẽ tự động được kích hoạt. Bạn chỉ có thể thêm khóa dự trữ khi đã có khóa hiện hoạt.

Một khóa cho giấy phép dùng thử chỉ có thể được thêm làm khóa hiện hoạt. Bạn không thể thêm nó làm khóa dự trữ. Một khóa cho giấy phép dùng thử không thể thay thế khóa hiện hoạt của một giấy phép thương mại.

Nếu một khóa được thêm vào danh sách các khóa bị cấm thì chức năng ứng dụng được xác định theo [giấy phép được sử dụng để kích hoạt ứng dụng](#) vẫn khả dụng trong tám ngày. Ứng dụng sẽ thông báo cho người dùng biết rằng khóa đã được thêm vào danh sách các khóa bị cấm. Sau tám ngày, chức năng ứng dụng sẽ bị giới hạn ở cấp độ chức năng khả dụng sau khi giấy phép đã hết hạn. Bạn có thể sử dụng các thành phần bảo vệ và kiểm soát, và chạy tác vụ quét sử dụng các cơ sở dữ liệu đã được cài đặt trước khi giấy phép bị hết hạn. Ứng dụng cũng sẽ tiếp tục mã hóa các tập tin đã được thay đổi và mã hóa trước khi hết hạn giấy phép, nhưng sẽ không mã hóa các tập tin mới. Kaspersky Security Network sẽ không còn khả dụng.

Thông tin về mã kích hoạt

Mã kích hoạt là một chuỗi duy nhất, bao gồm 20 ký tự chữ cái và chữ số. Bạn nhập mã kích hoạt để thêm khóa giấy phép kích hoạt Kaspersky Endpoint Security. Bạn nhận được mã kích hoạt tại địa chỉ email mà bạn đã chỉ định sau khi mua 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 bằng một mã kích hoạt, khóa hiện hoạt sẽ được thêm. Bạn chỉ có thể thêm khóa dự trữ bằng cách sử dụng mã kích hoạt và bạn không thể thêm bằng cách sử dụng tập tin khóa.

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](#). Nếu mã kích hoạt bị mất sau khi kích hoạt ứng dụng, hãy liên hệ với đối tác của Kaspersky mà bạn đã mua giấy phép.

Thông tin về tập tin khóa

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

Bạn nhận được một tập tin khóa tại địa chỉ email mà bạn đã cung cấp khi mua Kaspersky Endpoint Security hoặc đặt phiên bản dùng thử của Kaspersky Endpoint Security.

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

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 đơn vị bán giấy phép.
- Nhận tập tin khóa 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 dự trữ bằng cách sử dụng tập tin khóa và bạn không thể thêm bằng cách sử dụng mã kích hoạt.

So sánh chức năng ứng dụng tùy thuộc vào loại giấy phép cho máy trạm

Bộ chức năng của Kaspersky Endpoint Security khả dụng trên máy trạm phụ thuộc vào loại giấy phép (xem bảng bên dưới).

[Bạn cũng nên xem thêm phần so sánh chức năng ứng dụng cho máy chủ](#)

So sánh các tính năng của Kaspersky Endpoint Security

Tính năng	Kaspersky Endpoint Security cho Business Select	Kaspersky Endpoint Security cho Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert
Bảo vệ mỗi đe dọa nâng cao						
Kaspersky Security Network	✓	✓	✓	✓	✓	✓
Phát hiện	✓	✓	✓	✓	✓	✓

hành vi						
Phòng chống khai thác	✓	✓	✓	✓	✓	✓
Phòng chống xâm nhập máy chủ	✓	✓	✓	✓	✓	✓
Công cụ khắc phục	✓	✓	✓	✓	✓	✓
Bảo vệ môi đe dọa thiết yếu						
Bảo vệ môi đe dọa tập tin	✓	✓	✓	✓	✓	✓
Bảo vệ môi đe dọa web	✓	✓	✓	✓	✓	✓
Bảo vệ môi đe dọa thư điện tử	✓	✓	✓	✓	✓	✓
Tường lửa	✓	✓	✓	✓	✓	✓
Bảo vệ môi đe dọa mạng	✓	✓	✓	✓	✓	✓
Phòng chống Tấn công BadUSB	✓	✓	✓	✓	✓	✓
Bảo vệ AMSI	✓	✓	✓	✓	✓	✓
Kiểm soát bảo mật						
Kiểm soát ứng dụng	✓	✓	✓	✓	✓	✓
Kiểm soát Thiết bị	✓	✓	✓	✓	✓	✓
Kiểm soát Web	✓	✓	✓	✓	✓	✓
Kiểm soát thích ứng sự cố	-	✓	✓	✓	✓	✓
Mã hóa dữ liệu						
Kaspersky Disk Encryption	-	✓	✓	✓	✓	✓

BitLocker Drive Encryption	-	✓	✓	✓	✓	✓
Mã hóa mức độ tập tin	-	✓	✓	✓	✓	✓
Mã hóa ổ đĩa di động	-	✓	✓	✓	✓	✓
Detection and Response						
Endpoint Detection and Response Optimum	-	-	-	✓	✓	-
Endpoint Detection and Response Expert	-	-	-	-	-	✓
Kaspersky Sandbox <i>(Phải mua giấy phép Kaspersky Sandbox riêng)</i>	✓	✓	✓	✓	✓	✓

So sánh chức năng ứng dụng tùy thuộc vào loại giấy phép cho máy chủ

Bộ chức năng của Kaspersky Endpoint Security khả dụng trên máy chủ phụ thuộc vào loại giấy phép (xem bảng bên dưới).

[Bạn cũng nên xem thêm phần so sánh chức năng ứng dụng cho máy trạm](#)

So sánh các tính năng của Kaspersky Endpoint Security

Tính năng	Kaspersky Endpoint Security cho Business Select	Kaspersky Endpoint Security cho Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard
Bảo vệ mối đe dọa nâng cao							
Kaspersky	✓	✓	✓	✓	✓	✓	✓

Security Network							
Phát hiện hành vi	✓	✓	✓	✓	✓	✓	✓
Phòng chống khai thác	✓	✓	✓	✓	✓	✓	✓
Phòng chống xâm nhập máy chủ	-	-	-	-	-	-	-
Công cụ khắc phục	✓	✓	✓	✓	✓	✓	✓
Bảo vệ mối đe dọa thiết yếu							
Bảo vệ mối đe dọa tập tin	✓	✓	✓	✓	✓	✓	✓
Bảo vệ mối đe dọa web	-	✓	✓	✓	✓	✓	✓
Bảo vệ mối đe dọa thư điện tử	-	✓	✓	✓	✓	✓	✓
Tường lửa	✓	✓	✓	✓	✓	✓	✓
Bảo vệ mối đe dọa mạng	✓	✓	✓	✓	✓	✓	✓
Phòng chống Tấn công BadUSB	✓	✓	✓	✓	✓	✓	✓
Bảo vệ AMSI	✓	✓	✓	✓	✓	✓	✓
Kiểm soát bảo mật							
Kiểm soát ứng dụng	-	✓	✓	✓	✓	✓	-
Kiểm soát Thiết bị	-	✓	✓	✓	✓	✓	✓
Kiểm soát Web	-	✓	✓	✓	✓	✓	✓
Kiểm soát thích ứng sự cố	-	-	-	-	-	-	-

Mã hóa dữ liệu							
Kaspersky Disk Encryption	-	-	-	-	-	-	-
BitLocker Drive Encryption	-	✓	✓	✓	✓	✓	-
Mã hóa mức độ tập tin	-	-	-	-	-	-	-
Mã hóa ổ đĩa di động	-	-	-	-	-	-	-
Detection and Response							
Endpoint Detection and Response Optimum	-	-	-	✓	✓	-	-
Endpoint Detection and Response Expert	-	-	-	-	-	✓	-
Kaspersky Sandbox <i>(Phải mua giấy phép Kaspersky Sandbox riêng)</i>	✓	✓	✓	✓	✓	✓	✓

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. Quá trình kích hoạt ứng dụng liên quan đến việc bổ sung một [khóa giấy phép](#).

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

- Cục bộ từ giao diện ứng dụng, bằng cách sử dụng [Trình hướng dẫn Kích hoạt](#). Bạn có thể thêm cả khóa hiện hoạt và khóa dự trữ bằng cách này.
- Từ xa với [bộ phần mềm Kaspersky Security Center](#) bằng cách tạo, sau đó khởi chạy một tác vụ thêm khóa giấy phép. Bạn có thể thêm cả khóa hiện hoạt và khóa dự trữ bằng cách này.

- Từ xa bằng cách phân phối tập tin khóa và mã kích hoạt được lưu trữ trong ổ lưu trữ khóa của Máy chủ quản trị Kaspersky Security Center đến các máy khách. Để biết thêm chi tiết về việc phân phối khóa, vui lòng tham khảo [Trợ giúp của Kaspersky Security Center](#). Bạn có thể thêm cả khóa hiện hoạt và khóa dự trữ 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.

Kích hoạt ứng dụng thông qua Kaspersky Security Center

Bạn có thể kích hoạt ứng dụng từ xa thông qua Kaspersky Security Center theo các cách sau:

- Sử dụng tác vụ *Thêm khóa*.

Phương thức này cho phép bạn thêm một khóa vào một máy tính cụ thể hoặc các máy tính thuộc một nhóm quản trị.

- Thông qua việc phân phối một khóa được lưu trữ trên Máy chủ quản trị Kaspersky Security Center đến các máy tính.

Phương thức này cho phép bạn thêm tự động một khóa cho các máy tính đã được kết nối đến Kaspersky Security Center, và cho các máy tính mới. Để dùng phương thức này, trước hết, bạn cần thêm khóa vào Máy chủ quản trị Kaspersky Security Center. Để biết thêm chi tiết về việc thêm khóa vào Máy chủ quản trị Kaspersky Security Center, vui lòng tham khảo [Trợ giúp của Kaspersky Security Center](#).


- Bằng cách thêm khóa vào gói cài đặt Kaspersky Endpoint Security.

Phương thức này cho phép bạn thêm khóa vào [Thuộc tính gói cài đặt](#) trong quá trình triển khai Kaspersky Endpoint Security. Ứng dụng sẽ tự động được kích hoạt sau khi cài đặt.

Phiên bản dùng thử được cung cấp cho Bảng điều khiển đám mây Kaspersky Security Center. *Phiên bản dùng thử* là phiên bản đặc biệt của Bảng điều khiển đám mây Kaspersky Security Center, được thiết kế để giúp người dùng làm quen với các tính năng của ứng dụng. Trong phiên bản này, bạn có thể thực hiện các hành động trong không gian làm việc trong vòng 30 ngày. Tất cả các ứng dụng được quản lý sẽ tự động được chạy theo giấy phép dùng thử dành cho Bảng điều khiển đám mây Kaspersky Security Center, bao gồm cả Kaspersky Endpoint Security. Tuy nhiên, bạn không thể kích hoạt Kaspersky Endpoint Security bằng giấy phép dùng thử của chính nó khi giấy phép dùng thử cho Bảng điều khiển đám mây Kaspersky Security Center hết hạn. Để biết thông tin chi tiết về việc cấp giấy phép cho Kaspersky Security Center, vui lòng tham khảo [Trợ giúp của Bảng điều khiển đám mây Kaspersky Security Center](#).

Phiên bản dùng thử của Bảng điều khiển đám mây Kaspersky Security Center không cho phép bạn chuyển sang phiên bản thương mại sau đó. Bất kỳ không gian làm việc dùng thử nào cũng sẽ tự động bị xóa cùng tất cả nội dung sau khi hết thời gian 30 ngày.

Bạn có thể giám sát việc sử dụng giấy phép theo các cách sau:

- Xem *Báo cáo về việc sử dụng khóa* trong cơ sở hạ tầng của tổ chức (**Monitoring and reporting** → **Reports**).
- Xem trạng thái của máy tính trên thẻ **Devices** → **Managed devices**. Nếu ứng dụng không được kích hoạt, máy tính sẽ có trạng thái  *Ứng dụng chưa được kích hoạt*.
- Xem thông tin giấy phép trong thuộc tính máy tính.
- Xem thuộc tính khóa (**Hoạt động** → **Cấp giấy phép**).

[Cách kích hoạt ứng dụng trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Trong Bảng điều khiển quản trị, hãy vào thư mục **Administration Server** → **Tác vụ**.

Danh sách tác vụ sẽ mở.

2. Nhấn nút **New task**.

Trình hướng dẫn Tác vụ sẽ được bắt đầu. Làm theo chỉ dẫn của Trình hướng dẫn.

Bước 1. Chọn loại tác vụ

Chọn **Kaspersky Endpoint Security cho Windows (11.9.0)** → **Thêm khóa**.

Bước 2. Thêm khóa

Nhập [mã kích hoạt](#) hoặc chọn một tập tin khóa.

Để biết thêm chi tiết về việc thêm khóa vào kho lưu trữ Kaspersky Security Center, vui lòng tham khảo [Trợ giúp của Kaspersky Security Center](#).

Bước 3. Chọn các thiết bị sẽ được gán tác vụ

Chọn các máy tính sẽ được thực hiện tác vụ trên đó. Các tùy chọn sau có thể được sử dụng:

- Gán tác vụ vào một nhóm quản trị. Trong trường hợp này, tác vụ sẽ được gán cho các máy tính được bao gồm trong một nhóm quản trị đã được tạo trước đó.
- Chọn các máy tính được Máy chủ quản trị phát hiện trong mạng – *các thiết bị chưa được gán*. Các thiết bị được quy định có thể bao gồm các thiết bị trong nhóm quản trị cũng như các thiết bị chưa được gán.
- Nhập vào thủ công địa chỉ của thiết bị, hoặc nhập các địa chỉ từ một danh sách. Bạn có thể quy định tên NetBIOS, địa chỉ IP, và địa chỉ IP mạng con của các thiết bị mà bạn muốn gán tác vụ.

Bước 4. Cấu hình lịch khởi chạy tác vụ

Cấu hình lịch khởi chạy một tác vụ, ví dụ như khởi chạy thủ công hoặc khi máy tính rảnh.

Bước 5. Xác định tên tác vụ

Nhập tên cho tác vụ, ví dụ như *Kích hoạt Kaspersky Endpoint Security cho Windows*.

Bước 6. Hoàn tất việc tạo tác vụ

Thoát Trình hướng dẫn. Nếu cần, hãy chọn hộp kiểm **Run the task after the Wizard finishes**. Bạn có thể giám sát tiến độ của tác vụ trong thuộc tính tác vụ. Kết quả là Kaspersky Endpoint Security sẽ được kích hoạt trên máy tính của người dùng trong chế độ im lặng.

Cách kích hoạt ứng dụng trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.

Danh sách tác vụ sẽ mở.

2. Nhấn vào nút **Thêm**.

Trình hướng dẫn Tác vụ sẽ được bắt đầu. Làm theo chỉ dẫn của Trình hướng dẫn.

Bước 1. Cấu hình thiết lập tác vụ tổng quát

Cấu hình thiết lập của tác vụ tổng quát:

1. Trong danh sách thả xuống **Ứng dụng**, hãy chọn **Kaspersky Endpoint Security cho Windows (11.9.0)**.
2. Trong danh sách thả xuống **Loại tác vụ**, hãy chọn **Thêm khóa**.
3. Trong trường **Task name**, nhập một mô tả ngắn gọn, ví dụ như *Kích hoạt Kaspersky Endpoint Security cho Windows*.
4. Trong phần **Select devices to which the task will be assigned**, chọn phạm vi tác vụ. Chuyển sang bước tiếp theo.

Bước 2. Chọn các thiết bị sẽ được gán tác vụ

Chọn các máy tính sẽ được thực hiện tác vụ trên đó. Các tùy chọn sau có thể được sử dụng:

- Gán tác vụ vào một nhóm quản trị. Trong trường hợp này, tác vụ sẽ được gán cho các máy tính được bao gồm trong một nhóm quản trị đã được tạo trước đó.
- Chọn các máy tính được Máy chủ quản trị phát hiện trong mạng – *các thiết bị chưa được gán*. Các thiết bị được quy định có thể bao gồm các thiết bị trong nhóm quản trị cũng như các thiết bị chưa được gán.
- Nhập vào thủ công địa chỉ của thiết bị, hoặc nhập các địa chỉ từ một danh sách. Bạn có thể quy định tên NetBIOS, địa chỉ IP, và địa chỉ IP mạng con của các thiết bị mà bạn muốn gán tác vụ.

Bước 3. Chọn một giấy phép

Chọn giấy phép mà bạn muốn sử dụng để kích hoạt ứng dụng. Chuyển sang bước tiếp theo.

Bạn có thể thêm khóa vào Bảng điều khiển web (**Hoạt động** → **Cấp giấy phép**).

Bước 4. Hoàn tất việc tạo tác vụ

Hoàn tất trình hướng dẫn bằng cách nhấn nút **Hoàn tất**. Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ. Để thực hiện một tác vụ, chọn hộp kiểm cạnh tác vụ đó và nhấn nút **Bắt đầu**. Kết quả là Kaspersky Endpoint Security sẽ được kích hoạt trên máy tính của người dùng trong chế độ im lặng.

Trong thuộc tính của tác vụ *Thêm khóa*, bạn có thể thêm một khóa dự trữ cho máy tính. Một *khóa dự trữ* sẽ có trạng thái đang hoạt động khi khóa hiện hoạt hết hạn hoặc bị xóa. Sự sẵn có của một khóa dự trữ cho phép bạn tránh tình trạng giới hạn chức năng ứng dụng khi một giấy phép hết hạn.

Cách tự động thêm khóa giấy phép vào máy tính thông qua Bảng điều khiển quản trị (MMC)

1. Trong Bảng điều khiển quản trị, hãy vào thư mục **Administration Server** → **Kaspersky licenses**.
Một danh sách khóa giấy phép sẽ mở ra.
2. Mở thuộc tính khóa giấy phép.
3. Trong phần **Tổng quát**, hãy chọn hộp kiểm **Automatically distributed license key**.
4. Lưu các thay đổi của bạn.

Kết quả là, khóa sẽ được phân phối tự động đến các máy tính phù hợp. Trong quá trình phân phối tự động một khóa làm khóa hiện hoạt hoặc khóa dự trữ, giới hạn giấy phép về số máy tính (được thiết lập trong thuộc tính của khóa) sẽ được tính đến. Nếu giới hạn giấy phép này bị vượt quá, việc phân phối khóa này đến các máy tính sẽ tự động dừng lại. Bạn có thể xem số máy tính đã được thêm khóa này và các dữ liệu khác trong thuộc tính khóa trong mục **Devices**.

Cách tự động thêm khóa giấy phép cho máy tính thông qua Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Operations** → **Licensing** → **Kaspersky Licenses**.
Một danh sách khóa giấy phép sẽ mở ra.
2. Mở thuộc tính khóa giấy phép.
3. Trên thẻ **General**, hãy bật nút bật/tắt **Deploy license key automatically**.
4. Lưu các thay đổi của bạn.

Kết quả là, khóa sẽ được phân phối tự động đến các máy tính phù hợp. Trong quá trình phân phối tự động một khóa làm khóa hiện hoạt hoặc khóa dự trữ, giới hạn giấy phép về số máy tính (được thiết lập trong thuộc tính của khóa) sẽ được tính đến. Nếu giới hạn giấy phép này bị vượt quá, việc phân phối khóa này đến các máy tính sẽ tự động dừng lại. Bạn có thể xem số máy tính đã được thêm khóa này và các dữ liệu khác trong thuộc tính khóa trên thẻ **Devices**.

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:

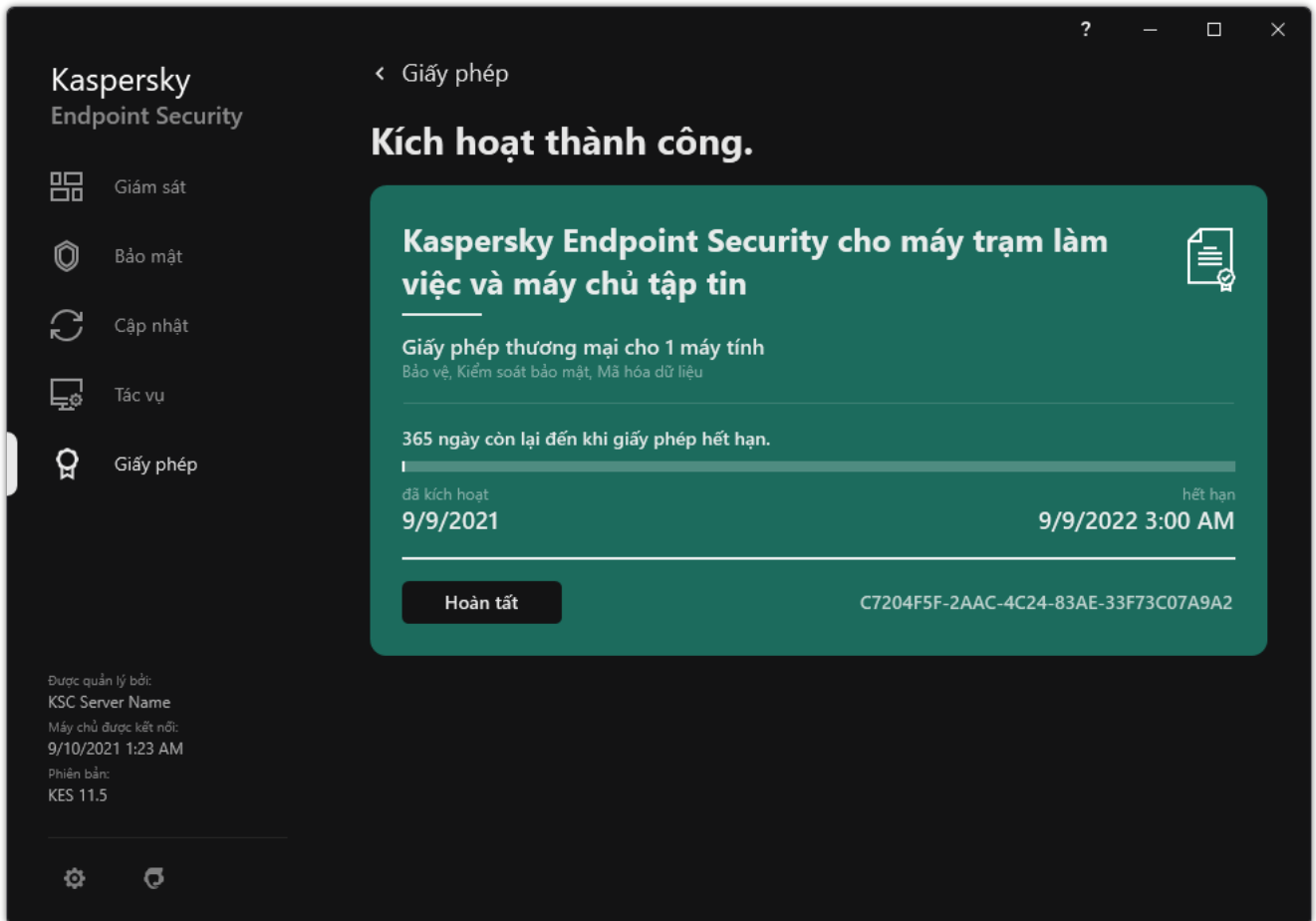
1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Giấy phép**.
2. Nhấn vào **Kích hoạt ứng dụng bằng một giấy phép mới**.

Trình hướng dẫn Kích hoạt Ứng dụng sẽ được bắt đầu. Làm theo chỉ dẫn của Trình hướng dẫn Kích hoạt.

Xem thông tin giấy phép

Để xem thông tin về một giấy phép:

Trong cửa sổ chính của ứng dụng, hãy vào mục **Giấy phép** (xem hình bên dưới).



Cửa sổ Cấp giấy phép

Mục sẽ hiển thị thông tin chi tiết sau:

- **Trạng thái khóa.** Nhiều [khóa](#) có thể được lưu trữ trên một máy tính. Có hai loại khóa: hiện hoạt và dự trữ. Ứng dụng không thể có nhiều hơn một khóa hiện hoạt. Khóa dự trữ chỉ chuyển sang trạng thái hoạt động sau khi khóa hiện hoạt hết hạn hoặc sau khi khóa hiện hoạt bị xóa bằng cách nhấn vào **Xóa**.
- **Tên ứng dụng.** Tên đầy đủ của ứng dụng Kaspersky đã mua.
- **Loại giấy phép.** [Các loại giấy phép](#) sau đây có thể được sử dụng: dùng thử và thương mại.
- **Chức năng.** Các tính năng ứng dụng khả dụng theo giấy phép của bạn. Các tính năng có thể bao gồm Bảo vệ, Kiểm soát bảo mật, Mã hóa dữ liệu, v.v. Danh sách tính năng khả dụng cũng được cung cấp trong [Chứng chỉ giấy phép](#).
- **Thông tin bổ sung về giấy phép.** Ngày bắt đầu và ngày kết thúc của thời hạn giấy phép (chỉ dành cho khóa hiện hoạt), thời lượng còn lại của thời hạn giấy phép.

Thời gian hết hạn giấy phép được hiển thị theo múi giờ được cấu hình trong hệ điều hành.

- **Khóa.** Một khóa là một chuỗi chữ số duy nhất được tạo từ một mã kích hoạt hoặc tập tin khóa.

Trong cửa sổ Cấp giấy phép, bạn cũng có thể thực hiện một trong các thao tác sau:

- **Mua giấy phép / Gia hạn giấy phép.** Mở website cửa hàng trực tuyến của Kaspersky, ở đó bạn có thể mua hoặc gia hạn một giấy phép. Để làm điều này, hãy nhập thông tin công ty của bạn và thanh toán cho đơn hàng.
- **Kích hoạt ứng dụng bằng một giấy phép mới.** Bắt đầu Trình hướng dẫn Kích hoạt ứng dụng. Trong Trình hướng dẫn, bạn có thể thêm một khóa sử dụng một mã kích hoạt hoặc một tập tin khóa. Trình hướng dẫn Kích hoạt ứng dụng cho phép bạn thêm một khóa hiện hoạt và chỉ một khóa dự trữ.

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. Trong cửa sổ chính của ứng dụng, hãy vào mục **Giấy phép**.
2. 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 **Mua giấy phép**.
 - Nếu một khóa cho giấy phép thương mại đã được bổ sung, nhấn nút **Gia hạn giấy phép**.

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 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 đang sử dụng ứng dụng theo gói đăng ký giới hạn, vào ngày hết hạn gói đăng ký (hoặc ngày kết thúc thời gian ân hạn để gia hạn), Kaspersky Endpoint Security sẽ thông báo cho bạn về điều này và ngừng nỗ lực tự động gia hạn gói đăng ký. 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.

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

1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Giấy phép**.
2. Nhấn vào **Liên hệ với nhà cung cấp gói đăng ký của bạn**.

Bạn có thể cập nhật trạng thái gói đăng ký một cách thủ công. Việc này có thể là cần thiết nếu gói đăng ký đã được gia hạn sau thời gian ân hạn và ứng dụng đã không tự động cập nhật trạng thái gói đăng ký.

Cung cấp dữ liệu

Cung cấp dữ liệu theo Thỏa thuận giấy phép người dùng cuối

Nếu một [mã kích hoạt](#) được áp dụng để kích hoạt Kaspersky Endpoint Security, bạn đồng ý sẽ tự động gửi định kỳ cho Kaspersky các thông tin sau đây cho mục đích xác minh việc sử dụng đúng ứng dụng:

- Loại, phiên bản và ngôn ngữ bản địa của Kaspersky Endpoint Security;
- Phiên bản của bản cập nhật được cài đặt cho Kaspersky Endpoint Security;
- ID của máy tính và ID của bản cài đặt Kaspersky Endpoint Security cụ thể trên máy tính;
- Số sê-ri và mã định danh của khóa hiện hoạt;
- Loại, phiên bản và tốc độ bit của hệ điều hành, và tên của môi trường ảo (nếu Kaspersky Endpoint Security được cài đặt trong một môi trường ảo);
- ID của thành phần Kaspersky Endpoint Security đang hoạt động khi thông tin được chuyển đi.

Kaspersky cũng có thể sử dụng thông tin này để tạo số liệu thống kê cho việc phân tích và sử dụng phần mềm Kaspersky.

Thông qua việc sử dụng mã kích hoạt, bạn đồng ý tự động truyền tải dữ liệu ở trên. Nếu bạn không đồng ý truyền thông tin này đến Kaspersky, bạn nên sử dụng một [tập tin khóa](#) để kích hoạt Kaspersky Endpoint Security.

Thông qua việc chấp nhận các điều khoản của Thỏa thuận giấy phép người dùng cuối, bạn đồng ý tự động truyền tải những thông tin sau:

- Khi nâng cấp Kaspersky Endpoint Security:
 - Phiên bản của Kaspersky Endpoint Security;
 - ID của Kaspersky Endpoint Security;
 - Khóa hiện hoạt;
 - ID riêng của tác vụ bắt đầu nâng cấp;
 - ID riêng của bản cài đặt Kaspersky Endpoint Security.
- Khi truy cập các liên kết từ giao diện Kaspersky Endpoint Security:
 - Phiên bản của Kaspersky Endpoint Security;
 - Các phiên bản của hệ điều hành;
 - Ngày kích hoạt Kaspersky Endpoint Security;
 - ngày hết hạn giấy phép;
 - Ngày tạo khóa;

- Ngày cài đặt Kaspersky Endpoint Security;
- ID của Kaspersky Endpoint Security;
- ID của lỗ hổng bảo mật được phát hiện trong hệ điều hành;
- ID của bản cập nhật mới nhất được cài đặt cho Kaspersky Endpoint Security;
- Hash của tập tin chứa mối đe dọa được phát hiện, và tên của mối đe dọa này theo phân loại của Kaspersky;
- Danh mục lỗi kích hoạt Kaspersky Endpoint Security;
- Mã lỗi kích hoạt Kaspersky Endpoint Security;
- Số ngày đến khi khóa hết hạn;
- Số ngày đã trôi qua kể từ khi khóa được bổ sung;
- Số ngày đã trôi qua kể từ khi giấy phép hết hạn;
- Số máy tính được áp dụng giấy phép hiện hoạt;
- Khóa hiện hoạt;
- Thời hạn giấy phép Kaspersky Endpoint Security;
- Tình trạng hiện tại của giấy phép;
- Loại giấy phép hiện hoạt;
- Loại ứng dụng;
- ID riêng của tác vụ bắt đầu nâng cấp;
- ID riêng của bản cài đặt Kaspersky Endpoint Security trên máy tính;
- Ngôn ngữ giao diện của Kaspersky Endpoint Security.

Thông tin được nhận sẽ được bảo vệ bởi Kaspersky theo luật pháp, các yêu cầu và quy định hiện hành của Kaspersky. Dữ liệu được truyền qua các kênh giao tiếp được mã hóa.

Đọc Thỏa thuận giấy phép người dùng cuối và truy cập [website Kaspersky](#) để tìm hiểu thêm về cách chúng tôi nhận, 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 Kaspersky Security Network. Các tập tin license.txt và ksn_<language ID>.txt chứa nội dung của Thỏa thuận giấy phép người dùng cuối và Tuyên bố Kaspersky Security Network và được bao gồm trong [gói phân phối](#) của ứng dụng.

Cung cấp dữ liệu khi sử dụng Kaspersky Security Network

Tập dữ liệu mà Kaspersky Endpoint Security gửi đến Kaspersky tùy thuộc vào loại giấy phép và thiết lập sử dụng Kaspersky Security Network.

Sử dụng KSN theo giấy phép trên không quá 4 máy tính

Thông qua việc chấp nhận Tuyên bố Kaspersky Security Network, bạn đồng ý tự động truyền tải những thông tin sau:

- thông tin về bản cập nhật cấu hình KSN: mã định danh của cấu hình hoạt động, mã định danh của cấu hình được nhận, mã lỗi của bản cập nhật cấu hình;
- thông tin về các tập tin và địa chỉ URL sẽ được quét: giá trị tổng kiểm (MD5, SHA2-256, SHA1) của tập tin được quét và mẫu hình tập tin (MD5), kích thước mẫu, loại mối đe dọa được phát hiện và tên mối đe dọa đó theo phân loại của Đơn vị sở hữu bản quyền, mã định danh cho các cơ sở dữ liệu diệt virus, địa chỉ URL mà tại đó yêu cầu độ tin cậy, cũng như địa chỉ URL tham chiếu, mã định danh giao thức kết nối và số hiệu cổng đang được sử dụng;
- ID của tác vụ quét đã phát hiện ra mối đe dọa;
- thông tin về chứng chỉ kỹ thuật số được sử dụng cần để xác minh tính xác thực của chúng: giá trị tổng kiểm (SHA256) của chứng chỉ được sử dụng để ký vào đối tượng được quét và khóa công khai của chứng chỉ;
- mã định danh của thành phần Phần mềm tiến hành quét;
- ID của cơ sở dữ liệu diệt virus và bản ghi trong các cơ sở dữ liệu diệt virus này;
- Thông tin về việc kích hoạt Phần mềm trên Máy tính: đầu đề được ký của phiếu từ dịch vụ kích hoạt (mã định danh của trung tâm kích hoạt khu vực, giá trị tổng kiểm của mã kích hoạt, giá trị tổng kiểm của phiếu, ngày tạo phiếu, mã định danh riêng của phiếu, phiên bản phiếu, trạng thái của giấy phép, ngày và giờ bắt đầu/kết thúc hiệu lực của phiếu, mã định danh riêng của giấy phép, phiên bản giấy phép), mã định danh của chứng chỉ được sử dụng để ký đầu đề phiếu, giá trị tổng kiểm (MD5) của tập tin khóa;
- Thông tin về Phần mềm của Đơn vị sở hữu bản quyền: loại và phiên bản của giao thức được sử dụng để kết nối đến các dịch vụ Kaspersky.

Sử dụng KSN theo giấy phép trên 5 máy tính trở lên

Thông qua việc chấp nhận Tuyên bố Kaspersky Security Network, bạn đồng ý tự động truyền tải những thông tin sau:

Nếu hộp kiểm **Kaspersky Security Network** được chọn và hộp kiểm **Bật chế độ KSN mở rộng** bị xóa, ứng dụng sẽ gửi các thông tin sau:

- thông tin về bản cập nhật cấu hình KSN: mã định danh của cấu hình hoạt động, mã định danh của cấu hình được nhận, mã lỗi của bản cập nhật cấu hình;
- thông tin về các tập tin và địa chỉ URL sẽ được quét: giá trị tổng kiểm (MD5, SHA2-256, SHA1) của tập tin được quét và mẫu hình tập tin (MD5), kích thước mẫu, loại mối đe dọa được phát hiện và tên mối đe dọa đó theo phân loại của Đơn vị sở hữu bản quyền, mã định danh cho các cơ sở dữ liệu diệt virus, địa chỉ URL mà tại đó yêu cầu độ tin cậy, cũng như địa chỉ URL tham chiếu, mã định danh giao thức kết nối và số hiệu cổng đang được sử dụng;
- ID của tác vụ quét đã phát hiện ra mối đe dọa;
- thông tin về chứng chỉ kỹ thuật số được sử dụng cần để xác minh tính xác thực của chúng: giá trị tổng kiểm (SHA256) của chứng chỉ được sử dụng để ký vào đối tượng được quét và khóa công khai của chứng chỉ;
- mã định danh của thành phần Phần mềm tiến hành quét;

- ID của cơ sở dữ liệu diệt virus và bản ghi trong các cơ sở dữ liệu diệt virus này;
- Thông tin về việc kích hoạt Phần mềm trên Máy tính: đầu đề được ký của phiếu từ dịch vụ kích hoạt (mã định danh của trung tâm kích hoạt khu vực, giá trị tổng kiểm của mã kích hoạt, giá trị tổng kiểm của phiếu, ngày tạo phiếu, mã định danh riêng của phiếu, phiên bản phiếu, trạng thái của giấy phép, ngày và giờ bắt đầu/kết thúc hiệu lực của phiếu, mã định danh riêng của giấy phép, phiên bản giấy phép), mã định danh của chứng chỉ được sử dụng để ký đầu đề phiếu, giá trị tổng kiểm (MD5) của tập tin khóa;
- Thông tin về Phần mềm của Đơn vị sở hữu bản quyền: loại và phiên bản của giao thức được sử dụng để kết nối đến các dịch vụ Kaspersky.

Nếu hộp kiểm **Bật chế độ KSN mở rộng** được chọn ngoài hộp kiểm **Kaspersky Security Network**, ứng dụng sẽ gửi các thông tin sau đây, ngoài các thông tin được liệt kê ở trên:

- thông tin về kết quả phân loại các tài nguyên web được yêu cầu, các tài nguyên này chứa URL đã được xử lý và địa chỉ IP của máy chủ lưu trữ, phiên bản của thành phần Phần mềm đã thực hiện phân loại, phương pháp phân loại và bộ danh mục được xác định cho tài nguyên web;
- thông tin về Phần mềm được cài đặt trên Máy tính: tên của các nhà cung cấp phần mềm và ứng dụng Phần mềm, khóa registry cùng giá trị của khóa này, thông tin về các tập tin của các thành phần phần mềm đã cài đặt (tổng kiểm (MD5, SHA2-256, SHA1), tên, đường dẫn đến tập tin trên Máy tính, dung lượng, phiên bản và chữ ký số);
- thông tin về trạng thái bảo vệ chống virus của Máy tính: các phiên bản và dấu thời gian phát hành của cơ sở dữ liệu diệt virus đang được sử dụng, ID của tác vụ và ID của Phần mềm thực hiện quét;
- thông tin về các tập tin được Người dùng cuối tải về: URL và địa chỉ IP từ đó các tập tin được tải về và trang tải về, mã định danh của giao thức tải về và số hiệu cổng kết nối, chỉ báo URL là độc hại hay không, thuộc tính, kích cỡ của tập tin cùng giá trị tổng kiểm (MD5, SHA2-256, SHA1), thông tin về tiến trình đã tải về tập tin (giá trị tổng kiểm (MD5, SHA2-256, SHA1), ngày và giờ tạo/bản dựng, trạng thái tự động chạy, thuộc tính, tên trình đóng gói, thông tin về chữ ký, cờ tập tin thực thi, mã định danh định dạng, và entropy), tên tập tin và đường dẫn đến nó trên Máy tính, chữ ký kỹ thuật số và dấu thời gian của tập tin, địa chỉ URL mà trên đó xảy ra phát hiện, số kịch bản trên trang bị nghi vấn hoặc là độc hại, thông tin về các yêu cầu HTTP được tạo và các phản hồi đến chúng;
- thông tin về các ứng dụng đang chạy và các mô-đun của chúng: dữ liệu về các tiến trình đang chạy trên hệ thống (ID tiến trình (PID), tên tiến trình, thông tin về tài khoản đã bắt đầu tiến trình, ứng dụng và lệnh đã bắt đầu tiến trình, chỉ báo chương trình hoặc tiến trình được tin tưởng, đường dẫn đầy đủ đến các tập tin tiến trình và giá trị tổng kiểm của chúng (MD5, SHA2-256, SHA1), và dòng lệnh bắt đầu, mức độ toàn vẹn của tiến trình, mô tả về phần mềm chứa tiến trình (tên của phần mềm và thông tin về nhà phát hành), thông tin về các chứng chỉ kỹ thuật số được sử dụng và thông tin cần thiết để xác minh tính xác thực của chúng, hoặc thông tin về việc tập tin không có một chữ ký kỹ thuật số), thông tin về các mô-đun được nạp vào tiến trình (tên, dung lượng, loại, ngày tạo, thuộc tính, giá trị tổng kiểm (MD5, SHA2-256, SHA1), và đường dẫn đến chúng trên Máy tính), thông tin đầu đề của tập tin PE, tên của trình đóng gói (nếu tập tin đã được đóng gói);
- thông tin về tất cả các đối tượng độc hại tiềm năng cùng hoạt động của chúng: tên của đối tượng được phát hiện và đường dẫn đầy đủ đến đối tượng trên máy tính, giá trị tổng kiểm của các tập tin được xử lý (MD5, SHA2-256, SHA1), ngày và giờ phát hiện, tên và kích cỡ của các tập tin nhiễm mã độc và đường dẫn đến chúng, mã khuôn mẫu đường dẫn, cờ chỉ báo tập tin thực thi, chỉ báo liệu đối tượng này có phải là một vỏ bọc hay không, tên của trình đóng gói (nếu tập tin được đóng gói), mã loại tập tin, ID định dạng tập tin, danh sách các hành động được thực hiện bởi phần mềm độc hại và quyết định của phần mềm và người dùng trong việc xử lý chúng, ID của cơ sở dữ liệu diệt virus và của các bản ghi trong những cơ sở dữ liệu diệt virus đã được sử dụng để đưa ra quyết định, chỉ báo đối tượng độc hại tiềm tàng, tên của mối đe dọa được phát hiện theo phân loại của Đơn vị sở hữu bản quyền, cấp độ nguy hiểm, trạng thái phát hiện và phương thức phát hiện, lý do bao gồm trong ngữ cảnh phân tích và số hiệu trình tự của tập tin trong ngữ cảnh, giá trị tổng kiểm (MD5, SHA2-256, SHA1), tên và thuộc tính của tập tin thực thi của ứng dụng mà qua đó tin nhắn hoặc liên kết nhiễm mã

độc được truyền tải, địa chỉ IP phi cá nhân hóa (IPv4 và IPv6) của máy chủ đã chặn đối tượng, entropy tập tin, chỉ báo tự động chạy tập tin, thời gian khi tập tin được phát hiện lần đầu trong hệ thống, số lần tập tin được chạy kể từ khi số liệu thống kê gần nhất được gửi đi, thông tin về tên, giá trị tổng kiểm (MD5, SHA2-256, SHA1) và kích cỡ của trình khách email thông qua đó đối tượng độc hại được tiếp nhận, ID của tác vụ phần mềm đã thực hiện việc quét, chỉ báo liệu danh tiếng hay chữ ký tập tin đã được kiểm tra, kết quả xử lý tập tin, giá trị tổng kiểm (MD5) của mẫu được thu thập cho đối tượng, kích cỡ của mẫu tính theo byte, và thông số kỹ thuật của công nghệ phát hiện được áp dụng;

- thông tin về các đối tượng được quét: nhóm tin tưởng mà tập tin được đặt cho và/hoặc từ nhóm đó mà tập tin được đặt, lý do tập tin được xác định là thuộc thể loại đó, mã định danh thể loại, thông tin về nguồn gốc của các thể loại và phiên bản của cơ sở dữ liệu thể loại, cờ chứng chỉ được tin tưởng của tập tin, tên của nhà cung cấp tập tin, phiên bản tập tin, tên và phiên bản của ứng dụng phần mềm chứa tập tin đó;
- thông tin về các lỗ hổng bảo mật được phát hiện: ID của từng lỗ hổng trong cơ sở dữ liệu lỗ hổng, mức độ nguy hiểm của lỗ hổng;
- thông tin về việc mô phỏng của tập tin thực thi: dung lượng và giá trị tổng kiểm của tập tin (MD5, SHA2-256, SHA1), phiên bản của thành phần giả lập, độ sâu giả lập, một dãy các thuộc tính của khối logic và các hàm bên trong khối logic có được trong quá trình giả lập, dữ liệu từ tiêu đề PE của tập tin thực thi;
- địa chỉ IP của máy tính tấn công (IPv4 và IPv6), số hiệu cổng trên Máy tính mà các cuộc tấn công mạng đang nhắm vào, mã định danh giao thức của gói tin IP có chứa cuộc tấn công, mục tiêu tấn công (tên tổ chức, trang web), cờ hiệu cho phản ứng đến cuộc tấn công, sức mạnh của cuộc tấn công, mức độ tin cậy;
- thông tin về các cuộc tấn công liên quan đến tài nguyên mạng giả mạo, DNS và địa chỉ IP (IPv4 và IPv6) của các website được truy cập;
- DNS và địa chỉ IP (IPv4 hoặc IPv6) của tài nguyên web được yêu cầu, thông tin về tập tin và ứng dụng web truy cập vào tài nguyên web, tên, dung lượng và giá trị tổng kiểm (MD5, SHA2-256, SHA1) của tập tin, đường dẫn đầy đủ và mã mẫu của đường dẫn, kết quả kiểm tra chữ ký số và trạng thái chữ ký số trong KSN;
- thông tin về việc hoàn tác các hành động của phần mềm độc hại: dữ liệu trên tập tin có hoạt động được hoàn tác (tên tập tin, đường dẫn đầy đủ đến tập tin, kích cỡ và giá trị tổng kiểm (MD5, SHA2-256, SHA1) của nó), dữ liệu về kết quả của hành động xóa, đổi tên, sao chép các tập tin và khôi phục giá trị trong registry (tên của các khóa registry và giá trị của chúng), cũng như thông tin về các tập tin hệ thống bị sửa đổi bởi phần mềm độc hại trước và sau khi hoàn tác;
- thông tin về các loại trừ được thiết lập cho thành phần Kiểm soát thích ứng sự cố: ID và trạng thái của quy tắc được kích hoạt, hành động do Phần mềm thực hiện khi quy tắc được kích hoạt, loại tài khoản người dùng mà tiến trình hoặc luồng thực hiện hoạt động đáng ngờ, thông tin về tiến trình thực hiện hoặc phải chịu hoạt động đáng ngờ (ID tập lệnh hoặc tên tập tin tiến trình, đường dẫn đầy đủ đến tập tin tiến trình, mã mẫu của đường dẫn, giá trị tổng kiểm (MD5, SHA2-256, SHA1) của tập tin tiến trình); thông tin về đối tượng đã thực hiện hành động đáng ngờ và về đối tượng chịu các thao tác đáng ngờ (tên khóa registry hoặc tên tập tin, đường dẫn đầy đủ đến tập tin, mã mẫu của đường dẫn và giá trị tổng kiểm (MD5, SHA2-256, SHA1) của tập tin);
- thông tin về mô-đun phần mềm được tải: tên, kích cỡ và giá trị tổng kiểm (MD5, SHA2-256, SHA1) của tập tin mô-đun, đường dẫn đầy đủ đến nó cùng mã khuôn mẫu đường dẫn, thiết lập chữ ký kỹ thuật số của tập tin mô-đun, ngày và giờ tạo chữ ký, tên của chủ thể và tổ chức đã ký duyệt tập tin mô-đun, ID của tiến trình đã nạp mô-đun, tên của nhà cung cấp mô-đun, và số hiệu trình tự của mô-đun trong hàng chờ nạp;
- thông tin về chất lượng tương tác Phần mềm với các dịch vụ KSN: ngày giờ bắt đầu và kết thúc khoảng thời gian tạo số liệu thống kê, thông tin về chất lượng của các yêu cầu và kết nối với từng dịch

vụ KSN đã sử dụng (ID dịch vụ KSN, số các yêu cầu thành công, số các yêu cầu có phản hồi từ bộ nhớ đệm, số các yêu cầu không thành công (sự cố mạng, KSN bị tắt trong mục cài đặt Phần mềm, định tuyến không chính xác), luồng thời gian của các yêu cầu thành công, luồng thời gian của các yêu cầu bị hủy, luồng thời gian của các yêu cầu bị hủy vượt quá giới hạn thời gian, số các kết nối với KSN được lấy từ bộ nhớ đệm, số các kết nối với KSN thành công, số các kết nối với KSN không thành công, số các giao dịch thành công, số các giao dịch không thành công, luồng thời gian của các kết nối với KSN thành công, luồng thời gian của các kết nối với KSN không thành công, luồng thời gian của các giao dịch thành công, luồng thời gian của các giao dịch không thành công);

- nếu phát hiện một đối tượng độc hại tiềm tàng, thông tin sẽ được cung cấp về dữ liệu trong bộ nhớ của các tiến trình: các phần tử của cấu trúc phân cấp đối tượng hệ thống (ObjectManager), dữ liệu trong bộ nhớ UEFI BIOS, tên và giá trị của các khóa registry;
- thông tin về các sự kiện trong bản ghi hệ thống: dấu thời gian của sự kiện, tên bản ghi trong đó đã tìm thấy sự kiện, loại và danh mục của sự kiện, tên của nguồn sự kiện và mô tả của sự kiện;
- thông tin về các kết nối mạng: phiên bản và giá trị tổng kiểm (MD5, SHA2-256, SHA1) của tập tin bắt đầu tiến trình mở cổng, đường dẫn đến tập tin của tiến trình và chữ ký số, địa chỉ IP cục bộ và từ xa, số lượng cổng kết nối cục bộ và từ xa, trạng thái kết nối, dấu thời gian khi mở cổng;
- thông tin về ngày cài đặt và kích hoạt Phần mềm trên Máy tính: ID của đối tác đã bán giấy phép, số sê-ri của giấy phép, tiêu đề được ký của phiếu từ dịch vụ kích hoạt (ID của trung tâm kích hoạt khu vực, giá trị tổng kiểm của mã kích hoạt, giá trị tổng kiểm của phiếu, ngày tạo phiếu, ID duy nhất của phiếu, phiên bản phiếu, trạng thái giấy phép, ngày và giờ bắt đầu/kết thúc phiếu, ID duy nhất của giấy phép, phiên bản giấy phép), ID của chứng chỉ được sử dụng để ký tiêu đề phiếu, giá trị tổng kiểm (MD5) của tập tin khóa, ID duy nhất của bản cài đặt Phần mềm trên Máy tính, loại và ID của ứng dụng được cập nhật, ID của tác vụ cập nhật;
- thông tin về tập hợp tất cả các bản cập nhật được cài đặt và tập hợp các cập nhật đã được cài đặt/gỡ bỏ gần đây nhất, loại sự kiện khiến thông tin cập nhật được gửi, thời lượng kể từ khi cài đặt bản cập nhật mới nhất, thông tin về bất kỳ cơ sở dữ liệu diệt virus nào được cài đặt gần đây;
- thông tin về hoạt động của phần mềm trên máy tính: dữ liệu sử dụng CPU, dữ liệu sử dụng bộ nhớ (Byte Cá nhân, Tổng bộ nhớ thật, Tổng bộ nhớ ảo), số luồng đang hoạt động trong tiến trình phần mềm và các luồng đang chờ duyệt, cũng như thời gian hoạt động của phần mềm trước lỗi;
- số lượng lỗi màn hình xanh phần mềm và lỗi màn hình xanh hệ thống (Màn hình xanh chết chóc) kể từ khi Phần mềm được cài đặt và kể từ thời điểm cập nhật lần cuối, mã định danh và phiên bản của mô-đun Phần mềm bị lỗi, stack bộ nhớ trong tiến trình của Phần mềm và thông tin về các cơ sở dữ liệu diệt virus tại thời điểm xảy ra lỗi;
- dữ liệu về lỗi màn hình xanh hệ thống (Màn hình xanh chết chóc): cờ hiệu chỉ báo sự xuất hiện của Màn hình xanh chết chóc trên Máy tính, tên trình điều khiển gây ra Màn hình xanh chết chóc, địa chỉ và stack bộ nhớ trong trình điều khiển, cờ hiệu chỉ báo thời lượng phiên làm việc của hệ điều hành trước khi xảy ra Màn hình xanh chết chóc, stack bộ nhớ của trình điều khiển bị lỗi, loại lỗi bộ nhớ được lưu trữ, cờ cho phiên làm việc của hệ điều hành trước khi Màn hình xanh chết chóc kéo dài hơn 10 phút, mã định danh riêng của lỗi đó, dấu thời gian của Màn hình xanh chết chóc;
- thông tin về lỗi hoặc sự cố hiệu suất xảy ra trong quá trình hoạt động của các thành phần của Phần mềm: ID của tình trạng Phần mềm, loại lỗi, mã, nguyên nhân cũng như thời gian xảy ra lỗi, các ID của thành phần, mô-đun và tiến trình của sản phẩm xảy ra lỗi, ID tác vụ hoặc loại cập nhật xảy ra lỗi, bản ghi của trình điều khiển do Phần mềm sử dụng (mã lỗi, tên mô-đun, tên tập tin nguồn và dòng nơi xảy ra lỗi);
- thông tin về các bản cập nhật cơ sở dữ liệu diệt virus và thành phần của Phần mềm: tên, ngày giờ của tập tin chỉ mục được tải về khi cập nhật lần cuối và đang được tải về trong quá trình cập nhật hiện tại;

- thông tin về việc chấm dứt bất thường hoạt động của Phần mềm: dấu thời gian tạo lỗi màn hình xanh, loại lỗi màn hình xanh, loại sự kiện gây ra chấm dứt bất thường hoạt động của Phần mềm (mất điện đột xuất, lỗi ứng dụng bên thứ ba), ngày và giờ mất điện đột xuất;
- thông tin về khả năng tương thích của trình điều khiển Phần mềm với phần cứng và Phần mềm: thông tin về các thuộc tính hệ điều hành (OS) hạn chế chức năng của các thành phần Phần mềm (Secure Boot, KPTI, WHQL Enforce, BitLocker, Case Sensitive), loại Phần mềm tải xuống đã cài đặt (UEFI, BIOS), Mã định danh Mô-đun Nền tảng Tin tưởng (TPM), phiên bản đặc tả TPM, thông tin về CPU được cài đặt trên Máy tính, chế độ hoạt động và các tham số của Bảo vệ thiết bị và toàn vẹn mã, chế độ vận hành của trình điều khiển và lý do sử dụng chế độ hiện hành, phiên bản trình điều khiển Phần mềm, trạng thái hỗ trợ ảo hóa phần mềm và phần cứng của Máy tính;
- thông tin về các ứng dụng của bên thứ ba đã gây ra lỗi: tên, phiên bản và ngôn ngữ địa phương, mã lỗi và thông tin về lỗi từ nhật ký hệ thống của các ứng dụng, địa chỉ lỗi và stack bộ nhớ trong ứng dụng của bên thứ ba, cờ chỉ báo sự xuất hiện lỗi trong thành phần của Phần mềm, khoảng thời gian ứng dụng của bên thứ ba đã hoạt động trước khi xảy ra lỗi, giá trị tổng kiểm (MD5, SHA2-256, SHA1) của hình ảnh tiến trình ứng dụng mà trong đó đã xảy ra lỗi, đường dẫn đến hình ảnh tiến trình ứng dụng đó và mã mẫu của đường dẫn, thông tin từ nhật ký hệ thống với mô tả về lỗi liên quan đến ứng dụng, thông tin về mô-đun ứng dụng đã xảy ra lỗi (mã định danh lỗi ngoại lệ, địa chỉ bộ nhớ lỗi dưới dạng độ dời trong mô-đun ứng dụng, tên và phiên bản của mô-đun, mã định danh lỗi ứng dụng trong plugin của Đơn vị sở hữu bản quyền và stack bộ nhớ của lỗi, thời lượng của phiên ứng dụng trước khi bị lỗi);
- phiên bản của thành phần chương trình cập nhật Phần mềm, số lượng lỗi thành phần chương trình cập nhật trong khi chạy các tác vụ cập nhật trong suốt thời gian hoạt động của thành phần, ID của kiểu tác vụ cập nhật, số lần thử không thành công của thành phần chương trình cập nhật để hoàn thành các tác vụ cập nhật;
- thông tin về hoạt động của thành phần giám sát hệ thống Phần mềm: phiên bản đầy đủ của thành phần, ngày và giờ khởi động các thành phần, mã sự kiện làm tràn hàng đợi sự kiện và số lượng các sự kiện như vậy, tổng số sự kiện làm tràn hàng đợi, thông tin về tập tin của tiến trình bộ khởi tạo sự kiện (tên và đường dẫn tập tin trên Máy tính, mã mẫu của đường dẫn tập tin, giá trị tổng kiểm (MD5, SHA2-256, SHA1) của tiến trình liên kết với tập tin, phiên bản tập tin), mã định danh việc chặn sự kiện đã xảy ra, phiên bản đầy đủ của bộ lọc chặn, mã định danh của loại sự kiện bị chặn, kích cỡ hàng đợi sự kiện và số lượng sự kiện giữa sự kiện đầu tiên trong hàng đợi và sự kiện hiện tại, số các sự kiện quá hạn trong hàng đợi, thông tin về tập tin của tiến trình của bộ khởi tạo sự kiện hiện tại (tên và đường dẫn tập tin trên Máy tính, mã mẫu của đường dẫn tập tin, giá trị tổng kiểm (MD5, SHA2-256, SHA1) của tiến trình được liên kết với tập tin đó), thời lượng xử lý sự kiện, thời lượng tối đa cho việc xử lý sự kiện, xác suất gửi số liệu thống kê; thông tin về các sự kiện hệ điều hành đã vượt quá giới hạn thời gian xử lý (ngày và giờ của sự kiện, số lần khởi tạo lặp lại của cơ sở dữ liệu diệt virus, ngày và giờ khởi tạo cơ sở dữ liệu diệt virus lặp lại lần cuối cùng sau khi cập nhật, thời gian trì hoãn xử lý sự kiện cho từng thành phần giám sát hệ thống, số sự kiện được xếp hàng, số sự kiện được xử lý, số sự kiện bị trì hoãn của loại sự kiện hiện tại, tổng thời gian trì hoãn cho các loại sự kiện hiện tại, tổng thời gian trì hoãn cho tất cả các sự kiện);
- thông tin từ công cụ truy vết sự kiện cho Windows (Theo dõi sự kiện cho Windows, ETW) trong trường hợp xảy ra sự cố về hiệu suất Phần mềm, nhà cung cấp các sự kiện SysConfig / SysConfigEx / WinSATAssessment từ Microsoft: thông tin về Máy tính (kiểu, nhà sản xuất, hệ số hình thức của vỏ, phiên bản), thông tin về số liệu hiệu suất của Windows (đánh giá WinSAT, chỉ số hiệu suất Windows), tên miền, thông tin về bộ xử lý vật lý và logic (số bộ xử lý vật lý và logic, nhà sản xuất, kiểu, cấp độ bước, số lõi, tần số xung nhịp, CPUID, đặc tính bộ nhớ đệm, đặc tính bộ xử lý logic, chỉ báo của các chế độ và hướng dẫn được hỗ trợ), thông tin về các mô-đun RAM (loại, yếu tố hình thức, nhà sản xuất, kiểu, dung lượng, mức độ chi tiết của phân bố bộ nhớ), thông tin về giao diện mạng (địa chỉ IP và MAC, tên, mô tả, cấu hình giao diện mạng, phân tích số lượng và dung lượng gói mạng theo loại, tốc độ trao đổi mạng, phân tích số lỗi mạng theo loại), cấu hình bộ điều khiển IDE, địa chỉ IP của máy chủ DNS, thông tin về thẻ video (kiểu, mô tả, nhà sản xuất, khả năng tương thích, dung lượng bộ nhớ video, quyền truy cập màn hình, số bit trên mỗi pixel, phiên bản BIOS), thông tin về các thiết bị cắm và chạy (tên, mô tả, mã định danh thiết bị [PnP, ACPI]), thông tin về đĩa và thiết bị lưu trữ (số đĩa hoặc ổ đĩa flash, nhà sản xuất, kiểu, dung lượng đĩa, số lượng trụ, số các rãnh trên mỗi trụ, số lượng rãnh

trên mỗi trụ, dung lượng của cung, đặc tính bộ nhớ đệm, số trình tự, số phân vùng, cấu hình của bộ điều khiển SCSI), thông tin về các đĩa logic (số trình tự, dung lượng phân vùng, dung lượng ổ đĩa, ký tự ổ đĩa, loại phân vùng, loại hệ thống tập tin, số cụm, kích thước cụm, số lượng cung trên mỗi cụm, số cụm trống và cụm đã có dữ liệu, ký tự của ổ đĩa khởi động, địa chỉ bù của phân vùng liên quan đến khởi động ổ đĩa), thông tin về bo mạch chủ BIOS (nhà sản xuất, ngày phát hành, phiên bản), thông tin về bo mạch chủ (nhà sản xuất, kiểu, loại), thông tin về bộ nhớ vật lý (dung lượng dùng chung và dung lượng trống)), thông tin về các dịch vụ của hệ điều hành (tên, mô tả, trạng thái, thẻ, thông tin về các tiến trình [tên và PID]), thông số tiêu thụ năng lượng cho Máy tính, cấu hình của bộ điều khiển ngắt quang, đường dẫn đến các thư mục hệ thống Windows (Windows và System32), thông tin về hệ điều hành (phiên bản, bản dựng, ngày phát hành, tên, loại, ngày cài đặt), kích thước tập tin trang, thông tin về màn hình (số, nhà sản xuất, quyền màn hình, dung lượng độ phân giải, loại), thông tin về trình điều khiển card video (nhà sản xuất, ngày phát hành, phiên bản);

- thông tin từ Theo dõi sự kiện cho Windows (ETW), nhà cung cấp các sự kiện EventTrace / EventMetadata từ Microsoft: thông tin về chuỗi sự kiện hệ thống (loại, thời gian, ngày, múi giờ), siêu dữ liệu về tập tin với kết quả theo dõi (tên, cấu trúc, tham số truy vết, phân tích về số lượng các hoạt động theo dõi theo loại), thông tin về HĐH (tên, loại, phiên bản, bản dựng, ngày phát hành, thời gian bắt đầu);
- thông tin từ Theo dõi sự kiện cho Windows (ETW), nhà cung cấp các sự kiện Process / Microsoft Windows Kernel Process / Microsoft Windows Kernel Processor Power từ Microsoft: thông tin về các tiến trình đã bắt đầu và đã hoàn thành (tên, PID, tham số bắt đầu, dòng lệnh, mã trả về, tham số quản lý nguồn, thời điểm bắt đầu và thời điểm hoàn thành, loại mã thông báo truy cập, SID, SessionID, số lượng bộ mô tả được cài đặt), thông tin về sự thay đổi của mức độ ưu tiên luồng (TID, mức độ ưu tiên, thời gian), thông tin về hoạt động của ổ đĩa trong tiến trình (loại, thời gian, dung lượng, số), lịch sử thay đổi đến cấu trúc và dung lượng của các tiến trình bộ nhớ có thể sử dụng;
- thông tin từ Theo dõi sự kiện cho Windows (ETW), nhà cung cấp các sự kiện StackWalk / Perfinfo từ Microsoft: thông tin về bộ đếm hiệu suất (hiệu suất của các phần mã riêng lẻ, trình tự của lệnh gọi hàm, PID, TID, địa chỉ và thuộc tính của ISR và DPC);
- thông tin từ Theo dõi sự kiện cho Windows (ETW), nhà cung cấp các sự kiện KernelTraceControl-ImageID từ Microsoft: thông tin về các tập tin thực thi và thư viện động (tên, kích thước hình ảnh, đường dẫn đầy đủ), thông tin về các tập tin PDB (tên, mã định danh), dữ liệu tài nguyên VERSIONINFO cho các tập tin thực thi (tên, mô tả, người tạo, bản địa hóa, phiên bản ứng dụng và mã định danh, phiên bản tập tin và mã định danh);
- thông tin từ Theo dõi sự kiện cho Windows (ETW), nhà cung cấp các sự kiện FileIo / DiskIo / Image / Windows Kernel Disk từ Microsoft: thông tin về hoạt động của tập tin và ổ đĩa (loại, dung lượng, thời điểm bắt đầu, thời điểm hoàn thành, thời lượng, trạng thái hoàn thành, PID, TID, địa chỉ lệnh gọi hàm trình điều khiển, Gói yêu cầu I/O (IRP), thuộc tính đối tượng tập tin Windows), thông tin về các tập tin liên quan đến hoạt động của tập tin và ổ đĩa (tên, phiên bản, kích thước, đường dẫn đầy đủ, thuộc tính, độ dài, kiểm tra hình ảnh, tùy chọn mở và truy cập);
- thông tin từ Theo dõi sự kiện cho Windows (ETW), nhà cung cấp các sự kiện PageFault từ Microsoft: thông tin về lỗi truy cập trang bộ nhớ (địa chỉ, thời gian, dung lượng, PID, TID, các thuộc tính của đối tượng tập tin Windows, tham số phân bổ bộ nhớ);
- thông tin từ Theo dõi sự kiện cho Windows (ETW), nhà cung cấp các sự kiện Thread từ Microsoft: thông tin về việc tạo/hoàn thành luồng, thông tin về các luồng đã bắt đầu (PID, TID, kích thước của ngăn xếp, mức độ ưu tiên và phân bổ tài nguyên CPU, tài nguyên I/O, trang bộ nhớ giữa các luồng, địa chỉ ngăn xếp, địa chỉ của hàm init, địa chỉ của Khối môi trường luồng (TEB), thẻ dịch vụ Windows);
- thông tin từ Theo dõi sự kiện cho Windows (ETW), nhà cung cấp các sự kiện Microsoft Windows Kernel Memory từ Microsoft: thông tin về các hoạt động quản lý bộ nhớ (trạng thái hoàn thành, thời gian, số lượng, PID), cấu trúc phân bổ bộ nhớ (loại, dung lượng, SessionID, PID);
- thông tin về hoạt động của Phần mềm trong trường hợp có vấn đề về hiệu suất: mã định danh cài đặt Phần mềm, loại và giá trị giảm hiệu suất, thông tin về trình tự sự kiện trong Phần mềm (thời gian, múi

giờ, loại, trạng thái hoàn thành, mã định danh thành phần Phần mềm, mã định danh kịch bản hoạt động Phần mềm, TID, PID, địa chỉ lệnh gọi hàm), thông tin về các kết nối mạng cần kiểm tra (URL, hướng kết nối, dung lượng gói mạng), thông tin về các tập tin PDB (tên, mã định danh, kích thước hình ảnh của tập tin thực thi), thông tin về các tập tin cần kiểm tra (tên, đường dẫn đầy đủ, giá trị tổng kiểm), thông số giám sát hiệu suất Phần mềm;

- thông tin về khởi động lại hệ điều hành không thành công cuối cùng: số lần khởi động lại không thành công kể từ khi cài đặt hệ điều hành, dữ liệu về lỗi hệ thống (mã và thông số lỗi, tên, phiên bản và giá trị tổng kiểm (CRC32) của mô đun gây ra lỗi trong hoạt động hệ điều hành, địa chỉ lỗi dưới dạng độ dời trong mô-đun, giá trị tổng kiểm (MD5, SHA2-256, SHA1) của lỗi hệ thống);
- thông tin để xác minh tính hợp lệ của các chứng chỉ kỹ thuật số được sử dụng để ký tên vào các tập tin: vân tay của chứng chỉ, thuật toán giá trị tổng kiểm, khóa công khai và số sê-ri của chứng chỉ, tên của đơn vị cấp chứng chỉ, kết quả xác thực chứng chỉ và mã định danh cơ sở dữ liệu của chứng chỉ;
- thông tin về tiến trình đang tấn công hệ thống tự bảo vệ của Phần mềm: tên và kích cỡ của tập tin tiến trình, giá trị tổng kiểm (MD5, SHA2-256, SHA1) của nó, đường dẫn đầy đủ đến tập tin tiến trình và mã khuôn mẫu đường dẫn tập tin, dấu thời gian tạo/bản dựng, cờ chỉ báo tập tin thực thi, thuộc tính của tập tin tiến trình, thông tin về chứng chỉ được sử dụng để ký cho tập tin tiến trình, mã tài khoản được sử dụng để khởi động tiến trình, ID của hoạt động đã được thực hiện để truy cập tiến trình, loại tài nguyên thực hiện tiến trình (tiến trình, tập tin, đối tượng registry, chức năng tìm kiếm FindWindow), tên của tài nguyên thực hiện hoạt động, cờ chỉ báo thành công của hoạt động, trạng thái của tập tin tiến trình và chữ ký của nó trong KSN;
- thông tin về Phần mềm của Đơn vị sở hữu bản quyền: phiên bản đầy đủ, loại, bản địa hóa và trạng thái hoạt động của Phần mềm được sử dụng, phiên bản của các thành phần Phần mềm đã cài đặt và trạng thái hoạt động của chúng, thông tin về các bản cập nhật Phần mềm đã cài đặt, giá trị của bộ lọc TARGET, phiên bản giao thức được sử dụng để kết nối với các dịch vụ của Đơn vị sở hữu bản quyền;
- thông tin về phần cứng được lắp đặt trên Máy tính: loại, tên, tên model, phiên bản firmware, thông số của những thiết bị được tích hợp và được kết nối, mã định danh riêng của Máy tính cài đặt Phần mềm;
- thông tin về phiên bản của hệ điều hành và các bản cập nhật được cài đặt, dung lượng thanh ghi, phiên bản và tham số của chế độ chạy hệ điều hành, phiên bản và giá trị tổng kiểm (MD5, SHA2-256, SHA1) của tập tin nhân hệ điều hành và ngày giờ khởi động hệ điều hành;
- các tập tin thực thi và không thực thi, toàn bộ hoặc một phần;
- các phần của RAM máy tính;
- các sector liên quan đến quá trình khởi động HĐH;
- các gói tin dữ liệu lưu lượng mạng;
- các trang web và email chứa đối tượng đáng ngờ và độc hại;
- mô tả về các lớp và thể hiện của các lớp của kho lưu trữ WMI;
- các báo cáo về hoạt động ứng dụng:
 - tên, dung lượng và phiên bản của tập tin được gửi, mô tả và giá trị tổng kiểm của tập tin (MD5, SHA2-256, SHA1), mã định danh của định dạng tập tin, tên nhà cung cấp tập tin, tên sản phẩm chứa tập tin, đường dẫn đầy đủ đến tập tin trên Máy tính, mã mẫu của đường dẫn, dấu thời gian tạo và sửa đổi tập tin;
 - ngày/giờ bắt đầu và kết thúc thời hạn hiệu lực của chứng chỉ (nếu tập tin có chữ ký số), ngày và giờ của chữ ký, tên đơn vị cấp chứng chỉ, thông tin về người được cấp chứng chỉ, dấu vân tay, khóa công khai của chứng chỉ và các thuật toán thích hợp cũng như số sê-ri của chứng chỉ;

- tên của tài khoản có tiến trình đang chạy từ đó;
- giá trị tổng kiểm (MD5, SHA2-256, SHA1) của tên Máy tính mà tiến trình đang chạy;
- tiêu đề của các cửa sổ tiến trình;
- Định danh cho cơ sở dữ liệu diệt virus, tên của mối đe dọa được phát hiện theo phân loại của Đơn vị sở hữu bản quyền;
- dữ liệu về giấy phép đã cài đặt, định danh, loại và ngày hết hạn;
- giờ địa phương của Máy tính tại thời điểm cung cấp thông tin;
- tên và đường dẫn của các tập tin được tiến trình này truy cập;
- tên của các khóa registry và giá trị của chúng đã được quá tiến trình này truy cập;
- URL và địa chỉ IP đã được truy cập bởi tiến trình;
- URL và địa chỉ IP mà từ đó tập tin đang chạy được tải xuống.

Cung cấp dữ liệu khi sử dụng giải pháp Detection and Response

Trên máy tính được cài đặt Kaspersky Endpoint Security, dữ liệu được chuẩn bị để tự động gửi tới các máy chủ [Kaspersky Endpoint Detection and Response](#) và [Kaspersky Sandbox](#) được lưu trữ. Các tập tin được lưu trữ trên máy tính ở dạng văn bản thuần, không được mã hóa.

Bộ dữ liệu cụ thể phụ thuộc vào giải pháp mà Kaspersky Endpoint Security được sử dụng.

Kaspersky Endpoint Detection and Response

Toàn bộ dữ liệu mà ứng dụng lưu trữ cục bộ trên máy tính sẽ bị xóa khỏi máy tính khi gỡ cài đặt Kaspersky Endpoint Security.

Dữ liệu nhận được do kết quả thực thi tác vụ Quét IOC (tác vụ tiêu chuẩn)

Kaspersky Endpoint Security sẽ tự động gửi dữ liệu về kết quả thực thi tác vụ *Quét IOC* tới Kaspersky Security Center.

Dữ liệu trong kết quả thực hiện tác vụ *Quét IOC* có thể chứa các thông tin sau:

- Địa chỉ IP từ bảng ARP
- Địa chỉ vật lý từ bảng ARP
- Tên và loại bản ghi DNS
- Địa chỉ IP của máy tính được bảo vệ

- Địa chỉ vật lý (địa chỉ MAC) của máy tính được bảo vệ
- Định danh trong mục nhật ký sự kiện
- Tên nguồn dữ liệu trong nhật ký
- Tên nhật ký
- Thời gian sự kiện
- Giá trị băm MD5 và SHA256 của tập tin
- Tên đầy đủ của tập tin (bao gồm cả đường dẫn)
- Kích thước tập tin
- Địa chỉ IP từ xa và cổng có kết nối được thiết lập trong quá trình quét
- Địa chỉ IP của bộ điều hợp cục bộ
- Cổng mở trên bộ điều hợp cục bộ
- Giao thức dưới dạng số (theo tiêu chuẩn IANA)
- Tên tiến trình
- Đối số của tiến trình
- Đường dẫn đến tập tin của tiến trình
- Định danh Windows (PID) của tiến trình
- Định danh Windows (PID) của tiến trình gốc
- Tài khoản người dùng đã khởi tạo tiến trình
- Ngày và thời gian khởi tạo tiến trình
- Tên dịch vụ
- Mô tả về dịch vụ
- Đường dẫn và tên của dịch vụ DLL (đối với svchost)
- Đường dẫn và tên của tập tin thực thi dịch vụ
- Định danh Windows (PID) của dịch vụ
- Loại dịch vụ (ví dụ: trình điều khiển nhân hoặc bộ điều hợp)
- Trạng thái dịch vụ
- Chế độ khởi chạy dịch vụ
- Tên tài khoản người dùng

- Tên phân vùng
- Chữ cái phân vùng
- Loại phân vùng
- Giá trị registry Windows
- Giá trị thư mục registry
- Đường dẫn khóa registry (không có thư mục và tên giá trị)
- Thiết lập registry
- Hệ thống (môi trường)
- Tên và phiên bản của hệ điều hành được cài đặt trên máy tính
- Tên mạng của máy tính được bảo vệ
- Tên miền hoặc nhóm chứa máy tính được bảo vệ
- Tên trình duyệt
- Phiên bản trình duyệt
- Thời gian khi tài nguyên web được truy cập lần cuối
- URL từ yêu cầu HTTP
- Tên của tài khoản được sử dụng cho yêu cầu HTTP
- Tên tập tin của tiến trình đã thực hiện yêu cầu HTTP
- Đường dẫn đầy đủ đến tập tin của tiến trình đã thực hiện yêu cầu HTTP
- Định danh Windows (PID) của tiến trình đã thực hiện yêu cầu HTTP
- Liên kết giới thiệu HTTP (URL nguồn yêu cầu HTTP)
- URI của tài nguyên được yêu cầu qua HTTP
- Thông tin về tác nhân người dùng HTTP (ứng dụng đã thực hiện yêu cầu HTTP)
- Thời gian thực hiện yêu cầu HTTP
- Định danh duy nhất của tiến trình đã thực hiện yêu cầu HTTP

Dữ liệu để tạo chuỗi phát triển mối đe dọa

Theo mặc định, dữ liệu để tạo chuỗi phát triển mối đe dọa được lưu trữ trong vòng bảy ngày. Dữ liệu được tự động gửi đến Kaspersky Security Center.

Dữ liệu để tạo chuỗi phát triển mối đe dọa có thể chứa các thông tin sau:

- Ngày và giờ xảy ra sự cố
- Tên phát hiện
- Chế độ quét
- Trạng thái của hành động gần đây nhất liên quan đến sự phát hiện
- Lý do không thể xử lý phát hiện
- Loại đối tượng được phát hiện
- Tên đối tượng được phát hiện
- Trạng thái đe dọa sau khi đối tượng được xử lý
- Lý do không thể thực thi các hành động trên đối tượng
- Các hành động được thực hiện để hoàn tác các hành động độc hại
- Thông tin về đối tượng được xử lý:
 - Định danh duy nhất của tiến trình
 - Định danh duy nhất của tiến trình gốc
 - Định danh duy nhất của tập tin tiến trình
 - Định danh tiến trình Windows (PID)
 - Xử lý dòng lệnh
 - Tài khoản người dùng đã khởi tạo tiến trình
 - Mã của phiên đăng nhập trong đó tiến trình đang chạy
 - Loại phiên mà tiến trình đang chạy
 - Mức độ toàn vẹn của tiến trình đang được xử lý
 - Quyền thành viên của tài khoản người dùng đã khởi chạy tiến trình trong các nhóm miền và nhóm cục bộ đặc quyền
 - Định danh của đối tượng được xử lý
 - Tên đầy đủ của đối tượng được xử lý
 - Định danh của thiết bị được bảo vệ
 - Tên đầy đủ của đối tượng (tên tập tin cục bộ hoặc địa chỉ web của tập tin được tải xuống)
 - Giá trị băm MD5 hoặc SHA256 của đối tượng được xử lý
 - Loại đối tượng được xử lý
 - Ngày tạo đối tượng được xử lý

- Ngày khi đối tượng được xử lý được sửa đổi lần cuối
- Kích thước của đối tượng được xử lý
- Thuộc tính của đối tượng được xử lý
- Tổ chức đã ký đối tượng được xử lý
- Kết quả xác minh chứng chỉ số của đối tượng được xử lý
- Định danh bảo mật (SID) của đối tượng được xử lý
- Định danh múi giờ của đối tượng được xử lý
- Địa chỉ web tải xuống đối tượng được xử lý (chỉ dành cho các tập tin trên đĩa)
- Tên của ứng dụng đã tải xuống tập tin
- Giá trị băm MD5 và SHA256 của ứng dụng đã tải xuống tập tin
- Tên của ứng dụng đã sửa đổi tập tin lần cuối
- Giá trị băm MD5 và SHA256 của ứng dụng đã sửa đổi tập tin lần cuối
- Số lần khởi chạy đối tượng được xử lý
- Ngày và giờ khi đối tượng được xử lý được khởi chạy lần đầu
- Định danh duy nhất của tập tin
- Tên đầy đủ của tập tin (tên tập tin cục bộ hoặc địa chỉ web của tập tin đã tải xuống)
- Đường dẫn đến biến registry Windows được xử lý
- Tên của biến registry Windows được xử lý
- Giá trị của biến registry Windows được xử lý
- Loại biến registry Windows được xử lý
- Chỉ báo về quyền thành viên khóa registry được xử lý trong mục tự động chạy
- Địa chỉ web của yêu cầu web được xử lý
- Nguồn liên kết của yêu cầu web được xử lý
- Tác nhân người dùng của yêu cầu web được xử lý
- Loại yêu cầu web được xử lý (GET hoặc POST).
- Cổng IP cục bộ của yêu cầu web được xử lý
- Cổng IP từ xa của yêu cầu web được xử lý
- Hướng kết nối (vào hoặc ra) của yêu cầu web được xử lý

- Định danh của tiến trình mã độc được nhúng vào

Kaspersky Sandbox

Toàn bộ dữ liệu mà ứng dụng lưu trữ cục bộ trên máy tính sẽ bị xóa khỏi máy tính khi gỡ cài đặt Kaspersky Endpoint Security.

Dữ liệu dịch vụ

Kaspersky Endpoint Security sẽ lưu trữ các dữ liệu sau được xử lý trong quá trình phản hồi tự động:

- Các tập tin và dữ liệu được xử lý do người dùng nhập trong quá trình cấu hình tác nhân tích hợp sẵn của Kaspersky Endpoint Security:
 - Các tập tin được cách ly
 - Khóa công khai của chứng chỉ được sử dụng để tích hợp với Kaspersky Sandbox
- Bộ nhớ đệm của tác nhân tích hợp sẵn của Kaspersky Endpoint Security:
 - Thời gian khi kết quả quét được ghi vào bộ nhớ đệm
 - Giá trị băm MD5 của tác vụ quét
 - Định danh của tác vụ quét
 - Kết quả quét đối tượng
- Hàng chờ yêu cầu quét đối tượng:
 - ID của đối tượng trong hàng chờ
 - Thời gian khi đối tượng được đặt trong hàng chờ
 - Trạng thái xử lý của đối tượng trong hàng chờ
 - ID phiên người dùng trong hệ điều hành nơi tác vụ quét đối tượng được tạo
 - Định danh hệ thống (SID) của người dùng hệ điều hành có tài khoản được sử dụng để tạo tác vụ
 - Giá trị băm MD5 của tác vụ quét đối tượng
- Thông tin về các tác vụ mà tác nhân tích hợp sẵn của Kaspersky Endpoint Security đang chờ kết quả quét từ Kaspersky Sandbox:
 - Thời gian nhận được tác vụ quét đối tượng
 - Trạng thái xử lý đối tượng
 - ID phiên người dùng trong hệ điều hành nơi tác vụ quét đối tượng được tạo

- Định danh của tác vụ quét đối tượng
- Giá trị băm MD5 của tác vụ quét đối tượng
- Định danh hệ thống (SID) của người dùng hệ điều hành có tài khoản được sử dụng để tạo tác vụ
- Lược đồ XML của IOC được tạo tự động
- Giá trị băm MD5 hoặc SHA256 của đối tượng được quét
- Các lỗi xử lý
- Tên của các đối tượng mà tác vụ được tạo để quét
- Kết quả quét đối tượng

Dữ liệu trong các yêu cầu gửi tới Kaspersky Sandbox

Dữ liệu sau đây từ các yêu cầu từ tác nhân tích hợp của Kaspersky Endpoint Security tới Kaspersky Sandbox được lưu trữ cục bộ trên máy tính:

- Giá trị băm MD5 của tác vụ quét
- Định danh của tác vụ quét
- Đối tượng được quét và tất cả các tập tin liên quan

Dữ liệu nhận được do kết quả thực thi tác vụ Quét IOC (tác vụ độc lập)

Kaspersky Endpoint Security sẽ tự động gửi dữ liệu về kết quả thực thi tác vụ *Quét IOC* tới Kaspersky Security Center.

Dữ liệu trong kết quả thực hiện tác vụ *Quét IOC* có thể chứa các thông tin sau:

- Địa chỉ IP từ bảng ARP
- Địa chỉ vật lý từ bảng ARP
- Tên và loại bản ghi DNS
- Địa chỉ IP của máy tính được bảo vệ
- Địa chỉ vật lý (địa chỉ MAC) của máy tính được bảo vệ
- Định danh trong mục nhật ký sự kiện
- Tên nguồn dữ liệu trong nhật ký
- Tên nhật ký
- Thời gian sự kiện
- Giá trị băm MD5 và SHA256 của tập tin

- Tên đầy đủ của tập tin (bao gồm cả đường dẫn)
- Kích thước tập tin
- Địa chỉ IP từ xa và cổng có kết nối được thiết lập trong quá trình quét
- Địa chỉ IP của bộ điều hợp cục bộ
- Cổng mở trên bộ điều hợp cục bộ
- Giao thức dưới dạng số (theo tiêu chuẩn IANA)
- Tên tiến trình
- Đối số của tiến trình
- Đường dẫn đến tập tin của tiến trình
- Định danh Windows (PID) của tiến trình
- Định danh Windows (PID) của tiến trình gốc
- Tài khoản người dùng đã khởi tạo tiến trình
- Ngày và thời gian khởi tạo tiến trình
- Tên dịch vụ
- Mô tả về dịch vụ
- Đường dẫn và tên của dịch vụ DLL (đối với svchost)
- Đường dẫn và tên của tập tin thực thi dịch vụ
- Định danh Windows (PID) của dịch vụ
- Loại dịch vụ (ví dụ: trình điều khiển nhân hoặc bộ điều hợp)
- Trạng thái dịch vụ
- Chế độ khởi chạy dịch vụ
- Tên tài khoản người dùng
- Tên phân vùng
- Chữ cái phân vùng
- Loại phân vùng
- Giá trị registry Windows
- Giá trị thư mục registry
- Đường dẫn khóa registry (không có thư mục và tên giá trị)

- Thiết lập registry
- Hệ thống (môi trường)
- Tên và phiên bản của hệ điều hành được cài đặt trên máy tính
- Tên mạng của máy tính được bảo vệ
- Tên miền hoặc nhóm chứa máy tính được bảo vệ
- Tên trình duyệt
- Phiên bản trình duyệt
- Thời gian khi tài nguyên web được truy cập lần cuối
- URL từ yêu cầu HTTP
- Tên của tài khoản được sử dụng cho yêu cầu HTTP
- Tên tập tin của tiến trình đã thực hiện yêu cầu HTTP
- Đường dẫn đầy đủ đến tập tin của tiến trình đã thực hiện yêu cầu HTTP
- Định danh Windows (PID) của tiến trình đã thực hiện yêu cầu HTTP
- Liên kết giới thiệu HTTP (URL nguồn yêu cầu HTTP)
- URI của tài nguyên được yêu cầu qua HTTP
- Thông tin về tác nhân người dùng HTTP (ứng dụng đã thực hiện yêu cầu HTTP)
- Thời gian thực hiện yêu cầu HTTP
- Định danh duy nhất của tiến trình đã thực hiện yêu cầu HTTP

Tuân thủ luật của Liên minh châu Âu (GDPR)

Kaspersky Endpoint Security có thể truyền dữ liệu tới Kaspersky trong các trường hợp sau:

- Sử dụng Kaspersky Security Network.
- Kích hoạt ứng dụng bằng một mã kích hoạt.
- Cập nhật mô-đun ứng dụng và cơ sở dữ liệu diệt virus.
- Truy cập theo liên kết trong giao diện ứng dụng.
- Ghi kết xuất.

Bất kể phân loại dữ liệu và lãnh thổ mà dữ liệu được nhận, Kaspersky tuân thủ các tiêu chuẩn cao về bảo mật dữ liệu và sử dụng các biện pháp pháp lý, tổ chức và kỹ thuật khác nhau để bảo vệ dữ liệu của người dùng, để đảm bảo an toàn và bảo mật dữ liệu, đồng thời đảm bảo thực hiện các quyền của người dùng được pháp luật hiện hành bảo đảm. Văn bản của Chính sách quyền riêng tư được kèm theo [gói phân phối ứng dụng](#) và có sẵn trên [website của Kaspersky](#).

Trước khi sử dụng Kaspersky Endpoint Security, vui lòng đọc kỹ mô tả về dữ liệu được truyền trong [Thỏa thuận giấy phép người dùng cuối](#) và [Tuyên bố Kaspersky Security Network](#). Nếu dữ liệu cụ thể được truyền từ Kaspersky Endpoint Security theo bất kỳ kịch bản đã mô tả có thể được phân loại là dữ liệu cá nhân theo luật hoặc tiêu chuẩn địa phương của bạn, bạn phải đảm bảo rằng dữ liệu đó được xử lý hợp pháp và được sự đồng ý của người dùng cuối đối với việc thu thập và truyền dữ liệu đó.

Đọc Thỏa thuận giấy phép người dùng cuối và truy cập [website Kaspersky](#) để tìm hiểu thêm về cách chúng tôi nhận, 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 Kaspersky Security Network. Các tập tin license.txt và ksn_<language ID>.txt chứa nội dung của Thỏa thuận giấy phép người dùng cuối và Tuyên bố Kaspersky Security Network và được bao gồm trong [gói phân phối](#) của ứng dụng.

Nếu bạn không muốn truyền dữ liệu đến Kaspersky, bạn có thể tắt cung cấp dữ liệu.

Sử dụng Kaspersky Security Network

Bằng cách sử dụng Kaspersky Security Network, bạn đồng ý tự động cung cấp dữ liệu được liệt kê trong [Tuyên bố Kaspersky Security Network](#). Nếu bạn không đồng ý cung cấp dữ liệu này cho Kaspersky, hãy sử dụng KSN Riêng hoặc [tắt sử dụng KSN](#). Để biết thêm chi tiết về KSN Riêng, vui lòng tham khảo [tài liệu về Kaspersky Private Security Network](#).

Kích hoạt ứng dụng bằng một mã kích hoạt

Bằng cách sử dụng mã kích hoạt, bạn đồng ý tự động cung cấp dữ liệu được liệt kê trong [Thỏa thuận giấy phép người dùng cuối](#). Nếu bạn không đồng ý cung cấp dữ liệu này cho Kaspersky, hãy sử dụng một [tập tin khóa để kích hoạt Kaspersky Endpoint Security](#).

Cập nhật mô-đun ứng dụng và cơ sở dữ liệu diệt virus

Bằng cách sử dụng máy chủ Kaspersky, bạn đồng ý tự động cung cấp dữ liệu được liệt kê trong [Thỏa thuận giấy phép người dùng cuối](#). Kaspersky yêu cầu thông tin này để xác minh rằng Kaspersky Endpoint Security đang được sử dụng hợp pháp. Nếu bạn không đồng ý cung cấp thông tin này cho Kaspersky, hãy sử dụng [Kaspersky Security Center để cập nhật cơ sở dữ liệu](#) hoặc sử dụng [Kaspersky Update Utility](#).

Truy cập theo liên kết trong giao diện ứng dụng

Bằng cách sử dụng các liên kết trong giao diện ứng dụng, bạn đồng ý tự động cung cấp dữ liệu được liệt kê trong [Thỏa thuận giấy phép người dùng cuối](#). Danh sách chính xác của dữ liệu được truyền trong từng liên kết cụ thể phụ thuộc vào vị trí của liên kết trong giao diện ứng dụng và vấn đề mà liên kết đó muốn khắc phục. Nếu bạn không đồng ý cung cấp dữ liệu này cho Kaspersky, hãy sử dụng [giao diện ứng dụng đơn giản hóa](#) hoặc [ẩn giao diện ứng dụng](#).

Ghi kết xuất

Nếu bạn đã [bật tính năng ghi tập tin kết xuất](#), Kaspersky Endpoint Security sẽ tạo một tập tin kết xuất chứa tất cả dữ liệu bộ nhớ từ các quy trình ứng dụng tại thời điểm tập tin kết xuất này được tạo.

Bắt đầu

Sau khi cài đặt Kaspersky Endpoint Security, bạn có thể quản lý ứng dụng bằng các giao diện sau:

- [Giao diện cục bộ của ứng dụng.](#)
- Bảng điều khiển quản trị Kaspersky Security Center.
- Bảng điều khiển web Kaspersky Security Center.
- Bảng điều khiển đám mây Kaspersky Security Center.

Bảng điều khiển quản trị Kaspersky Security Center

Kaspersky Security Center cho phép bạn cài đặt và gỡ bỏ, khởi động và dừng Kaspersky Endpoint Security từ xa, cấu hình thiết lập ứng dụng, thay đổi các thành phần ứng dụng có thể được sử dụng, bổ sung khóa, cũng như bắt đầu và dừng các tác vụ cập nhật và tác vụ quét.

Ứng dụng có thể được quản lý qua Kaspersky Security Center sử dụng Tiện ích quản lý Kaspersky Endpoint Security.

Để biết thêm chi tiết về việc quản lý ứng dụng thông qua Kaspersky Security Center, hãy tham khảo [Trợ giúp Kaspersky Security Center](#).

Bảng điều khiển web Kaspersky Security Center hoặc Bảng điều khiển đám mây Kaspersky Security Center

Bảng điều khiển web Kaspersky Security Center (sau đây cũng được gọi là "*Bảng điều khiển web*") là một ứng dụng web để tập trung việc thực hiện các tác vụ chính nhằm quản lý và bảo trì hệ thống bảo mật cho mạng lưới của một tổ chức. Bảng điều khiển web là một thành phần của Kaspersky Security Center với một giao diện người dùng. Để biết thông tin chi tiết về Bảng điều khiển web Kaspersky Security Center, hãy [tham khảo Trợ giúp Kaspersky Security Center](#).

Bảng điều khiển đám mây Kaspersky Security Center (sau đây gọi là "*Bảng điều khiển đám mây*") là một giải pháp dựa trên đám mây để bảo vệ và quản lý mạng của tổ chức. Để biết thông tin chi tiết về Bảng điều khiển đám mây Kaspersky Security Center, [vui lòng tham khảo Trợ giúp Bảng điều khiển đám mây Kaspersky Security Center](#).

Bảng điều khiển web và Bảng điều khiển đám mây cho phép bạn thực hiện các thao tác sau:

- Giám sát trạng thái hệ thống bảo mật của tổ chức bạn.
- Cài đặt các ứng dụng Kaspersky trên những thiết bị trong mạng của bạn.
- Quản lý các ứng dụng được cài đặt.
- Xem báo cáo về trạng thái của hệ thống bảo mật.

Việc quản lý Kaspersky Endpoint Security thông qua Bảng điều khiển web, Bảng điều khiển đám mây và Bảng điều khiển quản trị Kaspersky Security Center đều cung cấp các khả năng quản lý khác nhau. Các [thành phần và tác vụ khả dụng](#) cũng khác nhau đối với các Bảng điều khiển khác nhau.

Thông tin về Tiện ích Quản lý Kaspersky Endpoint Security cho Windows

Tiện ích quản lý Kaspersky Endpoint Security cho Windows cho phép tương tác giữa Kaspersky Endpoint Security và Kaspersky Security Center. Tiện ích quản lý cho phép bạn quản lý Kaspersky Endpoint Security bằng cách sử dụng [chính sách, tác vụ](#), và [thiết lập cục bộ của ứng dụng](#). Tương tác với Bảng điều khiển web Kaspersky Security Center được cung cấp bởi tiện ích web.

Phiên bản của Tiện ích quản lý có thể khác với phiên bản của ứng dụng Kaspersky Endpoint Security được cài đặt trên máy khách. Nếu phiên bản được cài đặt của Tiện ích quản lý 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 lý. Các cấu hình này có thể được sửa đổi bởi người dùng trong giao diện cục bộ của Kaspersky Endpoint Security. Các thiết lập này có thể được sửa đổi bởi người dùng trong giao diện cục bộ của Kaspersky Endpoint Security.

Theo mặc định, tiện ích web không được cài đặt trong Bảng điều khiển web Kaspersky Security Center. Khác với Tiện ích quản lý cho Bảng điều khiển quản trị Kaspersky Security Center, vốn được cài đặt lên một máy trạm của quản trị viên, tiện ích web phải được cài đặt lên một máy tính có cài đặt Bảng điều khiển web Kaspersky Security Center. Chức năng của tiện ích web này được cung cấp đến tất cả các quản trị viên có quyền truy cập Bảng điều khiển web trong một trình duyệt. Bạn có thể xem danh sách các tiện ích web được cài đặt trong giao diện Bảng điều khiển web: **Console settings** → **Web plug-ins**. Để biết thêm chi tiết về khả năng tương thích của các phiên bản tiện ích web và Bảng điều khiển web, vui lòng tham khảo [Trợ giúp của Kaspersky Security Center](#).

Cài đặt tiện ích web

Bạn có thể cài đặt tiện ích web như sau:

- Cài đặt tiện ích web sử dụng Trình hướng dẫn bắt đầu nhanh của Bảng điều khiển web Kaspersky Security Center.

Bảng điều khiển web sẽ tự động nhắc bạn chạy Quick Start Wizard khi kết nối Bảng điều khiển web đến Máy chủ quản trị lần đầu tiên. Bạn cũng có thể chạy Trình hướng dẫn bắt đầu nhanh trong giao diện Bảng điều khiển web (**Discovery & Deployment** → **Deployment & Assignment** → **Quick Start Wizard**). Trình hướng dẫn bắt đầu nhanh cũng có thể kiểm tra liệu các tiện ích web được cài đặt có là bản mới nhất và tải về các bản cập nhật cần thiết. Để biết thêm chi tiết về Trình hướng dẫn bắt đầu nhanh cho Bảng điều khiển web Kaspersky Security Center, vui lòng tham khảo [Trợ giúp của Kaspersky Security Center](#).

- Cài đặt tiện ích web từ danh sách các gói phân phối khả dụng trong Bảng điều khiển web.

Để cài đặt tiện ích web, chọn gói phân phối của tiện ích web Kaspersky Endpoint Security trong giao diện Bảng điều khiển web: **Console settings** → **Web plug-ins**. Danh sách các gói phân phối khả dụng được cập nhật tự động sau khi các phiên bản mới của ứng dụng Kaspersky được phát hành.

- Tải về gói phân phối cho Bảng điều khiển web từ một nguồn bên ngoài.

Để cài đặt tiện ích web, thêm tập nén ZIP của gói phân phối cho tiện ích web Kaspersky Endpoint Security vào giao diện Bảng điều khiển web: **Console settings** → **Web plug-ins**. Ví dụ, gói phân phối của tiện ích web có thể được tải về từ website Kaspersky.

Cập nhật Tiện ích quản lý

Để cập nhật Tiện ích quản lý Kaspersky Endpoint Security cho Windows, hãy tải xuống phiên bản mới nhất của tiện ích (có trong [gói phân phối](#)) và chạy trình hướng dẫn cài đặt tiện ích.

Nếu một phiên bản mới của tiện ích web được phát hành, Bảng điều khiển web sẽ hiển thị thông báo *Có sẵn bản cập nhật cho các tiện ích được sử dụng*. Bạn có thể tiếp tục cập nhật phiên bản tiện ích web từ thông báo Bảng điều khiển web này. Bạn cũng có thể kiểm tra thủ công các bản cập nhật mới cho tiện ích web trong giao diện Bảng điều khiển web (**Console settings** → **Web plug-ins**). Các phiên bản cũ của tiện ích web sẽ tự động bị gỡ bỏ trong quá trình cập nhật.

Khi tiện ích web được cập nhật, các mục có sẵn (ví dụ như các chính sách hoặc tác vụ) sẽ được lưu. Các thiết lập mới của các mục để bổ sung chức năng mới của Kaspersky Endpoint Security sẽ xuất hiện trong các mục hiện có và có giá trị mặc định.

Bạn có thể cập nhật tiện ích web như sau:

- Cập nhật tiện ích web trong danh sách các tiện ích web trong chế độ trực tuyến.
Để cập nhật tiện ích web, bạn phải chọn gói phân phối của tiện ích web Kaspersky Endpoint Security trong giao diện Bảng điều khiển web (**Console settings** → **Web plug-ins**). Bảng điều khiển web sẽ kiểm tra các bản cập nhật có sẵn trên máy chủ Kaspersky và tải về các bản cập nhật liên quan.
- Cập nhật tiện ích web từ một tập tin.
Để cập nhật tiện ích web, bạn phải chọn tập nén ZIP của gói phân phối cho tiện ích web Kaspersky Endpoint Security trong giao diện Bảng điều khiển web: **Console settings** → **Web plug-ins**. Ví dụ, gói phân phối của tiện ích web có thể được tải về từ website Kaspersky. Bạn chỉ có thể cập nhật tiện ích web Kaspersky Endpoint Security đến một phiên bản mới hơn. Tiện ích web không thể được cập nhật đến một phiên bản cũ hơn.

Nếu có bất kỳ mục nào được mở (ví dụ như một chính sách hoặc tác vụ), tiện ích web sẽ kiểm tra thông tin tương thích của nó. Nếu phiên bản của tiện ích web bằng hoặc mới hơn phiên bản được quy định trong thông tin tương thích, bạn có thể thay đổi thiết lập của mục này. Nếu không, bạn không thể sử dụng tiện ích web để thay đổi các thiết lập của mục được chọn. Bạn nên cập nhật tiện ích web.

Các cân nhắc đặc biệt khi làm việc với các phiên bản khác nhau của tiện ích quản lý

Bạn chỉ có thể quản lý Kaspersky Endpoint Security qua Kaspersky Security Center nếu bạn có một Tiện ích quản lý 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 lý. Bạn có thể xem phiên bản tối thiểu được yêu cầu của Tiện ích quản lý trong tập tin installer.ini trong [gói phân phối](#).

Nếu có bất kỳ mục nào được mở (ví dụ như một chính sách hoặc tác vụ), Tiện ích quản lý sẽ kiểm tra thông tin tương thích của nó. Nếu phiên bản của Tiện ích quản lý bằng hoặc mới hơn phiên bản được quy định trong thông tin tương thích, bạn có thể thay đổi thiết lập của mục này. Nếu không, bạn không thể sử dụng Tiện ích quản lý để thay đổi các thiết lập của mục được chọn. Bạn được khuyến nghị nâng cấp Tiện ích quản lý.

Nâng cấp Tiện ích Quản trị Kaspersky Endpoint Security 10 cho Windows

Nếu Tiện ích quản lý Kaspersky Endpoint Security 10 cho Windows được cài đặt trong Bảng điều khiển quản trị, vui lòng cân nhắc các điều sau khi cài đặt Tiện ích Quản trị Kaspersky Endpoint Security 11 cho Windows:


- Tiện ích quản lý Kaspersky Endpoint Security 10 cho Windows sẽ không bị gỡ bỏ, và sẽ vẫn khả dụng để hoạt động. Do đó, bạn sẽ có quyền truy cập vào hai Tiện ích quản lý để làm việc với phiên bản ứng dụng 10 và 11.
- Tiện ích Quản trị Kaspersky Endpoint Security 11 cho Windows không hỗ trợ việc quản lý Kaspersky Endpoint Security 10 cho Windows trên máy tính của người dùng.
- Tiện ích quản lý Kaspersky Endpoint Security 11 cho Windows không hỗ trợ các mục (ví dụ như chính sách hay tác vụ) được tạo bằng Tiện ích quản lý Kaspersky Endpoint Security 10 cho Windows.

Bạn có thể sử dụng Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ để chuyển đổi các chính sách và tác vụ từ phiên bản 10 sang phiên bản 11. Để biết thêm chi tiết về việc chuyển đổi các chính sách và tác vụ, vui lòng tham khảo [Trợ giúp của Kaspersky Security Center](#).



Nâng cấp Tiện ích Quản trị Kaspersky Endpoint Security 11 cho Windows

Nếu Tiện ích Quản trị Kaspersky Endpoint Security 11 cho Windows được cài đặt trong Bảng điều khiển quản trị, vui lòng cân nhắc các điều sau khi cài đặt một phiên bản mới của Tiện ích Quản trị Kaspersky Endpoint Security 11 cho Windows:

- Các phiên bản cũ của Tiện ích Quản trị Kaspersky Endpoint Security 11 cho Windows sẽ bị gỡ bỏ.
- Phiên bản mới của Tiện ích Quản trị Kaspersky Endpoint Security 11 cho Windows hỗ trợ việc quản lý các phiên bản cũ của Kaspersky Endpoint Security 11 cho Windows trên máy tính của người dùng.
- Bạn có thể sử dụng phiên bản mới của Tiện ích quản lý để thay đổi các thiết lập trong chính sách, tác vụ và các mục khác được tạo bởi phiên bản cũ của Tiện ích quản lý.
- Đối với các thiết lập mới, một phiên bản mới của Tiện ích quản lý 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 Tiện ích quản lý được nâng cấp, bạn nên kiểm tra và lưu các giá trị cho thiết lập mới trong chính sách và hồ sơ chính sách. Nếu bạn không làm việc này, các nhóm thiết lập mới của Kaspersky Endpoint Security trên máy tính của người dùng sẽ nhận giá trị mặc định và có thể được chỉnh sửa (thuộc tính ) . Bạn nên kiểm tra thiết lập bắt đầu với các chính sách và hồ sơ chính sách ở phân cấp cao nhất. Bạn cũng nên sử dụng tài khoản người dùng có quyền truy cập đến tất cả các khu vực chức năng của Kaspersky Security Center.

Để tìm hiểu về các tính năng mới của ứng dụng, vui lòng tham khảo Lưu ý phát hành hoặc [trợ giúp ứng dụng](#).

- Nếu một tham số mới đã được thêm vào một nhóm các thiết lập trong phiên bản mới của Tiện ích quản lý, trạng thái đã quy định trước đó của thuộc tính  /  cho nhóm thiết lập này sẽ không được thay đổi.
- Khi nâng cấp Tiện ích quản lý lên phiên bản 11.2.0, bạn cần mở một chính sách để tự động chuyển đổi chính sách đó. Khi làm như vậy, Kaspersky Endpoint Security sẽ nhắc bạn xác nhận để tham gia KSN. Nếu bạn đã nâng cấp ứng dụng lên phiên bản 11.20 trên máy tính của tổ chức mình, việc tham gia KSN sẽ bị vô hiệu hóa cho đến khi bạn chấp nhận các điều khoản tham gia KSN.

Những lưu ý đặc biệt khi sử dụng các giao thức được mã hóa để tương tác với các dịch vụ bên ngoài

Kaspersky Endpoint Security và Kaspersky Security Center sử dụng kênh giao tiếp được mã hóa với TLS (Transport Layer Security) để làm việc với các dịch vụ bên ngoài của Kaspersky. Kaspersky Endpoint Security sử dụng các dịch vụ bên ngoài cho các chức năng sau:

- cập nhật cơ sở dữ liệu và các mô-đun phần mềm ứng dụng;
- kích hoạt ứng dụng bằng mã kích hoạt (kích hoạt 2.0);
- sử dụng Kaspersky Security Network.

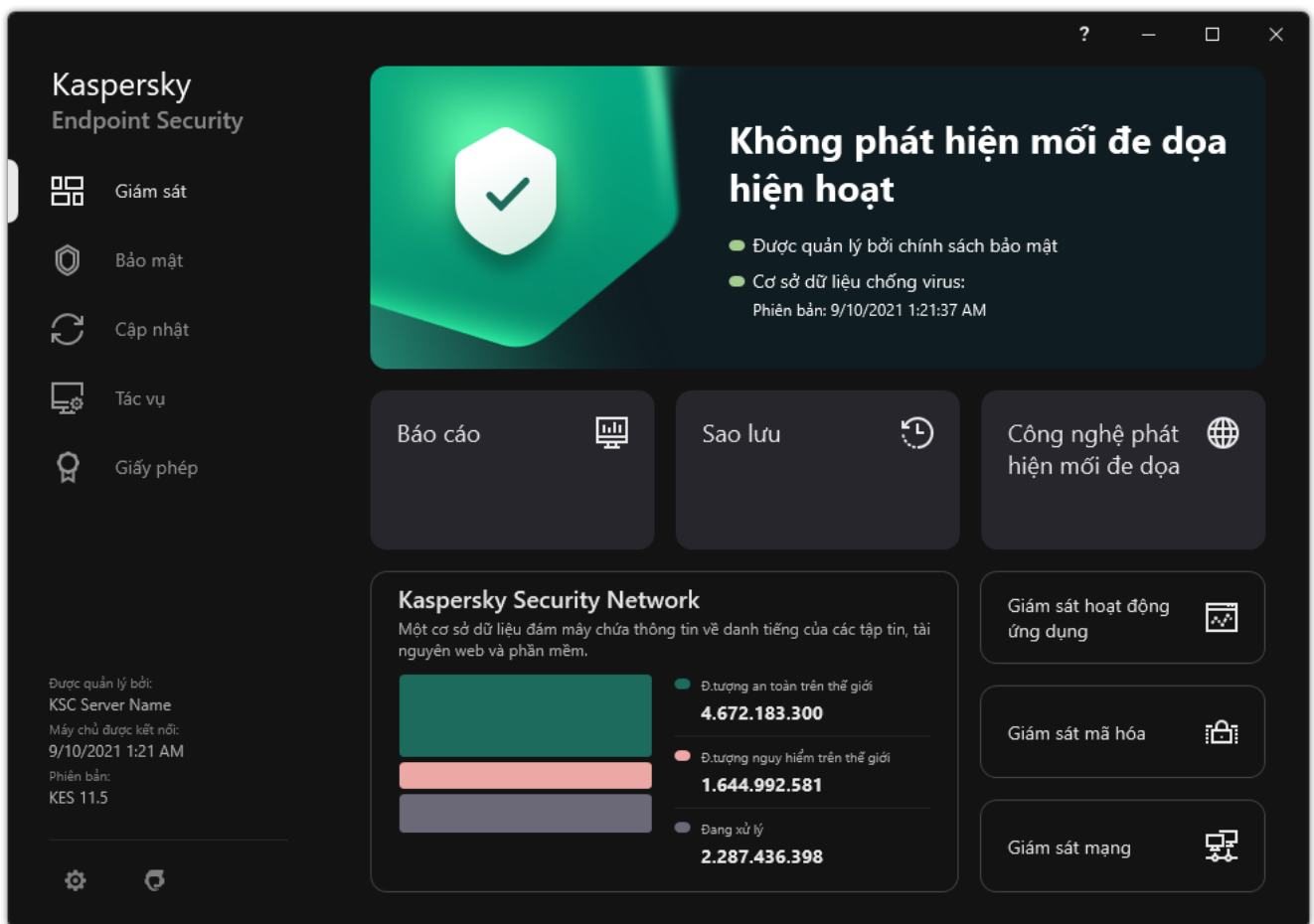
Việc sử dụng TLS bảo mật cho ứng dụng bằng cách cung cấp các tính năng sau:

- Mã hóa. Nội dung của tin nhắn được giữ bí mật và không được tiết lộ cho người dùng bên thứ ba.
- Tính toàn vẹn. Người nhận tin nhắn chắc chắn rằng nội dung tin nhắn không bị sửa đổi vì tin nhắn đã được chuyển tiếp bởi người gửi.
- Chứng thực. Người nhận chắc chắn rằng giao tiếp chỉ được thiết lập với máy chủ Kaspersky được tin tưởng.

Kaspersky Endpoint Security sử dụng chứng chỉ khóa công khai để xác thực máy chủ. Cần có cơ sở hạ tầng khóa công khai (PKI) để làm việc với các chứng chỉ. Cơ quan cấp chứng chỉ là một phần của PKI. Kaspersky sử dụng Cơ quan cấp chứng chỉ của riêng mình vì các dịch vụ của Kaspersky có tính kỹ thuật cao và không công khai. Trong trường hợp này, khi các chứng chỉ gốc của Thawte, VeriSign, GlobalTrust và các chứng chỉ khác bị thu hồi, Kaspersky PKI vẫn hoạt động mà không bị gián đoạn.

Các môi trường có MITM (công cụ phần mềm và phần cứng hỗ trợ phân tích giao thức HTTPS) được Kaspersky Endpoint Security coi là không an toàn. Các lỗi có thể gặp phải khi làm việc với các dịch vụ của Kaspersky. Ví dụ: có thể có lỗi liên quan đến việc sử dụng chứng chỉ tự ký. Những lỗi này có thể xảy ra do công cụ Kiểm tra HTTPS từ môi trường của bạn không nhận dạng được Kaspersky PKI. Để khắc phục những vấn đề này, bạn phải định cấu hình [loại trừ để tương tác với các dịch vụ bên ngoài](#).




Giao diện ứng dụng



Cửa sổ chính của ứng dụng

Giám sát

- **Báo cáo.** Xem các sự kiện đã xảy ra trong quá trình hoạt động của ứng dụng, các thành phần và tác vụ riêng lẻ.
- **Sao lưu.** Xem danh sách các bản sao đã lưu của các tập tin bị lây nhiễm mà ứng dụng đã xóa.
- **Công nghệ phát hiện mối đe dọa.** Xem thông tin về các công nghệ phát hiện mối đe dọa và số lượng các mối đe dọa được phát hiện bởi các công nghệ này.
- **Kaspersky Security Network.** Trạng thái kết nối giữa Kaspersky Endpoint Security và Kaspersky Security Network, và số liệu thống kê KSN toàn cầu. *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. Nếu bạn đang tham gia vào Kaspersky Security Network, các dịch vụ KSN sẽ cung cấp cho Kaspersky Endpoint Security thông tin về danh mục và danh tiếng của các tập tin được quét, cũng như thông tin về danh tiếng của các địa chỉ trang web được quét.
- **Giám sát hoạt động ứng dụng.** Xem thông tin về hoạt động của các ứng dụng được cài đặt. Giám sát hệ thống theo dõi các tập tin, các sự kiện hệ thống liên kết với các ứng dụng.
- **Giám sát mạng.** [Xem thông tin về hoạt động mạng của máy tính](#) theo thời gian thực.
- **Giám sát mã hóa.** Giám sát quá trình mã hóa hoặc giải mã đĩa theo thời gian thực. Giám sát mã hóa khả dụng nếu thành phần Kaspersky Disk Encryption hoặc thành phần

	BitLocker Drive Encryption được cài đặt.
Bảo mật	Tình trạng hoạt động của các thành phần được cài đặt. Bạn cũng có thể tiến hành cấu hình các thành phần hoặc xem báo cáo.
Cập nhật	Quản lý các tác vụ cập nhật của Kaspersky Endpoint Security. Bạn có thể cập nhật cơ sở dữ liệu diệt virus và mô-đun ứng dụng và khôi phục bản cập nhật gần đây nhất . Quản trị viên có thể ẩn mục đồ khởi người dùng hoặc hạn chế quản lý tác vụ .
Tác vụ	Quản lý các tác vụ quét của Kaspersky Endpoint Security. Bạn có thể chạy quét virus và kiểm tra tính toàn vẹn của ứng dụng . Quản trị viên có thể ẩn tác vụ khởi người dùng hoặc hạn chế quản lý tác vụ .
Giấy phép	Cấp giấy phép cho ứng dụng. Bạn có thể mua giấy phép , kích hoạt ứng dụng hoặc gia hạn gói đăng ký . Bạn cũng có thể xem thông tin về giấy phép hiện tại .
	Cấu hình thiết lập ứng dụng. Quản trị viên có thể cấm thay đổi thiết lập trong Kaspersky Security Center .
	Thông tin về ứng dụng: phiên bản hiện tại của Kaspersky Endpoint Security, ngày phát hành cơ sở dữ liệu, khóa và các thông tin khác. Bạn cũng có thể truy cập các tài nguyên thông tin của Kaspersky. Đây là nguồn 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.
	Thông báo chứa thông tin về các bản cập nhật có sẵn và các yêu cầu quyền truy cập tập tin và thiết bị được mã hóa.





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.

Các trạng thái biểu tượng ứng dụng sau được cung cấp để hiển thị thông tin hoạt động của ứng dụng:

- Biểu tượng  thể hiện rằng các thành phần bảo vệ đặc biệt quan trọng của ứng dụng đều được bật. Kaspersky Endpoint Security sẽ hiển thị một cảnh báo  nếu người dùng được yêu cầu thực hiện một hành động, ví dụ như khởi động lại máy tính sau khi cập nhật ứng dụng.
- Biểu tượng  thể hiện rằng các thành phần bảo vệ đặc biệt quan trọng của ứng dụng đang bị tắt hoặc bị trục trặc. Các thành phần bảo vệ có thể gặp trục trặc, ví dụ như nếu giấy phép đã hết hạn hoặc do lỗi ứng dụng. Kaspersky Endpoint Security sẽ hiển thị một cảnh báo  kèm mô tả vấn đề về bảo vệ máy tính.

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

- **Kaspersky Endpoint Security cho Windows.** Mở cửa sổ chính của ứng dụng. Trong cửa sổ này, bạn có thể 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.

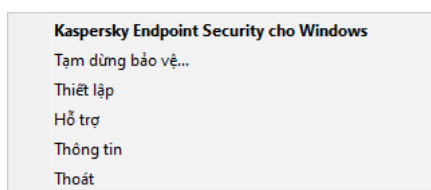
- **Tạm dừng bảo vệ / Khôi phục bảo vệ.** Tạm dừng hoạt động của tất cả các thành phần bảo vệ và kiểm soát không được đánh dấu khóa (🔒) trong chính sách. Trước khi thực hiện tác vụ này, chúng tôi khuyến cáo bạn tắt chính sách của Kaspersky Security Center.

Trước khi tạm dừng hoạt động của các thành phần bảo vệ và kiểm soát, ứng dụng sẽ yêu cầu [mật khẩu truy cập Kaspersky Endpoint Security](#) (mật khẩu tài khoản hoặc mật khẩu tạm thời). Khi đó, bạn có thể chọn thời gian tạm dừng: trong một khoảng thời gian nhất định, cho đến khi khởi động lại hoặc sau khi có yêu cầu của người dùng.

Mục menu ngữ cảnh này khả dụng nếu [Bảo vệ bằng mật khẩu được bật](#). Để khôi phục hoạt động của các thành phần bảo vệ và kiểm soát, hãy nhấn **Khôi phục bảo vệ** trong menu ngữ cảnh của ứng dụng.

Việc tạm dừng hoạt động của các thành phần bảo vệ và kiểm soát không ảnh hưởng đến việc thực thi hoạt động cập nhật và tác vụ quét. Ứng dụng cũng sẽ tiếp tục sử dụng Kaspersky Security Network.

- **Tắt chính sách / Bật chính sách.** Tắt một chính sách Kaspersky Security Center trên máy tính. Tất cả thiết lập của Kaspersky Endpoint Security đều có thể được cấu hình, bao gồm các thiết lập có khóa đóng trong chính sách (🔒). Nếu chính sách bị tắt, ứng dụng sẽ yêu cầu [mật khẩu để truy cập Kaspersky Endpoint Security](#) (mật khẩu tài khoản hoặc mật khẩu tạm thời). Mục menu ngữ cảnh này khả dụng nếu [Bảo vệ bằng mật khẩu được bật](#). Để bật chính sách, hãy chọn **Bật chính sách** trong menu ngữ cảnh của ứng dụng.
- **Thiết lập.** Sẽ mở cửa sổ thiết lập ứng dụng.
- **Hỗ trợ.** Thao tác này sẽ mở ra cửa sổ chứa thông tin cần thiết để liên hệ với bộ phận Hỗ trợ kỹ thuật Kaspersky.
- **Thông tin.** 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.



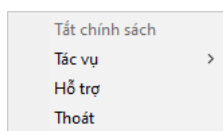
Menu ngữ cảnh của biểu tượng ứng dụng

Giao diện ứng dụng đơn giản hóa

Nếu chính sách Kaspersky Security Center được cấu hình [hiển thị giao diện ứng dụng đơn giản hóa](#) được áp dụng cho máy khách có cài đặt Kaspersky Endpoint Security, cửa sổ chính của ứng dụng sẽ không khả dụng trên máy khách này. Nhấn chuột phải để mở menu ngữ cảnh của biểu tượng Kaspersky Endpoint Security (xem hình dưới đây) chứa các mục sau:

- **Tắt chính sách / Bật chính sách.** Tắt một chính sách Kaspersky Security Center trên máy tính. Tất cả thiết lập của Kaspersky Endpoint Security đều có thể được cấu hình, bao gồm các thiết lập có khóa đóng trong chính sách (🔒). Nếu chính sách bị tắt, ứng dụng sẽ yêu cầu [mật khẩu để truy cập Kaspersky Endpoint Security](#) (mật khẩu tài khoản hoặc mật khẩu tạm thời). Mục menu ngữ cảnh này khả dụng nếu [Bảo vệ bằng mật khẩu được bật](#). Để bật chính sách, hãy chọn **Bật chính sách** trong menu ngữ cảnh của ứng dụng.

- **Tác vụ.** Danh sách thả xuống chứa các mục sau:
 - **Kiểm tra tính toàn vẹn.**
 - **Khôi phục cơ sở dữ liệu về phiên bản trước đây.**
 - **Quét toàn bộ.**
 - **Quét tùy chọn.**
 - **Quét khu vực quan trọng.**
 - **Chạy cập nhật cơ sở dữ liệu.**
- **Hỗ trợ.** Thao tác này sẽ mở ra cửa sổ chứa thông tin cần thiết để liên hệ với bộ phận Hỗ trợ kỹ thuật Kaspersky.
- **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 khi hiển thị giao diện đơn giản hóa

Cấu hình việc hiển thị giao diện ứng dụng

Bạn có thể cấu hình chế độ hiển thị giao diện ứng dụng cho người dùng. Người dùng có thể tương tác với ứng dụng theo các cách sau:

- **With simplified interface.** Trên một máy khách, cửa sổ chính của ứng dụng không thể truy cập và chỉ có [biểu tượng trong khu vực thông báo của Windows](#) khả dụng. Trong menu ngữ cảnh của biểu tượng, [thực hiện số lượng giới hạn các hoạt động với Kaspersky Endpoint Security](#). Kaspersky Endpoint Security cũng sẽ hiển thị các thông báo trên biểu tượng của ứng dụng.
- **With full interface.** Trên một máy tính khách, cửa sổ chính của Kaspersky Endpoint Security và [biểu tượng trong khu vực thông báo của Windows](#) sẽ khả dụng. Trong menu ngữ cảnh của biểu tượng, người dùng có thể thực hiện các thao tác với Kaspersky Endpoint Security. Kaspersky Endpoint Security cũng sẽ hiển thị các thông báo trên biểu tượng của ứng dụng.
- **No interface.** Trên một máy khách, không có dấu hiệu hoạt động của Kaspersky Endpoint Security được hiển thị. [Biểu tượng trong khu vực thông báo của Windows](#) và các thông báo không khả dụng.

[Cách cấu hình chế độ hiển thị giao diện ứng dụng trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Giao diện**.
6. Trong mục **Tương tác với người dùng**, hãy thực hiện một trong những hành động sau:
 - Chọn hộp kiểm **Hiển thị giao diện người dùng** nếu bạn muốn các thành phần giao diện sau được hiển thị trên máy khách:
 - Thư mục chứa tên ứng dụng trong menu **Start**
 - [Biểu tượng Kaspersky Endpoint Security](#) trong khu vực thông báo trên thanh tác vụ của Microsoft Windows
 - Thông báo bật lên

Nếu hộp kiểm này được chọn, người dùng có thể xem và tùy thuộc vào các quyền khả dụng, thay đổi thiết lập ứng dụng từ giao diện ứng dụng.

 - Xóa hộp kiểm **Hiển thị giao diện người dùng** nếu bạn muốn ẩn tất cả các dấu hiệu của Kaspersky Endpoint Security trên máy khách.
7. Trong mục **Tương tác với người dùng**, chọn hộp kiểm **Hiển thị giao diện giảm lược** nếu bạn muốn [giao diện ứng dụng đơn giản hóa](#) được hiển thị trên một máy khách có cài đặt Kaspersky Endpoint Security.

[Cách cấu hình chế độ hiển thị giao diện của ứng dụng trong Bảng điều khiển web và Bảng điều khiển đám mây](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Thiết lập tổng quát** → **Giao diện**.
5. Trong mục **Tương tác với người dùng**, hãy cấu hình cách hiển thị giao diện ứng dụng:
 - **With simplified interface.** Trên một máy khách, cửa sổ chính của ứng dụng không thể truy cập và chỉ có [biểu tượng trong khu vực thông báo của Windows](#) khả dụng. Trong menu ngữ cảnh của biểu tượng, [thực hiện số lượng giới hạn các hoạt động với Kaspersky Endpoint Security](#). Kaspersky Endpoint Security cũng sẽ hiển thị các thông báo trên biểu tượng của ứng dụng.
 - **With full interface.** Trên một máy tính khách, cửa sổ chính của Kaspersky Endpoint Security và [biểu tượng trong khu vực thông báo của Windows](#) sẽ khả dụng. Trong menu ngữ cảnh của biểu tượng, người dùng có thể thực hiện các thao tác với Kaspersky Endpoint Security. Kaspersky Endpoint Security cũng sẽ hiển thị các thông báo trên biểu tượng của ứng dụng.
 - **No interface.** Trên một máy khách, không có dấu hiệu hoạt động của Kaspersky Endpoint Security được hiển thị. [Biểu tượng trong khu vực thông báo của Windows](#) và các thông báo không khả dụng.
6. Lưu các thay đổi của bạn.

Bắt đầu

Sau khi triển khai ứng dụng trên các máy khách, để làm việc với Kaspersky Endpoint Security từ Bảng điều khiển Kaspersky Security Center, bạn cần thực hiện các hành động sau:

- Tạo và cấu hình một 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. Trình hướng dẫn bắt đầu nhanh của Kaspersky Security Center sẽ tự động tạo một chính sách cho Kaspersky Endpoint Security.
- Tạo các tác vụ *Cập nhật* và *Quét virus*.
Tác vụ *Cập nhật* là bắt buộc để cập nhật tính năng bảo mật của máy tính. Khi tác vụ này được thực hiện, Kaspersky Endpoint Security [sẽ cập nhật cơ sở dữ liệu diệt virus và mô-đun ứng dụng](#). Tác vụ *Update* được tạo tự động bởi Trình hướng dẫn bắt đầu nhanh của Kaspersky Security Center. Để tạo tác vụ *Update*, hãy cài đặt tiện ích web của Kaspersky Endpoint Security cho Windows khi đang chạy Trình hướng dẫn.
Tác vụ *Quét virus* là bắt buộc để phát hiện kịp thời virus cùng các loại phần mềm độc hại khác. Bạn cần tạo thủ công tác vụ *Quét Virus*.

[Cách tạo tác vụ Quét virus trong Bảng điều khiển quản trị.\(MMC\)](#) 

1. Trong Bảng điều khiển quản trị, hãy vào thư mục **Administration Server** → **Tác vụ**.

Danh sách tác vụ sẽ mở.

2. Nhấn nút **New task**.

Trình hướng dẫn Tác vụ sẽ được bắt đầu. Làm theo chỉ dẫn của Trình hướng dẫn.

Bước 1. Chọn loại tác vụ

Chọn **Kaspersky Endpoint Security cho Windows (11.9.0)** → **Quét virus**.

Bước 2. Phạm vi quét

Tạo danh sách các đối tượng được Kaspersky Endpoint Security quét khi thực hiện một tác vụ quét.

Bước 3. Hành động của Kaspersky Endpoint Security

Chọn hành động khi phát hiện mối đe dọa:

- **Khử mã độc; xóa nếu không thể khử mã độc.** Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ tự động khử nhiễm tất cả các tập tin bị nhiễm virus được phát hiện. Nếu việc khử nhiễm thất bại, Kaspersky Endpoint Security sẽ xóa các tập tin đó.
- **Khử mã độc; thông báo nếu không thể khử mã độc.** Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ tự động khử nhiễm tất cả các tập tin bị nhiễm virus được phát hiện. Nếu không thể khử mã độc, Kaspersky Endpoint Security sẽ bổ sung thông tin về tập tin nhiễm mã độc được phát hiện vào danh sách các mối đe dọa đang hoạt động.
- **Thông báo.** Nếu tùy chọn này được sử dụng, Kaspersky Endpoint Security sẽ bổ sung thông tin về tập tin nhiễm mã độc vào danh sách các mối đe dọa đang hoạt động khi phát hiện những tập tin này.
- **Chạy Khử mã độc nâng cao ngay lập tức.** Nếu hộp kiểm được chọn, Kaspersky Endpoint Security sẽ sử dụng công nghệ Khử mã độc nâng cao để xử lý các mối đe dọa hoạt động trong quá trình quét.

Công nghệ khử mã độc nâng cao nhằm tẩy sạch các ứng dụng độc hại ra khỏi hệ điều hành. Đó là các ứng dụng độc hại đã khởi chạy 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 mã độc nâng cao 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 mã độc nâng cao hoàn thành, Kaspersky Endpoint Security sẽ khởi động lại máy tính mà không nhắc người dùng xác nhận.

Cấu hình chế độ chạy tác vụ bằng cách sử dụng **Chỉ chạy khi máy tính đang rảnh**. Hộp kiểm này bật / tắt chức năng đình chỉ tác vụ *Quét virus* khi tài nguyên máy tính bị hạn chế. Kaspersky Endpoint Security sẽ tạm ngưng tác vụ *Quét virus* nếu trình bảo vệ màn hình đang tắt và máy tính đang được mở khóa.

Bước 4. Chọn các thiết bị sẽ được gán tác vụ

Chọn các máy tính sẽ được thực hiện tác vụ trên đó. Các tùy chọn sau có thể được sử dụng:

- Gán tác vụ vào một nhóm quản trị. Trong trường hợp này, tác vụ sẽ được gán cho các máy tính được bao gồm trong một nhóm quản trị đã được tạo trước đó.
- Chọn các máy tính được Máy chủ quản trị phát hiện trong mạng – *các thiết bị chưa được gán*. Các thiết bị được quy định có thể bao gồm các thiết bị trong nhóm quản trị cũng như các thiết bị chưa được gán.
- Nhập vào thủ công địa chỉ của thiết bị, hoặc nhập các địa chỉ từ một danh sách. Bạn có thể quy định tên NetBIOS, địa chỉ IP, và địa chỉ IP mạng con của các thiết bị mà bạn muốn gán tác vụ.

Bước 5. Chọn tài khoản để chạy tác vụ

Chọn một tài khoản để chạy tác vụ *Quét virus*. Theo mặc định, Kaspersky Endpoint Security khởi chạy tác vụ với quyền của tài khoản người dùng cục bộ. Nếu phạm vi quét bao gồm các ổ đĩa mạng hoặc các đối tượng khác có quyền truy cập hạn chế, hãy chọn tài khoản người dùng có đủ quyền truy cập.

Bước 6. Cấu hình lịch khởi chạy tác vụ

Cấu hình lịch để bắt đầu một tác vụ, ví dụ như thủ công hoặc sau khi cơ sở dữ liệu diệt virus được tải xuống kho lưu trữ.

Bước 7. Xác định tên tác vụ

Nhập tên cho tác vụ, ví dụ: *Quét toàn bộ hàng ngày*.

Bước 8. Hoàn tất việc tạo tác vụ

Thoát Trình hướng dẫn. Nếu cần, hãy chọn hộp kiểm **Run the task after the Wizard finishes**. Bạn có thể giám sát tiến độ của tác vụ trong thuộc tính tác vụ. Kết quả là, tác vụ Quét virus sẽ được thực thi trên máy tính của người dùng theo lịch được quy định.

[Cách tạo tác vụ Quét virus trong Bảng điều khiển web](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.
Danh sách tác vụ sẽ mở.
2. Nhấn vào nút **Thêm**.
Trình hướng dẫn Tác vụ sẽ được bắt đầu.
3. Cấu hình các thiết lập của tác vụ:
 - a. Trong danh sách thả xuống **Ứng dụng**, hãy chọn **Kaspersky Endpoint Security cho Windows (11.9.0)**.
 - b. Trong danh sách thả xuống **Loại tác vụ**, hãy chọn **Quét virus**.
 - c. Trong trường **Task name**, nhập một mô tả ngắn, ví dụ như *Quét hàng tuần*.
 - d. Trong phần **Select devices to which the task will be assigned**, chọn phạm vi tác vụ.
4. Chọn các thiết bị theo phạm vi tác vụ được chọn. Chuyển sang bước tiếp theo.
5. Thoát Trình hướng dẫn.
Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ.
6. Để cấu hình lịch tác vụ, vào thuộc tính tác vụ.
Bạn nên lên lịch cho tác vụ chạy ít nhất mỗi tuần một lần.
7. Chọn hộp kiểm cạnh tác vụ.
8. Nhấn vào nút **Chạy**.
Bạn có thể giám sát trạng thái của tác vụ, và số thiết bị trên đó tác vụ được hoàn tất thành công hoặc hoàn tất với một lỗi.

Kết quả là, tác vụ Quét virus sẽ được thực thi trên máy tính của người dùng theo lịch được quy định.

Quản lý chính sách

Chính sách là một tập hợp các thiết lập ứng dụng được quy định trong một nhóm quản trị. Bạn có thể cấu hình nhiều chính sách với các giá trị khác nhau cho một ứng dụng. Một ứng dụng có thể chạy dưới các thiết lập khác nhau cho các nhóm quản trị khác nhau. Mỗi nhóm quản trị có thể có chính sách riêng cho một ứng dụng.

Các thiết lập chính sách được gửi đến máy khách qua Network Agent trong quá trình *đồng bộ hóa*. Theo mặc định, Máy chủ quản trị thực hiện đồng bộ ngay sau khi thiết lập chính sách được thay đổi. Cổng UDP 15000 trên máy khách được sử dụng để đồng bộ. Theo mặc định, Máy chủ quản trị sẽ tiến hành đồng bộ sau mỗi 15 phút. Nếu đồng bộ thất bại sau khi thiết lập chính sách được thay đổi, nỗ lực đồng bộ tiếp theo sẽ được thực hiện theo lịch đã được cấu hình.

Chính sách hoạt động và không hoạt động

Một chính sách dành cho một nhóm máy tính được quản lý và có thể hoạt động hoặc không hoạt động. Các thiết lập của một chính sách hoạt động được lưu trên máy khách trong quá trình đồng bộ. Bạn không thể áp dụng đồng thời nhiều chính sách cho một máy tính, do đó chỉ một chính sách có thể hoạt động trong mỗi nhóm.



Bạn có thể tạo số lượng không giới hạn các chính sách không hoạt động. Một chính sách không hoạt động không ảnh hưởng đến các thiết lập ứng dụng trên máy tính trong mạng. Các chính sách không hoạt động nhằm chuẩn bị cho các tình huống khẩn cấp, ví dụ như tấn công virus. Nếu có một cuộc tấn công qua ổ đĩa flash, bạn có thể kích hoạt một chính sách chặn truy cập đến các ổ đĩa flash. Trong trường hợp này, chính sách hoạt động sẽ tự động bị vô hiệu.

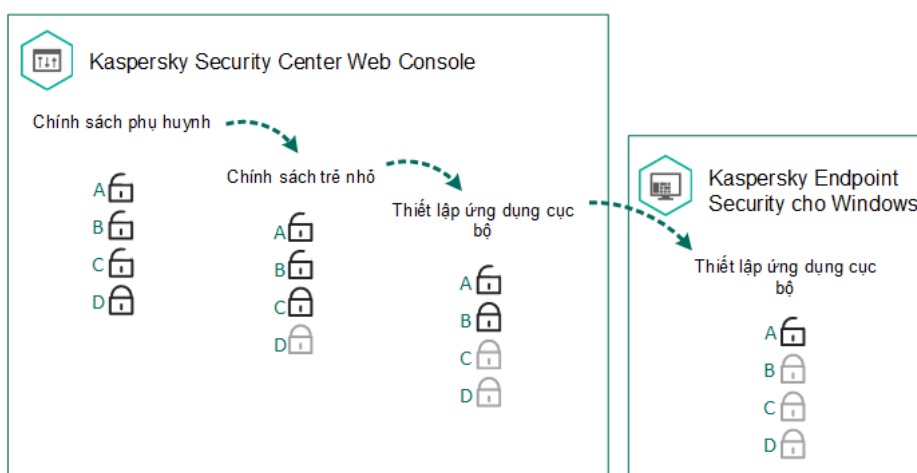
Chính sách ngoài văn phòng

Một chính sách ngoài văn phòng được kích hoạt khi máy tính rời khỏi mạng doanh nghiệp.

Kế thừa thiết lập

Các chính sách, giống như các nhóm quản trị, được sắp xếp theo cấp bậc. Theo mặc định, chính sách con sẽ kế thừa thiết lập từ chính sách cha. *Chính sách con* là một chính sách cho các phân cấp con, nghĩa là một chính sách cho các nhóm quản trị con và Máy chủ quản trị thứ cấp. Bạn có thể vô hiệu hóa việc kế thừa thiết lập từ chính sách cha.

Mỗi thiết lập chính sách đều có thuộc tính  chỉ báo rằng liệu thiết lập có thể được sửa đổi trong chính sách con hoặc trong [thiết lập cục bộ của ứng dụng](#). Chỉ áp dụng được  thuộc tính nếu chế độ kế thừa thiết lập chính sách cha được bật cho chính sách con. Các chính sách ngoài văn phòng không ảnh hưởng đến các chính sách khác trong phân cấp nhóm quản trị.



Kế thừa thiết lập




Quyền 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.



Tạo một chính sách

[Cách tạo chính sách trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Nhấn nút **New policy**.
Trình hướng dẫn Chính sách sẽ được bắt đầu.
5. Làm theo chỉ dẫn của Trình hướng dẫn Chính sách.

[Cách tạo chính sách trong Bảng điều khiển web và Bảng điều khiển đám mây](#)²

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào nút **Thêm**.
Trình hướng dẫn Chính sách sẽ được bắt đầu.
3. Chọn Kaspersky Endpoint Security và nhấn **Tiếp theo**.
4. Vui lòng đọc và chấp nhận các điều khoản của Tuyên bố Kaspersky Security Network (KSN) và nhấn **Tiếp theo**.
5. Trên thẻ **Tổng quát**, bạn có thể thực hiện những hành động sau:
 - Thay đổi tên chính sách.
 - Chọn trạng thái chính sách:
 - **Hoạt động**. Sau lần đồng bộ tiếp theo, chính sách sẽ được sử dụng làm chính sách hoạt động trên máy tính.
 - **Không hoạt động**. Chính sách sao lưu. Nếu cần thiết, một chính sách không hoạt động có thể được chuyển trạng thái thành hoạt động.
 - **Out-of-office**. Chính sách này được kích hoạt khi máy tính rời khỏi mạng doanh nghiệp.
 - Cấu hình việc kế thừa thiết lập:
 - **Inherit settings from parent policy**. Nếu công tắc này được bật, các giá trị thiết lập chính sách sẽ được kế thừa từ chính sách cấp cao nhất. Các thiết lập chính sách không thể được chỉnh sửa nếu  được thiết lập cho chính sách cha.
 - **Force inheritance of settings in child policies**. Nếu nút công tắc này được bật, giá trị của thiết lập chính sách sẽ được sao chép đến các chính sách con. Trong thuộc tính của các chính sách con, nút bật/tắt **Inherit settings from parent policy** sẽ được bật tự động và bạn không thể tắt. Cấu hình chính sách con được kế thừa từ chính sách cha, ngoại trừ cho các thiết lập được đánh dấu . Các thiết lập chính sách con không thể được chỉnh sửa nếu  được thiết lập cho chính sách cha.
6. Trên thẻ **Application settings**, bạn có thể cấu hình [Cấu hình chính sách Kaspersky Endpoint Security](#).
7. Lưu các thay đổi của bạn.

Kết quả là, các thiết lập của Kaspersky Endpoint Security sẽ được cấu hình trên máy khách ở lần đồng bộ hóa tiếp theo. Bạn có thể xem thông tin về chính sách đang được áp dụng cho máy tính trong giao diện Kaspersky Endpoint Security bằng cách nhấn vào nút  trên màn hình chính (ví dụ như tên chính sách). Để thực hiện, trong thiết lập của chính sách Network Agent, bạn cần bật nhận dữ liệu chính sách mở rộng. Để biết thêm chi tiết về chính sách Network Agent, vui lòng tham khảo [Trợ giúp của Kaspersky Security Center](#) .

Chỉ báo mức độ bảo mật

Chỉ báo mức độ bảo mật được hiển thị ở phần trên của cửa sổ **Properties: <Policy name>**. Chỉ báo này có thể nhận một trong các giá trị sau:

- **Cấp độ bảo vệ cao.** Chỉ báo nhận giá trị này và chuyển sang màu xanh lục nếu tất cả các thành phần từ danh mục sau được bật:
 - **Nghiêm trọng.** Danh mục này bao gồm các thành phần sau đây:
 - Bảo vệ mối đe dọa tập tin.
 - Phát hiện hành vi.
 - Phòng chống khai thác.
 - Công cụ khắc phục.
 - **Quan trọng.** Danh mục này bao gồm các thành phần sau đây:
 - Kaspersky Security Network.
 - Bảo vệ mối đe dọa web.
 - Bảo vệ mối đe dọa thư điện tử.
 - Phòng chống xâm nhập máy chủ.
- **Cấp độ bảo vệ trung bình.** Chỉ báo nhận giá trị này và chuyển sang màu vàng nếu một trong các thành phần quan trọng bị tắt.
- **Cấp độ bảo vệ thấp.** Chỉ báo nhận giá trị này và chuyển sang màu đỏ trong các trường hợp sau:
 - Một hoặc nhiều thành phần thiết yếu bị tắt.
 - Hai thành phần quan trọng hoặc nhiều hơn bị tắt.

Nếu chỉ báo có giá trị **Cấp độ bảo vệ trung bình** hoặc **Cấp độ bảo vệ thấp** thì một liên kết mở cửa sổ **Các thành phần bảo vệ được khuyến nghị** sẽ xuất hiện bên phải của chỉ báo. Trong cửa sổ này, bạn có thể bật bất kỳ thành phần bảo vệ được khuyến nghị nào.

Quản lý tác vụ

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 nhóm tác vụ được thiết lập cho các máy khách trong các nhóm quản trị.
- Các tác vụ cho một nhóm máy tính.

Bạn có thể tạo số lượng không giới hạn các nhóm tác vụ, tác vụ cho một nhóm máy tính, hoặc tác vụ cục bộ. Để biết thêm chi tiết về làm việc với các nhóm quản trị và chọn máy tính, vui lòng tham khảo [Trợ giúp của Kaspersky Security Center](#).

Kaspersky Endpoint Security hỗ trợ các tác vụ sau:

- **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. Tác vụ *Quét virus* là bắt buộc cho hoạt động của

Kaspersky Endpoint Security và được tạo trong Trình hướng dẫn bắt đầu nhanh. Bạn nên [lên lịch cho tác vụ chạy](#) ít nhất mỗi tuần một lần.

- **[Thêm khóa](#)**. Kaspersky Endpoint Security sẽ thêm một khóa để kích hoạt ứng dụng, bao gồm một khóa bổ sung. Trước khi chạy tác vụ này, hãy đảm bảo số máy tính được thực thi tác vụ không vượt quá số máy tính được giấy phép cho phép.
- **[Change application components](#)**. 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. Thành phần Bảo vệ mỗi đe dọa tập tin không thể bị xóa. Số lượng tối ưu các thành phần Kaspersky Endpoint Security để tiết kiệm tài nguyên máy tính.
- **[Kho](#)**. Kaspersky Endpoint Security sẽ nhận thông tin về tất cả các tập tin thực thi của ứng dụng được lưu trữ trên máy tính. Tác vụ *Kho* được thực hiện bởi thành phần Kiểm soát ứng dụng. Nếu thành phần Kiểm soát ứng dụng không được cài đặt, tác vụ sẽ kết thúc với một lỗi.
- **[Cập nhật](#)**. Kaspersky Endpoint Security sẽ cập nhật các cơ sở dữ liệu và mô-đun ứng dụng. Tác vụ *Cập nhật* là bắt buộc cho hoạt động của Kaspersky Endpoint Security và được tạo trong Trình hướng dẫn bắt đầu nhanh. Bạn nên cấu hình một lịch thực hiện tác vụ ít nhất mỗi lần một ngày.
- **[Xóa sạch dữ liệu](#)**. Kaspersky Endpoint Security sẽ xóa các tập tin và thư mục trên máy tính của người dùng ngay lập tức hoặc nếu không có kết nối với Kaspersky Security Center trong một khoảng thời gian dài.
- **[Hoàn tác bản cập nhật](#)**. Kaspersky Endpoint Security sẽ khôi phục lại bản cập nhật cơ sở dữ liệu và mô-đun ứng dụng gần nhất. Điều này có thể là cần thiết nếu, chẳng hạn, các cơ sở dữ liệu mới chứa dữ liệu không chính xác có thể khiến Kaspersky Endpoint Security chặn một ứng dụng an toàn.
- **[Kiểm tra tính toàn vẹn](#)**. Kaspersky Endpoint Security sẽ phân tích các tập tin ứng dụng, kiểm tra tập tin hỏng hoặc bị sửa đổi và xác minh chữ ký số của các tập tin ứng dụng.
- **[Quản lý tài khoản Authentication Agent](#)**. Kaspersky Endpoint Security sẽ cấu hình thiết lập tài khoản Authentication Agent. Cần phải có một Authentication Agent để làm việc với các ổ đĩa được mã hóa. Trước khi hệ điều hành được nạp, người dùng cần hoàn thành xác thực với Agent.

Các tác vụ chỉ được thực hiện trên máy tính nếu [Kaspersky Endpoint Security đang chạy](#).

Thêm một tác vụ mới

[Cách tạo tác vụ trong Bảng điều khiển quản trị \(MMC\)](#)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Chọn thư mục **Tác vụ** trong cây Bảng điều khiển quản trị.
3. Nhấn nút **New task**.
Trình hướng dẫn Tác vụ sẽ được bắt đầu.
4. Làm theo chỉ dẫn của Trình hướng dẫn Tác vụ.

[Cách tạo tác vụ trong Bảng điều khiển web và Bảng điều khiển đám mây](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.
Danh sách tác vụ sẽ mở.
2. Nhấn vào nút **Thêm**.
Trình hướng dẫn Tác vụ sẽ được bắt đầu.
3. Cấu hình các thiết lập của tác vụ:
 - a. Trong danh sách thả xuống **Ứng dụng**, hãy chọn **Kaspersky Endpoint Security cho Windows (11.9.0)**.
 - b. Trong danh sách thả xuống **Loại tác vụ**, chọn tác vụ mà bạn muốn chạy trên máy tính của người dùng.
 - c. Trong trường **Task name**, hãy nhập một mô tả ngắn.
 - d. Trong phần **Select devices to which the task will be assigned**, chọn phạm vi tác vụ.
4. Chọn các thiết bị theo phạm vi tác vụ được chọn. Chuyển sang bước tiếp theo.
5. Thoát Trình hướng dẫn.

Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ. Tác vụ này sẽ có các thiết lập mặc định. Để cấu hình thiết lập tác vụ, bạn cần vào mục thuộc tính của tác vụ. Để thực hiện một tác vụ, bạn cần chọn hộp kiểm cạnh tác vụ đó và nhấn nút **Bắt đầu**. Sau khi tác vụ đã khởi chạy, bạn có thể tạm dừng tác vụ và tiếp tục lại sau.

Trong danh sách tác vụ, bạn có thể giám sát kết quả tác vụ, bao gồm trạng thái của tác vụ và số liệu thống kê đối với hiệu năng của tác vụ trên máy tính. Bạn cũng có thể tạo một nhóm các sự kiện để giám sát việc hoàn tất các tác vụ (**Monitoring and reporting** → **Event selections**). Để biết thêm chi tiết về việc lựa chọn sự kiện, hãy tham khảo [Trợ giúp Kaspersky Security Center](#). Kết quả thực thi tác vụ cũng được lưu cục bộ trong nhật ký sự kiện của Windows và trong [báo cáo của Kaspersky Endpoint Security](#).

Kiểm soát truy cập tác vụ

Quyền truy cập vào 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 Kaspersky Security Center, thông qua thiết lập 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 Kaspersky Security Center. Để biết thêm chi tiết về việc quản lý tác vụ thông qua Kaspersky Security Center, vui lòng tham khảo [Trợ giúp của Kaspersky Security Center](#).

Bạn có thể cấu hình quyền của người dùng để truy cập các tác vụ bằng chính sách (*chế độ quản lý tác vụ*). Ví dụ: bạn có thể ẩn các tác vụ nhóm trong giao diện Kaspersky Endpoint Security.

[Cách cấu hình chế độ quản lý tác vụ trong giao diện Kaspersky Endpoint Security thông qua Bảng điều khiển quản trị \(MMC\)](#)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Tác vụ cục bộ** → **Quản lý tác vụ**.
6. Cấu hình chế độ quản lý tác vụ (xem bảng bên dưới).
7. Lưu các thay đổi của bạn.

Cách cấu hình chế độ quản lý tác vụ trong giao diện Kaspersky Endpoint Security thông qua Bảng điều khiển web


1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Tác vụ cục bộ** → **Quản lý tác vụ**.
5. Cấu hình chế độ quản lý tác vụ (xem bảng bên dưới).
6. Lưu các thay đổi của bạn.

Cấu hình Quản lý tác vụ

Tham số	Mô tả
Cho phép sử dụng tác vụ nội bộ	<p>Nếu hộp kiểm này được chọn, các tác vụ cục bộ sẽ được hiển thị trong giao diện cục bộ của Kaspersky Endpoint Security. Khi không có hạn chế chính sách nào khác, người dùng có thể thiết lập và chạy các tác vụ. Tuy nhiên, người dùng đó vẫn không thể cấu hình lịch chạy tác vụ. Người dùng chỉ có thể chạy tác vụ theo cách thủ công.</p> <p>Nếu hộp kiểm này bị xóa, việc sử dụng các tác vụ cục bộ sẽ bị dừng lại. Trong chế độ này, các tác vụ cục bộ sẽ không được chạy theo lịch. Các tác vụ không thể được khởi động hoặc thiết lập trong giao diện cục bộ của Kaspersky Endpoint Security, hoặc khi làm việc với dòng lệnh.</p> <p>Một người dùng vẫn có thể khởi động một tác vụ quét virus cho một tập tin hoặc thư mục bằng cách chọn mục Quét virus trong menu ngữ cảnh của tập tin hoặc thư mục đó. Tác vụ quét sẽ được khởi động với các giá trị cấu hình mặc định cho tác vụ quét tùy chỉnh.</p>
Cho phép các tác vụ nhóm	<p>Nếu hộp kiểm này được chọn, các tác vụ nhóm sẽ được hiển thị trong giao diện cục bộ của Kaspersky Endpoint Security. Người dùng có thể xem danh sách tất cả các tác vụ trong giao diện của ứng dụng.</p>

được hiển thị	Khi hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ hiển thị một danh sách tác vụ trống.
Cho phép quản lý tác vụ nhóm	<p>Nếu hộp kiểm được chọn, người dùng có thể khởi chạy và dừng các tác vụ nhóm được chỉ định trong Kaspersky Security Center. Người dùng có thể khởi chạy và dừng các tác vụ trong giao diện ứng dụng hoặc trong giao diện ứng dụng giảm lược.</p> <p>Nếu hộp kiểm bị xóa, Kaspersky Endpoint Security sẽ tự động khởi chạy các tác vụ theo lịch hoặc quản trị viên khởi chạy các tác vụ một cách thủ công trong Kaspersky Security Center.</p>

Cấu hình các thiết lập cục bộ của ứng dụng

Trong Kaspersky Security Center, bạn có thể cấu hình thiết lập Kaspersky Endpoint Security trên một máy tính cụ thể. Chúng là các *thiết lập cục bộ của ứng dụng*. Bạn có thể không truy cập được một số thiết lập để chỉnh sửa. Các thiết lập này bị chặn bởi  thuộc tính trong [thuộc tính của chính sách](#).

[Cách cấu hình thiết lập ứng dụng cục bộ trong Bảng điều khiển quản trị.\(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
 2. Trong thư mục **Managed devices** 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 **Devices**.
 4. Chọn máy tính mà bạn muốn thiết lập cấu hình Kaspersky Endpoint Security.
 5. Trong menu ngữ cảnh của máy khách, chọn **Properties**.
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.
 8. Nhấn nút **Thuộc tính** ở dưới danh sách các ứng dụng Kaspersky.
Thao tác này sẽ mở ra cửa sổ **Kaspersky Endpoint Security for Windows application settings**.
 9. Trong mục **Thiết lập tổng quát**, hãy cấu hình Kaspersky Endpoint Security cũng như Các báo cáo và lưu trữ.
Các mục khác của cửa sổ **Kaspersky Endpoint Security for Windows application settings** đều là các mục tiêu chuẩn dành cho Kaspersky Security Center. Một mô tả về những mục này cũng được cung cấp trong Trợ giúp Kaspersky Security Center.
- Nếu một ứng dụng phải tuân thủ một chính sách cấm các thay đổi đến những thiết lập cụ thể, bạn sẽ không thể sửa chúng trong khi cấu hình thiết lập ứng dụng trong mục **Thiết lập tổng quát**.
10. Lưu các thay đổi của bạn.

[Cách cấu hình thiết lập ứng dụng cục bộ trong Bảng điều khiển web và Bảng điều khiển đám mây](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Managed devices**.
2. Chọn máy tính mà bạn muốn cấu hình thiết lập cục bộ của ứng dụng.
Việc này sẽ mở ra thuộc tính máy tính.
3. Chọn thẻ **Ứng dụng**.
4. Nhấn vào **Kaspersky Endpoint Security cho Windows**.
Việc này sẽ mở ra thiết lập cục bộ của ứng dụng.
5. Chọn thẻ **Application settings**.
6. Cấu hình thiết lập cục bộ của ứng dụng.
7. Lưu các thay đổi của bạn.

Thiết lập ứng dụng cục bộ cũng giống [thiết lập chính sách](#), ngoại trừ thiết lập mã hóa.

Bắt đầu và dừng Kaspersky Endpoint Security

Sau khi cài đặt Kaspersky Endpoint Security lên máy tính của một người dùng, ứng dụng sẽ tự động được cài đặt. Ở chế độ mặc định, Kaspersky Endpoint Security sẽ tự động bắt đầu sau khi khởi động hệ điều hành. Không thể cấu hình tự động khởi động ứng dụng trong thiết lập của 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 mất đến hai phút tùy thuộc vào công năng máy tính. Trong thời gian này, cấp độ bảo vệ máy tính sẽ bị giảm sút. Việc tải về cơ sở dữ liệu diệt virus khi Kaspersky Endpoint Security được chạy trên một hệ điều hành đã được khởi động sẽ không gây suy giảm cấp độ bảo vệ máy tính.


[Cách cấu hình khởi động Kaspersky Endpoint Security trong Bảng điều khiển quản trị \(MMC\)](#)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Thiết lập ứng dụng**.
6. Sử dụng hộp kiểm **Bắt đầu Kaspersky Endpoint Security cho Windows khi khởi động máy tính** để cấu hình việc khởi chạy ứng dụng.
7. Lưu các thay đổi của bạn.

Cách cấu hình khởi động Kaspersky Endpoint Security trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Thiết lập tổng quát** → **Thiết lập ứng dụng**.
5. Sử dụng hộp kiểm **Khởi chạy Kaspersky Endpoint Security khi máy tính khởi động (khuyến dùng)** để cấu hình khởi chạy ứng dụng.
6. Lưu các thay đổi của bạn.



Cách cấu hình khởi động Kaspersky Endpoint Security trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Thiết lập ứng dụng**.
3. Sử dụng hộp kiểm **Bắt đầu Kaspersky Endpoint Security cho Windows khi khởi động máy tính** để cấu hình việc khởi chạy ứng dụng.
4. Lưu các thay đổi của bạn.

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.

Bạn có thể theo dõi trạng thái ứng dụng bằng cách sử dụng tiện ích **Protection status**.

Cách khởi chạy hoặc dừng Kaspersky Endpoint Security trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Devices**.
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 **Properties**.
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.
8. Làm các bước sau:
 - Để khởi chạy ứng dụng, hãy nhấn nút  ở bên phải danh sách các ứng dụng Kaspersky.
 - Để dừng ứng dụng, hãy nhấn nút  ở bên phải danh sách các ứng dụng Kaspersky.

Cách khởi chạy hoặc dừng Kaspersky Endpoint Security trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Managed devices**.
2. Nhấn vào tên của máy tính mà bạn muốn bắt đầu hoặc dừng Kaspersky Endpoint Security trên đó.
Cửa sổ thuộc tính máy tính sẽ được mở ra.
3. Chọn thẻ **Ứng dụng**.
4. Chọn hộp kiểm đối diện **Kaspersky Endpoint Security cho Windows**.
5. Nhấn nút **Bắt đầu** hoặc **Dừng**.

Cách khởi chạy hoặc dừng Kaspersky Endpoint Security từ dòng lệnh

Để dừng ứng dụng từ dòng lệnh, [hãy cho phép quản lý các dịch vụ hệ thống từ bên ngoài](#).



Tập tin klpsm.exe, vốn được bao gồm trong gói phân phối của Kaspersky Endpoint Security được sử dụng để bắt đầu hoặc dừng ứng dụng từ dòng lệnh.

1. Chạy trình thông dịch dòng lệnh (cmd.exe) với tư cách quản trị viên.
2. Tới thư mục chứa tập tin thực thi Kaspersky Endpoint Security.
3. Để khởi chạy ứng dụng từ dòng lệnh, hãy nhập `klpsm.exe start_avp_service`.
4. Để dừng ứng dụng từ dòng lệnh, hãy nhập `klpsm.exe stop_avp_service`.

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 được bật.

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.

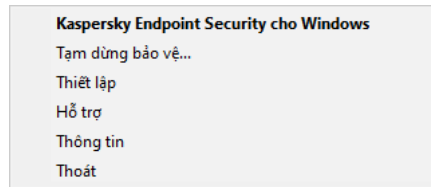
Để tạm ngưng bảo vệ và kiểm soát máy tính:

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, hãy chọn **Tạm dừng bảo vệ** (xem hình bên dưới).
Mục menu ngữ cảnh này khả dụng nếu [Bảo vệ bằng mật khẩu được bật](#).
3. Chọn một trong các tùy chọn sau:
 - **Tạm dừng trong <khoảng thời gian>** – tính năng bảo vệ và kiểm soát máy tính sẽ tiếp tục hoạt động sau khoảng thời gian được chỉ định trong danh sách thả xuống bên dưới.
 - **Tạm dừng cho đến khi ứng dụng khởi động lại** – tính năng bảo vệ và kiểm soát máy tính sẽ tiếp tục hoạt động sau khi bạn khởi động 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 tiếp tục hoạt động khi bạn quyết định bật lại chúng.

4. Nhấn vào **Tạm dừng bảo vệ**.

Kaspersky Endpoint Security sẽ tạm dừng hoạt động của tất cả các thành phần bảo vệ và kiểm soát không được đánh dấu khóa (🔒) trong chính sách. Trước khi thực hiện tác vụ này, chúng tôi khuyến cáo bạn tắt chính sách của Kaspersky Security Center.



Menu ngữ cảnh của biểu tượng ứng dụng

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, hãy chọn **Khôi phục bảo vệ**.

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.

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 thực hiện, bạn phải lưu lại tập tin cấu hình trong cùng thư mục chứa 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. Trong cửa sổ chính của ứng dụng, hãy nhấn nút ⚙️.
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Quản lý thiết lập**.
3. Nhấn vào **Xuất**.
4. Trong cửa sổ mở ra, hãy chỉ định đường dẫn tới nơi mà bạn muốn lưu lại tập tin cấu hình 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. Lưu tập tin.

Để nhập cấu hình của Kaspersky Endpoint Security từ một tập tin thiết lập:


1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Quản lý thiết lập**.
3. Nhấn **Nhập**.
4. Trong cửa sổ mở ra, hãy nhập đường dẫn đến tập tin cấu hình.
5. Mở tập tin.

Tất cả giá trị của cấu hình Kaspersky Endpoint Security sẽ được đặt theo tập tin thiết lập được chọn.

Khôi phục các thiết lập mặc định của ứng dụng

Bạn có thể khôi phục các thiết lập mặc định theo khuyến nghị của Kaspersky cho Endpoint Security bất kỳ thời điểm nào. Khi thiết lập được khôi phục, mức độ bảo mật **Khuyến dùng** được thiết lập cho tất cả các thành phần bảo vệ.

Để khôi phục các thiết lập mặc định của ứng dụng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Quản lý thiết lập**.
3. Nhấn vào **Khôi phục**.
4. Lưu các thay đổi của bạn.

Quét virus của 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.

Kaspersky Endpoint Security không quét các tập tin có nội dung có trong ổ lưu trữ đám mây OneDrive và sẽ tạo các mục nhật ký cho biết các tập tin này chưa được quét.

Quét toàn bộ

Quét kỹ lưỡng toàn bộ máy tính. Kaspersky Endpoint Security sẽ quét các đối tượng sau:

- Bộ nhớ kernel
- Các đối tượng được nạp lúc khởi động hệ điều hành
- Sector khởi động
- Bản sao lưu hệ điều hành
- Toàn bộ ổ cứng và ổ đĩa di động

Các chuyên gia của Kaspersky khuyên bạn không nên thay đổi phạm vi quét của tác vụ *Quét toàn bộ*.

Để tiết kiệm tài nguyên máy tính, bạn nên sử dụng một [tác vụ quét trong nền](#) thay cho tác vụ quét toàn bộ. Việc này sẽ không ảnh hưởng đến mức độ bảo mật của máy tính.

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.

Các chuyên gia của Kaspersky khuyên bạn không nên thay đổi phạm vi quét của tác vụ *Quét khu vực quan trọng*.

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 hệ thống
- Các đối tượng được nạp lúc khởi động hệ điều hành
- Bản sao lưu hệ điều hành

- Hộp thư Microsoft Outlook
- Ổ đĩa cứng, ổ đĩa di động và ổ đĩa mạng
- Bất kỳ tập tin nào được lựa chọn

Quét trong nền

Quét trong nền là một chế độ quét của Kaspersky Endpoint Security không hiển thị thông báo cho người dùng. Quét trong nền yêu cầu ít tài nguyên máy tính hơn các loại quét khác (ví dụ như quét toàn bộ). Trong chế độ này, Kaspersky Endpoint Security sẽ quét các đối tượng khởi động, sector khởi động, bộ nhớ hệ thống và phân vùng hệ thống.

Kiểm tra tính toàn vẹn

Kaspersky Endpoint Security sẽ kiểm tra các mô-đun ứng dụng để phát hiện hư hỏng hoặc sửa đổi.

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. Thành phần này giúp bảo vệ máy tính với sự trợ giúp của cơ sở dữ liệu diệt virus, [dịch vụ đám mây của Kaspersky Security Network](#) và phân tích theo hành vi.

Kaspersky Endpoint Security có các tác vụ tiêu chuẩn *Quét toàn bộ*, *Quét khu vực quan trọng*, *Quét tùy chỉnh* được định nghĩa sẵn. Nếu tổ chức của bạn đã triển khai hệ thống quản trị Kaspersky Security Center, bạn có thể [tạo một tác vụ Quét virus](#) và cấu hình tác vụ quét. [Tác vụ Quét trong nền](#) cũng có sẵn trong Kaspersky Security Center. Không thể cấu hình tác vụ quét trong nền.

[Cách chạy tác vụ Quét virus trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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, hãy chọn thẻ **Tác vụ**.
4. Chọn một tác vụ quét và nhấn đúp để mở các thuộc tính tác vụ.
Nếu cần, [hãy tạo một tác vụ Quét virus](#).
5. Trong cửa sổ thuộc tính tác vụ, hãy chọn mục **Thiết lập**.
6. Cấu hình tác vụ quét (xem bảng bên dưới).
Nếu cần, [hãy cấu hình lịch tác vụ quét](#).
7. Lưu các thay đổi của bạn.
8. Chạy tác vụ quét.


Kaspersky Endpoint Security sẽ bắt đầu quét máy tính. Nếu người dùng đã làm gián đoạn quá trình thực thi tác vụ (ví dụ: bằng cách tắt nguồn máy tính), Kaspersky Endpoint Security sẽ tự động chạy tác vụ, tiếp tục từ thời điểm tác vụ quét bị gián đoạn.

Cách chạy Quét virus trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.
Danh sách tác vụ sẽ mở.
2. Nhấn vào tác vụ quét.
Cửa sổ thuộc tính tác vụ sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Cấu hình tác vụ quét (xem bảng bên dưới).
Nếu cần, [hãy cấu hình lịch tác vụ quét](#).
5. Lưu các thay đổi của bạn.
6. Chạy tác vụ quét.

Kaspersky Endpoint Security sẽ bắt đầu quét máy tính. Nếu người dùng đã làm gián đoạn quá trình thực thi tác vụ (ví dụ: bằng cách tắt nguồn máy tính), Kaspersky Endpoint Security sẽ tự động chạy tác vụ, tiếp tục từ thời điểm tác vụ quét bị gián đoạn.

Cách chạy Quét virus trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn vào mục **Tác vụ**.
2. Trong danh sách tác vụ, hãy chọn tác vụ quét và nhấn vào .
3. Cấu hình tác vụ quét (xem bảng bên dưới).
Nếu cần, [hãy cấu hình lịch tác vụ quét](#).
4. Lưu các thay đổi của bạn.
5. Chạy tác vụ quét.

Kaspersky Endpoint Security sẽ bắt đầu quét máy tính. Ứng dụng sẽ hiển thị tiến độ quét, số lượng tập tin đã quét và thời gian quét còn lại. Bạn có thể dừng tác vụ bất kỳ lúc nào bằng cách nhấn nút **Dừng**. Nếu tác vụ quét không được hiển thị, điều đó có nghĩa là quản trị viên [đã cấm sử dụng các tác vụ cục bộ trong chính sách](#).

Cấu hình quét

Tham số	Mô tả
Mức độ bảo mật	<p>Kaspersky Endpoint Security có thể sử dụng các nhóm thiết lập khác nhau để chạy tác vụ quét. Các nhóm thiết lập được lưu trữ trong ứng dụng được gọi là <i>mức độ bảo mật</i>:</p> <ul style="list-style-type: none"> • Cao. Kaspersky Endpoint Security sẽ quét tất cả các loại tập tin. Khi quét các tập tin hỗn hợp, Kaspersky Endpoint Security cũng quét tập tin định dạng thư. • Khuyến dùng. Kaspersky Endpoint Security sẽ chỉ quét các định dạng tập tin được quy định trên tất cả các ổ cứng, ổ đĩa mạng và ổ di động của máy tính, và cả các đối tượng OLE nhúng. Kaspersky Endpoint Security không quét các tập nén hay gói cài đặt. • Thấp. Kaspersky Endpoint Security sẽ chỉ quét các tập tin mới hoặc được sửa đổi với các phần mở rộng cụ thể trên tất cả các ổ cứng, ổ đĩa di động và ổ đĩa mạng của máy tính. Kaspersky Endpoint Security không quét các tập tin hỗn hợp. <p>Bạn có thể chọn một trong các mức độ bảo mật được thiết lập sẵn hoặc tự cấu hình thiết lập mức độ bảo mật. Nếu bạn đã thay đổi thiết lập mức độ bảo mật, bạn luôn có thể quay lại thiết lập mức độ bảo mật được khuyến nghị.</p>
Hành động khi phát hiện mối đe dọa	<p>Khử mã độc; xóa nếu không thể khử mã độc. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ tự động khử nhiễm tất cả các tập tin bị nhiễm virus được phát hiện. Nếu việc khử nhiễm thất bại, Kaspersky Endpoint Security sẽ xóa các tập tin đó.</p> <p>Khử mã độc; chặn nếu không thể khử mã độc. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ tự động khử nhiễm tất cả các tập tin bị nhiễm virus được phát hiện. Nếu không thể khử mã độc, Kaspersky Endpoint Security sẽ bổ sung thông tin về tập tin nhiễm mã độc được phát hiện vào danh sách các mối đe dọa đang hoạt động.</p> <p>Thông báo. Nếu tùy chọn này được sử dụng, Kaspersky Endpoint Security sẽ bổ sung thông tin về tập tin nhiễm mã độc vào danh sách các mối đe dọa đang hoạt động khi phát hiện những tập tin này.</p>

	<p>Trước khi cố gắng khử mã độc hoặc xóa một tập tin bị nhiễm, Kaspersky Endpoint Security sẽ tạo một bản sao lưu của tập tin trong trường hợp bạn cần khôi phục tập tin hoặc nếu nó có thể khử mã độc tập tin trong tương lai.</p> <p>Khi phát hiện các tập tin nhiễm mã độc là một phần của ứng dụng Windows Store, Kaspersky Endpoint Security sẽ cố xóa tập tin đó.</p>
<p>Chạy khử mã độc nâng cao ngay lập tức</p> <p><i>(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)</i></p>	<p>Khử mã độc nâng cao trong một tác vụ quét virus trên máy tính chỉ được thực hiện nếu tính năng Khử mã độc nâng cao được bật trong thuộc tính của chính sách được áp dụng cho máy tính này.</p> <p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ lập tức khử mã độc lây nhiễm đang hoạt động sau khi nó được phát hiện trong quá trình thực thi tác vụ quét virus. Sau khi khử mã độc hoạt động lây nhiễm đang hoạt động, Kaspersky Endpoint Security sẽ khởi động lại máy tính mà không cần nhắc người dùng.</p> <p>Nếu hộp này kiểm bị xóa, Kaspersky Endpoint Security sẽ không lập tức khử mã độc hoạt động lây nhiễm đang hoạt động sau khi nó được phát hiện trong quá trình thực thi tác vụ quét. Kaspersky Endpoint Security sẽ tạo các sự kiện hoạt động lây nhiễm đang hoạt động trong báo cáo của ứng dụng cục bộ và ở phía Kaspersky Security Center. Hoạt động lây nhiễm đang hoạt động có thể được khử mã độc khi tác vụ quét virus được chạy lại và tính năng Khử mã độc nâng cao được bật. Bằng cách này, quản trị viên hệ thống có thể chọn thời gian thích hợp để thực hiện Khử mã độc nâng cao và sau đó tự động khởi động lại máy tính.</p>
<p>Phạm vi quét</p>	<p>Danh sách các đối tượng được Kaspersky Endpoint Security quét khi thực hiện một tác vụ quét. Các đối tượng trong phạm vi quét có thể bao gồm bộ nhớ kernel, các tiến trình đang chạy, phân vùng khởi động, ổ lưu trữ sao lưu hệ thống, cơ sở dữ liệu email, ổ đĩa cứng, ổ đĩa di động hoặc ổ đĩa mạng, tập tin hoặc thư mục.</p>
<p>Lịch quét</p>	<p>Thủ công. Chế độ chạy trong đó bạn có thể tiến hành quét thủ công tại một thời điểm thuận tiện cho bạn.</p> <p>Theo lịch. Trong chế độ chạy tác vụ quét này, Kaspersky Endpoint Security sẽ chạy tác vụ quét theo lịch mà bạn đã quy định. Nếu chế độ chạy tác vụ quét này được chọn, bạn cũng có thể khởi động tác vụ quét một cách thủ công.</p>
<p>Trì hoãn chạy sau khi ứng dụng khởi động N phút</p>	<p>Hoãn bắt đầu tác vụ quét sau khi ứng dụng khởi động. Khi khởi động hệ điều hành, nhiều tiến trình đang chạy, do đó sẽ có lợi nếu bạn hoãn chạy tác vụ quét thay vì chạy quét ngay sau khi khởi động Kaspersky Endpoint Security.</p>
<p>Chạy các tác vụ bị bỏ qua</p>	<p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ bắt đầu lại tác vụ quét bị bỏ qua ngay khi có thể. Có thể bỏ qua tác vụ quét, ví dụ như nếu máy tính bị tắt vào thời điểm bắt đầu tác vụ quét được lên lịch. Khi hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ không chạy các tác vụ quét bị bỏ qua. Thay vào đó, ứng dụng sẽ chạy tác vụ quét kế tiếp dựa theo lịch hiện tại.</p>
<p>Chỉ chạy khi máy tính đang rảnh</p>	<p>Hoãn bắt đầu tác vụ quét khi tài nguyên máy tính đang bận. Kaspersky Endpoint Security sẽ bắt đầu tác vụ quét nếu máy tính bị khóa hoặc nếu trình bảo vệ màn hình được bật. Nếu bạn đã làm gián đoạn việc thực thi tác vụ, chẳng hạn như bằng cách mở khóa máy tính, Kaspersky Endpoint Security sẽ tự động chạy tác vụ, tiếp tục từ thời điểm tác vụ bị gián đoạn.</p>

Chạy quét dưới quyền	<p>Theo mặc định, tác vụ quét được chạy dưới tên của người dùng có quyền mà bạn được đăng ký trong hệ điều hành. Phạm vi bảo vệ có thể bao gồm các ổ đĩa mạng hoặc các đối tượng khác yêu cầu quyền truy cập đặc biệt. Bạn có thể chỉ định một người dùng có quyền theo yêu cầu trong thiết lập Kaspersky Endpoint Security và chạy tác vụ quét bằng tài khoản của người dùng này.</p>
Loại tập tin	<div style="border: 1px solid #ccc; padding: 10px; margin-bottom: 10px;"> <p>Kaspersky Endpoint Security coi các tập tin không có phần mở rộng là các tập tin có thể được thực thi. Kaspersky Endpoint Security sẽ luôn quét các tập tin thực thi bất kể kiểu tập tin mà bạn đã lựa chọn để quét.</p> </div> <p>Tất cả tập tin. Nếu thiết lập này được bật, Kaspersky Endpoint Security sẽ kiểm tra tất cả các tập tin và không có ngoại lệ (tất cả định dạng và phần mở rộng).</p> <p>Quét các tập tin theo định dạng. Nếu thiết lập này được bật, Kaspersky Endpoint Security sẽ chỉ quét các tập tin có thể bị nhiễm virus. Trước khi quét một tập tin để tìm mã độc, đầu đề nội bộ của tập tin sẽ được phân tích để xác định định dạng của tập tin đó (ví dụ, .txt, .doc, hoặc .exe). Tác vụ quét cũng tìm kiếm các tập tin có đuôi mở rộng tập tin cụ thể.</p> <p>Quét các tập tin theo phần mở rộng. Nếu thiết lập này được bật, Kaspersky Endpoint Security sẽ chỉ quét các tập tin có thể bị nhiễm virus. Sau đó, định dạng tập tin sẽ được xác định dựa trên phần mở rộng của tập tin.</p> <p>Theo mặc định, Kaspersky Endpoint Security sẽ quét các tập tin theo định dạng của chúng. Quét tập tin theo phần mở rộng kém an toàn hơn vì tập tin độc hại có thể có phần mở rộng không nằm trong danh sách có khả năng lây nhiễm (ví dụ: .123).</p>
Chỉ quét các tập tin mới và bị thay đổi	<p>Chỉ quét các tập tin mới và được thay đổi kể từ lần cuối cùng chúng được quét. Điều này giảm thời lượng của một lần quét. Chế độ này được áp dụng cho cả các tập tin đơn và tập tin hỗn hợp.</p>
Bỏ qua các đối tượng với thời gian quét cao hơn N giây	<p>Thao tác này đặt giới hạn thời gian để quét một đối tượng duy nhất. Sau một khoảng thời gian được quy định, Kaspersky Endpoint Security sẽ ngừng quét một tập tin. Điều này giảm thời lượng của một lần quét.</p>
Quét tập tin nén	<p>Quét định dạng ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE, và các định dạng tập tin nén khác. Kaspersky Endpoint Security quét các tập tin nén không chỉ theo phần mở rộng mà còn theo định dạng. Khi kiểm tra tập tin nén, ứng dụng sẽ thực hiện quy trình giải nén đệ quy. Điều này cho phép phát hiện các mối đe dọa bên trong tập tin nén nhiều cấp (tập tin nén bên trong tập tin nén).</p>
Quét các gói phân phối	<p>Hộp kiểm này bật/tắt tính năng quét các gói phân phối thuộc bên thứ ba.</p>
Quét các tập tin có định dạng Microsoft Office	<p>Quét các tập tin Microsoft Office (DOC, DOCX, XLS, PPT và đuôi mở rộng khác của Microsoft). Các tập tin định dạng Office cũng bao gồm các đối tượng OLE.</p>
Quét định dạng email	<p>Quét các tập tin định dạng email và cơ sở dữ liệu email. Ứng dụng sẽ quét các tập tin PST và OST được sử dụng bởi các trình quản lý thư MS Outlook và Windows</p>

	<p>Mail/Outlook Express cũng như các tập tin EML.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Kaspersky Endpoint Security không hỗ trợ phiên bản 64 bit của ứng dụng email MS Outlook. Điều này có nghĩa là Kaspersky Endpoint Security sẽ không quét các tập tin MS Outlook (tập tin PST và OST) nếu phiên bản 64 bit của MS Outlook được cài đặt trên máy tính, ngay cả khi bạn thêm thư vào trong phạm vi quét.</p> </div> <p>Nếu hộp kiểm được chọn, Kaspersky Endpoint Security sẽ chia nhỏ tập tin định dạng email thành các cấu phần (đầu đề, thân, tập tin đính kèm) và quét chúng để tìm mối đe dọa.</p> <p>Nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ quét tập tin định dạng email như một tập tin duy nhất.</p>
<p>Quét tập tin nén có mật khẩu bảo vệ</p>	<p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ quét các tập nén có mật khẩu bảo vệ. Trước khi các tập tin trong một tập nén có thể được quét, bạn sẽ được nhắc nhập mật khẩu.</p> <p>Nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ bỏ qua việc quét các tập nén có mật khẩu bảo vệ.</p>
<p>Không giải nén các tập tin phức hợp lớn</p>	<p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ không quét các tập tin hỗn hợp nếu dung lượng của chúng vượt quá giá trị được quy định.</p> <p>Nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ quét các tập tin hỗn hợp thuộc mọi kích cỡ.</p> <p>Kaspersky Endpoint Security sẽ quét các tập tin lớn được trích xuất từ tập tin nén bất kể hộp kiểm này có được chọn hay không.</p>
<p>Công nghệ máy học và phân tích dấu hiệu</p>	<p>Phương thức máy học và phân tích dấu hiệu sử dụng cơ sở dữ liệu Kaspersky Endpoint Security chứa mô tả về các mối đe dọa đã biết và các cách để vô hiệu chúng. Tính năng bảo vệ sử dụng phương thức này cho mức độ bảo mật tối thiểu được chấp nhận.</p> <p>Dựa trên khuyến nghị của các chuyên gia Kaspersky, máy học và phân tích dấu hiệu luôn được bật.</p>
<p>Phân tích hành vi</p>	<p>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.</p> <p>Khi quét các tập tin để tìm mã độc, trình phân tích theo hành vi sẽ thực thi các lệnh trong các tập tin thực thi. Số lượng các lệnh được thực thi bởi trình phân tích theo hành vi phụ thuộc vào cấp độ được chỉ định cho trình phân tích theo hành vi. Cấp độ Phân tích hành vi đảm bảo một sự cân bằng giữa việc quét kỹ lưỡng để tìm các mối đe dọa mới, tải lên tài nguyên hệ điều hành, và thời gian phân tích theo hành vi.</p>
<p>Công nghệ iSwift</p>	<p>Công nghệ này cho phép tăng tốc độ quét bằng cách loại trừ một số tập tin nhất định khỏi quá trình quét. Các tập tin được loại trừ khỏi quá trình quét bằng một thuật toán đặc biệt có tính đến ngày phát hành cơ sở dữ liệu Kaspersky Endpoint Security, ngày mà tập tin được quét lần cuối cùng và mọi thay đổi được thực hiện với thiết lập quét. Công nghệ iSwift được cải tiến từ công nghệ iChecker cho hệ thống tập tin NTFS.</p>

<p>(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)</p>	
<p>Công nghệ iChecker</p> <p>(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)</p>	<p>Công nghệ này cho phép tăng tốc độ quét bằng cách loại trừ một số tập tin nhất định khỏi quá trình quét. Các tập tin được loại trừ khỏi quá trình quét bằng một thuật toán đặc biệt có tính đến ngày phát hành cơ sở dữ liệu Kaspersky Endpoint Security, ngày khi tập tin được quét lần cuối cùng và mọi thay đổi được thực hiện với thiết lập quét. Công nghệ iChecker có một số hạn chế: công nghệ này không hoạt động với tập tin lớn và chỉ áp dụng cho các tập tin có cấu trúc mà ứng dụng nhận dạng được (ví dụ như EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP và RAR).</p>

Quét ổ đĩa di động khi chúng được kết nối với máy tính

Kaspersky Endpoint Security sẽ quét tất cả các tập tin mà bạn chạy hoặc sao chép, ngay cả khi tập tin có trên ổ đĩa di động (thành phần Bảo vệ mỗi đe dọa tập tin). Để ngăn phát tán virus và các phần mềm độc hại khác, bạn có thể cấu hình các tác vụ quét tự động ổ đĩa di động khi chúng được kết nối với máy tính. Kaspersky Endpoint Security sẽ tự động cố gắng khử mã độc tất cả các tập tin bị nhiễm mã độc được phát hiện. Nếu việc khử nhiễm thất bại, Kaspersky Endpoint Security sẽ xóa các tập tin đó. Thành phần này sẽ bảo đảm bảo mật cho máy tính bằng cách chạy các tác vụ quét sử dụng công nghệ máy học, phân tích hành vi (cấp độ cao) và phân tích dấu hiệu. Kaspersky Endpoint Security cũng sử dụng công nghệ iSwift và iChecker để tối ưu quá trình quét. Các công nghệ này luôn được bật và bạn không thể tắt.


[Cấu hình chạy Quét ổ đĩa di động trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Tác vụ cục bộ** → **Quét ổ đĩa di động**.
6. Trong danh sách thả xuống **Hành động khi ổ đĩa di động được kết nối**, hãy chọn **Quét chi tiết** hoặc **Quét nhanh**.
7. Cấu hình các tùy chọn nâng cao cho Quét ổ đĩa di động (xem bảng bên dưới).
8. Lưu các thay đổi của bạn.

Cách cấu hình chạy Quét ổ đĩa di động trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Tác vụ cục bộ** → **Quét ổ đĩa di động**.
5. Trong danh sách thả xuống **Hành động khi ổ đĩa di động được kết nối**, hãy chọn **Quét chi tiết** hoặc **Quét nhanh**.
6. Cấu hình các tùy chọn nâng cao cho Quét ổ đĩa di động (xem bảng bên dưới).
7. Lưu các thay đổi của bạn.

Cách cấu hình chạy Quét ổ đĩa di động trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn vào mục **Tác vụ**.
2. Trong danh sách tác vụ, hãy chọn tác vụ quét và nhấn vào .
3. Sử dụng nút bật/tắt **Quét ổ đĩa di động** để bật hoặc tắt tính năng quét ổ đĩa di động khi kết nối với máy tính.
4. Cấu hình các tùy chọn nâng cao cho Quét ổ đĩa di động (xem bảng bên dưới).
5. Lưu các thay đổi của bạn.

Do đó, Kaspersky Endpoint Security sẽ chạy Quét ổ đĩa di động để tìm các ổ đĩa di động không lớn hơn dung lượng tối đa được chỉ định. Nếu tác vụ *Quét ổ đĩa di động* không được hiển thị, điều đó có nghĩa là quản trị viên [đã cấm sử dụng các tác vụ cục bộ trong chính sách](#).

Thiết lập tác vụ quét ổ đĩa di động

Tham số	Mô tả
Hành động khi ổ đĩa di động được kết nối	<p>Quét chi tiết. Nếu mục này được chọn, khi ổ đĩa di động được kết nối thì Kaspersky Endpoint Security sẽ quét tất cả các tập tin trên ổ đĩa di động, bao gồm các tập tin được nhúng trong các đối tượng phức hợp, tập tin nén, gói phân phối và tập tin có định dạng văn bản. Kaspersky Endpoint Security không quét các tập tin có định dạng thư hoặc tập tin nén được bảo vệ bằng mật khẩu.</p> <p>Quét nhanh. Nếu đề mục này được chọn, sau khi ổ đĩa di động được kết nối, Kaspersky Endpoint Security sẽ chỉ quét các tập tin có định dạng cụ thể để bị nhiễm virus nhất, và sẽ không giải nén các tập tin hỗn hợp.</p>
Dung lượng tối đa của ổ đĩa di động	<p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ thực hiện hành động được chọn trong danh sách thả xuống Hành động khi ổ đĩa di động được kết nối trên các ổ đĩa di động với kích cỡ không quá kích cỡ ổ đĩa tối đa được quy định.</p> <p>Nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ thực hiện hành động được chọn trong danh sách thả xuống Hành động khi ổ đĩa di động được kết nối trên các ổ đĩa di động thuộc mọi kích cỡ.</p>
Hiện thị tiến độ quét	<p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ hiển thị tiến trình quét ổ đĩa di động trong một cửa sổ riêng và trong mục Tác vụ.</p> <p>Khi hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ thực hiện quét ổ đĩa di động trong nền.</p>
Chặn hành động dừng tác vụ quét	<p>Nếu chọn hộp kiểm này, thì đối với các tác vụ quét ổ đĩa di động trong giao diện cục bộ của Kaspersky Endpoint Security, nút Dừng trong mục Tác vụ và nút Dừng nút trong cửa sổ quét ổ đĩa di động sẽ không khả dụng.</p>

Quét trong nền

Quét trong nền là một chế độ quét của Kaspersky Endpoint Security không hiển thị thông báo cho người dùng. Quét trong nền yêu cầu ít tài nguyên máy tính hơn các loại quét khác (ví dụ như quét toàn bộ). Trong chế độ này, Kaspersky Endpoint Security sẽ quét các đối tượng khởi động, sector khởi động, bộ nhớ hệ thống và phân vùng hệ thống. Một tác vụ quét trong nền được khởi chạy trong các trường hợp sau:

- Sau khi cập nhật cơ sở dữ liệu diệt virus.
- 30 phút sau khi Kaspersky Endpoint Security được khởi động.
- Mỗi 6 tiếng.
- Khi máy tính rảnh từ năm phút trở lên (máy tính bị khóa hoặc trình bảo vệ màn hình đang bật).

Quét trong nền khi máy tính rảnh sẽ bị ngắt khi bất kỳ tình trạng nào sau đây là đúng:

- Máy tính chuyển sang chế độ hoạt động.

Nếu quét trong nền không được chạy trong hơn 10 ngày, việc quét sẽ không bị ngắt quãng.

- Máy tính (máy tính xách tay) đã chuyển sang chế độ chạy pin.

Khi thực hiện tác vụ quét trong nền, Kaspersky Endpoint Security sẽ không quét các tập tin có nội dung nằm trên ổ lưu trữ đám mây OneDrive.


Cách bật quét trong nền trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Tác vụ cục bộ** → **Quét trong nền**.
6. Sử dụng hộp kiểm **Bật quét trong nền** để bật hoặc tắt quét trong nền.
7. Lưu các thay đổi của bạn.

Cách bật quét trong nền trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Tác vụ cục bộ** → **Quét trong nền**.
5. Sử dụng hộp kiểm **Bật quét trong nền** để bật hoặc tắt quét trong nền.
6. Lưu các thay đổi của bạn.

Cách bật quét trong nền trong giao diện ứng dụng

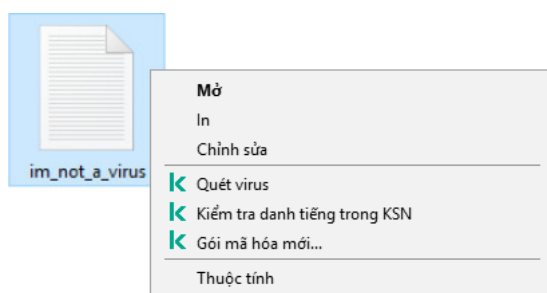
1. Trong cửa sổ chính của ứng dụng, hãy nhấn vào mục **Tác vụ**.
2. Trong danh sách tác vụ, hãy chọn tác vụ quét và nhấn vào .
3. Sử dụng nút bật/tắt **Quét trong nền** để bật hoặc tắt thành phần.
4. Lưu các thay đổi của bạn.

Nếu *Quét trong nền* không được hiển thị, điều đó có nghĩa là quản trị viên [đã cấm sử dụng các tác vụ cục bộ trong chính sách](#).

Quét từ menu ngữ cảnh

Kaspersky Endpoint Security cho phép bạn thực hiện tác vụ quét virus và phần mềm độc hại khác cho từng tập tin thông qua menu ngữ cảnh (xem hình bên dưới).

Khi thực hiện tác vụ quét từ menu ngữ cảnh, Kaspersky Endpoint Security sẽ không quét các tập tin có nội dung nằm trên ổ lưu trữ đám mây OneDrive.



Quét từ menu ngữ cảnh


Cách cấu hình Quét từ Menu ngữ cảnh trong Bảng điều khiển Quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Tác vụ cục bộ** → **Quét từ Menu ngữ cảnh**.
6. Cấu hình Quét từ Menu ngữ cảnh (xem bảng bên dưới).
7. Lưu các thay đổi của bạn.

Cách cấu hình Quét từ Menu ngữ cảnh trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Tác vụ cục bộ** → **Quét từ Menu ngữ cảnh**.
5. Cấu hình Quét từ Menu ngữ cảnh (xem bảng bên dưới).
6. Lưu các thay đổi của bạn.

Cách cấu hình Quét từ Menu ngữ cảnh trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn vào mục **Tác vụ**.
2. Trong danh sách tác vụ, hãy chọn tác vụ quét và nhấn vào .
3. Cấu hình Quét từ Menu ngữ cảnh (xem bảng bên dưới).
4. Lưu các thay đổi của bạn.

Nếu tác vụ *Quét từ Menu ngữ cảnh* không được hiển thị, điều đó có nghĩa là quản trị viên [đã cấm sử dụng các tác vụ cục bộ trong chính sách](#).

Cấu hình tác vụ Quét từ menu ngữ cảnh

Tham số	Mô tả
Mức độ bảo mật	Kaspersky Endpoint Security có thể sử dụng các nhóm thiết lập khác nhau để chạy tác vụ quét. Các nhóm thiết lập được lưu trữ trong ứng dụng được gọi là <i>mức độ bảo mật</i> .

	<ul style="list-style-type: none"> • Cao. Kaspersky Endpoint Security sẽ quét tất cả các loại tập tin. Khi quét các tập tin hỗn hợp, Kaspersky Endpoint Security cũng quét tập tin định dạng thư. • Khuyến dùng. Kaspersky Endpoint Security sẽ chỉ quét các định dạng tập tin được quy định trên tất cả các ổ cứng, ổ đĩa mạng và ổ di động của máy tính, và cả các đối tượng OLE nhúng. Kaspersky Endpoint Security không quét các tập nén hay gói cài đặt. • Thấp. Kaspersky Endpoint Security sẽ chỉ quét các tập tin mới hoặc được sửa đổi với các phần mở rộng cụ thể trên tất cả các ổ cứng, ổ đĩa di động và ổ đĩa mạng của máy tính. Kaspersky Endpoint Security không quét các tập tin hỗn hợp.
<p>Hành động khi phát hiện mối đe dọa</p>	<p>Khử mã độc; xóa nếu không thể khử mã độc. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ tự động khử nhiễm tất cả các tập tin bị nhiễm virus được phát hiện. Nếu việc khử nhiễm thất bại, Kaspersky Endpoint Security sẽ xóa các tập tin đó.</p> <p>Khử mã độc; chặn nếu không thể khử mã độc. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ tự động khử nhiễm tất cả các tập tin bị nhiễm virus được phát hiện. Nếu không thể khử mã độc, Kaspersky Endpoint Security sẽ bổ sung thông tin về tập tin nhiễm mã độc được phát hiện vào danh sách các mối đe dọa đang hoạt động.</p> <p>Thông báo. Nếu tùy chọn này được sử dụng, Kaspersky Endpoint Security sẽ bổ sung thông tin về tập tin nhiễm mã độc vào danh sách các mối đe dọa đang hoạt động khi phát hiện những tập tin này.</p>
<p>Loại tập tin</p>	<div style="border: 1px solid #ccc; padding: 10px; margin-bottom: 10px;"> <p>Kaspersky Endpoint Security coi các tập tin không có phần mở rộng là các tập tin có thể được thực thi. Kaspersky Endpoint Security sẽ luôn quét các tập tin thực thi bất kể kiểu tập tin mà bạn đã lựa chọn để quét.</p> </div> <p>Tất cả tập tin. Nếu thiết lập này được bật, Kaspersky Endpoint Security sẽ kiểm tra tất cả các tập tin và không có ngoại lệ (tất cả định dạng và phần mở rộng).</p> <p>Quét các tập tin theo định dạng. Nếu thiết lập này được bật, Kaspersky Endpoint Security sẽ chỉ quét các tập tin có thể bị nhiễm virus. Trước khi quét một tập tin để tìm mã độc, đầu đề nội bộ của tập tin sẽ được phân tích để xác định định dạng của tập tin đó (ví dụ, .txt, .doc, hoặc .exe). Tác vụ quét cũng tìm kiếm các tập tin có đuôi mở rộng tập tin cụ thể.</p> <p>Quét các tập tin theo phần mở rộng. Nếu thiết lập này được bật, Kaspersky Endpoint Security sẽ chỉ quét các tập tin có thể bị nhiễm virus. Sau đó, định dạng tập tin sẽ được xác định dựa trên phần mở rộng của tập tin.</p> <p>Theo mặc định, Kaspersky Endpoint Security sẽ quét các tập tin theo định dạng của chúng. Quét tập tin theo phần mở rộng kém an toàn hơn vì tập tin độc hại có thể có phần mở rộng không nằm trong danh sách có khả năng lây nhiễm (ví dụ: .123).</p>
<p>Chỉ quét các tập tin mới và bị thay đổi</p>	<p>Chỉ quét các tập tin mới và được thay đổi kể từ lần cuối cùng chúng được quét. Điều này giảm thời lượng của một lần quét. Chế độ này được áp dụng cho cả các tập tin đơn và tập tin hỗn hợp.</p>
<p>Bỏ qua các đối tượng với thời gian quét</p>	<p>Thao tác này đặt giới hạn thời gian để quét một đối tượng duy nhất. Sau một khoảng thời gian được quy định, Kaspersky Endpoint Security sẽ ngừng quét một tập tin. Điều này giảm thời lượng của một lần quét.</p>

cao hơn N giây	
Quét tập tin nén	Quét định dạng ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE, và các định dạng tập tin nén khác. Kaspersky Endpoint Security quét các tập tin nén không chỉ theo phần mở rộng mà còn theo định dạng. Khi kiểm tra tập tin nén, ứng dụng sẽ thực hiện quy trình giải nén đệ quy. Điều này cho phép phát hiện các mối đe dọa bên trong tập tin nén nhiều cấp (tập tin nén bên trong tập tin nén).
Quét các gói phân phối	Hộp kiểm này bật hoặc tắt tính năng quét các gói phân phối.
Quét các tập tin có định dạng Microsoft Office	Quét các tập tin Microsoft Office (DOC, DOCX, XLS, PPT và đuôi mở rộng khác của Microsoft). Các tập tin định dạng Office cũng bao gồm các đối tượng OLE.
Quét định dạng email	<p>Quét các tập tin định dạng email và cơ sở dữ liệu email. Ứng dụng sẽ quét các tập tin PST và OST được sử dụng bởi các trình quản lý thư MS Outlook và Windows Mail/Outlook Express cũng như các tập tin EML.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Kaspersky Endpoint Security không hỗ trợ phiên bản 64 bit của ứng dụng email MS Outlook. Điều này có nghĩa là Kaspersky Endpoint Security sẽ không quét các tập tin MS Outlook (tập tin PST và OST) nếu phiên bản 64 bit của MS Outlook được cài đặt trên máy tính, ngay cả khi bạn thêm thư vào trong phạm vi quét.</p> </div> <p>Nếu hộp kiểm được chọn, Kaspersky Endpoint Security sẽ chia nhỏ tập tin định dạng email thành các cấu phần (đầu đề, thân, tập tin đính kèm) và quét chúng để tìm mối đe dọa.</p> <p>Nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ quét tập tin định dạng email như một tập tin duy nhất.</p>
Quét tập tin nén có mật khẩu bảo vệ	<p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ quét các tập nén có mật khẩu bảo vệ. Trước khi các tập tin trong một tập nén có thể được quét, bạn sẽ được nhắc nhập mật khẩu.</p> <p>Nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ bỏ qua việc quét các tập nén có mật khẩu bảo vệ.</p>
Không giải nén các tập tin phức hợp lớn	<p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ không quét các tập tin hỗn hợp nếu dung lượng của chúng vượt quá giá trị được quy định.</p> <p>Nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ quét các tập tin hỗn hợp thuộc mọi kích cỡ.</p> <p>Kaspersky Endpoint Security sẽ quét các tập tin lớn được trích xuất từ tập tin nén bất kể hộp kiểm này có được chọn hay không.</p>
Công nghệ máy học và phân tích dấu hiệu	<p>Phương thức máy học và phân tích dấu hiệu sử dụng cơ sở dữ liệu Kaspersky Endpoint Security chứa mô tả về các mối đe dọa đã biết và các cách để vô hiệu chúng. Tính năng bảo vệ sử dụng phương thức này cho mức độ bảo mật tối thiểu được chấp nhận.</p> <p>Dựa trên khuyến nghị của các chuyên gia Kaspersky, máy học và phân tích dấu hiệu luôn được bật.</p>
Phân tích hành vi	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

	<p>tập tin bị nhiễm một loại virus không xác định, hoặc một biến thể mới của một virus đã biết.</p> <p>Khi quét các tập tin để tìm mã độc, trình phân tích theo hành vi sẽ thực thi các lệnh trong các tập tin thực thi. Số lượng các lệnh được thực thi bởi trình phân tích theo hành vi phụ thuộc vào cấp độ được chỉ định cho trình phân tích theo hành vi. Cấp độ Phân tích hành vi đảm bảo một sự cân bằng giữa việc quét kỹ lưỡng để tìm các mối đe dọa mới, tải lên tài nguyên hệ điều hành, và thời gian phân tích theo hành vi.</p>
Công nghệ iSwift	<p>Công nghệ này cho phép tăng tốc độ quét bằng cách loại trừ một số tập tin nhất định khỏi quá trình quét. Các tập tin được loại trừ khỏi quá trình quét bằng một thuật toán đặc biệt có tính đến ngày phát hành cơ sở dữ liệu Kaspersky Endpoint Security, ngày mà tập tin được quét lần cuối cùng và mọi thay đổi được thực hiện với thiết lập quét. Công nghệ iSwift được cải tiến từ công nghệ iChecker cho hệ thống tập tin NTFS.</p>
Công nghệ iChecker	<p>Công nghệ này cho phép tăng tốc độ quét bằng cách loại trừ một số tập tin nhất định khỏi quá trình quét. Các tập tin được loại trừ khỏi quá trình quét bằng một thuật toán đặc biệt có tính đến ngày phát hành cơ sở dữ liệu Kaspersky Endpoint Security, ngày khi tập tin được quét lần cuối cùng và mọi thay đổi được thực hiện với thiết lập quét. Công nghệ iChecker có một số hạn chế: công nghệ này không hoạt động với tập tin lớn và chỉ áp dụng cho các tập tin có cấu trúc mà ứng dụng nhận dạng được (ví dụ như EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP và RAR).</p>

Kiểm soát tính toàn vẹn của ứng dụng

Kaspersky Endpoint Security sẽ kiểm tra các mô-đun ứng dụng để phát hiện hư hỏng hoặc sửa đổi. Ví dụ như nếu một thư viện ứng dụng có một chữ ký số sai, thư viện đó sẽ được coi là bị hỏng. Tác vụ *Kiểm tra tính toàn vẹn* được dự định dành cho quét các tập tin ứng dụng. Chạy tác vụ *Kiểm tra tính toàn vẹn* nếu Kaspersky Endpoint Security phát hiện một đối tượng độc hại nhưng không vô hiệu đối tượng đó.

Bạn có thể tạo tác vụ *Kiểm tra tính toàn vẹn* trong cả Bảng điều khiển web và Bảng điều khiển quản trị Kaspersky Security Center. Bạn không thể tạo tác vụ trong Bảng điều khiển đám mây Kaspersky Security Center.

Tính toàn vẹn của ứng dụng có thể bị phá vỡ trong các trường hợp sau:

- Một đối tượng độc hại đã sửa đổi các tập tin của Kaspersky Endpoint Security. Trong trường hợp này, hãy thực hiện quy trình khôi phục Kaspersky Endpoint Security bằng các công cụ của hệ điều hành. Sau khi khôi phục, hãy chạy tác vụ quét toàn bộ máy tính và lặp lại kiểm tra tính toàn vẹn.
- Chữ ký số đã hết hạn. Trong trường hợp này, hãy cập nhật Kaspersky Endpoint Security.

[Cách chạy kiểm tra tính toàn vẹn của ứng dụng thông qua Bảng điều khiển quản trị \(MMC\)](#) 

1. Trong Bảng điều khiển quản trị, hãy vào thư mục **Administration Server** → **Tác vụ**.

Danh sách tác vụ sẽ mở.

2. Nhấn nút **New task**.

Trình hướng dẫn Tác vụ sẽ được bắt đầu. Làm theo chỉ dẫn của Trình hướng dẫn.

Bước 1. Chọn loại tác vụ

Chọn **Kaspersky Endpoint Security cho Windows (11.9.0)** → **Kiểm tra tính toàn vẹn**.

Bước 2. Chọn các thiết bị sẽ được gán tác vụ

Chọn các máy tính sẽ được thực hiện tác vụ trên đó. Các tùy chọn sau có thể được sử dụng:

- Gán tác vụ vào một nhóm quản trị. Trong trường hợp này, tác vụ sẽ được gán cho các máy tính được bao gồm trong một nhóm quản trị đã được tạo trước đó.
- Chọn các máy tính được Máy chủ quản trị phát hiện trong mạng – *các thiết bị chưa được gán*. Các thiết bị được quy định có thể bao gồm các thiết bị trong nhóm quản trị cũng như các thiết bị chưa được gán.
- Nhập vào thủ công địa chỉ của thiết bị, hoặc nhập các địa chỉ từ một danh sách. Bạn có thể quy định tên NetBIOS, địa chỉ IP, và địa chỉ IP mạng con của các thiết bị mà bạn muốn gán tác vụ.

Bước 3. Cấu hình lịch khởi chạy tác vụ

Cấu hình lịch khởi chạy một tác vụ, ví dụ như khởi chạy thủ công hoặc khi phát hiện lây nhiễm virus.

Bước 4. Xác định tên tác vụ

Nhập tên cho tác vụ, ví dụ: *Kiểm tra tính toàn vẹn sau khi máy tính bị nhiễm*.

Bước 5. Hoàn tất việc tạo tác vụ

Thoát Trình hướng dẫn. Nếu cần, hãy chọn hộp kiểm **Run the task after the Wizard finishes**. Bạn có thể giám sát tiến độ của tác vụ trong thuộc tính tác vụ. Kết quả là Kaspersky Endpoint Security sẽ kiểm tra tính toàn vẹn của ứng dụng. Bạn cũng có thể cấu hình lịch kiểm tra tính toàn vẹn của ứng dụng trong thuộc tính tác vụ (xem bảng bên dưới).

[Cách chạy kiểm tra tính toàn vẹn của ứng dụng thông qua Bảng điều khiển web](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.
Danh sách tác vụ sẽ mở.
2. Nhấn vào nút **Thêm**.
Trình hướng dẫn Tác vụ sẽ được bắt đầu.
3. Cấu hình các thiết lập của tác vụ:
 - a. Trong danh sách thả xuống **Ứng dụng**, hãy chọn **Kaspersky Endpoint Security cho Windows (11.9.0)**.
 - b. Trong danh sách thả xuống **Loại tác vụ**, hãy chọn **Kiểm tra tính toàn vẹn**.
 - c. Nhập một mô tả ngắn vào trường **Task name**, ví dụ như *Kiểm tra tính toàn vẹn của ứng dụng sau khi máy tính bị nhiễm virus*.
 - d. Trong phần **Select devices to which the task will be assigned**, chọn phạm vi tác vụ.
4. Chọn các thiết bị theo phạm vi tác vụ được chọn. Chuyển sang bước tiếp theo.
5. Thoát Trình hướng dẫn.
Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ.
6. Chọn hộp kiểm cạnh tác vụ.

Kết quả là Kaspersky Endpoint Security sẽ kiểm tra tính toàn vẹn của ứng dụng. Bạn cũng có thể cấu hình lịch kiểm tra tính toàn vẹn của ứng dụng trong thuộc tính tác vụ (xem bảng bên dưới).

Cách chạy kiểm tra tính toàn vẹn trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn vào mục **Tác vụ**.
2. Thao tác này sẽ mở ra danh sách tác vụ; chọn tác vụ *Kiểm tra tính toàn vẹn* và nhấn vào **Chạy quét**.

Kết quả là Kaspersky Endpoint Security sẽ kiểm tra tính toàn vẹn của ứng dụng. Bạn cũng có thể cấu hình lịch kiểm tra tính toàn vẹn của ứng dụng trong thuộc tính tác vụ (xem bảng bên dưới). Nếu *Kiểm tra tính toàn vẹn* không được hiển thị, điều đó có nghĩa là quản trị viên [đã cấm sử dụng các tác vụ cục bộ trong chính sách](#).

Thiết lập tác vụ kiểm tra tính toàn vẹn

Tham số	Mô tả
Lịch quét	<p>Thủ công. Chế độ chạy trong đó bạn có thể tiến hành quét thủ công tại một thời điểm thuận tiện cho bạn.</p> <p>Theo lịch. Trong chế độ chạy tác vụ quét này, Kaspersky Endpoint Security sẽ chạy tác vụ quét theo lịch mà bạn đã quy định. Nếu chế độ chạy tác vụ quét này được chọn, bạn cũng có thể khởi động tác vụ quét một cách thủ công.</p>
Chạy	Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ bắt đầu lại tác vụ quét bị bỏ

các tác vụ bị bỏ qua	qua ngay khi có thể. Có thể bỏ qua tác vụ quét, ví dụ như nếu máy tính bị tắt vào thời điểm bắt đầu tác vụ quét được lên lịch. Khi hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ không chạy các tác vụ quét bị bỏ qua. Thay vào đó, ứng dụng sẽ chạy tác vụ quét kế tiếp dựa theo lịch hiện tại.
Chỉ chạy khi máy tính đang rảnh	Hoãn bắt đầu tác vụ quét khi tài nguyên máy tính đang bận. Kaspersky Endpoint Security sẽ bắt đầu tác vụ quét nếu máy tính bị khóa hoặc nếu trình bảo vệ màn hình được bật. Nếu bạn đã làm gián đoạn việc thực thi tác vụ, chẳng hạn như bằng cách mở khóa máy tính, Kaspersky Endpoint Security sẽ tự động chạy tác vụ, tiếp tục từ thời điểm tác vụ bị gián đoạn.

Chỉnh sửa phạm vi quét

Phạm vi quét là danh sách các đường dẫn đến các thư mục và đường dẫn mà Kaspersky Endpoint Security quét khi thực thi tác vụ. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự * cùng ? khi nhập tên đại diện.

Để chỉnh sửa phạm vi quét, chúng tôi khuyên bạn nên sử dụng tác vụ *Quét tùy chỉnh*. Các chuyên gia của Kaspersky khuyên bạn không nên thay đổi phạm vi quét của tác vụ *Quét toàn bộ* và *Quét khu vực quan trọng*.

Kaspersky Endpoint Security có các đối tượng được định nghĩa trước sau đây là một phần của phạm vi quét:

- **Email của tôi.**
Các tập tin liên quan đến ứng dụng thư điện tử Outlook: tập tin dữ liệu (PST), tập tin dữ liệu ngoại tuyến (OST).
- **Bộ nhớ hệ thống.**
- **Các đối tượng khởi động.**
Bộ nhớ bị chiếm dụng các tiến trình và tập tin thực thi ứng dụng được chạy khi khởi động hệ thống.
- **Các sector khởi động của ổ đĩa.**
Các sector khởi động của ổ đĩa cứng và ổ đĩa di động.
- **Sao lưu hệ thống.**
Nội dung của thư mục Thông tin ổ đĩa hệ thống.
- **Tất cả các thiết bị lắp ngoài.**
- **Tất cả các ổ đĩa cứng.**
- **Tất cả ổ đĩa mạng.**

Để loại trừ các thư mục hoặc tập tin khỏi phạm vi quét, [hãy thêm thư mục hoặc tập tin vào khu vực tin tưởng](#).

[Cách chỉnh sửa phạm vi quét trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
 2. Trong thư mục **Managed devices** 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, hãy chọn thẻ **Tác vụ**.
 4. Chọn một tác vụ quét và nhấn đúp để mở các thuộc tính tác vụ.
Nếu cần, [hãy tạo một tác vụ Quét virus](#).
 5. Trong cửa sổ thuộc tính tác vụ, hãy chọn mục **Thiết lập**.
 6. Trong mục **Phạm vi quét**, hãy nhấn vào **Thiết lập**.
 7. Trong cửa sổ mở ra, hãy chọn các đối tượng mà bạn muốn thêm vào phạm vi quét hoặc loại trừ khỏi phạm vi đó.
 8. Nếu bạn muốn bổ sung một đối tượng mới vào phạm vi quét:
 - a. Nhấn vào **Thêm**.
 - b. Trong trường **Đối tượng**, hãy nhập đường dẫn đến thư mục hoặc tập tin.
Sử dụng ký tự đại diện:
 - Ký tự `*` (hoa thị) thay thế bất kỳ nhóm ký tự nào bộ ký tự, ngoại trừ các ký tự `\` và `/` (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ, ký tự đại diện `C:**.txt` sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng TXT nằm trong các thư mục trên ổ C:, nhưng không phải trong các thư mục con.
 - Hai ký tự `**` liên tiếp thay thế bất kỳ nhóm ký tự nào (bao gồm nhóm rỗng) trong tên tập tin hoặc thư mục, bao gồm các ký tự `\` và `/` (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ, ký tự đại diện `C:\Folder***.txt` sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng TXT nằm trong thư mục được đặt tên là `Folder` và các thư mục con. Một đại diện phải có ít nhất một cặp lồng ghép. `C:***.txt` không phải là một đại diện hợp lệ.
 - Ký tự `?` (dấu hỏi) thay thế bất kỳ ký tự đơn nào, ngoại trừ các ký tự `\` và `/` (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ: đại diện `C:\Folder\???.txt` sẽ bao gồm các đường dẫn đến tất cả các tập tin có trong thư mục `Folder` có phần mở rộng TXT và tên có ba ký tự.
 9. Lưu các thay đổi của bạn.
- Bạn có thể loại trừ một đối tượng khỏi tác vụ quét mà không cần xóa nó khỏi danh sách các đối tượng trong phạm vi quét. Để thực hiện, hãy bỏ chọn hộp kiểm bên cạnh đối tượng.

[Cách chỉnh sửa phạm vi quét trong Bảng điều khiển web và Bảng điều khiển đám mây](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.

Danh sách tác vụ sẽ mở.

2. Nhấn vào tác vụ quét.

Cửa sổ thuộc tính tác vụ sẽ được mở ra. Nếu cần, [hãy tạo một tác vụ Quét virus](#).

3. Chọn thẻ **Application settings**.

4. Trong mục **Phạm vi quét**, hãy chọn các đối tượng mà bạn muốn thêm vào phạm vi quét hoặc loại trừ khỏi phạm vi đó.

5. Nếu bạn muốn bổ sung một đối tượng mới vào phạm vi quét:

a. Nhấn vào nút **Thêm**.

b. Trong trường **Đường dẫn**, hãy nhập đường dẫn đến thư mục hoặc tập tin.

Sử dụng ký tự đại diện:

- Ký tự ***** (hoa thị) thay thế bất kỳ nhóm ký tự nào bộ ký tự, ngoại trừ các ký tự **** và **/** (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ, ký tự đại diện `C:**.txt` sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng TXT nằm trong các thư mục trên ổ C:, nhưng không phải trong các thư mục con.
- Hai ký tự ****** liên tiếp thay thế bất kỳ nhóm ký tự nào (bao gồm nhóm rỗng) trong tên tập tin hoặc thư mục, bao gồm các ký tự **** và **/** (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ, ký tự đại diện `C:\Folder***.txt` sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng TXT nằm trong thư mục được đặt tên là `Folder` và các thư mục con. Một đại diện phải có ít nhất một cặp lồng ghép. `C:***.txt` không phải là một đại diện hợp lệ.
- Ký tự **?** (dấu hỏi) thay thế bất kỳ ký tự đơn nào, ngoại trừ các ký tự **** và **/** (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ: đại diện `C:\Folder\???.txt` sẽ bao gồm các đường dẫn đến tất cả các tập tin có trong thư mục `Folder` có phần mở rộng TXT và tên có ba ký tự.

Bạn có thể loại trừ một đối tượng khỏi tác vụ quét mà không cần xóa nó khỏi danh sách các đối tượng trong phạm vi quét. Để thực hiện, hãy gạt công tắc bật/tắt bên cạnh sang vị trí tắt.

6. Lưu các thay đổi của bạn.

[Cách chỉnh sửa phạm vi quét trong giao diện ứng dụng](#)

1. Trong cửa sổ chính của ứng dụng, hãy nhấn vào mục **Tác vụ**.
2. Trong danh sách tác vụ, hãy chọn tác vụ *Quét tùy chỉnh* và nhấn vào **Lựa chọn**.
Bạn cũng có thể chỉnh sửa phạm vi quét cho các tác vụ khác. Các chuyên gia của Kaspersky khuyên bạn không nên thay đổi phạm vi quét của tác vụ *Quét toàn bộ* và *Quét khu vực quan trọng*.
3. Trong cửa sổ mở ra, hãy chọn đối tượng mà bạn muốn thêm vào phạm vi quét.
4. Lưu các thay đổi của bạn.

Nếu tác vụ quét không được hiển thị, điều đó có nghĩa là quản trị viên [đã cấm sử dụng các tác vụ cục bộ trong chính sách](#).

Chạy tác vụ quét được lên lịch

Quét toàn bộ máy tính sẽ mất một khoảng thời gian và tài nguyên của máy tính. Bạn nên chọn thời gian tối ưu để chạy quét máy tính để tránh ảnh hưởng xấu đến hiệu năng của các phần mềm khác. Kaspersky Endpoint Security cho phép bạn cấu hình lịch thông thường để quét máy tính. Đây là điều tiện lợi nếu tổ chức của bạn có lịch trình làm việc. Bạn có thể cấu hình quét máy tính để chạy vào ban đêm hoặc vào cuối tuần. 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.

Nếu không thể cấu hình lịch quét tối ưu, Kaspersky Endpoint Security cho phép bạn quét máy tính khi đáp ứng các điều kiện đặc biệt sau:

- Sau khi cập nhật cơ sở dữ liệu.

Kaspersky Endpoint Security chạy quét máy tính với cơ sở dữ liệu mã nhận diện được cập nhật.

- Sau khi ứng dụng khởi động.

Kaspersky Endpoint Security sẽ chạy quét máy tính sau khi một khoảng thời gian nhất định trôi qua, sau khi ứng dụng khởi động. Khi khởi động hệ điều hành, nhiều tiến trình đang chạy, do đó sẽ có lợi nếu bạn hoãn chạy tác vụ quét thay vì chạy quét ngay sau khi khởi động Kaspersky Endpoint Security.

- Wake-on-LAN.

Kaspersky Endpoint Security chạy quét máy tính theo lịch trình ngay cả khi máy tính đã tắt nguồn. Để làm như vậy, ứng dụng sử dụng tính năng Wake-on-LAN của hệ điều hành. Tính năng Wake-on-LAN cho phép bật nguồn máy tính từ xa bằng cách gửi một tín hiệu đặc biệt qua mạng cục bộ. Để sử dụng tính năng này, bạn phải bật Wake-on-LAN trong thiết lập BIOS.

Bạn chỉ có thể cấu hình chạy quét bằng Wake-on-LAN cho tác vụ *Quét virus* trong Kaspersky Security Center. Bạn không thể bật Wake-on-LAN để quét máy tính trong giao diện ứng dụng.

- Khi máy tính đang rảnh.

Kaspersky Endpoint Security sẽ chạy quét máy tính theo lịch trình khi trình bảo vệ màn hình đang hoạt động hoặc màn hình bị khóa. Nếu người dùng mở khóa máy tính, Kaspersky Endpoint Security sẽ tạm dừng quét. Điều này có nghĩa là có thể mất vài ngày để ứng dụng hoàn tất quá trình quét toàn bộ máy tính.

[Cách cấu hình lịch quét trong Bảng điều khiển quản trị \(MMC\)](#) ²


1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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, hãy chọn thẻ **Tác vụ**.
4. Chọn một tác vụ quét và nhấn đúp để mở các thuộc tính tác vụ.
Nếu cần, [hãy tạo một tác vụ Quét virus](#).
5. Trong cửa sổ thuộc tính tác vụ, hãy chọn mục **Lịch**.
6. Cấu hình lịch tác vụ quét.
7. Tùy thuộc vào tần suất được chọn, hãy cấu hình thiết lập nâng cao để quy định lịch chạy tác vụ (xem bảng bên dưới).
8. Lưu các thay đổi của bạn.

Cách cấu hình lịch quét trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.
Danh sách tác vụ sẽ mở.
2. Nhấn vào tác vụ quét.
Cửa sổ thuộc tính tác vụ sẽ được mở ra.
3. Chọn thẻ **Lịch**.
4. Cấu hình lịch tác vụ quét.
5. Tùy thuộc vào tần suất được chọn, hãy cấu hình thiết lập nâng cao để quy định lịch chạy tác vụ (xem bảng bên dưới).
6. Lưu các thay đổi của bạn.

Cách cấu hình lịch quét trong giao diện ứng dụng

Bạn chỉ có thể cấu hình lịch quét nếu một chính sách không được áp dụng với máy tính. Đối với các máy tính áp dụng chính sách, bạn có thể cấu hình lịch tác vụ *Quét virus* trong Kaspersky Security Center.

1. Trong cửa sổ chính của ứng dụng, hãy nhấn vào mục **Tác vụ**.
2. Trong danh sách tác vụ, hãy chọn tác vụ quét và nhấn vào .
Bạn có thể cấu hình lịch chạy Quét toàn bộ, Quét khu vực quan trọng hoặc Kiểm tra tính toàn vẹn. Bạn chỉ có thể chạy Quét tùy chỉnh theo cách thủ công.
3. Nhấn vào **Lịch quét**.
4. Trong cửa sổ mở ra, hãy cấu hình lịch chạy tác vụ quét.
5. Tùy thuộc vào tần suất được chọn, hãy cấu hình thiết lập nâng cao để quy định lịch chạy tác vụ (xem bảng bên dưới).
6. Lưu các thay đổi của bạn.

Thiết lập lịch quét

Tham số	Mô tả
Lịch quét	<p>Thủ công. Chế độ chạy trong đó bạn có thể tiến hành quét thủ công tại một thời điểm thuận tiện cho bạn.</p> <p>Theo lịch. Trong chế độ chạy tác vụ quét này, Kaspersky Endpoint Security sẽ chạy tác vụ quét theo lịch mà bạn đã quy định. Nếu chế độ chạy tác vụ quét này được chọn, bạn cũng có thể khởi động tác vụ quét một cách thủ công.</p>
Trì hoãn chạy sau khi ứng dụng khởi động N phút	Hoãn bắt đầu tác vụ quét sau khi ứng dụng khởi động. Khi khởi động hệ điều hành, nhiều tiến trình đang chạy, do đó sẽ có lợi nếu bạn hoãn chạy tác vụ quét thay vì chạy quét ngay sau khi khởi động Kaspersky Endpoint Security.
Chạy các tác vụ bị bỏ qua	Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ bắt đầu lại tác vụ quét bị bỏ qua ngay khi có thể. Có thể bỏ qua tác vụ quét, ví dụ như nếu máy tính bị tắt vào thời điểm bắt đầu tác vụ quét được lên lịch. Khi hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ không chạy các tác vụ quét bị bỏ qua. Thay vào đó, ứng dụng sẽ chạy tác vụ quét kế tiếp dựa theo lịch hiện tại.
Chỉ chạy khi máy tính đang rảnh	Hoãn bắt đầu tác vụ quét khi tài nguyên máy tính đang bận. Kaspersky Endpoint Security sẽ bắt đầu tác vụ quét nếu máy tính bị khóa hoặc nếu trình bảo vệ màn hình được bật. Nếu bạn đã làm gián đoạn việc thực thi tác vụ, chẳng hạn như bằng cách mở khóa máy tính, Kaspersky Endpoint Security sẽ tự động chạy tác vụ, tiếp tục từ thời điểm tác vụ bị gián đoạn.
Use automatically randomized delay for task starts	Nếu hộp kiểm này được chọn, tác vụ không được chạy đúng theo lịch mà được chạy ngẫu nhiên trong một khoảng thời gian nhất định, tức là thời gian bắt đầu của tác vụ được dàn trải. Thời gian bắt đầu ngẫu nhiên giúp tránh một số lượng lớn máy tính đồng thời truy cập vào Máy chủ quản trị khi tác vụ được chạy theo lịch.

<p><i>(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)</i></p>	<p>Dài thời gian bắt đầu ngẫu nhiên được tính toán tự động khi tác vụ được tạo, tùy thuộc vào số lượng máy tính được gán tác vụ. Sau đó, tác vụ luôn được chạy vào thời gian bắt đầu đã được tính toán của tác vụ đó. Tuy nhiên, bất cứ khi nào thiết lập tác vụ được sửa đổi hoặc tác vụ được chạy theo cách thủ công, thời gian bắt đầu được tính toán sẽ thay đổi.</p> <p>Nếu hộp kiểm này bị xóa, tác vụ được chạy vào đúng thời gian đã lên lịch.</p>
<p>Dừng tác vụ nếu tác vụ đó đã chạy lâu hơn N (phút)</p> <p><i>(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)</i></p>	<p>Giới hạn thời gian thực thi tác vụ Sau khoảng thời gian được chỉ định, Kaspersky Endpoint Security sẽ dừng tác vụ. Tác vụ không được đánh dấu là đã hoàn thành. Lần tới Kaspersky Endpoint Security chạy tác vụ thì tác vụ đó sẽ được chạy lại từ đầu và đúng lịch.</p> <p>Ví dụ như để giảm thời gian thực thi tác vụ, bạn có thể: cấu hình phạm vi quét hoặc tối ưu tác vụ quét.</p>
<p>Activate the device before the task is started through Wake-on-LAN (min)</p> <p><i>(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)</i></p>	<p>Nếu hộp kiểm này được chọn, hệ điều hành của máy tính sẽ có thời gian khởi động trước chỉ định để hoàn thành khởi động trước khi tác vụ được chạy. Thời gian khởi động trước mặc định là 5 phút.</p> <p>Chọn hộp kiểm này nếu bạn muốn chạy tác vụ trên tất cả các máy tính kể cả máy tính đã tắt nguồn.</p>

Chạy quét với dưới quyền người dùng khác

Theo mặc định, tác vụ quét được chạy dưới tên của người dùng có quyền mà bạn được đăng ký trong hệ điều hành. Phạm vi bảo vệ có thể bao gồm các ổ đĩa mạng hoặc các đối tượng khác yêu cầu quyền truy cập đặc biệt. Bạn có thể chỉ định một người dùng có quyền theo yêu cầu trong thiết lập Kaspersky Endpoint Security và chạy tác vụ quét bằng tài khoản của người dùng này.

Bạn có thể chạy các tác vụ quét sau dưới quyền một người dùng khác:

- Quét khu vực quan trọng.
- Quét toàn bộ.
- Quét tùy chỉnh.
- [Quét từ Menu ngữ cảnh](#).

Bạn không thể cấu hình quyền người dùng để chạy một tác vụ [Quét ổ đĩa di động](#), [Quét trong nền](#) hoặc [Kiểm tra tính toàn vẹn](#).


[Cách chạy một tác vụ quét trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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, hãy chọn thẻ **Tác vụ**.
4. Chọn một tác vụ quét và nhấn đúp để mở các thuộc tính tác vụ.
5. Trong cửa sổ thuộc tính tác vụ, hãy chọn mục **Tài khoản**.
6. Nhập thông tin đăng nhập tài khoản của người dùng có quyền mà bạn muốn sử dụng để chạy tác vụ quét.
7. Lưu các thay đổi của bạn.

Cách chạy tác vụ quét dưới quyền người dùng khác trong Bảng điều khiển web hoặc Bảng điều khiển đám mây ²

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.
Danh sách tác vụ sẽ mở.
2. Nhấn vào tác vụ quét.
Cửa sổ thuộc tính tác vụ sẽ được mở ra.
3. Chọn thẻ **Thiết lập**.
4. Trong mục **Tài khoản**, hãy nhấn **Thiết lập**.
5. Nhập thông tin đăng nhập tài khoản của người dùng có quyền mà bạn muốn sử dụng để chạy tác vụ quét.
6. Lưu các thay đổi của bạn.

Cách chạy một tác vụ quét trong giao diện ứng dụng ²

1. Trong cửa sổ chính của ứng dụng, hãy nhấn vào mục **Tác vụ**.
2. Trong danh sách tác vụ, hãy chọn tác vụ quét và nhấn vào .
3. Trong thuộc tính tác vụ, hãy chọn **Advanced settings** → **Run scan as**.
4. Trong cửa sổ mở ra, hãy nhập thông tin đăng nhập tài khoản của người dùng có quyền mà bạn muốn sử dụng để chạy tác vụ quét.
5. Lưu các thay đổi của bạn.

Nếu tác vụ quét không được hiển thị, điều đó có nghĩa là quản trị viên [đã cấm sử dụng các tác vụ cục bộ trong chính sách](#).

Tối ưu hóa 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).

Một kỹ thuật phổ biến để che giấu virus và các phần mềm độc hại khác là nhúng chúng trong các tập tin hỗn 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.

Bạn cũng có thể bật các công nghệ iChecker và iSwift. Các công nghệ iChecker và iSwift sẽ 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.

[Cách tối ưu hóa quét trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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, hãy chọn thẻ **Tác vụ**.
4. Chọn một tác vụ quét và nhấn đúp để mở các thuộc tính tác vụ.
Nếu cần, [hãy tạo một tác vụ Quét virus](#).
5. Trong cửa sổ thuộc tính tác vụ, hãy chọn mục **Thiết lập**.
6. Trong mục **Mức độ bảo mật**, hãy nhấn nút **Thiết lập**.
Thao tác này sẽ mở ra cửa sổ thiết lập tác vụ quét.
7. Trong mục **Tối ưu hóa quét**, hãy cấu hình thiết lập quét:
 - **Chỉ quét các tập tin mới và bị thay đổi.** Chỉ quét các tập tin mới và được thay đổi kể từ lần cuối cùng chúng được quét. Điều này giảm thời lượng của một lần quét. Chế độ này được áp dụng cho cả các tập tin đơn và tập tin hỗn hợp.
Bạn cũng có thể cấu hình quét các tập tin mới theo loại. Ví dụ: bạn có thể quét tất cả các gói phân phối và chỉ quét các tập tin nén mới và các tập tin định dạng văn phòng.
 - **Bỏ qua các tập tin quét trong thời gian dài hơn N giây** Thao tác này sẽ đặt giới hạn thời gian để quét một đối tượng duy nhất. Sau một khoảng thời gian được quy định, Kaspersky Endpoint Security sẽ ngừng quét một tập tin. Điều này giảm thời lượng của một lần quét.
8. Nhấn vào **Bổ sung**.
Thao tác này sẽ mở ra cửa sổ thiết lập quét tập tin phức hợp.
9. Trong mục **Dung lượng giới hạn**, hãy chọn hộp kiểm **Không giải nén các tập tin phức hợp lớn**.
Thao tác này đặt giới hạn thời gian để quét một đối tượng duy nhất. Sau một khoảng thời gian được quy định, Kaspersky Endpoint Security sẽ ngừng quét một tập tin. Điều này giảm thời lượng của một lần quét.

Kaspersky Endpoint Security sẽ quét các tập tin lớn được giải nén từ tập nén, bất kể là hộp kiểm **Không giải nén các tập tin phức hợp lớn** có được chọn hay không.
10. Nhấn **OK**.
11. Chọn thẻ **Bổ sung**.
12. Trong mục **Công nghệ quét**, chọn hộp kiểm cạnh tên của các công nghệ mà bạn muốn sử dụng trong một tác vụ quét:
 - **Công nghệ iSwift.** Công nghệ này cho phép tăng tốc độ quét bằng cách loại trừ một số tập tin nhất định khỏi quá trình quét. Các tập tin được loại trừ khỏi quá trình quét bằng một thuật toán đặc biệt có tính đến ngày phát hành cơ sở dữ liệu Kaspersky Endpoint Security, ngày mà tập tin được quét lần cuối cùng và mọi thay đổi được thực hiện với thiết lập quét. Công nghệ iSwift được cải tiến từ công nghệ iChecker cho hệ thống tập tin NTFS.

- **Công nghệ iChecker.** Công nghệ này cho phép tăng tốc độ quét bằng cách loại trừ một số tập tin nhất định khỏi quá trình quét. Các tập tin được loại trừ khỏi quá trình quét bằng một thuật toán đặc biệt có tính đến ngày phát hành cơ sở dữ liệu Kaspersky Endpoint Security, ngày khi tập tin được quét lần cuối cùng và mọi thay đổi được thực hiện với thiết lập quét. Công nghệ iChecker có một số hạn chế: công nghệ này không hoạt động với tập tin lớn và chỉ áp dụng cho các tập tin có cấu trúc mà ứng dụng nhận dạng được (ví dụ như EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP và RAR).

13. Lưu các thay đổi của bạn.

Cách tối ưu hóa quét trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.

Danh sách tác vụ sẽ mở.

2. Nhấn vào tác vụ quét.

Cửa sổ thuộc tính tác vụ sẽ được mở ra. Nếu cần, [hãy tạo một tác vụ Quét virus](#).

3. Chọn thẻ **Application settings**.

4. Trong mục **Hành động khi phát hiện mối đe dọa**, hãy chọn hộp kiểm **Chỉ quét các tập tin mới và bị thay đổi**. Chỉ quét các tập tin mới và được thay đổi kể từ lần cuối cùng chúng được quét. Điều này giảm thời lượng của một lần quét. Chế độ này được áp dụng cho cả các tập tin đơn và tập tin hỗn hợp.

Bạn cũng có thể cấu hình quét các tập tin mới theo loại. Ví dụ: bạn có thể quét tất cả các gói phân phối và chỉ quét các tập tin nén mới và các tập tin định dạng văn phòng.

5. Chọn hộp kiểm **Không giải nén các tập tin phức hợp lớn**. Thao tác này đặt giới hạn thời gian để quét một đối tượng duy nhất. Sau một khoảng thời gian được quy định, Kaspersky Endpoint Security sẽ ngừng quét một tập tin. Điều này giảm thời lượng của một lần quét.


Kaspersky Endpoint Security sẽ quét các tập tin lớn được giải nén từ tập nén, bất kể là hộp kiểm **Không giải nén các tập tin phức hợp lớn** có được chọn hay không.

6. Trong mục **Thiết lập nâng cao**, hãy chọn hộp kiểm **Bỏ qua các tập tin quét trong thời gian dài hơn N giây**. Thao tác này đặt giới hạn thời gian để quét một đối tượng duy nhất. Sau một khoảng thời gian được quy định, Kaspersky Endpoint Security sẽ ngừng quét một tập tin. Điều này giảm thời lượng của một lần quét.

7. Lưu các thay đổi của bạn.

Cách tối ưu hóa quét trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn vào mục **Tác vụ**.

2. Trong danh sách tác vụ, hãy chọn tác vụ quét và nhấn vào .

3. Nhấn vào **Thiết lập nâng cao**.

4. Trong mục **Tối ưu hóa quét**, hãy cấu hình thiết lập quét:

- **Chỉ quét các tập tin mới và bị thay đổi.** Chỉ quét các tập tin mới và được thay đổi kể từ lần cuối cùng chúng được quét. Điều này giảm thời lượng của một lần quét. Chế độ này được áp dụng cho cả các tập tin đơn và tập tin hỗn hợp.

Bạn cũng có thể cấu hình quét các tập tin mới theo loại. Ví dụ: bạn có thể quét tất cả các gói phân phối và chỉ quét các tập tin nén mới và các tập tin định dạng văn phòng.

- **Bỏ qua các đối tượng với thời gian quét cao hơn N giây.** Thao tác này đặt giới hạn thời gian để quét một đối tượng duy nhất. Sau một khoảng thời gian được quy định, Kaspersky Endpoint Security sẽ ngừng quét một tập tin. Điều này giảm thời lượng của một lần quét.

5. Trong mục **Dung lượng giới hạn**, hãy chọn hộp kiểm **Không giải nén các tập tin phức hợp lớn**. Thao tác này đặt giới hạn thời gian để quét một đối tượng duy nhất. Sau một khoảng thời gian được quy định, Kaspersky Endpoint Security sẽ ngừng quét một tập tin. Điều này giảm thời lượng của một lần quét.

Kaspersky Endpoint Security sẽ quét các tập tin lớn được giải nén từ tập nén, bất kể là hộp kiểm **Không giải nén các tập tin phức hợp lớn** có được chọn hay không.

6. Trong mục **Công nghệ quét**, chọn hộp kiểm cạnh tên của các công nghệ mà bạn muốn sử dụng trong một tác vụ quét:

- **Công nghệ iSwift.** Công nghệ này cho phép tăng tốc độ quét bằng cách loại trừ một số tập tin nhất định khỏi quá trình quét. Các tập tin được loại trừ khỏi quá trình quét bằng một thuật toán đặc biệt có tính đến ngày phát hành cơ sở dữ liệu Kaspersky Endpoint Security, ngày mà tập tin được quét lần cuối cùng và mọi thay đổi được thực hiện với thiết lập quét. Công nghệ iSwift được cải tiến từ công nghệ iChecker cho hệ thống tập tin NTFS.
- **Công nghệ iChecker.** Công nghệ này cho phép tăng tốc độ quét bằng cách loại trừ một số tập tin nhất định khỏi quá trình quét. Các tập tin được loại trừ khỏi quá trình quét bằng một thuật toán đặc biệt có tính đến ngày phát hành cơ sở dữ liệu Kaspersky Endpoint Security, ngày khi tập tin được quét lần cuối cùng và mọi thay đổi được thực hiện với thiết lập quét. Công nghệ iChecker có một số hạn chế: công nghệ này không hoạt động với tập tin lớn và chỉ áp dụng cho các tập tin có cấu trúc mà ứng dụng nhận dạng được (ví dụ như EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP và RAR).

7. Lưu các thay đổi của bạn.

Nếu tác vụ quét không được hiển thị, điều đó có nghĩa là quản trị viên [đã cấm sử dụng các tác vụ cục bộ trong chính sách](#).

Cập nhật cơ sở dữ liệu và các mô-đun phần mềm 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 mới 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 đang sử dụng một máy chủ proxy, bạn cần cấu hình thiết lập máy chủ proxy.

Các bản cập nhật được tải về qua giao thức HTTPS. Chúng cũng có thể được tải về qua giao thức HTTP khi bạn không thể tải về bản cập nhật qua giao thức HTTPS.

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. 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 lỗi hỏng 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 cửa sổ chính của ứng dụng hoặc chú giải công cụ mà bạn nhìn thấy khi di con trỏ qua biểu tượng của ứng dụng trong vùng thông báo.

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](#).

Các kịch bản cập nhật mô-đun ứng dụng và cơ sở dữ liệu

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 mới 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.

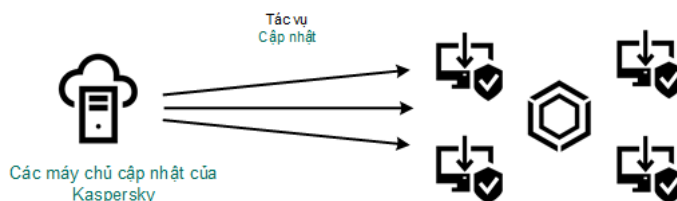
Các đối tượng sau sẽ được cập nhật trên máy tính của người dùng:

- Cơ sở dữ liệu diệt virus. Cơ sở dữ liệu diệt virus bao gồm các cơ sở dữ liệu dấu hiệu phần mềm độc hại, một mô tả về các cuộc tấn công mạng, cơ sở dữ liệu các địa chỉ web độc hại và lừa đảo, cơ sở dữ liệu bảng quảng cáo, cơ sở dữ liệu thư rác và các dữ liệu khác.
- Mô-đun ứng dụng. Các bản cập nhật mô-đun nhằm loại trừ lỗ hổng bảo mật trong ứng dụng và cải thiện phương thức bảo vệ máy tính. Các bản cập nhật mô-đun có thể thay đổi hành vi của thành phần ứng dụng và bổ sung các tính năng mới.

Kaspersky Endpoint Security hỗ trợ các tình huống sau để cập nhật cơ sở dữ liệu và mô-đun ứng dụng:

- Cập nhật từ máy chủ Kaspersky.

Các máy chủ cập nhật của Kaspersky được đặt ở nhiều quốc gia khác nhau trên thế giới. Điều này đảm bảo độ tin cậy khi cập nhật. Nếu một bản cập nhật không thể được thực hiện từ một máy chủ, Kaspersky Endpoint Security sẽ chuyển sang máy chủ tiếp theo.



Cập nhật từ các máy chủ Kaspersky

- Cập nhật tập trung.

Cập nhật tập trung giảm thiểu lưu lượng Internet bên ngoài, và cho phép giám sát quá trình cập nhật một cách tiện lợi.

Cập nhật tập trung bao gồm các bước sau:

1. Tải gói cập nhật về một kho lưu trữ trong mạng lưới của tổ chức.

Gói cập nhật được tải về kho lưu trữ bởi tác vụ Máy chủ quản trị có tên là *Tải bản cập nhật về kho lưu trữ Máy chủ quản trị*.

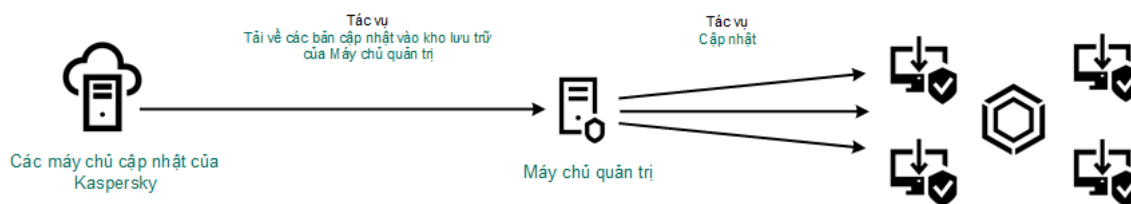
2. Tải gói cập nhật về thư mục chia sẻ (tùy chọn).

Bạn có thể tải gói cập nhật về một thư mục chia sẻ bằng các phương thức sau:

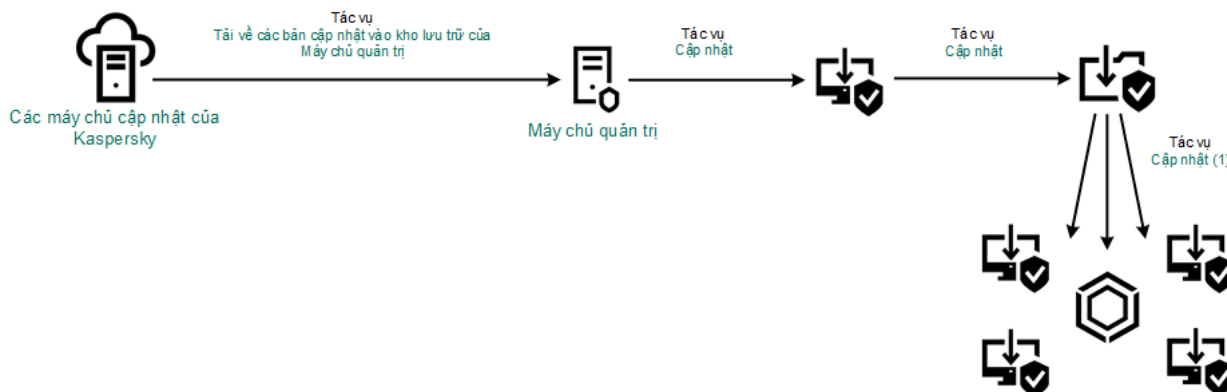
- Sử dụng tác vụ *Cập nhật* của Kaspersky Endpoint Security. Tác vụ này dành cho một máy tính trong mạng cục bộ của công ty.
- Sử dụng Kaspersky Update Utility. Để biết thông tin chi tiết về việc sử dụng Kaspersky Update Utility, hãy tham khảo [Cơ sở tri thức của Kaspersky](#).

3. Phân phối gói cập nhật đến các máy khách.

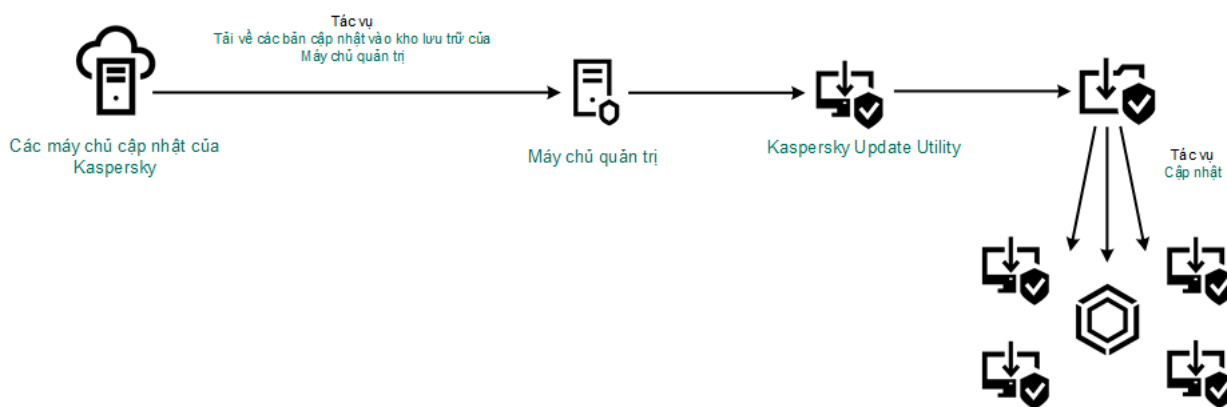
Gói cập nhật được phân phối đến các máy khách thông qua tác vụ *Cập nhật* Kaspersky Endpoint Security. Bạn có thể tạo số lượng không giới hạn tác vụ cập nhật cho mỗi nhóm quản trị.



Cập nhật từ một máy chủ lưu trữ



Cập nhật từ một thư mục được chia sẻ



Cập nhật sử dụng Kaspersky Update Utility

Đối với Bảng điều khiển web, danh sách nguồn cập nhật mặc định chứa Máy chủ quản trị Kaspersky Security Center và các máy chủ cập nhật của Kaspersky. Đối với Bảng điều khiển đám mây Kaspersky Security Center, danh sách nguồn cập nhật mặc định chứa điểm phân phối và các máy chủ cập nhật của Kaspersky. Để biết thêm chi tiết về các điểm phân phối, hãy tham khảo [Trợ giúp của Bảng điều khiển đám mây Kaspersky Security Center](#)¹². 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 một bản cập nhật không thể được thực hiện từ một nguồn cập nhật, Kaspersky Endpoint Security sẽ chuyển sang nguồn tiếp theo.

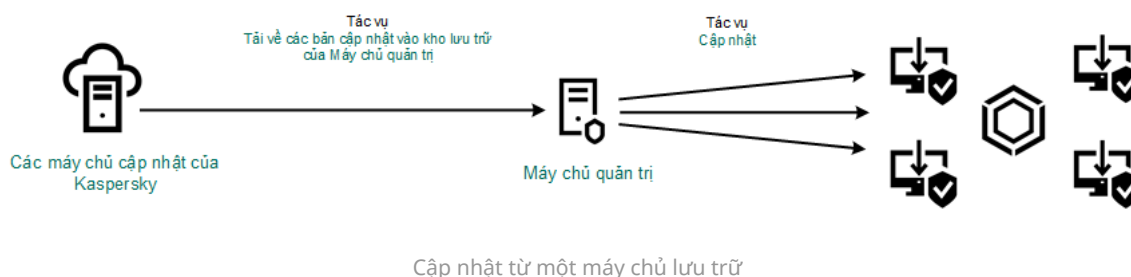
Các bản cập nhật được tải về từ máy chủ cập nhật của Kaspersky hoặc từ các máy chủ FTP hay HTTP khác qua các giao thức mạng tiêu chuẩn. Nếu cần kết nối đến một máy chủ proxy để truy cập nguồn cập nhật, hãy [nhập các thiết lập máy chủ proxy vào thiết lập chính sách của Kaspersky Endpoint Security](#).

Cập nhật từ một máy chủ lưu trữ

Để tiết kiệm lưu lượng Internet, bạn có thể cấu hình các bản cập nhật cơ sở dữ liệu và mô-đun ứng dụng trên các máy tính trong mạng LAN doanh nghiệp từ một máy chủ lưu trữ. Để làm điều này, Kaspersky Security Center phải tải một gói cập nhật về kho lưu trữ (máy chủ FTP hoặc HTTP, thư mục cục bộ hoặc thư mục mạng) từ các máy chủ cập nhật Kaspersky. Các máy tính khác trên mạng LAN doanh nghiệp sẽ có thể nhận gói cập nhật từ máy chủ lưu trữ này.

Cấu hình việc cập nhật cơ sở dữ liệu và mô-đun ứng dụng từ một máy chủ lưu trữ bao gồm các bước sau:

1. Cấu hình việc tải một gói cập nhật về kho lưu trữ trên Máy chủ quản trị (Tác vụ *Tải bản cập nhật về kho lưu trữ Máy chủ quản trị*).
2. Cấu hình việc cập nhật cơ sở dữ liệu và mô-đun ứng dụng từ một máy chủ lưu trữ cụ thể đến các máy tính còn lại trên mạng LAN doanh nghiệp (Tác vụ *Cập nhật*).



Để cấu hình việc tải một gói cập nhật về kho lưu trữ trên máy chủ:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.
Danh sách tác vụ sẽ mở.
2. Chọn tác vụ Máy chủ quản trị **Download updates to the Administration Server repository**.
Cửa sổ thuộc tính tác vụ sẽ được mở ra.
Tác vụ Máy chủ quản trị *Tải bản cập nhật về kho lưu trữ của Máy chủ quản trị* được tạo tự động bởi Trình hướng dẫn bắt đầu nhanh của Bảng điều khiển web Kaspersky Security Center, và tác vụ này chỉ có một trường hợp duy nhất.
3. Chọn thẻ **Application settings**.
4. Trong mục **Thiết lập khác**, hãy nhấn **Cấu hình**.
5. Trong trường **Folder for storing updates**, hãy chỉ định địa chỉ của máy chủ FTP hoặc HTTP, thư mục mạng hoặc thư mục cục bộ mà Kaspersky Security Center sẽ sao chép gói cập nhật nhận được từ các máy chủ cập nhật Kaspersky vào đó.

Định dạng đường dẫn sau có thể được sử dụng để làm nguồn cập nhật:

- Đối với một máy chủ FTP hoặc HTTP, nhập địa chỉ web hoặc địa chỉ IP của nó.
Ví dụ, `http://dn1-01.geo.kaspersky.com/` hoặc `93.191.13.103`.
Đối với máy chủ FTP, bạn có thể quy định thiết lập xác thực trong địa chỉ, theo định dạng sau:
`ftp://<tên người dùng>:<mật khẩu>@<nút>:<cổng>`.
- Đối với thư mục mạng, hãy nhập đường dẫn UNC.
Ví dụ: `\\ Server\Share\Update distribution`.
- Đối với thư mục nội bộ, hãy nhập đường dẫn đầy đủ đến thư mục đó.
Ví dụ, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

6. Lưu các thay đổi của bạn.

Để cấu hình việc cập nhật Kaspersky Endpoint Security từ một ổ lưu trữ máy chủ được quy định:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.

Danh sách tác vụ sẽ mở.

2. Nhấn vào tác vụ **Update** cho Kaspersky Endpoint Security.

Cửa sổ thuộc tính tác vụ sẽ được mở ra.

Tác vụ *Update* được tạo tự động bởi Trình hướng dẫn bắt đầu nhanh của của Kaspersky Security Center. Để tạo tác vụ *Update*, hãy cài đặt tiện ích web của Kaspersky Endpoint Security cho Windows khi đang chạy Trình hướng dẫn.

3. Chọn thẻ **Application settings** → **Local mode**.

4. Trong danh sách các nguồn cập nhật, nhấn nút **Add**.

5. Trong trường **Source**, quy định địa chỉ của máy chủ FTP hoặc HTTP, thư mục mạng hoặc thư mục cục bộ mà Kaspersky Security Center sẽ sao chép gói cập nhật nhận được từ các máy chủ Kaspersky vào đó.

Địa chỉ của nguồn cập nhật phải khớp với địa chỉ mà bạn đã nhập trong trường **Folder for storing updates** khi bạn cấu hình tải bản cập nhật vào ổ lưu trữ máy chủ (xem *hướng dẫn ở trên*).

6. Trong mục **Trạng thái**, hãy chọn **Đã bật**.

7. Nhấn **OK**.

8. Cấu hình các ưu tiên của nguồn cập nhật bằng cách sử dụng nút **Up** và **Down**.

9. Lưu các thay đổi của bạn.

Nếu không thể thực hiện một bản cập nhật từ nguồn cập nhật đầu tiên, Kaspersky Endpoint Security sẽ tự động chuyển sang nguồn tiếp theo.

Cập nhật từ một thư mục được chia sẻ

Để tiết kiệm lưu lượng Internet, bạn có thể cấu hình các bản cập nhật cơ sở dữ liệu và mô-đun ứng dụng trên các máy tính trong mạng LAN doanh nghiệp từ một thư mục được chia sẻ. Để làm điều này, một máy tính trên mạng LAN doanh nghiệp phải nhận gói cập nhật từ Máy chủ quản trị Kaspersky Security Center hoặc từ máy chủ cập nhật Kaspersky, và sao chép gói cập nhật nhận được đến thư mục được chia sẻ. Các máy tính khác trên mạng LAN doanh nghiệp sẽ có thể nhận gói cập nhật từ thư mục được chia sẻ này.

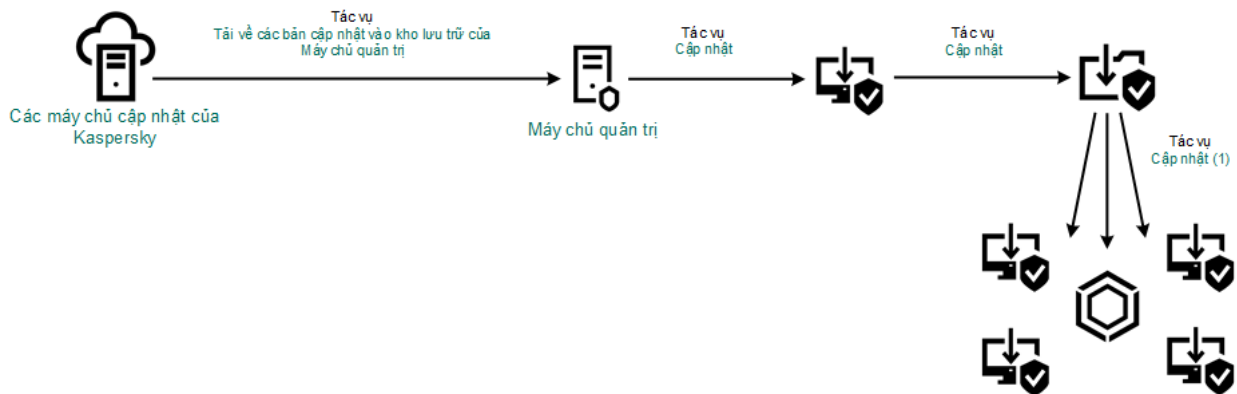
Cấu hình việc cập nhật cơ sở dữ liệu và mô-đun ứng dụng từ một thư mục được chia sẻ bao gồm các bước sau:

1. [Cấu hình cơ sở dữ liệu và các bản cập nhật mô-đun ứng dụng từ kho lưu trữ của máy chủ](#).

2. Cho phép sao chép gói cập nhật đến một thư mục được chia sẻ trên một máy tính trên mạng LAN doanh nghiệp (xem hướng dẫn bên dưới).

3. Cấu hình cập nhật cơ sở dữ liệu và mô-đun ứng dụng từ một thư mục được chia sẻ được chỉ định đến các máy tính còn lại trên mạng LAN doanh nghiệp (xem hướng dẫn bên dưới).

Phiên bản và bản địa hóa của ứng dụng Kaspersky Endpoint Security sao chép gói cập nhật vào thư mục chia sẻ phải khớp với phiên bản và bản địa hóa của ứng dụng cập nhật cơ sở dữ liệu thư mục được chia sẻ. Nếu các phiên bản hoặc bản địa hóa của các ứng dụng không khớp, bản cập nhật cơ sở dữ liệu có thể kết thúc kèm một lỗi.



Cập nhật từ một thư mục được chia sẻ

Để bật việc sao chép gói cập nhật đến thư mục được chia sẻ:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.
Danh sách tác vụ sẽ mở.

Tác vụ *Cập nhật* phải được gán cho một máy tính làm nguồn cập nhật.

2. Nhấn vào tác vụ **Update** cho Kaspersky Endpoint Security.

Cửa sổ thuộc tính tác vụ sẽ được mở ra.

Tác vụ *Update* được tạo tự động bởi Trình hướng dẫn bắt đầu nhanh của của Kaspersky Security Center. Để tạo tác vụ *Update*, hãy cài đặt tiện ích web của Kaspersky Endpoint Security cho Windows khi đang chạy Trình hướng dẫn.

3. Chọn thẻ **Application settings** → **Local mode**.

4. Cấu hình nguồn cập nhật.

Nguồn cập nhật có thể là các máy chủ cập nhật của Kaspersky, Máy chủ quản trị Kaspersky Security Center, các máy chủ FTP hoặc HTTP khác, các thư mục cục bộ, hoặc thư mục mạng.

5. Chọn hộp kiểm **Copy updates to folder**.

6. Trong trường **Path**, hãy nhập đường dẫn UNC đến thư mục được chia sẻ (ví dụ: \\Server\Share\Update distribution).

Nếu trường này được để trống, Kaspersky Endpoint Security sẽ sao chép gói cập nhật vào thư mục C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\.

7. Lưu các thay đổi của bạn.

Để cấu hình cập nhật từ một thư mục được chia sẻ:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.
Danh sách tác vụ sẽ mở.
2. Nhấn vào nút **Thêm**.
Trình hướng dẫn Tác vụ sẽ được bắt đầu.
3. Cấu hình các thiết lập của tác vụ:
 - a. Trong danh sách thả xuống **Ứng dụng**, hãy chọn **Kaspersky Endpoint Security cho Windows (11.9.0)**.
 - b. Trong danh sách thả xuống **Loại tác vụ**, hãy chọn **Cập nhật**.
 - c. Trong trường **Task name**, hãy nhập một mô tả ngắn, ví dụ như *Cập nhật từ thư mục được chia sẻ*.
 - d. Trong phần **Select devices to which the task will be assigned**, chọn phạm vi tác vụ.

Tác vụ *Cập nhật* phải được gán cho các máy tính của mạng LAN doanh nghiệp, ngoại trừ máy tính làm nguồn cập nhật.

4. Chọn các thiết bị theo phạm vi tác vụ được chọn và tới bước tiếp theo.
5. Thoát Trình hướng dẫn.
Một tác vụ mới sẽ được hiển thị trong bảng các tác vụ.
6. Nhấn vào tác vụ *Cập nhật* mới được tạo.
Cửa sổ thuộc tính tác vụ sẽ được mở ra.
7. Vào phần **Application settings**.
8. Chọn thẻ **Local mode**.
9. Trong mục **Nguồn cập nhật**, hãy nhấn vào **Thêm**.
10. Trong trường **Nguồn**, nhập đường dẫn đến thư mục được chia sẻ.

Địa chỉ nguồn phải trùng với địa chỉ bạn đặt trước đây trong trường **Đường dẫn** khi bạn cấu hình sao chép gói cập nhật vào thư mục chia sẻ (xem các *hướng dẫn bên trên*).

11. Nhấn **OK**.
12. Cấu hình các ưu tiên của nguồn cập nhật bằng cách sử dụng nút **Up** và **Down**.
13. Lưu các thay đổi của bạn.

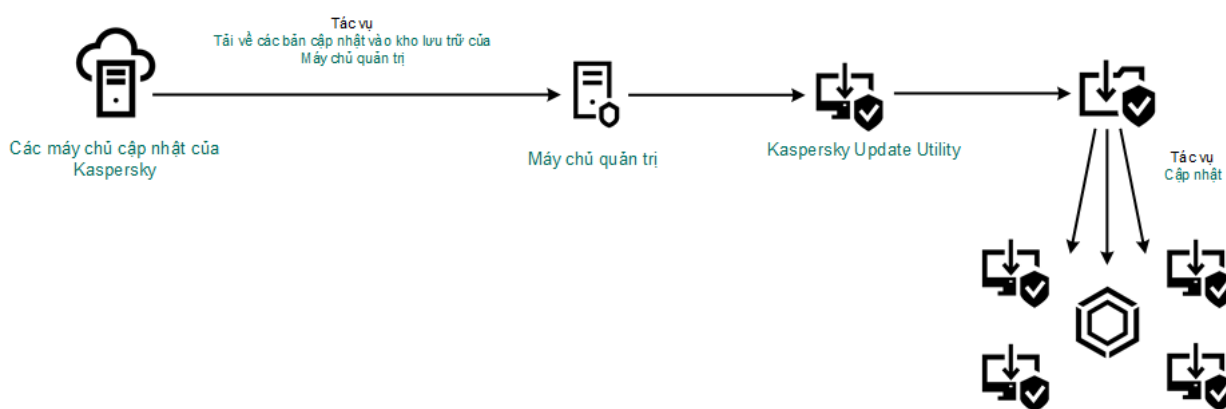
Cập nhật sử dụng Kaspersky Update Utility

Để tiết kiệm lưu lượng Internet, bạn có thể cấu hình các bản cập nhật cơ sở dữ liệu và mô-đun ứng dụng trên các máy tính trong mạng LAN của doanh nghiệp từ một thư mục được chia sẻ bằng cách sử dụng Kaspersky Update Utility. Để làm điều này, một máy tính trên mạng LAN của doanh nghiệp phải nhận gói cập nhật từ Máy chủ quản trị Kaspersky Security Center hoặc từ máy chủ cập nhật Kaspersky, và sao chép các gói cập nhật nhận được đến thư mục được chia sẻ bằng tiện ích này. Các máy tính khác trên mạng LAN doanh nghiệp sẽ có thể nhận gói cập nhật từ thư mục được chia sẻ này.

Cấu hình việc cập nhật cơ sở dữ liệu và mô-đun ứng dụng từ một thư mục được chia sẻ bao gồm các bước sau:

1. [Cấu hình cơ sở dữ liệu và các bản cập nhật mô-đun ứng dụng từ kho lưu trữ của máy chủ.](#)
2. Cài đặt Kaspersky Update Utility trên một trong các máy tính của mạng LAN doanh nghiệp.
3. Cấu hình sao chép gói cập nhật vào thư mục chia sẻ trong thiết lập của Kaspersky Update Utility.
4. Cấu hình việc cập nhật cơ sở dữ liệu và mô-đun ứng dụng từ một thư mục được chia sẻ cụ thể đến các máy tính còn lại trên mạng LAN doanh nghiệp.

Phiên bản và bản địa hóa của ứng dụng Kaspersky Endpoint Security sao chép gói cập nhật vào thư mục chia sẻ phải khớp với phiên bản và bản địa hóa của ứng dụng cập nhật cơ sở dữ liệu từ thư mục được chia sẻ. Nếu các phiên bản hoặc bản địa hóa của các ứng dụng không khớp, bản cập nhật cơ sở dữ liệu có thể kết thúc kèm một lỗi.



Cập nhật sử dụng Kaspersky Update Utility

Bạn có thể tải về gói phân phối Kaspersky Update Utility từ [website Hỗ trợ kỹ thuật của Kaspersky](#). Sau khi cài đặt tiện ích, hãy chọn nguồn cập nhật (ví dụ như kho lưu trữ Máy chủ quản trị) và thư mục chia sẻ nơi Kaspersky Update Utility sẽ sao chép các gói cập nhật vào. Để biết thông tin chi tiết về việc sử dụng Kaspersky Update Utility, hãy tham khảo [Cơ sở tri thức của Kaspersky](#).

Để cấu hình cập nhật từ một thư mục được chia sẻ:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.

Danh sách tác vụ sẽ mở.

2. Nhấn vào tác vụ **Update** cho Kaspersky Endpoint Security.

Cửa sổ thuộc tính tác vụ sẽ được mở ra.

Tác vụ *Update* được tạo tự động bởi Trình hướng dẫn bắt đầu nhanh của của Kaspersky Security Center. Để tạo tác vụ *Update*, hãy cài đặt tiện ích web của Kaspersky Endpoint Security cho Windows khi đang chạy Trình hướng dẫn.

3. Chọn thẻ **Application settings** → **Local mode**.
4. Trong danh sách các nguồn cập nhật, nhấn nút **Thêm**.
5. Trong trường **Source**, hãy nhập đường dẫn UNC đến thư mục được chia sẻ (ví dụ: \\Server\Share\Update distribution).

Địa chỉ nguồn phải trùng với địa chỉ được ghi trong thiết lập của Kaspersky Update Utility.

6. Nhấn **OK**.
7. Cấu hình các ưu tiên của nguồn cập nhật bằng cách sử dụng nút **Lên** và **Xuống**.
8. Lưu các thay đổi của bạn.

Cập nhật trong chế độ di động

Chế độ di động là chế độ hoạt động của Kaspersky Endpoint Security khi một máy tính rời khỏi mạng của tổ chức (*máy tính ngoại tuyến*). Để biết thêm chi tiết về làm việc với máy tính ngoại tuyến và người dùng ngoài văn phòng, vui lòng tham khảo [Trợ giúp của Kaspersky Security Center](#).

Một máy tính ngoại tuyến bên ngoài mạng của tổ chức không thể kết nối đến Máy chủ quản trị để cập nhật các cơ sở dữ liệu và mô-đun ứng dụng. Theo mặc định, chỉ máy chủ cập nhật của Kaspersky được sử dụng làm nguồn cập nhật để cập nhật các cơ sở dữ liệu và mô-đun ứng dụng trong chế độ di động. Việc sử dụng máy chủ proxy để kết nối đến Internet được xác định bởi một [chính sách ngoài văn phòng](#) đặc biệt. Chính sách ngoài văn phòng phải được tạo riêng. Khi Kaspersky Endpoint Security được chuyển sang chế độ di động, tác vụ cập nhật sẽ được khởi chạy hai giờ một lần.

Để cấu hình thiết lập cập nhật cho chế độ di động:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.
Danh sách tác vụ sẽ mở.
2. Nhấn vào tác vụ **Update** cho Kaspersky Endpoint Security.
Cửa sổ thuộc tính tác vụ sẽ được mở ra.
Tác vụ *Update* được tạo tự động bởi Trình hướng dẫn bắt đầu nhanh của Kaspersky Security Center. Để tạo tác vụ *Update*, hãy cài đặt tiện ích web của Kaspersky Endpoint Security cho Windows khi đang chạy Trình hướng dẫn.
Chọn thẻ **Application settings** → **Mobile mode**.
3. Cấu hình nguồn cập nhật. Nguồn cập nhật có thể là các máy chủ cập nhật Kaspersky, các máy chủ FTP và HTTP khác, các thư mục cục bộ, hoặc thư mục mạng.
4. Lưu các thay đổi của bạn.

Kết quả là, các cơ sở dữ liệu và mô-đun ứng dụng sẽ được cập nhật trên máy tính của người dùng khi chúng được chuyển sang chế độ di động.

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 bắt đầu hoặc dừng một tác vụ cập nhật:

1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Cập nhật**.
2. Trong ô **Cập nhật cơ sở dữ liệu và mô-đun ứng dụng**, hãy nhấn nút **Cập nhật** nếu bạn muốn bắt đầu tác vụ cập nhật.

Kaspersky Endpoint Security sẽ tiến hành cập nhật các mô-đun ứng dụng và cơ sở dữ liệu. Ứng dụng sẽ hiển thị tiến độ tác vụ, dung lượng của các tập tin được tải xuống và nguồn cập nhật. Bạn có thể dừng tác vụ bất kỳ lúc nào bằng cách nhấn nút **Ngừng cập nhật**.


Để bắt đầu hoặc dừng một tác vụ cập nhật khi giao diện ứng dụng đơn giản hóa được hiển thị:

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 danh sách thả xuống **Tác vụ** của menu ngữ cảnh, thực hiện một trong các thao tác sau:
 - chọn một tác vụ cập nhật đang không chạy để bắt đầu nó
 - chọn một tác vụ cập nhật đang chạy để dừng nó
 - chọn một tác vụ cập nhật đang được tạm ngưng để khôi phục hoặc khởi động lại nó

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 một nguồn cập nhật không được cấu hình máy chủ proxy. 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. Trong cửa sổ chính của ứng dụng, hãy vào mục **Cập nhật**.
2. Thao tác này sẽ mở ra danh sách tác vụ; hãy chọn tác vụ cập nhật và nhấn vào .
3. Nhấn vào **Chạy cập nhật cơ sở dữ liệu với quyền người dùng**.
4. Trong cửa sổ mở ra, hãy chọn **Người dùng khác**.
5. Nhập thông tin đăng nhập tài khoản của người dùng với các quyền cần thiết để truy cập nguồn cập nhật.
6. Lưu các thay đổi của bạn.

Chọn chế độ chạy tác vụ cập nhật

Nếu không thể chạy tác vụ cập nhật 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 lịch**, và nếu thời gian bắt đầu 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.

Để chọn chế độ chạy tác vụ cập nhật:

1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Cập nhật**.
2. Thao tác này sẽ mở ra danh sách tác vụ; hãy chọn tác vụ cập nhật và nhấn vào .
3. Nhấn vào **Chế độ chạy**.
4. Trong cửa sổ mở ra, hãy chọn chế độ chạy 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 cấu hình một lịch chạy tác vụ cập nhật, hãy chọn các tùy chọn khác. Cấu hình thiết lập nâng cao để bắt đầu tác vụ cập nhật:
 - Trong trường **Trì hoãn chạy sau khi ứng dụng khởi động N phút**, hãy chỉ định khoảng thời gian bạn muốn tạm hoãn khởi chạy tác vụ cập nhật sau khi khởi động Kaspersky Endpoint Security.
 - Chọn **Chạy quét theo lịch vào ngày hôm sau nếu máy tính được tắt** nếu bạn muốn Kaspersky Endpoint Security chạy các tác vụ cập nhật bị bỏ lỡ ngay khi có cơ hội đầu tiên.
5. Lưu các thay đổi của bạn.

Bổ sung một 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, máy chủ cập nhật của Kaspersky và các thư mục cục bộ hoặc thư mục mạng.

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.

Kaspersky Endpoint Security không hỗ trợ các bản cập nhật từ máy chủ HTTPS, trừ khi chúng là các máy chủ cập nhật của Kaspersky.

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 hỏi gói cập nhật từ nguồn khả dụng đầu tiên.

Để bổ sung một nguồn cập nhật:

1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Cập nhật**.
2. Thao tác này sẽ mở ra danh sách tác vụ; hãy chọn tác vụ cập nhật và nhấn vào .
3. Nhấn nút **Chọn nguồn cập nhật**.
4. Trong cửa sổ mở ra, hãy nhấn vào nút **Thêm**.
5. Trong cửa sổ mở ra, hãy chỉ định địa chỉ của máy chủ FTP hoặc HTTP, thư mục mạng hoặc thư mục trên máy chứa gói cập nhật.

Định dạng đường dẫn sau có thể được sử dụng để làm nguồn cập nhật:

- Đối với một máy chủ FTP hoặc HTTP, nhập địa chỉ web hoặc địa chỉ IP của nó.
Ví dụ, `http://dn1-01.geo.kaspersky.com/` hoặc `93.191.13.103`.
Đối với máy chủ FTP, bạn có thể quy định thiết lập xác thực trong địa chỉ, theo định dạng sau:
`ftp://<tên người dùng>:<mật khẩu>@<nút>:<cổng>`.
- Đối với thư mục mạng, hãy nhập đường dẫn UNC.
Ví dụ: `\\ Server\Share\Update distribution`.
- Đối với thư mục nội bộ, hãy nhập đường dẫn đầy đủ đến thư mục đó.
Ví dụ, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

6. Nhấn nút **Lựa chọn**.
7. Cấu hình các ưu tiên của nguồn cập nhật bằng cách sử dụng nút **Up** và **Down**.
8. Lưu các thay đổi của bạn.


Cấu hình cập nhật từ một thư mục được chia sẻ

Để tiết kiệm lưu lượng Internet, bạn có thể cấu hình các bản cập nhật cơ sở dữ liệu và mô-đun ứng dụng trên các máy tính trong mạng LAN doanh nghiệp từ một thư mục được chia sẻ. Để làm điều này, một máy tính trên mạng LAN doanh nghiệp phải nhận gói cập nhật từ Máy chủ quản trị Kaspersky Security Center hoặc từ máy chủ cập nhật Kaspersky, và sao chép gói cập nhật nhận được đến thư mục được chia sẻ. Các máy tính khác trên mạng LAN doanh nghiệp sẽ có thể nhận gói cập nhật từ thư mục được chia sẻ này.


Cấu hình việc cập nhật cơ sở dữ liệu và mô-đun ứng dụng từ một thư mục được chia sẻ bao gồm các bước sau:

1. Bất 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. Cấu hình việc cập nhật cơ sở dữ liệu và mô-đun ứng dụng từ một thư mục được chia sẻ cụ thể đến các máy tính còn lại trên mạng LAN doanh nghiệp.

Để bật việc sao chép gói cập nhật đến thư mục được chia sẻ:

1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Cập nhật**.
2. Thao tác này sẽ mở ra danh sách tác vụ; hãy chọn tác vụ cập nhật và nhấn vào .
3. Trong mục **Phân phối cập nhật**, hãy chọn hộp kiểm **Sao chép các bản cập nhật vào thư mục**.
4. Nhập đường dẫn UNC đến thư mục được chia sẻ (ví dụ: \\Server\Share\Update distribution).
5. Lưu các thay đổi của bạn.


Để cấu hình cập nhật từ một thư mục được chia sẻ:

1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Cập nhật**.
2. Thao tác này sẽ mở ra danh sách tác vụ; hãy chọn tác vụ cập nhật và nhấn vào .
3. Nhấn nút **Chọn nguồn cập nhật**.
4. Trong cửa sổ mở ra, hãy nhấn vào nút **Thêm**.
5. Trong cửa sổ mở ra, hãy nhập đường dẫn đến thư mục được chia sẻ.

Địa chỉ nguồn phải trùng với địa chỉ bạn chỉ định từ trước khi bạn cấu hình sao chép gói cập nhật vào thư mục chia sẻ (xem các *hướng dẫn bên trên*).


6. Nhấn nút **Lựa chọn**.
7. Cấu hình các ưu tiên của nguồn cập nhật bằng cách sử dụng nút **Up** và **Down**.
8. Lưu các thay đổi của bạn.

Cập nhật mô-đun ứng dụng

Các bản cập nhật mô-đun ứng dụng sẽ sửa lỗi, nâng cao hiệu năng và thêm các tính năng mới. Khi có bản cập nhật mô-đun ứng dụng mới, bạn cần xác nhận việc cài đặt bản cập nhật. Bạn có thể xác nhận việc cài đặt bản cập nhật mô-đun ứng dụng trong giao diện ứng dụng hoặc trong Kaspersky Security Center. Bất cứ khi nào có bản cập nhật, ứng dụng sẽ hiển thị thông báo trong cửa sổ chính của Kaspersky Endpoint Security: . Nếu các bản cập nhật mô-đun ứng dụng yêu cầu việc xem lại và chấp nhận các điều khoản của Thỏa thuận giấy phép người dùng cuối, ứng dụng sẽ chỉ cài đặt các bản cập nhật sau khi các điều khoản của Thỏa thuận giấy phép người dùng cuối đã được chấp nhận. Để biết chi tiết về việc theo dõi các bản cập nhật mô-đun ứng dụng và xác nhận bản cập nhật trong Kaspersky Security Center, vui lòng tham khảo [Trợ giúp của Kaspersky Security Center](#).

Sau khi cài đặt bản cập nhật ứng dụng, bạn có thể được yêu cầu khởi động lại máy tính.


Để cấu hình các bản cập nhật mô-đun ứng dụng:

1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Cập nhật**.
2. Thao tác này sẽ mở ra danh sách tác vụ; hãy chọn tác vụ cập nhật và nhấn vào .
3. Trong mục **Tải xuống và cài đặt các bản cập nhật của mô-đun ứng dụng**, hãy chọn hộp kiểm **Tải xuống các bản cập nhật của mô-đun ứng dụng**.
4. Chọn các bản cập nhật mô-đun ứng dụng mà bạn muốn cài đặt.
 - **Cài đặt các bản cập nhật quan trọng và được phê duyệt.** Nếu tùy chọn này được lựa chọn, khi có các bản cập nhật mô-đun ứng dụng, Kaspersky Endpoint Security sẽ tự động cài đặt các bản cập nhật thiết yếu, và chỉ cài đặt tất cả các bản cập nhật mô-đun ứng dụng khác sau khi chúng đã được phê duyệt cục bộ thông qua giao diện ứng dụng hoặc qua Kaspersky Security Center.
 - **Chỉ cài đặt các bản cập nhật được phê duyệt.** Nếu tùy chọn này được lựa chọn, khi có các bản cập nhật mô-đun ứng dụng, Kaspersky Endpoint Security sẽ chỉ cài đặt chúng sau khi chúng đã được phê duyệt cục bộ thông qua giao diện ứng dụng hoặc qua Kaspersky Security Center. Tùy chọn này được chọn mặc định.
5. Lưu các thay đổi của bạn.

Sử dụng một máy chủ proxy để cập nhật

Bạn có thể được yêu cầu quy định các thiết lập máy chủ proxy để tải về các bản cập nhật cơ sở dữ liệu và mô-đun ứng dụng từ nguồn cập nhật. Có nhiều nguồn cập nhật khác nhau, thiết lập máy chủ proxy sẽ được áp dụng cho tất cả các nguồn. Nếu một số nguồn cập nhật không cần máy chủ proxy, bạn có thể tắt việc sử dụng máy chủ proxy trong thuộc tính chính sách. Kaspersky Endpoint Security cũng sẽ sử dụng máy chủ proxy để truy cập Kaspersky Security Network và máy chủ kích hoạt.

Để cấu hình một kết nối đến các nguồn cập nhật thông qua một máy chủ proxy:

1. Trong cửa sổ chính của Bảng điều khiển web, nhấn vào .
Cửa sổ thuộc tính Máy chủ quản trị sẽ được mở ra.
2. Vào mục **Configuring Internet access**.
3. Chọn hộp kiểm **Use proxy server**.
4. Cấu hình các thiết lập kết nối của máy chủ proxy: địa chỉ máy chủ proxy, cổng và thiết lập xác thực (tên người dùng và mật khẩu).
5. Lưu các thay đổi của bạn.

Để tắt việc sử dụng máy chủ proxy cho một nhóm quản trị cụ thể:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.

Cửa sổ thuộc tính chính sách sẽ được mở ra.

3. Chọn thẻ **Application settings**.

4. Vào **Thiết lập tổng quát** → **Thiết lập mạng**.

5. Trong mục **Thiết lập máy chủ proxy**, hãy chọn **Bỏ qua máy chủ proxy đối với các địa chỉ cục bộ**.

6. Lưu các thay đổi của bạn.

Để cấu hình thiết lập máy chủ proxy trong giao diện ứng dụng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .

2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Thiết lập mạng**.

3. Trong mục **Máy chủ proxy**, hãy nhấn liên kết **Thiết lập máy chủ proxy**.

4. Trong cửa sổ mở ra, hãy chọn một trong các tùy chọn sau để xác định địa chỉ của máy chủ proxy:

- **Tự động phát hiện thiết lập máy chủ proxy.**

Tùy chọn này được chọn mặc định. Kaspersky Endpoint Security sử dụng thiết lập máy chủ proxy được xác định trong thiết lập hệ điều hành.

- **Sử dụng thiết lập máy chủ proxy được chỉ định.**

Nếu bạn đã chọn tùy chọn này, hãy cấu hình thiết lập để kết nối với máy chủ proxy: địa chỉ và cổng máy chủ proxy.

5. Nếu bạn muốn bật xác thực trên máy chủ proxy, hãy chọn hộp kiểm **Sử dụng chứng thực máy chủ proxy** và cung cấp thông tin đăng nhập tài khoản người dùng.

6. Nếu bạn muốn tắt sử dụng máy chủ proxy khi [cập nhật cơ sở dữ liệu và mô-đun ứng dụng](#) từ thư mục được chia sẻ, hãy chọn hộp kiểm **Bỏ qua máy chủ proxy đối với các địa chỉ cục bộ**.

7. Lưu các thay đổi của bạn.

Kết quả là Kaspersky Endpoint Security sẽ sử dụng máy chủ proxy để tải xuống mô-đun ứng dụng và các bản cập nhật cơ sở dữ liệu. Kaspersky Endpoint Security cũng sẽ sử dụng máy chủ proxy để truy cập máy chủ KSN và máy chủ kích hoạt của Kaspersky. Nếu cần phải xác thực trên máy chủ proxy nhưng thông tin đăng nhập tài khoản người dùng không được cung cấp hoặc không chính xác, Kaspersky Endpoint Security sẽ nhắc bạn nhập tên người dùng và mật khẩu.

Lần hoàn tác 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 lưu 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 mã nhận diện không hợp lệ khiến Kaspersky Endpoint Security chặn một ứng dụng an toàn.

Để khôi phục lại bản cập nhật gần nhất:

1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Cập nhật**.

2. Trong ô **Khôi phục cơ sở dữ liệu về phiên bản trước đây**, hãy nhấn nút **Hoàn tác**.

Kaspersky Endpoint Security sẽ bắt đầu khôi phục về bản cập nhật cơ sở dữ liệu gần đây nhất. Ứng dụng sẽ hiển thị tiến độ khôi phục, dung lượng của các tập tin được tải xuống và nguồn cập nhật. Bạn có thể dừng tác vụ bất kỳ lúc nào bằng cách nhấn vào **Ngừng cập nhật**.

Để bắt đầu hoặc dừng một tác vụ hoàn tác khi giao diện ứng dụng đơn giản hóa được hiển thị:

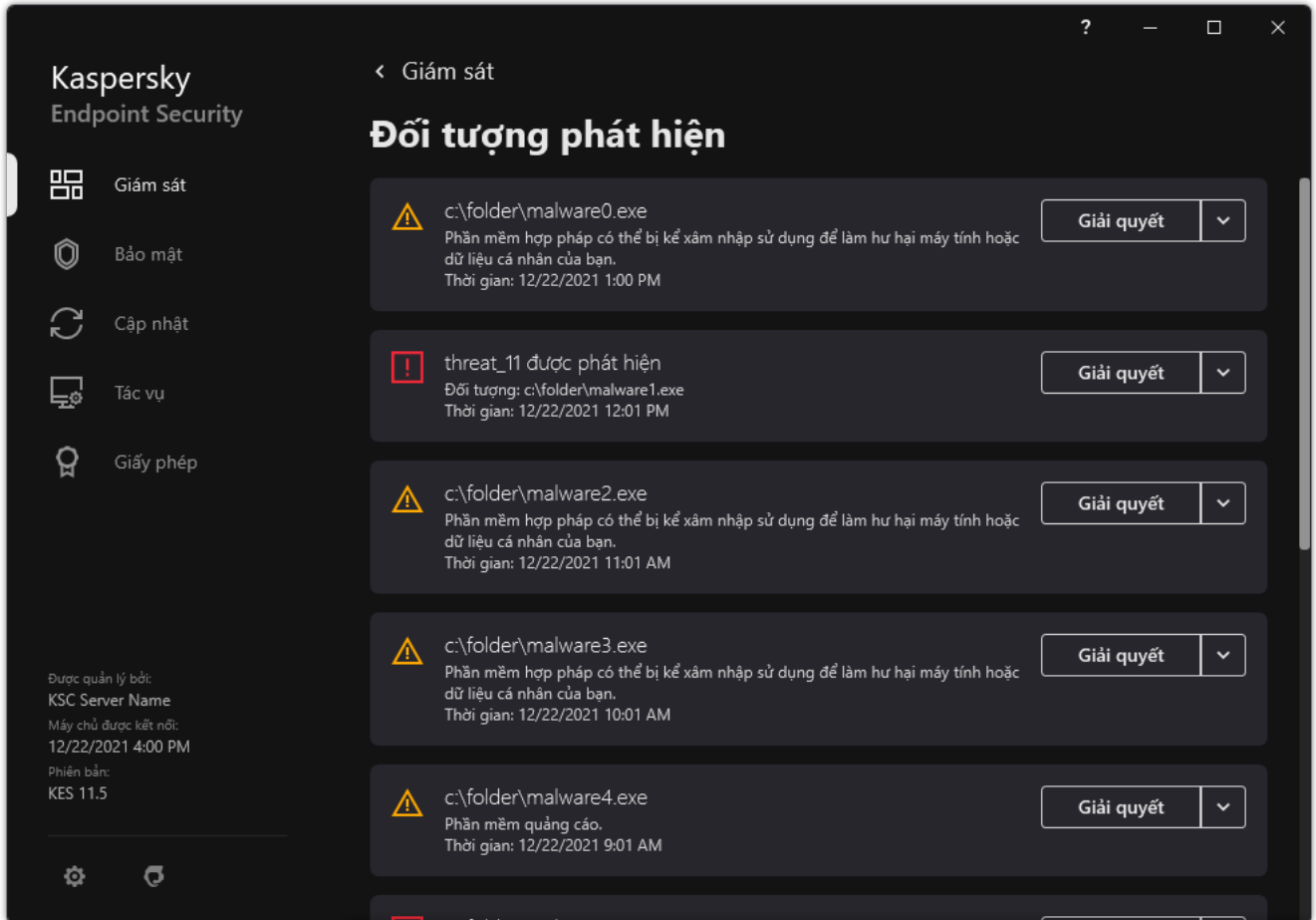
1. Nhấn phải chuột để gọi menu ngữ cảnh của biểu tượng ứng dụng trong khu vực thông báo trên thanh tác vụ.

2. Trong danh sách thả xuống **Tác vụ** của menu ngữ cảnh, thực hiện một trong các thao tác sau:

- Chọn một tác vụ hoàn tác đang không chạy để bắt khởi chạy tác vụ đó.
- Chọn một tác vụ hoàn tác đang chạy để dừng tác vụ đó.
- Chọn một tác vụ hoàn tác đang tạm dừng để khôi phục hoặc khởi chạy lại tác vụ đó.

Làm việc với các mối đe dọa đang hoạt động

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 mối đe dọa đang hoạt động (xem hình bên dưới). Để xử lý các mối đe dọa đang hoạt động, Kaspersky Endpoint Security sử dụng [Công nghệ khử mã độc nâng cao](#). Khử mã độc nâng cao hoạt động khác nhau trên máy trạm và máy chủ. Bạn có thể cấu hình khử mã độc nâng cao trong thiết lập tác vụ [Quét virus](#) và trong [thiết lập ứng dụng](#).

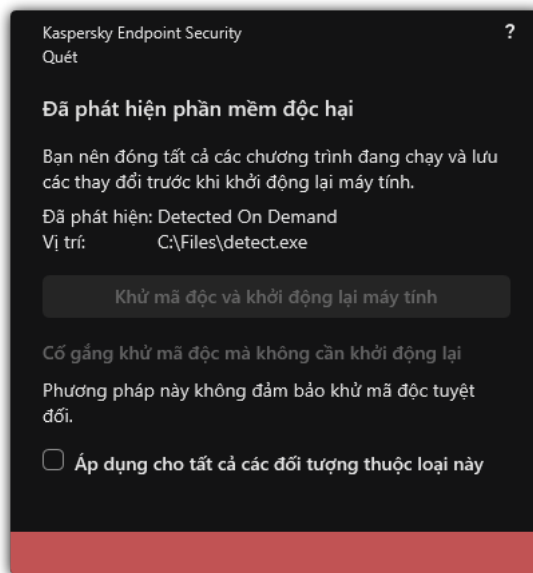


Danh sách các mối đe dọa đang hoạt động

Khử mã độc các mối đe dọa đang hoạt động trên máy trạm

Để xử lý các mối đe dọa đang hoạt động trên máy trạm, [hãy bật công nghệ Khử mã độc nâng cao](#) trong thiết lập ứng dụng. Tiếp theo, hãy cấu hình trải nghiệm người dùng trong thuộc tính tác vụ [Quét virus](#). Có một hộp kiểm **Chạy khử mã độc nâng cao ngay lập tức** trong thuộc tính tác vụ. Nếu đặt cờ này, Kaspersky Endpoint Security sẽ thực hiện khử mã độc mà không thông báo cho người dùng. Khi quá trình khử mã độc hoàn tất, máy tính sẽ được khởi động lại. Nếu không đặt cờ này, Kaspersky Endpoint Security sẽ hiển thị một thông báo về các mối đe dọa đang hoạt động (xem hình bên dưới). Bạn không thể đóng thông báo này mà không xử lý tập tin.

Khử mã độc nâng cao trong một tác vụ quét virus trên máy tính chỉ được thực hiện nếu [tính năng Khử mã độc nâng cao được bật](#) trong thuộc tính của chính sách được áp dụng cho máy tính này.



Thông báo về mối đe dọa đang hoạt động

Khử mã độc các mối đe dọa đang hoạt động trên máy chủ

Để xử lý các mối đe dọa đang hoạt động trên máy chủ, bạn cần thao tác như sau:

- [bật công nghệ Khử mã độc nâng cao](#) trong thiết lập ứng dụng;
- [bật Khử mã độc nâng cao ngay lập tức](#) trong thuộc tính tác vụ *Quét virus*.

Nếu Kaspersky Endpoint Security được cài đặt trên máy tính chạy Windows dành cho Máy chủ thì Kaspersky Endpoint Security sẽ không hiển thị thông báo. Do đó, người dùng không thể chọn hành động để khử mã độc mối đe dọa đang hoạt động. Để khử mã độc một mối đe dọa, bạn cần [bật công nghệ Khử mã độc nâng cao](#) trong thiết lập của ứng dụng và [bật Khử mã độc nâng cao ngay lập tức](#) trong thiết lập tác vụ *Quét virus*. Sau đó bạn cần khởi chạy tác vụ *Quét virus*.

Bật hoặc tắt Công nghệ khử mã độc nâng cao

Nếu Kaspersky Endpoint Security không thể dừng thực thi một phần mềm độc hại, bạn có thể sử dụng công nghệ Khử mã độc nâng cao. Khử mã độc nâng cao bị tắt theo mặc định bởi vì công nghệ này sử dụng một lượng đáng kể tài nguyên hệ thống. Do đó, bạn chỉ có thể bật Khử mã độc nâng cao khi [xử lý các mối đe dọa đang hoạt động](#).

Khử mã độc nâng cao hoạt động khác nhau trên máy trạm và máy chủ. Để sử dụng công nghệ này trên máy chủ, bạn phải [bật khử mã độc nâng cao ngay lập tức](#) trong thuộc tính của tác vụ *Quét diệt virus*. Bạn không cần điều kiện tiên quyết này để sử dụng công nghệ này trên máy trạm.


[Cách bật hoặc tắt Công nghệ khử mã độc nâng cao trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Thiết lập ứng dụng**.
6. Trong mục **Operating mode**, hãy chọn hộp kiểm **Bật Công nghệ khử mã độc nâng cao** để bật hoặc tắt Công nghệ khử mã độc nâng cao.
7. Lưu các thay đổi của bạn.

Cách bật hoặc tắt Công nghệ khử mã độc nâng cao trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Hãy chọn **Thiết lập tổng quát** → **Thiết lập ứng dụng**.
5. Trong mục **Operating mode**, hãy chọn hộp kiểm **Bật Công nghệ khử mã độc nâng cao** để bật hoặc tắt Công nghệ khử mã độc nâng cao.
6. Lưu các thay đổi của bạn.

Cách bật hoặc tắt Công nghệ khử mã độc nâng cao trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Thiết lập ứng dụng**.
3. Trong mục **Operating mode**, hãy chọn hộp kiểm **Sử dụng công nghệ Khử mã độc nâng cao (cần tài nguyên máy tính đáng kể)** để bật hoặc tắt Công nghệ khử mã độc nâng cao.
4. Lưu các thay đổi của bạn.

Kết quả là người dùng không thể sử dụng hầu hết các tính năng của hệ điều hành khi Khử mã độc chủ động đang chạy. Khi quá trình khử mã độc hoàn tất, máy tính được khởi động lại.



Xử lý các mối đe dọa đang hoạt động

Một tập tin bị nhiễm mã độc được coi là *được xử lý* nếu Kaspersky Endpoint Security đã khử mã độc tập tin hoặc loại bỏ mối đe dọa trong quá trình quét máy tính để tìm virus và phần mềm độc hại khác.

Kaspersky Endpoint Security sẽ di chuyển tập tin này vào danh sách các mối đe dọa đang hoạt động nếu, vì bất cứ lý do gì, Kaspersky Endpoint Security đã không thực hiện một hành động trên tập tin đó theo thiết lập 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).
- Trong thiết lập tác vụ [Quét virus](#), hành động khi phát hiện mối đe dọa được đặt thành **Thông báo**. Sau đó, khi thông báo tập tin bị nhiễm mã độc đã được hiển thị trên màn hình, người dùng đã chọn **Bỏ qua**.

Nếu có bất kỳ mối đe dọa nào chưa được xử lý, Kaspersky Endpoint Security sẽ thay đổi biểu tượng thành . Trong cửa sổ chính của ứng dụng, thông báo về mối đe dọa sẽ được hiển thị (xem hình bên dưới). Trong bảng điều khiển Kaspersky Security Center, trạng thái của máy tính được thay đổi thành **Nghiêm trọng** - .

[Cách xử lý một mối đe dọa trong Bảng điều khiển quản trị \(MMC\)](#)

1. Trong Bảng điều khiển quản trị, hãy vào thư mục **Máy chủ quản trị** → **Bổ sung** → **Kho lưu trữ** → **Mối đe dọa hoạt động**.

Danh sách các mối đe dọa đang hoạt động sẽ mở ra.

2. Chọn đối tượng mà bạn muốn xử lý.

3. Chọn cách bạn muốn xử lý mối đe dọa:

- **Khử mã độc**. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ tự động khử nhiễm tất cả các tập tin bị nhiễm virus được phát hiện. Nếu việc khử nhiễm thất bại, Kaspersky Endpoint Security sẽ xóa các tập tin đó.
- **Xóa**.

[Cách xử lý một mối đe dọa trong Bảng điều khiển web và Bảng điều khiển đám mây](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Hoạt động** → **Kho lưu trữ** → **Mối đe dọa hoạt động**.

Danh sách các mối đe dọa đang hoạt động sẽ mở ra.

2. Chọn đối tượng mà bạn muốn xử lý.

3. Chọn cách bạn muốn xử lý mối đe dọa:

- **Khử mã độc.** Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ tự động khử nhiễm tất cả các tập tin bị nhiễm virus được phát hiện. Nếu việc khử nhiễm thất bại, Kaspersky Endpoint Security sẽ xóa các tập tin đó.
- **Xóa.**

Cách xử lý một mối đe dọa trong giao diện ứng dụng

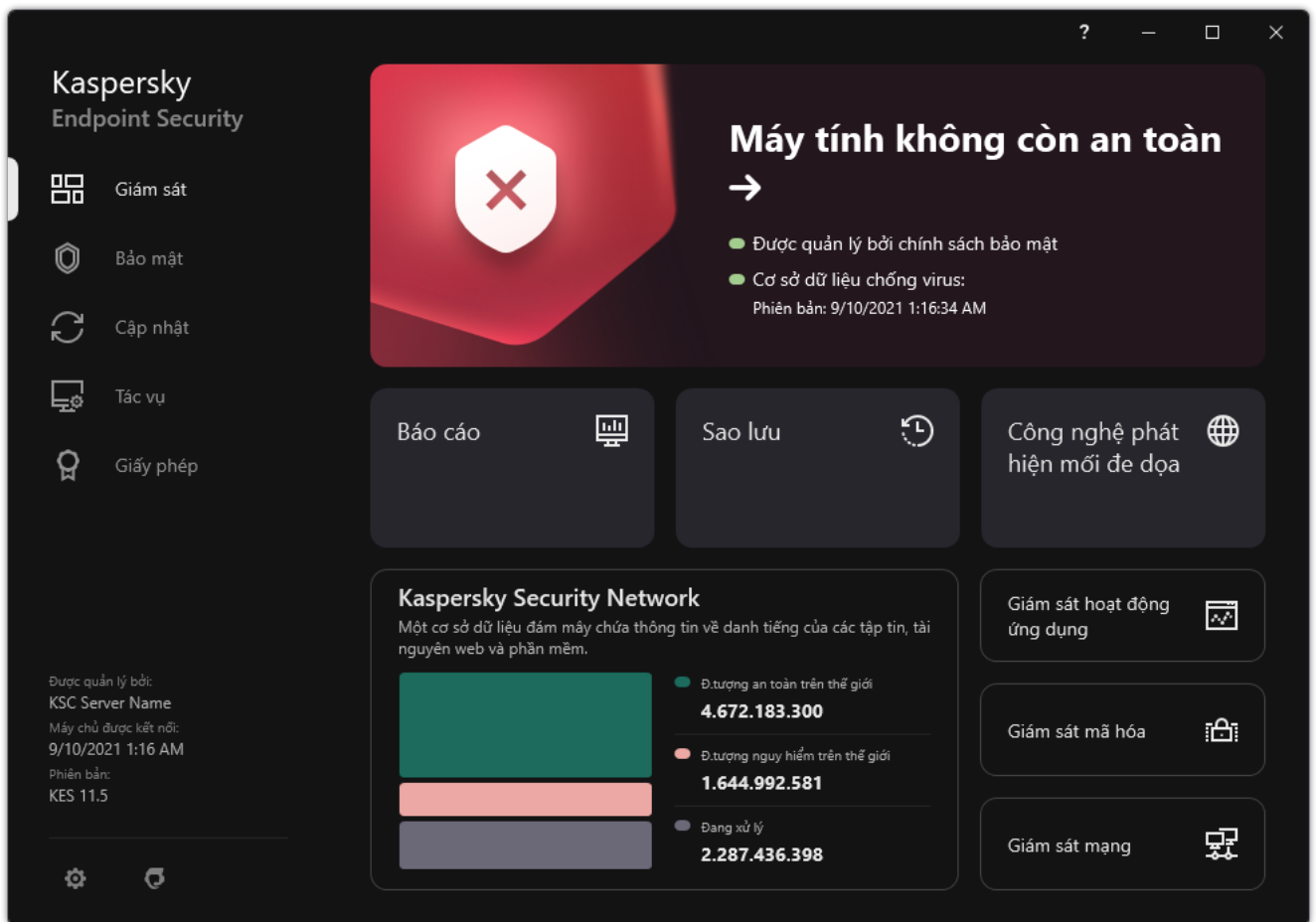
1. Trong cửa sổ chính của ứng dụng, trong mục **Giám sát**, hãy nhấn vào ô **Máy tính không còn an toàn**.

Danh sách các mối đe dọa đang hoạt động sẽ mở ra.

2. Chọn đối tượng mà bạn muốn xử lý.

3. Chọn cách bạn muốn xử lý mối đe dọa:

- **Giải quyết.** Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ tự động khử nhiễm tất cả các tập tin bị nhiễm virus được phát hiện. Nếu việc khử nhiễm thất bại, Kaspersky Endpoint Security sẽ xóa các tập tin đó.
- **Thêm vào loại trừ.** Nếu chọn hành động này, Kaspersky Endpoint Security sẽ đề xuất [thêm tập tin vào danh sách loại trừ quét](#). Thiết lập loại trừ được cấu hình tự động. Nếu thêm loại trừ không khả dụng, điều đó có nghĩa là quản trị viên đã vô hiệu hóa việc thêm loại trừ trong thiết lập chính sách.
- **Bỏ qua.** Nếu chọn tùy chọn này, Kaspersky Endpoint Security sẽ xóa mục đó khỏi danh sách các mối đe dọa đang hoạt động. Nếu không có mối đe dọa đang hoạt động nào còn lại trong danh sách, trạng thái máy tính sẽ được thay đổi thành *OK*. Nếu phát hiện đối tượng lần nữa, Kaspersky Endpoint Security sẽ thêm một mục mới vào danh sách các mối đe dọa đang hoạt động.
- **Mở trong thư mục.** Nếu chọn tùy chọn này, Kaspersky Endpoint Security sẽ mở thư mục chứa đối tượng trong trình quản lý tập tin. Sau đó, bạn có thể xóa đối tượng theo cách thủ công hoặc di chuyển đối tượng vào thư mục ngoài phạm vi bảo vệ.
- **Tìm hiểu thêm.** Nếu chọn tùy chọn này, Kaspersky Endpoint Security sẽ mở [website Bách khoa toàn thư về virus của Kaspersky](#) .



Cửa sổ chính của ứng dụng khi phát hiện ra mối đe dọa

Bảo vệ máy tính

Bảo vệ mối đe dọa tập tin

Thành phần Bảo vệ mối đe dọa tập tin cho phép bạn ngăn chặn nguy cơ nhiễm mã độc cho hệ thống tập tin của máy tính. Theo mặc định, thành phần Bảo vệ mối đe dọa tập tin sẽ chạy thường trực trong RAM của máy tính. Thành phần này quét các tập tin trên tất cả các ổ đĩa của máy tính cũng như trên các ổ đĩa được kết nối. Thành phần này giúp bảo vệ máy tính với sự trợ giúp của cơ sở dữ liệu diệt virus, [dịch vụ đám mây của Kaspersky Security Network](#) và phân tích theo hành vi.


Thành phần này sẽ quét các tập tin được truy cập bởi người dùng hoặc ứng dụng. Nếu phát hiện tập tin độc hại, Kaspersky Endpoint Security sẽ chặn hoạt động của tập tin đó. Sau đó ứng dụng sẽ khử mã độc hoặc xóa tập tin độc hại, tùy thuộc vào thiết lập của thành phần Bảo vệ mối đe dọa tập tin.

Khi cố truy cập tập tin có toàn bộ nội dung được lưu trữ trên ổ lưu trữ đám mây OneDrive, Kaspersky Endpoint Security sẽ tải về và quét nội dung tập tin.

Bật và tắt Bảo vệ mối đe dọa tập tin

Theo mặc định, thành phần Bảo vệ mối đe dọa tập tin sẽ được bật và chạy trong chế độ được khuyến nghị bởi các chuyên gia của Kaspersky. Đối với thành phần Bảo vệ mối đe dọa tập tin, Kaspersky Endpoint Security có thể áp dụng các nhóm thiết lập khác nhau. Các nhóm thiết lập được lưu trữ trong ứng dụng này được gọi là *mức độ bảo mật*: **Cao, Khuyến dùng, Thấp**. Thiết lập mức độ bảo mật **Khuyến dùng** được coi là thiết lập tối ưu được khuyến nghị bởi các chuyên gia Kaspersky (xem bảng bên dưới). Bạn có thể chọn một trong các mức độ bảo mật được thiết lập sẵn hoặc tự cấu hình thiết lập mức độ bảo mật. Nếu bạn đã thay đổi thiết lập mức độ bảo mật, bạn luôn có thể quay lại thiết lập mức độ bảo mật được khuyến nghị.

Để bật hoặc tắt thành phần Bảo vệ mối đe dọa tập tin:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa tập tin**.
3. Sử dụng nút bật/tắt **Bảo vệ mối đe dọa tập tin** để bật hoặc tắt thành phần này.
4. Nếu bạn đã bật thành phần này, hãy thực hiện một trong các hành động sau trong mục **Mức độ bảo mật**:
 - Nếu bạn muốn áp dụng một trong những mức độ bảo mật được thiết lập sẵn, hãy chọn nó bằng thanh trượt:
 - **Cao**. Khi mức độ bảo mật tập tin này được chọn, thành phần Bảo vệ mối đe dọa tập tin sẽ áp dụng cấp kiểm soát chặt chẽ nhất cho tất cả các tập tin được mở, lưu lại và khởi động. Thành phần Bảo vệ mối đe dọa tập tin quét tất cả các loại tập tin trên tất cả các ổ cứng, ổ đĩa di động và ổ đĩa mạng của máy tính. Thành phần này cũng sẽ quét các tập nén, gói cài đặt và đối tượng OLE nhúng.

- **Khuyến dùng.** Mức độ bảo mật tập tin này được khuyến nghị bởi các chuyên gia của Kaspersky Lab. Thành phần Bảo vệ mỗi đe dọa tập tin chỉ quét các định dạng tập tin cụ thể trên tất cả các ổ cứng, ổ đĩa di động và ổ đĩa mạng của máy tính, và các đối tượng OLE được nhúng. Thành phần Bảo vệ mỗi đe dọa tập tin sẽ không quét các tập nén hay gói cài đặt. Các giá trị của thiết lập cho mức độ bảo mật khuyến nghị được cung cấp trong bảng bên dưới.
- **Thấp.** Cấu hình bảo mật tập tin này đảm bảo tốc độ quét tối đa. Thành phần Bảo vệ mỗi đe dọa tập tin chỉ quét các tập tin có phần mở rộng cụ thể trên tất cả các ổ cứng, ổ đĩa di động và ổ đĩa mạng của máy tính. Thành phần Bảo vệ mỗi đe dọa tập tin sẽ không quét các tập tin hỗn hợp.
- Nếu bạn muốn cấu hình mức độ bảo mật tùy chỉnh, hãy nhấn nút **Thiết lập nâng cao** và định nghĩa thiết lập thành phần của riêng bạn.
Bạn có thể khôi phục các giá trị mức độ bảo mật đặt trước bằng cách nhấn nút **Khôi phục cấp bảo mật được khuyến nghị** ở phần trên của cửa sổ.

5. Lưu các thay đổi của bạn.

Thiết lập Bảo vệ mỗi đe dọa tập tin được các chuyên gia Kaspersky khuyến nghị (mức bảo mật được khuyến nghị)

Tham số	Giá trị	Mô tả
Loại tập tin	Quét các tập tin theo định dạng	Nếu thiết lập này được bật, Kaspersky Endpoint Security sẽ chỉ quét <u>các tập tin có thể bị nhiễm virus</u> . Trước khi quét một tập tin để tìm mã độc, đầu đề nội bộ của tập tin sẽ được phân tích để xác định định dạng của tập tin đó (ví dụ, .txt, .doc, hoặc .exe). Tác vụ quét cũng tìm kiếm các tập tin có đuôi mở rộng tập tin cụ thể.
Phân tích hành vi	quét nhanh	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. Khi quét các tập tin để tìm mã độc, trình phân tích theo hành vi sẽ thực thi các lệnh trong các tập tin thực thi. Số lượng các lệnh được thực thi bởi trình phân tích theo hành vi phụ thuộc vào cấp độ được chỉ định cho trình phân tích theo hành vi. Cấp độ Phân tích hành vi đảm bảo một sự cân bằng giữa việc quét kỹ lưỡng để tìm các mối đe dọa mới, tải lên tài nguyên hệ điều hành, và thời gian phân tích theo hành vi.
Chỉ quét các tập tin mới và bị thay đổi	Bật	Chỉ quét các tập tin mới và được thay đổi kể từ lần cuối cùng chúng được quét. Điều này giảm thời lượng của một lần quét. Chế độ này được áp dụng cho cả các tập tin đơn và tập tin hỗn hợp.
Công nghệ iSwift	Bật	Công nghệ này cho phép tăng tốc độ quét bằng cách loại trừ một số tập tin nhất định khỏi quá trình quét. Các tập tin được loại trừ khỏi quá trình quét bằng một thuật toán đặc biệt có tính đến ngày phát hành cơ sở dữ liệu Kaspersky Endpoint Security, ngày mà tập tin được quét lần cuối cùng và mọi thay đổi được thực hiện với thiết lập quét. Công nghệ iSwift được cải tiến từ công nghệ iChecker cho hệ thống tập tin NTFS.
Công nghệ iChecker	Bật	Công nghệ này cho phép tăng tốc độ quét bằng cách loại trừ một số tập tin nhất định khỏi quá trình quét. Các tập tin được loại trừ khỏi quá trình quét bằng một thuật toán đặc biệt có tính đến ngày phát hành cơ sở dữ liệu Kaspersky Endpoint Security, ngày khi tập tin được quét lần cuối cùng và mọi thay đổi được thực hiện với thiết lập quét. Công nghệ iChecker có một số hạn chế: công nghệ này không hoạt động với tập tin lớn và chỉ áp dụng cho các tập tin có cấu trúc mà ứng dụng nhận dạng được (ví dụ như EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP và RAR).


Quét các tập tin có định dạng Microsoft Office	Bật	Quét các tập tin Microsoft Office (DOC, DOCX, XLS, PPT và đuôi mở rộng khác của Microsoft). Các tập tin định dạng Office cũng bao gồm các đối tượng OLE.
Chế độ quét	Chế độ thông minh	Ở chế độ này, Bảo vệ mỗi đe dọa tập tin sẽ quét một đối tượng dựa trên phân tích về hành động đã thực hiện trên đối tượng. Ví dụ: khi làm việc với tài liệu Microsoft Office, 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.
Hành động khi phát hiện mỗi đe dọa	Khử mã độc; xóa nếu không thể khử mã độc	Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ tự động khử nhiễm tất cả các tập tin bị nhiễm virus được phát hiện. Nếu việc khử nhiễm thất bại, Kaspersky Endpoint Security sẽ xóa các tập tin đó.

Tự động tạm ngưng Bảo vệ mỗi đe dọa tập tin

Bạn có thể cấu hình Bảo vệ mỗi đe dọa tập tin để tự động tạm ngưng tại một thời điểm cụ thể, hoặc khi làm việc với các ứng dụng cụ thể.

Bảo vệ mỗi đe dọa tập tin chỉ nên được tạm ngưng trong trường hợp bất khả kháng khi nó xung đột với một số ứng dụng. Nếu có bất kỳ xung đột nào phát sinh khi một thành phần đang chạy, bạn nên liên hệ với [bộ phận Hỗ trợ kỹ thuật của Kaspersky](#). Các chuyên gia hỗ trợ sẽ giúp bạn thiết lập Bảo vệ mỗi đe dọa tập tin để chạy cùng với các ứng dụng khác trên máy tính của bạn.


Để cấu hình tự động tạm ngưng Bảo vệ mỗi đe dọa tập tin:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Bảo vệ mỗi đe dọa tập tin**.
3. Nhấn vào **Thiết lập nâng cao**.
4. Trong mục **Tạm dừng Bảo vệ mỗi đe dọa tập tin**, hãy nhấn liên kết **Tạm dừng Bảo vệ mỗi đe dọa tập tin**.
5. Trong cửa sổ mở ra, hãy cấu hình thiết lập để tạm dừng Bảo vệ mỗi đe dọa tập tin:
 - a. Cấu hình lịch tự động tạm dừng Bảo vệ mỗi đe dọa tập tin.
 - b. Tạo một danh sách các ứng dụng có hoạt động khiến thành phần Bảo vệ mỗi đe dọa tập tin tạm dừng các hoạt động.
6. Lưu các thay đổi của bạn.

Thay đổi hành động xử lý tập tin bị nhiễm của thành phần Bảo vệ mối đe dọa tập tin

Theo mặc định, thành phần Bảo vệ mối đe dọa tập tin sẽ tự động khử nhiễm tất cả các tập tin bị nhiễm virus được phát hiện. Nếu khử mã độc thất bại, thành phần Bảo vệ mối đe dọa tập tin sẽ xóa các tập tin này.

Để thay đổi hành động xử lý tập tin bị nhiễm của thành phần Bảo vệ mối đe dọa tập tin:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa tập tin**.
3. Trong mục **Hành động khi phát hiện mối đe dọa**, hãy chọn tùy chọn liên quan:
 - **Khử mã độc; xóa nếu không thể khử mã độc.** Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ tự động khử nhiễm tất cả các tập tin bị nhiễm virus được phát hiện. Nếu việc khử nhiễm thất bại, Kaspersky Endpoint Security sẽ xóa các tập tin đó.
 - **Khử mã độc; chặn nếu không thể khử mã độc.** Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ tự động khử nhiễm tất cả các tập tin bị nhiễm virus được phát hiện. Nếu không thể khử mã độc, Kaspersky Endpoint Security sẽ bổ sung thông tin về tập tin nhiễm mã độc được phát hiện vào danh sách các mối đe dọa đang hoạt động.
 - **Chặn.** Nếu tùy chọn này được chọn, thành phần Bảo vệ mối đe dọa tập tin sẽ tự động chặn tất cả các tập tin bị nhiễm mà không cố gắng khử nhiễm chúng.

Trước khi cố gắng khử mã độc hoặc xóa một tập tin bị nhiễm, Kaspersky Endpoint Security sẽ tạo một bản sao lưu của tập tin trong trường hợp bạn cần [khôi phục tập tin hoặc nếu nó có thể khử mã độc tập tin trong tương lai](#).

4. Lưu các thay đổi của bạn.

Cấu hình phạm vi bảo vệ của thành phần Bảo vệ mối đe dọa 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 thành phần Bảo vệ mối đe dọa tập tin. Theo mặc định, thành phần Bảo vệ mối đe dọa tập tin chỉ quét [các tập tin có khả năng bị nhiễm mã độc](#) được chạy từ ổ cứng, ổ đĩa di động và ổ đĩa mạng.

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

1. Có xác suất thấp làm lây nhiễm mã độc vào các tập tin thuộc các định dạng nhất định và kích hoạt tập tin đó sau này (ví dụ: định dạng TXT). Đồng thời, cũng có những định dạng tập tin chứa mã thực thi (ví dụ như .exe, .dll). Mã thực thi cũng có thể được chứa trong các tập tin có định dạng không dành cho

mục đích này (ví dụ như định dạng DOC). Nguy cơ xâm nhập và kích hoạt mã độc trên các tập tin này là cao.

2. Một kẻ xâm nhập có thể gửi một virus hoặc một ứng dụng 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, Kaspersky Endpoint Security sẽ phân tích đầu mục tập tin bất kể đuôi mở rộng là gì. Nếu phân tích này cho thấy tập tin có định dạng của một tập tin thực thi (ví dụ như EXE), ứng dụng sẽ quét nó.

Để tạo phạm vi bảo vệ:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Bảo vệ mỗi đe dọa tập tin**.
3. Nhấn vào **Thiết lập nâng cao**.
4. Trong mục **Loại tập tin**, quy định loại tập tin mà bạn muốn được quét bởi thành phần Bảo vệ mỗi đe dọa tập tin:
 - **Tất cả tập tin.** Nếu thiết lập này được bật, Kaspersky Endpoint Security sẽ kiểm tra tất cả các tập tin và không có ngoại lệ (tất cả định dạng và phần mở rộng).
 - **Quét các tập tin theo định dạng.** Nếu thiết lập này được bật, Kaspersky Endpoint Security sẽ chỉ quét [các tập tin có thể bị nhiễm virus](#). Trước khi quét một tập tin để tìm mã độc, đầu đề nội bộ của tập tin sẽ được phân tích để xác định định dạng của tập tin đó (ví dụ, .txt, .doc, hoặc .exe). Tác vụ quét cũng tìm kiếm các tập tin có đuôi mở rộng tập tin cụ thể.
 - **Quét các tập tin theo phần mở rộng.** Nếu thiết lập này được bật, Kaspersky Endpoint Security sẽ chỉ quét [các tập tin có thể bị nhiễm virus](#). Sau đó, định dạng tập tin sẽ được xác định dựa trên phần mở rộng của tập tin.
5. Nhấn vào liên kết **Chỉnh sửa phạm vi bảo vệ**.
6. Trong cửa sổ mở ra, hãy chọn các đối tượng mà bạn muốn thêm vào phạm vi bảo vệ hoặc loại trừ khỏi phạm vi bảo vệ.

Bạn không thể xóa hoặc sửa các đối tượng được bao gồm trong phạm vi bảo vệ mặc định.

7. Nếu bạn muốn bổ sung một đối tượng mới vào phạm vi bảo vệ:

- a. Nhấn vào **Thêm**.

Cây thư mục sẽ mở ra.

- b. Chọn một đối tượng để thêm vào phạm vi bảo vệ.

Bạn có thể loại trừ một đối tượng khỏi tác vụ quét mà không cần xóa nó khỏi danh sách các đối tượng trong phạm vi quét. Để thực hiện, hãy bỏ chọn hộp kiểm bên cạnh đối tượng.


8. Lưu các thay đổi của bạn.

Sử dụng các phương thức quét

Kaspersky Endpoint Security sử dụng một kỹ thuật quét gọi là Máy học và 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. Dựa trên khuyến nghị của các chuyên gia Kaspersky, máy học và phân tích dấu hiệu luôn được bật.


Để tăng hiệu quả bảo vệ, bạn có thể sử dụng phân tích hành vi. Khi quét các tập tin để tìm mã độc, trình phân tích theo hành vi sẽ thực thi các lệnh trong các tập tin thực thi. Số lượng các lệnh được thực thi bởi trình phân tích theo hành vi phụ thuộc vào cấp độ được chỉ định cho trình phân tích theo hành vi. Cấp độ Phân tích hành vi đảm bảo một sự cân bằng giữa việc quét kỹ lưỡng để tìm các mối đe dọa mới, tải lên tài nguyên hệ điều hành, và thời gian phân tích theo hành vi.

Để cấu hình việc sử dụng phân tích theo hành vi trong hoạt động của thành phần Bảo vệ mối đe dọa tập tin:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa tập tin**.
3. Nhấn vào **Thiết lập nâng cao**.
4. Nếu bạn muốn ứng dụng sử dụng tính năng phân tích hành vi để bảo vệ trước các mối đe dọa tập tin, hãy chọn hộp kiểm **Phân tích hành vi** trong mục **Phương pháp quét**. Sau đó sử dụng thanh trượt để đặt cấp độ phân tích theo hành vi: **Quét nhanh**, **Quét vừa** hoặc **Quét sâu**.
5. Lưu các thay đổi của bạn.

Sử dụng công nghệ quét trong hoạt động của thành phần Bảo vệ mối đe dọa tập tin

Để cấu hình việc sử dụng các công nghệ quét trong hoạt động của thành phần Bảo vệ mối đe dọa tập tin:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa tập tin**.
3. Nhấn vào **Thiết lập nâng cao**.
4. Trong mục **Công nghệ quét**, hãy chọn hộp kiểm cạnh tên của các công nghệ mà bạn muốn sử dụng bảo vệ mối đe dọa tập tin:
 - **Công nghệ iSwift**. Công nghệ này cho phép tăng tốc độ quét bằng cách loại trừ một số tập tin nhất định khỏi quá trình quét. Các tập tin được loại trừ khỏi quá trình quét bằng một thuật toán đặc biệt có tính đến ngày phát hành cơ sở dữ liệu Kaspersky Endpoint Security, ngày mà tập tin được quét lần cuối cùng và mọi thay đổi được thực hiện với thiết lập quét. Công nghệ iSwift được cải tiến từ công nghệ iChecker cho hệ thống tập tin NTFS.

- **Công nghệ iChecker.** Công nghệ này cho phép tăng tốc độ quét bằng cách loại trừ một số tập tin nhất định khỏi quá trình quét. Các tập tin được loại trừ khỏi quá trình quét bằng một thuật toán đặc biệt có tính đến ngày phát hành cơ sở dữ liệu Kaspersky Endpoint Security, ngày khi tập tin được quét lần cuối cùng và mọi thay đổi được thực hiện với thiết lập quét. Công nghệ iChecker có một số hạn chế: công nghệ này không hoạt động với tập tin lớn và chỉ áp dụng cho các tập tin có cấu trúc mà ứng dụng nhận dạng được (ví dụ như EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP và RAR).


5. Lưu các thay đổi của bạn.

Tối ưu quét tập tin

Bạn có thể tối ưu tác vụ quét tập tin của thành phần Bảo vệ mỗi đe dọa tập tin bằng cách 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.

Để tối ưu quét tập tin:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Bảo vệ mỗi đe dọa tập tin**.
3. Nhấn vào **Thiết lập nâng cao**.
4. Trong mục **Tối ưu hóa quét**, chọn hộp kiểm **Chỉ quét các tập tin mới và bị thay đổi**.
5. Lưu các thay đổi của bạn.


Quét các tập tin phức hợp

Một kỹ thuật phổ biến để che giấu virus và các phần mềm độc hại khác là nhúng chúng trong các tập tin hỗn 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.

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

Thành phần Bảo vệ mỗi đe dọa tập tin sẽ khử nhiễm các tập tin hỗn hợp trong định dạng ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR và ICE, và xóa các tập tin ở mọi định dạng khác (ngoại trừ cơ sở dữ liệu email).

Để thiết lập quét các tập tin hỗn hợp:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa tập tin**.
3. Nhấn vào **Thiết lập nâng cao**.
4. Trong mục **Quét các tập tin tổng hợp**, quy định loại tập tin hỗn hợp mà bạn muốn quét: tập nén, gói phân phối, hoặc tập tin trong định dạng văn bản.
5. Nếu tắt [chế độ chỉ quét các tập tin mới và được đổi](#), hãy cấu hình thiết lập để quét từng loại tập tin tổng hợp: quét tất cả các tập tin thuộc loại này hoặc chỉ các tập tin mới.
Nếu bật chế độ chỉ quét các tập tin mới và được thay đổi, Kaspersky Endpoint Security sẽ chỉ quét các tập tin mới và được thay đổi thuộc tất cả các loại tập tin hỗn hợp.
6. Cấu hình thiết lập nâng cao để quét các tập tin tổng hợp.

- **Không giải nén các tập tin phức hợp lớn.**

Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ không quét các tập tin hỗn hợp nếu dung lượng của chúng vượt quá giá trị được quy định.

Nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ quét các tập tin hỗn hợp thuộc mọi kích cỡ.

Kaspersky Endpoint Security sẽ quét các tập tin lớn được giải nén từ tập nén, bất kể là hộp kiểm **Không giải nén các tập tin phức hợp lớn** có được chọn hay không.

- **Giải nén các tập tin hỗn hợp trong nền.**

Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ cấp quyền truy cập vào các tập tin tổng hợp lớn hơn giá trị được chỉ định trước khi quét các tập tin này. Trong trường hợp này, Kaspersky Endpoint Security sẽ giải nén và quét các tập tin tổng hợp trong nền.

Kaspersky Endpoint Security sẽ chỉ cấp quyền truy cập vào các tập tin tổng hợp nhỏ hơn giá trị này sau khi giải nén và quét các tập tin này.

Nếu hộp kiểm này không được chọn, Kaspersky Endpoint Security sẽ chỉ cấp quyền truy cập vào các tập tin tổng hợp sau khi giải nén và quét các tập tin thuộc mọi kích thước.

7. Lưu các thay đổi của bạn.

Thay đổi chế độ quét

Chế độ quét nói đến điều kiện kích hoạt tác vụ quét tập tin bởi thành phần Bảo vệ mối đe dọa 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, thành phần Bảo vệ mối đe dọa 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. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .

2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa tập tin**.

3. Nhấn vào **Thiết lập nâng cao**.

4. Trong mục **Chế độ quét**, chọn chế độ cần thiết:

- **Chế độ thông minh.** Ở chế độ này, Bảo vệ mối đe dọa tập tin sẽ quét một đối tượng dựa trên phân tích về hành động đã thực hiện trên đối tượng. Ví dụ: khi làm việc với tài liệu Microsoft Office, 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.
- **Khi truy cập và sửa đổi.** Ở chế độ này, Bảo vệ mối đe dọa tập tin sẽ quét các đối tượng bất cứ khi nào các đối tượng đó được mở hoặc bị sửa đổi.
- **Khi truy cập.** Ở chế độ này, Bảo vệ mối đe dọa tập tin sẽ quét các đối tượng chỉ khi các đối tượng đó được mở.
- **Khi thực thi.** Ở chế độ này, Bảo vệ mối đe dọa tập tin sẽ chỉ quét đối tượng khi chúng được chạy.

5. Lưu các thay đổi của bạn.

Bảo vệ mối đe dọa web

Thành phần Bảo vệ mối đe dọa web ngăn các bản tải xuống tập tin độc hại từ mạng Internet và cũng chặn các website độc hại và lừa đảo. Thành phần này giúp bảo vệ máy tính với sự trợ giúp của cơ sở dữ liệu diệt virus, [dịch vụ đám mây của Kaspersky Security Network](#) và phân tích theo hành vi.

Kaspersky Endpoint Security sẽ quét lưu lượng HTTP, HTTPS và FTP. Kaspersky Endpoint Security sẽ quét các URL và địa chỉ IP. Bạn có thể [chỉ định các cổng mà Kaspersky Endpoint Security sẽ giám sát](#), hoặc chọn tất cả các cổng.

Để giám sát lưu lượng HTTPS, bạn cần [bật quét kết nối được mã hóa](#).

Khi người dùng cố gắng mở một website độc hại hoặc lừa đảo, Kaspersky Endpoint Security sẽ chặn truy cập và hiển thị cảnh báo (xem hình bên dưới).



Thông báo truy cập website bị từ chối

Bật và tắt Bảo vệ mối đe dọa web

Theo mặc định, thành phần Bảo vệ mối đe dọa web sẽ được bật và chạy trong chế độ được khuyến nghị bởi các chuyên gia của Kaspersky. Đối với thành phần Bảo vệ mối đe dọa web, Kaspersky Endpoint Security có thể áp dụng các nhóm thiết lập khác nhau. Các nhóm thiết lập được lưu trữ trong ứng dụng này được gọi là *mức độ bảo mật*: **Cao, Khuyến dùng, Thấp**. Thiết lập mức độ bảo mật lưu lượng web **Khuyến dùng** được coi là thiết lập tối ưu được khuyến nghị bởi các chuyên gia Kaspersky (xem bảng bên dưới). Bạn có thể chọn một trong nhiều mức 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 mức độ bảo mật tùy chỉnh cho lưu lượng web. Nếu bạn đã thay đổi cấu hình mức độ bảo mật lưu lượng web, bạn luôn có thể hoàn tác lại đến cấu hình mức độ bảo mật lưu lượng web được khuyến nghị.

Bạn chỉ có thể chọn hoặc cấu hình mức độ bảo mật trong Bảng điều khiển quản trị (MMC) hoặc trong giao diện cục bộ của ứng dụng. Bạn không thể chọn hoặc cấu hình mức độ bảo mật trong Bảng điều khiển web hoặc Bảng điều khiển đám mây.

[**Cách bật hoặc tắt thành phần Bảo vệ mối đe dọa web trong Bảng điều khiển quản trị \(MMC\)**](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Bảo vệ mỗi đe dọa web**.
6. Sử dụng hộp kiểm **Bảo vệ mỗi đe dọa web** để bật hoặc tắt thành phần.
7. Nếu bạn đã bật thành phần này, hãy thực hiện một trong các hành động sau trong mục **Mức độ bảo mật**:
 - Nếu bạn muốn áp dụng một trong những mức độ bảo mật được thiết lập sẵn, hãy chọn nó bằng thanh trượt:
 - **Cao**. Mức độ bảo mật mà theo đó thành phần Bảo vệ mỗi đe dọa web quét tối đa lưu lượng web mà máy tính tiếp nhận qua giao thức HTTP và FTP. Bảo vệ mỗi đe dọa web sẽ thực hiện quét chi tiết mọi đối tượng lưu lượng web, sử dụng toàn bộ các cơ sở dữ liệu ứng dụng, và thực hiện [phân tích theo hành vi](#) cấp sâu nhất.
 - **Khuyến dùng**. Mức độ bảo mật email mang đến sự cân bằng tối ưu giữa hiệu năng của Kaspersky Endpoint Security và bảo mật lưu lượng web. Thành phần Bảo vệ mỗi đe dọa web thực hiện phân tích theo hành vi ở cấp quét vừa. Mức độ bảo mật lưu lượng web này được khuyến khích bởi các chuyên gia Kaspersky. Các giá trị của thiết lập cho mức độ bảo mật khuyến nghị được cung cấp trong bảng bên dưới.
 - **Thấp**. Thiết lập của mức độ bảo mật lưu lượng web này đảm bảo tốc độ quét lưu lượng web tối đa. Thành phần Bảo vệ mỗi đe dọa web thực hiện phân tích theo hành vi ở cấp quét vừa.


Nếu bạn muốn cấu hình mức độ bảo mật tùy chỉnh, hãy nhấn nút **Thiết lập** và định nghĩa thiết lập thành phần của riêng bạn.

Bạn có thể khôi phục các giá trị của các mức độ bảo mật cài đặt sẵn bằng cách nhấn vào nút **Mặc định** trong mục **Mức độ bảo mật**.
8. Trong mục **Hành động khi phát hiện mỗi đe dọa**, chọn hành động được Kaspersky Endpoint Security thực hiện khi phát hiện các đối tượng lưu lượng web độc hại:
 - **Chặn tải về**. Nếu mục này được chọn và một đối tượng bị nhiễm mã độc được phát hiện trong lưu lượng web, thành phần Bảo vệ mỗi đe dọa web sẽ chặn truy cập vào đối tượng đó và hiển thị thông báo trong trình duyệt.
 - **Thông báo**. Nếu mục này được chọn và một đối tượng bị nhiễm mã độc được phát hiện trong lưu lượng web, Kaspersky Endpoint Security cho phép đối tượng này được tải xuống máy tính nhưng sẽ thêm thông tin về đối tượng bị nhiễm mã độc vào danh sách các mối đe dọa đang hoạt động.
9. Lưu các thay đổi của bạn.

[Cách bật hoặc tắt thành phần Bảo vệ mỗi đe dọa web trong Bảng điều khiển web và Bảng điều khiển đám mây](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Bảo vệ mỗi đe dọa thiết yếu** → **Bảo vệ mỗi đe dọa web**.
5. Sử dụng nút bật/tắt **Bảo vệ mỗi đe dọa web** để bật hoặc tắt thành phần.
6. Trong mục **Hành động khi phát hiện mỗi đe dọa**, chọn hành động được Kaspersky Endpoint Security thực hiện khi phát hiện các đối tượng lưu lượng web độc hại:
 - **Chặn tải về.** Nếu mục này được chọn và một đối tượng bị nhiễm mã độc được phát hiện trong lưu lượng web, thành phần Bảo vệ mỗi đe dọa web sẽ chặn truy cập vào đối tượng đó và hiển thị thông báo trong trình duyệt.
 - **Thông báo.** Nếu mục này được chọn và một đối tượng bị nhiễm mã độc được phát hiện trong lưu lượng web, Kaspersky Endpoint Security cho phép đối tượng này được tải xuống máy tính nhưng sẽ thêm thông tin về đối tượng bị nhiễm mã độc vào danh sách các mối đe dọa đang hoạt động.
7. Lưu các thay đổi của bạn.

[Cách bật hoặc tắt thành phần Bảo vệ mỗi đe dọa web](#)

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa web**.
3. Sử dụng nút bật/tắt **Bảo vệ mối đe dọa web** để bật hoặc tắt thành phần.
4. Nếu bạn đã bật thành phần này, hãy thực hiện một trong các hành động sau trong mục **Mức độ bảo mật**:
 - Nếu bạn muốn áp dụng một trong những mức độ bảo mật được thiết lập sẵn, hãy chọn nó bằng thanh trượt:
 - **Cao**. Mức độ bảo mật mà theo đó thành phần Bảo vệ mối đe dọa web quét tối đa lưu lượng web mà máy tính tiếp nhận qua giao thức HTTP và FTP. Bảo vệ mối đe dọa web sẽ thực hiện quét chi tiết mọi đối tượng lưu lượng web, sử dụng toàn bộ các cơ sở dữ liệu ứng dụng, và thực hiện [phân tích theo hành vi](#) cấp sâu nhất.
 - **Khuyến dùng**. Mức độ bảo mật email mang đến sự cân bằng tối ưu giữa hiệu năng của Kaspersky Endpoint Security và bảo mật lưu lượng web. Thành phần Bảo vệ mối đe dọa web thực hiện phân tích theo hành vi ở cấp quét vừa. Mức độ bảo mật lưu lượng web này được khuyến khích bởi các chuyên gia Kaspersky. Các giá trị của thiết lập cho mức độ bảo mật khuyến nghị được cung cấp trong bảng bên dưới.
 - **Thấp**. Thiết lập của mức độ bảo mật lưu lượng web này đảm bảo tốc độ quét lưu lượng web tối đa. Thành phần Bảo vệ mối đe dọa web thực hiện phân tích theo hành vi ở cấp quét vừa.
 - Nếu bạn muốn cấu hình mức độ bảo mật tùy chỉnh, hãy nhấn nút **Thiết lập nâng cao** và định nghĩa thiết lập thành phần của riêng bạn.
Bạn có thể khôi phục các giá trị mức độ bảo mật đặt trước bằng cách nhấn nút **Khôi phục cấp bảo mật được khuyến nghị** ở phần trên của cửa sổ.
5. Trong mục **Hành động khi phát hiện mối đe dọa**, chọn hành động được Kaspersky Endpoint Security thực hiện khi phát hiện các đối tượng lưu lượng web độc hại:
 - **Chặn tải về**. Nếu mục này được chọn và một đối tượng bị nhiễm mã độc được phát hiện trong lưu lượng web, thành phần Bảo vệ mối đe dọa web sẽ chặn truy cập vào đối tượng đó và hiển thị thông báo trong trình duyệt.
 - **Thông báo**. Nếu mục này được chọn và một đối tượng bị nhiễm mã độc được phát hiện trong lưu lượng web, Kaspersky Endpoint Security cho phép đối tượng này được tải xuống máy tính nhưng sẽ thêm thông tin về đối tượng bị nhiễm mã độc vào danh sách các mối đe dọa đang hoạt động.
6. Lưu các thay đổi của bạn.

Thiết lập Bảo vệ mối đe dọa web được các chuyên gia Kaspersky khuyến nghị (mức độ bảo mật được khuyến nghị)

Tham số	Giá trị	Mô tả
Kiểm tra địa chỉ web bằng cách đối chiếu với	Bật	Quét các liên kết để xác định xem chúng có được đưa vào trong cơ sở dữ liệu của các địa chỉ web độc hại hay không để cho phép bạn theo dõi các website đã được thêm vào danh sách không được phép. Cơ sở dữ liệu các địa chỉ web độc hại được duy trì bởi Kaspersky, được bao gồm trong gói cài đặt ứng

Cơ sở dữ liệu địa chỉ web độc hại		dụng và cập nhật trong quá trình cập nhật cơ sở dữ liệu của Kaspersky Endpoint Security.
Kiểm tra địa chỉ web bằng cách đối chiếu với cơ sở dữ liệu địa chỉ web lừa đảo	Bật	Cơ sở dữ liệu địa chỉ web lừa đảo bao gồm các địa chỉ website đã biết, thường được sử dụng để tạo các cuộc tấn công lừa đảo. Kaspersky bổ sung cho cơ sở dữ liệu về các liên kết lừa đảo này bằng các địa chỉ thu được từ tổ chức quốc tế có tên gọi là Tổ chức toàn cầu về chống lừa đảo trên mạng. Cơ sở dữ liệu các địa chỉ lừa đảo được bao gồm trong gói cài đặt ứng dụng và được bổ sung trong quá trình cập nhật cơ sở dữ liệu của Kaspersky Endpoint Security.
Sử dụng phân tích hành vi (Bảo vệ mỗi đe dọa web)	quét vừa	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. Khi lưu lượng web được quét virus và các ứng dụng khác có mối đe dọa, trình phân tích theo hành vi sẽ thực hiện các lệnh trong các tập tin thực thi. Số lượng các lệnh được thực thi bởi trình phân tích theo hành vi phụ thuộc vào cấp độ được chỉ định cho trình phân tích theo hành vi. Cấp độ Phân tích hành vi đảm bảo một sự cân bằng giữa việc quét kỹ lưỡng để tìm các mối đe dọa mới, tải lên tài nguyên hệ điều hành, và thời gian phân tích theo hành vi.
Sử dụng phân tích hành vi (Chống lừa đảo)	Bật	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.
Hành động khi phát hiện mối đe dọa	Chặn tải về	Nếu mục này được chọn và một đối tượng bị nhiễm mã độc được phát hiện trong lưu lượng web, thành phần Bảo vệ mỗi đe dọa web sẽ chặn truy cập vào đối tượng đó và hiển thị thông báo trong trình duyệt.

Cấu hình các phương pháp phát hiện địa chỉ web độc hại

Thành phần Bảo vệ mỗi đe dọa web phát hiện các địa chỉ web độc hại bằng cách sử dụng cơ sở dữ liệu chống virus, [dịch vụ đám mây Kaspersky Security Network](#) và phân tích hành vi.

Bạn chỉ có thể chọn các phương pháp phát hiện địa chỉ web độc hại trong Bảng điều khiển quản trị (MMC) hoặc trong giao diện cục bộ của ứng dụng. Bạn không thể chọn các phương pháp phát hiện địa chỉ web độc hại trong Bảng điều khiển web hoặc Bảng điều khiển đám mây. Tùy chọn mặc định là kiểm tra các địa chỉ web bằng cách đối chiếu với cơ sở dữ liệu của các địa chỉ độc hại thông qua phân tích hành vi (quét vừa).

Quét bằng cơ sở dữ liệu các địa chỉ độc hại


Quét các liên kết để xác định xem chúng có được đưa vào trong cơ sở dữ liệu của các địa chỉ web độc hại hay không để cho phép bạn theo dõi các website đã được thêm vào danh sách không được phép. Cơ sở dữ liệu các địa chỉ web độc hại được duy trì bởi Kaspersky, được bao gồm trong gói cài đặt ứng dụng và cập nhật trong quá trình cập nhật cơ sở dữ liệu của Kaspersky Endpoint Security.

Kaspersky Endpoint sẽ quét tất cả các liên kết để xác định xem chúng có được liệt kê trong cơ sở dữ liệu các địa chỉ web độc hại hay không. Thiết lập [quét kết nối bảo mật của ứng dụng](#) không ảnh hưởng đến chức năng quét liên kết. Nói cách khác, nếu quét kết nối được mã hóa bị tắt, Kaspersky Endpoint Security sẽ kiểm tra các liên kết bằng cách đối chiếu với cơ sở dữ liệu các địa chỉ web độc hại ngay cả khi lưu lượng mạng được truyền qua kết nối được mã hóa.

Cách bật hoặc tắt tính năng kiểm tra địa chỉ web bằng cách đối chiếu với cơ sở dữ liệu địa chỉ web độc hại thông qua Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Bảo vệ mỗi đe dọa web**.
6. Trong mục **Mức độ bảo mật**, hãy nhấn nút **Thiết lập**.
7. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, trong mục **Phương pháp quét**, hãy chọn hoặc xóa hộp kiểm **Kiểm tra địa chỉ web bằng cách đối chiếu với cơ sở dữ liệu địa chỉ web độc hại** để bật hoặc tắt tính năng kiểm tra địa chỉ bằng cách đối chiếu với cơ sở dữ liệu của các địa chỉ web độc hại.
8. Lưu các thay đổi của bạn.

Cách bật hoặc tắt tính năng kiểm tra địa chỉ bằng cách đối chiếu với cơ sở dữ liệu địa chỉ độc hại trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Bảo vệ mỗi đe dọa web**.
3. Nhấn vào **Thiết lập nâng cao**.
4. Trong mục **Phương pháp quét**, hãy chọn hoặc xóa hộp kiểm **Kiểm tra địa chỉ web bằng cách đối chiếu với cơ sở dữ liệu địa chỉ web độc hại** để bật hoặc tắt tính năng kiểm tra địa chỉ bằng cách đối chiếu với cơ sở dữ liệu của các địa chỉ web độc hại.
5. Lưu các thay đổi của bạn.

Phân tích hành vi

Trong phân tích hành vi, Kaspersky Endpoint Security sẽ phân tích hoạt động của các ứng dụng trong hệ điều hành. Phân tích hành vi có thể phát hiện các mối đe dọa chưa có hồ sơ trong cơ sở dữ liệu của Kaspersky Endpoint Security.

Khi lưu lượng web được quét virus và các ứng dụng khác có mối đe dọa, trình phân tích theo hành vi sẽ thực hiện các lệnh trong các tập tin thực thi. Số lượng các lệnh được thực thi bởi trình phân tích theo hành vi phụ thuộc vào cấp độ được chỉ định cho trình phân tích theo hành vi. Cấp độ Phân tích hành vi đảm bảo một sự cân bằng giữa việc quét kỹ lưỡng để tìm các mối đe dọa mới, tải lên tài nguyên hệ điều hành, và thời gian phân tích theo hành vi.


Cách bật hoặc tắt phân tích hành vi trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa web**.
6. Trong mục **Mức độ bảo mật**, hãy nhấn nút **Thiết lập**.
7. Trong mục **Phương pháp quét**, hãy chọn hộp kiểm **Sử dụng phân tích hành vi** nếu bạn muốn ứng dụng sử dụng phân tích hành vi khi quét lưu lượng web để tìm virus và phần mềm độc hại khác.
8. Sử dụng thanh trượt để đặt cấp độ phân tích theo hành vi: **Quét nhanh**, **Quét vừa** hoặc **Quét sâu**.

Khi lưu lượng web được quét virus và các ứng dụng khác có mối đe dọa, trình phân tích theo hành vi sẽ thực hiện các lệnh trong các tập tin thực thi. Số lượng các lệnh được thực thi bởi trình phân tích theo hành vi phụ thuộc vào cấp độ được chỉ định cho trình phân tích theo hành vi. Cấp độ Phân tích hành vi đảm bảo một sự cân bằng giữa việc quét kỹ lưỡng để tìm các mối đe dọa mới, tải lên tài nguyên hệ điều hành, và thời gian phân tích theo hành vi.

9. Lưu các thay đổi của bạn.

Cách bật hoặc tắt sử dụng phân tích hành vi trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa web**.
3. Nhấn vào **Thiết lập nâng cao**.
4. Trong mục **Phương pháp quét**, hãy chọn hộp kiểm **Sử dụng phân tích hành vi** nếu bạn muốn ứng dụng sử dụng phân tích hành vi khi quét lưu lượng web để tìm virus và phần mềm độc hại khác.

Khi lưu lượng web được quét virus và các ứng dụng khác có mối đe dọa, trình phân tích theo hành vi sẽ thực hiện các lệnh trong các tập tin thực thi. Số lượng các lệnh được thực thi bởi trình phân tích theo hành vi phụ thuộc vào cấp độ được chỉ định cho trình phân tích theo hành vi. Cấp độ Phân tích hành vi đảm bảo một sự cân bằng giữa việc quét kỹ lưỡng để tìm các mối đe dọa mới, tải lên tài nguyên hệ điều hành, và thời gian phân tích theo hành vi.
5. Lưu các thay đổi của bạn.

Chống lừa đảo

Thành phần Bảo vệ mối đe dọa web sẽ kiểm tra các liên kết để xem chúng có thuộc địa chỉ web lừa đảo hay không. Điều này giúp ngăn các *cuộc tấn công lừa đảo*. Một cuộc tấn công lừa đảo có thể bị che giấu, chẳng hạn như dưới dạng một email được cho là 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 trình tin nhắn, thành phần Bảo vệ mối đe dọa web sẽ giám sát mọi nỗ lực truy cập một website lừa đảo trên cấp độ quét 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.

Bạn chỉ có thể cấu hình thành phần Chống lừa đảo trong Bảng điều khiển quản trị (MMC) hoặc giao diện cục bộ của ứng dụng. Bạn không thể cấu hình thành phần Chống lừa đảo trong Bảng điều khiển web hoặc Bảng điều khiển đám mây. Theo mặc định, thành phần Chống lừa đảo được bật cùng phân tích hành vi.

[Cách bật hoặc tắt thành phần Chống lừa đảo trong Bảng điều khiển quản trị \(MMC\)](#) 


1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Bảo vệ mỗi đe dọa web**.
6. Trong mục **Mức độ bảo mật**, hãy nhấn nút **Thiết lập**.
7. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, trong mục **Thiết lập Chống lừa đảo**, hãy chọn hoặc xóa hộp kiểm **Kiểm tra địa chỉ web bằng cách đối chiếu với cơ sở dữ liệu địa chỉ web lừa đảo** để bật hoặc tắt Chống lừa đảo.

Cơ sở dữ liệu địa chỉ web lừa đảo bao gồm các địa chỉ website đã biết, thường được sử dụng để tạo các cuộc tấn công lừa đảo. Kaspersky bổ sung cho cơ sở dữ liệu về các liên kết lừa đảo này bằng các địa chỉ thu được từ tổ chức quốc tế có tên gọi là Tổ chức toàn cầu về chống lừa đảo trên mạng. Cơ sở dữ liệu các địa chỉ lừa đảo được bao gồm trong gói cài đặt ứng dụng và được bổ sung trong quá trình cập nhật cơ sở dữ liệu của Kaspersky Endpoint Security.
8. Hãy chọn hộp kiểm **Sử dụng phân tích hành vi** nếu bạn muốn ứng dụng sử dụng phân tích hành vi khi quét các trang web để tìm liên kết lừa đảo.

Trong phân tích hành vi, Kaspersky Endpoint Security sẽ phân tích hoạt động của các ứng dụng trong hệ điều hành. Phân tích hành vi có thể phát hiện các mối đe dọa chưa có hồ sơ trong cơ sở dữ liệu của Kaspersky Endpoint Security.

Để quét các liên kết, ngoài cơ sở dữ liệu chống virus và phân tích hành vi, bạn có thể sử dụng cơ sở dữ liệu danh tiếng của [Kaspersky Security Network](#).
9. Lưu các thay đổi của bạn.

[Cách bật hoặc tắt thành phần Chống lừa đảo trong giao diện ứng dụng](#)

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa web**.
3. Nhấn vào **Thiết lập nâng cao**.
4. Nếu bạn muốn thành phần Bảo vệ mối đe dọa web kiểm tra các liên kết bằng cách đối chiếu với cơ sở dữ liệu các địa chỉ web lừa đảo, hãy chọn hộp kiểm **Kiểm tra địa chỉ web bằng cách đối chiếu với cơ sở dữ liệu địa chỉ web lừa đảo** trong mục **Chống lừa đảo**. Cơ sở dữ liệu địa chỉ web lừa đảo bao gồm các địa chỉ website đã biết, thường được sử dụng để tạo các cuộc tấn công lừa đảo. Kaspersky bổ sung cho cơ sở dữ liệu về các liên kết lừa đảo này bằng các địa chỉ thu được từ tổ chức quốc tế có tên gọi là Tổ chức toàn cầu về chống lừa đảo trên mạng. Cơ sở dữ liệu các địa chỉ lừa đảo được bao gồm trong gói cài đặt ứng dụng và được bổ sung trong quá trình cập nhật cơ sở dữ liệu của Kaspersky Endpoint Security.
5. Hãy chọn hộp kiểm **Sử dụng phân tích hành vi** nếu bạn muốn ứng dụng sử dụng phân tích hành vi khi quét các trang web để tìm liên kết lừa đảo.

Trong phân tích hành vi, Kaspersky Endpoint Security sẽ phân tích hoạt động của các ứng dụng trong hệ điều hành. Phân tích hành vi có thể phát hiện các mối đe dọa chưa có hồ sơ trong cơ sở dữ liệu của Kaspersky Endpoint Security.

Để quét các liên kết, ngoài cơ sở dữ liệu chống virus và phân tích hành vi, bạn có thể sử dụng cơ sở dữ liệu danh tiếng của [Kaspersky Security Network](#).
6. Lưu các thay đổi của bạn.

Tạo danh sách các địa chỉ web được tin tưởng

Ngoài các trang web độc hại và lừa đảo, thành phần Bảo vệ mối đe dọa web còn có thể chặn các trang web khác. Ví dụ: Bảo vệ mối đe dọa web sẽ chặn lưu lượng HTTP không đáp ứng các tiêu chuẩn RFC. Bạn có thể tạo ra một danh sách các URL có nội dung mà bạn tin tưởng. Thành phần Bảo vệ mối đe dọa web sẽ không phân tích thông tin từ các địa chỉ web được tin tưởng để phát hiện virus và các mối đe dọa khác. Tùy chọn này có thể hữu ích, chẳng hạn như khi thành phần Bảo vệ mối đe dọa 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.


[Cách thêm địa chỉ web được tin tưởng trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Bảo vệ mỗi đe dọa web**.
6. Trong mục **Mức độ bảo mật**, hãy nhấn nút **Thiết lập**.
7. Trong cửa sổ mở ra, hãy chọn thẻ **Địa chỉ web được tin tưởng**.
8. Chọn hộp kiểm **Không quét lưu lượng web từ liên kết tin tưởng**.
Nếu hộp kiểm này được chọn, thành phần Bảo vệ mỗi đe dọa web sẽ không quét nội dung của các trang web hoặc website có địa chỉ nằm trong danh sách các địa chỉ web được tin tưởng. Bạn có thể thêm cả địa chỉ cụ thể và địa chỉ đại diện của một trang web / website vào danh sách các địa chỉ web được tin tưởng.
9. Tạo một danh sách các URL / trang web có nội dung mà bạn tin tưởng.
Kaspersky Endpoint Security hỗ trợ các ký tự * và ? khi nhập tên đại diện.
Bạn cũng có thể [nhập danh sách địa chỉ web được tin tưởng từ tập tin XML](#).
10. Lưu các thay đổi của bạn.

[Cách thêm địa chỉ web được tin tưởng trong Bảng điều khiển web và Bảng điều khiển đám mây](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa web**.
5. Trong mục **Địa chỉ web được tin tưởng**, hãy chọn hộp kiểm **Không quét lưu lượng web từ các địa chỉ web được tin tưởng**.
Nếu hộp kiểm này được chọn, thành phần Bảo vệ mối đe dọa web sẽ không quét nội dung của các trang web hoặc website có địa chỉ nằm trong danh sách các địa chỉ web được tin tưởng. Bạn có thể thêm cả địa chỉ cụ thể và địa chỉ đại diện của một trang web / website vào danh sách các địa chỉ web được tin tưởng.
6. Tạo một danh sách các URL / trang web có nội dung mà bạn tin tưởng.
Kaspersky Endpoint Security hỗ trợ các ký tự * và ? khi nhập tên đại diện.
Bạn cũng có thể [nhập danh sách địa chỉ web được tin tưởng từ tập tin XML](#).
7. Lưu các thay đổi của bạn.

Cách thêm địa chỉ web được tin tưởng trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa web**.
3. Nhấn vào **Thiết lập nâng cao**.
4. Chọn hộp kiểm **Không quét lưu lượng web từ liên kết tin tưởng**.
Nếu hộp kiểm này được chọn, thành phần Bảo vệ mối đe dọa web sẽ không quét nội dung của các trang web hoặc website có địa chỉ nằm trong danh sách các địa chỉ web được tin tưởng. Bạn có thể thêm cả địa chỉ cụ thể và địa chỉ đại diện của một trang web / website vào danh sách các địa chỉ web được tin tưởng.
5. Tạo một danh sách các URL / trang web có nội dung mà bạn tin tưởng.
Kaspersky Endpoint Security hỗ trợ các ký tự * và ? khi nhập tên đại diện.
Bạn cũng có thể [nhập danh sách địa chỉ web được tin tưởng từ tập tin XML](#).
6. Lưu các thay đổi của bạn.

Do đó, thành phần Bảo vệ mối đe dọa web sẽ không quét lưu lượng truy cập của các địa chỉ web được tin tưởng. Người dùng luôn có thể mở một trang web được tin tưởng và tải xuống tập tin từ trang web đó. Nếu bạn không thể truy cập vào trang web đó, hãy kiểm tra thiết lập của các thành phần [Quét kết nối được mã hóa](#), [Kiểm soát web](#) và [Giám sát cổng mạng](#). Nếu Kaspersky Endpoint Security coi một tập tin được tải xuống từ một trang web được tin tưởng là tập tin độc hại thì bạn có thể [thêm tập tin này vào loại trừ](#).

Bạn cũng có thể [tạo danh sách loại trừ chung cho các kết nối được mã hóa](#). Trong trường hợp này, Kaspersky Endpoint Security sẽ không quét lưu lượng HTTPS của các địa chỉ web được tin tưởng khi các thành phần Bảo vệ mỗi đe dọa web, Bảo vệ mỗi đe dọa thư điện tử, Kiểm soát web đang hoạt động.

Xuất và nhập danh sách địa chỉ web được tin tưởng

Bạn có thể xuất danh sách địa chỉ web được tin tưởng vào một tập tin XML. Sau đó, bạn có thể sửa đổi tập tin, ví dụ như thêm một số lượng lớn các địa chỉ web cùng loại. Bạn cũng có thể sử dụng chức năng xuất/nhập để sao lưu danh sách địa chỉ web được tin tưởng hoặc để chuyển danh sách sang máy chủ khác.

[Cách xuất và nhập danh sách địa chỉ web được tin tưởng trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Bảo vệ mỗi đe dọa web**.
6. Trong mục **Mức độ bảo mật**, hãy nhấn nút **Thiết lập**.
7. Trong cửa sổ mở ra, hãy chọn thẻ **Địa chỉ web được tin tưởng**.
8. Để xuất danh sách địa chỉ web được tin tưởng:
 - a. Chọn địa chỉ web được tin tưởng mà bạn muốn xuất. Để chọn nhiều cổng, hãy sử dụng phím **CTRL** hoặc **SHIFT**.

Nếu bạn không chọn địa chỉ được tin tưởng nào, Kaspersky Endpoint Security sẽ xuất tất cả các địa chỉ web.
 - b. Nhấn liên kết **Xuất**.
 - c. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin XML mà bạn muốn xuất danh sách các địa chỉ web được tin tưởng vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
 - d. Lưu tập tin.

Kaspersky Endpoint Security sẽ xuất toàn bộ danh sách địa chỉ web được tin tưởng vào tập tin XML.
9. Để nhập danh sách địa chỉ được tin tưởng:
 - a. Nhấn liên kết **Nhập**.

Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách địa chỉ được tin tưởng.
 - b. Mở tập tin.

Nếu máy tính đã có danh sách địa chỉ được tin tưởng, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.
10. Lưu các thay đổi của bạn.

[Cách xuất và nhập danh sách địa chỉ web được tin tưởng trong Bảng điều khiển web và Bảng điều khiển đám mây](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa web**.
5. Để xuất danh sách loại trừ trong mục **Địa chỉ web được tin tưởng**:
 - a. Chọn địa chỉ web được tin tưởng mà bạn muốn xuất.
 - b. Nhấn liên kết **Xuất**.
 - c. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin XML mà bạn muốn xuất danh sách các địa chỉ web được tin tưởng vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
 - d. Lưu tập tin.
Kaspersky Endpoint Security sẽ xuất toàn bộ danh sách địa chỉ web được tin tưởng vào tập tin XML.
6. Để nhập danh sách loại trừ trong mục **Địa chỉ web được tin tưởng**:
 - a. Nhấn liên kết **Nhập**.
Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách địa chỉ được tin tưởng.
 - b. Mở tập tin.
Nếu máy tính đã có danh sách địa chỉ được tin tưởng, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.
7. Lưu các thay đổi của bạn.

Bảo vệ mối đe dọa thư điện tử

Thành phần Bảo vệ mối đe dọa thư điện tử sẽ quét các tập tin đính kèm của email đến và đi để phát hiện virus và các mối đe dọa khác. Thành phần này giúp bảo vệ máy tính với sự trợ giúp của cơ sở dữ liệu diệt virus, [dịch vụ đám mây của Kaspersky Security Network](#) và phân tích theo hành vi.

Bảo vệ mối đe dọa thư điện tử có thể quét cả thư đến và thư đi. Ứng dụng này hỗ trợ POP3, SMTP, IMAP và NNTP trong các ứng dụng thư điện tử sau:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Microsoft Outlook Express
- Windows Mail

Bảo vệ mối đe dọa thư điện tử không hỗ trợ các giao thức và ứng dụng thư điện tử khác.

Bảo vệ mối đe dọa thư điện tử có thể không phải lúc nào cũng có được quyền truy cập *cấp độ giao thức* vào thư (ví dụ: khi sử dụng giải pháp Microsoft Exchange). Do đó, Bảo vệ mối đe dọa thư điện tử có một [phần mở rộng cho Microsoft Office Outlook](#). Phần mở rộng này cho phép quét thư ở *cấp độ của ứng dụng thư điện tử*. Phần mở rộng Bảo vệ mối đe dọa thư điện tử hỗ trợ hoạt động với Outlook 2010, 2013, 2016 và 2019.


Thành phần Bảo vệ mối đe dọa thư điện tử không quét thư nếu ứng dụng thư khách được mở trong trình duyệt.

Khi phát hiện tập tin độc hại trong tập tin đính kèm, Kaspersky Endpoint Security sẽ đổi tên chủ đề thư như sau: [Việc xử lý thư cần sự tham gia của bạn] <chủ đề thư> hoặc [Thư đã được xử lý] <chủ đề thư>.

Bật và tắt Bảo vệ mối đe dọa thư điện tử

Theo mặc định, thành phần Bảo vệ mối đe dọa thư điện tử sẽ được bật và chạy trong chế độ được khuyến nghị bởi các chuyên gia của Kaspersky. Đối với thành phần Bảo vệ mối đe dọa thư điện tử, Kaspersky Endpoint Security sẽ áp dụng các nhóm thiết lập khác nhau. Các nhóm thiết lập được lưu trữ trong ứng dụng này được gọi là *mức độ bảo mật*: **Cao, Khuyến dùng, Thấp**. Thiết lập mức độ bảo mật thư điện tử **Khuyến dùng** được coi là thiết lập tối ưu được khuyến nghị bởi các chuyên gia Kaspersky (xem bảng bên dưới). Bạn có thể chọn một trong các mức độ bảo mật email được thiết lập sẵn hoặc thiết lập một mức độ bảo mật email tùy chỉnh. Nếu bạn đã thay đổi cấu hình mức độ bảo mật email, bạn luôn có thể hoàn tác lại đến cấu hình mức độ bảo mật email được khuyến nghị.

Để bật hoặc tắt thành phần Bảo vệ mối đe dọa thư điện tử:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa thư điện tử**.
3. Sử dụng nút bật/tắt **Bảo vệ mối đe dọa thư điện tử** để bật hoặc tắt thành phần.
4. Nếu bạn đã bật thành phần này, hãy thực hiện một trong các hành động sau trong mục **Mức độ bảo mật**:
 - Nếu bạn muốn áp dụng một trong những mức độ bảo mật được thiết lập sẵn, hãy chọn nó bằng thanh trượt:
 - **Cao**. Khi mức độ bảo mật email này được chọn, thành phần Bảo vệ mối đe dọa thư điện tử sẽ quét kỹ các email. Thành phần Bảo vệ mối đe dọa thư điện tử sẽ quét các email đến và đi, đồng thời tiến hành phân tích theo hành vi mức độ sâu. Mức độ bảo mật thư điện tử Cao được khuyến nghị cho các môi trường có nguy cơ cao. Một ví dụ về một môi trường như vậy là một kết nối đến một dịch vụ thư điện tử miễn phí từ một mạng gia đình mà không được bảo vệ bởi bảo vệ thư điện tử.
 - **Khuyến dùng**. Mức độ bảo mật email mang đến sự cân bằng tối ưu giữa hiệu năng của Kaspersky Endpoint Security và bảo mật email. Thành phần Bảo vệ mối đe dọa thư điện tử sẽ quét các email đến và đi, đồng thời tiến hành phân tích theo hành vi mức độ trung bình. Mức độ bảo mật lưu lượng email này được khuyến khích bởi các chuyên gia Kaspersky. Các giá trị của thiết lập cho mức độ bảo mật khuyến nghị được cung cấp trong bảng bên dưới.

- **Thấp.** Khi mức độ bảo mật email này được chọn, thành phần Bảo vệ mối đe dọa thư điện tử sẽ chỉ quét các email đến, thực hiện phân tích theo hành vi nhanh và không quét các tập nén đính kèm email. Ở mức độ bảo mật email này, thành phần Bảo vệ mối đe dọa thư điện tử sẽ quét tất cả email ở tốc độ tối đa và sử dụng mức tài nguyên hệ điều hành tối thiểu. Mức độ bảo mật email Thấp được khuyến nghị sử dụng ở các môi trường bảo mật tốt. Một ví dụ về môi trường như vậy có thể là một mạng LAN doanh nghiệp có hệ thống bảo mật email tập trung.
- Nếu bạn muốn cấu hình mức độ bảo mật tùy chỉnh, hãy nhấn nút **Thiết lập nâng cao** và định nghĩa thiết lập thành phần của riêng bạn.
Bạn có thể khôi phục các giá trị mức độ bảo mật đặt trước bằng cách nhấn nút **Khôi phục cấp bảo mật được khuyến nghị** ở phần trên của cửa sổ.

5. Lưu các thay đổi của bạn.

Thiết lập Bảo vệ mối đe dọa thư điện tử được các chuyên gia Kaspersky khuyến nghị (cấp độ bảo mật được khuyến nghị)


Tham số	Giá trị	Mô tả
Phạm vi bảo vệ	Tin nhắn đến và đi	<i>Phạm vi bảo vệ</i> bao gồm các đối tượng được thành phần kiểm tra khi nó được chạy: tin nhắn đến và đi hoặc chỉ tin nhắn gửi đến. Để bảo vệ máy tính của mình, bạn chỉ cần quét các thư đến. Bạn có thể bật quét các thư đi để ngăn các tập tin bị nhiễm được gửi trong các tập tin nén. Bạn cũng có thể bật quét các thư đi nếu bạn muốn ngăn các tập tin ở các định dạng cụ thể được gửi, chẳng hạn như các tập tin âm thanh và video chẳng hạn.
Kết nối phần mở rộng Microsoft Outlook	Bật	Nếu hộp kiểm này được chọn, tính năng quét các email được truyền tải qua giao thức POP3, SMTP, NNTP, IMAP sẽ được bật cho từ phía tiện ích mở rộng tích hợp vào Microsoft Outlook. Nếu thư điện tử được quét bằng phần mở rộng dành cho Microsoft Outlook, bạn nên sử dụng Chế độ Exchange đã lưu trong Bộ đệm ẩn. Để biết thêm chi tiết về Cached Exchange Mode và khuyến nghị về việc sử dụng của nó, vui lòng tham khảo Cơ sở tri thức của Microsoft .
Quét các tập tin nén đính kèm	Bật	Quét định dạng ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE, và các định dạng tập tin nén khác. Kaspersky Endpoint Security quét các tập tin nén không chỉ theo phần mở rộng mà còn theo định dạng.
Quét các tập tin đính kèm có định dạng Microsoft Office	Bật	Quét các tập tin Microsoft Office (DOC, DOCX, XLS, PPT và đuôi mở rộng khác của Microsoft). Các tập tin định dạng Office cũng bao gồm các đối tượng OLE.
Lọc tập tin đính kèm	Đổi tên tập tin nén đính kèm của loại đã chọn	Nếu tùy chọn này được chọn, Bảo vệ mối đe dọa thư điện tử sẽ thay thế ký tự cuối cùng của đuôi mở rộng được tìm thấy trong các tập tin đính kèm của các loại được chỉ định bằng ký tự gạch dưới (ví dụ: <code>tattachment.doc_</code>). Vì vậy, để mở tập tin này, người dùng phải đổi tên tập tin.
Phân tích hành vi	quét vừa	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

		<p>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.</p> <p>Khi quét các tập tin để tìm mã độc, trình phân tích theo hành vi sẽ thực thi các lệnh trong các tập tin thực thi. Số lượng các lệnh được thực thi bởi trình phân tích theo hành vi phụ thuộc vào cấp độ được chỉ định cho trình phân tích theo hành vi. Cấp độ Phân tích hành vi đảm bảo một sự cân bằng giữa việc quét kỹ lưỡng để tìm các mối đe dọa mới, tải lên tài nguyên hệ điều hành, và thời gian phân tích theo hành vi.</p>
Hành động khi phát hiện mối đe dọa	Khử mã độc; xóa nếu không thể khử mã độc	<p>Khi phát hiện một đối tượng bị nhiễm mã độc trong một thư được gửi đến hoặc thư được gửi đi, Kaspersky Endpoint Security sẽ cố gắng khử mã độc đối tượng được phát hiện. Người dùng có thể truy cập thư có tập tin đính kèm an toàn. Nếu không thể khử mã độc đối tượng, Kaspersky Endpoint Security sẽ xóa đối tượng bị nhiễm. Kaspersky Endpoint Security sẽ thêm thông tin về hành động được thực hiện vào chủ đề thư: [Thư đã được xử lý] <chủ đề thư>.</p>

Thay đổi hành động xử lý các email bị nhiễm

Theo mặc định, thành phần Bảo vệ mối đe dọa thư điện tử sẽ tự động khử nhiễm tất cả các email bị nhiễm mã độc được phát hiện. Nếu khử mã độc thất bại, thành phần Bảo vệ mối đe dọa thư điện tử sẽ xóa các email bị nhiễm mã độc.

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

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa thư điện tử**.
3. Trong mục **Hành động khi phát hiện mối đe dọa**, chọn hành động mà Kaspersky Endpoint Security sẽ thực hiện khi phát hiện một email bị nhiễm:
 - **Khử mã độc; xóa nếu không thể khử mã độc.** Khi phát hiện một đối tượng bị nhiễm mã độc trong một thư được gửi đến hoặc thư được gửi đi, Kaspersky Endpoint Security sẽ cố gắng khử mã độc đối tượng được phát hiện. Người dùng có thể truy cập thư có tập tin đính kèm an toàn. Nếu không thể khử mã độc đối tượng, Kaspersky Endpoint Security sẽ xóa đối tượng bị nhiễm. Kaspersky Endpoint Security sẽ thêm thông tin về hành động được thực hiện vào chủ đề thư: [Thư đã được xử lý] <chủ đề thư>.
 - **Khử mã độc; chặn nếu không thể khử mã độc.** Khi phát hiện một đối tượng bị nhiễm mã độc trong một thư được gửi đến, Kaspersky Endpoint Security sẽ cố gắng khử mã độc đối tượng được phát hiện. Người dùng có thể truy cập thư có tập tin đính kèm an toàn. Nếu không thể khử mã độc đối tượng, Kaspersky Endpoint Security sẽ thêm cảnh báo vào chủ đề thư: [Việc xử lý thư cần sự tham gia của bạn] <chủ đề thư>. Người dùng có thể truy cập thư có tập tin đính kèm ban đầu. Khi phát hiện một đối tượng bị nhiễm mã độc trong một thư được gửi đi, Kaspersky Endpoint Security sẽ cố gắng khử mã độc đối tượng được phát hiện. Nếu không thể khử mã độc đối tượng, Kaspersky Endpoint Security sẽ chặn việc gửi thư và ứng dụng thư điện tử sẽ hiển thị lỗi.
 - **Chặn.** Nếu phát hiện một đối tượng bị nhiễm mã độc trong thư được gửi đến, Kaspersky Endpoint Security sẽ thêm cảnh báo vào chủ đề thư: [Việc xử lý thư cần sự tham gia của bạn] <chủ


đề thư>. Người dùng có thể truy cập thư có tập tin đính kèm ban đầu. Nếu phát hiện một đối tượng bị nhiễm mã độc trong thư được gửi đi, Kaspersky Endpoint Security sẽ chặn gửi thư và ứng dụng thư điện tử sẽ hiển thị lỗi.

4. Lưu các thay đổi của bạn.

Cấu hình phạm vi bảo vệ của thành phần Bảo vệ mỗi đe dọa thư điện tử

Phạm vi bảo vệ chỉ 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. Các thuộc tính của phạm vi bảo vệ của thành phần Bảo vệ mỗi đe dọa thư điện tử bao gồm các thiết lập để tích hợp thành phần Bảo vệ mỗi đe dọa thư điện tử vào các trình khách email, và loại email và giao thức email có lưu lượng được quét bởi thành phần Bảo vệ mỗi đe dọa 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 thiết lập phạm vi bảo vệ của thành phần Bảo vệ mỗi đe dọa thư điện tử:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Bảo vệ mỗi đe dọa thư điện tử**.
3. Nhấn vào **Thiết lập nâng cao**.
4. Trong mục **Phạm vi bảo vệ**, hãy chọn thư để quét:
 - **Tin nhắn đến và đi.**
 - **Chỉ tin nhắn gửi đến.**

Để bảo vệ máy tính của mình, bạn chỉ cần quét các thư đến. Bạn có thể bật quét các thư đi để ngăn các tập tin bị nhiễm được gửi trong các tập tin nén. Bạn cũng có thể bật quét các thư đi nếu bạn muốn ngăn các tập tin ở các định dạng cụ thể được gửi, chẳng hạn như các tập tin âm thanh và video chẳng hạn.

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.

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

- Nếu bạn muốn thành phần Bảo vệ mỗi đe dọa thư điện tử quét các email được truyền qua các giao thức POP3, SMTP, NNTP, và IMAP trước khi chúng đến máy tính của người dùng, hãy chọn hộp kiểm **Quét lưu lượng POP3, SMTP, NNTP, và IMAP**.

Nếu bạn không muốn thành phần Bảo vệ mối đe dọa thư điện tử quét các email được truyền qua các giao thức POP3, SMTP, NNTP và IMAP trước khi chúng đến máy tính của người dùng, hãy xóa hộp kiểm **Quét lưu lượng POP3, SMTP, NNTP, và IMAP**. Trong trường hợp này, các email sẽ được quét bởi tiện ích mở rộng Bảo vệ mối đe dọa 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 **Kết nối phần mở rộng Microsoft Outlook** được chọn.

Nếu bạn sử dụng ứng dụng thư điện tử không phải là Microsoft Office Outlook thì thành phần Bảo vệ mối đe dọa thư điện tử sẽ không quét các thư được truyền qua các giao thức POP3, SMTP, NNTP và IMAP khi **Quét lưu lượng POP3, SMTP, NNTP, và IMAP** hộp kiểm không được chọn.

- Nếu bạn muốn cho phép truy cập đến thiết lập của thành phần Bảo vệ mối đe dọa 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 tiện ích mở rộng được nhúng vào Microsoft Office Outlook, hãy chọn hộp kiểm **Kết nối phần mở rộng Microsoft Outlook**.
Nếu bạn muốn chặn truy cập đến thiết lập của thành phần Bảo vệ mối đe dọa 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 tiện ích mở rộng được nhúng vào Microsoft Office Outlook, hãy xóa hộp kiểm **Kết nối phần mở rộng Microsoft Outlook**.


Tiện ích mở rộng Bảo vệ mối đe dọa thư điện tử sẽ được nhúng trong ứng dụng Microsoft Office Outlook trong quá trình cài đặt Kaspersky Endpoint Security.

6. Lưu các thay đổi của bạn.

Quét các tập tin phức 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.

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

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa thư điện tử**.
3. Nhấn vào **Thiết lập nâng cao**.
4. Trong mục **Quét các tập tin tổng hợp**, hãy cấu hình thiết lập quét:
 - **Quét các tập tin đính kèm có định dạng Microsoft Office**. Quét các tập tin Microsoft Office (DOC, DOCX, XLS, PPT và đuôi mở rộng khác của Microsoft). Các tập tin định dạng Office cũng bao gồm các đối tượng OLE.
 - **Quét các tập tin nén đính kèm**. Quét định dạng ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE, và các định dạng tập tin nén khác. Kaspersky Endpoint Security quét các tập tin nén không chỉ theo phần mở rộng mà còn theo định dạng.

Nếu trong quá trình quét, Kaspersky Endpoint Security phát hiện mật khẩu cho một tập tin nén trong văn bản của tin nhắn, mật khẩu này sẽ được sử dụng để quét nội dung của tập tin nén để tìm các ứng dụng độc hại. Trong trường hợp này, mật khẩu không được lưu lại. Một tập tin nén được giải nén trong quá trình quét. Nếu xảy ra lỗi ứng dụng trong quá trình giải nén, bạn có thể xóa các tập tin đã giải nén được lưu vào đường dẫn sau theo cách thủ công: %systemroot%\temp. Tập tin có tiền tố PR.

- **Không quét tập tin nén lớn hơn N MB.** Nếu hộp kiểm này được chọn, thành phần Bảo vệ mối đe dọa thư điện tử sẽ loại trừ các tập tin đính kèm email khỏi tác vụ quét nếu kích cỡ của chúng vượt quá giá trị được quy định. Nếu hộp kiểm này bị xóa, thành phần Bảo vệ mối đe dọa thư điện tử sẽ quét các tập tin đính kèm email thuộc mọi kích cỡ.
- **Giới hạn thời gian kiểm tra các tập tin nén thành N giây.** Nếu hộp kiểm này được chọn, thời gian phân bổ cho việc quét các tập tin đính kèm email sẽ bị hạn chế trong khoảng thời gian được quy định.


5. Lưu các thay đổi của bạn.

Lọc tập tin đính kèm nội dung email

Chức năng lọc tập tin đính kèm không được áp dụng cho các email gửi đi.

Các ứng dụng 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 ứng dụng độc hại.

Để thiết lập bộ lọc tập tin đính kèm:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa thư điện tử**.
3. Nhấn vào **Thiết lập nâng cao**.
4. Trong mục **Lọc tập tin đính kèm**, hãy thực hiện một trong những hành động sau:
 - **Vô hiệu lọc.** Nếu tùy chọn này được chọn, thành phần Bảo vệ mối đe dọa thư điện tử sẽ không lọc các tập tin được đính kèm email.
 - **Đổi tên tập tin nén đính kèm của loại đã chọn.** Nếu tùy chọn này được chọn, Bảo vệ mối đe dọa thư điện tử sẽ thay thế ký tự cuối cùng của đuôi mở rộng được tìm thấy trong các tập tin đính kèm của các loại được chỉ định bằng ký tự gạch dưới (ví dụ: attachment.doc_). Vì vậy, để mở tập tin này, người dùng phải đổi tên tập tin.
 - **Xóa tập tin nén đính kèm của loại đã chọn.** Nếu tùy chọn này được lựa chọn, thành phần Bảo vệ mối đe dọa thư điện tử sẽ xóa tập tin đính kèm thuộc loại được quy định khỏi email.
5. Nếu bạn đã chọn **Đổi tên tập tin nén đính kèm của loại đã chọn** hoặc **Xóa tập tin nén đính kèm của loại đã chọn** ở bước trước, hãy chọn hộp kiểm đối diện các loại tập tin tương ứng.

6. Lưu các thay đổi của bạn.

Xuất và nhập phần mở rộng để lọc tập tin đính kèm

Bạn có thể xuất danh sách các phần mở rộng lọc tập tin đính kèm vào tập tin XML. Bạn có thể sử dụng chức năng xuất/nhập để sao lưu danh sách các phần mở rộng hoặc để di chuyển danh sách sang một máy chủ khác.

[Cách xuất và nhập danh sách các phần mở rộng lọc tập tin đính kèm trong Bảng điều khiển quản trị \(MMC\)](#)²

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Bảo vệ mỗi đe dọa thư điện tử**.
6. Trong mục **Mức độ bảo mật**, hãy nhấn nút **Thiết lập**.
7. Trong cửa sổ mở ra, hãy chọn thẻ **Lọc tập tin đính kèm**.
8. Để xuất danh sách các phần mở rộng:
 - a. Chọn các phần mở rộng mà bạn muốn xuất. Để chọn nhiều cổng, hãy sử dụng phím **CTRL** hoặc **SHIFT**.
 - b. Nhấn liên kết **Xuất**.
 - c. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin XML mà bạn muốn xuất danh sách các phần mở rộng vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
 - d. Lưu tập tin.

Kaspersky Endpoint Security sẽ xuất toàn bộ danh sách các phần mở rộng vào tập tin XML.
9. Để nhập danh sách các phần mở rộng:
 - a. Nhấn liên kết **Nhập**.
 - b. Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách các phần mở rộng.
 - c. Mở tập tin.

Nếu máy tính đã có danh sách các phần mở rộng, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.
10. Lưu các thay đổi của bạn.

[Cách xuất và nhập danh sách các phần mở rộng lọc tập tin đính kèm trong Bảng điều khiển web và Bảng điều khiển đám mây](#)²

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa thư điện tử**.
5. Để xuất danh sách các phần mở rộng trong mục **Lọc tập tin đính kèm**:
 - a. Chọn các phần mở rộng mà bạn muốn xuất.
 - b. Nhấn liên kết **Xuất**.
 - c. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin XML mà bạn muốn xuất danh sách các phần mở rộng vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
 - d. Lưu tập tin.
Kaspersky Endpoint Security sẽ xuất toàn bộ danh sách các phần mở rộng vào tập tin XML.
6. Để nhập danh sách các phần mở rộng trong mục **Lọc tập tin đính kèm**:
 - a. Nhấn liên kết **Nhập**.
 - b. Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách các phần mở rộng.
 - c. Mở tập tin.
Nếu máy tính đã có danh sách các phần mở rộng, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.
7. Lưu các thay đổi của bạn.

Quét email trong Microsoft Office Outlook

Trong quá trình cài đặt Kaspersky Endpoint Security, tiện ích mở rộng Bảo vệ mối đe dọa thư điện tử sẽ được nhúng vào Microsoft Office Outlook (sau đây còn được gọi là Outlook). Nó cho phép bạn mở thiết lập thành phần Bảo vệ mối đe dọa 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. Tiện ích mở rộng Bảo vệ mối đe dọa 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. Kaspersky Endpoint Security cũng hỗ trợ làm việc với các trình khách email khác (bao gồm Microsoft Outlook Express®, Windows Mail và Mozilla™ Thunderbird™).

Phần mở rộng Bảo vệ mối đe dọa thư điện tử hỗ trợ hoạt động với Outlook 2010, 2013, 2016 và 2019.

Khi làm việc với trình khách email Mozilla Thunderbird, thành phần Bảo vệ mối đe dọa 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.

Trong Outlook, các email đến sẽ được quét trước tiên bởi thành phần Bảo vệ mối đe dọa thư điện tử (nếu hộp kiểm [Quét POP3, SMTP, NNTP và IMAP](#) được chọn trong giao diện của Kaspersky Endpoint Security) và sau đó là bởi tiện ích mở rộng Bảo vệ mối đe dọa thư điện tử cho Outlook. Nếu thành phần Bảo vệ mối đe dọa thư điện tử phát hiện một đối tượng độc hại trong email, nó sẽ cảnh báo cho bạn về sự kiện này.

Thiết lập thành phần Bảo vệ mối đe dọa thư điện tử có thể được cấu hình trực tiếp trong Outlook nếu hộp kiểm [Phần mở rộng Microsoft Office Outlook được kết nối](#) trong giao diện của Kaspersky Endpoint Security.

Các email đi sẽ được quét trước tiên bởi tiện ích mở rộng Bảo vệ mối đe dọa thư điện tử cho Outlook, và sau đó được quét bởi thành phần Bảo vệ mối đe dọa thư điện tử.

Nếu email được quét sử dụng tiện ích mở rộng Bảo vệ mối đe dọa thư điện tử cho Outlook, bạn nên sử dụng Chế độ bộ nhớ đệm Exchange. Để biết thêm chi tiết về Cached Exchange Mode và khuyến nghị về việc sử dụng của nó, vui lòng tham khảo [Cơ sở tri thức của Microsoft](#).

Để thiết lập chế độ hoạt động của tiện ích mở rộng Bảo vệ mối đe dọa thư điện tử cho Outlook sử dụng Kaspersky Security Center:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa thư điện tử**.
6. Trong mục **Mức độ bảo mật**, hãy nhấn nút **Thiết lập**.
7. Trong mục **Khả năng kết nối**, hãy nhấn nút **Thiết lập**.
8. Trong cửa sổ **Bảo vệ email**, hãy thực hiện một trong các thao tác sau:
 - Chọn hộp kiểm **Quét khi nhận** nếu bạn muốn tiện ích mở rộng Bảo vệ mối đe dọa thư điện tử cho Outlook quét các email đến khi chúng vào hộp thư.
 - Chọn hộp kiểm **Quét khi đọc** nếu bạn muốn tiện ích mở rộng Bảo vệ mối đe dọa thư điện tử cho Outlook quét các email đến khi người sử dụng đọc chúng.
 - Chọn hộp kiểm **Quét khi gửi** nếu bạn muốn tiện ích mở rộng Bảo vệ mối đe dọa thư điện tử cho Outlook quét các email đi khi chúng được gửi.
9. Lưu các thay đổi của bạn.


Bảo vệ mỗi đe dọa mạng

Thành phần Bảo vệ mỗi đe dọa mạng sẽ quét lưu lượng mạng vào để phát hiện các hoạt động tương tự với các cuộc tấn công mạng. Khi Kaspersky Endpoint Security phát hiện một nỗ lực tấn công mạng vào máy tính của người dùng, ứng dụng sẽ chặn kết nối mạng với 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 Bảo vệ mỗi đe dọa mạng phát hiện sẽ được cập nhật trong [bản cập nhật cơ sở dữ liệu và mô-đun ứng dụng](#).

Bật và tắt Bảo vệ mỗi đe dọa mạng

Theo mặc định, Bảo vệ mỗi đe dọa mạng sẽ được bật và hoạt động trong chế độ tối ưu. Bạn có thể tắt Bảo vệ mỗi đe dọa mạng nếu cần thiết.


Để bật hoặc tắt Bảo vệ mỗi đe dọa mạng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Bảo vệ mỗi đe dọa mạng**.
3. Sử dụng nút bật/tắt **Bảo vệ mỗi đe dọa mạng** để bật hoặc tắt thành phần.
4. Lưu các thay đổi của bạn.

Kết quả là nếu tính năng Bảo vệ mỗi đe dọa mạng được bật, Kaspersky Endpoint Security sẽ quét lưu lượng mạng đến để tìm hoạt động điển hình của các cuộc tấn công mạng. Khi Kaspersky Endpoint Security phát hiện một nỗ lực tấn công mạng vào máy tính của người dùng, ứng dụng sẽ chặn kết nối mạng với máy tính tấn công.

Chặn máy tính tấn công

Để chặn máy tính tấn công:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Bảo vệ mỗi đe dọa mạng**.
3. Chọn hộp kiểm **Thêm máy tính tấn công vào danh sách chặn trong N phút**.

Nếu hộp kiểm này được chọn, thành phần Bảo vệ mỗi đe dọa mạng sẽ thêm máy tính tấn công vào danh sách chặn. Điều này có nghĩa là thành phần Bảo vệ mỗi đe dọa mạng sẽ chặn kết nối mạng từ máy tính tấn công sau nỗ lực tấn công mạng đầu tiên trong một khoảng thời gian được quy định. Lệnh chặn này sẽ tự động bảo vệ máy tính của người dùng chống lại tất cả các cuộc tấn công mạng có thể có trong tương lai từ cùng một địa chỉ.

Thời gian tối thiểu mà máy tính tấn công phải cần trong danh sách chặn là một phút. Thời gian tối đa là 32768 phút.

Bạn có thể xem danh sách chặn trong cửa sổ [công cụ Giám sát mạng](#).

Kaspersky Endpoint Security sẽ xóa danh sách chặn khi ứng dụng được khởi chạy lại và khi thiết lập Bảo vệ mỗi đe dọa mạng bị thay đổi.


1. Đặt thời lượng chặn khác cho một máy tính tấn công trong trường ở bên phải của hộp kiểm **Thêm máy tính tấn công vào danh sách chặn trong N phút**.
2. Lưu các thay đổi của bạn.

Kết quả là khi Kaspersky Endpoint Security phát hiện một nỗ lực tấn công mạng được phát động nhắm vào máy tính của người dùng, ứng dụng sẽ chặn tất cả các kết nối mạng với máy tính tấn công.

Cấu hình các địa chỉ được loại trừ khỏi quy tắc chặn

Kaspersky Endpoint Security có thể nhận ra cuộc tấn công mạng và chặn kết nối mạng không an toàn đang truyền một số lượng lớn các gói tin (ví dụ: từ camera an ninh). Để làm việc với các thiết bị được tin tưởng, bạn có thể thêm địa chỉ IP của các thiết bị này vào danh sách loại trừ.

Để thiết lập các địa chỉ được loại trừ khỏi quy tắc chặn:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Bảo vệ mỗi đe dọa mạng**.
3. Nhấn liên kết **Quản lý loại trừ**.
4. Trong cửa sổ mở ra, hãy nhấn vào nút **Thêm**.
5. Nhập vào địa chỉ IP của máy tính mà các cuộc tấn công mạng xuất phát từ đó sẽ không bị chặn.
6. Lưu các thay đổi của bạn.

Kết quả là Kaspersky Endpoint Security không theo dõi hoạt động từ các thiết bị trong danh sách loại trừ.

Xuất và nhập danh sách các loại trừ khỏi hoạt động chặn

Bạn có thể xuất danh sách loại trừ ra tập tin XML. Sau đó, bạn có thể sửa đổi tập tin, ví dụ như thêm một số lượng lớn các địa chỉ cùng loại. Bạn cũng có thể sử dụng chức năng xuất/nhập để sao lưu danh sách các loại trừ hoặc để chuyển danh sách sang máy chủ khác.

[Cách xuất và nhập danh sách loại trừ trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Bảo vệ mỗi đe dọa mạng**.
6. Trong mục **Thiết lập Bảo vệ mỗi đe dọa mạng**, hãy nhấn nút **Loại trừ**.
7. Để xuất danh sách quy tắc:
 - a. Chọn các loại trừ mà bạn muốn xuất. Để chọn nhiều cổng, hãy sử dụng phím **CTRL** hoặc **SHIFT**. Nếu bạn không chọn loại trừ nào, Kaspersky Endpoint Security sẽ xuất tất cả các loại trừ.
 - b. Nhấn liên kết **Xuất**.
 - c. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin XML mà bạn muốn xuất danh sách các loại trừ vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
 - d. Lưu tập tin.
Kaspersky Endpoint Security sẽ xuất toàn bộ danh sách các loại trừ vào tập tin XML.
8. Để nhập danh sách loại trừ:
 - a. Nhấn **Nhập**.
 - b. Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách các loại trừ.
 - c. Mở tập tin.
Nếu máy tính đã có danh sách các loại trừ, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.
9. Lưu các thay đổi của bạn.

[Cách xuất và nhập danh sách loại trừ trong Bảng điều khiển web và Bảng điều khiển đám mây](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Bảo vệ mỗi đe dọa thiết yếu** → **Bảo vệ mỗi đe dọa mạng**.
5. Trong mục **Thiết lập Bảo vệ mỗi đe dọa mạng**, hãy nhấn liên kết **Loại trừ**.
Danh sách loại trừ sẽ mở ra.
6. Để xuất danh sách quy tắc:
 - a. Chọn các loại trừ mà bạn muốn xuất.
 - b. Nhấn vào **Xuất**.
 - c. Xác nhận rằng bạn chỉ muốn xuất các loại trừ đã chọn hoặc xuất toàn bộ danh sách loại trừ.
 - d. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin XML mà bạn muốn xuất danh sách các loại trừ vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
 - e. Lưu tập tin.
Kaspersky Endpoint Security sẽ xuất toàn bộ danh sách các loại trừ vào tập tin XML.
7. Để nhập danh sách loại trừ:
 - a. Nhấn **Nhập**.
 - b. Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách các loại trừ.
 - c. Mở tập tin.
Nếu máy tính đã có danh sách các loại trừ, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.
8. Lưu các thay đổi của bạn.

Cấu hình bảo vệ ngăn các cuộc tấn công mạng theo loại

Kaspersky Endpoint Security cho phép bạn quản lý tính năng bảo vệ trước các loại tấn công mạng sau:

- *Làm nghẽn mạng* là một cuộc tấn công vào tài nguyên mạng của một tổ chức (chẳng hạn như máy chủ web). Cuộc tấn công này bao gồm việc gửi một số lượng lớn các yêu cầu làm quá tải băng thông của tài nguyên mạng. Khi điều này xảy ra, người dùng không thể truy cập tài nguyên mạng của tổ chức.
- Tấn công *Quét cổng* bao gồm hoạt động quét các cổng UDP, cổng TCP và các dịch vụ mạng trên máy tính. Cuộc tấn công này cho phép kẻ tấn công xác định mức độ lỗ hổng bảo mật của máy tính trước khi tiến hành các kiểu tấn công mạng nguy hiểm hơn. Hoạt động Quét cổng cũng cho phép kẻ tấn


công xác định hệ điều hành trên máy tính và lựa chọn các cuộc tấn công mạng thích hợp cho hệ điều hành này.

- Một cuộc *tấn công giả mạo MAC* bao gồm hoạt động thay đổi địa chỉ MAC của một thiết bị mạng (card mạng). Do đó, kẻ tấn công có thể chuyển hướng dữ liệu được gửi đến một thiết bị sang thiết bị khác và chiếm quyền truy cập vào dữ liệu này. Kaspersky Endpoint Security cho phép bạn chặn các cuộc tấn công Giả mạo MAC và nhận thông báo về các cuộc tấn công.

Bạn có thể vô hiệu hóa tính năng phát hiện các loại tấn công này trong trường hợp một số ứng dụng được phép của bạn thực hiện các hoạt động tiêu biểu cho các loại tấn công này. Điều này sẽ giúp tránh cảnh báo nhầm.

Theo mặc định, Kaspersky Endpoint Security sẽ không giám sát các cuộc tấn công làm nghẽn mạng, quét cổng và tấn công giả mạo MAC.

Để cấu hình bảo vệ chống các cuộc tấn công mạng theo loại:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Bảo vệ mỗi đe dọa mạng**.
3. Sử dụng nút bật/tắt **Coi hoạt động quét cổng và làm nghẽn mạng là các cuộc tấn công** để bật hoặc tắt tính năng phát hiện các cuộc tấn công này.
4. Sử dụng nút bật/tắt **Chống giả mạo MAC**.
5. Trong mục **Khi phát hiện một cuộc tấn công giả mạo MAC**, hãy chọn một trong các tùy chọn sau:
 - **Chỉ thông báo.**
 - **Thông báo và chặn.**
6. Lưu các thay đổi của bạn.

Tường lửa

Tường lửa chặn các kết nối trái phép đến máy tính khi đang làm việc trên Internet hoặc mạng cục bộ. Tường lửa cũng kiểm soát hoạt động mạng của các ứng dụng trên máy tính. Điều này cho phép bạn bảo vệ mạng LAN công ty trước hành vi trộm danh tính và các cuộc tấn công khác. Thành phần này giúp bảo vệ máy tính với sự trợ giúp của cơ sở dữ liệu diệt virus, dịch vụ đám mây của Kaspersky Security Network và các *quy tắc mạng* được xác định trước.

Network Agent được sử dụng để tương tác với Kaspersky Security Center. Tường lửa sẽ tự động tạo quy tắc mạng cần thiết cho ứng dụng và Network Agent để làm việc. Kết quả là Tường lửa sẽ mở vài cổng trên máy tính. Việc cổng nào được mở phụ thuộc vào vai trò của máy tính (ví dụ: điểm phân phối). Để tìm hiểu thêm về các cổng sẽ được mở trên máy tính, hãy tham khảo [Trợ giúp của Kaspersky Security Center](#).

Quy tắc mạng

Bạn có thể cấu hình quy tắc mạng ở các cấp sau:

- *Những quy tắc cho gói tin mạng.* Các quy tắc gói tin mạng áp đặt hạn chế cho các gói tin mạng, bất kể ứng dụng 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. Kaspersky Endpoint Security đã xác định trước các quy tắc gói tin mạng bằng các quyền được khuyến nghị bởi các chuyên gia của Kaspersky.
- *Quy tắc ứng dụng mạng.* 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.

Quyền truy cập được kiểm soát của ứng dụng vào tài nguyên hệ điều hành, tiến trình và dữ liệu cá nhân được cung cấp bởi [thành phần Phòng chống xâm nhập máy chủ](#) bằng cách sử dụng *các quyền của ứng dụng*.

Trong lần khởi động đầu tiên của ứng dụng, Tường lửa sẽ thực hiện các hành động sau:

1. Kiểm tra tính bảo mật của ứng dụng bằng cách cơ sở dữ liệu diệt virus đã tải xuống.
2. Kiểm tra tính bảo mật của ứng dụng trong Kaspersky Security Network.
Bạn nên [tham gia vào Kaspersky Security Network](#) để giúp Tường lửa hoạt động hiệu quả hơn.
3. Đưa ứng dụng vào một trong các *nhóm tin tưởng*: Tin tưởng, Giới hạn mức Thấp, Giới hạn mức Cao, Không tin tưởng.

Một [nhóm tin tưởng quy định các quyền](#) được Kaspersky Endpoint Security áp dụng khi kiểm soát hoạt động của các ứng dụng trong nhóm đó. Kaspersky Endpoint Security sẽ đặt ứng dụng vào một nhóm tin tưởng tùy thuộc vào mức độ nguy hiểm mà ứng dụng này có thể gây ra cho máy tính.

Kaspersky Endpoint Security sẽ đặt ứng dụng vào nhóm tin tưởng cho các thành phần Tường lửa và Phòng chống xâm nhập máy chủ. Bạn chỉ không thể thay đổi nhóm tin tưởng cho Tường lửa hoặc Phòng chống xâm nhập máy chủ.

Nếu bạn từ chối tham gia vào KSN hoặc không có mạng, Kaspersky Endpoint Security sẽ đặt ứng dụng vào một nhóm tin tưởng tùy thuộc vào [thiết lập của thành phần Phòng chống xâm nhập máy chủ](#). Sau khi nhận được danh tiếng của ứng dụng từ KSN, nhóm tin tưởng có thể được thay đổi tự động.

4. Nó sẽ chặn hoạt động mạng của các ứng dụng, tùy thuộc vào nhóm tin tưởng. Ví dụ: các ứng dụng trong nhóm tin tưởng Giới hạn mức Cao không được phép sử dụng bất kỳ kết nối mạng nào.

Khi ứng dụng được khởi chạy vào lần tới, Kaspersky Endpoint Security sẽ kiểm tra tính toàn vẹn của ứng dụng. Nếu ứng dụng không bị thay đổi, thành phần này sử dụng các quy tắc mạng hiện tại cho ứng dụng. Nếu ứng dụng đã bị sửa đổi, Kaspersky Endpoint Security sẽ phân tích ứng dụng đó như khi ứng dụng đó được khởi chạy lần đầu tiên.

Các mức ưu tiên của quy tắc mạng

Mỗi quy tắc có một mức ưu tiên. Quy tắc có vị trí càng cao trên danh sách thì càng có mức ưu tiên cao. Nếu hoạt động mạng được thêm vào một vài quy tắc, Tường lửa sẽ điều chỉnh hoạt động mạng theo quy tắc có mức ưu tiên cao nhất.

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 hành 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.

Các trạng thái kết nối mạng

Tường lửa cho phép bạn kiểm soát hoạt động mạng tùy thuộc vào trạng thái của kết nối mạng. Kaspersky Endpoint Security sẽ nhận trạng thái kết nối mạng từ hệ điều hành của máy tính. Trạng thái của kết nối mạng trong hệ điều hành được người dùng đặt khi thiết lập kết nối. Bạn có thể [thay đổi trạng thái của kết nối mạng trong mục thiết lập của Kaspersky Endpoint Security](#). Tường lửa sẽ giám sát hoạt động mạng tùy thuộc vào trạng thái mạng trong mục thiết lập của Kaspersky Endpoint Security chứ không phải trong hệ điều hành.

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

- **Mạng công cộng.** Mạng không được bảo vệ bởi các ứng dụng diệt virus, tường lửa hoặc bộ lọc (như mạng Wi-Fi trong quán cà phê). 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 cục bộ.** Mạng dành cho người dùng có quyền truy cập hạn chế vào các tập tin và máy in trên máy tính này (ví dụ như mạng LAN công ty hoặc mạng gia đình).
- **Mạng tin tưởng.** Mạng an toàn trong đó máy tính không bị nguy cơ tấn công hay các nỗ lực truy cập dữ liệu trái phép. Tường lửa cho phép mọi hoạt động mạng trong các mạng có trạng thái này.

Bật hoặc tắt Tường lửa

Theo mặc định, Tường lửa sẽ được bật và hoạt động trong chế độ tối ưu.

Để bật hoặc tắt Tường lửa:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Tường lửa**.

3. Sử dụng nút bật/tắt **Tường lửa** để bật hoặc tắt thành phần.

4. Lưu các thay đổi của bạn.


Do đó, nếu Tường lửa được bật, Kaspersky Endpoint Security sẽ kiểm soát hoạt động mạng và chặn các kết nối mạng trái phép đến máy tính của bạn, cũng như chặn hoạt động mạng trái phép của các ứng dụng trên máy tính của bạn. Hoạt động mạng cũng được kiểm soát bởi [thành phần Bảo vệ mối đe dọa mạng](#). Thành phần Bảo vệ mối đe dọa mạng sẽ quét lưu lượng mạng vào để phát hiện các hoạt động tương tự với các cuộc tấn công mạng.

Kaspersky Endpoint Security sẽ ghi nhật ký các sự kiện tấn công mạng trong các báo cáo của ứng dụng, bất kể thiết lập của Tường lửa. Ngay cả khi Tường lửa chặn kết nối mạng bằng cách sử dụng các quy tắc và do đó ngăn chặn một cuộc tấn công mạng thì thành phần Bảo vệ mối đe dọa mạng vẫn sẽ ghi lại các sự kiện tấn công mạng. Đây là thành phần không thể thiếu để tạo thông tin thống kê về các cuộc tấn công mạng vào các máy tính trong tổ chức của bạn.

Thay đổi trạng thái kết nối mạng

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.

Để thay đổi trạng thái kết nối mạng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Tường lửa**.
3. Nhấn vào **Các mạng khả dụng**.
4. Chọn kết nối mạng mà bạn muốn thay đổi trạng thái.
5. Trong cột **Loại mạng**, hãy chọn trạng thái kết nối mạng:
 - **Mạng công cộng.** Mạng không được bảo vệ bởi các ứng dụng diệt virus, tường lửa hoặc bộ lọc (như mạng Wi-Fi trong quán cà phê). 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.
 - **Mạng cục bộ.** Mạng dành cho người dùng có quyền truy cập hạn chế vào các tập tin và máy in trên máy tính này (ví dụ như mạng LAN công ty hoặc mạng gia đình).
 - **Mạng tin tưởng.** Mạng an toàn trong đó máy tính không bị nguy cơ tấn công hay các nỗ lực truy cập dữ liệu trái phép. Tường lửa cho phép mọi hoạt động mạng trong các mạng có trạng thái này.
6. Lưu các thay đổi của bạn.

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 thêm 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 một quy tắc gói tin mạng

Bạn có thể tạo quy tắc gói tin mạng theo những cách sau:

- Sử dụng [công cụ 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 theo thời gian thực. Đây là cách tiện lợi vì bạn không cần phải cấu hình tất cả các thiết lập quy tắc. Một số thiết lập Tường lửa sẽ được chèn tự động từ dữ liệu của công cụ Giám sát mạng. Công cụ Giám sát mạng chỉ khả dụng trong giao diện ứng dụng.

- Cấu hình các thiết lập Tường lửa.

Đây là cách cho phép bạn tinh chỉnh thiết lập Tường lửa. Bạn có thể tạo quy tắc cho bất kỳ hoạt động mạng nào, ngay cả khi không có hoạt động mạng nào tại thời điểm hiện tại.


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

Cách sử dụng công cụ Giám sát mạng để tạo quy tắc gói tin mạng trong giao diện ứng dụng


1. Trong cửa sổ chính của ứng dụng, trong mục **Giám sát**, hãy nhấn ô **Giám sát mạng**.
2. Chọn thẻ **Hoạt động mạng**.
Thẻ **Hoạt động mạng** 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.
3. Trong menu ngữ cảnh của kết nối mạng, hãy chọn **Tạo quy tắc gói tin mạng**.
Thao tác này sẽ mở các thuộc tính quy tắc mạng.
4. Đặt trạng thái **Hoạt động** cho quy tắc gói tin.
5. Nhập vào thủ công tên của dịch vụ mạng vào trường **Tên**.
6. Cấu hình thiết lập quy tắc mạng (xem bảng bên dưới).
Bạn có thể chọn một mẫu quy tắc được định nghĩa trước bằng cách nhấn vào liên kết **Mẫu quy tắc mạng**. Mẫu quy tắc mô tả các kết nối mạng được sử dụng thường xuyên nhất.
Tất cả thiết lập quy tắc mạng sẽ được điền tự động.
7. Nếu bạn muốn hành động của quy tắc mạng được phản ánh trong [báo cáo](#), hãy chọn hộp kiểm **Ghi lại sự kiện**.
8. Nhấn vào **Lưu**.
Quy tắc mạng mới sẽ được thêm vào danh sách.
9. Sử dụng các nút **Lên** / **Xuống** để đặt mức độ ưu tiên của quy tắc mạng.
10. Lưu các thay đổi của bạn.

Cách sử dụng thiết lập Tường lửa để tạo quy tắc gói tin mạng cho ứng dụng trong giao diện ứng dụng



1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Tường lửa**.
3. Nhấn vào **Quy tắc gói tin**.
Thao tác này sẽ mở danh sách các quy tắc mạng mặc định được thiết lập bởi Tường lửa.
4. Nhấn vào **Thêm**.
Thao tác này sẽ mở các thuộc tính quy tắc mạng.
5. Đặt trạng thái **Hoạt động** cho quy tắc gói tin.
6. Nhập vào thủ công tên của dịch vụ mạng vào trường **Tên**.
7. Cấu hình thiết lập quy tắc mạng (xem bảng bên dưới).
Bạn có thể chọn một mẫu quy tắc được định nghĩa trước bằng cách nhấn vào liên kết **Mẫu quy tắc mạng**. Mẫu quy tắc mô tả các kết nối mạng được sử dụng thường xuyên nhất.
Tất cả thiết lập quy tắc mạng sẽ được điền tự động.
8. Nếu bạn muốn hành động của quy tắc mạng được phản ánh trong [báo cáo](#), hãy chọn hộp kiểm **Ghi lại sự kiện**.
9. Nhấn vào **Lưu**.
Quy tắc mạng mới sẽ được thêm vào danh sách.
10. Sử dụng các nút **Lên** / **Xuống** để đặt mức độ ưu tiên của quy tắc mạng.
11. Lưu các thay đổi của bạn.

[Cách tạo quy tắc gói tin mạng trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Tường lửa**.
6. Trong mục **Thiết lập Tường lửa**, hãy nhấn nút **Thiết lập**.
Thao tác này sẽ mở ra danh sách các quy tắc gói tin mạng và danh sách các quy tắc mạng cho ứng dụng.
7. Chọn thẻ **Những quy tắc cho gói tin mạng**.
Thao tác này sẽ mở danh sách các quy tắc mạng mặc định được thiết lập bởi Tường lửa.
8. Nhấn vào **Thêm**.
Thao tác này sẽ mở các thuộc tính quy tắc gói tin.
9. Nhập vào thủ công tên của dịch vụ mạng vào trường **Tên**.
10. Cấu hình thiết lập quy tắc mạng (xem bảng bên dưới).
Bạn có thể chọn một mẫu quy tắc được định sẵn bằng cách nhấn vào nút . Mẫu quy tắc mô tả các kết nối mạng được sử dụng thường xuyên nhất.
Tất cả thiết lập quy tắc mạng sẽ được điền tự động.
11. Nếu bạn muốn hành động của quy tắc mạng được phản ánh trong [báo cáo](#), hãy chọn hộp kiểm **Ghi lại sự kiện**.
12. Lưu quy tắc mạng mới.
13. Sử dụng các nút **Lên** / **Xuống** để đặt mức độ ưu tiên của quy tắc mạng.
14. Lưu các thay đổi của bạn.

Tường lửa sẽ kiểm soát các gói tin mạng theo quy tắc. Bạn có thể vô hiệu quy tắc gói tin khỏi hoạt động của Tường lửa mà không cần xóa nó khỏi danh sách. Để thực hiện, hãy bỏ chọn hộp kiểm bên cạnh đối tượng.

[Cách tạo quy tắc gói tin mạng trong Bảng điều khiển web và Bảng điều khiển đám mây](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Tường lửa**.
5. Trong mục **Thiết lập tường lửa**, hãy nhấn vào liên kết **Những quy tắc cho gói tin mạng**.
Thao tác này sẽ mở danh sách các quy tắc mạng mặc định được thiết lập bởi Tường lửa.
6. Nhấn vào nút **Thêm**.
Thao tác này sẽ mở các thuộc tính quy tắc gói tin.
7. Nhập vào thủ công tên của dịch vụ mạng vào trường **Tên**.
8. Cấu hình thiết lập quy tắc mạng (xem bảng bên dưới).
Bạn có thể chọn một mẫu quy tắc được định sẵn bằng cách nhấn vào liên kết **Chọn mẫu**. Mẫu quy tắc mô tả các kết nối mạng được sử dụng thường xuyên nhất.
Tất cả thiết lập quy tắc mạng sẽ được điền tự động.
9. Nếu bạn muốn hành động của quy tắc mạng được phản ánh trong [báo cáo](#), hãy chọn hộp kiểm **Ghi lại sự kiện**.
10. Lưu quy tắc mạng.
Quy tắc mạng mới sẽ được thêm vào danh sách.
11. Sử dụng các nút **Lên / Xuống** để đặt mức độ ưu tiên của quy tắc mạng.
12. Lưu các thay đổi của bạn.

Tường lửa sẽ kiểm soát các gói tin mạng theo quy tắc. Bạn có thể vô hiệu quy tắc gói tin khỏi hoạt động của Tường lửa mà không cần xóa nó khỏi danh sách. Sử dụng nút bật/tắt trong cột **Trạng thái** để bật hoặc tắt quy tắc gói tin.


Thiết lập Quy tắc gói tin mạng

Tham số	Mô tả
Hành động	<p>Cho phép. Chặn.</p> <p>Theo các quy tắc ứng dụng. Nếu chọn tùy chọn này, Tường lửa sẽ áp dụng các quy tắc mạng ứng dụng cho kết nối mạng.</p>
Giao thức	<p>Kiểm soát hoạt động mạng qua giao thức đã chọn: TCP, UDP, ICMP, ICMPv6, IGMP và GRE.</p> <p>Nếu chọn giao thức ICMP hoặc ICMPv6, bạn có thể xác định loại gói tin và mã ICMP.</p> <p>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.</p>

Hướng	<p>Gói tin vào (gói). Tường lửa sẽ áp dụng quy tắc mạng cho tất cả các gói mạng gửi đến.</p> <p>Gói tin vào. Tường lửa sẽ áp dụng quy tắc mạng cho tất cả các gói tin mạng gửi qua kết nối được khởi tạo bởi máy tính từ xa.</p> <p>Gói tin vào / Gói tin ra. Tường lửa sẽ áp dụng quy tắc mạng cho cả gói tin mạng gửi đến hoặc gửi đi, bất kể kết nối mạng này đã được khởi tạo bởi máy tính người dùng hay một máy tính từ xa.</p> <p>Gói tin ra (gói). Tường lửa áp dụng quy tắc mạng cho tất cả các gói mạng gửi đi.</p> <p>Gói tin ra. Tường lửa sẽ áp dụng quy tắc mạng cho tất cả các gói tin mạng gửi qua kết nối được khởi tạo bởi máy tính của người dùng.</p>
Bộ điều hợp mạng	<p>Bộ điều hợp mạng có thể gửi và/hoặc nhận các gói mạng. Việc quy định cấu hình của các bộ điều hợp mạng giúp máy tính có thể phân biệt giữa các gói tin mạng được gửi hoặc nhận bởi các bộ điều hợp mạng với địa chỉ IP giống nhau.</p>
Thời gian sống (TTL)	<p>Hạn chế kiểm soát các gói tin mạng dựa trên thời gian tồn tại của chúng (TTL).</p>
Địa chỉ từ xa	<p>Các địa chỉ mạng của các máy tính từ xa có thể gửi và nhận gói tin mạng. Tường lửa sẽ áp đặt quy tắc mạng cho dải địa chỉ mạng từ xa được chỉ định. Bạn có thể thêm tất cả các địa chỉ IP vào một quy tắc mạng, tạo một danh sách địa chỉ IP riêng, chỉ định một dải địa chỉ IP hoặc chọn một mạng con (Mạng tin tưởng, Mạng cục bộ, Mạng công cộng). Bạn cũng có thể chỉ định tên DNS của máy tính thay vì địa chỉ IP. Bạn chỉ nên sử dụng tên DNS cho các máy tính mạng LAN hoặc các dịch vụ nội bộ. Tương tác với các dịch vụ đám mây (như Microsoft Azure) và các tài nguyên Internet khác nên được xử lý bởi thành phần Kiểm soát Web.</p> <div data-bbox="296 1104 1493 1263" style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Kaspersky Endpoint Security hỗ trợ tên DNS kể từ phiên bản 11.7.0. Nếu bạn chỉ định tên DNS cho phiên bản 11.6.0 hoặc thấp hơn, Kaspersky Endpoint Security có thể áp dụng quy tắc liên quan cho mọi địa chỉ.</p> </div>
Địa chỉ nội bộ	<p>Các địa chỉ mạng của các máy tính có thể gửi và nhận gói tin mạng. Tường lửa sẽ áp đặt một quy tắc mạng đến khoảng địa chỉ mạng nội bộ được quy định. Bạn có thể thêm tất cả các địa chỉ IP vào một quy tắc mạng, tạo một danh sách địa chỉ IP riêng hoặc chỉ định một dải địa chỉ IP.</p> <div data-bbox="296 1503 1493 1662" style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Kaspersky Endpoint Security hỗ trợ tên DNS kể từ phiên bản 11.7.0. Nếu bạn chỉ định tên DNS cho phiên bản 11.6.0 hoặc thấp hơn, Kaspersky Endpoint Security có thể áp dụng quy tắc liên quan cho mọi địa chỉ.</p> </div> <div data-bbox="296 1704 1493 1827" style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Đôi khi địa chỉ nội bộ không thể được lấy cho các ứng dụng. Nếu đúng, tham số này sẽ bị bỏ qua.</p> </div>


Bật hoặc tắt một quy tắc gói tin mạng

Để bật hoặc tắt một quy tắc gói tin mạng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Tường lửa**.
3. Nhấn vào **Quy tắc gói tin**.
Thao tác này sẽ mở một danh sách các quy tắc gói tin mạng được đặt bởi Tường lửa.
4. Chọn quy tắc gói tin mạng cần thiết trong danh sách.
5. Sử dụng nút bật/tắt trong cột **Trạng thái** để bật hoặc tắt quy tắc.
6. Lưu các thay đổi của bạn.

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. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Tường lửa**.
3. Nhấn vào **Quy tắc gói tin**.
Thao tác này sẽ mở một danh sách các quy tắc gói tin mạng được đặt bởi Tường lửa.
4. Chọn nó trong danh sách các quy tắc gói tin mạng và nhấn nút **Chỉnh sửa**.
5. 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**.
 - **Chặn**.
 - **Theo các quy tắc ứng dụng**. Nếu chọn tùy chọn này, Tường lửa sẽ áp dụng các [quy tắc mạng ứng dụng](#) cho kết nối mạng.
6. Lưu các thay đổi của bạn.


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. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Tường lửa**.
3. Nhấn vào **Quy tắc gói tin**.
Thao tác này sẽ mở một danh sách các quy tắc gói tin mạng được đặt bởi Tường lửa.
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 **Lên** / **Xuống** để đặt mức độ ưu tiên của quy tắc mạng.
6. Lưu các thay đổi của bạn.

Xuất và nhập quy tắc gói tin mạng

Bạn có thể xuất danh sách các quy tắc gói tin mạng vào tập tin XML. Sau đó, bạn có thể sửa đổi tập tin, ví dụ như thêm một số lượng lớn các quy tắc cùng loại. Bạn có thể sử dụng chức năng xuất/nhập để sao lưu danh sách quy tắc gói tin mạng hoặc để chuyển danh sách sang máy chủ khác.

[Cách xuất và nhập danh sách quy tắc gói tin mạng trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Tường lửa**.
6. Trong mục **Thiết lập Tường lửa**, hãy nhấn nút **Thiết lập**.
Thao tác này sẽ mở ra danh sách các quy tắc gói tin mạng và danh sách các quy tắc mạng cho ứng dụng.
7. Chọn thẻ **Những quy tắc cho gói tin mạng**.
8. Để xuất danh sách các quy tắc gói tin mạng:
 - a. Chọn các quy tắc mà bạn muốn xuất. Để chọn nhiều cổng, hãy sử dụng phím **CTRL** hoặc **SHIFT**.
Nếu bạn không chọn quy tắc nào, Kaspersky Endpoint Security sẽ xuất tất cả các quy tắc.
 - b. Nhấn liên kết **Xuất**.
 - c. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin XML mà bạn muốn xuất danh sách các quy tắc vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
 - d. Lưu tập tin.
Kaspersky Endpoint Security sẽ xuất danh sách các quy tắc vào tập tin XML.
9. Để nhập danh sách các quy tắc gói tin mạng:
 - a. Nhấn liên kết **Nhập**.
Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách các quy tắc.
 - b. Mở tập tin.
Nếu máy tính đã có danh sách các quy tắc, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.
10. Lưu các thay đổi của bạn.

[Cách xuất và nhập danh sách các quy tắc gói tin mạng trong Bảng điều khiển web và Bảng điều khiển đám mây](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Tường lửa**.
5. Nhấn vào liên kết **Những quy tắc cho gói tin mạng**.
6. Để xuất danh sách các quy tắc gói tin mạng:
 - a. Chọn các quy tắc mà bạn muốn xuất.
 - b. Nhấn vào **Xuất**.
 - c. Xác nhận rằng bạn chỉ muốn xuất các quy tắc đã chọn hoặc xuất toàn bộ danh sách.
 - d. Lưu tập tin.
Kaspersky Endpoint Security sẽ xuất danh sách các quy tắc vào tập tin XML trong thư mục tải xuống mặc định.
7. Để nhập danh sách các quy tắc gói tin mạng:
 - a. Nhấn liên kết **Nhập**.
Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách các quy tắc.
 - b. Mở tập tin.
Nếu máy tính đã có danh sách các quy tắc, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.
8. Lưu các thay đổi của bạn.

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.

Cũng như thành phần [Phòng chống xâm nhập máy chủ](#), 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. Các 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. Các quy tắc mạng đó sẽ có mức ưu tiên cao hơn quy tắc mạng của cả nhóm chứa ứng dụng đó.

Tạo một quy tắc mạng cho ứng dụng

Theo mặc định, hoạt động của ứng dụng được kiểm soát bởi các quy tắc mạng được quy định cho [nhóm tin tưởng](#) được Kaspersky Endpoint Security gán ứng dụng vào khi ứng dụng khởi chạy lần đầu. Nếu cần, bạn có thể tạo các quy tắc mạng cho toàn bộ một nhóm tin tưởng, cho một ứng dụng riêng lẻ, hoặc một nhóm các ứng dụng trong một nhóm tin tưởng.

Các quy tắc mạng được quy định một cách thủ công có mức độ ưu tiên cao hơn các quy tắc mạng được xác định cho một nhóm tin tưởng. Nói cách khác, nếu các quy tắc cho ứng dụng được quy định theo cách thủ công khác với các quy tắc cho ứng dụng được xác định cho một nhóm tin tưởng, thì Tường lửa sẽ kiểm soát hoạt động của ứng dụng theo các quy tắc được quy định theo cách thủ công cho các ứng dụng.

Theo mặc định, Tường lửa sẽ tạo các quy tắc mạng sau cho từng ứng dụng:

- Bất kỳ hoạt động mạng nào trong Mạng tin tưởng.
- Bất kỳ hoạt động mạng nào trong Mạng cục bộ.
- Bất kỳ hoạt động mạng nào trong các mạng Công cộng.

Kaspersky Endpoint Security kiểm soát hoạt động mạng của các ứng dụng theo các quy tắc mạng được định trước như sau:

- Tin tưởng và Hạn chế thấp: cho phép tất cả hoạt động mạng.
- Hạn chế cao và Không tin tưởng: chặn tất cả hoạt động mạng.

Không thể chỉnh sửa hoặc xóa các quy tắc ứng dụng được định trước.

Bạn có thể tạo quy tắc mạng cho ứng dụng theo các cách sau:

- Sử dụng [công cụ 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 theo thời gian thực. Đây là cách tiện lợi vì bạn không cần phải cấu hình tất cả các thiết lập quy tắc. Một số thiết lập Tường lửa sẽ được chèn tự động từ dữ liệu của công cụ Giám sát mạng. Công cụ Giám sát mạng chỉ khả dụng trong giao diện ứng dụng.

- Cấu hình các thiết lập Tường lửa.


Đây là cách cho phép bạn tinh chỉnh thiết lập Tường lửa. Bạn có thể tạo quy tắc cho bất kỳ hoạt động mạng nào, ngay cả khi không có hoạt động mạng nào tại thời điểm hiện tại.

Khi tạo quy tắc mạng cho ứng dụng, hãy nhớ rằng quy tắc gói tin mạng có quyền ưu tiên hơn quy tắc mạng cho ứng dụng.


Cách sử dụng công cụ Giám sát mạng để tạo quy tắc mạng cho ứng dụng trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, trong mục **Giám sát**, hãy nhấn ô **Giám sát mạng**.
2. Chọn thẻ **Hoạt động mạng** hoặc **Mở cổng**.
Thẻ **Hoạt động mạng** 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 cổng mạng mở của máy tính.
3. Trong menu ngữ cảnh của kết nối mạng, hãy chọn **Tạo một quy tắc mạng cho ứng dụng**.
Cửa sổ thuộc tính và quy tắc ứng dụng sẽ mở ra.
4. Chọn thẻ **Quy tắc mạng**.
Thao tác này sẽ mở danh sách các quy tắc mạng mặc định được thiết lập bởi Tường lửa.
5. Nhấn vào **Thêm**.
Thao tác này sẽ mở các thuộc tính quy tắc mạng.
6. Nhập vào thủ công tên của dịch vụ mạng vào trường **Tên**.
7. Cấu hình thiết lập quy tắc mạng (xem bảng bên dưới).
Bạn có thể chọn một mẫu quy tắc được định nghĩa trước bằng cách nhấn vào liên kết **Mẫu quy tắc mạng**. Mẫu quy tắc mô tả các kết nối mạng được sử dụng thường xuyên nhất.
Tất cả thiết lập quy tắc mạng sẽ được điền tự động.
8. Nếu bạn muốn hành động của quy tắc mạng được phản ánh trong [báo cáo](#), hãy chọn hộp kiểm **Ghi lại sự kiện**.
9. Nhấn vào **Lưu**.
Quy tắc mạng mới sẽ được thêm vào danh sách.
10. Sử dụng các nút **Lên / Xuống** để đặt mức độ ưu tiên của quy tắc mạng.
11. Lưu các thay đổi của bạn.

Cách sử dụng thiết lập Tường lửa để tạo quy tắc mạng cho ứng dụng trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Tường lửa**.
3. Nhấn vào **Quy tắc cho ứng dụng**.
Thao tác này sẽ mở danh sách các quy tắc mạng mặc định được thiết lập bởi Tường lửa.
4. Trong danh sách ứng dụng, hãy chọn ứng dụng hoặc nhóm ứng dụng mà bạn muốn cho tạo một quy tắc mạng.
5. Nhấn chuột phải để mở menu ngữ cảnh và chọn **Chi tiết và quy tắc**.
Cửa sổ thuộc tính và quy tắc ứng dụng sẽ mở ra.
6. Chọn thẻ **Quy tắc mạng**.
7. Nhấn vào **Thêm**.
Thao tác này sẽ mở các thuộc tính quy tắc mạng.
8. Nhập vào thủ công tên của dịch vụ mạng vào trường **Tên**.
9. Cấu hình thiết lập quy tắc mạng (xem bảng bên dưới).
Bạn có thể chọn một mẫu quy tắc được định nghĩa trước bằng cách nhấn vào liên kết **Mẫu quy tắc mạng**. Mẫu quy tắc mô tả các kết nối mạng được sử dụng thường xuyên nhất.
Tất cả thiết lập quy tắc mạng sẽ được điền tự động.
10. Nếu bạn muốn hành động của quy tắc mạng được phản ánh trong [báo cáo](#), hãy chọn hộp kiểm **Ghi lại sự kiện**.
11. Nhấn vào **Lưu**.
Quy tắc mạng mới sẽ được thêm vào danh sách.
12. Sử dụng các nút **Lên** / **Xuống** để đặt mức độ ưu tiên của quy tắc mạng.
13. Lưu các thay đổi của bạn.

[Cách tạo quy tắc mạng cho ứng dụng trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Tường lửa**.
6. Trong mục **Thiết lập Tường lửa**, hãy nhấn nút **Thiết lập**.
Thao tác này sẽ mở ra danh sách các quy tắc gói tin mạng và danh sách các quy tắc mạng cho ứng dụng.
7. Chọn thẻ **Quy tắc cho ứng dụng mạng**.
8. Nhấn vào **Thêm**.
9. Trong cửa sổ mở ra, hãy nhập các tiêu chí để tìm kiếm ứng dụng mà bạn muốn tạo một quy tắc mạng.
Bạn có thể nhập tên của ứng dụng hoặc tên của nhà cung cấp. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự * cùng ? khi nhập tên đại diện.
10. Nhấn vào nút **Làm mới**.
Kaspersky Endpoint Security sẽ tìm kiếm ứng dụng trong danh sách tổng hợp các ứng dụng được cài đặt trên máy tính được quản lý. Kaspersky Endpoint Security sẽ hiển thị danh sách các ứng dụng đáp ứng các tiêu chí tìm kiếm của bạn.
11. Chọn ứng dụng cần thiết.
12. Trong danh sách thả xuống **Thêm ứng dụng được chọn vào nhóm tin tưởng**, hãy chọn **Nhóm mặc định** và nhấn **OK**.
Ứng dụng sẽ được thêm vào nhóm mặc định.
13. Chọn ứng dụng liên quan rồi chọn **Các quyền của ứng dụng** từ menu ngữ cảnh của ứng dụng.
Cửa sổ thuộc tính và quy tắc ứng dụng sẽ mở ra.
14. Chọn thẻ **Quy tắc mạng**.
Thao tác này sẽ mở danh sách các quy tắc mạng mặc định được thiết lập bởi Tường lửa.
15. Nhấn vào nút **Thêm**.
Thao tác này sẽ mở các thuộc tính quy tắc mạng.
16. Nhập vào thủ công tên của dịch vụ mạng vào trường **Tên**.
17. Cấu hình thiết lập quy tắc mạng (xem bảng bên dưới).
Bạn có thể chọn một mẫu quy tắc được định sẵn bằng cách nhấn vào nút . Mẫu quy tắc mô tả các kết nối mạng được sử dụng thường xuyên nhất.
Tất cả thiết lập quy tắc mạng sẽ được điền tự động.

18. Nếu bạn muốn hành động của quy tắc mạng được phản ánh trong [báo cáo](#), hãy chọn hộp kiểm **Ghi lại sự kiện**.
19. Lưu quy tắc mạng mới.
20. Sử dụng các nút **Lên / Xuống** để đặt mức độ ưu tiên của quy tắc mạng.
21. Lưu các thay đổi của bạn.

[Cách tạo một quy tắc mạng cho ứng dụng trong Bảng điều khiển web và Bảng điều khiển đám mây](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Tường lửa**.
5. Trong mục **Thiết lập Tường lửa**, hãy nhấn vào liên kết **Quy tắc cho ứng dụng mạng**.
Thao tác này sẽ mở ra cửa sổ cấu hình quyền của ứng dụng và danh sách các tài nguyên được bảo vệ.
6. Chọn thẻ **Các quyền của ứng dụng**.
Bạn sẽ thấy danh sách các nhóm tin tưởng ở bên trái cửa sổ và thuộc tính của chúng ở bên phải.
7. Nhấn vào nút **Thêm**.
Thao tác này sẽ khởi chạy Trình hướng dẫn để thêm ứng dụng vào nhóm tin tưởng.
8. Chọn nhóm tin tưởng liên quan cho ứng dụng.
9. Chọn loại **Ứng dụng**. Nhấn nút **Tiếp theo**.
Nếu bạn muốn tạo quy tắc mạng cho nhiều ứng dụng, hãy chọn loại **Nhóm** và quy định tên cho nhóm ứng dụng.
10. Trong danh sách ứng dụng được mở, hãy chọn các ứng dụng mà bạn muốn tạo một quy tắc mạng.
Sử dụng bộ lọc. Bạn có thể nhập tên của ứng dụng hoặc tên của nhà cung cấp. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự * cùng ? khi nhập tên đại diện.
11. Kết thúc Trình hướng dẫn bằng cách nhấp vào **OK**.
Ứng dụng sẽ được thêm vào nhóm tin tưởng.
12. Ở phần bên phải của cửa sổ, hãy chọn ứng dụng liên quan.
13. Ở phần bên phải của cửa sổ, hãy chọn **Quy tắc mạng** từ danh sách thả xuống.
Thao tác này sẽ mở danh sách các quy tắc mạng mặc định được thiết lập bởi Tường lửa.
14. Nhấn vào nút **Thêm**.
Thao tác này sẽ mở các thuộc tính quy tắc ứng dụng.
15. Nhập vào thủ công tên của dịch vụ mạng vào trường **Tên**.
16. Cấu hình thiết lập quy tắc mạng (xem bảng bên dưới).
Bạn có thể chọn một mẫu quy tắc được định sẵn bằng cách nhấn vào liên kết **Chọn mẫu**. Mẫu quy tắc mô tả các kết nối mạng được sử dụng thường xuyên nhất.
Tất cả thiết lập quy tắc mạng sẽ được điền tự động.
17. Nếu bạn muốn hành động của quy tắc mạng được phản ánh trong [báo cáo](#), hãy chọn hộp kiểm **Ghi lại sự kiện**.

18. Lưu quy tắc mạng.

Quy tắc mạng mới sẽ được thêm vào danh sách.

19. Sử dụng các nút **Lên / Xuống** để đặt mức độ ưu tiên của quy tắc mạng.


20. Lưu các thay đổi của bạn.

Thiết lập Quy tắc cho ứng dụng mạng

Tham số	Mô tả
Hành động	Cho phép. Chặn.
Giao thức	Kiểm soát hoạt động mạng qua giao thức đã chọn: TCP, UDP, ICMP, ICMPv6, IGMP và GRE. Nếu chọn giao thức ICMP hoặc ICMPv6, bạn có thể xác định loại gói tin và mã ICMP. 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.
Hướng	Gói tin vào. Gói tin vào / Gói tin ra. Gói tin ra.
Địa chỉ từ xa	Các địa chỉ mạng của các máy tính từ xa có thể gửi và nhận gói tin mạng. Tường lửa sẽ áp đặt quy tắc mạng cho dải địa chỉ mạng từ xa được chỉ định. Bạn có thể thêm tất cả các địa chỉ IP vào một quy tắc mạng, tạo một danh sách địa chỉ IP riêng, chỉ định một dải địa chỉ IP hoặc chọn một mạng con (Mạng tin tưởng, Mạng cục bộ, Mạng công cộng). Bạn cũng có thể chỉ định tên DNS của máy tính thay vì địa chỉ IP. Bạn chỉ nên sử dụng tên DNS cho các máy tính mạng LAN hoặc các dịch vụ nội bộ. Tương tác với các dịch vụ đám mây (như Microsoft Azure) và các tài nguyên Internet khác nên được xử lý bởi thành phần Kiểm soát Web. Kaspersky Endpoint Security hỗ trợ tên DNS kể từ phiên bản 11.7.0. Nếu bạn chỉ định tên DNS cho phiên bản 11.6.0 hoặc thấp hơn, Kaspersky Endpoint Security có thể áp dụng quy tắc liên quan cho mọi địa chỉ.
Địa chỉ nội bộ	Các địa chỉ mạng của các máy tính có thể gửi và nhận gói tin mạng. Tường lửa sẽ áp đặt một quy tắc mạng đến khoảng địa chỉ mạng nội bộ được quy định. Bạn có thể thêm tất cả các địa chỉ IP vào một quy tắc mạng, tạo một danh sách địa chỉ IP riêng hoặc chỉ định một dải địa chỉ IP. <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">Kaspersky Endpoint Security hỗ trợ tên DNS kể từ phiên bản 11.7.0. Nếu bạn chỉ định tên DNS cho phiên bản 11.6.0 hoặc thấp hơn, Kaspersky Endpoint Security có thể áp dụng quy tắc liên quan cho mọi địa chỉ.</div> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">Đôi khi địa chỉ nội bộ không thể được lấy cho các ứng dụng. Nếu đúng, tham số này sẽ bị bỏ qua.</div>

Bật và tắt một quy tắc mạng cho ứng dụng


Để bật hoặc tắt một quy tắc mạng cho ứng dụng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Tường lửa**.
3. Nhấn vào **Quy tắc cho ứng dụng**.
Thao tác này sẽ mở danh sách quy tắc 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 chuột phải để mở menu ngữ cảnh và chọn **Chi tiết và quy tắc**.
Cửa sổ thuộc tính và quy tắc ứng dụng sẽ mở ra.
6. Chọn thẻ **Quy tắc mạng**.
7. Trong danh sách các quy tắc mạng cho một nhóm ứng dụng, chọn quy tắc mạng liên quan.
Cửa sổ thuộc tính quy tắc mạng sẽ mở ra.
8. Đặt trạng thái **Hoạt động** hoặc **Không hoạt động** của quy tắc mạng.
Bạn không thể tắt một quy tắc mạng cho nhóm ứng dụng được tạo bởi Tường lửa ở chế độ mặc định.
9. Lưu các thay đổi của bạn.

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. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Tường lửa**.
3. Nhấn vào **Quy tắc cho ứng dụng**.
Thao tác này sẽ mở danh sách quy tắc 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. Nhấn chuột phải để mở menu ngữ cảnh, chọn **Quy tắc mạng**, sau đó chọn hành động bạn muốn gán:

- **Kế thừa.**
- **Cho phép.**
- **Chặn.**

6. Lưu các thay đổi của bạn.

Để thay đổi phản ứng của Tường lửa cho một quy tắc mạng cho một ứng dụng hoặc nhóm ứng dụng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Tường lửa**.
3. Nhấn vào **Quy tắc cho ứng dụng**.
Thao tác này sẽ mở danh sách quy tắc 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 chuột phải để mở menu ngữ cảnh và chọn **Chi tiết và quy tắc**.
Cửa sổ thuộc tính và quy tắc ứng dụng sẽ mở ra.
6. 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:
 - **Kế thừa.**
 - **Cho phép.**
 - **Từ chối.**
 - **Ghi lại sự kiện.**
9. Lưu các thay đổi của bạn.


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. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Tường lửa**.
3. Nhấn vào **Quy tắc cho ứng dụng**.
Thao tác này sẽ mở danh sách quy tắc 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 chuột phải để mở menu ngữ cảnh và chọn **Chi tiết và quy tắc**.
Cửa sổ thuộc tính và quy tắc ứng dụng sẽ mở ra.
6. 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 **Lên** / **Xuống** để đặt mức độ ưu tiên của quy tắc mạng.
9. Lưu các thay đổi của bạn.

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 theo thời gian thực.

Để bắt đầu *Giám sát mạng*:

Trong cửa sổ chính của ứng dụng, trong mục **Giám sát**, hãy nhấn ô **Giám sát mạng**.

Cửa sổ *Giám sát mạng* sẽ mở ra. Trong cửa sổ này, những thông tin về hoạt động mạng của máy tính sẽ được hiển thị trên bốn thẻ:

- Thẻ **Hoạt động mạng** 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. Trên thẻ này, bạn cũng có thể [tạo những quy tắc cho gói tin mạng](#) cho hoạt động của Tường lửa.
- Thẻ **Mở cổng** liệt kê tất cả cổng mạng mở của máy tính. Trên thẻ này, bạn cũng có thể [tạo những quy tắc cho gói tin mạng](#) và [quy tắc ứng dụng](#) cho hoạt động của Tường lửa.
- Thẻ **Lưu lượng 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 chặn** hiển thị các địa chỉ IP của những máy tính từ xa có hoạt động mạng bị chặn bởi thành phần Bảo vệ mối đe dọa mạng sau khi phát hiện các nỗ lực tấn công mạng từ những địa chỉ IP đó.

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. Một ví dụ về hậu quả đó là virus có thể thực thi các lệnh dưới quyền tài khoản người dùng của bạn để tải xuống phần mềm độc hại.

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 với máy tính và hệ điều hành xác định đó là một bàn phím thì ứng dụng sẽ nhắc người dùng nhập một mã số do ứng dụng tạo ra từ bàn phím này hoặc sử dụng [Bàn phím ảo](#) nếu có (xem hình bên dưới). Thủ tục này được gọi là xác thực bàn phím.

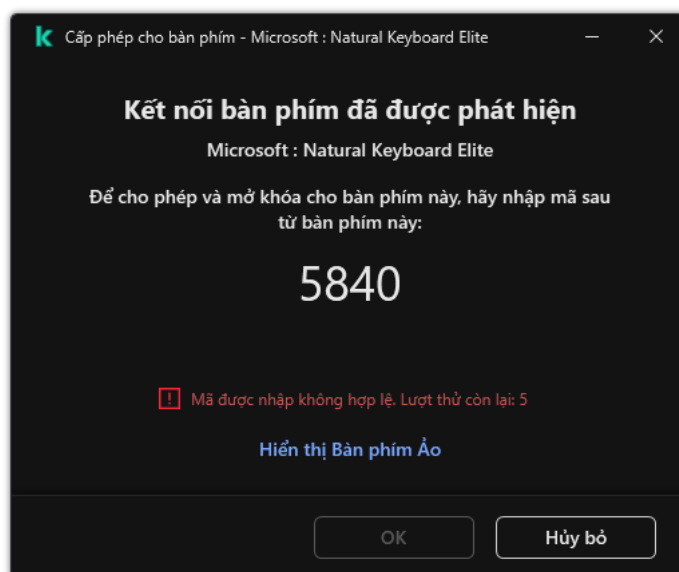
Nếu đã nhập đúng mã, ứng dụng sẽ lưu lại các tham số nhận dạng – VID/PID của bàn phím và số hiệu của cổng kết nối với ứng dụng – trong danh sách các bàn phím được xác thực. Không cần phải lặp lại việc xác thực bàn phím khi kết nối lại bàn phím hoặc sau khi khởi động lại hệ điều hành.

Khi kết nối bàn phím được xác thực với một cổng USB khác của máy tính, thì ứng dụng sẽ hiển thị một lời nhắc để xác thực lại bàn phím này.

Nếu mã số này không được nhập chính xác, ứng dụng sẽ tạo một mã mới. Bạn có thể [cấu hình số lượt thử nhập mã số](#). Nếu mã số được nhập sai vài lần hoặc cửa sổ cấp phép cho bàn phím bị đóng (xem hình bên dưới) thì ứng dụng sẽ chặn nhập vào từ bàn phím này. Khi hết thời gian chặn thiết bị USB hoặc hệ điều hành được khởi động lại, ứng dụng sẽ nhắc người dùng thực hiện lại quy trình cấp phép cho bàn phím.

Ứng dụng sẽ cho phép sử dụng một bàn phím được xác thực và chặn bàn phím không được xác thực.

Thành phần Phòng chống Tấn công BadUSB không được cài đặt theo mặc định. Nếu cần thành phần Phòng chống Tấn công BadUSB, bạn có thể thêm thành phần này trong thuộc tính của [gói cài đặt](#) trước khi cài đặt ứng dụng hoặc [thay đổi các thành phần ứng dụng có sẵn](#) sau khi cài đặt ứng dụng.




Chứng thực bàn phím

Bật và tắt Phòng chống Tấn công BadUSB

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.

Để bật hoặc tắt Phòng chống Tấn công BadUSB:


1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Phòng chống Tấn công BadUSB**.
3. Sử dụng nút bật/tắt **Phòng chống Tấn công BadUSB** để bật hoặc tắt thành phần.
4. Trong mục **Cấp phép cho bàn phím USB khi kết nối**, hãy điều chỉnh thiết lập bảo mật để nhập mã cho phép:
 - **Số lượng lời nhắc cho phép thiết bị USB tối đa.** Tự động chặn thiết bị USB nếu mã cho phép được nhập sai số lần được chỉ định. Giá trị hợp lệ là 1 đến 10. Ví dụ: nếu bạn cho phép 5 lần nhập mã cho phép, thiết bị USB sẽ bị chặn sau lần thứ năm không thành công. Kaspersky Endpoint Security sẽ hiển thị thời lượng chặn cho thiết bị USB. Sau khi hết thời gian này, bạn có thể có 5 lần thử nhập mã cho phép.
 - **Kết thúc thời gian chờ khi đạt số lượng lời nhắc tối đa.** Thời gian chặn của thiết bị USB sau số lần nhập mã cho phép không thành công được chỉ định. Giá trị hợp lệ là 1 đến 180 (phút).
5. Lưu các thay đổi của bạn.

Kết quả là nếu thành phần Phòng chống Tấn công BadUSB được bật, Kaspersky Endpoint Security yêu cầu cho phép một thiết bị USB được kết nối được xác định là bàn phím bởi hệ điều hành. Người dùng không thể sử dụng một bàn phím chưa được xác thực cho đến khi nó đã được xác thực.

Sử dụng Bàn phím ảo để xác thực các thiết bị USB

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.

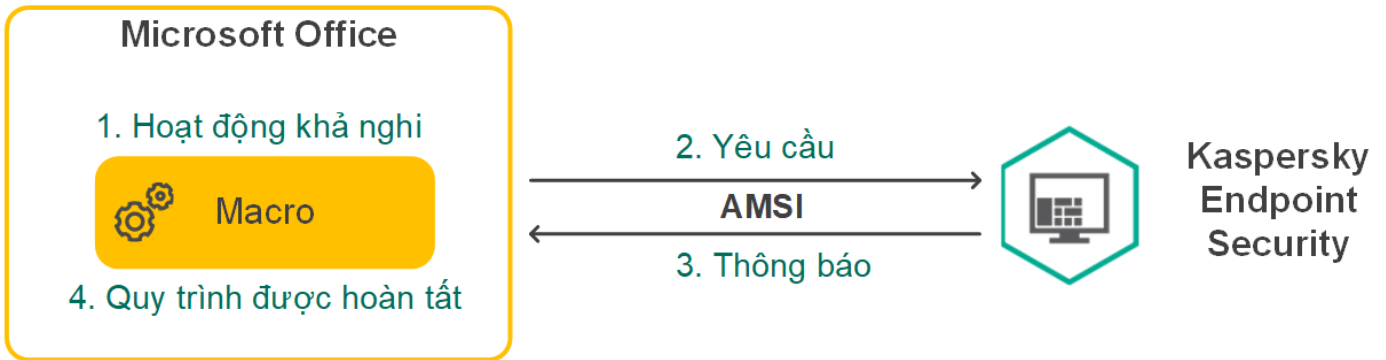
Để cho phép và cấm sử dụng Bàn phím Ảo để xác thực:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Phòng chống Tấn công BadUSB**.
3. Sử dụng hộp kiểm **Nghiêm cấm việc sử dụng Bàn phím ảo để xác thực các thiết bị USB** để chặn hoặc cho phép việc sử dụng Bàn phím ảo để xác thực.
4. Lưu các thay đổi của bạn.

Bảo vệ AMSI

Thành phần Bảo vệ AMSI được dành để hỗ trợ Antimalware Scan Interface của Microsoft. *Antimalware Scan Interface (AMSI)* cho phép các ứng dụng thuộc bên thứ ba có hỗ trợ AMSI gửi các đối tượng (ví dụ như kịch bản PowerShell) đến Kaspersky Endpoint Security để quét bổ sung và sau đó nhận kết quả từ việc quét cho các đối tượng này. Các ứng dụng thuộc bên thứ ba ví dụ như các ứng dụng Microsoft Office (xem hình bên dưới). Để biết chi tiết về AMSI, vui lòng tham khảo [tài liệu của Microsoft](#).

Thành phần Bảo vệ AMSI chỉ có thể phát hiện một mối đe dọa và thông báo cho một ứng dụng thuộc bên thứ ba về mối đe dọa được phát hiện. Ứng dụng thuộc bên thứ ba, sau khi nhận được thông báo về mối đe dọa, không cho phép thực hiện các hành động độc hại (ví dụ như chấm dứt).



Ví dụ về hoạt động của AMSI

Thành phần Bảo vệ AMSI có thể từ chối một yêu cầu từ một ứng dụng thuộc bên thứ ba, ví dụ như nếu ứng dụng này vượt quá số yêu cầu tối đa trong một chu kỳ quy định. Kaspersky Endpoint Security sẽ gửi thông tin về một yêu cầu bị từ chối từ ứng dụng thuộc bên thứ ba đến Máy chủ quản trị. Thành phần Bảo vệ AMSI không từ chối các yêu cầu từ các ứng dụng của bên thứ ba có [tích hợp liên tục với thành phần Bảo vệ AMSI](#) được bật.

Bảo vệ AMSI có thể được sử dụng cho các hệ điều hành sau đây cho máy trạm và máy chủ:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise;
- Windows 11;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2022.

Bật và tắt Bảo vệ AMSI

Theo mặc định, Bảo vệ AMSI được bật.

Để bật hoặc tắt Bảo vệ AMSI:


1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút

2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Bảo vệ AMSI**.
3. Sử dụng nút bật/tắt **Bảo vệ AMSI** để bật hoặc tắt thành phần.
4. Lưu các thay đổi của bạn.

Sử dụng Bảo vệ AMSI để 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 hỗn hợp ví dụ như tập nén. 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 các loại tập tin hỗn hợp được quét để tăng tốc độ quét.

Để cấu hình tính năng quét các tập tin tổng hợp của Bảo vệ AMSI:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa thiết yếu** → **Bảo vệ AMSI**.
3. Trong mục **Quét các tập tin tổng hợp**, quy định loại tập tin hỗn hợp mà bạn muốn quét: tập nén, gói phân phối, hoặc tập tin trong định dạng văn bản.
4. Trong mục **Dung lượng giới hạn**, hãy thực hiện một trong những hành động sau:
 - Để chặn thành phần Bảo vệ AMSI giải nén các tập tin hỗn hợp quá lớn, hãy chọn hộp kiểm **Không giải nén các tập tin phức hợp lớn** và chỉ định giá trị cần thiết trong trường **Dung lượng tối đa của tập tin**. Thành phần Bảo vệ AMSI sẽ không giải nén các tập tin hỗn hợp lớn hơn dung lượng được quy định.
 - Để cho phép Bảo vệ AMSI giải nén các tập tin hỗn hợp lớn, hãy xóa hộp kiểm **Không giải nén các tập tin phức hợp lớn**.

Thành phần Bảo vệ AMSI sẽ quét các tập tin lớn được giải nén từ tập nén, bất kể là hộp kiểm **Không giải nén các tập tin phức hợp lớn** có được chọn hay không.

5. Lưu các thay đổi của bạn.


Phòng chống khai thác

Thành phần Phòng chống khai thác sẽ phát hiện mã chương trình lợi dụng các lỗ hổng trên máy tính để khai thác quyền của quản trị viên hoặc thực hiện các hoạt động độc hại. Ví dụ như mã khai thác có thể sử dụng một cuộc tấn công tràn bộ đệm. Để thực hiện, mã khai thác sẽ gửi số lượng lớn dữ liệu đến một ứng dụng chứa lỗ hổng. Khi xử lý dữ liệu này, ứng dụng chứa lỗ hổng bảo mật sẽ thực thi mã độc. Kết quả của cuộc tấn công này là mã khai thác có thể tiến hành cài đặt trái phép phần mềm độc hại. Khi có một nỗ lực chạy một tập tin thực thi từ một ứng dụng có lỗ hổng bảo mật không được thực hiện bởi người dùng, Kaspersky Endpoint Security sẽ chặn việc khởi chạy tập tin đó hoặc thông báo cho người dùng.

Bật và tắt Phòng chống khai thác

Theo mặc định, Phòng chống khai thác sẽ được bật và chạy trong chế độ được khuyến nghị bởi các chuyên gia của Kaspersky. Bạn có thể tắt Phòng chống khai thác nếu cần thiết.

Để bật hoặc tắt Phòng chống khai thác:


1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa nâng cao** → **Phòng chống khai thác**.
3. Sử dụng nút bật/tắt **Phòng chống khai thác** để bật hoặc tắt thành phần.
4. Lưu các thay đổi của bạn.

Kết quả là nếu thành phần Phòng chống khai thác được bật, Kaspersky Endpoint Security sẽ giám sát các tập tin thực thi được chạy bởi các ứng dụng để bị tấn công. Nếu Kaspersky Endpoint Security phát hiện một tập tin thực thi từ một ứng dụng có lỗi hỏng bảo mật bị chạy bởi một người không phải người dùng của máy, Kaspersky Endpoint Security sẽ thực hiện hành động được chọn (ví dụ: sẽ chặn hoạt động).

Chọn một hành động để thực hiện khi phát hiện mã khai thác

Theo mặc định, khi phát hiện một mã khai thác, Kaspersky Endpoint Security sẽ chặn thao tác mà mã khai thác đó đang cố thực hiện.


Để chọn một hành động được thực hiện khi phát hiện mã khai thác:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa nâng cao** → **Phòng chống khai thác**.
3. Chọn hành động liên quan trong mục **Khi phát hiện khai thác**:
 - **Chặn hoạt động**. Nếu mục này được chọn, khi phát hiện một mã khai thác, Kaspersky Endpoint Security sẽ chặn hoạt động của mã khai thác này và lập một mục nhật ký chứa thông tin về mã khai thác.
 - **Thông báo**. Nếu mục này được chọn, khi Kaspersky Endpoint Security phát hiện một mã khai thác, ứng dụng sẽ ghi lại một sự kiện chứa thông tin về mã khai thác đó và bổ sung thông tin về mã khai thác vào [danh sách các mối đe dọa đang hoạt động](#).
4. Lưu các thay đổi của bạn.

Bảo vệ bộ nhớ của tiến trình hệ thống

Theo mặc định, tính năng bảo vệ bộ nhớ tiến trình hệ thống được bật.

Để bật hoặc tắt tính năng bảo vệ bộ nhớ tiến trình hệ thống:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa nâng cao** → **Phòng chống khai thác**.
3. Sử dụng nút bật/tắt **Bật bảo vệ bộ nhớ tiến trình hệ thống** để bật hoặc tắt tính năng này.
4. Lưu các thay đổi của bạn.

Kết quả là Kaspersky Endpoint Security sẽ chặn các tiến trình bên ngoài cố gắng truy cập các tiến trình hệ thống.

Phát hiện hành vi


Thành phần Phát hiện hành vi nhận dữ liệu về hành động của các ứng dụng trên máy tính của bạn và cung cấp thông tin này đến các thành phần bảo vệ khác để cải thiện hiệu quả của chúng. Thành phần Phát hiện hành vi sử dụng Dấu hiệu dòng hành vi (BSS) cho các ứng dụng. Nếu hoạt động của ứng dụng khớp với một dấu hiệu dòng hành vi cụ thể, Kaspersky Endpoint Security sẽ thực hiện hành động phản ứng được chọn. Chức năng của Kaspersky Endpoint Security dựa trên các dấu hiệu dòng hành vi cung cấp chủ động bảo vệ cho máy tính.

Bật và tắt Phát hiện hành vi

Theo mặc định, Phát hiện hành vi sẽ được bật và chạy trong chế độ được khuyến nghị bởi các chuyên gia của Kaspersky. Bạn có thể tắt Phát hiện hành vi nếu cần thiết.

Bạn không nên tắt Phát hiện hành vi trừ khi là tuyệt đối cần thiết, bởi điều này sẽ làm giảm hiệu năng của các thành phần bảo vệ. Thành phần bảo vệ có thể yêu cầu dữ liệu được thu thập bởi thành phần Phát hiện hành vi để phát hiện các mối đe dọa.

Để bật hoặc tắt Phát hiện hành vi:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa nâng cao** → **Phát hiện hành vi**.
3. Sử dụng nút bật/tắt **Phát hiện hành vi** để bật hoặc tắt thành phần.
4. Lưu các thay đổi của bạn.

Kết quả là nếu tính năng Phát hiện hành vi được bật, Kaspersky Endpoint Security sẽ sử dụng mã nhận diện dòng hành vi để phân tích hoạt động của các ứng dụng trong hệ điều hành.

Chọn hành động để thực hiện khi phát hiện hoạt động của phần mềm độc hại

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

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .

- Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa nâng cao** → **Phát hiện hành vi**.
- Chọn hành động liên quan trong mục **Khi phát hiện hoạt động của phần mềm độc hại**:
 - Delete file**. Nếu mục này được chọn, khi phát hiện hoạt động độc hại, Kaspersky Endpoint Security sẽ xóa tập tin thực thi của ứng dụng độc hại và tạo một bản sao lưu của tập tin đó trong Sao lưu.
 - Chấm dứt ứng dụng**. Nếu đề mục này được chọn, khi phát hiện hoạt động độc hại, Kaspersky Endpoint Security sẽ chấm dứt hoạt động của ứng dụng này.
 - Thông báo**. Nếu mục này được chọn và phát hiện hoạt động độc của phần mềm độc hại của một ứng dụng, Kaspersky Endpoint Security sẽ bổ sung thông tin về hoạt động độc hại của ứng dụng này đến danh sách các mối đe dọa đang hoạt động.
- Lưu các thay đổi của bạn.

Bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài

Thành phần này chỉ giám sát các hoạt động được thực hiện với những tập tin được lưu trữ trên thiết bị lưu trữ dung lượng lớn có hệ thống tập tin NTFS và không được mã hóa EFS.

Bật tính năng bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài cung cấp tính năng phân tích hoạt động trong các thư mục được chia sẻ. Nếu hoạt động này khớp với một dấu hiệu dòng hành vi giống với hoạt động mã hóa từ bên ngoài, Kaspersky Endpoint Security sẽ thực hiện hành động được chọn.


Theo mặc định, tính năng bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài bị tắt.

Sau khi Kaspersky Endpoint Security được cài đặt, tính năng bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài sẽ bị hạn chế cho đến khi máy tính được khởi động lại.

Bật hoặc tắt bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài

Sau khi Kaspersky Endpoint Security được cài đặt, tính năng bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài sẽ bị hạn chế cho đến khi máy tính được khởi động lại.


Để bật hoặc tắt bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài:

- Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
- Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa nâng cao** → **Phát hiện hành vi**.
- Sử dụng nút bật/tắt **Bật tính năng bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài** để bật hoặc tắt tính năng phát hiện hoạt động điển hình của mã hóa bên ngoài.

4. Lưu các thay đổi của bạn.

Chọn hành động khi phát hiện nỗ lực mã hóa các thư mục được chia sẻ từ bên ngoài

Để chọn hành động khi phát hiện nỗ lực mã hóa các thư mục được chia sẻ từ bên ngoài:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa nâng cao** → **Phát hiện hành vi**.
3. Chọn hành động liên quan trong mục **Bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài**:
 - **Chặn kết nối trong N phút (từ 1 đến 43800)**. Nếu chọn tùy chọn này và Kaspersky Endpoint Security phát hiện hành động cố sửa đổi tập tin trong thư mục chia sẻ thì ứng dụng sẽ thực hiện các hành động sau:
 - Chặn quyền truy cập sửa đổi tập tin cho phiên được khởi tạo hoạt động độc hại (tập tin sẽ ở chế độ chỉ đọc).
 - Tạo các bản sao lưu của tập tin đang được sửa đổi.
 - Thêm một mục vào [báo cáo giao diện ứng dụng cục bộ](#).
 - Gửi thông tin về hoạt động độc hại được phát hiện tới Kaspersky Security Center.

Ngoài ra, nếu thành phần Công cụ khắc phục được bật, các tập tin đã sửa đổi sẽ được khôi phục từ bản sao lưu.

 - **Thông báo**. Nếu chọn tùy chọn này và Kaspersky Endpoint Security phát hiện hành động cố sửa đổi tập tin trong thư mục chia sẻ thì ứng dụng sẽ thực hiện các hành động sau:
 - Thêm một mục vào [báo cáo giao diện ứng dụng cục bộ](#).
 - Thêm một mục vào danh sách các mối đe dọa đang hoạt động.
 - Gửi thông tin về hoạt động độc hại được phát hiện tới Kaspersky Security Center.

4. Lưu các thay đổi của bạn.

Tạo một loại trừ cho tính năng bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài

Việc loại trừ một thư mục có thể giảm số lượng cảnh báo nhầm nếu tổ chức của bạn sử dụng mã hóa dữ liệu khi trao đổi tập tin bằng các thư mục chia sẻ. Ví dụ: tính năng Phát hiện hành vi có thể làm tăng kết quả cảnh báo nhầm khi người dùng làm việc với các tập tin có phần mở rộng ENC trong một thư mục chia sẻ. Hoạt động như vậy phù hợp với một kiểu hành vi điển hình cho mã hóa bên ngoài. Nếu bạn có các tập tin được mã hóa trong một thư mục chia sẻ để bảo vệ dữ liệu, hãy thêm thư mục đó vào mục loại trừ.

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Exclusions**.
6. Trong mục **Loại trừ quét và ứng dụng được tin tưởng**, hãy nhấn nút **Thiết lập**.
7. Trong cửa sổ mở ra, hãy chọn thẻ **Loại trừ quét**.
Thao tác này sẽ mở cửa sổ chứa danh sách các loại trừ.
8. Chọn hộp kiểm **Merge values when inheriting** nếu bạn muốn tạo một danh sách tổng hợp các loại trừ cho tất cả các máy tính trong công ty. Danh sách các loại trừ trong chính sách cha và chính sách con sẽ được hợp nhất. Các danh sách sẽ được hợp nhất với điều kiện các giá trị hợp nhất khi kế thừa được bật. Các loại trừ từ chính sách cha được hiển thị trong chính sách con ở chế độ chỉ đọc. Không thể thay đổi hay xóa các loại trừ của chính sách cha.
9. Chọn hộp kiểm **Allow use of local trusted applications** nếu bạn muốn cho phép người dùng tạo danh sách loại trừ cục bộ. Bằng cách này, người dùng có thể tạo danh sách loại trừ của riêng họ ngoài danh sách loại trừ chung được tạo trong chính sách. Quản trị viên có thể sử dụng Kaspersky Security Center để xem, thêm, chỉnh sửa hoặc xóa các mục danh sách trong thuộc tính máy tính.
Nếu hộp kiểm bị xóa, người dùng chỉ có thể truy cập danh sách loại trừ được tạo trong chính sách.
10. Nhấn vào **Thêm**.
11. Trong mục **Thuộc tính**, hãy chọn hộp kiểm **Tập tin hoặc thư mục**.
12. Nhấn vào liên kết **chọn tập tin/thư mục** trong mục **Mô tả loại trừ quét (bấm vào mục gạch chân để chỉnh sửa)** để mở cửa sổ **Tên của tập tin hoặc thư mục**.
13. Nhấn vào **Duyệt** và chọn thư mục chia sẻ.
Bạn cũng có thể nhập đường dẫn theo cách thủ công. Kaspersky Endpoint Security hỗ trợ các ký tự * và ? khi nhập tên đại diện:
 - Ký tự * (hoa thị) thay thế bất kỳ nhóm ký tự nào bộ ký tự, ngoại trừ các ký tự \ và / (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ, ký tự đại diện C:**.txt sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng TXT nằm trong các thư mục trên ổ C:, nhưng không phải trong các thư mục con.
 - Hai ký tự * liên tiếp thay thế bất kỳ nhóm ký tự nào (bao gồm nhóm rỗng) trong tên tập tin hoặc thư mục, bao gồm các ký tự \ và / (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ, ký tự đại diện C:\Folder**.txt sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng TXT nằm trong các thư mục con bên trong Folder, ngoại trừ chính Folder. Một đại diện phải có ít nhất một cặp lồng ghép. C:**.txt không phải là một đại diện hợp lệ.

- Ký tự ? (dấu hỏi) thay thế bất kỳ ký tự đơn nào, ngoại trừ các ký tự \ và / (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ: đại diện C:\Folder\???.txt sẽ bao gồm các đường dẫn đến tất cả các tập tin có trong thư mục Folder có phần mở rộng TXT và tên có ba ký tự.

14. Nếu cần thiết, trong trường **Bình luận**, nhập một nhận xét ngắn về loại trừ quét mà bạn đang tạo.
15. Nhấn vào liên kết **bất kỳ** trong mục **Mô tả loại trừ quét (bấm vào mục gạch chân để chỉnh sửa)** để kích hoạt liên kết **lựa chọn các thành phần**.
16. Nhấn vào liên kết **lựa chọn các thành phần** để mở ra cửa sổ **Thành phần bảo vệ**.
17. Chọn hộp kiểm bên cạnh thành phần **Phát hiện hành vi**.
18. Lưu các thay đổi của bạn.

[Cách tạo một mục loại trừ để bảo vệ các thư mục chia sẻ bằng Bảng điều khiển web và Bảng điều khiển đám mây](#)


1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Thiết lập tổng quát** → **Exclusions**.
5. Trong mục **Scan exclusions and trusted applications**, hãy nhấn liên kết **Scan exclusions**.
6. Chọn hộp kiểm **Merge values when inheriting** nếu bạn muốn tạo một danh sách tổng hợp các loại trừ cho tất cả các máy tính trong công ty. Danh sách các loại trừ trong chính sách cha và chính sách con sẽ được hợp nhất. Các danh sách sẽ được hợp nhất với điều kiện các giá trị hợp nhất khi kế thừa được bật. Các loại trừ từ chính sách cha được hiển thị trong chính sách con ở chế độ chỉ đọc. Không thể thay đổi hay xóa các loại trừ của chính sách cha.
7. Chọn hộp kiểm **Allow use of local trusted applications** nếu bạn muốn cho phép người dùng tạo danh sách loại trừ cục bộ. Bằng cách này, người dùng có thể tạo danh sách loại trừ của riêng họ ngoài danh sách loại trừ chung được tạo trong chính sách. Quản trị viên có thể sử dụng Kaspersky Security Center để xem, thêm, chỉnh sửa hoặc xóa các mục danh sách trong thuộc tính máy tính.
Nếu hộp kiểm bị xóa, người dùng chỉ có thể truy cập danh sách loại trừ được tạo trong chính sách.
8. Nhấn vào nút **Thêm**.
9. Chọn cách bạn muốn thêm loại trừ **File or folder**.
10. Nhấn vào **Duyệt** và chọn thư mục chia sẻ.
Bạn cũng có thể nhập đường dẫn theo cách thủ công. Kaspersky Endpoint Security hỗ trợ các ký tự * và ? khi nhập tên đại diện:
 - Ký tự * (hoa thị) thay thế bất kỳ nhóm ký tự nào bộ ký tự, ngoại trừ các ký tự \ và / (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ, ký tự đại diện C:**.txt sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng TXT nằm trong các thư mục trên ổ C:, nhưng không phải trong các thư mục con.
 - Hai ký tự * liên tiếp thay thế bất kỳ nhóm ký tự nào (bao gồm nhóm rỗng) trong tên tập tin hoặc thư mục, bao gồm các ký tự \ và / (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ, ký tự đại diện C:\Folder***.txt sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng TXT nằm trong các thư mục con bên trong Folder, ngoại trừ chính Folder. Một đại diện phải có ít nhất một cặp lồng ghép. C:***.txt không phải là một đại diện hợp lệ.
 - Ký tự ? (dấu hỏi) thay thế bất kỳ ký tự đơn nào, ngoại trừ các ký tự \ và / (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ: đại diện C:\Folder\???.txt sẽ bao gồm các đường dẫn đến tất cả các tập tin có trong thư mục Folder có phần mở rộng TXT và tên có ba ký tự.
11. Trong mục **Thành phần bảo vệ**, hãy chọn thành phần **Phát hiện hành vi**.
12. Nếu cần thiết, trong trường **Bình luận**, nhập một nhận xét ngắn về loại trừ quét mà bạn đang tạo.

13. Chọn trạng thái **Hoạt động** cho loại trừ.

Bạn có thể sử dụng nút bật/tắt để [dừng loại trừ](#) bất kỳ lúc nào.

14. Lưu các thay đổi của bạn.

Cách tạo một mục loại trừ để bảo vệ các thư mục chia sẻ trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .

2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Mối đe dọa và loại trừ**.

3. Trong mục **Loại trừ**, hãy nhấn liên kết **Quản lý loại trừ**.

4. Nhấn vào **Thêm**.

5. Nhấn vào **Duyệt** và chọn thư mục chia sẻ.

Bạn cũng có thể nhập đường dẫn theo cách thủ công. Kaspersky Endpoint Security hỗ trợ các ký tự * và ? khi nhập tên đại diện:

- Ký tự * (hoa thị) thay thế bất kỳ nhóm ký tự nào bộ ký tự, ngoại trừ các ký tự \ và / (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ, ký tự đại diện C:**.txt sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng TXT nằm trong các thư mục trên ổ C:, nhưng không phải trong các thư mục con.
- Hai ký tự * liên tiếp thay thế bất kỳ nhóm ký tự nào (bao gồm nhóm rỗng) trong tên tập tin hoặc thư mục, bao gồm các ký tự \ và / (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ, ký tự đại diện C:\Folder***.txt sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng TXT nằm trong các thư mục con bên trong Folder, ngoại trừ chính Folder. Một đại diện phải có ít nhất một cặp lồng ghép. C:***.txt không phải là một đại diện hợp lệ.
- Ký tự ? (dấu hỏi) thay thế bất kỳ ký tự đơn nào, ngoại trừ các ký tự \ và / (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ: đại diện C:\Folder\???.txt sẽ bao gồm các đường dẫn đến tất cả các tập tin có trong thư mục Folder có phần mở rộng TXT và tên có ba ký tự.

6. Trong mục **Thành phần bảo vệ**, hãy chọn thành phần **Phát hiện hành vi**.

7. Nếu cần thiết, trong trường **Bình luận**, nhập một nhận xét ngắn về loại trừ quét mà bạn đang tạo.

8. Chọn trạng thái **Hoạt động** cho loại trừ.

Bạn có thể sử dụng nút bật/tắt để [dừng loại trừ](#) bất kỳ lúc nào.


9. Lưu các thay đổi của bạn.

Cấu hình các địa chỉ được loại trừ khỏi tính năng bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài

Dịch vụ Audit Logon phải được bật để có thể loại trừ các địa chỉ khởi tính năng bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài. Theo mặc định, dịch vụ Audit Logon sẽ bị tắt (để biết thêm thông tin về việc bật dịch vụ Audit Logon, vui lòng truy cập website của Microsoft).

Chức năng loại trừ các địa chỉ ra khỏi tính năng bảo vệ thư mục được chia sẻ không hoạt động trên một máy tính từ xa nếu bật máy tính từ xa đó đã được bật đó trước khi khởi động Kaspersky Endpoint Security được khởi động. Bạn có thể khởi động lại máy tính từ xa này sau khi khởi động Kaspersky Endpoint Security để đảm bảo chức năng loại trừ các địa chỉ rạch khỏi tính năng bảo vệ thư mục được chia sẻ hoạt động trên máy tính từ xa này.

Để loại trừ các máy tính từ xa thực hiện mã hóa từ bên ngoài cho các thư mục được chia sẻ:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa nâng cao** → **Phát hiện hành vi**.
3. Trong mục **Loại trừ**, hãy nhấn liên kết **Cấu hình danh sách loại trừ**.
4. Nếu bạn muốn thêm một địa chỉ IP hoặc tên máy tính vào danh sách loại trừ, hãy nhấn nút **Thêm**.
5. Nhập vào địa chỉ IP hoặc tên của máy tính mà ứng dụng sẽ không can thiệp vào các nỗ lực mã hóa từ bên ngoài từ đó.
6. Lưu các thay đổi của bạn.

Xuất và nhập danh sách loại trừ từ Bật tính năng bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài

Bạn có thể xuất danh sách loại trừ ra tập tin XML. Sau đó, bạn có thể sửa đổi tập tin, ví dụ như thêm một số lượng lớn các địa chỉ cùng loại. Bạn cũng có thể sử dụng chức năng xuất/nhập để sao lưu danh sách các loại trừ hoặc để chuyển danh sách sang máy chủ khác.

[Cách xuất và nhập danh sách loại trừ trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mỗi đe dọa nâng cao** → **Phát hiện hành vi**.
6. Trong mục **Thiết lập Bảo vệ mỗi đe dọa mạng**, hãy nhấn nút **Loại trừ**.
7. Để xuất danh sách quy tắc:
 - a. Chọn các loại trừ mà bạn muốn xuất. Để chọn nhiều cổng, hãy sử dụng phím **CTRL** hoặc **SHIFT**. Nếu bạn không chọn loại trừ nào, Kaspersky Endpoint Security sẽ xuất tất cả các loại trừ.
 - b. Nhấn liên kết **Xuất**.
 - c. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin XML mà bạn muốn xuất danh sách các loại trừ vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
 - d. Lưu tập tin.
Kaspersky Endpoint Security sẽ xuất toàn bộ danh sách các loại trừ vào tập tin XML.
8. Để nhập danh sách loại trừ:
 - a. Nhấn **Nhập**.
 - b. Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách các loại trừ.
 - c. Mở tập tin.
Nếu máy tính đã có danh sách các loại trừ, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.
9. Lưu các thay đổi của bạn.

[Cách xuất và nhập danh sách loại trừ trong Bảng điều khiển web và Bảng điều khiển đám mây](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Bảo vệ mối đe dọa nâng cao** → **Phát hiện hành vi**.
5. Để xuất danh sách loại trừ trong mục **Loại trừ**:
 - a. Chọn các loại trừ mà bạn muốn xuất.
 - b. Nhấn vào **Xuất**.
 - c. Xác nhận rằng bạn chỉ muốn xuất các loại trừ đã chọn hoặc xuất toàn bộ danh sách loại trừ.
 - d. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin XML mà bạn muốn xuất danh sách các loại trừ vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
 - e. Lưu tập tin.
Kaspersky Endpoint Security sẽ xuất toàn bộ danh sách các loại trừ vào tập tin XML.
6. Để nhập danh sách các loại trừ trong mục **Loại trừ**:
 - a. Nhấn **Nhập**.
 - b. Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách các loại trừ.
 - c. Mở tập tin.
Nếu máy tính đã có danh sách các loại trừ, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.
7. Lưu các thay đổi của bạn.

Phòng chống xâm nhập máy chủ

Thành phần này khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows dành cho máy trạm. Thành phần này không khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows cho máy chủ.

Thành phần Phòng chống xâm nhập máy chủ 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 cá nhân. Thành phần này giúp bảo vệ máy tính với sự trợ giúp của cơ sở dữ liệu diệt virus và dịch vụ đám mây của Kaspersky Security Network.

Thành phần này kiểm soát hoạt động của các ứng dụng bằng cách sử dụng *các quyền của ứng dụng*. Các quyền của ứng dụng bao gồm các tham số truy cập sau:

- Truy cập vào tài nguyên của hệ điều hành (ví dụ: các tùy chọn khởi động tự động, khóa registry)
- Truy cập vào dữ liệu cá nhân (như các tập tin và ứng dụng)

Hoạt động mạng của các ứng dụng được kiểm soát bởi [Tường lửa](#) bằng cách sử dụng *quy tắc mạng*.

Trong lần khởi động đầu tiên của ứng dụng, thành phần Phòng chống xâm nhập máy chủ sẽ thực hiện các hành động sau:

1. Kiểm tra tính bảo mật của ứng dụng bằng cách cơ sở dữ liệu diệt virus đã tải xuống.
2. Kiểm tra tính bảo mật của ứng dụng trong Kaspersky Security Network.

Bạn nên [tham gia vào Kaspersky Security Network](#) để giúp thành phần Phòng chống xâm nhập máy chủ hoạt động hiệu quả hơn.

3. Đưa ứng dụng vào một trong các *nhóm tin tưởng*: Tin tưởng, Giới hạn mức Thấp, Giới hạn mức Cao, Không tin tưởng.

Một [nhóm tin tưởng quy định các quyền](#) được Kaspersky Endpoint Security áp dụng khi kiểm soát hoạt động của các ứng dụng trong nhóm đó. Kaspersky Endpoint Security sẽ đặt ứng dụng vào một nhóm tin tưởng tùy thuộc vào mức độ nguy hiểm mà ứng dụng này có thể gây ra cho máy tính.

Kaspersky Endpoint Security sẽ đặt ứng dụng vào nhóm tin tưởng cho các thành phần Tường lửa và Phòng chống xâm nhập máy chủ. Bạn chỉ không thể thay đổi nhóm tin tưởng cho Tường lửa hoặc Phòng chống xâm nhập máy chủ.

Nếu bạn từ chối tham gia vào KSN hoặc không có mạng, Kaspersky Endpoint Security sẽ đặt ứng dụng vào một nhóm tin tưởng tùy thuộc vào [thiết lập của thành phần Phòng chống xâm nhập máy chủ](#). Sau khi nhận được danh tiếng của ứng dụng từ KSN, nhóm tin tưởng có thể được thay đổi tự động.

4. Chặn các hành động của ứng dụng tùy thuộc vào nhóm tin tưởng. Ví dụ: các ứng dụng trong nhóm tin tưởng Giới hạn mức Cao bị từ chối truy cập vào các mô-đun hệ điều hành.

Khi ứng dụng được khởi chạy vào lần tới, Kaspersky Endpoint Security sẽ kiểm tra tính toàn vẹn của ứng dụng. Nếu ứng dụng không thay đổi, thành phần sẽ áp dụng các quyền của ứng dụng hiện tại cho nó. Nếu ứng dụng đã bị sửa đổi, Kaspersky Endpoint Security sẽ phân tích ứng dụng đó như khi ứng dụng đó được khởi chạy lần đầu tiên.

Bật và tắt Phòng chống xâm nhập máy chủ

Theo mặc định, thành phần Phòng chống xâm nhập máy chủ sẽ được bật và chạy trong chế độ được khuyến nghị bởi các chuyên gia của Kaspersky.

[Cách bật hoặc tắt thành phần Phòng chống xâm nhập máy chủ trong Bảng điều khiển quản trị \(MMC\)](#)




1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mỗi đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
6. Sử dụng hộp kiểm **Phòng chống xâm nhập máy chủ** để bật hoặc tắt thành phần.
7. Lưu các thay đổi của bạn.

[Cách bật hoặc tắt thành phần Phòng chống xâm nhập máy chủ trong Bảng điều khiển web và Bảng điều khiển đám mây](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Bảo vệ mỗi đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
5. Sử dụng nút bật/tắt **Phòng chống xâm nhập máy chủ** để bật hoặc tắt thành phần.
6. Lưu các thay đổi của bạn.

[Cách bật hoặc tắt thành phần Phòng chống xâm nhập máy chủ trong giao diện ứng dụng](#)

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
3. Sử dụng nút bật/tắt **Phòng chống xâm nhập máy chủ** để bật hoặc tắt thành phần.
4. Lưu các thay đổi của bạn.

Nếu thành phần Phòng chống xâm nhập máy chủ được bật, Kaspersky Endpoint Security sẽ đặt ứng dụng vào một [nhóm tin tưởng](#), tùy thuộc vào mức độ nguy hiểm mà ứng dụng này có thể gây ra cho máy tính. Kaspersky Endpoint Security sau đó sẽ chặn các hành động của ứng dụng, tùy thuộc vào nhóm tin tưởng.

Quản lý các nhóm tin tưởng ứng dụng

Khi mỗi ứng dụng được khởi động lần đầu tiên, thành phần Phòng chống xâm nhập máy chủ 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 sau đó, 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 mà Kaspersky Endpoint Security phải [tự động gán mọi ứng dụng chưa xác định](#) vào. Các ứng dụng được khởi chạy trước Kaspersky Endpoint Security sẽ tự động được di chuyển vào nhóm tin tưởng [được xác định trong thiết lập thành phần Phòng chống xâm nhập máy chủ](#).

Đối với các ứng dụng đã được khởi động trước Kaspersky Endpoint Security, thành phần này chỉ kiểm soát hoạt động mạng của chúng. Tính năng kiểm soát được thực hiện thông qua các quy tắc mạng được [xác định trong thiết lập Tường lửa](#).

Thay đổi nhóm tin tưởng của một ứng dụng

Khi mỗi ứng dụng được khởi động lần đầu tiên, thành phần Phòng chống xâm nhập máy chủ sẽ kiểm tra tính bảo mật của ứng dụng đó và đặt nó vào một [nhóm tin tưởng](#).

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 đổi các quyền cho một ứng dụng riêng lẻ](#) nếu cần thiết.


[Cách thay đổi nhóm tin tưởng của một ứng dụng trong Bảng điều khiển quản trị \(MMC\)](#) 


1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mỗi đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
6. Trong mục **Các quyền cho ứng dụng và tài nguyên được bảo vệ**, hãy nhấn nút **Thiết lập**.
Thao tác này sẽ mở ra cửa sổ cấu hình quyền của ứng dụng và danh sách các tài nguyên được bảo vệ.
7. Chọn thẻ **Các quyền của ứng dụng**.
8. Nhấn vào **Thêm**.
9. Trong cửa sổ mở ra, hãy nhập tiêu chí cho ứng dụng có nhóm tin tưởng mà bạn muốn thay đổi.
Bạn có thể nhập tên của ứng dụng hoặc tên của nhà cung cấp. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự * cùng ? khi nhập tên đại diện.
10. Nhấn vào nút **Làm mới**.
Kaspersky Endpoint Security sẽ tìm kiếm ứng dụng trong danh sách tổng hợp các ứng dụng được cài đặt trên máy tính được quản lý. Kaspersky Endpoint Security sẽ hiển thị danh sách các ứng dụng đáp ứng các tiêu chí tìm kiếm của bạn.
11. Chọn ứng dụng cần thiết.
12. Trong danh sách thả xuống **Thêm ứng dụng được chọn vào nhóm tin tưởng**, hãy chọn nhóm tin tưởng cần thiết cho ứng dụng.
13. Lưu các thay đổi của bạn.

[Cách thay đổi nhóm tin tưởng của một ứng dụng trong Bảng điều khiển web và Bảng điều khiển đám mây](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Bảo vệ mối đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
5. Trong mục **Các quyền cho ứng dụng và tài nguyên được bảo vệ**, hãy nhấn vào liên kết **Các quyền cho ứng dụng và tài nguyên được bảo vệ**.
Thao tác này sẽ mở ra cửa sổ cấu hình quyền của ứng dụng và danh sách các tài nguyên được bảo vệ.
6. Chọn thẻ **Các quyền của ứng dụng**.
Bạn sẽ thấy danh sách các nhóm tin tưởng ở bên trái cửa sổ và thuộc tính của chúng ở bên phải.
7. Nhấn vào **Thêm**.
Thao tác này sẽ khởi chạy Trình hướng dẫn để thêm ứng dụng vào nhóm tin tưởng.
8. Chọn nhóm tin tưởng liên quan cho ứng dụng.
9. Chọn loại **Ứng dụng**. Nhấn nút **Tiếp theo**.
Nếu bạn muốn thay đổi nhóm tin tưởng cho nhiều ứng dụng, hãy chọn loại **Nhóm** và quy định tên cho nhóm ứng dụng.
10. Trong danh sách ứng dụng được mở, hãy chọn ứng dụng có nhóm tin tưởng mà bạn muốn thay đổi.
Sử dụng bộ lọc. Bạn có thể nhập tên của ứng dụng hoặc tên của nhà cung cấp. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự * cùng ? khi nhập tên đại diện.
11. Kết thúc Trình hướng dẫn bằng cách nhấp vào **OK**.
Ứng dụng sẽ được thêm vào nhóm tin tưởng.
12. Lưu các thay đổi của bạn.

[Cách thay đổi nhóm tin tưởng của một ứng dụng trong giao diện ứng dụng](#)

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
3. Nhấn nút **Quản lý ứng dụng**.
Thao tác này sẽ mở ra danh sách các ứng dụng được cài đặt.
4. Chọn ứng dụng cần thiết.
5. Trong menu ngữ cảnh của ứng dụng, hãy nhấn vào **Hạn chế** → **<nhóm tin tưởng>**.
6. Lưu các thay đổi của bạn.

Kết quả là ứng dụng sẽ được đưa vào nhóm tin tưởng khác. Kaspersky Endpoint Security sau đó sẽ chặn các hành động của ứng dụng, tùy thuộc vào nhóm tin tưởng. Trạng thái  (*do người dùng quy định*) sẽ được gán cho ứng dụng. Nếu danh tiếng của ứng dụng bị thay đổi trong Kaspersky Security Network, thành phần Phòng chống xâm nhập máy chủ sẽ không thay đổi nhóm tin tưởng của ứng dụng này.

Cấu hình quyền của nhóm tin tưởng

[Các quyền ứng dụng tối ưu](#) được tạo cho các nhóm tin tưởng khác nhau theo mặc định. Cấu hình quyền cho nhóm ứng dụng nằm trong một nhóm tin tưởng sẽ kế thừa các giá trị từ thiết lập quyền của các nhóm tin tưởng.


[Cách thay đổi quyền của nhóm tin tưởng trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
 2. Trong thư mục **Managed devices** 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 **Policies**.
 4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
 5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mỗi đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
 6. Trong mục **Các quyền cho ứng dụng và tài nguyên được bảo vệ**, hãy nhấn nút **Thiết lập**.
Thao tác này sẽ mở ra cửa sổ cấu hình quyền của ứng dụng và danh sách các tài nguyên được bảo vệ.
 7. Chọn thẻ **Các quyền của ứng dụng**.
 8. Chọn nhóm tin tưởng cần thiết.
 9. Trong menu ngữ cảnh của nhóm tin tưởng, hãy chọn **Quyền của nhóm**.
Thao tác này sẽ mở các thuộc tính của nhóm tin tưởng.
 10. Thực hiện một trong các thao tác sau:
 - Nếu bạn muốn chỉnh sửa các quyền của nhóm tin tưởng quản lý hoạt động với registry hệ điều hành, tập tin người dùng và thiết lập ứng dụng thì hãy chọn thẻ **Tập tin và registry hệ thống**.
 - Nếu bạn muốn chỉnh sửa các quyền của nhóm tin tưởng quản lý quyền truy cập vào các tiến trình và đối tượng của hệ điều hành thì hãy chọn thẻ **Quyền**.
- Hoạt động mạng của các ứng dụng được kiểm soát bởi [Tường lửa](#) bằng cách sử dụng *quy tắc mạng*.
11. Đối với tài nguyên liên quan, trong cột của hành động tương ứng, hãy nhấn chuột phải để mở menu ngữ cảnh và chọn tùy chọn cần thiết: **Kế thừa**, **Cho phép** (✓) hoặc **Chặn** (⊗).
 12. Nếu bạn muốn giám sát việc sử dụng tài nguyên máy tính, hãy chọn **Ghi lại sự kiện** (✓ / ⊗).
Kaspersky Endpoint Security sẽ ghi lại thông tin về hoạt động của thành phần Phòng chống xâm nhập máy chủ. Các báo cáo chứa thông tin về hoạt động với tài nguyên máy tính được thực hiện bởi ứng dụng (được phép hoặc bị cấm). Các báo cáo cũng chứa thông tin về những ứng dụng sử dụng từng tài nguyên.
 13. Lưu các thay đổi của bạn.




[Cách thay đổi quyền của nhóm tin tưởng trong Bảng điều khiển web và Bảng điều khiển đám mây](#) 


1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
 2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
 3. Chọn thẻ **Application settings**.
 4. Vào **Bảo vệ mối đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
 5. Trong mục **Các quyền cho ứng dụng và tài nguyên được bảo vệ**, hãy nhấn vào liên kết **Các quyền cho ứng dụng và tài nguyên được bảo vệ**.
Thao tác này sẽ mở ra cửa sổ cấu hình quyền của ứng dụng và danh sách các tài nguyên được bảo vệ.
 6. Chọn thẻ **Các quyền của ứng dụng**.
Bạn sẽ thấy danh sách các nhóm tin tưởng ở bên trái cửa sổ và thuộc tính của chúng ở bên phải.
 7. Ở phần bên trái của cửa sổ, hãy chọn nhóm tin tưởng liên quan.
 8. Ở bên phải của cửa sổ, trong danh sách thả xuống, hãy thực hiện một trong các hành động sau:
 - Nếu bạn muốn chỉnh sửa các quyền của nhóm tin tưởng quản lý hoạt động với registry hệ điều hành, tập tin người dùng và thiết lập ứng dụng thì hãy chọn **Tập tin và registry hệ thống**.
 - Nếu bạn muốn chỉnh sửa các quyền của nhóm tin tưởng quản lý quyền truy cập vào các tiến trình và đối tượng của hệ điều hành thì hãy chọn **Quyền**.
- Hoạt động mạng của các ứng dụng được kiểm soát bởi [Tường lửa](#) bằng cách sử dụng *quy tắc mạng*.
9. Đối với tài nguyên liên quan, trong cột của hành động tương ứng, hãy chọn tùy chọn cần thiết: **Kế thừa**, **Cho phép** (✓) hoặc **Cấm** (✗).
 10. Nếu bạn muốn giám sát việc sử dụng tài nguyên máy tính, hãy chọn **Ghi lại sự kiện** (📄 / 🚫).
Kaspersky Endpoint Security sẽ ghi lại thông tin về hoạt động của thành phần Phòng chống xâm nhập máy chủ. Các báo cáo chứa thông tin về hoạt động với tài nguyên máy tính được thực hiện bởi ứng dụng (được phép hoặc bị cấm). Các báo cáo cũng chứa thông tin về những ứng dụng sử dụng từng tài nguyên.
 11. Lưu các thay đổi của bạn.

Cách thay đổi quyền của nhóm tin tưởng trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
3. Nhấn nút **Quản lý ứng dụng**.
Thao tác này sẽ mở ra danh sách các ứng dụng được cài đặt.
4. Chọn nhóm tin tưởng cần thiết.
5. Trong menu ngữ cảnh của nhóm tin tưởng, hãy chọn **Chi tiết và quy tắc**.
Thao tác này sẽ mở các thuộc tính của nhóm tin tưởng.
6. Thực hiện một trong các thao tác sau:
 - Nếu bạn muốn chỉnh sửa các quyền của nhóm tin tưởng quản lý hoạt động với registry hệ điều hành, tập tin người dùng và thiết lập ứng dụng thì hãy chọn thẻ **Tập tin và registry hệ thống**.
 - Nếu bạn muốn chỉnh sửa các quyền của nhóm tin tưởng quản lý quyền truy cập vào các tiến trình và đối tượng của hệ điều hành thì hãy chọn thẻ **Quyền**.

Hoạt động mạng của các ứng dụng được kiểm soát bởi [Tường lửa](#) bằng cách sử dụng *quy tắc mạng*.

7. Đối với tài nguyên liên quan, trong cột của hành động tương ứng, hãy nhấn chuột phải để mở menu ngữ cảnh và chọn tùy chọn cần thiết: **Kế thừa**, **Cho phép**  hoặc **Từ chối** .
8. Nếu bạn muốn giám sát việc sử dụng tài nguyên máy tính, hãy chọn **Ghi lại sự kiện** .
Kaspersky Endpoint Security sẽ ghi lại thông tin về hoạt động của thành phần Phòng chống xâm nhập máy chủ. Các báo cáo chứa thông tin về hoạt động với tài nguyên máy tính được thực hiện bởi ứng dụng (được phép hoặc bị cấm). Các báo cáo cũng chứa thông tin về những ứng dụng sử dụng từng tài nguyên.
9. Lưu các thay đổi của bạn.

Các quyền của nhóm tin tưởng sẽ được thay đổi. Kaspersky Endpoint Security sau đó sẽ chặn các hành động của ứng dụng, tùy thuộc vào nhóm tin tưởng. Trạng thái  (*Thiết lập của người dùng*) sẽ được gán cho nhóm tin tưởng.

Chọn một nhóm tin tưởng cho các ứng dụng được khởi động trước Kaspersky Endpoint Security

Đối với các ứng dụng đã được khởi động trước Kaspersky Endpoint Security, thành phần này chỉ kiểm soát hoạt động mạng của chúng. Tính năng kiểm soát được thực hiện thông qua [các quy tắc mạng](#) được xác định trong thiết lập 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.


Cách chọn một nhóm tin tưởng cho các ứng dụng được khởi chạy trước Kaspersky Endpoint Security trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mỗi đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
6. Trong mục **Các quyền cho ứng dụng và tài nguyên được bảo vệ**, hãy nhấn nút **Chỉnh sửa**.
7. Đối với thiết lập **Nhóm tin tưởng cho các ứng dụng đã được khởi chạy trước khi Kaspersky Endpoint Security cho Windows bắt đầu hoạt động**, hãy chọn [nhóm tin tưởng](#) thích hợp.
8. Lưu các thay đổi của bạn.

Cách chọn một nhóm tin tưởng cho các ứng dụng được khởi chạy trước Kaspersky Endpoint Security trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Bảo vệ mỗi đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
5. Đối với thiết lập **Nhóm tin tưởng cho các ứng dụng đã được khởi chạy trước khi Kaspersky Endpoint Security cho Windows bắt đầu hoạt động**, hãy chọn [nhóm tin tưởng](#) thích hợp.
6. Lưu các thay đổi của bạn.

Cách chọn một nhóm tin tưởng cho các ứng dụng được khởi chạy trước Kaspersky Endpoint Security trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
3. Trong mục **Nhóm tin tưởng cho các ứng dụng đã được khởi chạy trước khi Kaspersky Endpoint Security cho Windows bắt đầu hoạt động**, hãy chọn [nhóm tin tưởng](#) thích hợp.
4. Lưu các thay đổi của bạn.

Kết quả là một ứng dụng được khởi chạy trước Kaspersky Endpoint Security sẽ được đưa vào nhóm tin tưởng khác. Kaspersky Endpoint Security sau đó sẽ chặn các hành động của ứng dụng, tùy thuộc vào nhóm tin tưởng.

Chọn một nhóm tin tưởng cho các ứng dụng không xác định

Trong lần khởi động đầu tiên của ứng dụng, thành phần Phòng chống xâm nhập máy chủ sẽ xác định [nhóm tin tưởng](#) cho ứng dụng. Nếu bạn không có quyền truy cập Internet hoặc nếu Kaspersky Security Network không có thông tin về ứng dụng này thì Kaspersky Endpoint Security sẽ đưa ứng dụng vào nhóm Hạn chế thấp theo mặc định. Khi phát hiện thông tin về một ứng dụng không xác định trước đó trong KSN, Kaspersky Endpoint Security sẽ cập nhật các quyền của ứng dụng này. Khi đó, bạn có thể [chỉnh sửa các quyền của ứng dụng một cách thủ công](#).


[Cách chọn nhóm tin tưởng cho các ứng dụng không xác định trong Bảng điều khiển quản trị \(MMC\)](#)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mỗi đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
6. Trong mục **Quy tắc xử lý ứng dụng**, hãy sử dụng danh sách thả xuống **Nhóm tin tưởng cho các ứng dụng không thể thêm được vào các nhóm có sẵn** để chọn nhóm tin tưởng cần thiết.
Nếu lựa chọn tham gia [Kaspersky Security Network được bật](#), Kaspersky Endpoint Security sẽ gửi đến KSN một yêu cầu danh tiếng của một ứng dụng mỗi khi ứng dụng được khởi động. Dựa trên phản hồi nhận được, ứng dụng có thể sẽ được di chuyển đến một nhóm tin tưởng khác với nhóm được quy định trong thiết lập của thành phần Phòng chống xâm nhập máy chủ.
7. Sử dụng hộp kiểm **Cập nhật quyền cho các ứng dụng trước đây chưa được xác định trong cơ sở dữ liệu KSN** để cấu hình cập nhật tự động quyền của các ứng dụng chưa biết.
8. Lưu các thay đổi của bạn.

Cách chọn nhóm tin tưởng cho các ứng dụng chưa biết trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Bảo vệ mối đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
5. Trong mục **Quy tắc xử lý ứng dụng**, hãy sử dụng danh sách thả xuống **Nhóm tin tưởng cho các ứng dụng không thể thêm được vào các nhóm có sẵn** để chọn nhóm tin tưởng cần thiết.
Nếu lựa chọn tham gia [Kaspersky Security Network được bật](#), Kaspersky Endpoint Security sẽ gửi đến KSN một yêu cầu danh tiếng của một ứng dụng mỗi khi ứng dụng được khởi động. Dựa trên phản hồi nhận được, ứng dụng có thể sẽ được di chuyển đến một nhóm tin tưởng khác với nhóm được quy định trong thiết lập của thành phần Phòng chống xâm nhập máy chủ.
6. Sử dụng hộp kiểm **Cập nhật quyền cho các ứng dụng trước đây chưa được xác định trong cơ sở dữ liệu KSN** để cấu hình cập nhật tự động quyền của các ứng dụng chưa biết.
7. Lưu các thay đổi của bạn.

Cách chọn nhóm tin tưởng cho các ứng dụng chưa biết trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
3. Trong mục **Quy tắc xử lý ứng dụng**, hãy chọn nhóm tin tưởng cần thiết.
Nếu lựa chọn tham gia [Kaspersky Security Network được bật](#), Kaspersky Endpoint Security sẽ gửi đến KSN một yêu cầu danh tiếng của một ứng dụng mỗi khi ứng dụng được khởi động. Dựa trên phản hồi nhận được, ứng dụng có thể sẽ được di chuyển đến một nhóm tin tưởng khác với nhóm được quy định trong thiết lập của thành phần Phòng chống xâm nhập máy chủ.
4. Sử dụng hộp kiểm **Cập nhật quy tắc cho các ứng dụng trước đó chưa biết từ KSN** để cấu hình cập nhật tự động quyền của các ứng dụng chưa biết.
5. Lưu các thay đổi của bạn.

Chọn một nhóm tin tưởng cho các ứng dụng được ký bằng chữ ký số

Kaspersky Endpoint Security luôn đặt các ứng dụng được ký bởi chứng chỉ Microsoft hoặc chứng chỉ Kaspersky vào nhóm Tin tưởng.


Cách chọn nhóm tin tưởng cho các ứng dụng được ký bằng chữ ký số trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mỗi đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
6. Trong mục **Quy tắc xử lý ứng dụng**, hãy sử dụng hộp kiểm **Tin tưởng các ứng dụng được ký số** để bật hoặc tắt gán tự động cho Nhóm tin tưởng đối với các ứng dụng chứa chữ ký số của nhà cung cấp được tin tưởng.
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](#).
Nếu hộp kiểm này bị xóa, thành phần Phòng chống xâm nhập máy chủ sẽ không coi các ứng dụng có chữ ký điện tử là đáng tin tưởng, và sử dụng các tham số khác để xác định [nhóm tin tưởng](#) của chúng.
7. Lưu các thay đổi của bạn.

Cách chọn nhóm tin tưởng cho các ứng dụng được ký bằng chữ ký số trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Bảo vệ mỗi đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
5. Trong mục **Quy tắc xử lý ứng dụng**, hãy sử dụng hộp kiểm **Tin tưởng các ứng dụng được ký số** để bật hoặc tắt gán tự động cho Nhóm tin tưởng đối với các ứng dụng chứa chữ ký số của nhà cung cấp được tin tưởng.
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](#).
Nếu hộp kiểm này bị xóa, thành phần Phòng chống xâm nhập máy chủ sẽ không coi các ứng dụng có chữ ký điện tử là đáng tin tưởng, và sử dụng các tham số khác để xác định [nhóm tin tưởng](#) của chúng.
6. Lưu các thay đổi của bạn.

Cách chọn nhóm tin tưởng cho các ứng dụng được ký bằng chữ ký số trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
3. Trong mục **Quy tắc xử lý ứng dụng**, hãy sử dụng hộp kiểm **Tin tưởng các ứng dụng được ký số** để bật hoặc tắt gán tự động cho Nhóm tin tưởng đối với các ứng dụng chứa chữ ký số của nhà cung cấp được tin tưởng.

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](#).

Nếu hộp kiểm này bị xóa, thành phần Phòng chống xâm nhập máy chủ sẽ không coi các ứng dụng có chữ ký điện tử là đáng tin tưởng, và sử dụng các tham số khác để xác định [nhóm tin tưởng](#) của chúng.

4. Lưu các thay đổi của bạn.

Quản lý các quyền của ứng dụng

Theo mặc định, hoạt động của ứng dụng được kiểm soát dựa trên các quyền ứng dụng được xác định cho [nhóm tin tưởng](#) cụ thể mà Kaspersky Endpoint Security đã gán cho ứng dụng khi nó khởi động lần đầu tiên. Nếu cần, bạn có thể [chỉnh sửa các quyền của 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 quyền của ứng dụng được quy định theo cách thủ công có mức độ ưu tiên cao hơn các quyền của ứng dụng đã được quy định cho một nhóm tin tưởng. Nói cách khác, nếu các quyền ứng dụng được quy định theo cách thủ công khác với các quyền ứng dụng được quy định cho một nhóm tin tưởng, thì thành phần Phòng chống xâm nhập máy chủ sẽ kiểm soát hoạt động của ứng dụng theo các quyền ứng dụng được quy định theo cách thủ công.

Những quy tắc mà bạn tạo cho các ứng dụng được các ứng dụng con kế thừa. Ví dụ: nếu bạn từ chối tất cả hoạt động mạng đối với cmd.exe thì tất cả hoạt động mạng cũng sẽ bị từ chối đối với notepad.exe nếu nó được khởi chạy bằng cmd.exe. Khi một ứng dụng không phải là ứng dụng con của ứng dụng khởi chạy nó, các quy tắc sẽ không được kế thừa.

Cách thay đổi quyền ứng dụng trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mỗi đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
6. Trong mục **Các quyền cho ứng dụng và tài nguyên được bảo vệ**, hãy nhấn nút **Thiết lập**.
Thao tác này sẽ mở ra cửa sổ cấu hình quyền của ứng dụng và danh sách các tài nguyên được bảo vệ.
7. Chọn thẻ **Các quyền của ứng dụng**.
8. Nhấn vào **Thêm**.
9. Trong cửa sổ mở ra, hãy nhập tiêu chí cho ứng dụng có các quyền của ứng dụng mà bạn muốn thay đổi.
Bạn có thể nhập tên của ứng dụng hoặc tên của nhà cung cấp. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự * cùng ? khi nhập tên đại diện.
10. Nhấn vào nút **Làm mới**.
Kaspersky Endpoint Security sẽ tìm kiếm ứng dụng trong danh sách tổng hợp các ứng dụng được cài đặt trên máy tính được quản lý. Kaspersky Endpoint Security sẽ hiển thị danh sách các ứng dụng đáp ứng các tiêu chí tìm kiếm của bạn.
11. Chọn ứng dụng cần thiết.
12. Trong danh sách thả xuống **Thêm ứng dụng được chọn vào nhóm tin tưởng**, hãy chọn **Nhóm mặc định** và nhấn **OK**.
Ứng dụng sẽ được thêm vào nhóm mặc định.
13. Chọn ứng dụng liên quan rồi chọn **Các quyền của ứng dụng** từ menu ngữ cảnh của ứng dụng.
Thao tác này sẽ mở ra thuộc tính ứng dụng.
14. Thực hiện một trong các thao tác sau:
 - Nếu bạn muốn chỉnh sửa các quyền của nhóm tin tưởng quản lý hoạt động với registry hệ điều hành, tập tin người dùng và thiết lập ứng dụng thì hãy chọn thẻ **Tập tin và registry hệ thống**.
 - Nếu bạn muốn chỉnh sửa các quyền của nhóm tin tưởng quản lý quyền truy cập vào các tiến trình và đối tượng của hệ điều hành thì hãy chọn thẻ **Quyền**.

Hoạt động mạng của các ứng dụng được kiểm soát bởi [Tường lửa](#) bằng cách sử dụng *quy tắc mạng*.

15. Đối với tài nguyên liên quan, trong cột của hành động tương ứng, hãy nhấn chuột phải để mở menu ngữ cảnh và chọn tùy chọn cần thiết: **Kế thừa**, **Cho phép** (✓) hoặc **Chặn** (⊗).

16. Nếu bạn muốn giám sát việc sử dụng tài nguyên máy tính, hãy chọn **Ghi lại sự kiện** (✓ / ⊗).

Kaspersky Endpoint Security sẽ ghi lại thông tin về hoạt động của thành phần Phòng chống xâm nhập máy chủ. Các báo cáo chứa thông tin về hoạt động với tài nguyên máy tính được thực hiện bởi ứng dụng (được phép hoặc bị cấm). Các báo cáo cũng chứa thông tin về những ứng dụng sử dụng từng tài nguyên.

17. Lưu các thay đổi của bạn.

[Cách thay đổi quyền ứng dụng trong Bảng điều khiển web và Bảng điều khiển đám mây](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Bảo vệ môi đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
5. Trong mục **Các quyền cho ứng dụng và tài nguyên được bảo vệ**, hãy nhấn vào liên kết **Các quyền cho ứng dụng và tài nguyên được bảo vệ**.
Thao tác này sẽ mở ra cửa sổ cấu hình quyền của ứng dụng và danh sách các tài nguyên được bảo vệ.
6. Chọn thẻ **Các quyền của ứng dụng**.
Bạn sẽ thấy danh sách các nhóm tin tưởng ở bên trái cửa sổ và thuộc tính của chúng ở bên phải.
7. Nhấn vào **Thêm**.
Thao tác này sẽ khởi chạy Trình hướng dẫn để thêm ứng dụng vào nhóm tin tưởng.
8. Chọn nhóm tin tưởng liên quan cho ứng dụng.
9. Chọn loại **Ứng dụng**. Nhấn nút **Tiếp theo**.
Nếu bạn muốn thay đổi nhóm tin tưởng cho nhiều ứng dụng, hãy chọn loại **Nhóm** và quy định tên cho nhóm ứng dụng.
10. Trong danh sách ứng dụng được mở, hãy chọn ứng dụng có các quyền ứng dụng mà bạn muốn thay đổi.
Sử dụng bộ lọc. Bạn có thể nhập tên của ứng dụng hoặc tên của nhà cung cấp. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự * cùng ? khi nhập tên đại diện.
11. Kết thúc Trình hướng dẫn bằng cách nhấp vào **OK**.
Ứng dụng sẽ được thêm vào nhóm tin tưởng.
12. Ở phần bên phải của cửa sổ, hãy chọn ứng dụng liên quan.
13. Ở bên phải của cửa sổ, trong danh sách thả xuống, hãy thực hiện một trong các hành động sau:
 - Nếu bạn muốn chỉnh sửa các quyền của nhóm tin tưởng quản lý hoạt động với registry hệ điều hành, tập tin người dùng và thiết lập ứng dụng thì hãy chọn **Tập tin và registry hệ thống**.
 - Nếu bạn muốn chỉnh sửa các quyền của nhóm tin tưởng quản lý quyền truy cập vào các tiến trình và đối tượng của hệ điều hành thì hãy chọn **Quyền**.

Hoạt động mạng của các ứng dụng được kiểm soát bởi [Tường lửa](#) bằng cách sử dụng *quy tắc mạng*.





14. Đối với tài nguyên liên quan, trong cột của hành động tương ứng, hãy chọn tùy chọn cần thiết: **Kế thừa**, **Cho phép** (✓) hoặc **Cấm** (✗).

15. Nếu bạn muốn giám sát việc sử dụng tài nguyên máy tính, hãy chọn **Ghi lại sự kiện** (📄 / 🗑️).

Kaspersky Endpoint Security sẽ ghi lại thông tin về hoạt động của thành phần Phòng chống xâm nhập máy chủ. Các báo cáo chứa thông tin về hoạt động với tài nguyên máy tính được thực hiện bởi ứng dụng (được phép hoặc bị cấm). Các báo cáo cũng chứa thông tin về những ứng dụng sử dụng từng tài nguyên.

16. Lưu các thay đổi của bạn.

[Cách thay đổi quyền ứng dụng trong giao diện ứng dụng](#) 

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
3. Nhấn nút **Quản lý ứng dụng**.
Thao tác này sẽ mở ra danh sách các ứng dụng được cài đặt.
4. Chọn ứng dụng cần thiết.
5. Trong menu ngữ cảnh của ứng dụng, hãy chọn **Chi tiết và quy tắc**.
Thao tác này sẽ mở ra thuộc tính ứng dụng.
6. Thực hiện một trong các thao tác sau:
 - Nếu bạn muốn chỉnh sửa các quyền của nhóm tin tưởng quản lý hoạt động với registry hệ điều hành, tập tin người dùng và thiết lập ứng dụng thì hãy chọn thẻ **Tập tin và registry hệ thống**.
 - Nếu bạn muốn chỉnh sửa các quyền của nhóm tin tưởng quản lý quyền truy cập vào các tiến trình và đối tượng của hệ điều hành thì hãy chọn thẻ **Quyền**.
7. Đối với tài nguyên liên quan, trong cột của hành động tương ứng, hãy nhấn chuột phải để mở menu ngữ cảnh và chọn tùy chọn cần thiết: **Kế thừa**, **Cho phép**  hoặc **Từ chối** .
8. Nếu bạn muốn giám sát việc sử dụng tài nguyên máy tính, hãy chọn **Ghi lại sự kiện** .
Kaspersky Endpoint Security sẽ ghi lại thông tin về hoạt động của thành phần Phòng chống xâm nhập máy chủ. Các báo cáo chứa thông tin về hoạt động với tài nguyên máy tính được thực hiện bởi ứng dụng (được phép hoặc bị cấm). Các báo cáo cũng chứa thông tin về những ứng dụng sử dụng từng tài nguyên.
9. Chọn thẻ **Loại trừ** và cấu hình thiết lập nâng cao của ứng dụng (xem bảng bên dưới).
10. Lưu các thay đổi của bạn.

Thiết lập nâng cao của ứng dụng

Tham số	Mô tả
Không quét các tập tin được mở	Kaspersky Endpoint Security sẽ không quét các tập tin được mở bởi ứng dụng đó. Ví dụ: nếu bạn đang sử dụng các ứng dụng để sao lưu tập tin, tính năng này giúp giảm mức sử dụng tài nguyên bởi Kaspersky Endpoint Security.
Không giám sát hoạt động ứng dụng	Kaspersky Endpoint Security sẽ không giám sát hoạt động mạng và tập tin của ứng dụng trong hệ điều hành. Hoạt động ứng dụng được giám sát bởi các thành phần sau: Phát hiện hành vi , Phòng chống khai thác , Phòng chống xâm nhập máy chủ , Công cụ khắc phục và Tường lửa .
Không kế thừa các hạn chế từ tiến trình cha (ứng dụng)	Các hạn chế được cấu hình cho tiến trình cha sẽ không được Kaspersky Endpoint Security áp dụng cho tiến trình con. Tiến trình cha được khởi chạy bởi một ứng dụng mà các quyền ứng dụng (Phòng chống xâm nhập máy chủ) và quy tắc mạng ứng dụng (Tường lửa) được cấu hình.
Không giám sát hoạt động	Kaspersky Endpoint Security sẽ không giám sát hoạt động mạng và hoạt động tập tin của các ứng dụng được khởi chạy bởi ứng dụng này.

của ứng dụng con	
Cho phép tương tác với giao diện ứng dụng	Thành phần Tự bảo vệ của Kaspersky Endpoint Security sẽ chặn mọi nỗ lực quản lý các dịch vụ ứng dụng trên máy tính từ xa. Nếu hộp kiểm này được chọn, ứng dụng truy cập từ xa sẽ được phép quản lý cấu hình của Kaspersky Endpoint Security thông qua giao diện Kaspersky Endpoint Security.
Không quét lưu lượng được mã hóa/Không quét tất cả lưu lượng	Lưu lượng mạng bắt nguồn từ ứng dụng này sẽ được Kaspersky Endpoint Security loại trừ khỏi tác vụ quét. Bạn có thể loại trừ tất cả lưu lượng hoặc chỉ lưu lượng được mã hóa khỏi tác vụ quét. Bạn cũng có thể loại trừ các địa chỉ IP và mã hiệu cổng riêng lẻ khỏi tác vụ quét.

Bảo vệ tài nguyên hệ điều hành và dữ liệu cá nhân

Thành phần Phòng chống xâm nhập máy chủ quản lý các quyền của ứng dụng trong việc thực hiện hành động đối với nhiều danh mục tài nguyên hệ điều hành và dữ liệu cá nhân. Các chuyên gia Kaspersky đã thiết lập sẵn các hạng mục tài nguyên được bảo vệ. Ví dụ: danh mục *Hệ điều hành* có danh mục con *Thiết lập khởi động* liệt kê tất cả các khóa registry liên quan đến hoạt động tự động chạy ứng dụng. 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.

Để bảo vệ tài nguyên HĐH có trong mục registry
\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet thì bạn cần thêm các khóa registry có trong
\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet???. Ví dụ:
\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet???\services**. Điều này là do các đặc điểm cụ thể của chức năng registry của Windows.



[Cách thêm tài nguyên được bảo vệ trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
6. Trong mục **Các quyền cho ứng dụng và tài nguyên được bảo vệ**, hãy nhấn nút **Thiết lập**.
Thao tác này sẽ mở ra cửa sổ cấu hình quyền của ứng dụng và danh sách các tài nguyên được bảo vệ.
7. Chọn thẻ **Bảo vệ tài nguyên**.
Bạn sẽ thấy danh sách các tài nguyên được bảo vệ ở phần bên trái của cửa sổ và các quyền tương ứng để truy cập các tài nguyên đó, tùy theo nhóm tin tưởng cụ thể.
8. Chọn danh mục tài nguyên được bảo vệ mà bạn muốn thêm tài nguyên được bảo vệ mới.
Nếu bạn muốn thêm một danh mục con, hãy nhấn **Thêm** → **Danh mục**.
9. Nhấn vào nút **Thêm**. Trong danh sách thả xuống, hãy chọn loại tài nguyên bạn muốn thêm: **Tập tin hoặc thư mục** hoặc **Khóa Registry**.
10. Trong cửa sổ mở ra, hãy chọn một tập tin, thư mục hoặc khóa registry.
Bạn có thể xem các quyền của ứng dụng để truy cập tài nguyên được thêm vào. Để làm như vậy, hãy chọn một tài nguyên được thêm ở phần bên trái của cửa sổ và Kaspersky Endpoint Security sẽ hiển thị các quyền truy cập cho từng nhóm tin tưởng. Bạn cũng có thể tắt kiểm soát hoạt động ứng dụng với tài nguyên bằng cách sử dụng hộp kiểm bên cạnh tài nguyên mới.
11. Lưu các thay đổi của bạn.

[Cách thêm tài nguyên được bảo vệ trong Bảng điều khiển web và Bảng điều khiển đám mây](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Bảo vệ mối đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
5. Trong mục **Các quyền cho ứng dụng và tài nguyên được bảo vệ**, hãy nhấn vào liên kết **Các quyền cho ứng dụng và tài nguyên được bảo vệ**.
Thao tác này sẽ mở ra cửa sổ cấu hình quyền của ứng dụng và danh sách các tài nguyên được bảo vệ.
6. Chọn thẻ **Bảo vệ tài nguyên**.
Bạn sẽ thấy danh sách các tài nguyên được bảo vệ ở phần bên trái của cửa sổ và các quyền tương ứng để truy cập các tài nguyên đó, tùy theo nhóm tin tưởng cụ thể.
7. Nhấn vào nút **Thêm**.
Trình hướng dẫn Tài nguyên mới sẽ khởi chạy.
8. Nhấn vào liên kết **Group name** để chọn danh mục tài nguyên được bảo vệ mà bạn muốn thêm tài nguyên được bảo vệ mới.
Nếu bạn muốn thêm một danh mục con, hãy chọn tùy chọn **Danh mục tài nguyên được bảo vệ**.
9. Chọn loại tài nguyên mà bạn muốn thêm: **Tập tin hoặc thư mục** hoặc **Khóa Registry**.
10. Chọn một tập tin, thư mục hoặc khóa registry.
11. Kết thúc Trình hướng dẫn bằng cách nhấp vào **OK**.
Bạn có thể xem các quyền của ứng dụng để truy cập tài nguyên được thêm vào. Để làm như vậy, hãy chọn một tài nguyên được thêm ở phần bên trái của cửa sổ và Kaspersky Endpoint Security sẽ hiển thị các quyền truy cập cho từng nhóm tin tưởng. Bạn cũng có thể sử dụng hộp kiểm trong cột **Trạng thái** để tắt kiểm soát hoạt động ứng dụng với tài nguyên.
12. Lưu các thay đổi của bạn.

[Cách thêm tài nguyên được bảo vệ trong giao diện ứng dụng](#)

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
3. Nhấn nút **Quản lý tài nguyên**.
Danh sách các tài nguyên được bảo vệ sẽ mở ra.
4. Chọn danh mục tài nguyên được bảo vệ mà bạn muốn thêm tài nguyên được bảo vệ mới.
Nếu bạn muốn thêm một danh mục con, hãy nhấn **Thêm** → **Danh mục**.
5. Nhấn vào nút **Thêm**. Trong danh sách thả xuống, hãy chọn loại tài nguyên bạn muốn thêm: **Tập tin hoặc thư mục** hoặc **Khóa Registry**.
6. Trong cửa sổ mở ra, hãy chọn một tập tin, thư mục hoặc khóa registry.
Bạn có thể xem các quyền của ứng dụng để truy cập tài nguyên được thêm vào. Để làm như vậy, hãy chọn một tài nguyên được thêm ở phần bên trái của cửa sổ và Kaspersky Endpoint Security sẽ hiển thị danh sách các ứng dụng và quyền truy cập cho từng ứng dụng. Bạn cũng có thể tắt kiểm soát hoạt động của ứng dụng với các tài nguyên bằng cách sử dụng nút  **Tắt kiểm soát** trong cột **Trạng thái**.
7. Lưu các thay đổi của bạn.

Kaspersky Endpoint Security sẽ kiểm soát quyền truy cập vào tài nguyên hệ điều hành được thêm và dữ liệu cá nhân. Kaspersky Endpoint Security kiểm soát quyền truy cập của ứng dụng vào tài nguyên dựa trên nhóm tin tưởng được gán cho ứng dụng. Bạn cũng có thể [thay đổi nhóm tin tưởng của một ứng dụng](#).

Xóa thông tin về các ứng dụng không sử dụng

Kaspersky Endpoint Security sử dụng các quyền của ứng dụng để kiểm soát các hoạt động của ứng dụng. Các quyền của ứng dụng được xác định bởi nhóm tin tưởng của chúng. Kaspersky Endpoint Security sẽ đưa ứng dụng vào [nhóm tin tưởng](#) khi ứng dụng được khởi chạy lần đầu tiên. Bạn có thể [thay đổi nhóm tin tưởng của một ứng dụng một cách thủ công](#). Bạn cũng có thể [cấu hình các quyền của một ứng dụng riêng lẻ một cách thủ công](#). Kaspersky Endpoint Security sẽ lưu trữ các thông tin sau về một ứng dụng: nhóm tin tưởng của ứng dụng và các quyền của ứng dụng.

Kaspersky Endpoint Security sẽ tự động xóa thông tin về các ứng dụng không sử dụng để tiết kiệm tài nguyên máy tính. Kaspersky Endpoint Security sẽ xóa thông tin ứng dụng theo các quy tắc sau:

- Nếu nhóm tin tưởng và quyền của ứng dụng được xác định tự động, Kaspersky Endpoint Security sẽ xóa thông tin về ứng dụng này sau 30 ngày. Không thể thay đổi thời hạn lưu trữ cho thông tin ứng dụng hoặc tắt tính năng tự động xóa.
- Nếu bạn đã cho ứng dụng vào nhóm tin tưởng hoặc cấu hình quyền truy cập của ứng dụng đó một cách thủ công, Kaspersky Endpoint Security sẽ xóa thông tin về ứng dụng này sau 60 ngày (thời hạn lưu trữ mặc định). Bạn có thể thay đổi thời hạn lưu trữ thông tin ứng dụng hoặc tắt tự động xóa (xem hướng dẫn bên dưới).

Khi bạn khởi chạy một ứng dụng có thông tin đã bị xóa, Kaspersky Endpoint Security sẽ phân tích ứng dụng đó như thể ứng dụng đó đang khởi chạy lần đầu tiên.

Cách cấu hình xóa tự động thông tin về các ứng dụng không sử dụng trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mỗi đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
6. Trong mục **Quy tắc xử lý ứng dụng**, hãy thực hiện một trong những hành động sau:

- Nếu bạn muốn cấu hình tự động xóa, hãy chọn hộp kiểm **Xóa quy tắc cho các ứng dụng không được khởi động nhiều hơn N ngày** và nhập số ngày.

Thông tin về các ứng dụng mà bạn cho vào nhóm tin tưởng một cách thủ công hoặc có quyền truy cập mà bạn đã cấu hình một cách thủ công sẽ bị xóa bởi Kaspersky Endpoint Security sau số ngày được xác định. Thông tin về các ứng dụng có nhóm tin tưởng và quyền của ứng dụng được xác định tự động cũng sẽ bị Kaspersky Endpoint Security xóa sau 30 ngày.

- Nếu bạn muốn tắt tự động xóa, hãy xóa hộp kiểm **Xóa quy tắc cho các ứng dụng không được khởi động nhiều hơn N ngày**.

Thông tin về các ứng dụng được bạn cho vào nhóm tin tưởng một cách thủ công hoặc có quyền truy cập mà bạn đã cấu hình một cách thủ công sẽ được Kaspersky Endpoint Security lưu trữ vô thời hạn, không có bất kỳ giới hạn thời hạn lưu trữ nào. Kaspersky Endpoint Security sẽ chỉ xóa thông tin về các ứng dụng có nhóm tin tưởng và quyền ứng dụng được xác định tự động sau 30 ngày.

7. Lưu các thay đổi của bạn.

Cách cấu hình xóa tự động thông tin về các ứng dụng không sử dụng trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.

2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.

Cửa sổ thuộc tính chính sách sẽ được mở ra.

3. Chọn thẻ **Application settings**.

4. Vào **Bảo vệ môi đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.

5. Trong mục **Quy tắc xử lý ứng dụng**, hãy thực hiện một trong những hành động sau:

- Nếu bạn muốn cấu hình tự động xóa, hãy chọn hộp kiểm **Xóa quy tắc cho các ứng dụng không được khởi động nhiều hơn N ngày** và nhập số ngày.


Thông tin về các ứng dụng mà bạn cho vào nhóm tin tưởng một cách thủ công hoặc có quyền truy cập mà bạn đã cấu hình một cách thủ công sẽ bị xóa bởi Kaspersky Endpoint Security sau số ngày được xác định. Thông tin về các ứng dụng có nhóm tin tưởng và quyền của ứng dụng được xác định tự động cũng sẽ bị Kaspersky Endpoint Security xóa sau 30 ngày.

- Nếu bạn muốn tắt tự động xóa, hãy xóa hộp kiểm **Xóa quy tắc cho các ứng dụng không được khởi động nhiều hơn N ngày**.

Thông tin về các ứng dụng được bạn cho vào nhóm tin tưởng một cách thủ công hoặc có quyền truy cập mà bạn đã cấu hình một cách thủ công sẽ được Kaspersky Endpoint Security lưu trữ vô thời hạn, không có bất kỳ giới hạn thời hạn lưu trữ nào. Kaspersky Endpoint Security sẽ chỉ xóa thông tin về các ứng dụng có nhóm tin tưởng và quyền ứng dụng được xác định tự động sau 30 ngày.

6. Lưu các thay đổi của bạn.

[Cách cấu hình xóa tự động thông tin về các ứng dụng không sử dụng trong giao diện ứng dụng](#) 

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa nâng cao** → **Phòng chống xâm nhập máy chủ**.
3. Trong mục **Quy tắc xử lý ứng dụng**, hãy thực hiện một trong những hành động sau:
 - Nếu bạn muốn cấu hình tự động xóa, hãy chọn hộp kiểm **Xóa quy tắc cho các ứng dụng không được khởi động nhiều hơn N ngày** và nhập số ngày.
Thông tin về các ứng dụng mà bạn cho vào nhóm tin tưởng một cách thủ công hoặc có quyền truy cập mà bạn đã cấu hình một cách thủ công sẽ bị xóa bởi Kaspersky Endpoint Security sau số ngày được xác định. Thông tin về các ứng dụng có nhóm tin tưởng và quyền của ứng dụng được xác định tự động cũng sẽ bị Kaspersky Endpoint Security xóa sau 30 ngày.
 - Nếu bạn muốn tắt tự động xóa, hãy xóa hộp kiểm **Xóa quy tắc cho các ứng dụng không được khởi động nhiều hơn N ngày**.
Thông tin về các ứng dụng được bạn cho vào nhóm tin tưởng một cách thủ công hoặc có quyền truy cập mà bạn đã cấu hình một cách thủ công sẽ được Kaspersky Endpoint Security lưu trữ vô thời hạn, không có bất kỳ giới hạn thời hạn lưu trữ nào. Kaspersky Endpoint Security sẽ chỉ xóa thông tin về các ứng dụng có nhóm tin tưởng và quyền ứng dụng được xác định tự động sau 30 ngày.
4. Lưu các thay đổi của bạn.

Giám sát Phòng chống xâm nhập máy chủ

Bạn có thể nhận báo cáo về hoạt động của thành phần Phòng chống xâm nhập máy chủ. Các báo cáo chứa thông tin về hoạt động với tài nguyên máy tính được thực hiện bởi ứng dụng (được phép hoặc bị cấm). Các báo cáo cũng chứa thông tin về những ứng dụng sử dụng từng tài nguyên.

Để giám sát các hoạt động Phòng chống xâm nhập máy chủ, bạn cần bật tính năng viết báo cáo. Ví dụ: bạn có thể [bật chuyển tiếp báo cáo cho các ứng dụng riêng lẻ trong thiết lập của thành phần phòng chống xâm nhập máy chủ](#).

Khi cấu hình giám sát Phòng chống xâm nhập máy chủ, hãy tính đến mức tải mạng tiềm tàng khi chuyển tiếp các sự kiện đến Kaspersky Security Center. Bạn cũng có thể bật tính năng chỉ lưu báo cáo trong nhật ký cục bộ của Kaspersky Endpoint Security.

Bảo vệ quyền truy cập âm thanh và video

Tội phạm mạng có thể sử dụng các chương trình đặc biệt để cố gắng truy cập vào các thiết bị ghi âm và quay video (như micrô hoặc webcam). Kaspersky Endpoint Security sẽ kiểm soát khi các ứng dụng nhận được luồng âm thanh hoặc luồng video và bảo vệ dữ liệu khỏi bị chặn trái phép.

Theo mặc định, Kaspersky Endpoint Security sẽ kiểm soát quyền truy cập của các ứng dụng vào luồng âm thanh và luồng video như sau:

- Theo mặc định, các ứng dụng được tin tưởng và bị hạn chế thấp được phép nhận luồng âm thanh và luồng video từ các thiết bị.
- Theo mặc định, các ứng dụng bị hạn chế cao và không được tin tưởng không được phép nhận luồng âm thanh và luồng video từ các thiết bị.

Bạn có thể [cho phép các ứng dụng nhận luồng âm thanh và video theo cách thủ công](#).

Các tính năng đặc biệt của bảo vệ luồng âm thanh

Bảo vệ luồng âm thanh có những đặc điểm đặc biệt sau:

- Thành phần [Phòng chống xâm nhập máy chủ phải được bật](#) để chức năng này có thể hoạt động.
- Nếu ứng dụng bắt đầu nhận dòng âm thanh trước khi thành phần Phòng chống xâm nhập máy chủ 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 Giới hạn mức Cao sau khi ứng dụng bắt đầu nhận luồng âm thanh, Kaspersky Endpoint Security sẽ cho phép ứng dụng nhận luồng âm thanh đó và không hiển thị bất kỳ thông báo nào.
- Sau khi thiết lập quyền truy cập của ứng dụng đến các thiết bị ghi âm đã được thay đổi (ví dụ: nếu [ứng dụng đã bị chặn nhận luồng âm thanh](#)) thì bạn phải khởi chạy lại ứng dụng này nếu muốn ứng dụng ngừng nhận luồng 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.
- Khi bạn chạy ứng dụng ghi lại hoặc phát lại âm thanh hay video lần đầu tiên kể từ khi cài đặt Kaspersky Endpoint Security, chức năng ghi lại hoặc phát lại âm thanh và 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.

Các tính năng đặc biệt của chức năng bảo vệ truy cập webcam của 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.
- 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.

Công cụ khắc phục

Công cụ khắc phục cho phép Kaspersky Endpoint Security có thể hoàn tác các hành động đã được thực hiện bởi phần mềm độc hại trong hệ điều hành.

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 độc hại sau đây:

- **Hoạt động trên tập tin**

Kaspersky Endpoint Security thực hiện các hành động sau:

- Xóa các tập tin thực thi đã được tạo bởi phần mềm độc hại (trên tất cả các ổ đĩa ngoại trừ ổ đĩa mạng).
- Xóa các tập tin thực thi được tạo bởi các chương trình bị xâm nhập bởi phần mềm độc hại.
- Khôi phục các tập tin đã bị sửa đổi hoặc xóa bởi phần mềm độc hại.

Tính năng phục hồi tập tin có [một số giới hạn](#).

- **Hoạt động registry**

Kaspersky Endpoint Security thực hiện các hành động sau:

- Xóa các khóa registry được tạo bởi phần mềm độc hại.
- Không khôi phục các khóa registry đã bị sửa đổi hoặc xóa bởi phần mềm độc hại.

- **Hoạt động hệ thống**

Kaspersky Endpoint Security thực hiện các hành động sau:

- Chấm dứt các tiến trình đã được khởi động bởi một phần mềm độc hại.
- Chấm dứt các tiến trình bị xâm nhập bởi một ứng dụng độc hại.
- Không khôi phục các tiến trình đã bị dừng bởi một phần mềm độc hại.
- **Hoạt động mạng**

Kaspersky Endpoint Security thực hiện các hành động sau:

- Chặn hoạt động mạng của phần mềm độc hại.
- Chặn hoạt động mạng của các tiến trình đã bị phần mềm độc hại xâm nhập.

Việc hoàn tác các hành động của phần mềm độc hại có thể được bắt đầu bởi thành phần [Bảo vệ môi đe dọa tập tin](#) hoặc [Phát hiện hành vi](#), hay 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.


[Cách bật hoặc tắt thành phần Công cụ khắc phục trong Bảng điều khiển quản trị \(MMC\)](#)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Bảo vệ môi đe dọa nâng cao** → **Công cụ khắc phục**.
6. Sử dụng hộp kiểm **Công cụ khắc phục** để bật hoặc tắt thành phần.
7. Lưu các thay đổi của bạn.

[Cách bật hoặc tắt thành phần Công cụ khắc phục trong Bảngg điều khiển web và Bảng điều khiển đám mây](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào mục **Bảo vệ môi đe dọa nâng cao** → **Công cụ khắc phục**.
5. Sử dụng **Công cụ khắc phục** để bật hoặc tắt thành phần.
6. Lưu các thay đổi của bạn.

Cách bật hoặc tắt thành phần Công cụ khắc phục trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa nâng cao** → **Công cụ khắc phục**.
3. Sử dụng **Công cụ khắc phục** để bật hoặc tắt thành phần.
4. Lưu các thay đổi của bạn.

Kết quả là nếu Công cụ khắc phục được bật, Kaspersky Endpoint Security sẽ khôi phục các hành động được thực hiện bởi các ứng dụng độc hại trong hệ điều hành.

Kaspersky Security Network

Để bảo vệ máy tính của bạn một cách hiệu quả hơn, Kaspersky Endpoint Security sẽ sử dụng dữ liệu được nhận từ người dùng trên khắp thế giới. Kaspersky Security Network được thiết kế để lấy 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. Nếu bạn đang tham gia vào Kaspersky Security Network, các dịch vụ KSN sẽ cung cấp cho Kaspersky Endpoint Security thông tin về danh mục và danh tiếng của các tập tin được quét, cũng như thông tin về danh tiếng của các địa chỉ trang web được quét.

Việc sử dụng Kaspersky Security Network là hoàn toàn tự nguyện. Ứng dụng sẽ nhắc bạn sử dụng KSN trong quá trình cấu hình ban đầu ứng dụng. Người dùng có thể bắt đầu hoặc ngừng tham gia KSN tại bất cứ thời điểm nào.

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 có văn bản của Tuyên bố Kaspersky Security Network cũng được bao gồm trong [gói phân phối](#) ứng dụng.

Để giảm tải cho các máy chủ KSN, các chuyên gia của Kaspersky có thể phát hành các bản cập nhật ứng dụng để tắt tạm thời hoặc hạn chế một phần các yêu cầu được gửi đến Kaspersky Security Network. Trong trường hợp này, trạng thái của kết nối đến KSN trong giao diện cục bộ của ứng dụng sẽ là *Cho phép với hạn chế*.

Hạ tầng KSN

Kaspersky Endpoint Security hỗ trợ các giải pháp hạ tầng KSN sau đây:

- *KSN Toàn cầu* là giải pháp được hầu hết các ứng dụng Kaspersky sử dụng. Người tham gia vào KSN sẽ nhận thông tin từ Kaspersky Security Network và gửi cho Kaspersky thông tin về các đối tượng được xóa trên máy tính của người dùng. Đây là những đối tượng sẽ được các chuyên gia phân tích của Kaspersky phân tích thêm và sẽ được đưa vào cơ sở dữ liệu danh tiếng và thống kê của Kaspersky Security Network.


- *KSN Riêng* là một giải pháp cho phép người dùng máy tính lưu trữ Kaspersky Endpoint Security hoặc các ứng dụng khác của Kaspersky để có quyền truy cập cơ sở dữ liệu danh tiếng của Kaspersky Security Network và truy cập các dữ liệu thống kê khác mà không cần gửi dữ liệu cho KSN từ máy tính của riêng họ. KSN Riêng được thiết kế dành cho khách hàng doanh nghiệp không thể tham gia vào Kaspersky Security Network vì bất kỳ lý do nào dưới đây:
 - Các máy trạm cục bộ không được kết nối vào mạng Internet.
 - Việc truyền tải bất kỳ dữ liệu nào bên ngoài quốc gia hoặc bên ngoài mạng LAN của doanh nghiệp đều bị cấm theo luật pháp hoặc bị hạn chế bởi các chính sách bảo mật của doanh nghiệp.

Theo mặc định, Kaspersky Security Center sẽ sử dụng KSN Toàn cầu. Bạn có thể cấu hình việc sử dụng KSN Riêng trong Bảng điều khiển quản trị (MMC), trong Bảng điều khiển web Kaspersky Security Center và trong [dòng lệnh](#). Không thể cấu hình việc sử dụng KSN Riêng trong Bảng điều khiển đám mây Kaspersky Security Center.

Để biết thêm chi tiết về KSN Riêng, vui lòng tham khảo tài liệu về Kaspersky Private Security Network.

Bật và tắt sử dụng Kaspersky Security Network

Để bật hoặc tắt sử dụng Kaspersky Security Network:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa nâng cao** → **Kaspersky Security Network**.
3. Sử dụng nút bật/tắt **Kaspersky Security Network** để bật hoặc tắt thành phần.

Nếu bạn đã cho phép sử dụng KSN, Kaspersky Endpoint Security sẽ hiển thị Tuyên bố Kaspersky Security Network. Vui lòng đọc và chấp nhận các điều khoản sử dụng của Tuyên bố Kaspersky Security Network (KSN) nếu bạn đồng ý với chúng.

Theo mặc định, Kaspersky Endpoint Security sử dụng chế độ KSN mở rộng. *Chế độ KSN mở rộng* là chế độ trong đó Kaspersky Endpoint Security sẽ gửi [dữ liệu bổ sung](#) đến Kaspersky.

4. Nếu cần, hãy tắt **Bật chế độ KSN mở rộng**.
5. Lưu các thay đổi của bạn.

Kết quả là nếu bật sử dụng KSN, Kaspersky Endpoint Security sẽ sử dụng thông tin về danh tiếng của các tập tin, tài nguyên web và ứng dụng nhận được từ Kaspersky Security Network.

Hạn chế của KSN Riêng

KSN Riêng (sau đây được gọi là KPSN) cho phép bạn sử dụng cơ sở dữ liệu danh tiếng cục bộ của riêng mình để kiểm tra danh tiếng của các đối tượng (tập tin hoặc địa chỉ web). Danh tiếng của một đối tượng được thêm vào cơ sở dữ liệu danh tiếng cục bộ có mức ưu tiên cao hơn đối tượng được thêm vào KSN/KPSN. Ví dụ: hãy hình dung Kaspersky Endpoint Security đang quét máy tính và yêu cầu danh tiếng của tập tin trong KSN/KPSN. Nếu tập tin có danh tiếng "không được tin tưởng" trong cơ sở dữ liệu danh tiếng cục bộ nhưng có danh tiếng "được tin tưởng" trong KSN/KPSN thì Kaspersky Endpoint Security sẽ phát hiện tập tin là "không được tin tưởng" và sẽ thực hiện hành động được định sẵn cho các mối đe dọa được phát hiện.

Tuy nhiên, trong một số trường hợp, Kaspersky Endpoint Security có thể không yêu cầu danh tiếng của một đối tượng trong KSN/KPSN. Trong trường hợp này, Kaspersky Endpoint Security sẽ không nhận được dữ liệu từ cơ sở dữ liệu danh tiếng cục bộ của KPSN. Kaspersky Endpoint Security có thể không yêu cầu danh tiếng của một đối tượng trong KSN/KPSN vì những lý do sau:


- Các ứng dụng Kaspersky đang sử dụng cơ sở dữ liệu danh tiếng ngoại tuyến. Cơ sở dữ liệu danh tiếng ngoại tuyến được thiết kế để tối ưu hóa tài nguyên trong quá trình vận hành các ứng dụng Kaspersky và để bảo vệ các đối tượng cực kỳ quan trọng trên máy tính. Cơ sở dữ liệu danh tiếng ngoại tuyến được tạo bởi các chuyên gia Kaspersky dựa trên dữ liệu từ Kaspersky Security Network. Các ứng dụng Kaspersky cập nhật cơ sở dữ liệu danh tiếng ngoại tuyến bằng cơ sở dữ liệu diệt virus của ứng dụng cụ thể. Nếu cơ sở dữ liệu danh tiếng ngoại tuyến chứa thông tin về một đối tượng đang được quét, ứng dụng sẽ không yêu cầu danh tiếng của đối tượng này từ KSN/KPSN.
- Loại trừ quét ([vùng tin tưởng](#)) được cấu hình trong thiết lập ứng dụng. Nếu đúng như vậy, ứng dụng không xem xét danh tiếng của đối tượng trong cơ sở dữ liệu danh tiếng cục bộ.
- Ứng dụng sử dụng các công nghệ tối ưu hóa quét, chẳng hạn như iSwift hoặc iChecker hoặc đang lưu vào bộ nhớ đệm các yêu cầu danh tiếng trong KSN / KPSN. Nếu đúng như vậy, ứng dụng có thể không yêu cầu danh tiếng của các đối tượng đã quét trước đó.
- Để tối ưu hóa khối lượng công việc, ứng dụng sẽ quét các tập tin có định dạng và dung lượng nhất định. Danh sách các định dạng và giới hạn dung lượng liên quan được xác định bởi các chuyên gia của Kaspersky. Danh sách này được cập nhật bằng cơ sở dữ liệu diệt virus của ứng dụng. Bạn cũng có thể cấu hình thiết lập tối ưu tác vụ quét trong giao diện ứng dụng, ví dụ như cho [thành phần Bảo vệ mỗi đe dọa tập tin](#).

Bật và tắt chế độ đám mây cho các thành phần bảo vệ

Chế độ đám mây chỉ chế độ hoạt động của ứng dụng trong đó Kaspersky Endpoint Security sử dụng phiên bản nhẹ của cơ sở dữ liệu diệt virus. Kaspersky Security Network hỗ trợ hoạt động của ứng dụng khi cơ sở dữ liệu diệt virus nhẹ đang được sử dụng. Phiên bản nhẹ của cơ sở dữ liệu diệt virus cho phép bạn sử dụng khoảng một nửa dung lượng RAM của máy tính so với dung lượng RAM được sử dụng với cơ sở dữ liệu thông thường. Nếu bạn không tham gia vào Kaspersky Security Network hoặc nếu chế độ đám mây bị tắt, Kaspersky Endpoint Security sẽ tải về phiên bản đầy đủ của cơ sở dữ liệu diệt virus từ các máy chủ của Kaspersky.

Khi sử dụng Kaspersky Private Security Network, chức năng chế độ đám mây có thể được sử dụng bắt đầu với Kaspersky Private Security Network phiên bản 3.0.

Để bật hoặc tắt chế độ đám mây cho các thành phần bảo vệ:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa nâng cao** → **Kaspersky Security Network**.
3. Sử dụng nút bật/tắt **Bật chế độ đám mây** để bật hoặc tắt thành phần này.
4. Lưu các thay đổi của bạn.

Kết quả là Kaspersky Endpoint Security sẽ tải xuống phiên bản nhẹ hoặc phiên bản đầy đủ của cơ sở dữ liệu diệt virus trong lần cập nhật tiếp theo.

Nếu phiên bản nhẹ của cơ sở dữ liệu diệt virus không sẵn có, Kaspersky Endpoint Security sẽ tự động chuyển sang phiên bản cao cấp của cơ sở dữ liệu diệt virus.

Thiết lập Proxy KSN

Máy tính của người dùng được quản lý bởi Máy chủ quản trị Kaspersky Security Center có thể tương tác với KSN thông qua dịch vụ Proxy KSN.

Dịch vụ Proxy KSN 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.
- Dịch vụ Proxy KSN sẽ lưu lại dữ liệu được xử lý, qua đó giảm tải cho mạng bên ngoài, kênh truyền thông và tăng tốc độ nhận thông tin được yêu cầu bởi máy tính của người dùng.

Theo mặc định, sau khi KSN được bật và Tuyên bố KSN được chấp nhận, ứng dụng sẽ sử dụng máy chủ proxy để kết nối với Kaspersky Security Network. Máy chủ proxy được ứng dụng sử dụng là Máy chủ quản trị Kaspersky Security Center qua cổng TCP 13111. Do đó, nếu Proxy KSN không khả dụng, bạn cần xác minh những điểm sau:

- Dịch vụ *ksnproxy* đang chạy trên Máy chủ quản trị.
- Tường lửa trên máy tính không chặn cổng 13111.

Bạn có thể cấu hình sử dụng Proxy KSN như sau: bật hoặc tắt Proxy KSN và cấu hình cổng cho kết nối. Để thực hiện, bạn cần mở thuộc tính Máy chủ quản trị. Để biết chi tiết về cấu hình Proxy KSN, vui lòng tham khảo Trợ giúp của Kaspersky Security Center. Bạn cũng có thể bật hoặc tắt Proxy KSN cho từng máy tính trong chính sách Kaspersky Endpoint Security.

[Cách bật hoặc tắt thành phần Proxy KSN trong Bảng điều khiển quản trị \(MMC\)](#)

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mỗi đe dọa nâng cao** → **Kaspersky Security Network**.
3. Trong mục **Thiết lập Proxy KSN**, hãy sử dụng hộp kiểm **Sử dụng Proxy KSN** để bật hoặc tắt Proxy KSN.
4. Nếu cần, hãy chọn hộp kiểm **Sử dụng máy chủ KSN khi Proxy KSN không có sẵn**.
Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ sử dụng các máy chủ KSN khi dịch vụ KSN Proxy không khả dụng. Máy chủ KSN có thể được đặt trên cả Kaspersky (khi KSN Toàn cầu được sử dụng) và trên một bên thứ ba (nếu KSN Riêng được sử dụng).
5. Lưu các thay đổi của bạn.

[Cách bật hoặc tắt thành phần Proxy KSN trong Bảng điều khiển web](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Advanced Threat Protection** → **Kaspersky Security Network**.
5. Sử dụng hộp kiểm **Use KSN Proxy** để bật hoặc tắt Proxy KSN.
6. Nếu cần, hãy chọn hộp kiểm **Use KSN servers when KSN Proxy is not available**.
Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ sử dụng các máy chủ KSN khi dịch vụ KSN Proxy không khả dụng. Máy chủ KSN có thể được đặt trên cả Kaspersky (khi KSN Toàn cầu được sử dụng) và trên một bên thứ ba (nếu KSN Riêng được sử dụng).
7. Lưu các thay đổi của bạn.

Địa chỉ Proxy KSN khớp với địa chỉ Máy chủ quản trị. Khi tên miền Máy chủ quản trị được thay đổi, bạn cần cập nhật địa chỉ Proxy KSN theo cách thủ công.

Để cấu hình địa chỉ Proxy KSN:

1. Trong Bảng điều khiển quản trị, hãy vào thư mục **Administration Server** → **Additional** → **Remote installation** → **Installation packages**.
2. Trong menu ngữ cảnh của thư mục **Installation packages**, hãy chọn **Properties**.
3. Trên thẻ **Tổng quát** trong cửa sổ được mở, hãy chỉ định địa chỉ mới của máy chủ Proxy KSN.
4. Lưu các thay đổi của bạn.

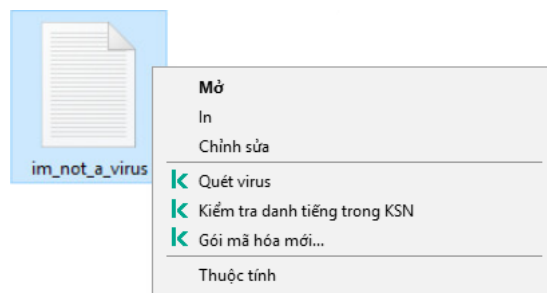
Kiểm tra danh tiếng của một tập tin trong Kaspersky Security Network

Nếu nghi ngờ về tính bảo mật của một tập tin, bạn có thể kiểm tra danh tiếng của tập tin đó trong Kaspersky Security Network.

Bạn có thể kiểm tra danh tiếng của một tập tin nếu bạn đã chấp nhận các điều khoản của [Tuyên bố Kaspersky Security Network](#).

Để kiểm tra danh tiếng của một tập tin trong Kaspersky Security Network:

Mở menu ngữ cảnh của tập tin và chọn tùy chọn **Kiểm tra danh tiếng trong KSN** (xem hình bên dưới).



Menu ngữ cảnh của tập tin

Kaspersky Endpoint Security hiển thị danh tiếng của tập tin:

✔ **Tin tưởng (Kaspersky Security Network)**. Hầu hết người dùng của Kaspersky Security Network đã xác nhận rằng tập tin này được tin cậy.

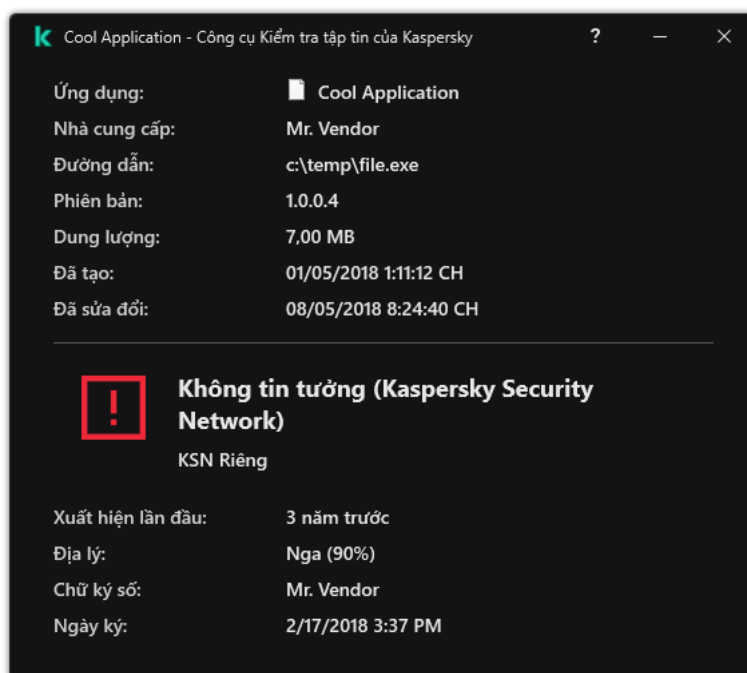
⚠ **Phần mềm hợp pháp có thể bị kẻ xâm nhập sử dụng để làm hư hại máy tính hoặc dữ liệu cá nhân của bạn.** Mặc dù chúng không có chức năng độc hại nào, nhưng các ứng dụng đó vẫn có thể bị kẻ xâm nhập khai thác. Để xem chi tiết về các phần mềm hợp pháp có thể bị bọn tội phạm lợi dụng để gây hại cho máy tính hoặc dữ liệu cá nhân của một người dùng, vui lòng tham khảo [trang web Bách khoa toàn thư của Kaspersky IT](#). Bạn có thể [thêm các ứng dụng này vào danh sách được tin tưởng](#).

❗ **Không tin tưởng (Kaspersky Security Network)**. Một virus hoặc ứng dụng khác [gây ra mối đe dọa](#).

❓ **Không xác định (Kaspersky Security Network)**. Kaspersky Security Network không có bất kỳ thông tin nào về tập tin. Bạn có thể quét tập tin bằng cơ sở dữ liệu diệt virus (tùy chọn **Quét virus** trong menu ngữ cảnh).

Kaspersky Endpoint Security sẽ hiển thị giải pháp KSN được sử dụng để xác định danh tiếng của tập tin: *KSN Toàn cầu* hoặc *KSN Riêng*.

Kaspersky Endpoint Security cũng sẽ hiển thị thông tin bổ sung về tập tin (xem hình bên dưới).



Danh tiếng của một tập tin trong Kaspersky Security Network

Quét kết nối được mã hóa


Sau khi cài đặt, Kaspersky Endpoint Security sẽ thêm chứng chỉ Kaspersky vào kho lưu trữ dành cho các chứng chỉ được tin tưởng của hệ thống (kho chứng chỉ Windows). Kaspersky Endpoint Security sẽ sử dụng chứng chỉ này để quét các kết nối được mã hóa. Kaspersky Endpoint Security cũng thêm việc sử dụng kho lưu trữ hệ thống các chứng chỉ được tin tưởng vào Firefox và Thunderbird để quét lưu lượng của các ứng dụng này.

Các thành phần [Kiểm soát Web](#), [Bảo vệ mỗi đe dọa thư điện tử](#) và [Bảo vệ mỗi đe dọa web](#) có thể giải mã và quét lưu lượng mạng được truyền tải qua các kết nối mã hóa sử dụng các giao thức sau:

- SSL 3.0.
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Bật quét kết nối được mã hóa

Để bật quét các kết nối được mã hóa:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Thiết lập mạng**.
3. Trong mục **Quét kết nối được mã hóa**, hãy chọn chế độ quét kết nối được mã hóa:
 - **Không quét các kết nối được mã hóa.** Kaspersky Endpoint Security sẽ không có quyền truy cập vào nội dung của các trang web có địa chỉ bắt đầu bằng `https://`.
 - **Quét các kết nối mã hóa khi được yêu cầu bởi các thành phần bảo vệ.** Kaspersky Endpoint Security sẽ chỉ quét lưu lượng được mã hóa khi được yêu cầu bởi các thành phần Bảo vệ mỗi đe dọa tập tin, Bảo vệ mỗi đe dọa thư điện tử và Kiểm soát Web.
 - **Luôn luôn quét các kết nối mã hóa.** Kaspersky Endpoint Security sẽ quét lưu lượng mạng được mã hóa ngay cả khi các thành phần bảo vệ bị tắt.

Kaspersky Endpoint Security không quét các kết nối được mã hóa được thiết lập bởi [các ứng dụng được tin tưởng có tính năng quét lưu lượng bị tắt](#). Kaspersky Endpoint Security không quét các kết nối được mã hóa trong danh sách website được tin tưởng được xác định trước. Các chuyên gia Kaspersky là những người tạo ra danh sách website được tin tưởng được định nghĩa trước. Danh sách này được cập nhật bằng cơ sở dữ liệu diệt virus của ứng dụng. Bạn chỉ có thể xem danh sách website được tin tưởng được định nghĩa trước trong giao diện Kaspersky Endpoint Security. Bạn không thể xem danh sách này trong Bảng điều khiển Kaspersky Security Center.

4. Nếu cần, hãy [thêm loại trừ quét: địa chỉ và ứng dụng được tin tưởng](#).
5. Cấu hình thiết lập để quét các kết nối được mã hóa (xem bảng bên dưới).
6. Lưu các thay đổi của bạn.

Thiết lập quét các kết nối được mã hóa

Tham số	Mô tả
Chứng chỉ gốc được tin tưởng	<p>Danh sách chứng chỉ gốc được tin tưởng. Kaspersky Endpoint Security cho phép bạn cài đặt chứng chỉ gốc được tin tưởng trên máy tính của người dùng, ví dụ như nếu bạn cần triển khai một trung tâm chứng thực mới. Ứng dụng cho phép bạn thêm chứng chỉ vào một kho chứng chỉ đặc biệt của Kaspersky Endpoint Security. Trong trường hợp này, chứng chỉ được coi là được tin tưởng cho riêng ứng dụng Kaspersky Endpoint Security. Nói cách khác, người dùng có thể lấy quyền truy cập vào một website bằng chứng chỉ mới trong trình duyệt. Nếu ứng dụng khác cố lấy quyền truy cập vào website đó thì bạn có thể nhận một lỗi kết nối do sự cố chứng chỉ. Để thêm vào kho chứng chỉ hệ thống, bạn có thể sử dụng các chính sách nhóm của Active Directory.</p>
Hành động khi cố truy cập một tên miền có chứng chỉ không được tin tưởng	<ul style="list-style-type: none"> Cho phép. Khi truy cập một tên miền với một chứng chỉ không được tin tưởng, Kaspersky Endpoint Security sẽ cho phép kết nối mạng. Khi mở một tên miền có chứng chỉ không được tin tưởng trong một trình duyệt, Kaspersky Endpoint Security sẽ hiển thị một trang HTML với cảnh báo và giải thích rằng việc truy cập tên miền cụ thể này là không được khuyến nghị. Người dùng có thể nhấn vào liên kết từ trang cảnh báo HTML để nhận quyền truy cập đến tài nguyên web được yêu cầu. Nếu ứng dụng hoặc dịch vụ của bên thứ ba thiết lập kết nối với tên miền có chứng chỉ không được tin tưởng thì Kaspersky Endpoint Security sẽ tạo chứng chỉ riêng để quét lưu lượng. Chứng chỉ mới có trạng thái <i>Không tin tưởng</i>. Đây là điều cần thiết để cảnh báo ứng dụng của bên thứ ba về kết nối không được tin tưởng vì không thể hiển thị trang HTML trong trường hợp này và kết nối có thể được thiết lập ở chế độ nền. Chặn kết nối. Khi truy cập một tên miền với một chứng chỉ không được tin tưởng, Kaspersky Endpoint Security sẽ chặn kết nối mạng. Khi mở một tên miền có chứng chỉ không được tin tưởng trong một trình duyệt, Kaspersky Endpoint Security sẽ hiển thị một trang HTML giải thích rằng tên miền này bị chặn.
Khi xảy ra lỗi quét kết nối được mã hóa	<ul style="list-style-type: none"> Chặn kết nối. Nếu mục này được chọn, khi xảy ra lỗi quét kết nối được mã hóa, Kaspersky Endpoint Security sẽ chặn kết nối mạng. Thêm tên miền vào mục loại trừ. Nếu mục này được chọn, khi xảy ra lỗi quét kết nối được mã hóa, Kaspersky Endpoint Security sẽ thêm tên miền đã gây ra lỗi vào danh sách các tên miền có lỗi quét và không giám sát lưu lượng mạng được mã hóa khi truy cập tên miền này. Bạn chỉ có thể xem danh sách các tên miền có lỗi quét kết nối được mã hóa trong giao diện cục bộ của ứng dụng. Để xóa nội dung danh sách, bạn cần chọn Chặn kết nối. Kaspersky Endpoint Security cũng sẽ tạo ra một sự kiện cho lỗi quét kết nối được mã hóa.
Chặn các kết nối SSL 2.0 (khuyến dùng)	<p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ chặn các kết nối mạng được thiết lập qua giao thức SSL 2.0.</p> <p>Nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ không chặn các kết nối mạng được thiết lập qua giao thức SSL 2.0 và không giám sát lưu lượng mạng được truyền tải qua các kết nối này.</p>
Giải mã kết nối mã hóa với các website sử dụng	<p>Các chứng chỉ EV (Chứng chỉ Chứng thực mở rộng) sẽ xác nhận tính xác thực của các website và tăng cường tính bảo mật của kết nối. Các trình duyệt sử dụng biểu tượng ổ khóa trong thanh địa chỉ của chúng để chỉ báo một trang web có chứng chỉ EV. Các trình duyệt cũng có thể tô màu toàn bộ hoặc một phần thanh địa chỉ bằng màu xanh lá cây.</p>

chứng chỉ EV

Nếu hộp kiểm được chọn, Kaspersky Endpoint Security sẽ giải mã và giám sát các kết nối được mã hóa với các website sử dụng chứng chỉ EV.

Nếu hộp kiểm không được chọn, Kaspersky Endpoint Security sẽ không có quyền truy cập nội dung của lưu lượng HTTPS. Vì lý do này, ứng dụng sẽ chỉ giám sát lưu lượng HTTPS dựa trên địa chỉ website mà thôi, ví dụ như <https://bing.com>.

Nếu bạn đang mở một website có chứng chỉ EV lần đầu tiên, kết nối được mã hóa sẽ được giải mã, cho dù hộp kiểm có được chọn hay không.

Cài đặt chứng chỉ gốc được tin tưởng

Kaspersky Endpoint Security cho phép bạn cài đặt chứng chỉ gốc được tin tưởng trên máy tính của người dùng, ví dụ như nếu bạn cần triển khai một trung tâm chứng thực mới. Ứng dụng cho phép bạn thêm chứng chỉ vào một kho chứng chỉ đặc biệt của Kaspersky Endpoint Security. Trong trường hợp này, chứng chỉ được coi là được tin tưởng cho riêng ứng dụng Kaspersky Endpoint Security. Nói cách khác, người dùng có thể lấy quyền truy cập vào một website bằng chứng chỉ mới trong trình duyệt. Nếu ứng dụng khác cố lấy quyền truy cập vào website đó thì bạn có thể nhận một lỗi kết nối do sự cố chứng chỉ. Để thêm vào kho chứng chỉ hệ thống, bạn có thể sử dụng các chính sách nhóm của Active Directory.


Cách cài đặt chứng chỉ gốc được tin tưởng trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Thiết lập mạng**.
6. Trong mục **Chứng chỉ gốc được tin tưởng**, hãy nhấn vào **Thêm**.
7. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy chọn một chứng chỉ gốc được tin tưởng. Kaspersky Endpoint Security hỗ trợ các chứng chỉ có phần mở rộng là PEM, DER và CRT.
8. Lưu các thay đổi của bạn.

Cách cài đặt chứng chỉ gốc được tin tưởng trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Thiết lập tổng quát** → **Thiết lập mạng**.
5. Nhấn vào **Hiển thị chứng chỉ**.
6. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy nhấn vào **Thêm** và chọn một chứng chỉ gốc được tin tưởng.
Kaspersky Endpoint Security hỗ trợ các chứng chỉ có phần mở rộng là PEM, DER và CRT.
7. Lưu các thay đổi của bạn.

Cách cài đặt chứng chỉ gốc được tin tưởng trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Thiết lập mạng**.
3. Trong mục **Quét kết nối được mã hóa**, hãy nhấn vào **Hiển thị chứng chỉ**.
4. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy nhấn vào **Thêm** và chọn một chứng chỉ gốc được tin tưởng.
Kaspersky Endpoint Security hỗ trợ các chứng chỉ có phần mở rộng là PEM, DER và CRT.
5. Lưu các thay đổi của bạn.

Kết quả là khi quét lưu lượng, ngoài kho chứng chỉ hệ thống, Kaspersky Endpoint Security sẽ sử dụng kho chứng chỉ của riêng mình.

Quét các kết nối được mã hóa bằng chứng chỉ không được tin tưởng

Sau khi cài đặt, Kaspersky Endpoint Security sẽ thêm chứng chỉ Kaspersky vào kho lưu trữ dành cho các chứng chỉ được tin tưởng của hệ thống (kho chứng chỉ Windows). Kaspersky Endpoint Security sẽ sử dụng chứng chỉ này để quét các kết nối được mã hóa. Khi truy cập một tên miền có chứng chỉ không được tin tưởng, bạn có thể cho phép hoặc từ chối quyền truy cập của người dùng vào tên miền đó (xem hướng dẫn bên dưới).

Nếu bạn đã cho phép người dùng truy cập các tên miền có chứng chỉ không được tin tưởng thì Kaspersky Endpoint Security sẽ thực hiện các hành động sau:

- Khi truy cập một tên miền có chứng chỉ không được tin tưởng trong *trình duyệt*, Kaspersky Endpoint Security sẽ sử dụng chứng chỉ của Kaspersky để quét lưu lượng. Kaspersky Endpoint Security sẽ hiển thị một trang HTML kèm cảnh báo và thông tin về lý do tại sao không nên truy cập vào tên miền liên quan (xem hình bên dưới). Người dùng có thể nhấn vào liên kết từ trang cảnh báo HTML để nhận

quyền truy cập đến tài nguyên web được yêu cầu. Sau khi vào liên kết này, trong một giờ tiếp theo, Kaspersky Endpoint Security sẽ không hiển thị các cảnh báo về một chứng chỉ không được tin tưởng khi truy cập các tài nguyên khác trên tên miền này. Kaspersky Endpoint Security cũng sẽ tạo ra một sự kiện về việc thiết lập kết nối được mã hóa bằng chứng chỉ không được tin tưởng.

- Nếu *ứng dụng hoặc dịch vụ của bên thứ ba* thiết lập kết nối với tên miền có chứng chỉ không được tin tưởng thì Kaspersky Endpoint Security sẽ tạo chứng chỉ riêng để quét lưu lượng. Chứng chỉ mới có trạng thái *Không tin tưởng*. Đây là điều cần thiết để cảnh báo ứng dụng của bên thứ ba về kết nối không được tin tưởng vì không thể hiển thị trang HTML trong trường hợp này và kết nối có thể được thiết lập ở chế độ nền. Do đó, nếu ứng dụng của bên thứ ba có các công cụ xác minh chứng chỉ được tích hợp sẵn thì kết nối đó có thể bị ngắt. Trong trường hợp đó, bạn phải liên hệ với chủ sở hữu tên miền và thiết lập kết nối được tin tưởng. Nếu không thể thiết lập kết nối được tin tưởng, bạn có thể [thêm ứng dụng của bên thứ ba đó vào danh sách các ứng dụng được tin tưởng](#). Kaspersky Endpoint Security cũng sẽ tạo ra một sự kiện về việc thiết lập kết nối được mã hóa bằng chứng chỉ không được tin tưởng.


[Cách cấu hình quét các kết nối được mã hóa bằng chứng chỉ không được tin tưởng trong Bảng điều khiển quản trị \(MMC\)](#)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Thiết lập mạng**.
6. Trong mục **Quét kết nối được mã hóa**, hãy nhấn nút **Địa chỉ được tin tưởng**.
7. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy chọn chế độ vận hành ứng dụng khi truy cập tên miền có chứng chỉ không được tin tưởng: **Cho phép** hoặc **Chặn kết nối**.
8. Lưu các thay đổi của bạn.

[Cách cấu hình quét các kết nối được mã hóa bằng chứng chỉ không được tin tưởng trong Bảng điều khiển web và Bảng điều khiển đám mây](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Thiết lập tổng quát** → **Thiết lập mạng**.
5. Trong mục **Quét kết nối được mã hóa**, hãy chọn chế độ vận hành ứng dụng khi truy cập tên miền có chứng chỉ không được tin tưởng: **Cho phép** hoặc **Chặn kết nối**.
6. Lưu các thay đổi của bạn.

Cách cấu hình quét các kết nối được mã hóa bằng chứng chỉ không được tin tưởng trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Thiết lập mạng**.
3. Trong mục **Quét kết nối được mã hóa**, hãy chọn chế độ vận hành ứng dụng khi truy cập tên miền có chứng chỉ không được tin tưởng: **Cho phép** hoặc **Chặn kết nối**.
4. Lưu các thay đổi của bạn.



Truy cập một tên miền với một chứng nhận không được tin tưởng

Kết nối của bạn không bảo mật. Tội phạm có thể đánh cắp dữ liệu riêng tư của bạn. Bạn nên ngừng làm việc với website này.

revoked.badssl.com

Lý do:

Sự tin tưởng đối với chứng nhận này hoặc một trong các chứng nhận trong chuỗi đã bị thu hồi.

[Xem chứng nhận](#)

[Tôi hiểu độ rủi ro, nhưng muốn tiếp tục](#)

kaspersky

Cảnh báo về việc truy cập một tên miền có chứng chỉ không được tin tưởng

Quét các kết nối được mã hóa trong Firefox và Thunderbird


Sau khi cài đặt, Kaspersky Endpoint Security sẽ thêm chứng chỉ Kaspersky vào kho lưu trữ dành cho các chứng chỉ được tin tưởng của hệ thống (kho chứng chỉ Windows). Theo mặc định, Firefox và Thunderbird sử dụng kho chứng chỉ Mozilla độc quyền của riêng họ thay vì kho chứng chỉ Windows. Nếu Kaspersky Security Center được triển khai trong tổ chức của bạn và đang có một chính sách được áp dụng cho máy tính thì Kaspersky Endpoint Security sẽ tự động cho phép sử dụng kho chứng chỉ Windows trong Firefox và Thunderbird để quét lưu lượng của các ứng dụng này. Nếu một chính sách không được áp dụng cho máy tính, bạn có thể chọn kho chứng chỉ sẽ được các ứng dụng Mozilla sử dụng. Nếu bạn đã chọn kho chứng chỉ Mozilla, hãy thêm chứng chỉ Kaspersky vào đó theo cách thủ công. Làm vậy sẽ giúp tránh các lỗi khi làm việc với lưu lượng HTTPS.

Để quét lưu lượng trong trình duyệt Mozilla Firefox và ứng dụng thư điện tử Thunderbird, bạn phải [bật Quét kết nối được mã hóa](#). Nếu Quét kết nối được mã hóa bị tắt, Kaspersky Endpoint Security sẽ không quét lưu lượng được mã hóa trong trình duyệt Mozilla Firefox và ứng dụng thư điện tử Thunderbird.

Trước khi thêm chứng chỉ vào kho của Mozilla, hãy xuất chứng chỉ Kaspersky từ Bảng điều khiển của Windows (thuộc tính trình duyệt). Để biết chi tiết về việc xuất chứng chỉ Kaspersky, vui lòng tham khảo [Cơ sở kiến thức Hỗ trợ kỹ thuật](#). Để biết chi tiết về việc thêm chứng chỉ vào kho, hãy truy cập [trang web hỗ trợ kỹ thuật của Mozilla](#).

Bạn chỉ có thể chọn kho chứng chỉ trong giao diện cục bộ của ứng dụng.


Để chọn một kho chứng chỉ để quét các kết nối được mã hóa trong Firefox và Thunderbird:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Thiết lập mạng**.
3. Trong mục **Mozilla Firefox và Thunderbird**, hãy chọn hộp kiểm **Sử dụng kho chứng chỉ đã chọn để quét các kết nối được mã hóa trong các ứng dụng Mozilla**.
4. Chọn kho chứng chỉ:
 - **Sử dụng kho chứng chỉ Windows (khuyến dùng)**. Chứng chỉ gốc của Kaspersky được thêm vào kho này trong quá trình cài đặt Kaspersky Endpoint Security.
 - **Sử dụng kho chứng chỉ Mozilla**. Mozilla Firefox và Thunderbird sử dụng kho chứng chỉ của riêng họ. Nếu chọn kho chứng chỉ của Mozilla, bạn cần thêm chứng chỉ gốc Kaspersky vào kho này theo cách thủ công thông qua các thuộc tính của trình duyệt.
5. Lưu các thay đổi của bạn.

Loại trừ các kết nối khỏi tác vụ quét

Hầu hết các tài nguyên web đều sử dụng các kết nối được mã hóa. Các chuyên gia của Kaspersky khuyên bạn bật [Quét kết nối được mã hóa](#). Nếu tác vụ quét các kết nối được mã hóa có cản trở hoạt động liên quan đến công việc, bạn có thể thêm một trang web vào các loại trừ được gọi là *địa chỉ được tin tưởng*. Nếu một ứng dụng được tin tưởng sử dụng kết nối được mã hóa, bạn có thể [tắt quét kết nối được mã hóa cho ứng dụng này](#). Ví dụ: bạn có thể tắt quét các kết nối được mã hóa để quét các ứng dụng lưu trữ đám mây sử dụng xác thực hai yếu tố với chứng chỉ của riêng chúng.

Để loại trừ một địa chỉ web khỏi các tác vụ quét kết nối được mã hóa:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Thiết lập mạng**.
3. Trong mục **Quét kết nối được mã hóa**, hãy nhấn nút **Địa chỉ được tin tưởng**.
4. Nhấn vào **Thêm**.
5. Nhập một tên miền hoặc địa chỉ IP nếu bạn không muốn Kaspersky Endpoint Security quét các kết nối được mã hóa đã thiết lập khi truy cập tên miền đó.

Kaspersky Endpoint Security hỗ trợ ký tự để nhập một tên đại diện trong tên miền.

Kaspersky Endpoint Security không hỗ trợ mặt nạ cho các địa chỉ IP. Bạn có thể nhập một dải địa chỉ IP vào giao diện cục bộ của ứng dụng (ví dụ: 198.51.100.0/24). Bạn không thể nhập một dải địa chỉ IP vào Bảng điều khiển Kaspersky Security Center.


Ví dụ:

- – bản ghi này gồm các địa chỉ sau: <https://domain.com>, <https://www.domain.com>, <https://domain.com/page123>. Bản ghi không bao gồm các tên miền con (ví dụ: subdomain.domain.com).
- – bản ghi bao gồm các địa chỉ sau: <https://subdomain.domain.com>, <https://subdomain.domain.com/page123>. Bản ghi không bao gồm tên miền domain.com.
- – bản ghi này bao gồm các địa chỉ sau: <https://movies.domain.com>, <https://images.domain.com/page123>. Bản ghi không bao gồm tên miền domain.com.

6. Lưu các thay đổi của bạn.

Theo mặc định, Kaspersky Endpoint Security không quét các kết nối được mã hóa khi xảy ra lỗi và thêm website đó vào danh sách đặc biệt *Tên miền có lỗi quét*. Kaspersky Endpoint Security sẽ tổng hợp một danh sách riêng cho từng người dùng và không gửi dữ liệu đến Kaspersky Security Center. Bạn có thể [bật chặn kết nối khi xảy ra lỗi quét](#). Bạn chỉ có thể xem danh sách các tên miền có lỗi quét kết nối được mã hóa trong giao diện cục bộ của ứng dụng.


Để xem danh sách các tên miền có lỗi quét:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Thiết lập mạng**.
3. Trong mục **Quét kết nối được mã hóa**, hãy nhấn nút **Tên miền có lỗi quét**.

Một danh sách các tên miền có lỗi quét sẽ mở ra. Để đặt lại danh sách, hãy bật chặn kết nối khi xảy ra lỗi quét trong chính sách, áp dụng chính sách, sau đó đặt lại tham số về giá trị ban đầu và áp dụng lại chính sách.

Các chuyên gia của Kaspersky tạo một danh sách các *loại trừ toàn cục* — các website được tin tưởng mà Kaspersky Endpoint Security sẽ không kiểm tra, bất kể thiết lập của ứng dụng.

Để xem các loại trừ toàn cục của tác vụ quét lưu lượng được mã hóa:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Thiết lập mạng**.
3. Trong mục **Quét kết nối được mã hóa**, hãy nhấn vào liên kết danh sách các trang web được tin tưởng.

Thao tác này sẽ mở ra danh sách các website do các chuyên gia của Kaspersky biên soạn. Kaspersky Endpoint Security không quét các kết nối được bảo vệ cho các website trong danh sách. Danh sách này có thể được cập nhật khi cơ sở dữ liệu và mô-đun Kaspersky Endpoint Security được cập nhật.

Xóa sạch dữ liệu

Kaspersky Endpoint Security cho phép bạn sử dụng một tác vụ để xóa dữ liệu từ xa trên máy tính của người dùng.

Kaspersky Endpoint Security sẽ xóa dữ liệu như sau:

- Trong chế độ im lặng;
- Trên ổ đĩa cứng và ổ đĩa di động;
- Đối với mọi tài khoản người dùng trên máy tính.

Kaspersky Endpoint Security sẽ thực hiện tác vụ *Xóa sạch dữ liệu* bất kể loại bản quyền nào đang được sử dụng, ngay cả sau khi giấy phép đã hết hạn.

Các chế độ Xóa sạch dữ liệu

Tác vụ này cho phép bạn xóa dữ liệu trong các chế độ sau:

- Xóa dữ liệu ngay lập tức.
Ví dụ như trong chế độ này, bạn có thể xóa dữ liệu cũ để giải phóng dung lượng ổ đĩa.

- Xóa dữ liệu được hoãn.

Đây là chế độ dành cho mục đích như bảo vệ dữ liệu trên máy tính xách tay trong trường hợp máy tính xách tay bị thất lạc hoặc bị mất cắp. Bạn có thể cấu hình xóa dữ liệu tự động nếu máy tính xách tay được chuyển ra ngoài ranh giới của mạng doanh nghiệp và chưa được đồng bộ hóa với Kaspersky Security Center trong một khoảng thời gian dài.

Không thể đặt lịch để xóa dữ liệu trong thuộc tính của tác vụ. Bạn chỉ có thể xóa dữ liệu ngay lập tức sau khi bắt đầu tác vụ một cách thủ công hoặc định cấu hình xóa dữ liệu bị trì hoãn nếu không có kết nối đến Kaspersky Security Center.

Các hạn chế

Tính năng Xóa sạch dữ liệu có các hạn chế sau:

- Chỉ có quản trị viên Kaspersky Security Center mới có thể quản lý tác vụ *Xóa sạch dữ liệu*. Bạn không thể cấu hình hoặc bắt đầu một tác vụ trong giao diện cục bộ của Kaspersky Endpoint Security.
- Đối với hệ thống tập tin NTFS, Kaspersky Endpoint Security chỉ xóa tên của các luồng dữ liệu chính. Không thể xóa tên luồng dữ liệu thay thế.
- Khi bạn xóa một tập tin liên kết biểu tượng, Kaspersky Endpoint Security cũng xóa các tập tin có đường dẫn được chỉ định trong liên kết biểu tượng.

Tạo tác vụ Xóa sạch dữ liệu

Để xóa dữ liệu trên máy tính của người dùng:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.
Danh sách tác vụ sẽ mở.
2. Nhấn vào nút **Thêm**.
Trình hướng dẫn Tác vụ sẽ được bắt đầu.
3. Cấu hình các thiết lập của tác vụ:
 - a. Trong danh sách thả xuống **Ứng dụng**, hãy chọn **Kaspersky Endpoint Security cho Windows (11.9.0)**.
 - b. Trong danh sách thả xuống **Loại tác vụ**, hãy chọn **Xóa sạch dữ liệu**.
 - c. Trong trường **Task name**, nhập một mô tả ngắn, ví dụ như *Xóa sạch dữ liệu (Chống mất cắp)*.
 - d. Trong phần **Select devices to which the task will be assigned**, chọn phạm vi tác vụ.
4. Chọn các thiết bị theo phạm vi tác vụ được chọn. Chuyển sang bước tiếp theo.

Nếu máy tính mới được thêm vào một nhóm quản trị trong phạm vi của tác vụ, tác vụ xóa dữ liệu ngay lập tức sẽ chỉ được thực hiện trên các máy tính mới đó nếu tác vụ được hoàn thành trong vòng 5 phút sau khi thêm máy tính mới.

5. Thoát Trình hướng dẫn.
Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ.
6. Nhấn vào tác vụ **Xóa sạch dữ liệu** cho Kaspersky Endpoint Security.
Cửa sổ thuộc tính tác vụ sẽ được mở ra.

7. Chọn thẻ **Application settings**.

8. Chọn phương thức xóa dữ liệu:

- **Xóa thông qua hệ điều hành.** Kaspersky Endpoint Security sẽ sử dụng các tài nguyên của hệ điều hành để xóa tập tin mà không gửi chúng vào thùng rác.
- **Xóa hoàn toàn, không thể phục hồi.** Kaspersky Endpoint Security sẽ ghi đè các tập tin bằng dữ liệu ngẫu nhiên. Thực tế, không thể khôi phục dữ liệu sau khi bị xóa.

9. Nếu bạn muốn xóa dữ liệu trì hoãn, hãy chọn hộp kiểm **Tự động xóa sạch dữ liệu khi không có kết nối đến Kaspersky Security Center trong thời gian lâu hơn N ngày**. Xác định số ngày.

Tác vụ xóa dữ liệu được hoãn sẽ được thực hiện sau mỗi lần không có kết nối đến Kaspersky Security Center trong khoảng thời gian xác định.

Khi cấu hình xóa dữ liệu được hoãn, xin lưu ý rằng các nhân viên có thể tắt máy tính của họ trước khi tham gia vào một kỳ nghỉ. Trong trường hợp này, khoảng thời gian không có kết nối có thể kéo dài vượt mức và dữ liệu sẽ bị xóa. Ngoài ra, bạn cũng cần lưu ý lịch làm việc của người dùng ngoại tuyến. Để biết thêm chi tiết về làm việc với máy tính ngoại tuyến và người dùng ngoài văn phòng, vui lòng tham khảo [Trợ giúp của Kaspersky Security Center](#).

Nếu hộp kiểm này không được chọn, tác vụ sẽ được thực hiện ngay lập tức sau khi đồng bộ hóa với Kaspersky Security Center.

10. Tạo một danh sách đối tượng cần xóa:

- **Thư mục.** Kaspersky Endpoint Security sẽ xóa mọi tập tin trong thư mục và các thư mục con. Kaspersky Endpoint Security không hỗ trợ ký tự đại diện và biết môi trường để nhập đường dẫn thư mục.
- **Các tập tin theo phần mở rộng.** Kaspersky Endpoint Security sẽ tìm kiếm các tập tin với phần mở rộng được quy định trên tất cả các ổ đĩa của máy tính, bao gồm ổ đĩa di động. Sử dụng ký tự ";" hoặc "," để nhập nhiều phần mở rộng.
- **Phạm vi được định sẵn.** Kaspersky Endpoint Security sẽ xóa các tập tin khỏi các khu vực sau:
 - **Documents.** Các tập tin trong thư mục *Documents* tiêu chuẩn của hệ điều hành và các thư mục con.
 - **Cookies.** Các tập tin được trình duyệt sử dụng để lưu dữ liệu từ các website được người dùng truy cập (ví dụ như dữ liệu cấp phép cho người dùng).
 - **Desktop.** Các tập tin trong thư mục *Desktop* tiêu chuẩn của hệ điều hành và các thư mục con.
 - **Các tập tin tạm Internet Explorer.** Các tập tin tạm thời liên quan đến hoạt động của Internet Explorer, ví dụ như các bản sao của các website, hình ảnh và tập tin đa phương tiện.
 - **Các tập tin tạm.** Các tập tin tạm thời liên quan đến hoạt động của các ứng dụng được cài đặt trên máy tính. Ví dụ: các ứng dụng Microsoft Office tạo các tập tin tạm thời chứa các bản sao lưu của tài liệu.
 - **Các tập tin Outlook.** Các tập tin liên quan đến hoạt động của ứng dụng trình khách Outlook: tập tin dữ liệu (PST), tập tin dữ liệu ngoại tuyến (OST), tập tin sổ địa chỉ ngoại tuyến (OAB) và tập tin sổ địa chỉ cá nhân (PAB).

- **Hồ sơ người dùng.** Bộ tập tin và thư mục lưu trữ các thiết lập của hệ điều hành dành cho tài khoản của người dùng cục bộ.

Bạn có thể tạo một danh sách các đối tượng cần xóa trên mỗi thẻ. Kaspersky Endpoint Security sẽ tạo một danh sách tổng hợp và xóa các tập tin khỏi danh sách này khi một tác vụ hoàn thành.

Bạn không thể xóa các tập tin cần thiết cho hoạt động của Kaspersky Endpoint Security.

11. Lưu các thay đổi của bạn.

12. Chọn hộp kiểm cạnh tác vụ.

13. Nhấn vào nút **Chạy**.

Kết quả là dữ liệu trên máy tính của người dùng sẽ bị xóa theo chế độ được chọn: xóa ngay lập tức hoặc xóa khi không có kết nối. Nếu Kaspersky Endpoint Security không thể xóa một tập tin, như khi người dùng đang sử dụng một tập tin thì ứng dụng không cố xóa tập tin đó lần nữa. Để xóa dữ liệu hoàn toàn, vui lòng chạy lại tác vụ.

Kiểm soát máy tính

Kiểm soát Web

Kiểm soát Web quản lý quyền truy cập của người dùng đối với các tài nguyên web. Điều này giúp giảm lưu lượng và việc sử dụng không hợp lý thời gian làm việc. Khi người dùng cố mở một website bị hạn chế bởi Kiểm soát Web, Kaspersky Endpoint Security sẽ chặn quyền truy cập hoặc hiển thị một cảnh báo (xem hình bên dưới).

Kaspersky Endpoint Security chỉ giám sát lưu lượng HTTP và lưu lượng HTTPS.

Để giám sát lưu lượng HTTPS, bạn cần [bật quét kết nối được mã hóa](#).

Các phương thức quản lý quyền truy cập website

Kiểm soát Web cho phép bạn cấu hình quyền truy cập đến các website bằng các phương thức sau đây:

- **Danh mục website.** Các website được phân loại theo dịch vụ đám mây của Kaspersky Security Network, phân tích theo hành vi và cơ sở dữ liệu của các website đã biết (đã được thêm vào cơ sở dữ liệu của ứng dụng). Ví dụ: bạn có thể hạn chế quyền truy cập của người dùng vào danh mục "Mạng xã hội" hoặc các [danh mục khác](#).
- **Loại dữ liệu.** Bạn có thể hạn chế truy cập của người dùng đến dữ liệu trên một website, ví dụ như ảnh các ảnh đồ họa. Kaspersky Endpoint Security xác định loại dữ liệu dựa theo định dạng tập tin, không dựa theo phần mở rộng của tập tin.

Kaspersky Endpoint Security không quét các tập tin bên trong tập tin nén. Ví dụ: nếu các tập tin ảnh được đặt trong một tập tin nén thì Kaspersky Endpoint Security sẽ coi đó là dữ liệu "Tập tin nén", không phải là "Tập tin đồ họa".

- **Địa chỉ được chỉ định.** Bạn có thể nhập một địa chỉ web hoặc [sử dụng các đại diện](#).

Bạn có thể sử dụng đồng thời nhiều phương thức để quản lý quyền truy cập đến các website. Ví dụ: bạn có thể hạn chế quyền truy cập loại dữ liệu "Tập tin văn phòng" chỉ với riêng danh mục website "Thư điện tử trên web".


Quy tắc truy cập website

Kiểm soát Web quản lý quyền truy cập của người dùng đến các website thông qua các *quy tắc truy cập*. Bạn có thể thiết lập các cấu hình nâng cao sau đối với một quy tắc truy cập website:

- Những người dùng là đối tượng áp dụng của quy tắc.
Ví dụ như bạn có thể hạn chế truy cập Internet của tất cả người dùng của công ty thông qua một trình duyệt, trừ bộ phận CNTT.
- Lịch quy tắc.
Ví dụ như bạn có thể chỉ hạn chế truy cập Internet thông qua một trình duyệt trong giờ làm việc.

Các mức ưu tiên của quy tắc truy cập

Mỗi quy tắc có một mức ưu tiên. Quy tắc có vị trí càng cao trên danh sách thì càng có mức ưu tiên cao. Nếu một website đã được thêm vào nhiều quy tắc, Kiểm soát Web sẽ quản lý quyền truy cập website đó dựa trên quy tắc có mức ưu tiên cao nhất. Ví dụ như Kaspersky Endpoint Security có thể xác định một cổng thông tin của doanh nghiệp là một mạng xã hội. Để hạn chế truy cập đến các mạng xã hội và cho phép truy cập cổng thông tin web của doanh nghiệp, hãy tạo hai quy tắc: một quy tắc chặn truy cập dành cho danh mục website "Mạng xã hội" và một quy tắc cho phép truy cập dành cho cổng thông tin web của doanh nghiệp. Quy tắc truy cập dành cho cổng thông tin web của doanh nghiệp phải có mức ưu tiên cao hơn so với quy tắc dành cho mạng xã hội.



Trang web yêu cầu không được cung cấp.


Địa chỉ: <http://kaspersky.ru/>.

Trang web bị ngăn chặn bởi quy tắc block.

Lý do: tài nguyên web thuộc về thể loại nội dung Không xác định và thể loại kiểu dữ liệu Không xác định.

Tài nguyên web bị cấm tại công ty. Nếu bạn nghĩ rằng việc ngăn chặn là nhầm lẫn hoặc nếu bạn cần truy cập đến nguồn tài nguyên web này, liên hệ quản trị viên của mạng nội bộ công ty ([Yêu cầu truy cập](#)).

Thư được tạo vào: 29.10.2020 13:09:53



Trang web yêu cầu có thể không an toàn hoặc bị cấm bởi chính sách công ty.

Địa chỉ: <http://kaspersky.com/>.

Trang web bị ngăn chặn bởi quy tắc warn.

Lý do: nguồn tài nguyên web thuộc các thể loại nội dung Không xác định và thể loại kiểu dữ liệu Không xác định.

Nhấn vào liên kết <http://kaspersky.com/> để yêu cầu mở trang web.
Nhấn vào liên kết http://kaspersky.com/* để được quyền truy cập vào toàn bộ nội dung của trang web mà trên đó các yêu cầu trang web.
Nhấn vào liên kết */*.kaspersky.com/* để được quyền truy cập vào tất cả lĩnh vực có mức độ thấp hơn hoặc bằng với "*".

Truy cập vào các nguồn tài nguyên web được liệt kê ở trên sẽ được cấp trong phiên làm việc hiện tại của Kaspersky Endpoint Security.
Trong trường hợp đây là cảnh báo sai, liên hệ quản trị viên của mạng nội bộ công ty ([Yêu cầu truy cập](#)).

Thư được tạo vào: 29.10.2020 13:09:59

Thông báo của Kiểm soát Web

Bật và tắt Kiểm soát Web

Theo mặc định, Kiểm soát Web sẽ được bật.

Để bật hoặc tắt Kiểm soát Web:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .

2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát Web**.
3. Sử dụng nút bật/tắt **Kiểm soát Web** để bật hoặc tắt thành phần.
4. Lưu các thay đổi của bạn.

Hành động với quy tắc truy cập tài nguyên web

Bạn không nên tạo nhiều hơn 1000 quy tắc truy cập các tài nguyên web, bởi điều này có thể khiến hệ thống trở nên bất ổn định.

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 dữ liệu thuộc các kiểu được quy định bởi những danh mục này. Khi người dùng truy cập các tài nguyên web thuộc một danh 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 danh 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 danh 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 Kịch bản và Bảng định kiểu, 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. Quy tắc này được áp dụng cho mọi tài nguyên web không được bao gồm bởi các quy tắc khác, và cho phép hoặc chặn truy cập của tất cả người dùng đến các tài nguyên web này.

Bổ sung một quy tắc truy cập tài nguyên web

Để bổ sung hoặc sửa một quy tắc truy cập tài nguyên web:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
 2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát Web**.
 3. Trong mục **Thiết lập**, hãy nhấp nút **Quy tắc truy cập tài nguyên web**.
 4. Trong cửa sổ mở ra, hãy nhấn vào nút **Thêm**.
Cửa sổ **Quy tắc truy cập tài nguyên web** sẽ được mở ra.
 5. Trong trường **Tên quy tắc**, hãy nhập tên của quy tắc.
 6. Chọn trạng thái **Bật** cho quy tắc truy cập tài nguyên web.
Bạn có thể sử dụng nút bật/tắt để [tắt quy tắc truy cập tài nguyên web](#) bất kỳ lúc nào.
 7. Trong mục **Hành động**, hãy chọn tùy chọn liên quan:
 - **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.
 - **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.
 8. Trong mục **Nội dung của bộ lọc**, hãy chọn bộ lọc nội dung liên quan:
 - **Theo danh mục nội dung**. Bạn có thể kiểm soát quyền truy cập của người dùng vào các tài nguyên web theo [danh mục](#) (ví dụ: danh mục *Mạng xã hội*).
 - **Theo loại dữ liệu**. Bạn có thể kiểm soát quyền truy cập của người dùng vào tài nguyên web dựa trên loại dữ liệu cụ thể của dữ liệu đã xuất bản (ví dụ: *Hình ảnh đồ họa*).
- Để cấu hình bộ lọc nội dung:
- a. Nhấn liên kết **Thiết lập**.
 - b. 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 danh 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 danh mục nội dung và / hoặc kiểu dữ liệu được lựa chọn.
 - c. Quay lại cửa sổ để cấu hình quy tắc truy cập tài nguyên web.
9. Trong mục **Địa chỉ**, hãy chọn bộ lọc địa chỉ tài nguyên web liên quan:
 - **Đến tất cả các địa chỉ**. Kiểm soát Web sẽ không lọc tài nguyên web theo địa chỉ.

- **Đến các địa chỉ được chỉ định.** Kiểm soát Web sẽ chỉ lọc các địa chỉ tài nguyên web trong danh sách. Để tạo một danh sách các địa chỉ tài nguyên web:

- a. Nhấn vào nút **Thêm địa chỉ** hoặc **Thêm nhóm địa chỉ**.
- b. Trong cửa sổ mở ra, hãy tạo danh sách địa chỉ tài nguyên web. Bạn có thể nhập một địa chỉ web hoặc [sử dụng các đại diện](#). Bạn cũng có thể [xuất danh sách địa chỉ tài nguyên web từ tập tin TXT](#).
- c. Quay lại cửa sổ để cấu hình quy tắc truy cập tài nguyên web.

Nếu [Quét các kết nối đã được mã hóa bị tắt](#), bạn chỉ có thể lọc theo tên máy chủ cho giao thức HTTPS.

10. Trong mục **Người dùng**, hãy chọn bộ lọc phù hợp cho người dùng:

- **Cho tất cả người dùng.** Kiểm soát Web sẽ không lọc tài các nguyên web cho người dùng cụ thể.
- **Cho người dùng cá nhân và / hoặc nhóm.** Kiểm soát Web sẽ chỉ lọc các tài nguyên web cho những người dùng cụ thể. Để tạo danh sách người dùng mà bạn muốn áp dụng quy tắc:

- a. Nhấn vào **Thêm**.
- b. Trong cửa sổ mở ra, hãy chọn người dùng hoặc nhóm người dùng mà bạn muốn áp dụng quy tắc truy cập tài nguyên web.
- c. Quay lại cửa sổ để cấu hình quy tắc truy cập tài nguyên web.

11. Trong danh sách thả xuống **Lịch quy tắc**, chọn tên của lịch cần thiết hoặc tạo một lịch mới dựa trên lịch quy tắc được lựa chọn. Để làm điều này:

- a. Nhấn vào **Chỉnh sửa hoặc thêm mới**.
- b. Trong cửa sổ mở ra, hãy nhấn vào nút **Thêm**.
- c. Trong cửa sổ mở ra, hãy nhập tên lịch quy tắc.
- d. Cấu hình lịch truy cập tài nguyên web cho người dùng.
- e. Quay lại cửa sổ để cấu hình quy tắc truy cập tài nguyên web.


12. Lưu các thay đổi của bạn.

Gán ưu tiên cho các quy tắc truy cập tài nguyên web

Mỗi quy tắc có một mức ưu tiên. Quy tắc có vị trí càng cao trên danh sách thì càng có mức ưu tiên cao. Nếu một website đã được thêm vào nhiều quy tắc, Kiểm soát Web sẽ quản lý quyền truy cập website đó dựa trên quy tắc có mức ưu tiên cao nhất. Ví dụ như Kaspersky Endpoint Security có thể xác định một cổng thông tin của doanh nghiệp là một mạng xã hội. Để hạn chế truy cập đến các mạng xã hội và cho phép truy cập cổng thông tin web của doanh nghiệp, hãy tạo hai quy tắc: một quy tắc chặn truy cập dành cho danh mục website "Mạng xã hội" và một quy tắc cho phép truy cập dành cho cổng thông tin web của doanh nghiệp. Quy tắc truy cập dành cho cổng thông tin web của doanh nghiệp phải có mức ưu tiên cao hơn so với quy tắc dành cho mạng xã hội.


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. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát Web**.
3. Trong mục **Thiết lập**, hãy nhấp nút **Quy tắc truy cập tài nguyên web**.
4. Trong cửa sổ mở ra, hãy chọn quy tắc có mức ưu tiên mà bạn muốn thay đổi.
5. Sử dụng các nút **Lên** và **Xuống** để di chuyển quy tắc đến vị trí liên quan trong danh sách quy tắc truy cập tài nguyên web.
6. Lưu các thay đổi của bạn.

Bật và tắt một quy tắc truy cập tài nguyên web

Để bật hoặc tắt một quy tắc truy cập tài nguyên web:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát Web**.
3. Trong mục **Thiết lập**, hãy nhấp nút **Quy tắc truy cập tài nguyên web**.
4. Trong cửa sổ được mở, hãy chọn quy tắc mà bạn muốn bật hoặc tắt.
5. Trong cột **Trạng thái**, thực hiện các thao tác sau:
 - Nếu bạn muốn bật quy tắc, hãy chọn giá trị **Bật**.
 - Nếu bạn muốn tắt quy tắc, hãy chọn giá trị **Tắt**.
6. Lưu các thay đổi của bạn.

Xuất và nhập danh sách địa chỉ web được tin tưởng

Bạn có thể xuất danh sách Quy tắc kiểm soát web ra một tập tin XML. Sau đó, bạn có thể sửa đổi tập tin, ví dụ như thêm một số lượng lớn các địa chỉ cùng loại. Bạn có thể sử dụng chức năng xuất/nhập để sao lưu danh sách Quy tắc kiểm soát web hoặc để chuyển danh sách sang máy chủ khác.

[Cách xuất và nhập danh sách Quy tắc kiểm soát web trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát Web**.
6. Để xuất danh sách Quy tắc kiểm soát web:
 - a. Chọn các quy tắc mà bạn muốn xuất. Để chọn nhiều cổng, hãy sử dụng phím **CTRL** hoặc **SHIFT**. Nếu bạn không chọn quy tắc nào, Kaspersky Endpoint Security sẽ xuất tất cả các quy tắc.
 - b. Nhấn liên kết **Xuất**.
 - c. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin XML mà bạn muốn xuất danh sách các quy tắc vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
 - d. Lưu tập tin.
Kaspersky Endpoint Security sẽ xuất danh sách các quy tắc vào tập tin XML.
7. Để nhập danh sách Quy tắc kiểm soát web:
 - a. Nhấn liên kết **Nhập**.
Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách các quy tắc.
 - b. Mở tập tin.
Nếu máy tính đã có danh sách các quy tắc, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.
8. Lưu các thay đổi của bạn.


[Cách xuất và nhập danh sách Quy tắc kiểm soát web trong Bảng điều khiển web và Bảng điều khiển đám mây](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Kiểm soát bảo mật** → **Kiểm soát web**.
5. Để xuất danh sách các quy tắc, trong mục **Rule List**:
 - a. Chọn các quy tắc mà bạn muốn xuất.
 - b. Nhấn vào **Xuất**.
 - c. Xác nhận rằng bạn chỉ muốn xuất các quy tắc đã chọn hoặc xuất toàn bộ danh sách.
 - d. Lưu tập tin.
Kaspersky Endpoint Security sẽ xuất danh sách các quy tắc vào tập tin XML trong thư mục tải xuống mặc định.
6. Để nhập danh sách quy tắc, trong mục **Rule List**:
 - a. Nhấn liên kết **Nhập**.
Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách các quy tắc.
 - b. Mở tập tin.
Nếu máy tính đã có danh sách các quy tắc, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.
7. Lưu các thay đổi của bạn.

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. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát Web**.
3. Trong mục **Thiết lập**, hãy nhấn liên kết **Chẩn đoán quy tắc**.
Cửa sổ **Chẩn đoán quy tắc** sẽ được mở ra.
4. 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 vào địa chỉ của tài nguyên web vào trường bên dưới.


5. 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.
6. Nếu bạn muốn kiểm tra các quy tắc mà Kaspersky Endpoint Security sử dụng để kiểm soát quyền truy cập các tài nguyên web thuộc các danh mục nội dung và/hoặc danh mục kiểu dữ liệu cụ thể, hãy chọn hộp kiểm **Lọc nội dung** và chọn tùy chọn liên quan trong danh sách thả xuống (**Theo danh mục nội dung, Theo loại dữ liệu** hoặc **Theo danh mục nội dung và loại dữ liệu**).
7. 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.
8. Nhấn vào **Quét**.

Sau khi kiểm tra xong, sẽ có một thông báo kèm 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 báo này được hiển thị ở bên phải của nút **Quét**. 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.

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 nhập hoặc xuất một danh sách các địa chỉ tài nguyên web ra một tập tin:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát Web**.
3. Trong mục **Thiết lập**, hãy nhấp nút **Quy tắc truy cập tài nguyên web**.
4. Chọn quy tắc có danh sách địa chỉ tài nguyên web mà bạn muốn xuất hoặc nhập.
5. Để xuất danh sách địa chỉ web được tin tưởng, hãy thực hiện như sau trong mục **Địa chỉ**:
 - a. Chọn các địa chỉ mà bạn muốn xuất.
Nếu bạn không chọn địa chỉ nào, Kaspersky Endpoint Security sẽ xuất tất cả các địa chỉ.
 - b. Nhấn vào **Xuất**.
 - c. Trong cửa sổ mở ra, hãy nhập tên của tập tin TXT mà bạn muốn xuất danh sách địa chỉ tài nguyên web vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
 - d. Lưu tập tin.
Kaspersky Endpoint Security sẽ xuất danh sách địa chỉ tài nguyên web vào một tập tin TXT.
6. Để nhập danh sách tài nguyên web, hãy thực hiện như sau trong mục **Địa chỉ**:

a. Nhấn **Nhập**.

Trong cửa sổ mở ra, hãy chọn tập tin TXT mà bạn muốn nhập danh sách tài nguyên web.

b. Mở tập tin.

Nếu máy tính đã có danh sách địa chỉ, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin TXT.




7. Lưu các thay đổi của bạn.

Giám sát hoạt động truy cập Internet của người dùng

Kaspersky Endpoint Security cho phép bạn lưu ký dữ liệu về lượt truy cập của người dùng vào mọi website, bao gồm các website được cho phép. Tính năng này cho phép bạn lấy toàn bộ lịch sử của các lượt xem trên trình duyệt. Kaspersky Endpoint Security sẽ gửi các sự kiện hoạt động của người dùng đến Kaspersky Security Center, đến [nhật ký cục bộ của Kaspersky Endpoint Security](#), và đến nhật ký Sự kiện của Windows. Để nhận các sự kiện trong Kaspersky Security Center, bạn cần cấu hình thiết lập của các sự kiện trong chính sách trong Bảng điều khiển quản trị hoặc Bảng điều khiển web. Bạn cũng có thể cấu hình truyền tải các sự kiện Kiểm soát Web bằng email và hiển thị các thông báo trên màn hình trên máy tính của người dùng.

Các trình duyệt hỗ trợ chức năng giám sát: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. Chức năng giám hoạt động của người dùng không hoạt động trong các trình duyệt khác.


Kaspersky Endpoint Security sẽ tạo các sự kiện hoạt động truy cập Internet sau của người dùng:

- Chặn website (trạng thái *Sự kiện rất quan trọng* .
- Truy cập vào một trang web không được khuyến nghị (trạng thái *Cảnh báo* .
- Truy cập vào một website được cho phép (trạng thái *Thông báo thông tin* .

Trước khi bật giám sát hoạt động Internet của người dùng, bạn phải thực hiện những việc sau:


- Chèn một mã tương tác trang web vào lưu lượng web (xem hướng dẫn bên dưới). Mã này cho phép đăng ký các sự kiện Kiểm soát Web.
- Để giám sát lưu lượng HTTPS, bạn cần [bật quét kết nối được mã hóa](#).

Để chèn mã tương tác trang web vào lưu lượng web:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Thiết lập mạng**.
3. Trong mục **Xử lý lưu lượng**, hãy chọn hộp kiểm **Chèn mã vào lưu lượng web để tương tác với các trang web**.
4. Lưu các thay đổi của bạn.

Kết quả là Kaspersky Endpoint Security sẽ chèn một mã tương tác trang web vào lưu lượng web. Mã này cho phép đăng ký các sự kiện Kiểm soát Web cho nhật ký sự kiện ứng dụng, nhật ký sự kiện HĐH và [báo cáo](#).

Để cấu hình lưu ký các sự kiện Kiểm soát Web trên máy tính của người dùng:


1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Giao diện**.
3. Trong mục **Thông báo**, hãy nhấn nút **Thiết lập thông báo**.
4. Trong cửa sổ mở ra, hãy chọn mục **Kiểm soát Web**.
Thao tác này sẽ mở bảng sự kiện Kiểm soát Web và các phương thức thông báo.
5. Cấu hình phương thức thông báo cho từng sự kiện: **Lưu trong báo cáo cục bộ** hoặc **Lưu trong nhật ký sự kiện của Windows**.
Để lưu ký các sự kiện truy cập website, bạn cũng cần cấu hình Kiểm soát Web (xem các hướng dẫn bên dưới).
Trong bảng sự kiện này, bạn cũng có thể bật một thông báo trên màn hình và một thông báo qua email. Để gửi thông báo qua email, bạn cần cấu hình thiết lập máy chủ SMTP. Để biết thêm chi tiết về việc gửi thông báo qua email, vui lòng tham khảo [Trợ giúp của Kaspersky Security Center](#).
6. Lưu các thay đổi của bạn.

Kết quả là Kaspersky Endpoint Security bắt đầu lưu ký các sự kiện truy cập Internet của người dùng.

Kiểm soát Web sẽ gửi các sự kiện hoạt động của người dùng đến Kaspersky Security Center như sau:

- Nếu bạn đang sử dụng Kaspersky Security Center, thành phần Kiểm soát Web sẽ gửi các sự kiện cho tất cả các đối tượng tạo nên trang web. Vì lý do này, nhiều sự kiện có thể được tạo khi một trang web bị chặn. Ví dụ: khi chặn trang web <http://www.example.com>, Kaspersky Endpoint Security có thể chuyển tiếp các sự kiện đối với các đối tượng sau: <http://www.example.com>, <http://www.example.com/icon.ico>, <http://www.example.com/file.js>, v.v.
- Nếu bạn đang sử dụng Bảng điều khiển đám mây Kaspersky Security Center, thành phần Kiểm soát Web sẽ nhóm các sự kiện và chỉ gửi giao thức và tên miền của website. Ví dụ: nếu một người dùng truy cập các trang web không được khuyến nghị <http://www.example.com/main>, <http://www.example.com/contact> và <http://www.example.com/gallery>, Kaspersky Endpoint Security sẽ chỉ gửi một sự kiện với đối tượng <http://www.example.com>.

Để bật lưu ký các sự kiện đối với các website được cho phép:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát Web**.
3. Trong mục **Bổ sung**, hãy nhấn nút **Thiết lập nâng cao**.
4. Trong cửa sổ mở ra, hãy chọn hộp kiểm **Ghi lại việc mở ra các trang được cho phép**.
5. Lưu các thay đổi của bạn.

Kết quả là bạn sẽ xem được toàn bộ lịch sử của trình duyệt.

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 báo cảnh báo nếu tùy chọn **Cảnh báo** được chọn trong thiết lập 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 báo để báo rằng một tài nguyên web sẽ bị chặn nếu tùy chọn **Chặn** được chọn trong thiết lập 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. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát Web**.
3. Trong mục **Mẫu**, hãy cấu hình các mẫu cho thông báo Kiểm soát Web:
 - **Cảnh báo** Trường nhập liệu này bao gồm một mẫu tin nhắn sẽ được hiển thị nếu một quy tắc cảnh báo về nỗ lực truy cập một tài nguyên web không mong muốn được kích hoạt.
 - **Tin nhắn về hoạt động chặn** Trường nhập liệu này chứa mẫu tin nhắn sẽ được hiển thị nếu một quy tắc chặn truy cập đến một tài nguyên web được kích hoạt.
 - **Thông điệp đến quản trị viên** Mẫu tin nhắn được gửi đến quản trị viên mạng LAN nếu người dùng cho rằng việc chặn là do nhầm lẫn. Sau khi người dùng yêu cầu cung cấp quyền truy cập, Kaspersky Endpoint Security sẽ gửi một sự kiện đến Kaspersky Security Center: **Thông báo chặn truy cập trang web gửi đến quản trị viên**. Phần mô tả sự kiện chứa một thông báo cho quản trị viên với các biến được thay thế. Bạn có thể xem các sự kiện này trong bảng điều khiển Kaspersky Security Center bằng cách sử dụng lựa chọn sự kiện được định sẵn **User requests**. Nếu tổ chức của bạn chưa triển khai Kaspersky Security Center hoặc không có kết nối với Máy chủ quản trị thì ứng dụng sẽ gửi một thông báo cho quản trị viên tới địa chỉ email được chỉ định.
4. Lưu các thay đổi của bạn.

Sửa mật 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 tên đại diện 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`.

2. Một chuỗi các ký tự `*` (được gọi là *tên miền đại diện*) cho phép bạn chọn tất cả các tên miền của một địa chỉ. Tên miền đại diện `*.` sẽ đại diện cho bất kỳ tên miền, tên miền con hoặc một dòng trống.

Ví dụ: tên đại diện `*.example.com` sẽ đại diện cho các địa chỉ sau:

- `http://pictures.example.com`. Tên miền đại diện `*.` sẽ đại diện cho `hình ảnh`.
- `http://user.pictures.example.com`. Tên miền đại diện `*.` sẽ đại diện cho `hình ảnh` và `người dùng`.
- `http://example.com`. Tên miền đại diện `*.` được hiểu là một dòng trống.

3. Chuỗi ký tự `www.` ở đầu mặt nạ địa chỉ được diễn giải như một chuỗi `*.`

Ví dụ: tên đại diện địa chỉ `www.example.com` được coi là `*.example.com`. Tên đại diện này bao gồm các địa chỉ `www2.example.com` và `www.pictures.example.com`.

4. 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 `*.`

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: tên đại diện địa chỉ `http://www.example.com` bao gồm các địa chỉ như `http://www.example.com/abc`, trong đó `a`, `b`, và `c` là các ký tự bất kỳ.

6. Nếu một tên đại diện địa chỉ kết thúc với ký tự `/`, nội dung của tên đại diện 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: tên đại diện địa chỉ `example.com` 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: tên đại diện 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.	Địa chỉ đại diện	Địa chỉ tài nguyên web cần kiểm chứng	Địa chỉ này có được bao gồm trong mặt nạ địa chỉ không	Bình luận
1	*.example.com	http://www.123example.com	Không	Xem quy tắc 1.
2	*.example.com	http://www.123.example.com	Có	Xem quy tắc 2.
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 3, 2, 1.
7	www.example.com	https://www.example.com	Có	Xem các quy tắc 3, 2, 1.
8	http://www.*.example.com	http://123.example.com	Có	Xem các quy tắc 3, 4, 1.
9	www.example.com	http://www.example.com/abc	Có	Xem các quy tắc 3, 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.

Di chuyển quy tắc truy cập tài nguyên web từ phiên bản cũ của ứng dụng

Khi Kaspersky Endpoint Security 10 Service Pack 2 cho Windows hoặc một phiên bản cũ của ứng dụng được nâng cấp lên Kaspersky Endpoint Security cho Windows 11.9.0, quy tắc truy cập tài nguyên web dựa trên danh mục nội dung tài nguyên web sẽ được di chuyển như sau:

- Các quy tắc truy cập tài nguyên web dựa trên một hoặc nhiều danh mục nội dung tài nguyên web từ danh sách "Trò chuyện và diễn đàn", "Thư điện tử trên web" và "Mạng xã hội" sẽ được di chuyển đến danh mục nội dung tài nguyên web "Giao tiếp trên Internet".
- Các quy tắc truy cập tài nguyên web dựa trên một hoặc nhiều danh mục nội dung tài nguyên web từ danh sách "Cửa hàng điện tử" và "Hệ thống thanh toán" sẽ được di chuyển đến danh mục nội dung tài nguyên web "Cửa hàng trực tuyến, ngân hàng, hệ thống thanh toán".
- Các quy tắc truy cập tài nguyên web dựa trên danh mục nội dung tài nguyên web "Đánh bạc" sẽ được di chuyển đến danh mục nội dung "Đánh bạc, xổ số, rút thăm".
- Các quy tắc truy cập tài nguyên web dựa trên danh mục nội dung tài nguyên web "Trò chơi trên trình duyệt" sẽ được di chuyển đến danh mục nội dung "Trò chơi máy tính".
- Các quy tắc truy cập tài nguyên web dựa trên các danh mục nội dung tài nguyên web không được liệt kê trong danh sách trên sẽ được di chuyển mà không thay đổi gì.

Kiểm soát Thiết bị

Kiểm soát thiết bị quản lý quyền truy cập của người dùng đến các thiết bị được cài đặt trên máy tính hoặc kết nối với máy tính (ví dụ, ổ cứng, camera, hoặc mô-đun Wi-Fi). Việc này cho phép bạn bảo vệ máy tính khỏi bị nhiễm độc khi các thiết bị đó được kết nối, và ngăn thất thoát hoặc rò rỉ dữ liệu.

Các cấp truy cập thiết bị

Kiểm soát thiết bị kiểm soát quyền truy cập ở các cấp độ sau:

- **Loại thiết bị.** Ví dụ, máy in, ổ đĩa di động và ổ CD/DVD.
Bạn có thể cấu hình quyền truy cập thiết bị như sau:
 - Cho phép – ✓.
 - Chặn – ✗.
 - Tùy thuộc vào bus kết nối (ngoại trừ Wi-Fi) – 🌐.
 - Chặn với ngoại lệ (chỉ mạng Wi-Fi) – 🌐.
- **Bus kết nối.** Một *bus kết nối* là một giao diện được sử dụng để kết nối các thiết bị đến máy tính (ví dụ: USB hoặc FireWire). Do đó, bạn có thể hạn chế kết nối của tất cả các thiết bị, ví dụ như qua USB.

Bạn có thể cấu hình quyền truy cập thiết bị như sau:

- Cho phép – ✓.
- Chặn – ✗.
- **Thiết bị được tin tưởng.** *Thiết bị được tin tưởng* là các thiết bị mà những người dùng được quy định trong thiết lập thiết bị được tin tưởng có thể truy cập vào bất cứ lúc nào.

Bạn có thể bổ sung các thiết bị được tin tưởng dựa trên dữ liệu sau:

- **Thiết bị bằng ID.** Mỗi thiết bị có một mã định danh duy nhất (ID phần cứng hay HWID). Bạn có thể xem ID trong thuộc tính thiết bị bằng cách sử dụng công cụ hệ điều hành. ID thiết bị mẫu: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Thêm thiết bị theo ID là một cách thuận tiện nếu bạn muốn thêm một số thiết bị cụ thể.
- **Thiết bị bằng model.** Mỗi thiết bị có một ID nhà cung cấp (VID) và một ID sản phẩm (PID). Bạn có thể xem ID trong thuộc tính thiết bị bằng cách sử dụng công cụ hệ điều hành. Mẫu để nhập VID và PID: `VID_1234&PID_5678`. Thêm thiết bị theo model là cách thuận tiện nếu bạn sử dụng các thiết bị thuộc một model nhất định trong tổ chức của mình. Bằng cách này, bạn có thể thêm tất cả các thiết bị thuộc model này.
- **Thiết bị bằng ID đại diện.** Nếu bạn đang sử dụng nhiều thiết bị có ID tương tự, bạn có thể thêm thiết bị vào danh sách được tin tưởng bằng cách sử dụng tên đại diện. Ký tự `*` sẽ thay thế bất kỳ bộ ký tự nào. Kaspersky Endpoint Security không hỗ trợ ký tự `?` khi nhập tên đại diện. Ví dụ: `WDC_C*`.
- **Thiết bị theo model đại diện.** Nếu bạn đang sử dụng nhiều thiết bị có VID hoặc PID tương tự (ví dụ: các thiết bị của cùng một nhà sản xuất), bạn có thể thêm thiết bị vào danh sách được tin tưởng bằng cách sử dụng tên đại diện. Ký tự `*` sẽ thay thế bất kỳ bộ ký tự nào. Kaspersky Endpoint Security không hỗ trợ ký tự `?` khi nhập tên đại diện. Ví dụ: `VID_05AC & PID_*`.

Kiểm soát thiết bị điều chỉnh quyền truy cập của người dùng đến các thiết bị thông qua các [quy tắc truy cập](#). Kiểm soát thiết bị cũng cho phép bạn lưu các sự kiện kết nối/ngắt kết nối thiết bị. Để lưu các sự kiện, bạn cần cấu hình việc đăng ký sự kiện trong một chính sách.

Nếu quyền truy cập một thiết bị tùy thuộc vào bus kết nối (trạng thái 🚫), Kaspersky Endpoint Security sẽ không lưu các sự kiện kết nối/ngắt kết nối thiết bị. Để cho phép Kaspersky Endpoint Security lưu các sự kiện kết nối/ngắt kết nối thiết bị, hãy cho phép truy cập đến loại thiết bị tương ứng (trạng thái ✅) hoặc thêm thiết bị vào danh sách tin tưởng.

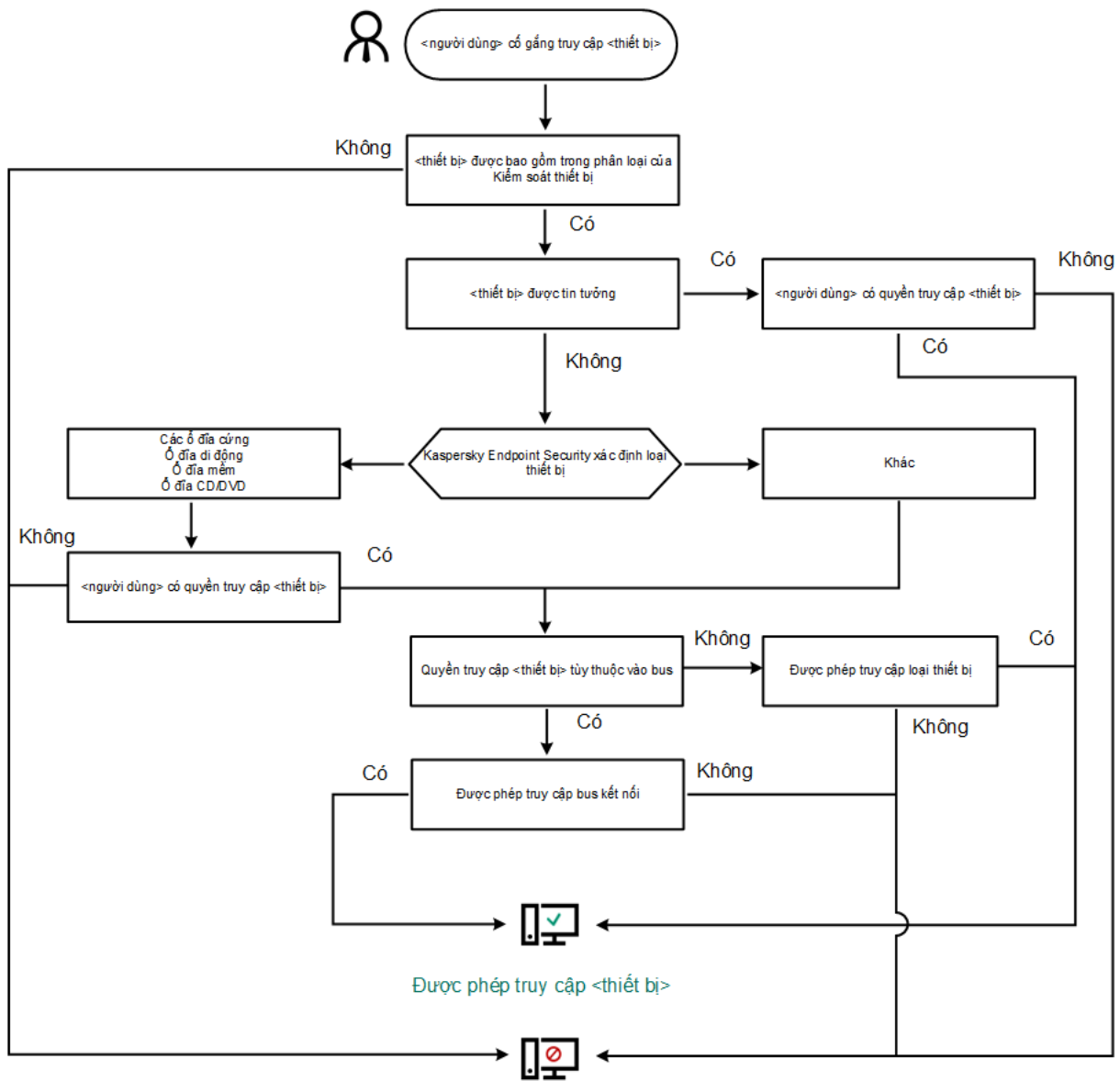
Khi một thiết bị bị chặn bởi Kiểm soát thiết bị được kết nối đến máy tính, Kaspersky Endpoint Security sẽ chặn quyền truy cập và hiển thị một thông báo (xem hình dưới đây).



Thông báo Kiểm soát thiết bị

Thuật toán vận hành Kiểm soát thiết bị

Kaspersky Endpoint Security sẽ đưa ra quyết định về việc cho phép truy cập đến một thiết bị hay không, sau khi người dùng kết nối thiết bị đến máy tính (xem hình bên dưới).



Truy cập vào <thiết bị> bị chặn

Thuật toán vận hành Kiểm soát thiết bị

Nếu một thiết bị được kết nối và được cho phép truy cập, bạn có thể chỉnh sửa quy tắc truy cập và chặn quyền truy cập. Trong trường hợp này, lần tới, khi có người cố truy cập thiết bị (như xem cây thư mục hoặc thực hiện hoạt động đọc hay ghi) thì Kaspersky Endpoint Security sẽ chặn quyền truy cập. 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](#).

Bật và tắt Kiểm soát thiết bị

Theo mặc định, Kiểm soát Thiết bị sẽ được bật.

Để bật hoặc tắt Kiểm soát thiết bị:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .

2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thiết bị**.

3. Sử dụng nút bật/tắt **Kiểm soát thiết bị** để bật hoặc tắt thành phần.

4. Lưu các thay đổi của bạn.

Kết quả là nếu thành phần Kiểm soát thiết bị được bật, ứng dụng sẽ chuyển tiếp thông tin về các thiết bị được kết nối tới Kaspersky Security Center. Bạn có thể xem danh sách các thiết bị được kết nối trong Kaspersky Security Center, trong thư mục **Nâng cao** → **Lưu trữ** → **Phần cứng**.

Thông tin về quy tắc truy cập

Quy tắc truy cập bao gồm một nhóm thiết lập quyết định người dùng nào có thể truy cập các thiết bị được cài đặt hoặc kết nối với máy tính. Bạn không thể thêm một thiết bị nằm ngoài phân loại của Kiểm soát thiết bị. Quyền truy cập đến các thiết bị đó được cho phép đối với tất cả người dùng.

Quy tắc truy cập thiết bị

Nhóm thiết lập cho một quy tắc truy cập khác nhau tùy thuộc vào loại thiết bị (xem bảng dưới đây).

Thiết lập quy tắc truy cập



Thiết bị	Kiểm soát truy cập	Lịch truy cập một thiết bị	Gán người dùng và/hoặc nhóm người dùng	Ưu tiên	Quyền đọc/ghi
Các ổ đĩa cứng	✓	✓	✓	✓	✓
Ổ đĩa di động	✓	✓	✓	✓	✓
Các máy in	✓	-	-	-	-
Ổ đĩa mềm	✓	✓	✓	✓	✓
Ổ đĩa CD/DVD	✓	✓	✓	✓	✓
Các Modem	✓	-	-	-	-
Thiết bị băng từ	✓	-	-	-	-
Thiết bị đa chức năng	✓	-	-	-	-
Đầu đọc thẻ thông minh	✓	-	-	-	-
Thiết bị Windows CE USB ActiveSync	✓	-	-	-	-
Thiết bị mạng gắn ngoài	✓	-	-	-	-
Thiết bị di động (MTP)	✓	✓	✓	✓	✓
Bluetooth	✓	-	-	-	-


Máy ảnh và máy quét	✓	-	-	-	-
---------------------	---	---	---	---	---

Quy tắc truy cập thiết bị di động




Các thiết bị di động chạy Android hoặc iOS được phân loại là thiết bị di động (MTP). Khi một thiết bị di động được kết nối với máy tính, hệ điều hành sẽ quyết định loại thiết bị. Nếu Android Debug Bridge (ADB), iTunes hoặc các ứng dụng tương đương của chúng được cài đặt trên máy tính, hệ điều hành sẽ xác định các thiết bị di động là thiết bị ADB hoặc iTunes. Trong mọi trường hợp, hệ điều hành có thể xác định thiết bị di động đó là thiết bị di động (MTP) để truyền tập tin, thiết bị PTP (camera) để truyền hình ảnh hoặc một thiết bị khác. Loại thiết bị phụ thuộc vào model của thiết bị di động.

Xin lưu ý rằng các điểm cân nhắc đặc biệt sau đây về việc truy cập vào các thiết bị ADB hoặc iTunes:



- Bạn không thể cấu hình lịch truy cập thiết bị. Nếu quyền truy cập vào thiết bị bị hạn chế bởi các quy tắc (chúng có trạng thái ) thì bạn luôn có thể truy cập các thiết bị ADB và iTunes.
- Bạn không thể cấu hình quyền truy cập thiết bị cho người dùng cá nhân hoặc cấu hình quyền truy cập (đọc/ghi). Nếu quyền truy cập vào thiết bị bị hạn chế bởi các quy tắc (chúng có trạng thái ) thì mọi người dùng đều có thể truy cập thiết bị ADB và iTunes với mọi quyền.
- Bạn không thể cấu hình quyền truy cập vào các thiết bị ADB hoặc iTunes được tin tưởng cho người dùng cá nhân. Nếu thiết bị được tin tưởng thì mọi người dùng đều có thể truy cập các thiết bị ADB và iTunes.
- Nếu bạn đã cài đặt ứng dụng ADB hoặc iTunes sau khi kết nối thiết bị với máy tính, ID duy nhất của thiết bị có thể bị đặt lại. Điều này có nghĩa là Kaspersky Endpoint Security sẽ xác định thiết bị này là một thiết bị mới. Nếu một thiết bị được tin tưởng, hãy thêm thiết bị đó vào danh sách được tin tưởng lần nữa.

Theo mặc định, các quy tắc truy cập cho phép tất cả người dùng toàn quyền truy cập đến các thiết bị vào mọi thời điểm, nếu quyền truy cập đến các bus kết nối của loại thiết bị tương ứng được cho phép (trạng thái )

Các quy tắc truy cập cho mạng Wi-Fi

Một quy tắc truy cập mạng Wi-Fi quyết định liệu việc sử dụng mạng Wi-Fi là được cho phép (trạng thái ) hay bị cấm (trạng thái ) . Bạn có thể thêm một *mạng Wi-Fi được tin tưởng* (trạng thái ) vào một quy tắc. Việc sử dụng mạng Wi-Fi được tin tưởng sẽ được cho phép mà không có giới hạn. Theo mặc định, quy tắc truy cập mạng Wi-Fi cho phép truy cập đến bất kỳ mạng Wi-Fi nào.


Quy tắc truy cập bus kết nối

Quy tắc truy cập bus kết nối quyết định liệu việc kết nối các thiết bị là được cho phép (trạng thái ) hay bị cấm (trạng thái ) . 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.

Sửa đổi một quy tắc truy cập thiết bị

Một *quy tắc truy cập thiết bị* là một nhóm thiết lập quyết định cách người dùng có thể truy cập các thiết bị được lắp vào hoặc kết nối với máy tính. Các thiết lập này bao gồm quyền truy cập một thiết bị cụ thể, lịch truy cập và quyền đọc hoặc ghi.


Để sửa đổi một quy tắc truy cập thiết bị:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thiết bị**.
3. Trong mục **Thiết lập truy cập**, hãy nhấn nút **Các thiết bị và mạng Wi-Fi**.
Cửa sổ được mở sẽ hiển thị các quy tắc truy cập cho tất cả các thiết bị được thêm vào danh mục thành phần Kiểm soát thiết bị.
4. Trong mục **Truy cập đến các Thiết bị lưu trữ**, hãy chọn quy tắc truy cập mà bạn muốn chỉnh sửa. Mục này chứa các thiết bị có hệ thống tập tin mà bạn có thể cấu hình thiết lập truy cập bổ sung. 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.
 - a. Trong cột **Truy cập**, hãy chọn tùy chọn truy cập thiết bị thích hợp:
 - **Cho phép.**
 - **Chặn.**
 - **Tùy thuộc vào bus kết nối.**
Để chặn hoặc cho phép truy cập vào một thiết bị, hãy [cấu hình quyền truy cập vào bus kết nối](#).
 - **Giới hạn bởi các quy tắc.**
Tùy chọn này cho phép bạn cấu hình quyền người dùng, quyền và lịch truy cập thiết bị.
 - b. Trong mục **Các quyền của người dùng**, hãy nhấn nút **Thêm**.
Thao tác này sẽ mở ra một cửa sổ để thêm quy tắc truy cập thiết bị mới.
 - c. Gán một cấp ưu tiên cho *quy tắc*. Một quy tắc bao gồm các thuộc tính sau: tài khoản người dùng, lịch, quyền (đọc/ghi) và mức ưu tiên.
Một quy tắc có một mức ưu tiên cụ thể. Nếu một người dùng đã được thêm vào nhiều nhóm, Kaspersky Endpoint Security sẽ điều chỉnh quyền truy cập của thiết bị dựa trên quy tắc có mức ưu tiên cao nhất. Kaspersky Endpoint Security cho phép gán mức độ ưu tiên từ 0 đến 10.000. Giá trị này càng cao thì mức độ ưu tiên càng cao. Nói cách khác, nhập giá trị 0 có nghĩa là mức độ ưu tiên thấp nhất.
Ví dụ: bạn có thể cấp quyền chỉ đọc cho nhóm Mọi người và cấp quyền đọc/ghi cho nhóm quản trị viên. Để làm như vậy, hãy gán mức ưu tiên bằng 1 cho nhóm quản trị viên và gán mức ưu tiên bằng 0 cho nhóm Mọi người.
Một quy tắc chặn được ưu tiên hơn một quy tắc cho phép. Nói cách khác, nếu một người dùng đã được thêm vào nhiều nhóm và mức ưu tiên của tất cả các quy tắc đều bằng nhau, Kaspersky Endpoint Security sẽ điều chỉnh quyền truy cập của thiết bị dựa trên bất kỳ quy tắc chặn nào hiện có.
 - d. Chọn trạng thái **Đã bật** cho quy tắc truy cập thiết bị.
 - e. Cấu hình quyền truy cập thiết bị của người dùng: đọc và/hoặc ghi.
 - f. Chọn người dùng hoặc nhóm người dùng mà bạn muốn áp dụng quy tắc truy cập thiết bị.

- g. Cấu hình lịch truy cập thiết bị cho người dùng.
- h. Nhấn vào nút **Thêm**.
5. Trong mục **Truy cập đến các Thiết bị bên ngoài**, hãy chọn quy tắc và cấu hình quyền truy cập: **Cho phép**, **Chặn** hoặc **Tùy thuộc vào bus kết nối**. Nếu cần, [cấu quyền truy cập vào bus kết nối](#).
6. Trong mục **Truy cập vào các mạng Wi-Fi**, hãy nhấn liên kết **Wi-Fi** và cấu hình quyền truy cập: **Cho phép**, **Chặn** hoặc **Chặn với ngoại lệ**. Nếu cần, [hãy thêm các mạng Wi-Fi vào danh sách được tin tưởng](#).
7. Lưu các thay đổi của bạn.

Sửa một quy tắc truy cập bus kết nối


Để sửa một quy tắc truy cập bus kết nối:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thiết bị**.
3. Trong mục **Thiết lập truy cập**, hãy nhấn nút **Các Bus kết nối**.
Cửa sổ được mở sẽ hiển thị các quy tắc truy cập cho tất cả các bus kết nối được thêm vào danh mục thành phần Kiểm soát thiết bị.
4. Chọn quy tắc truy cập mà bạn muốn sửa.
5. Trong cột **Truy cập**, hãy chọn cho phép hoặc không cho phép truy cập vào bus kết nối: **Cho phép** hoặc **Chặn**.
6. Lưu các thay đổi của bạn.

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. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thiết bị**.
3. Trong mục **Thiết lập truy cập**, hãy nhấn nút **Các thiết bị và mạng Wi-Fi**.
Cửa sổ được mở sẽ hiển thị các quy tắc truy cập cho tất cả các thiết bị được thêm vào danh mục thành phần Kiểm soát thiết bị.
4. Trong mục **Truy cập vào các mạng Wi-Fi**, hãy nhấn liên kết **Wi-Fi**.

Cửa sổ được mở ra sẽ hiển thị các quy tắc truy cập mạng Wi-Fi.

5. Trong mục **Truy cập**, hãy chọn **Chặn với ngoại lệ**.
6. Trong mục **Trusted Wi-Fi networks**, hãy nhấn nút **Add**.
7. Trong cửa sổ mở ra, hãy thực hiện như sau:
 - a. Trong trường **Tên mạng**, nhập tên của mạng Wi-Fi mà bạn muốn thêm vào danh sách tin tưởng.
 - b. 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.
 - c. 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.
 - d. 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.

8. Lưu các thay đổi của bạn.


Giám sát việc sử dụng ổ đĩa di động

Giám sát việc sử dụng ổ đĩa di động bao gồm:

- Giám sát hoạt động trên các tập tin trên ổ đĩa di động.
- Giám sát kết nối và ngắt kết nối của các ổ đĩa di động được tin tưởng.

Kaspersky Endpoint Security cho phép giám sát kết nối và ngắt kết nối của tất cả các thiết bị được tin tưởng và không chỉ ổ đĩa di động. Bạn có thể bật tính năng ghi nhật ký sự kiện trong [thiết lập thông báo](#) cho thành phần Kiểm soát thiết bị. Các sự kiện có mức độ bảo mật *Thông báo thông tin*.

Để cho phép giám sát việc sử dụng ổ đĩa di động:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thiết bị**.
3. Trong mục **Thiết lập truy cập**, hãy nhấn nút **Các thiết bị và mạng Wi-Fi**.

Cửa sổ được mở sẽ hiển thị các quy tắc truy cập cho tất cả các thiết bị được thêm vào danh mục thành phần Kiểm soát thiết bị.
4. Trong mục **Truy cập đến các thiết bị lưu trữ**, hãy chọn **Ổ đĩa di động**.
5. Trong cửa sổ mở ra, hãy chọn thẻ **Nhật ký**.
6. Bật nút bật/tắt **Nhật ký**.
7. Trong mục **Thao tác với tập tin**, hãy chọn các thao tác bạn muốn theo dõi: **Ghi, Xóa**.

8. Trong mục **Lọc theo định dạng tập tin**, hãy chọn định dạng tập tin có các hoạt động liên quan sẽ được thành phần Kiểm soát thiết bị lưu nhật ký.
9. Chọn người dùng hoặc nhóm người dùng có hoạt động sử dụng ổ đĩa di động mà bạn muốn giám sát.
10. Lưu các thay đổi của bạn.

Kết quả là khi người dùng ghi vào tập tin có trên ổ đĩa di động hoặc xóa tập tin khỏi ổ đĩa di động, Kaspersky Endpoint Security sẽ lưu thông tin về các hoạt động đó vào nhật ký sự kiện và gửi các sự kiện đến Kaspersky Security Center. 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 **Administration Server** trên thẻ **Các 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.

Thay đổi thời gian lưu vào bộ nhớ đệm

Thành phần Kiểm soát thiết bị ghi lại các sự kiện liên quan đến các thiết bị được giám sát, chẳng hạn như việc kết nối và ngắt kết nối của thiết bị, đọc tập tin từ thiết bị, ghi tập tin vào thiết bị và các sự kiện khác. Sau đó, thành phần Kiểm soát thiết bị sẽ cho phép hoặc chặn hành động theo thiết lập của Kaspersky Endpoint Security.

Thành phần Kiểm soát thiết bị sẽ lưu thông tin về các sự kiện trong một khoảng thời gian cụ thể được gọi là *thời gian lưu vào bộ nhớ đệm*. Nếu thông tin về một sự kiện được lưu vào bộ nhớ đệm và sự kiện này lặp lại thì Kaspersky Endpoint Security không cần được thông báo về sự kiện đó hoặc không cần hiển thị một lời nhắc khác để cấp quyền truy cập cho hành động tương ứng, chẳng hạn như kết nối thiết bị. Điều này tạo sự thuận tiện hơn khi làm việc với thiết bị.

Một sự kiện được coi là một sự kiện trùng lặp nếu tất cả các thiết lập sự kiện sau khớp với bản ghi trong bộ nhớ đệm:

- ID Thiết bị
- SID của tài khoản người dùng đang cố gắng truy cập
- Danh mục thiết bị
- Hành động được thực hiện với thiết bị
- Quyết định cho phép của ứng dụng đối với hành động này: được phép hay bị từ chối
- Đường dẫn đến tiến trình được sử dụng để thực hiện hành động
- Tập tin đang được truy cập

Trước khi thay đổi thời gian lưu vào bộ nhớ đệm, hãy [tắt tính năng Tự bảo vệ cho Kaspersky Endpoint Security](#). Sau khi thay đổi thời gian lưu vào bộ nhớ đệm, hãy bật Tự bảo vệ.

Để thay đổi thời gian lưu vào bộ nhớ đệm:

1. Mở trình chỉnh sửa registry trên máy tính.
2. Trong trình chỉnh sửa registry, hãy chuyển đến phần sau:

- Đối với hệ điều hành 64-bit:
[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\environment]
- Đối với hệ điều hành 32-bit:
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES\environment]

3. Mở `DeviceControlEventsCachePeriod` để chỉnh sửa.

4. Xác định số phút mà thành phần Kiểm soát thiết bị phải lưu thông tin về một sự kiện trước khi thông tin này bị xóa.

Hành động với các thiết bị được tin tưởng

Thiết bị được tin tưởng là các thiết bị mà những người dùng được quy định trong thiết lập thiết bị được tin tưởng có thể truy cập vào bất cứ lúc nào.

Để làm việc với các thiết bị được tin tưởng, bạn có thể cấp quyền truy cập cho một người dùng cá nhân, cho một nhóm người dùng hoặc cho tất cả người dùng của tổ chức.

Ví dụ: nếu tổ chức của bạn không cho phép sử dụng ổ đĩa di động nhưng quản trị viên lại sử dụng ổ đĩa di động trong công việc của họ, bạn chỉ có thể cho phép một nhóm quản trị viên sử dụng ổ đĩa di động. Để làm như vậy, hãy thêm ổ đĩa di động vào danh sách thiết bị được tin tưởng và cấu hình quyền truy cập của người dùng.

Bạn không nên thêm quá 1000 thiết bị được tin tưởng vì làm vậy có thể khiến hệ thống không ổn định.

Kaspersky Endpoint Security cho phép bạn thêm một thiết bị vào danh sách thiết bị được tin tưởng theo các cách sau:

- Nếu Kaspersky Security Center không được triển khai trong tổ chức của bạn thì bạn có thể kết nối thiết bị với máy tính và [thêm máy tính đó vào danh sách thiết bị được tin tưởng trong phần cài đặt của ứng dụng](#). Để phân phối danh sách các thiết bị được tin tưởng cho tất cả các máy tính trong tổ chức, bạn có thể bật hợp nhất các danh sách thiết bị được tin tưởng trong chính sách hoặc sử dụng [quy trình xuất / nhập](#).
- Nếu Kaspersky Security Center được triển khai trong tổ chức, bạn có thể phát hiện tất cả các thiết bị được kết nối từ xa và [tạo danh sách các thiết bị được tin tưởng trong chính sách](#). Danh sách các thiết bị được tin tưởng sẽ khả dụng trên tất cả các máy tính áp dụng chính sách.

Kaspersky Endpoint Security cho phép kiểm soát việc sử dụng các thiết bị được tin tưởng (kết nối và ngắt kết nối). Bạn có thể bật tính năng ghi nhật ký sự kiện trong [thiết lập thông báo](#) cho thành phần Kiểm soát thiết bị. Các sự kiện có mức độ bảo mật *Thông tin*.

Kaspersky Endpoint Security có các giới hạn sau khi làm việc với các thiết bị được tin tưởng:

- Tiện ích quản trị Kaspersky Endpoint Security phiên bản 11.0.0–11.2.0 không thể hoạt động với danh sách các thiết bị được tin tưởng đã được tạo trong Kaspersky Endpoint Security phiên bản 11.3.0 và 11.4.0. Để làm việc với danh sách thiết bị được tin tưởng từ các phiên bản này, tiện ích quản trị phải được nâng cấp lên phiên bản 11.3.0 và 11.4.0 tương ứng.
- Tiện ích quản trị Kaspersky Endpoint Security phiên bản 11.3.0 và 11.4.0 không thể hoạt động với danh sách các thiết bị được tin tưởng đã được tạo trong Kaspersky Endpoint Security phiên bản 11.2.0


trở về trước. Để các phiên bản này hoạt động với danh sách thiết bị được tin tưởng, ứng dụng phải được nâng cấp lên phiên bản 11.3.0 và 11.4.0 tương ứng. Bạn cũng có thể gửi một yêu cầu chứa mô tả tình huống của bạn tới bộ phận Hỗ trợ kỹ thuật thông qua [Kaspersky CompanyAccount](#).

- Để di chuyển danh sách thiết bị được tin tưởng từ Kaspersky Endpoint Security phiên bản 11.2.0 sang phiên bản 11.3.0, hãy gửi yêu cầu chứa mô tả về tình huống của bạn tới bộ phận Hỗ trợ kỹ thuật thông qua [Kaspersky CompanyAccount](#).

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 Mọi người).

Để bổ sung một thiết bị vào danh sách Được Tin tưởng từ giao diện ứng dụng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thiết bị**.
3. Trong mục **Thiết lập truy cập**, hãy nhấn nút **Thiết bị được tin tưởng**.
Thao tác này sẽ mở danh sách các thiết bị được tin tưởng.
4. Nhấn vào **Lựa chọn**.
Thao tác này sẽ mở danh sách các thiết bị được kết nối. Danh sách các thiết bị phụ thuộc vào giá trị được lựa chọn trong danh sách thả xuống **Hiển thị các thiết bị kết nối**.
5. Trong danh sách thiết bị, hãy chọn thiết bị mà bạn muốn thêm vào danh sách được tin tưởng.
6. Trong trường **Bình luận**, bạn có thể cung cấp bất kỳ thông tin liên quan nào về thiết bị được tin tưởng.
7. Chọn người dùng hoặc nhóm người dùng mà bạn muốn cho phép truy cập vào các thiết bị được tin tưởng.
8. Lưu các thay đổi của bạn.

Bổ sung một thiết bị vào danh sách Được Tin tưởng từ Kaspersky Security Center

Kaspersky Security Center sẽ nhận thông tin về các thiết bị nếu Kaspersky Endpoint Security được cài đặt trên máy tính và [Kiểm soát thiết bị được bật](#). Không thể thêm thiết bị vào danh sách được tin tưởng trừ khi thông tin về thiết bị đó có sẵn trong Kaspersky Security Center.

Bạn có thể thêm một thiết bị vào danh sách được tin tưởng theo dữ liệu sau:

- **Thiết bị bằng ID.** Mỗi thiết bị có một mã định danh duy nhất (ID phần cứng hay HWID). Bạn có thể xem ID trong thuộc tính thiết bị bằng cách sử dụng công cụ hệ điều hành. ID thiết bị mẫu: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Thêm thiết bị theo ID là một cách thuận tiện nếu bạn muốn thêm một số thiết bị cụ thể.

- **Thiết bị bằng model.** Mỗi thiết bị có một ID nhà cung cấp (VID) và một ID sản phẩm (PID). Bạn có thể xem ID trong thuộc tính thiết bị bằng cách sử dụng công cụ hệ điều hành. Mẫu để nhập VID và PID: VID_1234&PID_5678. Thêm thiết bị theo model là cách thuận tiện nếu bạn sử dụng các thiết bị thuộc một model nhất định trong tổ chức của mình. Bằng cách này, bạn có thể thêm tất cả các thiết bị thuộc model này.
- **Thiết bị bằng ID đại diện.** Nếu bạn đang sử dụng nhiều thiết bị có ID tương tự, bạn có thể thêm thiết bị vào danh sách được tin tưởng bằng cách sử dụng tên đại diện. Ký tự * sẽ thay thế bất kỳ bộ ký tự nào. Kaspersky Endpoint Security không hỗ trợ ký tự ? khi nhập tên đại diện. Ví dụ: WDC_C*.
- **Thiết bị theo model đại diện.** Nếu bạn đang sử dụng nhiều thiết bị có VID hoặc PID tương tự (ví dụ: các thiết bị của cùng một nhà sản xuất), bạn có thể thêm thiết bị vào danh sách được tin tưởng bằng cách sử dụng tên đại diện. Ký tự * sẽ thay thế bất kỳ bộ ký tự nào. Kaspersky Endpoint Security không hỗ trợ ký tự ? khi nhập tên đại diện. Ví dụ: VID_05AC & PID_ *.

Để thêm thiết bị vào danh sách các thiết bị được tin tưởng:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thiết bị**.
6. Ở phần bên phải của cửa sổ, chọn thẻ **Thiết bị được tin tưởng**.
7. Chọn hộp kiểm **Hợp nhất các giá trị khi kế thừa** nếu bạn muốn tạo một danh sách tổng hợp các thiết bị được tin tưởng cho tất cả các máy tính trong công ty.
Danh sách các thiết bị được tin tưởng trong chính sách cha và chính sách con sẽ được hợp nhất. Các danh sách sẽ được hợp nhất với điều kiện các giá trị hợp nhất khi kế thừa được bật. Thiết bị được tin tưởng từ chính sách cha được hiển thị trong chính sách con ở chế độ chỉ đọc. Không thể thay đổi hay xóa các thiết bị được tin tưởng của chính sách cha.
8. Nhấn vào nút **Thêm** và chọn phương thức để thêm thiết bị vào danh sách được tin tưởng.
9. Để lọc thiết bị, hãy chọn loại thiết bị trong danh sách thả xuống **Loại thiết bị** (ví dụ: **Ổ đĩa di động**).
10. Trong trường **Tên / Model**, hãy nhập ID thiết bị (VID và PID) hoặc tên đại diện, tùy thuộc vào phương pháp thêm được chọn.

Tính năng thêm thiết bị theo tên đại diện model (VID và PID) hoạt động như sau: nếu bạn nhập tên đại diện model không khớp với bất kỳ model nào thì Kaspersky Endpoint Security sẽ kiểm tra xem ID thiết bị (HWID) có khớp với tên đại diện hay không. Kaspersky Endpoint Security chỉ kiểm tra phần ID thiết bị chứa thông tin xác định nhà sản xuất và loại thiết bị (SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000). Nếu tên đại diện model khớp với phần này của ID thiết bị thì các thiết bị khớp với tên đại diện đó sẽ được thêm vào danh sách các thiết bị được tin tưởng trên máy tính. Đồng thời, danh sách các thiết bị trong Kaspersky Security Center vẫn được để trống khi bạn nhấn vào nút **Làm mới**. Để hiển thị đúng danh sách các thiết bị, bạn có thể thêm thiết bị theo tên đại diện ID thiết bị.

11. Để lọc các thiết bị, trong trường **Tên máy tính**, hãy nhập tên máy tính hoặc tên đại diện của máy tính mà thiết bị được kết nối.
Ký tự * sẽ thay thế bất kỳ bộ ký tự nào. Ký tự ? sẽ thay thế bất kỳ một ký tự đơn nào.
12. Nhấn vào nút **Làm mới**.
Bảng này hiển thị danh sách các thiết bị đáp ứng các tiêu chí lọc được xác định.
13. Chọn các hộp kiểm cạnh tên của thiết bị mà bạn muốn thêm vào danh sách các thiết bị được tin tưởng.
14. Trong trường **Bình luận**, hãy nhập mô tả lý do thêm thiết bị vào danh sách được tin tưởng.
15. Nhấn vào nút **Lựa chọn** ở bên phải trường **Cho phép người dùng và / hoặc nhóm người dùng**.
16. Chọn một người dùng hoặc nhóm trong Active Directory và xác nhận lựa chọn của bạn.
Theo mặc định, nhóm mọi người được phép truy cập vào các thiết bị được tin tưởng.
17. Lưu các thay đổi của bạn.

Khi một thiết bị được kết nối, Kaspersky Endpoint Security sẽ kiểm tra danh sách các thiết bị được tin tưởng cho người dùng được cho phép. Nếu thiết bị đó được tin tưởng, Kaspersky Endpoint Security cho phép truy cập vào thiết bị với tất cả các quyền, ngay cả khi quyền truy cập vào loại thiết bị hoặc bus kết nối bị từ chối. Nếu thiết bị không được tin tưởng và quyền truy cập bị từ chối, bạn có thể [yêu cầu quyền truy cập vào thiết bị bị khóa](#).


Xuất và nhập danh sách các thiết bị được tin tưởng

Để phân phối danh sách các thiết bị được tin tưởng cho tất cả các máy tính trong tổ chức, bạn có thể sử dụng quy trình xuất/nhập.

Ví dụ: nếu bạn cần phân phối danh sách các ổ đĩa di động được tin tưởng, bạn cần thực hiện các bước sau:

1. Kết nối tuần tự các ổ đĩa di động với máy tính của bạn.
2. Trong thiết lập Kaspersky Endpoint Security, [thêm các ổ đĩa di động vào danh sách được tin tưởng](#).
Nếu được yêu cầu, hãy cấu hình quyền truy cập của người dùng. Ví dụ: chỉ cho phép các quản trị viên truy cập ổ đĩa di động.
3. Xuất danh sách các thiết bị được tin tưởng trong thiết lập Kaspersky Endpoint Security (xem hướng dẫn bên dưới).
4. Phân phối tập tin danh sách các thiết bị được tin tưởng cho các máy tính khác trong tổ chức của bạn.
Ví dụ: đặt tập tin trong một thư mục chia sẻ.
5. Nhập danh sách các thiết bị được tin tưởng trong thiết lập Kaspersky Endpoint Security trên các máy tính khác trong tổ chức (xem hướng dẫn bên dưới).

Để nhập hoặc xuất danh sách các thiết bị được tin tưởng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thiết bị**.

3. Trong mục **Thiết lập truy cập**, hãy nhấn nút **Thiết bị được tin tưởng**.

Thao tác này sẽ mở danh sách các thiết bị được tin tưởng.

4. Để xuất danh sách các thiết bị được tin tưởng:

a. Chọn các thiết bị được tin tưởng mà bạn muốn xuất.

b. Nhấn vào **Xuất**.

c. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin XML mà bạn muốn xuất danh sách các thiết bị được tin tưởng vào đó rồi chọn thư mục bạn muốn lưu tập tin này.

d. Lưu tập tin.

Kaspersky Endpoint Security sẽ xuất toàn bộ danh sách các thiết bị được tin tưởng vào tập tin XML.

5. Để nhập danh sách các thiết bị được tin tưởng:

a. Trong danh sách thả xuống **Nhập**, hãy chọn hành động có liên quan: **Nhập và thêm vào danh sách hiện tại** hoặc **Nhập và thay thế danh sách hiện tại**.

b. Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách các thiết bị được tin tưởng.

c. Mở tập tin.

Nếu máy tính đã có danh sách các thiết bị được tin tưởng, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.

6. Lưu các thay đổi của bạn.

Khi một thiết bị được kết nối, Kaspersky Endpoint Security sẽ kiểm tra danh sách các thiết bị được tin tưởng cho người dùng được cho phép. Nếu thiết bị đó được tin tưởng, Kaspersky Endpoint Security cho phép truy cập vào thiết bị với tất cả các quyền, ngay cả khi quyền truy cập vào loại thiết bị hoặc bus kết nối bị từ chối.

Nhận truy cập đến một thiết bị bị chặn

Khi cấu hình Kiểm soát thiết bị, bạn có thể vô tình chặn quyền truy cập tới một thiết bị cần thiết cho công việc.

Nếu Kaspersky Security Center không được triển khai trong tổ chức của bạn thì bạn có thể cung cấp quyền truy cập tới một thiết bị trong thiết lập của Kaspersky Endpoint Security. Ví dụ như bạn có thể [thêm thiết bị vào danh sách được tin tưởng](#) hoặc tạm thời [tắt Kiểm soát thiết bị](#).

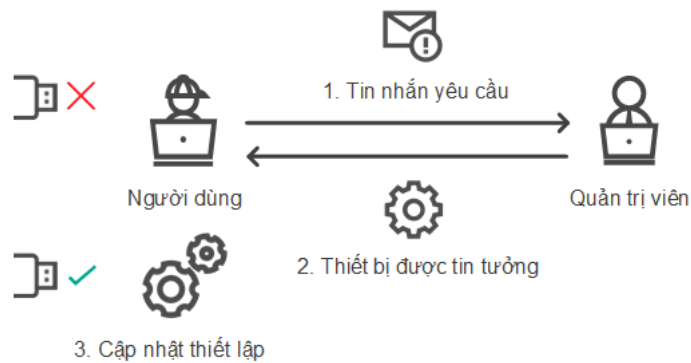
Nếu Kaspersky Security Center được triển khai trong tổ chức của bạn và các máy tính của bạn được áp dụng một chính sách thì bạn có thể cung cấp quyền truy cập tới một thiết bị trong Bảng điều khiển quản trị.

Chế độ trực tuyến để cấp quyền truy cập

Bạn chỉ có thể cấp quyền truy cập tới một thiết bị bị chặn ở chế độ trực tuyến nếu Kaspersky Security Center được triển khai trong tổ chức và máy tính đó đã được áp dụng chính sách. Máy tính đó phải có khả năng thiết lập một kết nối với Máy chủ quản trị.

Cấp quyền truy cập ở chế độ trực tuyến bao gồm các bước sau:

1. Người dùng gửi cho quản trị viên một tin nhắn có chứa yêu cầu truy cập.
2. Quản trị viên sẽ thêm thiết bị vào danh sách được tin tưởng.
Bạn có thể thêm một thiết bị được tin tưởng vào chính sách dành cho nhóm quản trị hoặc trong thiết lập cục bộ của ứng dụng đối với một máy tính cá nhân.
3. Quản trị viên sẽ cập nhật các thiết lập của Kaspersky Endpoint Security trên máy tính của người dùng.



Giản đồ cấp quyền truy cập tới một thiết bị ở chế độ trực tuyến

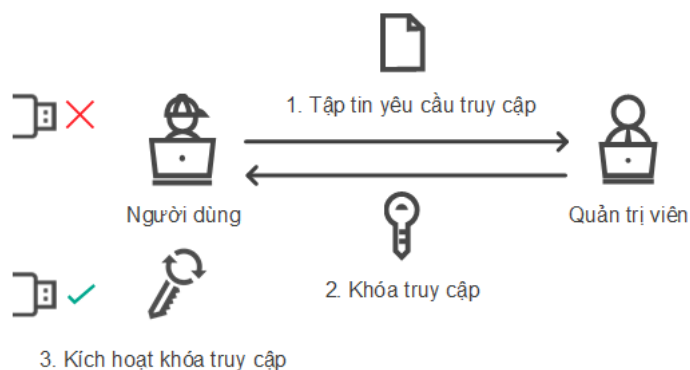
Chế độ ngoại tuyến để cấp quyền truy cập

Bạn chỉ có thể cấp quyền truy cập đến một thiết bị bị chặn ở chế độ ngoại tuyến nếu Kaspersky Security Center được triển khai trong tổ chức và máy tính đó đã được áp dụng chính sách. Trong thiết lập của chính sách, trong phần **Kiểm soát thiết bị**, phải chọn **Cho phép yêu cầu truy cập tạm thời**.

Nếu bạn cần cấp quyền truy cập tạm thời tới một thiết bị bị chặn nhưng bạn không thể [thêm thiết bị đó vào danh sách được tin tưởng](#) thì bạn có thể cấp quyền truy cập tới thiết bị ở chế độ ngoại tuyến. Bằng cách này, bạn có thể cấp quyền truy cập đến một thiết bị bị chặn cho dù máy tính không có quyền truy cập mạng hoặc nếu máy tính nằm ở ngoài mạng doanh nghiệp.

Cấp quyền truy cập ở chế độ ngoại tuyến bao gồm các bước sau:

1. Người dùng tạo một tập tin yêu cầu truy cập và gửi cho quản trị viên.
2. Quản trị viên sẽ tạo một khóa truy cập từ tập tin yêu cầu truy cập và khóa truy cập cho người dùng.
3. Người dùng kích hoạt khóa truy cập.



Giản đồ cấp quyền truy cập tới một thiết bị ở chế độ ngoại tuyến

Chế độ trực tuyến để cấp quyền truy cập

Bạn chỉ có thể cấp quyền truy cập tới một thiết bị bị chặn ở chế độ trực tuyến nếu Kaspersky Security Center được triển khai trong tổ chức và máy tính đó đã được áp dụng chính sách. Máy tính đó phải có khả năng thiết lập một kết nối với Máy chủ quản trị.

Người dùng yêu cầu truy cập đến thiết bị bị chặn như sau:

1. Kết nối thiết bị với máy tính.

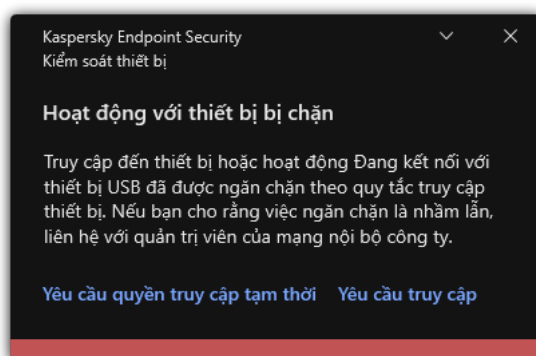
Kaspersky Endpoint Security sẽ hiển thị một thông báo để báo rằng quyền truy cập tới thiết bị đó đã bị chặn (xem hình bên dưới).

2. Nhấn vào liên kết **Yêu cầu truy cập**.

Thao tác này sẽ mở ra cửa sổ kèm một thông báo cho quản trị viên. Thông báo này chứa thông tin về thiết bị bị chặn.

3. Nhấn vào **Gửi**.

Quản trị viên sẽ nhận được thông báo chứa yêu cầu cung cấp quyền truy cập, ví dụ như qua email. Để biết thêm chi tiết về việc xử lý các yêu cầu của người dùng, vui lòng tham khảo [Trợ giúp của Kaspersky Security Center](#). Sau khi [thêm thiết bị vào danh sách được tin tưởng](#) và cập nhật thiết lập của Kaspersky Endpoint Security trên máy tính, người dùng sẽ nhận được quyền truy cập tới thiết bị đó.



Thông báo Kiểm soát thiết bị

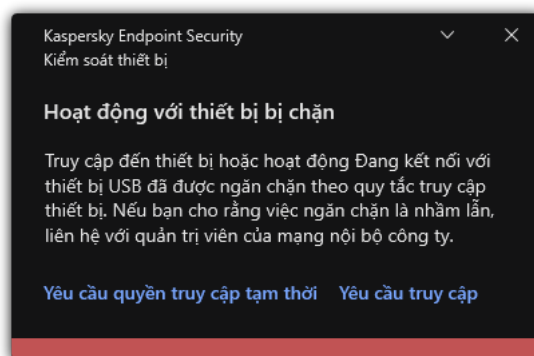
Chế độ ngoại tuyến để cấp quyền truy cập

Bạn chỉ có thể cấp quyền truy cập đến một thiết bị bị chặn ở chế độ ngoại tuyến nếu Kaspersky Security Center được triển khai trong tổ chức và máy tính đó đã được áp dụng chính sách. Trong thiết lập của chính sách, trong phần **Kiểm soát thiết bị**, phải chọn **Cho phép yêu cầu truy cập tạm thời**.

Người dùng yêu cầu truy cập đến thiết bị bị chặn như sau:

1. Kết nối thiết bị với máy tính.
Kaspersky Endpoint Security sẽ hiển thị một thông báo để báo rằng quyền truy cập tới thiết bị đó đã bị chặn (xem hình bên dưới).
2. Nhấn vào liên kết **Yêu cầu quyền truy cập tạm thời**.
Thao tác này sẽ mở cửa sổ chứa danh sách các thiết bị được kết nối.
3. Trong danh sách các thiết bị được kết nối, hãy chọn thiết bị bạn muốn truy cập.
4. Nhấn vào **Tạo tập tin yêu cầu truy cập**.
5. Trong trường **Thời gian truy cập**, quy định khoảng thời gian mà bạn muốn truy cập đến thiết bị.
6. Lưu tập tin vào bộ nhớ của máy tính.

Kết quả là một tập tin yêu cầu truy cập có phần mở rộng *.akey sẽ được tải về bộ nhớ của máy tính. Sử dụng bất kỳ phương thức khả dụng nào để gửi tập tin yêu cầu truy cập đến quản trị viên mạng LAN của doanh nghiệp.



Thông báo Kiểm soát thiết bị

[Cách quản trị viên có thể tạo khóa truy cập cho thiết bị đang bị chặn trong Bảng điều khiển quản trị \(MMC\)](#)


1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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, hãy chọn thẻ **Devices**.
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 đang bị chặn.
5. Trong menu ngữ cảnh của máy tính, chọn mục **Cấp quyền truy cập trong chế độ ngoại tuyến**.
6. Trong cửa sổ mở ra, hãy chọn thẻ **Kiểm soát thiết bị**.
7. Nhấn vào nút **Duyệt** và tải về tập tin yêu cầu truy cập nhận được từ người dùng.
Bạn sẽ thấy thông tin về thiết bị bị chặn mà người dùng đã yêu cầu quyền truy cập đến.
8. Nếu cần, hãy thay đổi giá trị của thiết lập **Thời gian truy cập**.
Theo mặc định, thiết lập **Thời gian truy cập** sẽ lấy giá trị được người dùng đặt khi tạo tập tin yêu cầu truy cập.
9. Chỉ định giá trị của thiết lập **Kích hoạt bằng**.
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.
10. Lưu tập tin khóa truy cập vào bộ nhớ máy tính.

[Cách quản trị viên có thể tạo khóa truy cập cho thiết bị đang bị chặn trong Bảng điều khiển web và Bảng điều khiển đám mây](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Managed devices**.
2. 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 đang bị chặn.
3. Nhấn vào nút dấu chấm lửng () trên danh sách máy tính rồi nhấn vào nút **Grant access to the device in offline mode**.
4. Trong cửa sổ mở ra, hãy chọn mục **Device Control**.
5. Nhấn vào nút **Browse** và tải về tập tin yêu cầu truy cập nhận được từ người dùng.
Bạn sẽ thấy thông tin về thiết bị bị chặn mà người dùng đã yêu cầu quyền truy cập đến.
6. Nếu cần, hãy thay đổi giá trị của thiết lập **Access duration (hours)**.
Theo mặc định, thiết lập **Access duration (hours)** sẽ lấy giá trị được người dùng đặt khi tạo tập tin yêu cầu truy cập.
7. Chỉ định khoảng thời gian khóa truy cập có thể được kích hoạt trên thiết bị.
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.
8. Lưu tập tin khóa truy cập vào bộ nhớ máy tính.

Kết quả là khóa truy cập thiết bị bị chặn sẽ được tải về bộ nhớ máy tính. Một tập tin khóa truy cập có phần mở rộng là *.acode. Sử dụng bất kỳ phương thức khả dụng nào để gửi khóa truy cập thiết bị bị chặn đến người dùng.

Người dùng sẽ kích hoạt khóa truy cập như sau:

1. Trong [cửa sổ chính của ứng dụng](#), hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thiết bị**.
3. Trong mục **Yêu cầu quyền truy cập**, hãy nhấn nút **Yêu cầu truy cập thiết bị**.
4. Trong cửa sổ mở ra, hãy nhấn nút **Kích hoạt khóa truy cập**.
5. Trong cửa sổ mở ra, hãy chọn tập tin có khóa truy cập nhận được từ quản trị viên mạng LAN của doanh nghiệp.
Thao tác này sẽ mở một cửa sổ chứa thông tin về việc cấp quyền truy cập.
6. Nhấn vào **OK**.


Kết quả là người dùng sẽ nhận được quyền truy cập đến thiết bị đó trong khoảng thời gian được quy định bởi quản trị viên. Người dùng sẽ nhận được nhóm quyền đầy đủ để truy cập thiết bị (quyền đọc và ghi). Khi khóa hết hạn, quyền truy cập thiết bị sẽ bị chặn. Nếu người dùng cần quyền truy cập vĩnh viễn đến thiết bị, [hãy thêm thiết bị vào danh sách được tin tưởng](#).

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. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thiết bị**.
3. Trong mục **Tin nhắn mẫu**, hãy cấu hình các mẫu cho tin nhắn Kiểm soát thiết bị:
 - **Tin nhắn về hoạt động chặn** Mẫu thông báo hiển thị khi người dùng cố truy cập thiết bị bị chặn. Thông báo này cũng sẽ hiển thị khi người dùng cố thực hiện một hành động lên nội dung thiết bị bị chặn đối với người dùng này.
 - **Thông điệp đến quản trị viên** Một mẫu tin nhắn sẽ được gửi đến quản trị viên mạng LAN khi người dùng tin rằng việc chặn truy cập đến ứng dụng hoặc cấm thao tác với ứng dụng là do nhầm lẫn. Sau khi người dùng yêu cầu cung cấp quyền truy cập, Kaspersky Endpoint Security sẽ gửi một sự kiện đến Kaspersky Security Center: **Thông báo chặn truy cập thiết bị gửi đến quản trị viên**. Phần mô tả sự kiện chứa một thông báo cho quản trị viên với các biến được thay thế. Bạn có thể xem các sự kiện này trong bảng điều khiển Kaspersky Security Center bằng cách sử dụng lựa chọn sự kiện được định sẵn **User requests**. Nếu tổ chức của bạn chưa triển khai Kaspersky Security Center hoặc không có kết nối với Máy chủ quản trị thì ứng dụng sẽ gửi một thông báo cho quản trị viên tới địa chỉ email được chỉ định.
4. Lưu các thay đổi của bạn.

Anti-Bridging

Anti-Bridging ngăn tạo các cầu nối mạng bằng cách ngăn thiết lập đồng thời nhiều kết nối mạng cho một máy tính. Tính năng này cho phép bạn bảo vệ mạng doanh nghiệp trước các cuộc tấn công qua mạng không được bảo vệ, mạng phép.

Anti-Bridging điều tiết thiết lập kết nối mạng bằng *các quy tắc kết nối*.

Các quy tắc kết nối được tạo cho những loại thiết bị quy định sẵn sau:

- Bộ điều hợp mạng;
- Bộ điều hợp Wi-Fi;
- Các Modem.

Nếu một quy tắc kết nối được bật, Kaspersky Endpoint Security:


- Đóng kết nối đang hoạt động khi thiết lập một kết nối mới, nếu loại thiết bị được quy định trong quy tắc được sử dụng cho cả hai kết nối;

- Chặn các kết nối được thiết lập sử dụng loại thiết bị có quy tắc ưu tiên thấp hơn.

Bật Anti-Bridging

Anti-Bridging bị tắt theo mặc định.


Để bật Anti-Bridging:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thiết bị**.
3. Trong mục **Thiết lập truy cập**, hãy nhấn nút **Anti-Bridging**.
4. Sử dụng nút bật/tắt **Bật Anti-Bridging** để bật hoặc tắt tính năng này.
5. Lưu các thay đổi của bạn.

Sau khi Anti-Bridging được bật, Kaspersky Endpoint Security sẽ chặn các kết nối đã được thiết lập theo quy tắc kết nối.


Thay đổi trạng thái của một quy tắc kết nối

Để thay đổi trạng thái của một quy tắc kết nối:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thiết bị**.
3. Trong mục **Thiết lập truy cập**, hãy nhấn nút **Anti-Bridging**.
4. Trong mục **Các quy tắc cho thiết bị**, hãy chọn quy tắc có trạng thái bạn muốn thay đổi.
5. Sử dụng nút bật/tắt trong cột **Kiểm soát** để bật hoặc tắt quy tắc.
6. Lưu các thay đổi của bạn.

Thay đổi mức độ ưu tiên của một quy tắc kết nối

Để thay đổi mức độ ưu tiên của một quy tắc mạng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thiết bị**.
3. Trong mục **Thiết lập truy cập**, hãy nhấn nút **Anti-Bridging**.
4. Trong mục **Các quy tắc cho thiết bị**, hãy chọn quy tắc có cấp độ ưu tiên bạn muốn thay đổi.

5. Sử dụng các nút **Lên / Xuống** để đặt cấp độ ưu tiên của quy tắc kết nối.

Một quy tắc càng cao trong bảng quy tắc thì càng được ưu tiên hơn. Anti-Bridging chặn tất cả kết nối ngoại trừ một kết nối được thiết lập sử dụng loại thiết bị có quy tắc ưu tiên cao nhất.

6. Lưu các thay đổi của bạn.

Kiểm soát thích ứng sự cố

Thành phần này khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows dành cho máy trạm. Thành phần này không khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows cho máy chủ.

Thành phần Kiểm soát thích ứng sự cố sẽ giám sát và chặn các hành động mà các máy tính trong mạng công ty ít có khả năng thực hiện. Kiểm soát thích ứng sự cố sử dụng một bộ quy tắc để theo dõi các hành vi khác biệt (ví dụ, quy tắc *Khởi động Microsoft PowerShell từ ứng dụng văn phòng*). Các quy tắc này được tạo bởi các chuyên gia của Kaspersky dựa trên các tình huống hoạt động độc hại thông thường. Bạn có thể cấu hình cách Kiểm soát thích ứng sự cố xử lý từng quy tắc và, chẳng hạn, cho phép thực thi các kịch bản PowerShell tự động hóa một số tác vụ dòng công việc nhất định. Kaspersky Endpoint Security cập nhật ộ quy tắc cùng với các cơ sở dữ liệu ứng dụng. Cập nhật đến các bộ quy tắc phải được [xác nhận thủ công](#).

Thiết lập Kiểm soát thích ứng sự cố

Cấu hình Kiểm soát thích ứng sự cố bao gồm các bước sau:

1. Rèn luyện Kiểm soát thích ứng sự cố.

Sau khi bạn bật Kiểm soát thích ứng sự cố, các quy tắc của nó sẽ hoạt động trong *chế độ rèn luyện*. Trong quá trình rèn luyện, Kiểm soát thích ứng sự cố sẽ theo dõi việc kích hoạt quy tắc và gửi các sự kiện kích hoạt đến Kaspersky Security Center. Mỗi quy tắc đều có thời lượng rèn luyện riêng. Thời lượng của chế độ rèn luyện được quy định bởi các chuyên gia Kaspersky. Thông thường, chế độ rèn luyện sẽ hoạt động trong 2 tuần.

Nếu một quy tắc hoàn toàn không được kích hoạt trong quá trình huấn luyện, Kiểm soát thích ứng sự cố sẽ coi các hành động liên quan đến quy tắc này là ít gặp. Kaspersky Endpoint Security sẽ chặn mọi hành động liên quan đến quy tắc đó.

Nếu một quy tắc được kích hoạt trong quá trình rèn luyện, Kaspersky Endpoint Security sẽ ghi lại sự kiện này trong [báo cáo kích hoạt quy tắc](#) và kho lưu trữ **Triggering of rules in Smart Training state**.

2. Phân tích báo cáo kích hoạt quy tắc.

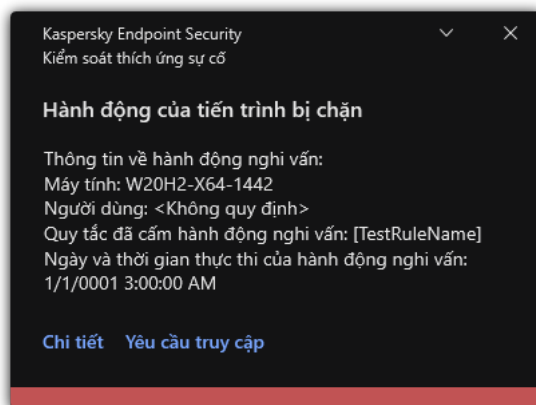
Quản trị viên sẽ phân tích [báo cáo kích hoạt quy tắc](#) hoặc nội dung của kho lưu trữ **Triggering of rules in Smart Training state**. Sau đó, quản trị viên có thể lựa chọn hành vi của Kiểm soát thích ứng sự cố khi quy tắc này được kích hoạt: chặn hoặc cho phép nó. Quản trị viên cũng có thể tiếp tục giám sát cách hoạt động của quy tắc và kéo dài thời lượng của chế độ rèn luyện. Nếu quản trị viên không có hành động nào, ứng dụng cũng sẽ tiếp tục hoạt động trong chế độ rèn luyện. Thời lượng của chế độ rèn luyện được bắt đầu lại.

Kiểm soát thích ứng sự cố được cấu hình trong thời gian thực. Kiểm soát thích ứng sự cố được cấu hình qua các kênh sau:

- Kiểm soát thích ứng sự cố khởi chạy tự động để chặn các hành động liên kết với các quy tắc không bao giờ được kích hoạt trong chế độ rèn luyện.

- Kaspersky Endpoint Security bổ sung các quy tắc mới hoặc xóa các quy tắc đã lỗi thời.
- Quản trị viên cấu hình hoạt động của Kiểm soát thích ứng sự cố sau khi xem lại báo cáo kích hoạt quy tắc và nội dung của kho lưu trữ **Triggering of rules in Smart Training state**. Bạn nên kiểm tra báo cáo kích hoạt quy tắc và nội dung của kho lưu trữ **Triggering of rules in Smart Training state**.

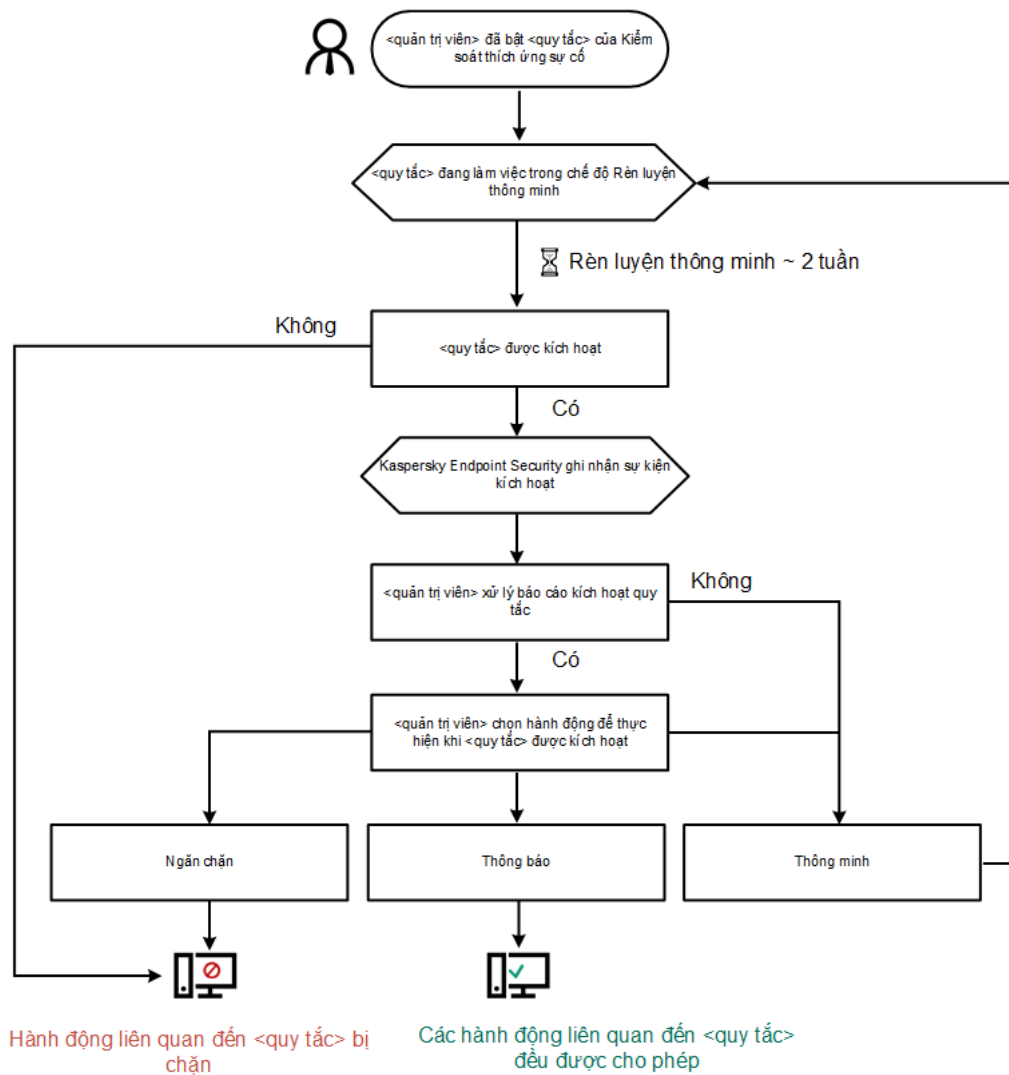
Khi một ứng dụng độc hại cố gắng thực hiện một hành động, Kaspersky Endpoint Security sẽ chặn hành động đó và hiển thị một thông báo (xem hình dưới đây).



Thông báo của Kiểm soát thích ứng sự cố

Thuật toán vận hành Kiểm soát thích ứng sự cố

Kaspersky Endpoint Security quyết định liệu có cho phép hay chặn một hành động liên kết với một quy tắc dựa trên thuật toán sau (xem hình dưới đây).




Thuật toán vận hành Kiểm soát thích ứng sự cố

Bật và tắt Kiểm soát thích ứng sự cố

Kiểm soát thích ứng sự cố được kích hoạt theo mặc định.

Để bật hoặc tắt Kiểm soát thích ứng sự cố:


1. Trong [cửa sổ chính của ứng dụng](#), hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thích ứng sự cố**.
3. Sử dụng nút bật/tắt **Kiểm soát thích ứng sự cố** để bật hoặc tắt thành phần này.
4. Lưu các thay đổi của bạn.

Kết quả là tính năng Kiểm soát thích ứng sự cố sẽ chuyển sang chế độ huấn luyện. Trong quá trình huấn luyện, Kiểm soát thích ứng sự cố sẽ giám sát việc kích hoạt quy tắc. Khi quá trình huấn luyện hoàn tất, Kiểm soát thích ứng sự cố sẽ tiến hành chặn các hành động lạ của các máy tính trong mạng của công ty.

Nếu tổ chức của bạn đã bắt đầu sử dụng một số công cụ mới và Kiểm soát thích ứng sự cố chặn hoạt động của những công cụ đó, thì bạn có thể đặt lại kết quả của chế độ huấn luyện và lặp lại quá trình huấn luyện. Để thực hiện việc này, bạn cần phải [thay đổi hành động được thực hiện khi quy tắc được kích hoạt](#) (ví dụ: hãy đặt nó thành **Thông báo**). Sau đó, bạn cần bật lại chế độ huấn luyện (đặt giá trị cho **Thông minh**).


Bật và tắt một quy tắc Kiểm soát thích ứng sự cố

Để bật hoặc tắt một quy tắc Kiểm soát thích ứng sự cố:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thích ứng sự cố**.
3. Trong mục **Quy tắc**, hãy nhấn nút **Chỉnh sửa quy tắc**.
Danh sách quy tắc Kiểm soát thích ứng sự cố sẽ mở ra.
4. Trong bảng, hãy chọn một bộ quy tắc (ví dụ: *Hoạt động của ứng dụng văn phòng*) và mở rộng bộ này.
5. Chọn một quy tắc (ví dụ: *Khởi động Windows PowerShell từ các ứng dụng văn phòng*).
6. Sử dụng nút bật/tắt trong cột **Trạng thái** để bật hoặc tắt Quy tắc Kiểm soát thích ứng sự cố.
7. Lưu các thay đổi của bạn.

Sửa hành động được thực hiện khi một quy tắc Kiểm soát thích ứng sự cố được kích hoạt

Để chỉnh sửa hành động được thực hiện khi một quy tắc Kiểm soát thích ứng sự cố được kích hoạt:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thích ứng sự cố**.
3. Trong mục **Quy tắc**, hãy nhấn nút **Chỉnh sửa quy tắc**.
Danh sách quy tắc Kiểm soát thích ứng sự cố sẽ mở ra.
4. Chọn một quy tắc trong bảng.
5. Nhấn vào **Chỉnh sửa**.
Cửa sổ thuộc tính quy tắc Kiểm soát thích ứng sự cố sẽ được mở ra.
6. Trong mục **Hành động**, chọn một trong các tùy chọn sau:
 - **Thông minh**. Nếu tùy chọn này được chọn, quy tắc Kiểm soát thích ứng sự cố sẽ hoạt động trong trạng thái Huấn luyện thông minh trong một khoảng thời gian được quy định bởi các chuyên gia Kaspersky. Trong chế độ này, khi một quy tắc Kiểm soát thích ứng sự cố được kích hoạt, Kaspersky Endpoint Security sẽ cho phép hoạt động kích hoạt quy tắc và ghi lại một mục vào lưu trữ

Triggering of rules in Smart Training state của Máy chủ quản trị Kaspersky Security Center. Khi khoảng thời gian được quy định cho trạng thái Huấn luyện thông minh kết thúc, Kaspersky Endpoint Security sẽ chặn hoạt động được bao gồm trong một quy tắc Kiểm soát thích ứng sự cố và ghi lại một mục chứa thông tin về hoạt động này.

- **Chặn.** Nếu hành động này được chọn, khi một quy tắc Kiểm soát thích ứng sự cố được kích hoạt, Kaspersky Endpoint Security sẽ chặn hoạt động kích hoạt quy tắc và ghi lại một mục chứa thông tin về hoạt động này.
- **Thông báo.** Nếu hành động này được chọn, khi một quy tắc Kiểm soát thích ứng sự cố được kích hoạt, Kaspersky Endpoint Security sẽ cho phép hoạt động kích hoạt quy tắc và ghi lại một mục chứa thông tin về hoạt động này.


7. Lưu các thay đổi của bạn.

Tạo loại trừ cho một quy tắc Kiểm soát thích ứng sự cố

Bạn không thể tạo nhiều hơn 1.000 mục loại trừ cho các quy tắc Kiểm soát thích ứng sự cố. Bạn không nên tạo nhiều hơn 200 quy tắc loại trừ. Để giảm số loại trừ được sử dụng, bạn nên sử dụng tên đại diện trong thiết lập loại trừ.

Một loại trừ cho một quy tắc Kiểm soát thích ứng sự cố bao gồm mô tả về các đối tượng nguồn và đích. *Đối tượng nguồn* là đối tượng thực hiện hành động. *Đối tượng đích* là đối tượng đón nhận hành động đó. Ví dụ, bạn đã mở một tập tin có tên `file.xlsx`. Kết quả là, một tập tin thư viện với phần mở rộng DLL được tải vào bộ nhớ máy tính. Thư viện này được một trình duyệt sử dụng (một tập tin thực thi có tên `browser.exe`). Trong ví dụ này, `file.xlsx` là đối tượng nguồn, Excel là tiến trình nguồn, `browser.exe` là đối tượng đích, và Browser là tiến trình đích.

Để tạo loại trừ cho một quy tắc Kiểm soát thích ứng sự cố:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thích ứng sự cố**.
3. Trong mục **Quy tắc**, hãy nhấn nút **Chỉnh sửa quy tắc**.
Danh sách quy tắc Kiểm soát thích ứng sự cố sẽ mở ra.
4. Chọn một quy tắc trong bảng.
5. Nhấn vào **Chỉnh sửa**.
Cửa sổ thuộc tính quy tắc Kiểm soát thích ứng sự cố sẽ được mở ra.
6. Trong mục **Loại trừ**, hãy nhấn vào nút **Thêm**.
Cửa sổ thuộc tính loại trừ sẽ mở ra.
7. Chọn người dùng mà bạn muốn cấu hình một mục loại trừ.

Kiểm soát thích ứng sự cố không hỗ trợ phần mở rộng dành cho nhóm người dùng. Nếu bạn chọn một nhóm người dùng thì Kaspersky Endpoint Security sẽ không áp dụng loại trừ.

8. Trong trường **Mô tả**, nhập mô tả về loại trừ này.

9. Quy định các thiết lập của đối tượng nguồn hoặc tiến trình nguồn được bắt đầu bởi đối tượng:

- **Tiến trình nguồn.** Đường dẫn hoặc đường dẫn đại diện đến tập tin hoặc thư mục chứa các tập tin (ví dụ: C:\Dir\File.exe hoặc Dir*.exe).
- **Hash tiến trình nguồn.** Mã băm tập tin.
- **Đối tượng nguồn.** Đường dẫn hoặc đường dẫn đại diện đến tập tin hoặc thư mục chứa các tập tin (ví dụ: C:\Dir\File.exe hoặc Dir*.exe). Ví dụ, đường dẫn tập tin document.docm, sử dụng một kịch bản hoặc macro để bắt đầu các tiến trình đích.

Bạn cũng có thể quy định các đối tượng khác để loại trừ, ví dụ như một địa chỉ web, macro, lệnh trong dòng lệnh, đường dẫn registry, v.v... Quy định đối tượng theo khuôn mẫu sau:

object://<object>, ở đó <object> là tên của đối tượng, ví dụ,

object://web.site.example.com, object://VBA, object://ipconfig, object://HKEY_USERS.

Bạn cũng có thể sử dụng các ký tự đại diện, ví dụ như object://*C:\Windows\temp*.

- **Hash đối tượng nguồn.** Mã băm tập tin.

Quy tắc Kiểm soát thích ứng sự cố không được áp dụng cho các hành động được đối tượng thực hiện, hoặc các tiến trình được đối tượng bắt đầu.

10. Quy định các thiết lập của đối tượng đích hoặc tiến trình đích được bắt đầu trên đối tượng này.

- **Tiến trình đích.** Đường dẫn hoặc đường dẫn đại diện đến tập tin hoặc thư mục chứa các tập tin (ví dụ: C:\Dir\File.exe hoặc Dir*.exe).
- **Hash tiến trình đích.** Mã băm tập tin.
- **Đối tượng đích.** Lệnh để khởi chạy tiến trình đích. Quy định lệnh theo dạng sau object://<lệnh>, ví dụ, object://cmdline:powershell -Command "\$result = 'C:\Windows\temp\result_local_users_pwdage.txt' ". Bạn cũng có thể sử dụng các ký tự đại diện, ví dụ như object://*C:\Windows\temp*.


- **Hash đối tượng đích.** Mã băm tập tin.

Quy tắc Kiểm soát thích ứng sự cố không được áp dụng cho các hành động được thực hiện trên đối tượng này, hoặc các tiến trình được bắt đầu trên đối tượng.

11. Lưu các thay đổi của bạn.

Xuất và nhập các loại trừ cho quy tắc Kiểm soát thích ứng sự cố

Để xuất hoặc nhập danh sách loại trừ cho các quy tắc đã chọn:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thích ứng sự cố**.
3. Trong mục **Quy tắc**, hãy nhấn nút **Chỉnh sửa quy tắc**.
Danh sách quy tắc Kiểm soát thích ứng sự cố sẽ mở ra.

4. Để xuất danh sách quy tắc:

- a. Chọn các quy tắc có ngoại lệ mà bạn muốn xuất.
- b. Nhấn vào **Xuất**.
- c. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin XML mà bạn muốn xuất danh sách các loại trừ vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
- d. Xác nhận rằng bạn chỉ muốn xuất các loại trừ đã chọn hoặc xuất toàn bộ danh sách loại trừ.
- e. Lưu tập tin.

5. Để nhập danh sách quy tắc:

- a. Nhấn **Nhập**.
- b. Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách các loại trừ.
- c. Mở tập tin.
Nếu máy tính đã có danh sách các loại trừ, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.


6. Lưu các thay đổi của bạn.

Áp dụng bản cập nhật cho các quy tắc của Kiểm soát thích ứng sự cố

Các quy tắc Kiểm soát thích ứng sự cố mới có thể được thêm vào bảng quy tắc và các quy tắc Kiểm soát thích ứng sự cố hiện tại có thể bị xóa từ bảng quy tắc khi cơ sở dữ liệu diệt virus được cập nhật. Kaspersky Endpoint Security phân biệt các quy tắc Kiểm soát thích ứng sự cố sẽ bị xóa hoặc được thêm vào bảng, nếu một bản cập nhật cho các quy tắc này chưa được áp dụng.

Cho đến khi cập nhật được áp dụng, Kaspersky Endpoint Security sẽ hiển thị các quy tắc Kiểm soát thích ứng sự cố sẽ được xóa bởi bản cập nhật trong bảng quy tắc và gán trạng thái *Tắt* cho chúng. Bạn không thể thay đổi thiết lập của các quy tắc này.

Để áp dụng bản cập nhật cho các quy tắc của Kiểm soát thích ứng sự cố:


1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thích ứng sự cố**.
3. Trong mục **Quy tắc**, hãy nhấn nút **Chỉnh sửa quy tắc**.
Danh sách quy tắc Kiểm soát thích ứng sự cố sẽ mở ra.
4. Trong cửa sổ mở ra, hãy nhấn nút **Phê duyệt các bản cập nhật**.
Nút **Phê duyệt các bản cập nhật** khả dụng nếu có một bản cập nhật cho các quy tắc Kiểm soát thích ứng sự cố.
5. Lưu các thay đổi của bạn.

Chỉnh sửa khuôn mẫu tin nhắn Kiểm soát thích ứng sự cố

Khi người dùng cố gắng thực hiện một hành động bị chặn bởi các quy tắc Kiểm soát thích ứng sự cố, Kaspersky Endpoint Security sẽ hiển thị một thông báo rằng các hành động có thể gây hại đã bị chặn. Nếu người dùng tin rằng hành động 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 khuôn mẫu đặc biệt có thể được sử dụng cho thông báo chặn các hành động có thể gây hại 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. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thích ứng sự cố**.
3. Trong mục **Mẫu**, hãy cấu hình các mẫu cho thông báo Kiểm soát thích ứng sự cố:
 - **Tin nhắn về hoạt động chặn** Mẫu thông báo được hiển thị cho người dùng khi một quy tắc Kiểm soát thích ứng sự cố chặn một hành động ít gặp.
 - **Thông điệp đến quản trị viên** Khuôn mẫu thông báo mà người dùng có thể gửi đến quản trị viên mạng doanh nghiệp cục bộ nếu người dùng cho rằng việc chặn là do nhầm lẫn. Sau khi người dùng yêu cầu cung cấp quyền truy cập, Kaspersky Endpoint Security sẽ gửi một sự kiện đến Kaspersky Security Center: **Thông báo chặn hoạt động của ứng dụng gửi đến quản trị viên**. Phần mô tả sự kiện chứa một thông báo cho quản trị viên với các biến được thay thế. Bạn có thể xem các sự kiện này trong bảng điều khiển Kaspersky Security Center bằng cách sử dụng lựa chọn sự kiện được định sẵn **User requests**. Nếu tổ chức của bạn chưa triển khai Kaspersky Security Center hoặc không có kết nối với Máy chủ quản trị thì ứng dụng sẽ gửi một thông báo cho quản trị viên tới địa chỉ email được chỉ định.
4. Lưu các thay đổi của bạn.

Xem các báo cáo Kiểm soát thích ứng sự cố

Để xem các báo cáo Kiểm soát thích ứng sự cố:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thích ứng sự cố**.
Cấu hình của thành phần Kiểm soát thích ứng sự cố sẽ được hiển thị trong phần bên phải của cửa sổ.
6. Thực hiện một trong các thao tác sau:

- Nếu bạn muốn xem một báo cáo về thiết lập các quy tắc Kiểm soát thích ứng sự cố, nhấn vào **Báo cáo về trạng thái các quy tắc Kiểm soát thích ứng sự cố**.
- Nếu bạn muốn xem một báo cáo về kích hoạt các quy tắc Kiểm soát thích ứng sự cố, hãy nhấn vào **Báo cáo về các quy tắc Kiểm soát thích ứng sự cố được kích hoạt**.

7. Tiến trình tạo báo cáo sẽ được bắt đầu.

Báo cáo sẽ được hiển thị trong một cửa sổ mới.

Kiểm soát ứng dụng

Thành phần Kiểm soát ứng dụng quản lý việc khởi động ứng dụng trên máy tính của người dùng. Điều này cho phép bạn thực hiện chính sách bảo mật của công ty khi sử dụng các ứng dụng. Thành phần Kiểm soát ứng dụng cũng làm giảm nguy cơ lây nhiễm máy tính bằng cách hạn chế quyền truy cập vào các ứng dụng.

Việc cấu hình Kiểm soát ứng dụng bao gồm các bước sau:

1. [Tạo danh mục ứng dụng](#).

Quản trị viên sẽ tạo các danh mục ứng dụng mà quản trị viên muốn quản lý. Các danh mục ứng dụng dành cho tất cả các máy tính trong mạng công ty, bất kể các nhóm quản trị. Để tạo một danh mục, bạn có thể sử dụng các tiêu chí sau: Danh mục KL (ví dụ: *Trình duyệt*), giá trị băm của tập tin, nhà cung cấp ứng dụng và các tiêu chí khác.

2. [Tạo các Quy tắc kiểm soát ứng dụng](#).

Quản trị viên sẽ tạo các quy tắc Kiểm soát ứng dụng trong chính sách cho nhóm quản trị. Quy tắc bao gồm các danh mục ứng dụng và trạng thái khởi động của các ứng dụng trong các danh mục này: bị chặn hoặc được phép.

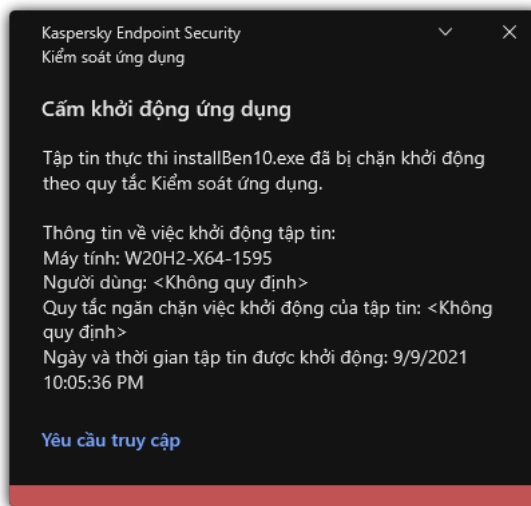
3. [Chọn chế độ Kiểm soát ứng dụng](#).

Quản trị viên sẽ chọn chế độ làm việc với các ứng dụng không có trong bất kỳ quy tắc nào (danh sách ứng dụng không được phép và được phép).

Khi người dùng cố khởi chạy một ứng dụng bị cấm, Kaspersky Endpoint Security sẽ chặn ứng dụng đó khởi chạy và sẽ hiển thị một thông báo (xem hình bên dưới).

Một *chế độ thử nghiệm* được cung cấp để kiểm tra cấu hình của Kiểm soát ứng dụng. Trong chế độ này, Kaspersky Endpoint Security thực hiện các hoạt động sau:

- Cho phép khởi động ứng dụng, bao gồm cả những ứng dụng bị cấm.
- Hiển thị một thông báo về việc khởi động ứng dụng bị cấm và thêm thông tin vào báo cáo trên máy tính của người dùng.
- Gửi dữ liệu về việc khởi động các ứng dụng bị cấm đến Kaspersky Security Center.



Thông báo của Kiểm soát ứng dụng

Chế độ hoạt động của Kiểm soát ứng dụng

Thành phần Kiểm soát ứng dụng hoạt động ở hai chế độ:

- **Danh sách không được phép.** Trong chế độ này, Kiểm soát ứng dụng cho phép người dùng khởi chạy tất cả các ứng dụng ngoại trừ các ứng dụng bị cấm trong Quy tắc kiểm soát ứng dụng. Chế độ này của thành phần Kiểm soát ứng dụng được bật theo mặc định.
- **Danh sách được phép.** Trong chế độ này, Kiểm soát ứng dụng chặn người dùng khởi chạy bất kỳ ứng dụng nào ngoại trừ các ứng dụng được phép và không bị cấm trong Quy tắc kiểm soát ứng dụng. Nếu quy tắc cho phép của thành phần Kiểm soát ứng dụng được cấu hình đầy đủ, thành phần này sẽ chặn khởi chạy tất cả các ứng dụng mới chưa được xác minh bởi quản trị viên mạng LAN, đồng thời cho phép hoạt động của hệ điều hành và của các ứng dụng được tin tưởng mà người dùng phụ thuộc để thực hiện công việc của họ.

Bạn có thể đọc [các đề xuất về cấu hình Quy tắc kiểm soát ứng dụng trong chế độ danh sách được phép](#).

Bạn có thể cấu hình Kiểm soát ứng dụng để hoạt động ở các chế độ này bằng cả hai cách: sử dụng giao diện cục bộ của Kaspersky Endpoint Security và bằng cách sử dụng Kaspersky Security Center.

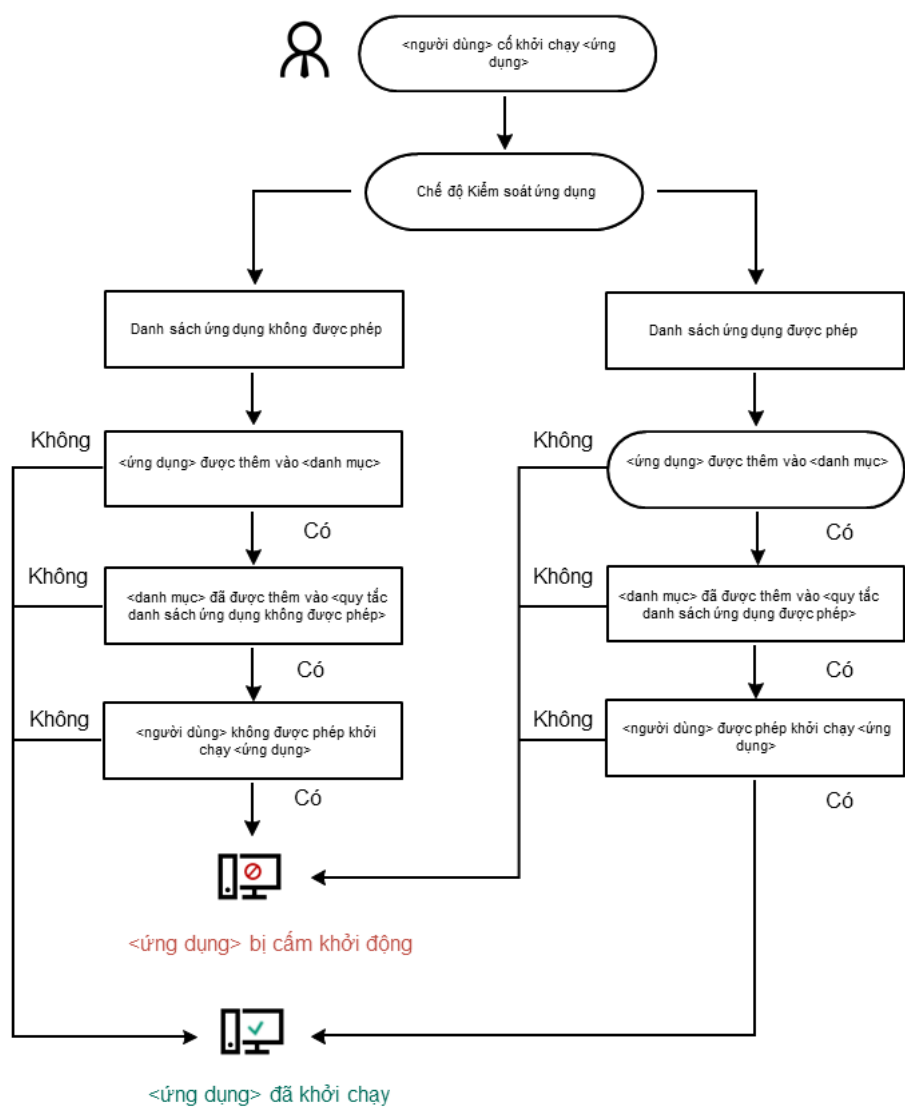
Tuy nhiên, Kaspersky Security Center cung cấp các công cụ không có sẵn trong giao diện cục bộ của Kaspersky Endpoint Security, ví dụ như các công cụ cần thiết cho các tác vụ sau:

- [Tạo danh mục ứng dụng](#). Quy tắc kiểm soát ứng dụng được tạo trong Bảng điều khiển quản trị Kaspersky Security Center dựa trên các danh mục ứng dụng tùy chỉnh của bạn chứ không dựa trên các điều kiện bao gồm và loại trừ như trong trường hợp trong giao diện cục bộ của Kaspersky Endpoint Security.
- [Tiếp nhận thông tin về các ứng dụng được cài đặt trên máy tính trong mạng LAN của công ty](#).

Đây là lý do tại sao bạn nên sử dụng Kaspersky Security Center để cấu hình hoạt động của thành phần Kiểm soát ứng dụng.

Thuật toán hoạt động của Kiểm soát ứng dụng

Kaspersky Endpoint Security sử dụng một thuật toán để đưa ra quyết định về việc khởi chạy một ứng dụng (xem hình bên dưới).



Thuật toán hoạt động của Kiểm soát ứng dụng

Giới hạn chức năng của Kiểm soát ứng dụng

Hoạt động của thành phần Kiểm soát 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 ứng dụng sẽ không được hỗ trợ.
- Khi phiên bản ứng dụng được nâng cấp, tính năng nhập thiết lập thành phần Kiểm soát ứng dụng chỉ được hỗ trợ nếu Kaspersky Endpoint Security 10 Service Pack 2 cho Windows hoặc mới hơn được nâng cấp lên Kaspersky Endpoint Security 11.9.0 cho Windows.

Khi các phiên bản ứng dụng ngoài Kaspersky Endpoint Security 10 Service Pack 2 cho Windows được nâng cấp, thiết lập Kiểm soát ứng dụng sẽ cần được cấu hình mới để khôi phục thành phần này về trạng thái hoạt động.

- 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.

Danh sách các ứng dụng mà Kaspersky Endpoint Security chỉ định là Danh mục KL **Other applications** \ **Các ứng dụng được tin tưởng theo danh tiếng trong KSN** có thể khác nhau tùy thuộc vào việc có sẵn kết nối với máy chủ KSN hay không.

- 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 thông dịch thông qua dòng lệnh.

Nếu việc khởi động một trình biên dịch là được cho phép bởi các quy tắc Kiểm soát ứng dụng, thành phần này sẽ không chặn một kịch bản được khởi chạy từ trình biên dịch này.

Nếu ít nhất một kịch bản được quy định trong dòng lệnh của trình biên dịch bị chặn khởi động bởi các quy tắc Kiểm soát ứng dụng, thành phần này sẽ chặn tất cả các kịch bản được quy định trong dòng lệnh của trình biên dịch.

- 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 thông dịch sau:

- Java
- PowerShell

Các loại trình biên dịch sau không được hỗ trợ:


- %ComSpec%;
- %SystemRoot%\system32\regedit.exe;
- %SystemRoot%\regedit.exe;
- %SystemRoot%\system32\regedt32.exe;
- %SystemRoot%\system32\cscript.exe;
- %SystemRoot%\system32\wscript.exe;
- %SystemRoot%\system32\msiexec.exe;

- %SystemRoot%\system32\mshta.exe;
- %SystemRoot%\system32\rundll32.exe;
- %SystemRoot%\system32\wwahost.exe;
- %SystemRoot%\syswow64\cmd.exe;
- %SystemRoot%\syswow64\regedit.exe;
- %SystemRoot%\syswow64\regedt32.exe;
- %SystemRoot%\syswow64\cscript.exe;
- %SystemRoot%\syswow64\wscript.exe;
- %SystemRoot%\syswow64\msiexec.exe;
- %SystemRoot%\syswow64\mshta.exe;
- %SystemRoot%\syswow64\rundll32.exe;
- %SystemRoot%\syswow64\wwahost.exe.

Bật và tắt Kiểm soát ứng dụng

Thành phần Kiểm soát ứng dụng bị tắt theo mặc định.


Để bật hoặc tắt Kiểm soát ứng dụng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát ứng dụng**.
3. Sử dụng nút bật/tắt **Kiểm soát ứng dụng** để bật hoặc tắt thành phần.
4. Lưu các thay đổi của bạn.

Kết quả là nếu thành phần Kiểm soát ứng dụng được bật, ứng dụng sẽ chuyển tiếp thông tin về các tập tin thực thi đang chạy tới Kaspersky Security Center. Bạn có thể xem danh sách các tập tin thực thi đang chạy trong Kaspersky Security Center, trong thư mục **Tập tin thực thi**. Để nhận thông tin về tất cả các tập tin thực thi thay vì chỉ nhận thông tin của các tập tin thực thi đang chạy, hãy chạy [Tác vụ kiểm kê](#).

Chọn chế độ Kiểm soát ứng dụng

Để chọn chế độ Kiểm soát ứng dụng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát ứng dụng**.

3. Trong mục **Chế độ Kiểm soát khởi động ứng dụng**, hãy chọn một trong các tùy chọn sau:

- **Danh sách không được phép.** Nếu mục này được chọn, Kiểm soát ứng dụng sẽ cho phép tất cả người dùng được bắt đầu bất kỳ ứng dụng nào, ngoại trừ các trường hợp thỏa mãn điều kiện trong quy tắc chặn của Kiểm soát ứng dụng.
- **Danh sách được phép.** Nếu mục này được chọn, Kiểm soát ứng dụng sẽ chặn tất cả người dùng khỏi việc bắt đầu bất kỳ ứng dụng nào, ngoại trừ trong các trường hợp thỏa mãn điều kiện trong quy tắc cho phép của Kiểm soát ứng dụng.

Quy tắc **Tập tin ảnh hoàn hảo** và quy tắc **Trình cập nhật được tin tưởng** ban đầu được định nghĩa cho chế độ Danh sách được phép. Các Quy tắc kiểm soát ứng dụng này tương ứng với các danh mục KL. Danh mục KL "Tập tin ảnh hoàn hảo" bao gồm các chương trình đảm bảo hoạt động bình thường của hệ điều hành. Danh mục KL "Trình cập nhật được tin tưởng" bao gồm các trình cập nhật cho hầu hết những nhà cung cấp phần mềm uy tín. Bạn không thể xóa các quy tắc này. Cấu hình của các quy tắc này không thể được sửa đổi. Theo mặc định, quy tắc **Tập tin ảnh hoàn hảo** 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, bạn chỉ cần chọn chế độ cần thiết.

4. Trong mục **Hành động tại thời điểm khởi động của các ứng dụng bị chặn**, hãy 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.
5. Chọn hộp kiểm **Kiểm soát nạp mô-đun DLL** nếu bạn muốn Kaspersky Endpoint Security giám sát việc nạp các mô-đun DLL khi ứng dụng được khởi chạy bởi người dùng.

Thông tin về mô-đun và ứng dụng nạp mô-đun sẽ được lưu vào một báo cáo.

Kaspersky Endpoint Security chỉ giám sát các mô-đun DLL và trình điều khiển được nạp kể từ khi hộp kiểm được chọn. Khởi động lại máy tính sau khi chọn hộp kiểm nếu bạn muốn Kaspersky Endpoint Security giám sát tất cả các mô-đun DLL và trình điều khiển, bao gồm những mô-đun và trình điều khiển được nạp trước khi khởi chạy Kaspersky Endpoint Security.

Khi bật chức năng kiểm soát quá trình nạp các mô-đun DLL và trình điều khiển, hãy đảm bảo rằng một trong các quy tắc sau đây được bật trong thiết lập Kiểm soát ứng dụng: quy tắc **Tập tin ảnh hoàn hảo** mặc định hoặc một quy tắc khác chứa danh mục KL "Chúng chỉ được tin tưởng" và đảm bảo rằng các mô-đun DLL và trình điều khiển được tin tưởng đã được nạp trước khi khởi chạy Kaspersky Endpoint Security. Việc bật tính năng kiểm soát nạp mô-đun DLL và trình điều khiển khi quy tắc **Tập tin ảnh hoàn hảo** bị tắt có thể gây bất ổn cho hệ điều hành.

Chúng tôi khuyến nghị bật chức năng [bảo vệ bằng mật khẩu](#) cho việc cấu hình thiết lập chương trình, để bạn có thể tắt các quy tắc chặn việc khởi chạy của những mô-đun DLL và trình điều khiển thiết yếu mà không thay đổi thiết lập chính sách của Kaspersky Security Center.

6. Lưu các thay đổi của bạn.

Làm việc với các quy tắc Kiểm soát ứng dụng trong giao diện ứng dụng

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 quy định điều kiện kích hoạt và các hành động được thực hiện bởi thành phần Kiểm soát ứng dụng 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

Điều kiện kích hoạt quy tắc có mối tương quan sau: "loại điều kiện - tiêu chí điều kiện - giá trị điều kiện". 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.

Các loại điều kiện sau được sử dụng trong quy tắc:

- *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 chỉ: đơn vị cấp, chủ thể, vân tay.
- Tình trạng bao gồm của ứng dụng trong một danh 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 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 sẽ không kiểm soát việc khởi động của ứng dụng.

Nếu bạn đã chọn chứng chỉ làm điều kiện kích hoạt quy tắc thì bạn cần đảm bảo rằng chứng chỉ này được thêm vào ổ lưu trữ hệ thống được tin tưởng trên máy tính và kiểm tra [thiết lập sử dụng ổ lưu trữ hệ thống được tin tưởng trong ứng dụng](#).

Các quyết định được đưa ra bởi thành phần Kiểm soát ứng dụng khi một quy tắc được kích hoạt

Khi một quy tắc được kích hoạt, Kiểm soát ứng dụng 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 đã được gán cho một nhóm người dùng trong khi một quy tắc chặn của Kiểm soát ứng dụng được gán 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 có thể có một trong hai trạng thái hoạt động sau:

- **Đã bật.** Trạng thái này có nghĩa rằng quy tắc được sử dụng khi thành phần Kiểm soát ứng dụng đang chạy.
- **Đã tắt.** Trạng thái này có nghĩa rằng quy tắc bị bỏ qua khi thành phần Kiểm soát ứng dụng đang chạy.
- **Đang kiểm tra.** Trạng thái này có nghĩa Kaspersky Endpoint Security cho phép việc khởi động ứng dụng được quản lý bởi quy tắc này, nhưng sẽ ghi lại thông tin về việc khởi động các ứng dụng đó trong báo cáo.

Thêm một Quy tắc kiểm soát ứng dụng

Để thêm một Quy tắc kiểm soát ứng dụng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát ứng dụng**.
3. Nhấn nút **Ứng dụng bị chặn** hoặc **Các ứng dụng được cho phép**.
Thao tác này sẽ mở danh sách Quy tắc kiểm soát ứng dụng.
4. Nhấn vào **Thêm**.
Thao tác này sẽ mở ra cửa sổ thiết lập Quy tắc Kiểm soát ứng dụng.
5. Trên thẻ **Thiết lập tổng quát**, xác định thiết lập chính của quy tắc:
 - a. Trong trường **Tên quy tắc**, hãy nhập tên của quy tắc.

b. Trong trường **Mô tả**, nhập mô tả về quy tắc này.

c. 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 **Các chủ thể và quyền của họ**.

Theo mặc định, giá trị **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.

d. Trong bảng **Các chủ thể và quyền của họ**, hãy dùng nút bật/tắt để xác định quyền khởi chạy ứng dụng của người dùng.

e. Chọn hộp kiểm **Từ chối người sử dụng khác** nếu bạn muốn ứng dụng ngăn ứng dụng đáp ứng các điều kiện kích hoạt quy tắc chạy cho tất cả người dùng không được liệt kê trong bảng **Các chủ thể và quyền của họ** và không phải là thành viên của các nhóm người dùng được liệt kê trong bảng **Các chủ thể và quyền của họ**.

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 **Các chủ thể và quyền của họ** và không thuộc nhóm người dùng được quy định trong bảng **Các chủ thể và quyền của họ**.

f. Chọn hộp kiểm **Trình cập nhật được tin tưởng** nếu bạn muốn Kaspersky Endpoint Security coi các ứng dụng phù hợp với điều kiện kích hoạt quy tắc là trình cập nhật được tin tưởng. *Trình cập nhật được tin tưởng* là các ứng dụng được phép tạo những tập tin thực thi khác, sẽ được phép chạy sau đó.

Nếu một ứng dụng kích hoạt nhiều quy tắc thì Kaspersky Endpoint Security sẽ đặt cờ "Trình cập nhật được tin tưởng" nếu thỏa mãn các điều kiện sau:

- Tất cả các quy tắc đều cho phép ứng dụng chạy.
- Ít nhất một quy tắc có hộp kiểm **Trình cập nhật được tin tưởng** được chọn.

6. Trên thẻ **Điều kiện**, hãy [tạo](#) hoặc chỉnh sửa danh sách các điều kiện loại trừ để kích hoạt quy tắc.


7. Trên thẻ **Loại trừ**, hãy tạo hoặc chỉnh sửa danh sách các điều kiện loại trừ để kích hoạt quy tắc.

Khi các thiết lập của Kaspersky Endpoint Security được chuyển, danh sách các tập tin thực thi được tạo bởi những cập nhật tin tưởng cũng sẽ được chuyển.

8. Lưu các thay đổi của bạn.

Bổ sung một điều kiện kích hoạt cho một quy tắc Kiểm soát ứng dụng

Để bổ sung một điều kiện kích hoạt cho một quy tắc Kiểm soát ứng dụng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát ứng dụng**.

3. Nhấn nút **Ứng dụng bị chặn** hoặc **Các ứng dụng được cho phép**.

Thao tác này sẽ mở danh sách Quy tắc kiểm soát ứng dụng.

4. Chọn quy tắc mà bạn muốn cấu hình điều kiện kích hoạt.

Thuộc tính Quy tắc kiểm soát ứng dụng sẽ mở ra.

5. Chọn thẻ **Điều kiện** hoặc thẻ **Loại trừ** và nhấn nút **Thêm**.

6. Chọn điều kiện kích hoạt cho Quy tắc kiểm soát ứng dụng:

- **Điều kiện từ thuộc tính của ứng dụng được khởi động.** Trong danh sách các ứng dụng đang chạy, bạn có thể chọn các ứng dụng mà Quy tắc kiểm soát ứng dụng sẽ được áp dụng. Kaspersky Endpoint Security cũng sẽ liệt kê các ứng dụng đã chạy trước đó trên máy tính. Bạn cần chọn tiêu chí mà bạn muốn sử dụng để tạo một hoặc nhiều điều kiện kích hoạt quy tắc: **Giá trị băm tập tin, Chứng chỉ, Danh mục KL, Siêu dữ liệu** hoặc **Đường dẫn đến tập tin/thư mục**.
- **Điều kiện "Danh mục KL".** Một *danh mục KL* là một danh sách các ứng dụng có cùng chủ đề. Danh sách này được duy trì bởi các chuyên gia Kaspersky. Ví dụ: danh mục KL mang tên "Ứng dụng văn phòng" bao gồm các ứng dụng từ bộ phần mềm Microsoft Office, Adobe® Acrobat®, v.v...
- **Điều kiện tùy chỉnh.** Bạn có thể chọn tập tin ứng dụng và chọn một trong các điều kiện kích hoạt quy tắc: **Giá trị băm tập tin, Chứng chỉ, Siêu dữ liệu** hoặc **Đường dẫn đến tập tin/thư mục**.
- **Điều kiện theo ổ đĩa tập tin (ổ đĩa di động).** Quy tắc kiểm soát ứng dụng chỉ được áp dụng cho các tập tin chạy trên ổ đĩa di động.
- **Điều kiện từ thuộc tính của tập tin trong thư mục chỉ định.** Quy tắc kiểm soát ứng dụng chỉ được áp dụng cho các tập tin trong thư mục được chỉ định. Bạn cũng có thể thêm hoặc loại trừ các tập tin khỏi các thư mục con. Bạn cần chọn tiêu chí mà bạn muốn sử dụng để tạo một hoặc nhiều điều kiện kích hoạt quy tắc: **Giá trị băm tập tin, Chứng chỉ, Danh mục KL, Siêu dữ liệu** hoặc **Đường dẫn đến tập tin/thư mục**.

7. Lưu các thay đổi của bạn.

Khi thêm các điều kiện, vui lòng lưu ý các điểm cần cân nhắc đặc biệt sau đối với Kiểm soát ứng dụng:

- Kaspersky Endpoint Security không hỗ trợ giá trị MD5 của tập tin và không kiểm soát việc khởi động ứng dụng dựa trên giá trị băm MD5. Một mã băm SHA256 được sử dụng làm điều kiện kích hoạt quy tắc.
- Không nên chỉ sử dụng các tiêu chí **Đơn vị cấp** và **Tiêu đề** làm điều kiện kích hoạt quy tắc. Việc sử dụng các tiêu chí này là không ổn định.
- Nếu bạn đang sử dụng một liên kết tượng trưng trong trường **Đường dẫn đến tập tin/thư mục**, bạn nên diễn giải liên kết tượng trưng đó để quy tắc Kiểm soát ứng dụng có thể hoạt động tốt. Để làm điều này, nhấn vào nút **Diễn giải liên kết tượng trưng**.

Thay đổi trạng thái của một quy tắc Kiểm soát ứng dụng

Để thay đổi trạng thái của một quy tắc Kiểm soát ứng dụng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .

2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát ứng dụng**.

3. Nhấn nút **Ứng dụng bị chặn** hoặc **Các ứng dụng được cho phép**.

Thao tác này sẽ mở danh sách Quy tắc kiểm soát ứng dụng.

4. Trong cột **Trạng thái**, hãy mở menu ngữ cảnh và chọn một trong các mục sau:

- **Đã bật.** Trạng thái này có nghĩa rằng quy tắc được sử dụng khi thành phần Kiểm soát ứng dụng đang chạy.
- **Đã tắt.** Trạng thái này có nghĩa rằng quy tắc bị bỏ qua khi thành phần Kiểm soát ứng dụng đang chạy.
- **Đang kiểm tra.** Trạng thái này có nghĩa Kaspersky Endpoint Security luôn cho phép việc khởi động ứng dụng được quản lý bởi quy tắc này, nhưng sẽ ghi lại thông tin về việc khởi động các ứng dụng đó trong báo cáo.

5. Lưu các thay đổi của bạn.

Quản lý các quy tắc Kiểm soát ứng dụng trong Kaspersky Security Center

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 quy định điều kiện kích hoạt và các hành động được thực hiện bởi thành phần Kiểm soát ứng dụng 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

Điều kiện kích hoạt quy tắc có mối tương quan sau: "loại điều kiện - tiêu chí điều kiện - giá trị điều kiện". 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.

Các loại điều kiện sau được sử dụng trong quy tắc:

- **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 chỉ: đơn vị cấp, chủ thể, vân tay.
- Tình trạng bao gồm của ứng dụng trong một danh 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 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 sẽ không kiểm soát việc khởi động của ứng dụng.

Nếu bạn đã chọn chứng chỉ làm điều kiện kích hoạt quy tắc thì bạn cần đảm bảo rằng chứng chỉ này được thêm vào ổ lưu trữ hệ thống được tin tưởng trên máy tính và kiểm tra [thiết lập sử dụng ổ lưu trữ hệ thống được tin tưởng trong ứng dụng](#).

Các quyết định được đưa ra bởi thành phần Kiểm soát ứng dụng khi một quy tắc được kích hoạt

Khi một quy tắc được kích hoạt, Kiểm soát ứng dụng 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 đã được gán cho một nhóm người dùng trong khi một quy tắc chặn của Kiểm soát ứng dụng được gán 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 có thể có một trong hai trạng thái hoạt động sau:

- **Đã bật.** Trạng thái này có nghĩa rằng quy tắc được sử dụng khi thành phần Kiểm soát ứng dụng đang chạy.
- **Đã tắt.** Trạng thái này có nghĩa rằng quy tắc bị bỏ qua khi thành phần Kiểm soát ứng dụng đang chạy.
- **Đang kiểm tra.** Trạng thái này có nghĩa Kaspersky Endpoint Security cho phép việc khởi động ứng dụng được quản lý bởi quy tắc này, nhưng sẽ ghi lại thông tin về việc khởi động các ứng dụng đó trong báo cáo.

Truy xuất 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 tối ưu, trước hết bạn nên tìm hiểu về các ứng dụng được sử dụng trên các máy tính trên mạng LAN doanh nghiệp. 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 **Applications registry** và **Executable files**. Thư mục **Applications registry** và thư mục **Executable files** được đặt trong thư mục **Application management** trên cây Bảng điều khiển quản trị Kaspersky Security Center.

Thư mục **Applications registry** chứa danh sách các ứng dụng được phát hiện bởi [Network Agent](#) cài đặt trên máy khách.

Thư mục **Executable files** 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 **Applications registry** hoặc thư mục **Executable files**.

Để mở cửa sổ thuộc tính ứng dụng trong thư mục Applications registry:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây Bảng điều khiển quản trị, hãy chọn **Additional** → **Application management** → **Applications registry**.
3. Chọn một ứng dụng.
4. Trong menu ngữ cảnh của ứng dụng, chọn **Properties**.

Để mở cửa sổ thuộc tính cho tập tin thực thi trong thư mục Executable files:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây Bảng điều khiển quản trị, chọn thư mục **Additional** → **Application management** → **Executable files**.
3. Chọn một tập tin thực thi.
4. Trong menu ngữ cảnh của tập tin thực thi, chọn **Properties**.

Tạo danh mục ứng dụng

Để tiện lợi hơn khi tạo các quy tắc Kiểm soát ứng dụng, bạn có thể tạo các danh mục ứng dụng.

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 danh mục ứng dụng riêng cũng có thể được tạo cho mỗi nhóm người dùng.

Để tạo một danh mục ứng dụng:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây Bảng điều khiển quản trị, chọn thư mục **Additional** → **Application management** → **Application categories**.
3. Nhấn nút **New category** 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.

Bước 1. Chọn loại danh mục

Ở bước này, chọn một trong các loại danh mục ứng dụng sau:

- **Category with content added manually.** Nếu bạn chọn loại danh mục này, ở bước "Cấu hình các điều kiện để thêm ứng dụng vào một danh mục" và bước "Cấu hình các điều kiện để loại trừ ứng dụng khỏi một danh mục", bạn sẽ có thể xác định các tiêu chí để thêm các tập tin thực thi vào trong danh mục đó.
- **Category that includes executable files from selected devices.** Nếu bạn đã chọn loại danh mục này, ở bước "Cấu hình", bạn có thể chỉ định một máy tính có tập tin thực thi sẽ được thêm vào trong danh mục đó.
- **Category that includes executable files from a specific folder.** Nếu bạn đã chọn loại danh mục này, ở bước "Thư mục kho lưu trữ", bạn có thể chỉ định một thư mục có các tập tin thực thi sẽ được tự động thêm vào trong danh mục đó.

Khi tạo một danh mục có nội dung được bổ sung tự động, Kaspersky Security Center sẽ tiến hành kiểm kê các tập tin có định dạng sau: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX, và SCR.

Bước 2. Nhập vào một tên danh mục người dùng

Ở bước này, quy định một tên cho danh mục ứng dụng.

Bước 3. Cấu hình các điều kiện bao gồm ứng dụng trong một danh mục

Bước này có thể được quy định nếu bạn đã chọn loại danh mục **Category with content added manually**.

Ở bước này, trong danh sách thả xuống **Add**, hãy chọn các điều kiện để thêm các ứng dụng vào danh mục đó:

- **From the list of executable files.** Thêm ứng dụng từ danh sách các tập tin thực thi trên thiết bị khách vào danh mục tùy chỉnh.
- **From file properties.** Quy định dữ liệu chi tiết của các tập tin thực thi như một điều kiện để bổ sung ứng dụng vào danh mục tùy chỉnh.
- **Metadata from files in folder.** Chọn một thư mục trên thiết bị khách chứa các tập tin thực thi. Kaspersky Security Center sẽ chỉ báo siêu dữ liệu của các tập tin thực thi này như một điều kiện để bổ sung ứng dụng vào danh mục tùy chỉnh.
- **Checksums of the files in the folder.** Chọn một thư mục trên thiết bị khách chứa các tập tin thực thi. Kaspersky Security Center sẽ chỉ báo hash của các tập tin thực thi này như một điều kiện để bổ sung ứng dụng vào danh mục tùy chỉnh.
- **Certificates for the files from the folder.** Chọn một thư mục trên thiết bị khách chứa các tập tin thực thi được ký duyệt chứng chỉ. Kaspersky Security Center sẽ chỉ báo chứng chỉ của các tập tin thực thi này như một điều kiện để bổ sung ứng dụng vào danh mục tùy chỉnh.

Bạn không nên sử dụng các điều kiện có thuộc tính không được quy định tham số **Certificate thumbprint**.

- **MSI installer files metadata.** Chọn gói MSI. Kaspersky Security Center sẽ chỉ báo siêu dữ liệu của tập tin thực thi được đóng gói trong gói cài đặt MSI này như một điều kiện để thêm các ứng dụng vào danh mục tùy chỉnh.
- **Checksums of the files from the MSI installer of the application.** Chọn gói MSI. Kaspersky Security Center sẽ chỉ báo các giá trị hash của tập tin thực thi được đóng gói trong gói cài đặt này như một điều kiện để thêm các ứng dụng vào danh mục tùy chỉnh.
- **From KL category.** Quy định một danh mục KL như một điều kiện để bổ sung ứng dụng vào danh mục tùy chỉnh. Một *danh mục KL* là một danh sách các ứng dụng có cùng chủ đề. Danh sách này được duy trì bởi các chuyên gia Kaspersky. Ví dụ, danh mục KL mang tên "Ứng dụng văn phòng" bao gồm các ứng dụng từ bộ phần mềm Microsoft Office, Adobe Acrobat, v.v...
Bạn có thể chọn tất cả các danh mục KL để tạo một danh sách mở rộng các ứng dụng được tin tưởng.
- **Specify path to application.** Chọn một thư mục trên thiết bị khách. Kaspersky Security Center sẽ bổ sung tập tin thực thi từ thư mục này vào danh mục tùy chỉnh đó.
- **Select certificate from repository.** Chọn các chứng chỉ đã được sử dụng để ký tập tin thực thi như một điều kiện để thêm các ứng dụng vào danh mục tùy chỉnh.

Bạn không nên sử dụng các điều kiện có thuộc tính không được quy định tham số **Certificate thumbprint**.

- **Drive type.** Quy định loại thiết bị lưu trữ (tất cả các ổ cứng và ổ đĩa di động, hoặc chỉ ổ đĩa di động) như một điều kiện để bổ sung ứng dụng vào danh mục tùy chỉnh.

Bước 4. Cấu hình các điều kiện để loại trừ ứng dụng từ một danh mục

Bước này có thể được quy định nếu bạn đã chọn loại danh mục **Category with content added manually**.

Các ứng dụng được quy định ở bước này được loại trừ khỏi danh mục kể cả khi chúng đã được quy định ở bước "Cấu hình các điều kiện bao gồm ứng dụng trong một danh mục".

Ở bước này, trong danh sách thả xuống **Add**, hãy chọn các điều kiện sau đây để loại trừ các ứng dụng khỏi danh mục đó:

- **From the list of executable files.** Thêm ứng dụng từ danh sách các tập tin thực thi trên thiết bị khách vào danh mục tùy chỉnh.
- **From file properties.** Quy định dữ liệu chi tiết của các tập tin thực thi như một điều kiện để bổ sung ứng dụng vào danh mục tùy chỉnh.
- **Metadata from files in folder.** Chọn một thư mục trên thiết bị khách chứa các tập tin thực thi. Kaspersky Security Center sẽ chỉ báo siêu dữ liệu của các tập tin thực thi này như một điều kiện để bổ sung ứng dụng vào danh mục tùy chỉnh.
- **Checksums of the files in the folder.** Chọn một thư mục trên thiết bị khách chứa các tập tin thực thi. Kaspersky Security Center sẽ chỉ báo hash của các tập tin thực thi này như một điều kiện để bổ sung ứng dụng vào danh mục tùy chỉnh.
- **Certificates for the files from the folder.** Chọn một thư mục trên thiết bị khách chứa các tập tin thực thi được ký duyệt chứng chỉ. Kaspersky Security Center sẽ chỉ báo chứng chỉ của các tập tin thực thi này như một điều kiện để bổ sung ứng dụng vào danh mục tùy chỉnh.
- **MSI installer files metadata.** Chọn gói MSI. Kaspersky Security Center sẽ chỉ báo siêu dữ liệu của tập tin thực thi được đóng gói trong gói cài đặt MSI này như một điều kiện để thêm các ứng dụng vào danh mục tùy chỉnh.
- **Checksums of the files from the MSI installer of the application.** Chọn gói MSI. Kaspersky Security Center sẽ chỉ báo các giá trị hash của tập tin thực thi được đóng gói trong gói cài đặt này như một điều kiện để thêm các ứng dụng vào danh mục tùy chỉnh.
- **From KL category.** Quy định một danh mục KL như một điều kiện để bổ sung ứng dụng vào danh mục tùy chỉnh. Một *danh mục KL* là một danh sách các ứng dụng có cùng chủ đề. Danh sách này được duy trì bởi các chuyên gia Kaspersky. Ví dụ, danh mục KL mang tên "Ứng dụng văn phòng" bao gồm các ứng dụng từ bộ phần mềm Microsoft Office, Adobe Acrobat, v.v...
Bạn có thể chọn tất cả các danh mục KL để tạo một danh sách mở rộng các ứng dụng được tin tưởng.
- **Specify path to application.** Chọn một thư mục trên thiết bị khách. Kaspersky Security Center sẽ bổ sung tập tin thực thi từ thư mục này vào danh mục tùy chỉnh đó.
- **Select certificate from repository.** Chọn các chứng chỉ đã được sử dụng để ký tập tin thực thi như một điều kiện để thêm các ứng dụng vào danh mục tùy chỉnh.
- **Drive type.** Quy định loại thiết bị lưu trữ (tất cả các ổ cứng và ổ đĩa di động, hoặc chỉ ổ đĩa di động) như một điều kiện để bổ sung ứng dụng vào danh mục tùy chỉnh.

Bước 5. Cấu hình

Bước này có thể được quy định nếu bạn đã chọn loại danh mục **Category that includes executable files from selected devices**.

Ở bước này, hãy nhấn nút **Thêm** và chỉ định máy tính có tập tin thực thi sẽ được thêm vào danh mục ứng dụng bởi Kaspersky Security Center. Tất cả các tập tin thực thi từ máy tính được quy định trong thư mục **Executable files** sẽ được thêm vào danh mục ứng dụng của Kaspersky Security Center.

Ở bước này, bạn cũng có thể cấu hình các thiết lập sau:

- Thuật toán tính toán hàm băm. Để chọn một thuật toán, bạn phải chọn ít nhất một trong các hộp kiểm sau:
 - **Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions).**
 - **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows).**

- Hộp kiểm **Synchronize data with Administration Server repository**. Chọn hộp kiểm này nếu bạn muốn Kaspersky Security Center xóa định kỳ danh mục ứng dụng và thêm vào đó tất cả các tập tin thực thi từ máy tính được quy định có trong thư mục **Executable files**.

Nếu hộp kiểm **Synchronize data with Administration Server repository** bị xóa, Kaspersky Security Center sẽ không bổ sung bất kỳ sửa đổi nào đến một danh mục ứng dụng sau khi nó được tạo.

- Trường **Scan period (h)**. Trong trường này, bạn có thể quy định khoảng thời gian (tính theo giờ) mà sau đó Kaspersky Security Center sẽ xóa danh mục ứng dụng và thêm vào đó tất cả các tập tin thực thi từ máy tính được quy định có trong thư mục **Tập tin thực thi**.

Trường này có thể được sử dụng nếu hộp kiểm **Synchronize data with Administration Server repository** được chọn.

Bước 6. Thư mục kho dữ liệu

Bước này có thể được quy định nếu bạn đã chọn loại danh mục **Category that includes executable files from a specific folder**.

Ở bước này, hãy chỉ định thư mục mà Kaspersky Security Center sẽ tìm kiếm tập tin thực thi để tự động thêm các ứng dụng trong đó vào danh mục ứng dụng.

Ở bước này, bạn cũng có thể cấu hình các thiết lập sau:

- Hộp kiểm **Include dynamic-link libraries (DLL) in this category**. Chọn hộp kiểm này nếu bạn muốn các thư viện liên kết động (tập tin DLL) được thêm vào danh mục ứng dụng.

Việc bao gồm các tập tin DLL trong danh mục ứng dụng có thể làm giảm hiệu quả của Kaspersky Security Center.

- Hộp kiểm **Include script data in this category**. Chọn hộp kiểm này nếu bạn muốn các kịch bản được thêm vào danh mục ứng dụng.

Việc thêm các kịch bản vào danh mục ứng dụng có thể làm giảm hiệu năng của Kaspersky Security Center.

- Thuật toán tính toán hàm băm. Để chọn một thuật toán, bạn phải chọn ít nhất một trong các hộp kiểm sau:
 - **Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions).**
 - **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows).**
- Hộp kiểm **Force folder scan for changes**. Chọn hộp kiểm này nếu bạn muốn Kaspersky Security Center tìm kiếm định kỳ các tập tin thực thi trong thư mục được sử dụng để tự động thêm chúng vào danh mục ứng dụng.

Nếu hộp kiểm **Force folder scan for changes** bị xóa, Kaspersky Security Center sẽ chỉ tự động tìm kiếm các tập tin thực thi trong thư mục được sử dụng để tự động thêm chúng vào danh mục ứng dụng trong trường hợp đã xảy ra thay đổi trong thư mục, các tập tin đã được thêm vào hoặc xóa khỏi đó.
- Trường **Scan period (h)**. Trong trường này, bạn có thể quy định chu kỳ thời gian (tính theo giờ) mà sau đó Kaspersky Security Center sẽ tìm kiếm một tập tin thực thi trong thư mục để tự động thêm chúng vào danh mục ứng dụng.

Trường này có thể được sử dụng nếu hộp kiểm **Force folder scan for changes** được chọn.

Bước 7. Tạo một danh mục tùy chỉnh

Thoát Trình hướng dẫn.

Bổ sung các tập tin thực thi từ thư mục Tập tin thực thi đến danh mục ứng dụng

Thư mục **Tập tin thực thi** hiển thị danh sách các tập tin thực thi được phát hiện trên máy tính. Kaspersky Endpoint Security tạo một danh sách các tập tin thực thi sau khi thực thi Tác vụ Kho.

Để bổ sung các tập tin thực thi từ thư mục Executable files đến danh mục ứng dụng:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây Bảng điều khiển quản trị, hãy chọn thư mục **Additional** → **Application management** → **Executable files**.
3. Trong không gian làm việc, chọn các tập tin thực thi mà bạn muốn thêm vào danh mục ứng dụng.
4. Nhấn phải chuột để mở menu ngữ cảnh cho các tập tin thực thi được chọn và chọn **Add to category**.
5. Trong cửa sổ mở ra, hãy thực hiện như sau:
 - Trong phần trên của cửa sổ, chọn một trong các tùy chọn sau:

- **Add to a new application category.** Chọn tùy chọn này nếu bạn muốn tạo một danh mục ứng dụng mới và bổ sung các tập tin thực thi vào đó.
- **Add to an existing application category.** Chọn tùy chọn này nếu bạn muốn chọn một danh mục ứng dụng hiện có và bổ sung các tập tin thực thi vào đó.
- Trong mục **Rule type**, hãy chọn một trong các tùy chọn sau:
 - **Rules for adding to inclusions.** Chọn tùy chọn này nếu bạn muốn tạo một điều kiện bổ sung các tập tin thực thi vào danh mục ứng dụng.
 - **Rules for adding to exclusions.** Chọn tùy chọn này nếu bạn muốn tạo một điều kiện loại trừ các tập tin thực thi khỏi danh mục ứng dụng.
- Trong mục **Parameter used as a condition**, hãy chọn một trong các tùy chọn sau:
 - **Certificate details (or SHA-256 hashes for files without a certificate).**
 - **Certificate details (files without a certificate will be skipped).**
 - **Only SHA-256 (files without a hash will be skipped).**
 - **Chỉ MD5 (chế độ bị ngừng hỗ trợ, chỉ dành cho phiên bản Kaspersky Endpoint Security 10 Service Pack 1).**

6. Lưu các thay đổi của bạn.

Bổ sung các tập tin thực thi liên quan đến sự kiện vào danh mục ứng dụng

Để bổ sung các tập tin thực thi liên quan đến các sự kiện Kiểm soát ứng dụng vào danh mục ứng dụng:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong nút **Administration Server** của cây Bảng điều khiển quản trị, chọn thẻ **Events**.
3. Chọn một số sự kiện liên quan đến việc vận hành thành phần Kiểm soát ứng dụng ([Xem các sự kiện từ hoạt động của thành phần Kiểm soát ứng dụng](#), [Xem các sự kiện từ hoạt động thử nghiệm của thành phần Kiểm soát ứng dụng](#)) trong danh sách thả xuống **Event selections**.
4. Nhấn nút **Run selection**.
5. Chọn các sự kiện có tập tin thực thi liên quan bạn muốn thêm vào danh mục ứng dụng.
6. Nhấn phải chuột để mở menu ngữ cảnh cho các sự kiện được chọn và chọn **Add to category**.
7. Trong cửa sổ mở, hãy cấu hình thiết lập của danh mục ứng dụng:
 - Trong phần trên của cửa sổ, chọn một trong các tùy chọn sau:
 - **Add to a new application category.** Chọn tùy chọn này nếu bạn muốn tạo một danh mục ứng dụng mới và bổ sung các tập tin thực thi vào đó.

- **Add to an existing application category.** Chọn tùy chọn này nếu bạn muốn chọn một danh mục ứng dụng hiện có và bổ sung các tập tin thực thi vào đó.
- Trong mục **Rule type**, hãy chọn một trong các tùy chọn sau:
 - **Rules for adding to inclusions.** Chọn tùy chọn này nếu bạn muốn tạo một điều kiện bổ sung các tập tin thực thi vào danh mục ứng dụng.
 - **Rules for adding to exclusions.** Chọn tùy chọn này nếu bạn muốn tạo một điều kiện loại trừ các tập tin thực thi khỏi danh mục ứng dụng.
- Trong mục **Parameter used as a condition**, hãy chọn một trong các tùy chọn sau:
 - **Certificate details (or SHA-256 hashes for files without a certificate).**
 - **Certificate details (files without a certificate will be skipped).**
 - **Only SHA-256 (files without a hash will be skipped).**
 - **Chỉ MD5 (chế độ bị ngừng hỗ trợ, chỉ dành cho phiên bản Kaspersky Endpoint Security 10 Service Pack 1).**

8. Lưu các thay đổi của bạn.

Bổ sung và sửa đổi một quy tắc Kiểm soát ứng dụng sử dụng Kaspersky Security Center

Để thêm hoặc sửa một quy tắc Kiểm soát ứng dụng sử dụng Kaspersky Security Center:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát ứng dụng**.
Ở phần bên phải của cửa sổ, thiết lập của thành phần Kiểm soát ứng dụng sẽ được hiển thị.
6. 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** sẽ được mở ra.

7. Thực hiện một trong các thao tác sau:
 - Nếu bạn muốn tạo một danh mục mới:

a. Nhấn vào **Tạo một danh mục**.

Trình hướng dẫn tạo hạng mục người dùng sẽ được bắt đầu.

b. Làm theo chỉ dẫn của trình hướng dẫn tạo hạng mục người dùng.

c. Trong danh sách thả xuống **Danh mục**, chọn danh mục ứng dụng được tạo.

• Nếu bạn muốn chỉnh sửa một danh mục hiện có:

a. Trong danh sách thả xuống **Danh mục**, chọn danh mục ứng dụng được tạo mà bạn muốn chỉnh sửa.

b. Nhấn vào **Thuộc tính**.

c. Sửa đổi các thiết lập của danh mục ứng dụng được chọn.

d. Lưu các thay đổi của bạn.

e. Trong danh sách thả xuống **Danh mục**, chọn danh mục ứng dụng được tạo mà dựa vào đó bạn muốn tạo một quy tắc.

8. Trong bảng **Các chủ thể và quyền của họ**, nhấn nút **Thêm**.

9. Trong cửa sổ mở ra, hãy chỉ định danh sách người dùng và/hoặc nhóm người dùng mà bạn muốn cấu hình quyền khởi động ứng dụng từ danh mục được chọn.

10. Trong bảng **Các chủ thể và quyền của họ**, bạn cần làm như sau:

- Nếu bạn muốn cho phép người dùng và / hoặc nhóm người dùng khởi động các ứng dụng thuộc danh mục được chọn, chọn hộp kiểm **Cho phép** trong hàng tương ứng.

- Nếu bạn muốn chặn người dùng và / hoặc nhóm người dùng khỏi việc khởi động các ứng dụng thuộc danh mục được chọn, chọn hộp kiểm **Từ chối** trong hàng tương ứng.

11. Chọn hộp kiểm **Từ chối người sử dụng khác** nếu bạn muốn tất cả người dùng không có tên trong cột **Tiêu đề** và không thuộc nhóm người dùng được quy định trong cột **Tiêu đề** bị chặn khỏi việc khởi động các ứng dụng thuộc danh mục được chọn.

12. Nếu bạn muốn Kaspersky Endpoint Security coi các ứng dụng được bao gồm trong danh mục ứng dụng được chọn là các trình cập nhật được tin tưởng, được phép tạo các tập tin thực thi khác có thể chạy sau đó, chọn hộp kiểm **Trình cập nhật được tin tưởng**.

Khi các thiết lập của Kaspersky Endpoint Security được chuyển, danh sách các tập tin thực thi được tạo bởi những cập nhật tin tưởng cũng sẽ được chuyển.

13. Lưu các thay đổi của bạn.

Thay đổi trạng thái của một quy tắc Kiểm soát ứng dụng qua Kaspersky Security Center

Để thay đổi trạng thái của một quy tắc Kiểm soát ứng dụng:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát ứng dụng**.
Ở phần bên phải của cửa sổ, thiết lập của thành phần Kiểm soát ứng dụng sẽ được hiển thị.
6. Trong cột **Trạng thái**, nhấn trái chuột để hiển thị menu ngữ cảnh và chọn một trong các mục sau:
 - **Bật**. Trạng thái này có nghĩa rằng quy tắc này sẽ được sử dụng khi Kiểm soát ứng dụng đang hoạt động.
 - **Tắt**. Trạng thái này có nghĩa rằng quy tắc sẽ bị bỏ qua khi Kiểm soát ứng dụng đang hoạt động.
 - **Kiểm tra**. Trạng thái này có nghĩa Kaspersky Endpoint Security luôn cho phép việc khởi động ứng dụng được quản lý bởi quy tắc này, nhưng sẽ ghi lại thông tin về việc khởi động các ứng dụng đó trong báo cáo.
7. Lưu các thay đổi của bạn.

Xuất và nhập các Quy tắc kiểm soát ứng dụng

Bạn có thể xuất danh sách Quy tắc kiểm soát ứng dụng vào một tập tin XML. Bạn có thể sử dụng chức năng xuất/nhập để sao lưu danh sách Quy tắc kiểm soát ứng dụng hoặc để chuyển danh sách sang máy chủ khác.

Khi xuất và nhập các Quy tắc kiểm soát ứng dụng, hãy nhớ những lưu ý đặc biệt sau:

- Kaspersky Endpoint Security chỉ xuất danh sách các quy tắc cho chế độ Kiểm soát ứng dụng đang hoạt động. Nói cách khác, nếu Kiểm soát ứng dụng đang hoạt động ở chế độ danh sách không được phép, Kaspersky Endpoint Security chỉ xuất các quy tắc cho chế độ này. Để xuất danh sách các quy tắc cho chế độ danh sách được phép, bạn cần chuyển chế độ và chạy lại thao tác xuất.
- Kaspersky Endpoint Security sử dụng các danh mục ứng dụng để các Quy tắc kiểm soát ứng dụng hoạt động được. Khi di chuyển danh sách Quy tắc kiểm soát ứng dụng sang một máy chủ khác, bạn cũng cần di chuyển danh sách các danh mục ứng dụng. Để biết thêm chi tiết về xuất hoặc nhập danh mục ứng dụng, vui lòng tham khảo [Trợ giúp của Kaspersky Security Center](#).

[Cách xuất và nhập danh sách Quy tắc kiểm soát ứng dụng trong Bảng điều khiển quản trị \(MMC\)](#)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát ứng dụng**.
6. Để xuất danh sách Quy tắc kiểm soát ứng dụng:
 - a. Chọn các quy tắc mà bạn muốn xuất. Để chọn nhiều cổng, hãy sử dụng phím **CTRL** hoặc **SHIFT**. Nếu bạn không chọn quy tắc nào, Kaspersky Endpoint Security sẽ xuất tất cả các quy tắc.
 - b. Nhấn liên kết **Xuất**.
 - c. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin XML mà bạn muốn xuất danh sách các quy tắc vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
 - d. Lưu tập tin.
Kaspersky Endpoint Security sẽ xuất danh sách các quy tắc vào tập tin XML.
7. Để xuất một danh sách Quy tắc kiểm soát ứng dụng:
 - a. Nhấn liên kết **Nhập**.
Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách các quy tắc.
 - b. Mở tập tin.
Nếu máy tính đã có danh sách các quy tắc, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.
8. Lưu các thay đổi của bạn.

[Cách xuất và nhập danh sách Quy tắc kiểm soát ứng dụng trong Bảng điều khiển web và Bảng điều khiển đám mây](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Kiểm soát bảo mật** → **Kiểm soát ứng dụng**.
5. Nhấn vào liên kết **Rules Lists Settings**.
6. Chọn danh sách các quy tắc: danh sách ứng dụng được phép và danh sách ứng dụng không được phép.
7. Để xuất danh sách Quy tắc kiểm soát ứng dụng:
 - a. Chọn các quy tắc mà bạn muốn xuất.
 - b. Nhấn vào **Xuất**.
 - c. Xác nhận rằng bạn chỉ muốn xuất các quy tắc đã chọn hoặc xuất toàn bộ danh sách.
 - d. Lưu tập tin.
Kaspersky Endpoint Security sẽ xuất danh sách các quy tắc vào tập tin XML trong thư mục tải xuống mặc định.
8. Để xuất một danh sách Quy tắc kiểm soát ứng dụng:
 - a. Nhấn liên kết **Nhập**.
Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách các quy tắc.
 - b. Mở tập tin.
Nếu máy tính đã có danh sách các quy tắc, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.
9. Lưu các thay đổi của bạn.

Kiểm tra các quy tắc Kiểm soát ứng dụng sử dụng Kaspersky Security Center

Để đảm bảo các quy tắc Kiểm soát ứng dụng không chặn ứng dụng cần cho công việc, bạn nên bật chế độ thử nghiệm cho các quy tắc Kiểm soát ứng dụng và phân tích hoạt động của chúng sau khi tạo các quy tắc mới. Khi chế độ thử nghiệm các Quy tắc Kiểm soát ứng dụng được bật, Kaspersky Endpoint Security sẽ không chặn các ứng dụng mà việc khởi động của chúng bị cấm bởi Kiểm soát ứng dụng, nhưng sẽ thông báo về sự kiện này đến Máy chủ quản trị.

Một phân tích về hoạt động của các Quy tắc Kiểm soát ứng dụng yêu cầu bạn xem lại kết quả của các sự kiện Kiểm soát ứng dụng được báo cáo đến Kaspersky Security Center. Nếu chế độ thử nghiệm không gây ra các sự kiện chặn khởi động cho tất cả các ứng dụng cần để làm việc trên máy tính người dùng, điều này có nghĩa các quy tắc đúng đã được thiết lập. Mặt khác, bạn nên cập nhật các thiết lập của quy tắc mà bạn đã tạo, tạo thêm các quy tắc, hoặc xóa các quy tắc hiện có.

Theo mặc định, Kaspersky Endpoint Security cho phép tất cả các ứng dụng khởi động, ngoại trừ các ứng dụng bị cấm theo quy tắc.

Để bật hoặc tắt kiểm tra các Quy tắc kiểm soát ứng dụng trong Kaspersky Security Center:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát ứng dụng**. Ở phần bên phải của cửa sổ, thiết lập của thành phần Kiểm soát ứng dụng sẽ được hiển thị.
6. Trong danh sách thả xuống **Chế độ kiểm soát**, chọn một trong các mục sau:
 - **Danh sách không được phép.** Nếu mục này được chọn, Kiểm soát ứng dụng sẽ cho phép tất cả người dùng được bắt đầu bất kỳ ứng dụng nào, ngoại trừ các trường hợp thỏa mãn điều kiện trong quy tắc chặn của Kiểm soát ứng dụng.
 - **Danh sách được phép.** Nếu mục này được chọn, Kiểm soát ứng dụng sẽ chặn tất cả người dùng khỏi việc bắt đầu bất kỳ ứng dụng nào, ngoại trừ trong các trường hợp thỏa mãn điều kiện trong quy tắc cho phép của Kiểm soát ứng dụng.
7. Thực hiện một trong các thao tác sau:
 - Nếu bạn muốn bật kiểm tra các Quy tắc kiểm soát ứng dụng, hãy chọn **Quy tắc kiểm tra** trong danh sách thả xuống **Hành động**.
 - Nếu bạn muốn bật Kiểm soát ứng dụng để quản lý việc khởi động ứng dụng trên máy tính người dùng, trong danh sách thả xuống, hãy chọn **Áp dụng quy tắc**.
8. Lưu các thay đổi của bạn.

Xem các sự kiện từ hoạt động thử nghiệm của thành phần Kiểm soát ứng dụng

Để xem các sự kiện kiểm tra của Kiểm soát ứng dụng được nhận bởi Kaspersky Security Center:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong nút **Administration Server** của cây Bảng điều khiển quản trị, chọn thẻ **Events**.
3. Nhấn nút **Create a selection**.

4. Trong cửa sổ mở ra, hãy vào mục **Events**.
5. Nhấn nút **Clear all**.
6. Trong bảng **Các sự kiện**, chọn các hộp kiểm **Cấm khởi động ứng dụng trong chế độ thử nghiệm** và **Cho phép ứng dụng khởi động trong chế độ thử nghiệm**.
7. Lưu các thay đổi của bạn.
8. Trong danh sách thả xuống **Event selections**, nhấn vào lựa chọn được tạo.
9. Nhấn nút **Run selection**.

Xem báo cáo về các ứng dụng bị chặn trong chế độ kiểm tra

Để xem báo cáo về các ứng dụng bị chặn trong chế độ kiểm tra:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong nút **Administration Server** của cây Bảng điều khiển quản trị, chọn thẻ **Reports**.
3. Nhấn nút **New report template**.
Trình hướng dẫn tạo mẫu báo cáo mới sẽ khởi chạy.
4. Làm theo chỉ dẫn của Trình hướng dẫn Mẫu Báo cáo. Ở bước **Selecting the report template type**, chọn **Khác** → **Report on prohibited applications in test mode**.
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 **Reports**.
5. Mở báo cáo bằng cách nhấn đúp vào nó.

Tiến trình tạo báo cáo sẽ được bắt đầu. Báo cáo sẽ được hiển thị trong một cửa sổ mới.

Xem các sự kiện từ hoạt động của thành phần Kiểm soát ứng dụng

Để xem các sự kiện mà Kaspersky Security Center tiếp nhận từ hoạt động của thành phần Kiểm soát ứng dụng:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong nút **Administration Server** của cây Bảng điều khiển quản trị, chọn thẻ **Events**.
3. Nhấn nút **Create a selection**.
4. Trong cửa sổ mở ra, hãy vào mục **Events**.
5. Nhấn nút **Clear all**.
6. Trong bảng **Events**, chọn hộp kiểm **Application startup prohibited**.
7. Lưu các thay đổi của bạn.

8. Trong danh sách thả xuống **Event selections**, nhấn vào lựa chọn được tạo.

9. Nhấn nút **Run selection**.

Xem một báo cáo về các ứng dụng bị chặn

Để xem báo cáo về các ứng dụng bị chặn:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.

2. Trong nút **Administration Server** của cây Bảng điều khiển quản trị, chọn thẻ **Reports**.

3. Nhấn nút **New report template**.

Trình hướng dẫn tạo mẫu báo cáo mới sẽ khởi chạy.

4. Làm theo chỉ dẫn của Trình hướng dẫn Mẫu Báo cáo. Ở bước **Selecting the report template type**, chọn **Khác** → **Report on prohibited applications**.

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 **Reports**.

5. Mở báo cáo bằng cách nhấn đúp vào nó.

Tiến trình tạo báo cáo sẽ được bắt đầu. Báo cáo sẽ được hiển thị trong một cửa sổ mới.

Kiểm tra các Quy tắc Kiểm soát ứng dụng

Để đảm bảo các quy tắc Kiểm soát ứng dụng không chặn ứng dụng cần cho công việc, bạn nên bật chế độ thử nghiệm cho các quy tắc Kiểm soát ứng dụng và phân tích hoạt động của chúng sau khi tạo các quy tắc mới.

Một phân tích về hoạt động của các Quy tắc Kiểm soát ứng dụng yêu cầu bạn xem lại kết quả của các sự kiện Kiểm soát ứng dụng được báo cáo đến Kaspersky Security Center. Nếu chế độ thử nghiệm không gây ra các sự kiện chặn khởi động cho tất cả các ứng dụng cần để làm việc trên máy tính người dùng, điều này có nghĩa các quy tắc đúng đã được thiết lập. Mặt khác, bạn nên cập nhật các thiết lập của quy tắc mà bạn đã tạo, tạo thêm các quy tắc, hoặc xóa các quy tắc hiện có.

Để bật chế độ thử nghiệm các Quy tắc Kiểm soát ứng dụng hoặc chọn một hành động chặn cho Kiểm soát ứng dụng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .

2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát ứng dụng**.

3. Nhấn nút **Ứng dụng bị chặn** hoặc **Các ứng dụng được cho phép**.

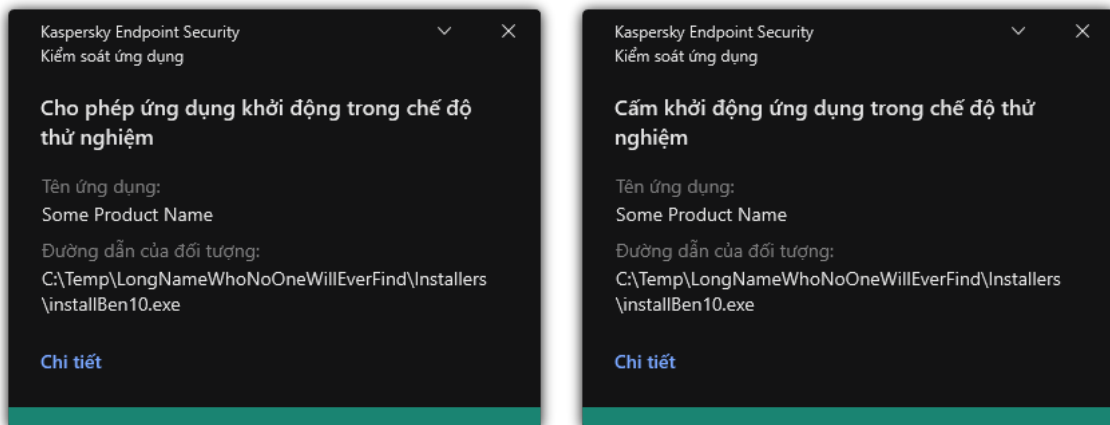
Thao tác này sẽ mở danh sách Quy tắc kiểm soát ứng dụng.

4. Trong cột **Trạng thái**, hãy chọn **Đang kiểm tra**.

Trạng thái này có nghĩa Kaspersky Endpoint Security luôn cho phép việc khởi động ứng dụng được quản lý bởi quy tắc này, nhưng sẽ ghi lại thông tin về việc khởi động các ứng dụng đó trong báo cáo.

5. Lưu các thay đổi của bạn.

Kaspersky Endpoint Security sẽ không chặn các ứng dụng mà việc khởi động của chúng bị cấm bởi thành phần Kiểm soát ứng dụng, nhưng sẽ thông báo về sự kiện này đến Máy chủ quản trị. Bạn cũng có thể [cấu hình hiển thị thông báo](#) về kiểm tra quy tắc trên máy tính của người dùng (xem hình bên dưới).



Thông báo của Kiểm soát ứng dụng ở chế độ thử nghiệm

Quản lý hoạt động ứng dụng

Giám sát hoạt động ứng dụng là một công cụ được thiết kế để xem thông tin về hoạt động của các ứng dụng trên máy tính người dùng theo thời gian thực.

Sử dụng Giám sát hoạt động ứng dụng yêu cầu cài đặt các thành phần Kiểm soát ứng dụng và Phòng chống xâm nhập máy chủ. Nếu các thành phần này chưa được cài đặt thì mục Giám sát hoạt động ứng dụng trong [cửa sổ ứng dụng chính](#) sẽ bị ẩn.

Để tiến hành *Giám sát hoạt động ứng dụng*:

Trong cửa sổ chính của ứng dụng, trong mục **Giám sát**, hãy nhấn vào ô **Giám sát hoạt động ứng dụng**.

Trong cửa sổ này, thông tin về hoạt động của các ứng dụng trên máy tính của người dùng sẽ được hiển thị trên ba thẻ:

- Thẻ **Tất cả ứng dụng** hiển thị thông tin về tất cả các ứng dụng được cài đặt trên máy tính.
- Thẻ **Đang chạy** hiển thị thông tin về mức tiêu thụ tài nguyên máy tính của từng ứng dụng theo thời gian thực. Thông qua thẻ này, bạn cũng có thể tiến hành cấu hình quyền cho một ứng dụng riêng lẻ.
- Thẻ **Chạy lúc khởi động** hiển thị danh sách các ứng dụng được khởi chạy khi hệ điều hành khởi động.

Nếu bạn muốn ẩn thông tin về hoạt động của ứng dụng trên máy tính của người dùng, bạn có thể hạn chế quyền truy cập của người dùng vào công cụ Giám sát hoạt động ứng dụng.

[Cách ẩn Giám sát hoạt động ứng dụng trong giao diện ứng dụng bằng Bảng điều khiển quản trị \(MMC\)](#)



1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Giao diện**.
6. Sử dụng hộp kiểm **Ẩn mục Giám sát hoạt động ứng dụng** để cấp hoặc thu hồi quyền truy cập vào công cụ.
7. Lưu các thay đổi của bạn.

Cách ẩn Giám sát hoạt động ứng dụng trong giao diện ứng dụng bằng Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Thiết lập tổng quát** → **Giao diện**.
5. Sử dụng hộp kiểm **Ẩn mục Giám sát hoạt động ứng dụng** để cấp hoặc thu hồi quyền truy cập vào công cụ.
6. Lưu các thay đổi của bạn.

Quy tắc tạo đại diện tên cho tập tin hoặc thư mục

Đại diện của một tên tập tin hoặc thư mục là đại diện của tên thư mục hoặc tên và phần mở rộng của một tập tin sử dụng các ký tự phổ thông.

Bạn có thể sử dụng các ký tự sau đây để tạo một tên đại diện tập tin hoặc thư mục:


- Ký tự ***** (dấu hoa thị), thay thế cho bất kỳ tập hợp ký tự nào (bao gồm cả tập hợp rỗng). Ví dụ: chuỗi ký tự đại diện `C:*.txt` sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng `txt` nằm trong các thư mục và thư mục con trên ổ (C:).
- Ký tự **?** (dấu hỏi) thay thế bất kỳ ký tự đơn nào, ngoại trừ các ký tự `\` và `/` (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ: đại diện `C:\Folder\???.txt` sẽ bao gồm các đường dẫn đến tất cả các tập tin có trong thư mục `Folder` có phần mở rộng `TXT` và tên có ba ký tự.

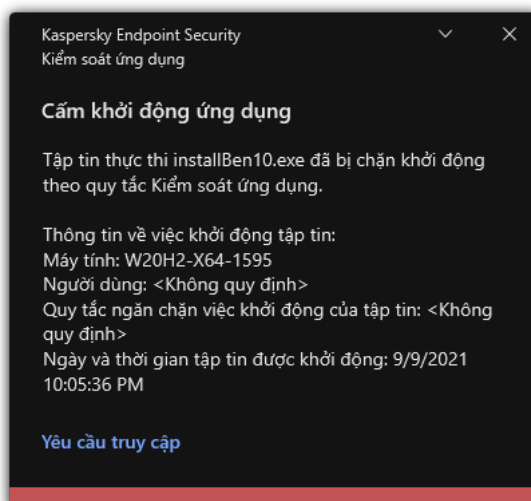
Sửa mẫu thông điệp Kiểm soát ứng dụng

Khi một người dùng cố gắng khởi động một ứng dụng bị chặn bởi quy tắc Kiểm soát ứng dụng, 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. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát ứng dụng**.
3. Trong mục **Mẫu tin nhắn về việc chặn ứng dụng**, hãy cấu hình các mẫu tin nhắn Kiểm soát ứng dụng:
 - **Tin nhắn về hoạt động chặn** Mẫu thông báo được hiển thị khi kích hoạt một quy tắc Kiểm soát ứng dụng chặn ứng dụng khởi chạy. Thông báo về một ứng dụng bị chặn được hiển thị trong hình bên dưới.
Bạn không thể cấu hình các mẫu tin nhắn cho Kiểm soát ứng dụng trong [chế độ thử nghiệm](#). Kiểm soát ứng dụng ở chế độ thử nghiệm sẽ hiển thị các thông báo cài đặt sẵn.
 - **Thông điệp đến quản trị viên** Mẫu tin nhắn mà người dùng có thể gửi cho quản trị viên mạng LAN doanh nghiệp nếu người dùng tin rằng một ứng dụng bị chặn do nhầm lẫn. Sau khi người dùng yêu cầu cung cấp quyền truy cập, Kaspersky Endpoint Security sẽ gửi một sự kiện đến Kaspersky Security Center: **Thông báo chặn việc khởi chạy ứng dụng gửi đến quản trị viên**. Phần mô tả sự kiện chứa một thông báo cho quản trị viên với các biến được thay thế. Bạn có thể xem các sự kiện này trong bảng điều khiển Kaspersky Security Center bằng cách sử dụng lựa chọn sự kiện được định sẵn **User requests**. Nếu tổ chức của bạn chưa triển khai Kaspersky Security Center hoặc không có kết nối với Máy chủ quản trị thì ứng dụng sẽ gửi một thông báo cho quản trị viên tới địa chỉ email được chỉ định.
4. Lưu các thay đổi của bạn.



Thông báo của Kiểm soát ứng dụng

Biện pháp tốt nhất để triển khai danh sách các ứng dụng được phép

Khi lập kế hoạch triển khai danh sách các ứng dụng được phép, bạn nên thực hiện các việc sau:

1. Tạo thành các loại nhóm sau:

- Nhóm người dùng. Nhóm người dùng mà bạn muốn cho phép sử dụng các bộ ứng dụng khác nhau.
- Nhóm quản trị. Một hoặc nhiều nhóm máy tính mà Kaspersky Security Center sẽ áp dụng danh sách các ứng dụng được phép. Cần tạo nhiều nhóm máy tính nếu thiết lập danh sách được phép khác nhau được sử dụng cho các nhóm đó.

2. Tạo một nhóm ứng dụng phải luôn được phép khởi động.

Trước khi tạo một danh sách, bạn nên làm các việc sau:

a. Chạy tác vụ kiểm kê.

Bạn có thể xem thông tin về việc tạo, cấu hình lại và khởi động một tác vụ kiểm kê trong mục Quản lý tác vụ.

b. Xem [danh sách các tập tin thực thi](#).

Cấu hình chế độ danh sách được phép cho các ứng dụng

Khi cấu hình chế độ danh sách được phép, bạn nên thực hiện các việc sau:

1. Tạo [các danh mục ứng dụng](#) chứa những ứng dụng phải luôn được phép khởi động.

Bạn có thể chọn một trong các phương thức tạo danh mục ứng dụng sau:

- **Category with content added manually.** Bạn có thể thêm thủ công vào danh mục này bằng cách sử dụng các điều kiện sau:

- Siêu dữ liệu của tập tin. Kaspersky Security Center sẽ thêm tất cả các tập tin thực thi đi kèm với siêu dữ liệu được chỉ định vào danh mục ứng dụng.
- Mã băm tập tin. Kaspersky Security Center sẽ thêm tất cả các tập tin thực thi có mã băm được chỉ định vào danh mục ứng dụng.

Việc sử dụng điều kiện này sẽ loại trừ khả năng tự động cài đặt các bản cập nhật bởi các phiên bản khác nhau của tập tin sẽ có hash khác nhau.

- Chứng chỉ tập tin. Kaspersky Security Center sẽ thêm tất cả các tập tin thực thi có chứng chỉ được chỉ định vào danh mục ứng dụng.
- Danh mục KL. Kaspersky Security Center sẽ thêm tất cả các ứng dụng thuộc danh mục KL được quy định vào danh mục ứng dụng.
- Thư mục ứng dụng. Kaspersky Security Center sẽ thêm tất cả các tập tin thực thi từ thư mục này vào danh mục tùy chỉnh đó.

Việc sử dụng điều kiện thư mục Ứng dụng có thể là không an toàn bởi bất kỳ ứng dụng nào từ thư mục được quy định cũng sẽ được phép khởi động. Bạn chỉ nên áp dụng các quy tắc sử dụng danh mục ứng dụng với điều kiện thư mục Ứng dụng cho những người dùng bắt buộc phải cho phép cài đặt tự động các bản cập nhật.

- **Category that includes executable files from a specific folder.** Bạn có thể quy định một thư mục mà từ đó các tập tin thực thi sẽ tự động được gán vào danh mục ứng dụng được tạo.
- **Category that includes executable files from selected devices.** Bạn có thể quy định một máy tính mà từ đó các tập tin thực thi sẽ tự động được gán vào danh mục ứng dụng được tạo.

Khi sử dụng phương thức tạo danh mục ứng dụng này, Kaspersky Security Center sẽ tiếp nhận thông tin về các ứng dụng trên máy tính từ thư mục **Executable files**.

2. [Chọn chế độ danh sách được phép](#) cho thành phần Kiểm soát ứng dụng.
3. [Tạo quy tắc Kiểm soát ứng dụng](#) sử dụng danh mục ứng dụng được tạo.

Quy tắc **Tập tin ảnh hoàn hảo** và quy tắc **Trình cập nhật được tin tưởng** ban đầu được định nghĩa cho chế độ Danh sách được phép. Các Quy tắc kiểm soát ứng dụng này tương ứng với các danh mục KL. Danh mục KL "Tập tin ảnh hoàn hảo" bao gồm các chương trình đảm bảo hoạt động bình thường của hệ điều hành. Danh mục KL "Trình cập nhật được tin tưởng" bao gồm các trình cập nhật cho hầu hết những nhà cung cấp phần mềm uy tín. Bạn không thể xóa các quy tắc này. Cấu hình của các quy tắc này không thể được sửa đổi. Theo mặc định, quy tắc **Tập tin ảnh hoàn hảo** 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.

4. Xác định các ứng dụng mà việc tự động cài đặt bản cập nhật phải được cho phép.

Bạn có thể cho phép tự động cài đặt các bản cập nhật bằng một trong những cách sau đây:

- Quy định một danh sách mở rộng các ứng dụng được cho phép bằng cách cho phép khởi động tất cả các ứng dụng thuộc một danh mục KL bất kỳ.
- Quy định một danh sách mở rộng các ứng dụng được cho phép bằng cách cho phép khởi động tất cả các ứng dụng được ký duyệt chứng chỉ.
Để cho phép khởi động tất cả các ứng dụng được ký duyệt chứng chỉ, bạn có thể tạo một danh mục với điều kiện chứng chỉ chỉ sử dụng tham số **Tiêu đề** với giá trị *.
- Đối với quy tắc kiểm soát Ứng dụng, chọn tham số **Trình cập nhật được tin tưởng**. Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ coi các ứng dụng được bao gồm trong quy tắc này là Trình cập nhật được tin tưởng. Kaspersky Endpoint Security sẽ cho phép việc khởi động các ứng dụng đã được cài đặt hoặc cập nhật bởi các ứng dụng được bao gồm trong quy tắc này, nếu không có quy tắc chặn nào được áp đặt cho các ứng dụng đó.

Khi các thiết lập của Kaspersky Endpoint Security được chuyển, danh sách các tập tin thực thi được tạo bởi những cập nhật tin tưởng cũng sẽ được chuyển.

- Tạo một thư mục và đặt vào đó tập tin thực thi của các ứng dụng mà bạn muốn cho phép tự động cài đặt bản cập nhật. Sau đó tạo một danh mục ứng dụng với điều kiện "Thư mục ứng dụng" và quy định đường dẫn đến thư mục đó. Sau đó tạo một quy tắc cho phép và chọn danh mục này.

Việc sử dụng điều kiện thư mục Ứng dụng có thể là không an toàn bởi bất kỳ ứng dụng nào từ thư mục được quy định cũng sẽ được phép khởi động. Bạn chỉ nên áp dụng các quy tắc sử dụng danh mục ứng dụng với điều kiện thư mục Ứng dụng cho những người dùng bắt buộc phải cho phép cài đặt tự động các bản cập nhật.

Kiểm tra chế độ danh sách được phép

Để đảm bảo các quy tắc Kiểm soát ứng dụng không chặn ứng dụng cần cho công việc, bạn nên bật chế độ thử nghiệm cho các quy tắc Kiểm soát ứng dụng và phân tích hoạt động của chúng sau khi tạo các quy tắc mới. Khi chế độ thử nghiệm được bật, Kaspersky Endpoint Security sẽ không chặn các ứng dụng mà việc khởi động của chúng bị cấm bởi các quy tắc Kiểm soát ứng dụng, nhưng sẽ thông báo về sự kiện này đến Máy chủ quản trị.

Khi thử nghiệm chế độ danh sách được phép, bạn nên thực hiện các việc sau:

1. Xác định thời gian thử nghiệm (từ vài ngày đến hai tháng).
2. Bật [chế độ thử nghiệm các quy tắc Kiểm soát ứng dụng](#).
3. Xem xét [các sự kiện xảy ra từ việc kiểm tra hoạt động của Quản lý ứng dụng](#) và [báo cáo về các ứng dụng bị chặn trong chế độ kiểm tra](#) để phân tích kết quả kiểm tra.
4. Dựa trên kết quả phân tích, thay đổi các thiết lập của chế độ danh sách được phép.
Cụ thể, dựa trên kết quả kiểm tra, bạn có thể thêm [các tệp thực thi liên quan đến các sự kiện vào danh mục ứng dụng](#).

Hỗ trợ cho chế độ danh sách được phép

Sau khi [chọn một hành động chặn cho Kiểm soát ứng dụng](#), bạn nên tiếp tục hỗ trợ chế độ danh sách được phép bằng cách thực hiện các hành động sau đây:

- [Xem xét các sự kiện xảy ra từ việc vận hành Kiểm soát ứng dụng](#) và [báo cáo về các lần chạy bị chặn trong thử nghiệm](#) để phân tích hiệu quả của Kiểm soát ứng dụng.
- Phân tích yêu cầu truy cập ứng dụng của người dùng.
- Phân tích các tệp tin thực thi không quen thuộc bằng cách kiểm tra danh tiếng của chúng trong [Kaspersky Security Network](#).
- Trước khi cài đặt bản cập nhật cho hệ điều hành hoặc cho phần mềm, cài đặt các bản cập nhật đó trên một nhóm máy tính thử nghiệm để kiểm tra cách chúng sẽ được xử lý bởi quy tắc Kiểm soát ứng dụng.
- Bổ sung các ứng dụng cần thiết vào danh mục được sử dụng trong quy tắc Kiểm soát ứng dụng.


Giám sát công mạng

Trong quá trình hoạt động của Kaspersky Endpoint Security, các thành phần [Kiểm soát Web](#), [Bảo vệ mỗi đe dọa thư điện tử](#) và [Bảo vệ mỗi đe dọa web](#) sẽ giám sát các luồng dữ liệu được truyền tải qua các giao thức cụ thể và đi qua những cổng TCP và UDP mở cụ thể trên máy tính người dùng. Ví dụ, thành phần Bảo vệ mỗi đe dọa thư điện tử sẽ phân tích thông tin được truyền tải qua SMTP, trong khi thành phần Bảo vệ mỗi đe dọa web phân tích thông tin được truyền tải qua HTTP và FTP.

Kaspersky Endpoint Security sẽ chia các cổng TCP và UDP của máy tính người dùng thành vài nhóm, tùy thuộc vào khả năng chúng bị xâm nhập. Một số cổng mạng được dành riêng cho các dịch vụ có lỗ hổng bảo mật. Bạn được khuyến cáo giám sát các cổng này kỹ lưỡng hơn bởi vì chúng có khả năng lớn hơn được chọn làm mục tiêu tấn công mạng. 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 Bảo vệ mỗi đe dọa thư điện tử và Bảo vệ mỗi đe dọa web trong hoạt động giám sát lưu lượng mạng.


Bật tính năng giám sát tất cả cổng mạng

Để bật tính năng giám sát tất cả cổng mạng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Thiết lập mạng**.
3. Trong mục **Giám sát các cổng**, hãy chọn **Giám sát tất cả các cổng mạng**.
4. Lưu các thay đổi của bạn.

Tạo một danh sách cổng mạng bị giám sát

Để tạo một danh sách cổng mạng bị giám sát:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Thiết lập mạng**.
3. Trong mục **Giám sát các cổng**, hãy chọn **Chỉ giám sát các cổng mạng được chọn**.
4. Nhấn vào **Lựa chọn**.

Thao tác này sẽ mở một danh sách cổng mạng thường được sử dụng để truyền tải email và lưu lượng mạng. Danh sách cổng mạng này được bao gồm trong gói Kaspersky Endpoint Security.

5. Sử dụng nút bật/tắt trong cột **Trạng thái** để bật hoặc tắt tính năng giám sát cổng mạng.
6. Nếu cổng mạng không được hiển thị trong danh sách cổng mạng, hãy thêm nó bằng cách:
 - a. Nhấn vào **Thêm**.
 - b. Trong cửa sổ mở ra, hãy nhập số hiệu cổng mạng và mô tả ngắn gọn.
 - c. Đặt trạng thái **Hoạt động** hoặc **Không hoạt động** để giám sát cổng mạng.

7. Lưu các thay đổi của bạn.


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 cổng mạng bị giám sát. Để bảo vệ các kết nối như vậy, hãy [bật tính năng giám sát tất cả cổng mạng](#) hoặc [cấu hình kiểm soát cổng mạng cho các ứng dụng thiết lập kết nối FTP](#).

Tạo một danh sách ứng dụng được giám sát tất cả cổng mạng

Bạn có thể tạo một danh sách ứng dụng sẽ được Kaspersky Endpoint Security giám sát tất cả 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 cổng mạng.

Để tạo một danh sách ứng dụng được giám sát tất cả cổng mạng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Thiết lập mạng**.
3. Trong mục **Giám sát các cổng**, hãy chọn **Chỉ giám sát các cổng mạng được chọn**.
4. Chọn hộp kiểm **Giám sát tất cả các cổng cho ứng dụng từ danh sách được khuyến nghị bởi Kaspersky**.
Nếu hộp kiểm này được lựa chọn, Kaspersky Endpoint Security sẽ giám sát tất cả các cổng cho các ứng dụng sau đây:
 - Adobe Reader.
 - Apple Application Support.
 - Google Chrome.
 - Microsoft Edge.
 - Mozilla Firefox.
 - Internet Explorer.
 - Java.
 - mIRC.
 - Opera.
 - Pidgin.
 - Safari.

- Mail.ru Agent.
 - Yandex Browser.
5. Chọn hộp kiểm **Theo dõi tất cả các cổng của những ứng dụng được chỉ định**.
 6. Nhấn vào **Lựa chọn**.
Thao tác này sẽ mở danh sách ứng dụng được Kaspersky Endpoint Security giám sát cổng mạng.
 7. Sử dụng nút bật/tắt trong cột **Trạng thái** để bật hoặc tắt tính năng giám sát cổng mạng.
 8. Nếu một ứng dụng không được bao gồm trong danh sách ứng dụng, hãy bổ sung chúng bằng cách sau:
 - a. Nhấn vào **Thêm**.
 - b. Trong cửa sổ mở ra, hãy nhập đường dẫn đến tập tin thực thi của ứng dụng kèm một mô tả ngắn gọn.
 - c. Đặt trạng thái **Hoạt động** hoặc **Không hoạt động** để giám sát các cổng mạng.
 9. Lưu các thay đổi của bạn.

Xuất và nhập danh sách các cổng được giám sát

Kaspersky Endpoint Security sử dụng các danh sách sau để giám sát cổng mạng: danh sách cổng mạng và danh sách các ứng dụng có cổng được Kaspersky Endpoint Security giám sát. Bạn có thể xuất danh sách các cổng được giám sát vào một tập tin XML. Sau đó, bạn có thể sửa đổi tập tin, ví dụ như thêm một số lượng lớn các cổng có cùng mô tả. Bạn cũng có thể sử dụng chức năng xuất/nhập để sao lưu danh sách các cổng được giám sát hoặc để chuyển danh sách sang máy chủ khác.

[Cách xuất và nhập danh sách các cổng được giám sát trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Thiết lập mạng**.
6. Trong mục **Giám sát các cổng**, hãy chọn **Chỉ giám sát các cổng mạng được chọn**.
7. Nhấn vào **Thiết lập**.

Cửa sổ **Cổng mạng** sẽ được mở ra. Cửa sổ **Cổng mạng** hiển thị một danh sách cổng mạng thường được sử dụng để truyền tải email và lưu lượng mạng. Danh sách cổng mạng này được bao gồm trong gói Kaspersky Endpoint Security.
8. Để xuất danh sách cổng mạng:
 - a. Trong danh sách cổng mạng, hãy chọn các cổng mà bạn muốn xuất. Để chọn nhiều cổng, hãy sử dụng phím **CTRL** hoặc **SHIFT**.

Nếu bạn không chọn cổng nào, Kaspersky Endpoint Security sẽ xuất tất cả các cổng.
 - b. Nhấn vào **Xuất**.
 - c. Trong cửa sổ mở ra, hãy nhập tên của tập tin XML mà bạn muốn xuất danh sách cổng mạng vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
 - d. Lưu tập tin.

Kaspersky Endpoint Security sẽ xuất toàn bộ danh sách cổng mạng vào tập tin XML.
9. Để xuất danh sách các ứng dụng có cổng được Kaspersky Endpoint Security giám sát:
 - a. Chọn hộp kiểm **Theo dõi tất cả các cổng của những ứng dụng được chỉ định**.
 - b. Trong danh sách ứng dụng, hãy chọn ứng dụng bạn muốn xuất. Để chọn nhiều cổng, hãy sử dụng phím **CTRL** hoặc **SHIFT**.

Nếu bạn không chọn ứng dụng nào, Kaspersky Endpoint Security sẽ xuất tất cả các ứng dụng.
 - c. Nhấn vào **Xuất**.
 - d. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin XML mà bạn muốn xuất danh sách các ứng dụng vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
 - e. Lưu tập tin.

Kaspersky Endpoint Security sẽ xuất toàn bộ danh sách các ứng dụng vào tập tin XML.
10. Để nhập danh sách cổng mạng:
 - a. Trong danh sách cổng mạng, hãy nhấn nút **Nhập**.

Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách cổng mạng.

b. Mở tập tin.

Nếu máy tính đã có danh sách cổng mạng, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.

11. Để nhập một danh sách các ứng dụng có cổng được Kaspersky Endpoint Security giám sát:

a. Trong danh sách các ứng dụng, hãy nhấn nút **Nhập**.

Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách ứng dụng.

b. Mở tập tin.

Nếu máy tính đã có danh sách các ứng dụng, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.

12. Lưu các thay đổi của bạn.

[Cách xuất/nhập danh sách các cổng được giám sát trong Bảng điều khiển web và Bảng điều khiển đám mây](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Thiết lập tổng quát** → **Thiết lập mạng**.
5. Để xuất danh sách cổng mạng:
 - a. Trong mục **Giám sát các cổng**, hãy chọn **Chỉ giám sát các cổng mạng được chọn**.
 - b. Nhấn vào liên kết **N cổng đã chọn**.
Cửa sổ **Cổng mạng** sẽ được mở ra. Cửa sổ **Cổng mạng** hiển thị một danh sách cổng mạng thường được sử dụng để truyền tải email và lưu lượng mạng. Danh sách cổng mạng này được bao gồm trong gói Kaspersky Endpoint Security.
 - c. Trong danh sách cổng mạng, hãy chọn các cổng mà bạn muốn xuất.
 - d. Nhấn vào **Xuất**.
 - e. Trong cửa sổ mở ra, hãy nhập tên của tập tin XML mà bạn muốn xuất danh sách cổng mạng vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
 - f. Lưu tập tin.
Kaspersky Endpoint Security sẽ xuất toàn bộ danh sách cổng mạng vào tập tin XML.
6. Để xuất danh sách các ứng dụng có cổng được Kaspersky Endpoint Security giám sát:
 - a. Trong mục **Giám sát các cổng**, hãy chọn hộp kiểm **Theo dõi tất cả các cổng của những ứng dụng được chỉ định**.
 - b. Nhấn vào liên kết **N ứng dụng đã chọn**.
 - c. Trong danh sách ứng dụng, hãy chọn ứng dụng bạn muốn xuất.
 - d. Nhấn vào **Xuất**.
 - e. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin XML mà bạn muốn xuất danh sách các ứng dụng vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
 - f. Lưu tập tin.
Kaspersky Endpoint Security sẽ xuất toàn bộ danh sách các ứng dụng vào tập tin XML.
7. Để nhập danh sách cổng mạng:
 - a. Trong danh sách cổng mạng, hãy nhấn nút **Nhập**.
Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách cổng mạng.
 - b. Mở tập tin.
Nếu máy tính đã có danh sách cổng mạng, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.

8. Để nhập một danh sách các ứng dụng có cổng được Kaspersky Endpoint Security giám sát:

a. Trong danh sách các ứng dụng, hãy nhấn nút **Nhập**.

Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách ứng dụng.

b. Mở tập tin.

Nếu máy tính đã có danh sách các ứng dụng, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.

9. Lưu các thay đổi của bạn.

Bảo vệ bằng mật khẩu

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. Bảo vệ bằng mật khẩu cho phép bạn hạn chế quyền truy cập của người dùng đến Kaspersky Endpoint Security theo các quyền truy cập được cấp cho họ (ví dụ, quyền thoát ứng dụng).

Nếu người dùng đó đã khởi chạy phiên Windows (*người dùng phiên*) có quyền thực hiện hành động thì Kaspersky Endpoint Security không yêu cầu tên người dùng và mật khẩu hoặc mật khẩu tạm thời. Người dùng đó sẽ nhận được quyền truy cập đến Kaspersky Endpoint Security theo các quyền được cấp.

Nếu người dùng phiên không có quyền thực hiện một hành động, người dùng đó có thể lấy quyền truy cập đến ứng dụng theo các cách sau:

- Nhập tên người dùng và mật khẩu.

Phương thức này phù hợp cho hoạt động hàng ngày. Để thực hiện một hành động được bảo vệ bằng mật khẩu, bạn phải nhập thông tin đăng nhập tài khoản miền của người dùng kèm theo quyền cần thiết. Trong trường hợp này, máy tính phải ở trong miền đó. Nếu máy tính không ở trong miền, bạn có thể sử dụng tài khoản KLocalAdmin.

- Nhập một mật khẩu tạm thời.

Phương thức này phù hợp để cấp quyền truy cập tạm thời để thực hiện hành động bị chặn (ví dụ, thoát ứng dụng) cho người dùng bên ngoài mạng doanh nghiệp. Khi một mật khẩu tạm thời hết hạn hoặc một phiên kết thúc, Kaspersky Endpoint Security sẽ hoàn tác các thiết lập về trạng thái trước đó.

Nếu người dùng cố gắng thực hiện một hành động được bảo vệ bằng mật khẩu, Kaspersky Endpoint Security sẽ nhắc người dùng nhập vào tên người dùng và mật khẩu hoặc mật khẩu tạm thời (xem hình dưới đây).

Trong cửa sổ nhập mật khẩu, bạn chỉ có thể chuyển đổi ngôn ngữ bằng cách nhấn **ALT+SHIFT**. Sử dụng các phím tắt khác, ngay cả khi chúng được cấu hình trong hệ điều hành, sẽ không có tác dụng để chuyển đổi ngôn ngữ.

Kaspersky

Bạn có chắc chắn muốn thay đổi thiết lập không?

Tên người dùng:

Giá trị mặc định của tên người dùng là: KLocalAdmin.

Nhập mật khẩu:

Không nhắc xác nhận trong lần tiếp theo:

Để chuyển đổi qua lại giữa các ngôn ngữ nhập liệu, hãy dùng **ENU**

Hỏi mật khẩu truy cập Kaspersky Endpoint Security

Tên người dùng và mật khẩu

Để truy cập Kaspersky Endpoint Security, bạn phải nhập thông tin tài khoản tên miền của mình. Bảo vệ bằng mật khẩu hỗ trợ các tài khoản sau:

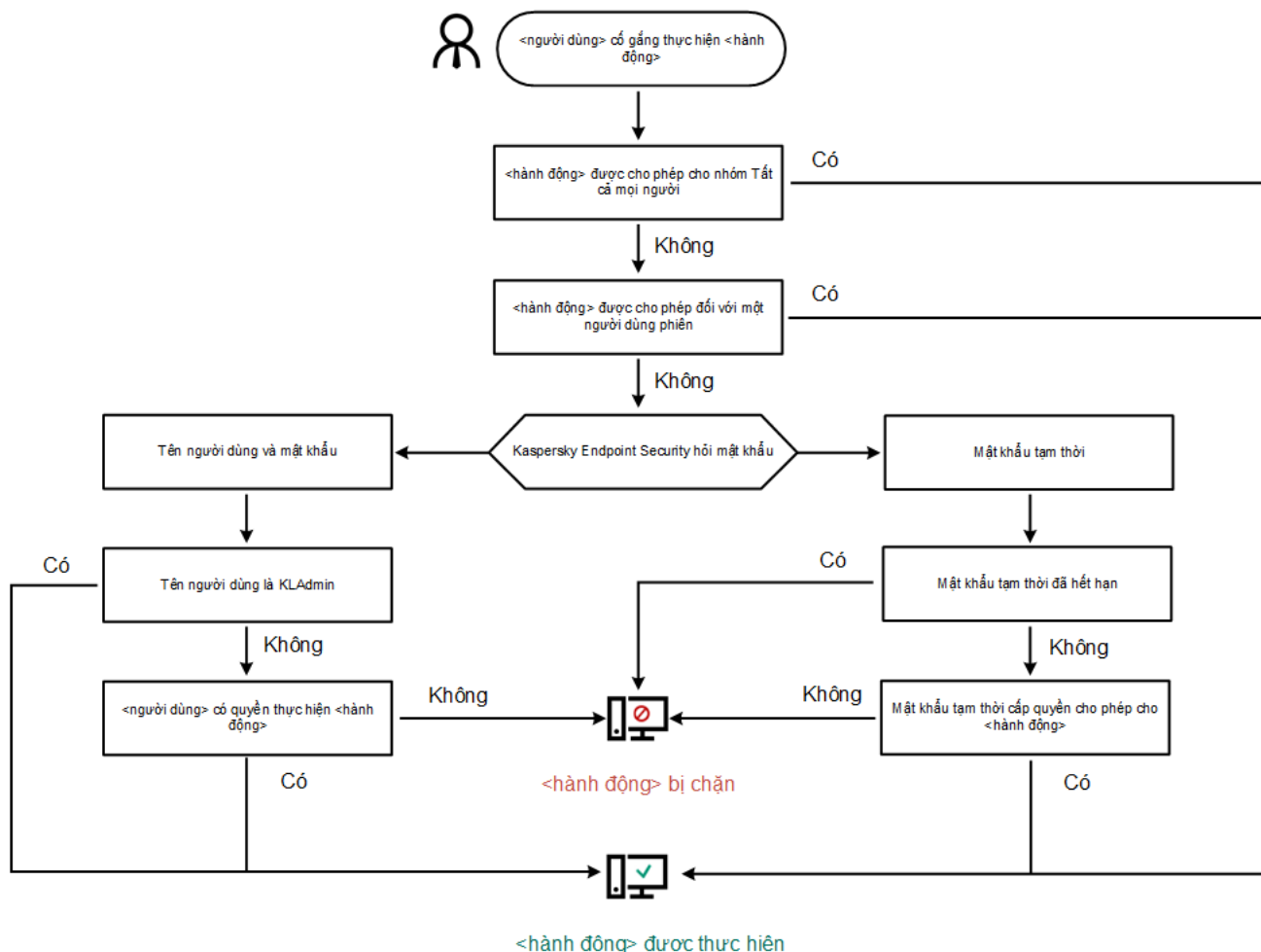
- **KLAdmin.** Một tài khoản Quản trị viên có quyền truy cập không hạn chế đến Kaspersky Endpoint Security. Tài khoản KLAdmin có quyền thực hiện mọi hành động được bảo vệ bởi mật khẩu. Quyền truy cập cho tài khoản KLAdmin không thể bị thu hồi. Khi bạn bật bảo vệ bằng mật khẩu, Kaspersky Endpoint Security sẽ nhắc bạn đặt một mật khẩu cho tài khoản KLAdmin.
- **Nhóm Mọi người.** Một nhóm Windows tích hợp bao gồm tất cả người dùng trong mạng doanh nghiệp. Người dùng trong nhóm Mọi người có thể truy cập ứng dụng theo các quyền truy cập được cấp cho họ.
- **Người dùng cá nhân hoặc nhóm.** Các tài khoản người dùng mà bạn có thể cấu hình quyền truy cập cá nhân. Ví dụ, nếu một hành động bị chặn cho nhóm Mọi người, bạn có thể cho phép hành động này cho một người dùng cá nhân hoặc một nhóm.
- **Người dùng phiên.** Tài khoản của người dùng đã bắt đầu phiên Windows. Bạn có thể chuyển sang một người dùng phiên khác khi được hỏi mật khẩu (hộp kiểm **Lưu mật khẩu cho phiên làm việc hiện tại**). Trong trường hợp này, Kaspersky Endpoint Security sẽ coi người dùng có thông tin tài khoản được nhập là người dùng phiên, thay cho người dùng đã bắt đầu phiên Windows.

Mật khẩu tạm thời

Một mật khẩu tạm thời có thể được sử dụng để cấp quyền truy cập tạm thời đến Kaspersky Endpoint Security cho một máy tính riêng biệt ngoài mạng doanh nghiệp. Quản trị viên tạo một mật khẩu tạm thời cho một máy tính riêng biệt trong thuộc tính máy tính trong Kaspersky Security Center. Quản trị viên lựa chọn hành động sẽ được bảo vệ bằng mật khẩu tạm thời, và quy định thời hạn hiệu lực của mật khẩu tạm thời đó.

Thuật toán hoạt động của bảo vệ bằng mật khẩu

Kaspersky Endpoint Security quyết định liệu có cho phép hay chặn một hành động được bảo vệ bằng mật khẩu dựa trên thuật toán sau (xem hình dưới đây).




Thuật toán hoạt động của bảo vệ bằng mật khẩu

Bật Bảo vệ bằng mật khẩu

Bảo vệ bằng mật khẩu cho phép bạn hạn chế quyền truy cập của người dùng đến Kaspersky Endpoint Security theo các quyền truy cập được cấp cho họ (ví dụ, quyền thoát ứng dụng).

Để bật bảo vệ bằng mật khẩu:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, chọn **Thiết lập tổng quát** → **Giao diện**.
3. Sử dụng nút bật/tắt **Bảo vệ bằng mật khẩu** để bật hoặc tắt thành phần.
4. Quy định mật khẩu cho tài khoản KAdmin và xác nhận nó.
Tài khoản KAdmin có quyền thực hiện mọi hành động được bảo vệ bởi mật khẩu.

Nếu máy tính của bạn đang sử dụng một chính sách, Quản trị viên có thể đặt lại mật khẩu cho tài khoản KAdmin trong thuộc tính chính sách. Nếu máy tính không được kết nối với Kaspersky Security Center và bạn đã quên mật khẩu cho tài khoản KAdmin, bạn sẽ không thể phục hồi mật khẩu.

5. Thiết lập quyền truy cập cho tất cả người dùng trong mạng doanh nghiệp:

a. Trong bảng tài khoản, hãy nhấn nút **Chỉnh sửa** để mở danh sách quyền truy cập cho nhóm Mọi người.

Nhóm Mọi người là một nhóm Windows tích hợp bao gồm tất cả người dùng trong mạng doanh nghiệp.

b. Chọn hộp kiểm cạnh các hành động mà người dùng sẽ được phép thực hiện mà không cần nhập mật khẩu.

Nếu một hộp kiểm bị xóa, người dùng sẽ bị chặn thực hiện hành động. Ví dụ, nếu hộp kiểm cạnh quyền truy cập **Thoát khỏi ứng dụng** bị xóa, bạn sẽ chỉ có thể thoát ứng dụng nếu bạn đăng nhập là KAdmin, hoặc là một [người dùng cá nhân có quyền truy cập cần thiết](#), hoặc nếu bạn nhập một [mật khẩu tạm thời](#).

Các quyền được bảo vệ bằng mật khẩu có một số [khía cạnh mà bạn cần cân nhắc](#). Đảm bảo tất cả các điều kiện truy cập để truy cập Kaspersky Endpoint Security đều được đáp ứng.

6. Lưu các thay đổi của bạn.

Khi bảo vệ bằng mật khẩu được bật, ứng dụng sẽ giới hạn quyền truy cập của người dùng đến Kaspersky Endpoint Security ở các quyền được cấp cho nhóm Mọi người. Bạn chỉ có thể thực hiện các hành động bị chặn cho nhóm Mọi người nếu bạn sử dụng tài khoản KAdmin, [một tài khoản khác được cấp quyền truy cập cần thiết](#), hoặc nếu bạn nhập một [mật khẩu tạm thời](#).

Bạn chỉ có thể tắt Bảo vệ bằng mật khẩu nếu bạn đăng nhập là KAdmin. 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.


Trong quá trình kiểm tra mật khẩu, bạn có thể chọn hộp kiểm **Lưu mật khẩu cho phiên làm việc hiện tại**. Trong trường hợp này, Kaspersky Endpoint Security sẽ không hỏi mật khẩu khi một người dùng cố gắng thực hiện một hành động được bảo vệ bằng mật khẩu khác trong suốt thời gian của phiên làm việc.

Cấp quyền truy cập cho người dùng cá nhân hoặc nhóm

Bạn có thể cấp quyền truy cập Kaspersky Endpoint Security cho người dùng cá nhân hoặc nhóm. Ví dụ, nếu hành động thoát ứng dụng bị chặn cho nhóm Mọi người, bạn có thể cấp quyền **Thoát khỏi ứng dụng** cho một người dùng cá nhân. Khi đó, bạn chỉ có thể thoát ứng dụng nếu bạn đăng nhập là người dùng đó hoặc là KAdmin.

Bạn chỉ có thể sử dụng thông tin đăng nhập tài khoản để truy cập ứng dụng nếu máy tính ở trong miền. Nếu máy tính không ở trong miền, bạn có thể sử dụng tài khoản KAdmin hoặc [mật khẩu tạm thời](#).

Để cấp quyền truy cập cho người dùng cá nhân hoặc nhóm:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, chọn **Thiết lập tổng quát** → **Giao diện**.
3. Trong bảng tài khoản, hãy nhấn vào **Thêm**.
4. Trong cửa sổ mở ra, hãy nhấn nút **Chọn người dùng hoặc nhóm**.

Hộp thoại Chọn người dùng hoặc nhóm tiêu chuẩn sẽ mở ra.

5. Chọn một người dùng hoặc nhóm trong Active Directory và xác nhận lựa chọn của bạn.
6. Trong danh sách **Quyền**, chọn hộp kiểm cạnh tên của các hành động mà người dùng hoặc nhóm được chọn có thể thực hiện mà không bị cần nhập mật khẩu.

Nếu một hộp kiểm bị xóa, người dùng sẽ bị chặn thực hiện hành động. Ví dụ, nếu hộp kiểm cạnh quyền truy cập **Thoát khỏi ứng dụng** bị xóa, bạn sẽ chỉ có thể thoát ứng dụng nếu bạn đăng nhập là KAdmin, hoặc là một [người dùng cá nhân có quyền truy cập cần thiết](#), hoặc nếu bạn nhập một [mật khẩu tạm thời](#).

Các quyền được bảo vệ bằng mật khẩu có một số [khía cạnh mà bạn cần cân nhắc](#). Đảm bảo tất cả các điều kiện truy cập để truy cập Kaspersky Endpoint Security đều được đáp ứng.

7. Lưu các thay đổi của bạn.

Khi đó, nếu quyền truy cập ứng dụng bị chặn cho nhóm Mọi người, người dùng sẽ được cấp quyền truy cập Kaspersky Endpoint Security theo quyền truy cập cá nhân của người dùng đó.

Sử dụng một mật khẩu tạm thời để cấp quyền truy cập

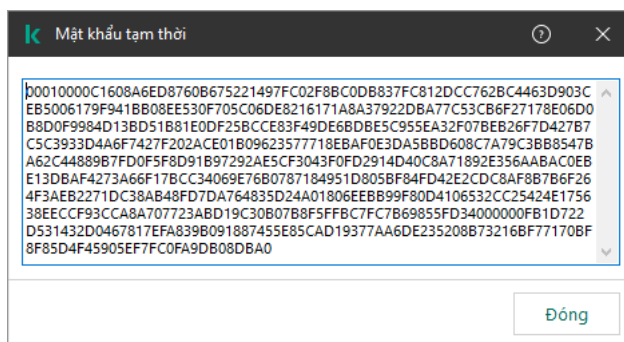
Một mật khẩu tạm thời có thể được sử dụng để cấp quyền truy cập tạm thời đến Kaspersky Endpoint Security cho một máy tính riêng biệt ngoài mạng doanh nghiệp. Việc này là cần thiết để cho phép người dùng thực hiện một hành động bị chặn mà không nhận thông tin tài khoản KAdmin. Để sử dụng một mật khẩu tạm thời, máy tính phải được thêm vào Kaspersky Security Center.

[Cách cho phép người dùng thực hiện hành động bị chặn bằng mật khẩu tạm thời thông qua Bảng điều khiển quản trị \(MMC\)](#) ²

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Devices**.
4. Nhấn đúp để mở cửa sổ thuộc tính máy tính.
5. Trong cửa sổ thuộc tính máy tính, chọn phần **Ứng dụng**.
6. Trong danh sách các ứng dụng Kaspersky được cài đặt trên máy tính, hãy chọn **Kaspersky Endpoint Security cho Windows** và nhấn đúp để mở thuộc tính ứng dụng.
Trong cửa sổ thiết lập ứng dụng, chọn **Thiết lập tổng quát** → **Giao diện**.
7. Trong mục **Bảo vệ bằng mật khẩu**, hãy nhấn nút **Thiết lập**.
8. Trong mục **Mật khẩu tạm thời**, nhấn nút **Thiết lập**.
9. Cửa sổ **Tạo mật khẩu tạm thời** sẽ được mở ra.
10. Trong trường **Expiration date**, quy định ngày hết hạn của mật khẩu tạm thời.
11. Trong bảng **Phạm vi mật khẩu tạm thời**, chọn hộp kiểm cạnh các hành động có thể được thực thi bởi người dùng sau khi họ nhập mật khẩu tạm thời.
12. Nhấn vào **Tạo**.
Một cửa sổ chứa mật khẩu tạm thời sẽ được mở ra (xem hình dưới đây).
13. Sao chép mật khẩu đó và cung cấp nó cho người dùng.

[Cách cho phép người dùng thực hiện hành động bị chặn bằng mật khẩu tạm thời thông qua Bảng điều khiển web và Bảng điều khiển đám mây](#)²

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Managed devices**.
2. Nhấn vào tên của máy tính mà bạn muốn cho phép người dùng thực hiện một hành động bị chặn.
3. Chọn thẻ **Ứng dụng**.
4. Nhấn vào **Kaspersky Endpoint Security cho Windows**.
Việc này sẽ mở ra thiết lập cục bộ của ứng dụng.
5. Chọn thẻ **Application settings**.
6. Trong cửa sổ thiết lập ứng dụng, chọn **Thiết lập tổng quát** → **Giao diện**.
7. Trong mục **Bảo vệ bằng mật khẩu**, hãy nhấn nút **Mật khẩu tạm thời**.
8. Trong trường **Expiration date**, quy định ngày hết hạn của mật khẩu tạm thời.
9. Trong bảng **Phạm vi mật khẩu tạm thời**, chọn hộp kiểm cạnh các hành động có thể được thực thi bởi người dùng sau khi họ nhập mật khẩu tạm thời.
10. Nhấn vào **Tạo**.
Một cửa sổ chứa mật khẩu tạm thời sẽ mở ra.
11. Sao chép mật khẩu đó và cung cấp nó cho người dùng.




Mật khẩu tạm thời

Các khía cạnh đặc biệt của quyền truy cập được Bảo vệ bằng mật khẩu

Các quyền được bảo vệ bằng mật khẩu có một số khía cạnh và giới hạn mà bạn cần cân nhắc.


Thiết lập ứng dụng

Nếu máy tính người dùng đang sử dụng một chính sách, hãy đảm bảo tất cả các thiết lập cần thiết trong chính sách đều có thể được chỉnh sửa (thuộc tính  được mở).


Thoát khỏi ứng dụng

Không có cân nhắc hay giới hạn đặc biệt nào.

Tắt các thành phần bảo vệ

- Không thể cấp quyền để tắt các thành phần bảo vệ cho nhóm Mọi người. Để cho phép những người dùng khác ngoài KAdmin tắt các thành phần kiểm soát, hãy [thêm một người dùng hoặc nhóm](#) có quyền **Tắt các thành phần bảo vệ** trong thiết lập Bảo vệ bằng mật khẩu.
- Nếu máy tính người dùng đang sử dụng một chính sách, hãy đảm bảo tất cả các thiết lập cần thiết trong chính sách đều có thể được chỉnh sửa (thuộc tính  được mở).
- Để tắt các thành phần bảo vệ trong thiết lập ứng dụng, một người dùng phải có quyền truy cập **Cấu hình thiết lập của ứng dụng**.
- Để tắt các thành phần bảo vệ từ menu ngữ cảnh (bằng cách sử dụng mục menu **Tạm dừng bảo vệ**), một người dùng phải có quyền **Tắt các thành phần bảo vệ** ngoài quyền **Tắt các thành phần kiểm soát**.

Tắt các thành phần kiểm soát

- Không thể cấp quyền để tắt các thành phần kiểm soát cho nhóm Mọi người. Để cho phép những người dùng khác ngoài KAdmin tắt các thành phần kiểm soát, hãy [thêm một người dùng hoặc nhóm](#) có quyền **Tắt các thành phần kiểm soát** trong thiết lập Bảo vệ bằng mật khẩu.
- Nếu máy tính người dùng đang sử dụng một chính sách, hãy đảm bảo tất cả các thiết lập cần thiết trong chính sách đều có thể được chỉnh sửa (thuộc tính  được mở).
- Để tắt các thành phần kiểm soát trong thiết lập ứng dụng, một người dùng phải có quyền truy cập **Cấu hình thiết lập của ứng dụng**.
- Để tắt các thành phần kiểm soát từ menu ngữ cảnh (bằng cách sử dụng mục menu **Tạm dừng bảo vệ**), một người dùng phải có quyền **Tắt các thành phần kiểm soát** ngoài quyền **Tắt các thành phần bảo vệ**.

Tắt chính sách Kaspersky Security Center

Bạn không thể cấp cho nhóm "Mọi người" quyền tắt chính sách của Kaspersky Security Center. Để cho phép những người dùng khác ngoài KAdmin tắt chính sách này, hãy [thêm một người dùng hoặc nhóm](#) có quyền **Tắt chính sách Kaspersky Security Center** trong thiết lập Bảo vệ bằng mật khẩu.

Xóa khóa

Không có cân nhắc hay giới hạn đặc biệt nào.

Gỡ bỏ / thay đổi / khôi phục ứng dụng

Nếu bạn đã cho phép gỡ bỏ, sửa đổi và khôi phục ứng dụng cho nhóm "Tất cả" thì Kaspersky Endpoint Security không yêu cầu mật khẩu khi người dùng thử thực hiện các hành động này. Do đó, bất kỳ người dùng nào, bao gồm người dùng ngoài miền, cũng có thể cài đặt, sửa đổi hoặc khôi phục ứng dụng.

Khôi phục quyền truy cập vào dữ liệu trên ổ đĩa mã hóa

Bạn chỉ có thể khôi phục quyền truy cập vào dữ liệu trên các ổ đĩa được mã hóa nếu bạn đăng nhập là KAdmin. Quyền thực hiện hành động này không thể được cấp cho bất kỳ người dùng nào khác.

Xem báo cáo

Không có cân nhắc hay giới hạn đặc biệt nào.

Khôi phục từ Sao lưu

Không có cân nhắc hay giới hạn đặc biệt nào.

Đặt lại mật khẩu KAdmin

Nếu quên mật khẩu tài khoản KAdmin thì bạn có thể đặt lại mật khẩu trong thuộc tính chính sách. Bạn không thể đặt lại mật khẩu trong giao diện ứng dụng.

Bạn có thể thực hiện các hành động được bảo vệ bằng mật khẩu bằng [mật khẩu tạm thời](#). Trong trường hợp này, bạn không cần nhập thông tin đăng nhập KAdmin.

Nếu máy tính không được kết nối với Kaspersky Security Center và bạn đã quên mật khẩu cho tài khoản KAdmin, bạn sẽ không thể phục hồi mật khẩu.

[Cách đặt lại mật khẩu tài khoản KAdmin bằng Bảng điều khiển quản trị \(MMC\)](#)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Giao diện**.
6. Trong mục **Bảo vệ bằng mật khẩu**, hãy nhấn nút **Thiết lập**.
7. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy xóa hộp kiểm **Bảo vệ bằng mật khẩu**.
8. Lưu các thay đổi của bạn.
9. Chọn hộp kiểm **Bảo vệ bằng mật khẩu** một lần nữa.
10. Nhấn **OK**.
Thao tác này sẽ mở ra cửa sổ mật khẩu quản trị viên.
11. Đặt mật khẩu mới cho tài khoản KLAdmin và xác nhận mật khẩu đó.
12. Lưu các thay đổi của bạn.

[Cách đặt lại mật khẩu tài khoản KLAdmin trong Bảng điều khiển web và Bảng điều khiển đám mây](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Managed devices**.
2. Chọn máy tính mà bạn muốn cấu hình thiết lập cục bộ của ứng dụng.
Việc này sẽ mở ra thuộc tính máy tính.
3. Chọn thẻ **Ứng dụng**.
4. Nhấn vào **Kaspersky Endpoint Security cho Windows**.
Việc này sẽ mở ra thiết lập cục bộ của ứng dụng.
5. Chọn thẻ **Application settings**.
6. Vào **Thiết lập tổng quát** → **Giao diện**.
7. Trong mục **Bảo vệ bằng mật khẩu**, hãy tắt nút bật/tắt **Bảo vệ bằng mật khẩu**.
8. Lưu các thay đổi của bạn.
9. Bật **Bảo vệ bằng mật khẩu** trở lại.
10. Đặt mật khẩu mới cho tài khoản KLAdmin và xác nhận mật khẩu đó.
11. Lưu các thay đổi của bạn.

Kết quả là mật khẩu của tài khoản KLAdmin của bạn sẽ được cập nhật sau khi chính sách được áp dụng.

Khu vực 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.

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 thêm các đối tượng và ứng dụng vào 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. Quản trị viên cũng có thể cho phép người dùng tạo vùng tin tưởng cục bộ của riêng họ cho một máy tính cụ thể. Bằng cách này, người dùng có thể tạo danh sách loại trừ cục bộ của riêng họ và các ứng dụng được tin tưởng ngoài vùng tin tưởng chung trong một chính sách.

Tạo một loại trừ quét

Loại trừ quét là một nhóm các điều kiện phải được đáp ứng để Kaspersky Endpoint Security không quét một đối tượng cụ thể 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 làm hỏng 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 bị kẻ xâm nhập khai thác. Để xem chi tiết về các phần mềm hợp pháp có thể bị bọn tội phạm lợi dụng để gây hại cho máy tính hoặc dữ liệu cá nhân của một người dùng, vui lòng tham khảo [trang web Bách khoa toàn thư của Kaspersky IT](#)².

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 tên đại diện của ứng dụng được liệt kê trong Bách khoa toàn thư của Kaspersky IT vào vùng tin tưởng. Ví dụ, bạn thường sử dụng ứng dụng Radmin để quản trị từ xa máy tính. 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 tên đại diện của ứng dụng được liệt kê trong Bách khoa toàn thư của Kaspersky IT.

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:

- [Phát hiện hành vi](#).
- [Phòng chống khai thác](#).
- [Phòng chống xâm nhập máy chủ](#).
- [Bảo vệ mối đe dọa tập tin](#).
- [Bảo vệ mối đe dọa web](#).
- [Bảo vệ mối đe dọa thư điện tử](#).
- [Tác vụ 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.

Cách tạo loại trừ quét trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Exclusions and types of detected objects**.
6. Trong mục **Loại trừ quét và ứng dụng được tin tưởng**, hãy nhấn nút **Thiết lập**.
7. Trong cửa sổ mở ra, hãy chọn thẻ **Loại trừ quét**.
Thao tác này sẽ mở cửa sổ chứa danh sách các loại trừ.
8. Chọn hộp kiểm **Merge values when inheriting** nếu bạn muốn tạo một danh sách tổng hợp các loại trừ cho tất cả các máy tính trong công ty. Danh sách các loại trừ trong chính sách cha và chính sách con sẽ được hợp nhất. Các danh sách sẽ được hợp nhất với điều kiện các giá trị hợp nhất khi kế thừa được bật. Các loại trừ từ chính sách cha được hiển thị trong chính sách con ở chế độ chỉ đọc. Không thể thay đổi hay xóa các loại trừ của chính sách cha.
9. Chọn hộp kiểm **Allow use of local trusted applications** nếu bạn muốn cho phép người dùng tạo danh sách loại trừ cục bộ. Bằng cách này, người dùng có thể tạo danh sách loại trừ của riêng họ ngoài danh sách loại trừ chung được tạo trong chính sách. Quản trị viên có thể sử dụng Kaspersky Security Center để xem, thêm, chỉnh sửa hoặc xóa các mục danh sách trong thuộc tính máy tính.
Nếu hộp kiểm bị xóa, người dùng chỉ có thể truy cập danh sách loại trừ được tạo trong chính sách.
10. Nhấn vào **Thêm**.
11. Để loại trừ một tập tin hoặc thư mục khỏi tác vụ quét:
 - a. Trong mục **Thuộc tính**, hãy chọn hộp kiểm **Tập tin hoặc thư mục**.
 - b. Nhấn vào liên kết **chọn tập tin/thư mục** trong mục **Mô tả loại trừ quét (bấm vào mục gạch chân để chỉnh sửa)** để mở cửa sổ **Tên của tập tin hoặc thư mục**.
 - c. Nhập vào tên tập tin/thư mục hoặc ký tự đại diện cho tên tập tin/thư mục hoặc chọn tập tin/thư mục trong cây thư mục bằng cách nhấn nút **Duyệt**.
Sử dụng ký tự đại diện:
 - Ký tự ***** (hoa thị) thay thế bất kỳ nhóm ký tự nào bộ ký tự, ngoại trừ các ký tự **** và **/** (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ, ký tự đại diện **C:**.txt** sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng TXT nằm trong các thư mục trên ổ C:, nhưng không phải trong các thư mục con.
 - Hai ký tự ***** liên tiếp thay thế bất kỳ nhóm ký tự nào (bao gồm nhóm rỗng) trong tên tập tin hoặc thư mục, bao gồm các ký tự **** và **/** (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ, ký tự đại diện **C:\Folder***.txt** sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng TXT nằm trong các thư mục con

bên trong Folder, ngoại trừ chính Folder. Một đại diện phải có ít nhất một cặp lồng ghép. C:**.txt không phải là một đại diện hợp lệ.

- Ký tự ? (dấu hỏi) thay thế bất kỳ ký tự đơn nào, ngoại trừ các ký tự \ và / (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ: đại diện C:\Folder\???.txt sẽ bao gồm các đường dẫn đến tất cả các tập tin có trong thư mục Folder có phần mở rộng TXT và tên có ba ký tự.

d. Lưu các thay đổi của bạn.

12. Để loại trừ các đối tượng có tên cụ thể khỏi tác vụ quét:

a. Trong mục **Thuộc tính**, hãy chọn hộp kiểm **Tên đối tượng**.

b. Nhấn vào liên kết **nhập tên đối tượng** trong mục **Mô tả loại trừ quét (bấm vào mục gạch chân để chỉnh sửa)** để mở cửa sổ **Tên đối tượng**.

c. Nhập tên của loại đối tượng theo phân loại của [Bách khoa toàn thư của Kaspersky](#) (ví dụ: Email-Worm, Rootkit hoặc RemoteAdmin).

Bạn có thể sử dụng tên đại diện có ký tự ? (thay thế bất kỳ ký tự đơn nào) và ký tự * (thay thế bất kỳ số lượng ký tự nào). Ví dụ: nếu nhập tên đại diện Client *, Kaspersky Endpoint Security sẽ loại trừ các đối tượng Client-IRC, Client-P2P và Client-SMTP khỏi quá trình quét.

d. Lưu các thay đổi của bạn.

13. Nếu bạn muốn loại trừ một tập tin riêng lẻ khỏi quá trình quét:

a. Trong mục **Thuộc tính**, hãy chọn hộp kiểm **Mã Hash đối tượng**.

b. Nhấn vào liên kết mục giá trị băm của đối tượng để mở cửa sổ **Mã Hash đối tượng**.

c. Nhập giá trị băm của tập tin hoặc chọn tập tin bằng cách nhấn vào nút **Duyệt**.

Nếu tập tin bị sửa đổi, giá trị băm của tập tin cũng sẽ được sửa đổi. Nếu điều này xảy ra, tập tin bị sửa đổi sẽ không được thêm vào loại trừ.

d. Lưu các thay đổi của bạn.

14. Nếu cần thiết, trong trường **Bình luận**, nhập một nhận xét ngắn về loại trừ quét mà bạn đang tạo.

15. 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 (bấm vào mục gạch chân để chỉnh sửa)** để kích hoạt liên kết **lựa chọn các thành phần**.

b. Nhấn vào liên kết **lựa chọn các 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. Lưu các thay đổi của bạn.

Nếu các thành phần này được quy định trong thiết lập 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 này không được quy định trong thiết lập 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.

16. Bạn có thể sử dụng hộp kiểm này để [dừng loại trừ](#) bất kỳ lúc nào.
17. Lưu các thay đổi của bạn.

[Cách tạo loại trừ quét trong Bảng điều khiển web và Bảng điều khiển đám mây](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **General settings** → **Exclusions and types of detected objects**.
5. Trong mục **Scan exclusions and trusted applications**, hãy nhấn liên kết **Scan exclusions**.
6. Chọn hộp kiểm **Merge values when inheriting** nếu bạn muốn tạo một danh sách tổng hợp các loại trừ cho tất cả các máy tính trong công ty. Danh sách các loại trừ trong chính sách cha và chính sách con sẽ được hợp nhất. Các danh sách sẽ được hợp nhất với điều kiện các giá trị hợp nhất khi kế thừa được bật. Các loại trừ từ chính sách cha được hiển thị trong chính sách con ở chế độ chỉ đọc. Không thể thay đổi hay xóa các loại trừ của chính sách cha.
7. Chọn hộp kiểm **Allow use of local trusted applications** nếu bạn muốn cho phép người dùng tạo danh sách loại trừ cục bộ. Bằng cách này, người dùng có thể tạo danh sách loại trừ của riêng họ ngoài danh sách loại trừ chung được tạo trong chính sách. Quản trị viên có thể sử dụng Kaspersky Security Center để xem, thêm, chỉnh sửa hoặc xóa các mục danh sách trong thuộc tính máy tính.
Nếu hộp kiểm bị xóa, người dùng chỉ có thể truy cập danh sách loại trừ được tạo trong chính sách.
8. Nhấn vào nút **Thêm**.
9. Chọn cách bạn muốn thêm loại trừ: **File or folder**, **Object name** hoặc **Object hash**.
10. Nếu bạn muốn loại trừ một tập tin hoặc thư mục khỏi tác vụ quét, hãy chọn tập tin hoặc thư mục bằng cách nhấn nút **Browse**.
Bạn cũng có thể nhập đường dẫn theo cách thủ công. Kaspersky Endpoint Security hỗ trợ các ký tự * cùng ? khi nhập tên đại diện:
 - Ký tự * (hoa thị) thay thế bất kỳ nhóm ký tự nào bộ ký tự, ngoại trừ các ký tự \ và / (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ, ký tự đại diện C:**.txt sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng TXT nằm trong các thư mục trên ổ C:, nhưng không phải trong các thư mục con.
 - Hai ký tự * liên tiếp thay thế bất kỳ nhóm ký tự nào (bao gồm nhóm rỗng) trong tên tập tin hoặc thư mục, bao gồm các ký tự \ và / (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ, ký tự đại diện C:\Folder***.txt sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng TXT nằm trong các thư mục con bên trong Folder, ngoại trừ chính Folder. Một đại diện phải có ít nhất một cặp lồng ghép. C:***.txt không phải là một đại diện hợp lệ.
 - Ký tự ? (dấu hỏi) thay thế bất kỳ ký tự đơn nào, ngoại trừ các ký tự \ và / (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ: đại diện C:\Folder\???.txt sẽ bao gồm các đường dẫn đến tất cả các tập tin có trong thư mục Folder có phần mở rộng TXT và tên có ba ký tự.
11. Nếu bạn muốn loại trừ một loại đối tượng cụ thể khỏi tác vụ quét, trong trường **Object name**, hãy nhập tên của loại đối tượng theo phân loại của [Bách khoa toàn thư của Kaspersky](#) (ví dụ: Email-Worm, Rootkit hoặc RemoteAdmin).

Bạn có thể sử dụng tên đại diện có ký tự ? (thay thế bất kỳ ký tự đơn nào) và ký tự * (thay thế bất kỳ số lượng ký tự nào). Ví dụ: nếu nhập tên đại diện Client *, Kaspersky Endpoint Security sẽ loại trừ các đối tượng Client-IRC, Client-P2P và Client-SMTP khỏi quá trình quét.

12. Nếu bạn muốn loại trừ một tập tin riêng lẻ khỏi tác vụ quét, hãy nhập giá trị băm của tập tin vào trường **Object hash**.

Nếu tập tin bị sửa đổi, giá trị băm của tập tin cũng sẽ được sửa đổi. Nếu điều này xảy ra, tập tin bị sửa đổi sẽ không được thêm vào loại trừ.


13. Trong mục **Protection components**, hãy chọn các thành phần mà bạn muốn áp dụng loại trừ quét.

14. Nếu cần thiết, trong trường **Comment**, nhập một nhận xét ngắn về loại trừ quét mà bạn đang tạo.

15. Bạn có thể sử dụng nút bật/tắt để [dừng loại trừ](#) bất kỳ lúc nào.

16. Lưu các thay đổi của bạn.

[Cách tạo loại trừ quét trong giao diện ứng dụng](#)

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Loại trừ và loại đối tượng được phát hiện**.
3. Trong mục **Loại trừ**, hãy nhấn liên kết **Quản lý loại trừ**.
4. Nhấn vào **Thêm**.
5. Nếu bạn muốn loại trừ một tập tin hoặc thư mục khỏi tác vụ quét, hãy chọn tập tin hoặc thư mục bằng cách nhấn nút **Duyệt**.
Bạn cũng có thể nhập đường dẫn theo cách thủ công. Kaspersky Endpoint Security hỗ trợ các ký tự * cùng ? khi nhập tên đại diện:
 - Ký tự * (hoa thị) thay thế bất kỳ nhóm ký tự nào bộ ký tự, ngoại trừ các ký tự \ và / (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ, ký tự đại diện C:**.txt sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng TXT nằm trong các thư mục trên ổ C:, nhưng không phải trong các thư mục con.
 - Hai ký tự * liên tiếp thay thế bất kỳ nhóm ký tự nào (bao gồm nhóm rỗng) trong tên tập tin hoặc thư mục, bao gồm các ký tự \ và / (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ, ký tự đại diện C:\Folder***.txt sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng TXT nằm trong các thư mục con bên trong Folder, ngoại trừ chính Folder. Một đại diện phải có ít nhất một cặp lồng ghép. C:***.txt không phải là một đại diện hợp lệ.
 - Ký tự ? (dấu hỏi) thay thế bất kỳ ký tự đơn nào, ngoại trừ các ký tự \ và / (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ: đại diện C:\Folder\???.txt sẽ bao gồm các đường dẫn đến tất cả các tập tin có trong thư mục Folder có phần mở rộng TXT và tên có ba ký tự.
6. Nếu bạn muốn loại trừ một loại đối tượng cụ thể khỏi tác vụ quét, trong trường **Object**, hãy nhập tên của loại đối tượng theo phân loại của [Bách khoa toàn thư của Kaspersky](#) (ví dụ: `Email-Worm`, `Rootkit` hoặc `RemoteAdmin`).
Bạn có thể sử dụng tên đại diện có ký tự ? (thay thế bất kỳ ký tự đơn nào) và ký tự * (thay thế bất kỳ số lượng ký tự nào). Ví dụ: nếu nhập tên đại diện `Client *`, Kaspersky Endpoint Security sẽ loại trừ các đối tượng `Client-IRC`, `Client-P2P` và `Client-SMTP` khỏi quá trình quét.
7. Nếu bạn muốn loại trừ một tập tin riêng lẻ khỏi tác vụ quét, hãy nhập giá trị băm của tập tin vào trường **Mã Hash đối tượng**.
Nếu tập tin bị sửa đổi, giá trị băm của tập tin cũng sẽ được sửa đổi. Nếu điều này xảy ra, tập tin bị sửa đổi sẽ không được thêm vào loại trừ.
8. Trong mục **Protection components**, hãy chọn các thành phần mà bạn muốn áp dụng loại trừ quét.
9. Nếu cần thiết, trong trường **Comment**, nhập một nhận xét ngắn về loại trừ quét mà bạn đang tạo.
10. Chọn trạng thái **Hoạt động** cho loại trừ.
Bạn có thể sử dụng nút bật/tắt để [dừng loại trừ](#) bất kỳ lúc nào.
11. Lưu các thay đổi của bạn.

Ví dụ về tên đại diện đường dẫn:

Đường dẫn đến các tập tin nằm trong bất kỳ thư mục nào:

- Tên đại diện `*.exe` sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng exe.
- Tên đại diện `example*` sẽ bao gồm tất cả đường dẫn đến các tập tin tên là EXAMPLE.

Đường dẫn đến các tập tin nằm trong một thư mục cụ thể:


- Tên đại diện `C:\dir*.*` sẽ bao gồm tất cả đường dẫn đến các tập tin nằm trong thư mục C:\dir\, nhưng không nằm trong các thư mục con của C:\dir\.
- Tên đại diện `C:\dir*` sẽ bao gồm tất cả đường dẫn đến các tập tin nằm trong thư mục C:\dir\, bao gồm các thư mục con.
- Tên đại diện `C:\dir\` sẽ bao gồm tất cả đường dẫn đến các tập tin nằm trong thư mục C:\dir\, bao gồm các thư mục con.
- Tên đại diện `C:\dir*.exe` sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng EXE nằm trong thư mục C:\dir\, nhưng không nằm trong các thư mục con của C:\dir\.
- Tên đại diện `C:\dir\test` sẽ bao gồm tất cả đường dẫn đến các tập tin có tên "test" nằm trong thư mục C:\dir\, nhưng không nằm trong các thư mục con của C:\dir\.
- Tên đại diện `C:\dir*\test` sẽ bao gồm tất cả đường dẫn đến các tập tin có tên "test" nằm trong thư mục C:\dir\ và trong các thư mục con của C:\dir\.

Đường dẫn đến các tập tin nằm trong tất cả các thư mục có một tên cụ thể:

- Tên đại diện `dir*.*` sẽ bao gồm tất cả đường dẫn đến các tập tin trong các thư mục có tên là "dir", nhưng không nằm trong các thư mục con của những thư mục đó.
- Tên đại diện `dir*` sẽ bao gồm tất cả đường dẫn đến các tập tin trong các thư mục có tên là "dir", nhưng không nằm trong các thư mục con của những thư mục đó.
- Tên đại diện `dir\` sẽ bao gồm tất cả đường dẫn đến các tập tin trong các thư mục có tên là "dir", nhưng không nằm trong các thư mục con của những thư mục đó.
- Tên đại diện `dir*.exe` sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng EXE trong các thư mục có tên là "dir", nhưng không nằm trong các thư mục con của những thư mục đó.
- Tên đại diện `dir\test` sẽ bao gồm tất cả đường dẫn đến các tập tin có tên là "test" trong các thư mục có tên là "dir", nhưng không nằm trong các thư mục con của những thư mục đó.

Bật và tắt một loại trừ quét



Để bật hoặc tắt một quy tắc loại trừ quét:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Mỗi đe dọa và loại trừ**.

3. Trong mục **Loại trừ**, hãy nhấn liên kết **Quản lý loại trừ**.
4. Chọn quy tắc loại trừ mà bạn cần trong danh sách loại trừ quét.
5. Sử dụng nút bật/tắt bên cạnh một đối tượng để đưa hoặc loại trừ đối tượng này vào/khỏi phạm vi quét.
6. Lưu các thay đổi của bạn.

Chọn các loại đối tượng có thể được phát hiện

Để chọn các loại đối tượng có thể được phát hiện:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Mối đe dọa và loại trừ**.
3. Trong mục **Loại đối tượng được phát hiện**, hãy chọn hộp kiểm đối diện các loại đối tượng mà bạn muốn Kaspersky Endpoint Security phát hiện:
 - **Virus và sâu** 

Danh mục con: virus và sâu (Viruses_and_Worms)

Mức độ mối đe dọa: cao

Các loại virus và sâu truyền thống thực hiện các hành động không được người dùng cho phép. Chúng có thể tự tạo ra bản sao của chính mình, các bản sao đó cũng có thể tự nhân bản.

Virus truyền thống

Khi một virus truyền thống xâm nhập vào máy tính, nó sẽ lây nhiễm vào một tập tin, kích hoạt, thực hiện hành động độc hại, và chèn các bản sao của nó vào những tập tin khác.

Một virus truyền thống sẽ tự sinh sôi trên tài nguyên mạng nội bộ của máy tính; nó không thể tự xâm nhập vào các máy tính khác. Nó chỉ có thể được truyền sang máy tính khác nếu nó chèn bản sao của mình vào một tập tin được lưu trữ trong một thư mục được chia sẻ, hoặc trên một đĩa CD trong máy, hoặc nếu một người dùng chuyển tiếp một email đính kèm tập tin bị nhiễm virus.

Mã virus truyền thống có thể xâm nhập các khu vực khác nhau của máy tính, hệ điều hành và ứng dụng. Tùy thuộc vào môi trường, các virus được chia thành *virus tập tin*, *virus khởi động*, *virus kích bản* và *virus macro*.

Virus có thể lây nhiễm cho các tập tin sử dụng nhiều kỹ thuật khác nhau. *Ghi đè virus* sẽ ghi đè mã của nó lên mã của tập tin bị lây nhiễm và xóa nội dung của tập tin. Tập tin bị lây nhiễm sẽ ngừng hoạt động và không thể được khôi phục. *Ký sinh virus* sẽ sửa nội dung tập tin, để chúng vận hành toàn bộ hoặc một phần chức năng. *Virus đồng hành* không sửa tập tin, nhưng tạo các bản sao. Khi một tập tin nhiễm virus được mở ra, một bản sao của nó (thực chất là một virus) sẽ được khởi chạy. Các loại virus sau cũng có thể được bắt gặp: *virus liên kết*, *virus OBJ*, *virus LIB*, *virus mã nguồn*, v.v...

Sâu

Tương tự như virus truyền thống, mã của sâu, sẽ được kích hoạt và thực hiện các hành động độc hại sau khi nó đã xâm nhập máy tính. Sâu được đặt tên như vậy bởi chúng có thể "bò" từ một máy tính sang máy tính khác và phát tán các bản sao thông qua nhiều kênh dữ liệu mà không có sự cho phép của người dùng.

Tính năng chính phân biệt giữa các loại sâu khác nhau là cách phát tán của chúng. Bảng sau đây cung cấp một cái nhìn tổng quan về các loại sâu khác nhau, được phân loại theo cách phát tán của chúng.

Cách phát tán của sâu

Loại	Tên	Mô tả
Sâu Email	Sâu Email	Phát tán qua email. Một email nhiễm virus chứa một tập tin đính kèm với một bản sao của sâu, hoặc một liên kết đến một tập tin được tải lên một website đã bị hack hoặc được tạo vì mục đích cụ thể này. Khi bạn mở tập tin đính kèm ra, sâu sẽ được kích hoạt. Khi bạn nhấn vào liên kết tải về, và mở tập tin, sâu sẽ bắt đầu thực hiện hành động độc hại của nó. Sau đó, nó sẽ tiếp tục phát tán các bản sao, tìm kiếm các địa chỉ email khác và gửi tin nhắn nhiễm virus đến họ.
IM-Worm	Sâu Trình nhắn	Chúng được phát tán qua các ứng dụng nhắn tin nhanh.

	tin nhanh	Thông thường, các loại sâu này gửi tin nhắn chứa liên kết đến một bản sao của sâu trên một website, tận dụng danh bạ của người dùng. Khi người dùng tải về và mở ra tập tin, sâu sẽ được kích hoạt.
IRC-Worm	Sâu trò chuyện Internet	Chúng được phát tán qua các Phòng Tán ngẫu IRC, là các hệ thống dịch vụ cho phép giao tiếp với những người khác qua Internet trong thời gian thực. Những loại sâu này sẽ đăng tải một tập tin với bản sao của chúng hoặc một liên kết đến tập tin trong một phòng tán ngẫu Internet. Khi người dùng tải về và mở ra tập tin, sâu sẽ được kích hoạt.
Sâu Net	Sâu Mạng	Những loại sâu này phát tán qua mạng máy tính. Khác với những loại sâu khác, một sâu mạng tiêu biểu sẽ phát tán mà không cần sự tham gia của người dùng. Nó sẽ quét mạng nội bộ để tìm các máy tính chứa những chương trình có lỗ hổng bảo mật. Để làm điều này, nó sẽ gửi đi một gói tin mạng đặc biệt (mã khai thác) chứa mã sâu hoặc một phần của nó. Nếu một máy tính có "lỗ hổng bảo mật" nằm trên mạng này, nó sẽ tiếp nhận gói tin mạng đó. Khi sâu đã hoàn thành việc xâm nhập máy tính, nó sẽ kích hoạt.
P2P-Worm	Sâu mạng chia sẻ tập tin	Chúng được phát tán qua các mạng chia sẻ tập tin ngang hàng. Để xâm nhập một mạng P2P, sâu sẽ tự sao chép bản thân nó vào một thư mục chia sẻ tập tin, thường được đặt trên máy tính của người dùng. Mạng P2P sẽ hiển thị thông tin về tập tin này để người dùng có thể "tìm thấy" tập tin nhiễm virus trên mạng như những tập tin khác, sau đó tải về và mở nó ra. Các loại sâu tinh vi hơn sẽ giả lập giao thức mạng của một mạng P2P cụ thể: chúng sẽ gửi trả phản hồi tích cực đến các truy vấn tìm kiếm và cung cấp bản sao của chính mình để tải về.
Sâu	Các loại sâu khác	Các loại sâu khác bao gồm: <ul style="list-style-type: none"> Sâu phát tán bản sao của chúng qua tài nguyên mạng. Bằng cách sử dụng chức năng của hệ điều hành, chúng sẽ quét các thư mục mạng khả dụng, kết nối đến các máy tính trên Internet, và cố gắng nhận quyền truy cập toàn diện đến ổ đĩa của chúng. Khác với những loại sâu được mô tả ở trên, các loại sâu khác không tự kích hoạt được, mà chỉ khi người dùng mở một tập tin chứa một bản sao của sâu. Các loại sâu không sử dụng bất kỳ cách phát tán nào được mô tả ở bảng trước (ví dụ, các loại sâu phát tán qua điện thoại di động).

- [Trojan \(bao gồm phần mềm tổng tiền\)](#) 

Danh mục con: Trojan

Mức độ mối đe dọa: cao

Khác với sâu và virus, Trojan không tự sinh sôi. Ví dụ, chúng sẽ xâm nhập một máy tính thông qua email hoặc một trình duyệt khi người dùng truy cập một trang web bị nhiễm virus. Trojan được khởi chạy với sự tham gia của người dùng. Chúng sẽ bắt đầu thực hiện hành động độc hại ngay khi được bắt đầu.

Các Trojan khác nhau sẽ hành xử khác nhau trên máy tính bị nhiễm. Chức năng chính của Trojan bao gồm chặn, sửa đổi hoặc phá hủy thông tin, và tắt máy tính hoặc mạng. Trojan cũng có thể nhận hoặc gửi tập tin, thực thi chúng, hiển thị thông báo lên màn hình, yêu cầu trang web, tải về và cài đặt các chương trình, và khởi động lại máy tính.

Tin tặc thường sử dụng "các nhóm" Trojan khác nhau.

Các loại hành vi Trojan được mô tả trong bảng dưới đây.

Loại hành vi Trojan trên một máy tính bị nhiễm

Loại	Tên	Mô tả
Trojan-ArcBomb	Trojan - "bom nén"	Khi giải nén, các tập nén này sẽ tăng kích cỡ đến mức mà hoạt động của máy tính sẽ bị ảnh hưởng. Khi người dùng cố gắng giải nén tập nén này, máy tính có thể bị chậm đến mức treo; ổ cứng có thể bị lấp đầy dữ liệu "trống". "Bom nén" đặc biệt nguy hiểm đối với các máy chủ tập tin và email. Nếu máy chủ sử dụng một hệ thống tự động để xử lý thông tin đến, một "bom nén" có thể ngừng hoạt động của máy chủ.
Backdoor	Trojan quản trị từ xa	Đây được coi là loại Trojan nguy hiểm nhất. Chức năng của chúng cũng tương tự như các ứng dụng quản trị từ xa được cài đặt trên máy tính. Những chương trình này sẽ cài đặt bản thân trên máy tính mà không được người dùng phát hiện, cho phép kẻ xâm nhập có thể quản lý máy tính từ xa.
Trojan	Trojan	Chúng bao gồm các ứng dụng độc hại sau: <ul style="list-style-type: none">• Trojan truyền thống. Những chương trình này chỉ thực hiện chức năng chính của Trojan: chặn, sửa đổi hoặc phá hủy thông tin, và tắt máy tính hoặc mạng. Chúng không có các tính năng cao cấp, khác với những loại Trojan khác được mô tả trong bảng này.• Trojan linh hoạt. Những chương trình này có các tính năng cao cấp giống nhiều loại Trojan khác nhau.
Trojan-Ransom	Trojan tống tiền	Chúng bắt thông tin người dùng "làm con tin", sửa đổi hoặc chặn nó, hoặc ảnh hưởng đến hoạt động của máy tính để người dùng mất khả năng sử dụng thông tin này. Kẻ xâm nhập sẽ đòi tiền chuộc từ người dùng, hứa hẹn sẽ gửi một ứng dụng khôi phục hiệu năng máy tính và dữ liệu đã được lưu trữ trên đó.
Trojan-Clicker	Trojan nhấn chuột	Chúng sẽ truy cập các trang web từ máy tính của người dùng, bằng cách gửi đi lệnh đến trình duyệt hoặc thay đổi các địa chỉ web được quy định trong tập tin hệ điều hành.

		Bằng cách sử dụng các chương trình này, kẻ xâm nhập có thể gây ra các cuộc tấn công mạng và tăng lượng truy cập website, tăng số lượt hiển thị bằng quảng cáo.
Trojan-Downloader	Trojan tải về	Chúng sẽ truy cập trang web của kẻ xâm nhập, tải về các ứng dụng độc hại khác và cài đặt chúng trên máy tính của người dùng. Chúng có thể chứa tên tập tin của ứng dụng độc hại để tải về, hoặc nhận nó từ trang web được truy cập.
Trojan-Dropper	Trojan đổ bộ	<p>Chúng chứa các Trojan khác sẽ được chúng giải nén trên ổ cứng và cài đặt.</p> <p>Kẻ xâm nhập có thể sử dụng Trojan đổ bộ vì các mục đích sau:</p> <ul style="list-style-type: none"> • Cài đặt một ứng dụng độc hại mà không bị người dùng phát hiện: các chương trình Trojan đổ bộ không hiển thị thông báo nào, hay hiển thị các thông báo giả mạo rằng, ví dụ, có một lỗi trong một tập nén hoặc một phiên bản không tương thích của hệ điều hành. • Bảo vệ một ứng dụng độc hại khác đã được biết khỏi bị phát hiện: không phải phần mềm chống virus nào cũng có thể phát hiện một ứng dụng độc hại trong một ứng dụng Trojan đổ bộ.
Trojan-Notifier	Trojan thông báo	<p>Chúng sẽ thông báo cho kẻ xâm nhập rằng máy tính bị nhiễm có thể được truy cập, gửi thông tin về máy tính đến kẻ xâm nhập: địa chỉ IP, số cổng đang mở, hoặc địa chỉ email. Chúng sẽ kết nối với kẻ xâm nhập qua email, FTP, truy cập trang web của kẻ xâm nhập, hoặc bằng một cách khác.</p> <p>Các chương trình Trojan thông báo thường được sử dụng theo nhóm gồm nhiều Trojan khác nhau. Chúng sẽ thông báo với kẻ xâm nhập rằng các Trojan khác đã được cài đặt thành công trên máy tính của người dùng.</p>
Trojan-Proxy	Trojan proxy	Chúng cho phép kẻ xâm nhập có thể truy cập các trang web một cách ẩn danh sử dụng máy tính của người dùng; chúng thường được sử dụng để gửi thư rác.
Trojan-PSW	Phần mềm đánh cắp mật khẩu	<p>Phần mềm đánh cắp mật khẩu là một loại Trojan đánh cắp tài khoản người dùng, ví dụ như dữ liệu đăng ký phần mềm. Những Trojan này tìm thấy thông tin bí mật trong tập tin hệ thống và trong registry và gửi chúng cho "kẻ tấn công" qua email, qua FTP, qua trang web của kẻ xâm nhập, hoặc bằng một cách khác.</p> <p>Một số loại Trojan này được phân loại vào các kiểu riêng biệt được mô tả trong bảng này. Đó là những Trojan đánh cắp tài khoản ngân hàng (Trojan-Banker), đánh cắp dữ liệu từ ứng dụng nhắn tin nhanh (Trojan-IM), và đánh cắp thông tin của người chơi game trực tuyến (Trojan-GameThief).</p>
Trojan-Spy	Trojan gián điệp	Chúng sẽ theo dõi người dùng, thu thập thông tin về các hành động của người dùng khi làm việc trên máy tính. Chúng có thể đánh cắp dữ liệu mà người dùng nhập vào bằng bàn phím, chụp ảnh màn hình, hoặc thu thập danh sách các ứng dụng đang hoạt động. Sau khi chúng đã nhận được thông tin, chúng sẽ chuyển nó đến kẻ xâm nhập qua email, qua FTP, qua trang web của kẻ xâm nhập, hoặc bằng một cách khác.
Trojan-DDoS	Trojan tấn công	Chúng sẽ gửi nhiều yêu cầu từ máy tính của người dùng đến một máy chủ từ xa. Máy chủ sẽ không đủ tài nguyên để xử lý

	mạng	<p>tất cả các yêu cầu, và sẽ ngừng hoạt động (Từ chối Dịch vụ, hoặc gọi tắt là DoS). Tin tặc thường sẽ lây nhiễm cho nhiều máy tính bằng các chương trình này, để chúng có thể sử dụng máy tính để đồng loạt tấn công một máy chủ.</p> <p>Các chương trình DoS gây ra một cuộc tấn công từ một máy tính với kiến thức của người dùng. Các chương trình DDoS (DoS Phân phối) sẽ phát động tấn công phân phối từ nhiều máy tính mà không được phát hiện bởi người dùng của máy tính bị nhiễm.</p>
Trojan-IM	Trojan đánh cắp thông tin từ người dùng các ứng dụng nhắn tin nhanh	Chúng sẽ đánh cắp tài khoản và mật khẩu của người dùng ứng dụng nhắn tin nhanh. Chúng sẽ truyền dữ liệu đến kẻ xâm nhập qua email, qua FTP, qua trang web của kẻ xâm nhập, hoặc bằng một cách khác.
Rootkit	Rootkit	Chúng sẽ che giấu các ứng dụng độc hại khác và hoạt động của chúng, kéo dài sự tồn tại của những ứng dụng này trong hệ điều hành. Chúng cũng có thể che giấu các tập tin hay tiến trình đang thực hiện các ứng dụng độc hại trong bộ nhớ hoặc khóa registry của máy tính bị nhiễm. Rootkit có thể che giấu việc trao đổi dữ liệu giữa các ứng dụng trên máy tính của người dùng và các máy tính khác trên mạng.
Trojan-SMS	Trojan dưới dạng tin nhắn SMS	Chúng có thể lây nhiễm cho điện thoại di động, gửi tin nhắn SMS đến các số điện thoại mất phí.
Trojan-GameThief	Trojan đánh cắp thông tin từ người chơi trò chơi trực tuyến	Chúng sẽ đánh cắp thông tin tài khoản từ người chơi game trực tuyến, sau đó truyền dữ liệu này đến kẻ xâm nhập qua email, qua FTP, qua trang web của kẻ xâm nhập, hoặc bằng một cách khác.
Trojan-Banker	Trojan đánh cắp tài khoản ngân hàng	Chúng sẽ đánh cắp dữ liệu tài khoản ngân hàng hoặc dữ liệu hệ thống tiền điện tử; gửi dữ liệu này đến tin tặc qua email, qua FTP, qua trang web của tin tặc hoặc bằng một cách khác.
Trojan-Mailfinder	Trojan thu thập địa chỉ email	Chúng sẽ thu thập các địa chỉ email được lưu trữ trên một máy tính và gửi thông tin này đến kẻ xâm nhập qua email, qua FTP, qua trang web của kẻ xâm nhập, hoặc bằng một cách khác. Kẻ xâm nhập có thể gửi thư rác đến các địa chỉ mà chúng đã thu thập.

- [Công cụ độc hại](#) 

Danh mục con: Công cụ độc hại

Cấp độ nguy hiểm: trung bình

Khác với các loại phần mềm độc hại khác, công cụ độc hại không thực hiện hành động độc hại ngay khi chúng được khởi chạy. Chúng có thể được lưu trữ và khởi chạy một cách an toàn trên máy tính của người dùng. Kẻ xâm nhập sẽ thường sử dụng các tính năng của những chương trình này để tạo các virus, sâu và Trojan, phát động tấn công mạng trên các máy chủ từ xa, hack máy tính, hoặc thực hiện các hành động độc hại khác.

Các tính năng khác nhau của công cụ độc hại được ghép nhóm theo phân loại được mô tả trong bảng sau.

Tính năng của công cụ độc hại

Loại	Tên	Mô tả
Tiện ích xây dựng	Tiện ích xây dựng	Chúng cho phép tạo ra các virus, sâu và Trojan mới. Một số tiện ích xây dựng có một giao diện cửa sổ tiêu chuẩn trong đó người dùng có thể lựa chọn kiểu ứng dụng độc hại mà họ muốn tạo, cách đối phó với trình gỡ lỗi, và các tính năng khác.
Dos	Tấn công mạng	Chúng sẽ gửi nhiều yêu cầu từ máy tính của người dùng đến một máy chủ từ xa. Máy chủ sẽ không đủ tài nguyên để xử lý tất cả các yêu cầu, và sẽ ngừng hoạt động (Từ chối Dịch vụ, hoặc gọi tắt là DoS).
Khai thác	Mã khai thác	<p><i>Mã khai thác</i> là một bộ dữ liệu hoặc mã chương trình sử dụng lỗ hổng bảo mật của ứng dụng xử lý nó để thực hiện một hành động độc hại trên máy tính. Ví dụ, một mã khai thác có thể ghi hoặc đọc tập tin, hoặc yêu cầu các trang web "bị nhiễm".</p> <p>Các mã khai thác khác nhau sử dụng lỗ hổng bảo mật trong các ứng dụng hoặc dịch vụ mạng khác nhau. Giả dạng dưới dạng một gói tin mạng, mã khai thác sẽ được truyền tải qua mạng đến nhiều máy tính khác nhau, tìm kiếm các máy tính có lỗ hổng bảo mật trong dịch vụ mạng. Một mã khai thác trong một tập tin DOC sử dụng lỗ hổng bảo mật của trình xử lý văn bản. Nó có thể bắt đầu thực hiện hành động đã được lập trình sẵn bởi tin tặc khi người dùng mở tập tin bị nhiễm. Một mã khai thác được nhúng trong một email sẽ tìm kiếm lỗ hổng bảo mật trong một trình khách email bất kỳ. Nó có thể bắt đầu thực thi hành động độc hại ngay khi người dùng mở ra một email bị nhiễm trong trình khách email này.</p> <p>Net-Worm được phát tán qua mạng sử dụng các mã khai thác này. Mã khai thác Nuker là các gói tin mạng làm vô hiệu máy tính.</p>
FileCryptor	Trình mã hóa	Chúng mã hóa các ứng dụng độc hại khác để che giấu các chương trình này khỏi ứng dụng chống virus.
Flooder	Chương trình "gây lụt" mạng	<p>Chúng sẽ gửi vô số tin nhắn qua các kênh mạng. Loại công cụ này bao gồm, ví dụ, các chương trình gây lụt Phòng Tán gẫu IRC.</p> <p>Các công cụ kiểu Flooder không chứa các chương trình "gây lụt" các kênh được sử dụng bởi email, ứng dụng nhắn tin nhanh và hệ thống truyền thông di động. Những chương trình này được phân loại là các kiểu riêng biệt được mô tả trong bảng (Email-Flooder, IM-Flooder, và SMS-Flooder).</p>

HackTool	Công cụ hack	Chúng hỗ trợ việc hack máy tính mà chúng được cài đặt trên đó hoặc tấn công một máy tính khác (ví dụ, bằng cách bổ sung các tài khoản hệ thống mới mà không có sự cho phép của người dùng hoặc xóa nhật ký hệ thống để che dấu vết hiện diện của chúng trong hệ điều hành). Loại công cụ này bao gồm một số sniffer có chức năng độc hại, như đánh cắp mật khẩu. Sniffer là các chương trình cho phép xem lưu lượng mạng.
Hoax	Mã lừa đảo	Chúng sẽ cảnh báo người dùng với các tin nhắn giống virus như: chúng có thể "phát hiện một virus" trong một tập tin không bị nhiễm hoặc thông báo với người dùng rằng ổ đĩa đã được định dạng lại, mặc dù thực tế điều này không xảy ra.
Spoofing	Công cụ spoof	Chúng sẽ gửi tin nhắn và yêu cầu mạng với địa chỉ người gửi giả mạo. Kẻ xâm nhập có thể sử dụng các công cụ Spoofing để giả mạo là người gửi tin nhắn thật.
VirTool	Công cụ sửa đổi các ứng dụng độc hại	Chúng cho phép sửa đổi các phần mềm độc hại khác, che giấu chúng khỏi ứng dụng chống virus.
Email-Flooder	Các chương trình "gây lụt" địa chỉ email	Chúng gửi nhiều tin nhắn đến các địa chỉ email khác nhau, "gây lụt" cho các địa chỉ này. Một lượng lớn thư đến sẽ khiến người dùng không thể xem các email hữu ích trong hộp thư đến của họ.
IM-Flooder	Các chương trình "gây lụt" cho ứng dụng nhắn tin nhanh	Chúng sẽ gửi tin nhắn gây lụt cho người dùng của các ứng dụng nhắn tin nhanh. Một lượng lớn tin nhắn sẽ khiến người dùng không thể xem các tin nhắn đến hữu ích.
SMS-Flooder	Các chương trình "gây lụt" cho tin nhắn SMS	Chúng sẽ gửi hàng loạt tin nhắn SMS đến điện thoại di động.

- [Phần mềm quảng cáo](#) 

Danh mục con: phần mềm quảng cáo;

Mức độ mối đe dọa: trung bình

Phần mềm quảng cáo hiển thị thông tin quảng cáo đến người dùng. Các chương trình phần mềm quảng cáo hiển thị bảng quảng cáo trong giao diện của các chương trình khác và điều hướng các truy vấn tìm kiếm đến những trang web quảng cáo. Một số còn thu thập thông tin tiếp thị về người dùng và gửi nó đến nhà phát triển: thông tin này có thể bao gồm tên của các website được truy cập bởi người dùng hoặc nội dung truy vấn tìm kiếm của người dùng. Khác với các chương trình Trojan-Gián điệp, phần mềm quảng cáo gửi thông tin này đến nhà phát triển với sự cho phép của người dùng.

- [Phần mềm quay số tự động](#) 

Danh mục con: 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 của bạn.

Cấp độ nguy hiểm: trung bình

Hầu hết các ứng dụng này đều hữu ích, vậy nên có rất nhiều người dùng sử dụng chúng. Các ứng dụng này bao gồm các trình khách IRC, phần mềm tự động quay số, chương trình tải về tập tin, trình giám sát hoạt động hệ thống máy tính, tiện ích mật khẩu, và máy chủ Internet cho FTP, HTTP và Telnet.

Tuy nhiên, nếu kẻ xâm nhập truy cập được vào những chương trình này, hoặc cấy chúng lên máy tính của người dùng, một số tính năng của ứng dụng có thể được sử dụng để phá hoại tính bảo mật.

Các ứng dụng này khác nhau theo chức năng; các phân loại của chúng được mô tả theo bảng dưới đây.

Loại	Tên	Mô tả
Client-IRC	Trình tán gẫu Internet	Người dùng cài đặt các chương trình này để nói chuyện với mọi người trong Phòng Tán gẫu IRC. Kẻ xâm nhập sử dụng chúng để phát tán phần mềm độc hại.
Trình gọi	Phần mềm quay số tự động	Chúng có thể thiết lập kết nối điện thoại qua modem trong chế độ ẩn.
Trình tải về	Chương trình để tải về	Chúng có thể tải về tập tin từ các trang web trong chế độ ẩn.
Giám sát	Chương trình giám sát	Chúng cho phép hoạt động giám sát trên máy tính mà chúng được cài đặt (xem ứng dụng nào đang hoạt động và cách chúng trao đổi dữ liệu với các ứng dụng được cài đặt trên máy tính khác).
PSWTool	Công cụ khôi phục mật khẩu	Chúng cho phép xem và khôi phục mật khẩu bị quên. Kẻ xâm nhập sẽ ngấm cấy chúng trên máy tính của người dùng với mục đích tương tự.
RemoteAdmin	Chương trình quản trị từ xa	Chúng thường được sử dụng bởi quản trị viên hệ thống. Những chương trình này cho phép truy cập đến giao diện của một máy tính từ xa nhằm mục đích giám sát và quản lý nó. Kẻ xâm nhập sẽ ngấm cấy chúng trên máy tính của người dùng với mục đích tương tự: để giám sát và quản lý các máy tính từ xa. Các chương trình quản trị từ xa hợp pháp khác với các Trojan Backdoor cho quản trị từ xa. Trojan có khả năng tự xâm nhập hệ điều hành và tự cài đặt; các chương trình hợp pháp không thể làm điều này.
Server-FTP	Máy chủ FTP	Chúng có chức năng là các máy chủ FTP. Kẻ xâm nhập sẽ cấy chúng lên máy tính của người dùng để truy cập từ xa đến máy tính qua FTP.
Server-Proxy	Máy chủ	Chúng có chức năng là các máy chủ proxy. Kẻ xâm nhập sẽ cấy chúng lên máy tính của người dùng để gửi thư rác với

	proxy	tên của người dùng.
Server-Telnet	Máy chủ Telnet	Chúng có chức năng là các máy chủ Telnet. Kẻ xâm nhập sẽ cấy chúng lên máy tính của người dùng để truy cập từ xa đến máy tính qua Telnet.
Server-Web	Máy chủ web	Chúng có chức năng là các máy chủ web. Kẻ xâm nhập sẽ cấy chúng lên máy tính của người dùng để truy cập từ xa đến máy tính qua HTTP.
RiskTool	Công cụ để làm việc trên máy tính nội bộ	Chúng cung cấp cho người dùng những tính năng bổ sung khi làm việc trên máy tính của người dùng. Các công cụ này cho phép người dùng ẩn tập tin hoặc cửa sổ của các ứng dụng đang hoạt động và chấm dứt các tiến trình đang hoạt động.
NetTool	Công cụ mạng	Chúng cung cấp cho người dùng những tính năng bổ sung khi làm việc với các máy tính khác trên mạng lưới. Các công cụ này cho phép khởi động lại chúng, phát hiện các cổng mở, và bắt đầu các ứng dụng được cài đặt trên máy tính.
Client-P2P	Trình khách mạng P2P	Chúng cho phép làm việc trên các mạng ngang hàng. Chúng có thể được sử dụng bởi kẻ xâm nhập để phát tán phần mềm độc hại.
Client-SMTP	Trình khách SMTP	Chúng gửi email mà không có kiến thức của người dùng. Kẻ xâm nhập sẽ cấy chúng lên máy tính của người dùng để gửi thư rác với tên của người dùng.
WebToolbar	Thanh công cụ web	Chúng bổ sung thanh công cụ vào giao diện của các ứng dụng khác để sử dụng công nghệ tìm kiếm.
FraudTool	Chương trình giả	Chúng giả làm các chương trình khác. Ví dụ, có các chương trình chống virus giả có tác dụng hiển thị thông báo về phát hiện phần mềm độc hại. Tuy nhiên, trong thực tế, chúng không tìm thấy hay khử nhiễm bất cứ thứ gì.

- **Phát hiện các phần mềm khác có thể được sử dụng bởi kẻ xâm nhập để phá hoại máy tính hoặc dữ liệu cá nhân của bạn** [\[2\]](#);

Danh mục con: 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 của bạn.

Cấp độ nguy hiểm: trung bình

Hầu hết các ứng dụng này đều hữu ích, vậy nên có rất nhiều người dùng sử dụng chúng. Các ứng dụng này bao gồm các trình khách IRC, phần mềm tự động quay số, chương trình tải về tập tin, trình giám sát hoạt động hệ thống máy tính, tiện ích mật khẩu, và máy chủ Internet cho FTP, HTTP và Telnet.

Tuy nhiên, nếu kẻ xâm nhập truy cập được vào những chương trình này, hoặc cấy chúng lên máy tính của người dùng, một số tính năng của ứng dụng có thể được sử dụng để phá hoại tính bảo mật.

Các ứng dụng này khác nhau theo chức năng; các phân loại của chúng được mô tả theo bảng dưới đây.

Loại	Tên	Mô tả
Client-IRC	Trình tán gẫu Internet	Người dùng cài đặt các chương trình này để nói chuyện với mọi người trong Phòng Tán gẫu IRC. Kẻ xâm nhập sử dụng chúng để phát tán phần mềm độc hại.
Trình gọi	Phần mềm quay số tự động	Chúng có thể thiết lập kết nối điện thoại qua modem trong chế độ ẩn.
Trình tải về	Chương trình để tải về	Chúng có thể tải về tập tin từ các trang web trong chế độ ẩn.
Giám sát	Chương trình giám sát	Chúng cho phép hoạt động giám sát trên máy tính mà chúng được cài đặt (xem ứng dụng nào đang hoạt động và cách chúng trao đổi dữ liệu với các ứng dụng được cài đặt trên máy tính khác).
PSWTool	Công cụ khôi phục mật khẩu	Chúng cho phép xem và khôi phục mật khẩu bị quên. Kẻ xâm nhập sẽ ngấm cấy chúng trên máy tính của người dùng với mục đích tương tự.
RemoteAdmin	Chương trình quản trị từ xa	Chúng thường được sử dụng bởi quản trị viên hệ thống. Những chương trình này cho phép truy cập đến giao diện của một máy tính từ xa nhằm mục đích giám sát và quản lý nó. Kẻ xâm nhập sẽ ngấm cấy chúng trên máy tính của người dùng với mục đích tương tự: để giám sát và quản lý các máy tính từ xa. Các chương trình quản trị từ xa hợp pháp khác với các Trojan Backdoor cho quản trị từ xa. Trojan có khả năng tự xâm nhập hệ điều hành và tự cài đặt; các chương trình hợp pháp không thể làm điều này.
Server-FTP	Máy chủ FTP	Chúng có chức năng là các máy chủ FTP. Kẻ xâm nhập sẽ cấy chúng lên máy tính của người dùng để truy cập từ xa đến máy tính qua FTP.
Server-Proxy	Máy chủ	Chúng có chức năng là các máy chủ proxy. Kẻ xâm nhập sẽ cấy chúng lên máy tính của người dùng để gửi thư rác với

	proxy	tên của người dùng.
Server-Telnet	Máy chủ Telnet	Chúng có chức năng là các máy chủ Telnet. Kẻ xâm nhập sẽ cấy chúng lên máy tính của người dùng để truy cập từ xa đến máy tính qua Telnet.
Server-Web	Máy chủ web	Chúng có chức năng là các máy chủ web. Kẻ xâm nhập sẽ cấy chúng lên máy tính của người dùng để truy cập từ xa đến máy tính qua HTTP.
RiskTool	Công cụ để làm việc trên máy tính nội bộ	Chúng cung cấp cho người dùng những tính năng bổ sung khi làm việc trên máy tính của người dùng. Các công cụ này cho phép người dùng ẩn tập tin hoặc cửa sổ của các ứng dụng đang hoạt động và chấm dứt các tiến trình đang hoạt động.
NetTool	Công cụ mạng	Chúng cung cấp cho người dùng những tính năng bổ sung khi làm việc với các máy tính khác trên mạng lưới. Các công cụ này cho phép khởi động lại chúng, phát hiện các cổng mở, và bắt đầu các ứng dụng được cài đặt trên máy tính.
Client-P2P	Trình khách mạng P2P	Chúng cho phép làm việc trên các mạng ngang hàng. Chúng có thể được sử dụng bởi kẻ xâm nhập để phát tán phần mềm độc hại.
Client-SMTP	Trình khách SMTP	Chúng gửi email mà không có kiến thức của người dùng. Kẻ xâm nhập sẽ cấy chúng lên máy tính của người dùng để gửi thư rác với tên của người dùng.
WebToolbar	Thanh công cụ web	Chúng bổ sung thanh công cụ vào giao diện của các ứng dụng khác để sử dụng công nghệ tìm kiếm.
FraudTool	Chương trình giả	Chúng giả làm các chương trình khác. Ví dụ, có các chương trình chống virus giả có tác dụng hiển thị thông báo về phát hiện phần mềm độc hại. Tuy nhiên, trong thực tế, chúng không tìm thấy hay khử nhiễm bất cứ thứ gì.

- Đối tượng được đóng gói mà việc đóng gói có thể được sử dụng để bảo vệ các mã độc hại;

Kaspersky Endpoint Security sẽ quét các đối tượng nén và mô-đun giải nén trong các tập nén SFX (tự động giải nén).

Để giấu các chương trình nguy hiểm khỏi ứng dụng chống virus, kẻ xâm nhập thường sẽ nén chúng sử dụng các trình nén đặc biệt hoặc tạo các tập tin đóng gói nhiều lớp.

Các chuyên gia phân tích virus của Kaspersky đã xác định các trình nén phổ biến nhất trong giới tin tặc.

Nếu Kaspersky Endpoint Security phát hiện một trình đóng gói như vậy trong một tập tin, tập tin đó có nhiều khả năng sẽ chứa một ứng dụng độc hại hoặc một ứng dụng có thể được sử dụng bởi bọn tội phạm để gây hại cho máy tính hoặc dữ liệu cá nhân của bạn.

Kaspersky Endpoint Security sẽ tập trung vào các loại chương trình sau:

- *Các tập tin được đóng gói có thể gây hại* – sử dụng để đóng gói phần mềm độc hại, ví dụ như virus, sâu và Trojan.
- *Các tập tin đóng gói nhiều lớp* (cấp độ đe dọa trung bình) – đối tượng này đã được đóng gói ba lần bởi một hoặc nhiều trình đóng gói.

- **Các đối tượng đóng gói đa thành phần** 

Kaspersky Endpoint Security sẽ quét các đối tượng nén và mô-đun giải nén trong các tập nén SFX (tự động giải nén).

Để giấu các chương trình nguy hiểm khỏi ứng dụng chống virus, kẻ xâm nhập thường sẽ nén chúng sử dụng các trình nén đặc biệt hoặc tạo các tập tin đóng gói nhiều lớp.

Các chuyên gia phân tích virus của Kaspersky đã xác định các trình nén phổ biến nhất trong giới tin tặc.

Nếu Kaspersky Endpoint Security phát hiện một trình đóng gói như vậy trong một tập tin, tập tin đó có nhiều khả năng sẽ chứa một ứng dụng độc hại hoặc một ứng dụng có thể được sử dụng bởi bọn tội phạm để gây hại cho máy tính hoặc dữ liệu cá nhân của bạn.

Kaspersky Endpoint Security sẽ tập trung vào các loại chương trình sau:

- *Các tập tin được đóng gói có thể gây hại* – sử dụng để đóng gói phần mềm độc hại, ví dụ như virus, sâu và Trojan.
- *Các tập tin đóng gói nhiều lớp* (cấp độ đe dọa trung bình) – đối tượng này đã được đóng gói ba lần bởi một hoặc nhiều trình đóng gói.

4. Lưu các thay đổi của bạn.

Sửa 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 của ứng dụng và kiểm soát hoạt động của tất cả các ứng dụng và lưu lượng mạng được tạo bởi chúng. Tuy nhiên, một ứng dụng đã được thêm vào danh sách các ứng dụng được tin tưởng sẽ được Kaspersky Endpoint Security loại trừ khỏi các 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 các 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.

[Cách thêm ứng dụng vào danh sách được tin tưởng trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Loại trừ**.
6. Trong mục **Loại trừ quét và ứng dụng được tin tưởng**, hãy nhấn nút **Thiết lập**.
7. Trong cửa sổ mở ra, hãy chọn thẻ **Ứng dụng được tin tưởng**.
Thao tác này sẽ mở cửa sổ chứa danh sách các ứng dụng được tin tưởng.
8. Chọn hộp kiểm **Hợp nhất các giá trị khi kế thừa** nếu bạn muốn tạo một danh sách tổng hợp các ứng dụng được tin tưởng cho tất cả các máy tính trong công ty. Danh sách các ứng dụng được tin tưởng trong chính sách cha và chính sách con sẽ được hợp nhất. Các danh sách sẽ được hợp nhất với điều kiện các giá trị hợp nhất khi kế thừa được bật. Các ứng dụng được tin tưởng từ chính sách cha được hiển thị trong chính sách con ở chế độ chỉ đọc. Không thể thay đổi hay xóa các ứng dụng được tin tưởng của chính sách cha.
9. Chọn hộp kiểm **Cho phép sử dụng các ứng dụng được tin tưởng cục bộ** nếu bạn muốn cho phép người dùng tạo danh sách ứng dụng cục bộ được tin tưởng. Bằng cách này, người dùng có thể tạo danh sách ứng dụng cục bộ được tin tưởng của riêng họ ngoài danh sách ứng dụng chung được tin tưởng được tạo trong chính sách. Quản trị viên có thể sử dụng Kaspersky Security Center để xem, thêm, chỉnh sửa hoặc xóa các mục danh sách trong thuộc tính máy tính.
Nếu hộp kiểm bị xóa, người dùng chỉ có thể truy cập danh sách ứng dụng chung được tin tưởng được tạo trong chính sách.
10. Nhấn vào **Thêm**.
11. Trong cửa sổ mở ra, hãy nhập đường dẫn đến tập tin thực thi của ứng dụng được tin tưởng.
Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự * cùng ? khi nhập tên đại diện.

Kaspersky Endpoint Security không hỗ trợ biến môi trường %userprofile% khi tạo một danh sách các ứng dụng được tin tưởng trên bảng điều khiển Kaspersky Security Center. Để áp dụng mục cho tất cả các tài khoản người dùng, bạn có thể sử dụng ký tự * (ví dụ: C:\Users*\Documents\File.exe).

Bất cứ khi nào thêm một biến môi trường mới, bạn cần khởi động lại ứng dụng.
12. Cấu hình thiết lập nâng cao cho ứng dụng được tin tưởng (xem bảng bên dưới).
13. Bạn có thể sử dụng hộp kiểm để [loại trừ một ứng dụng khỏi vùng tin tưởng](#) bất kỳ lúc nào.
14. Lưu các thay đổi của bạn.


Cách thêm một ứng dụng vào danh sách được tin tưởng trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Thiết lập tổng quát** → **Loại trừ**.
5. Trong mục **Loại trừ quét và ứng dụng được tin tưởng**, nhấn liên kết **Ứng dụng được tin tưởng**.
Thao tác này sẽ mở cửa sổ chứa danh sách các ứng dụng được tin tưởng.
6. Chọn hộp kiểm **Hợp nhất các giá trị khi kế thừa** nếu bạn muốn tạo một danh sách tổng hợp các ứng dụng được tin tưởng cho tất cả các máy tính trong công ty. Danh sách các ứng dụng được tin tưởng trong chính sách cha và chính sách con sẽ được hợp nhất. Các danh sách sẽ được hợp nhất với điều kiện các giá trị hợp nhất khi kế thừa được bật. Các ứng dụng được tin tưởng từ chính sách cha được hiển thị trong chính sách con ở chế độ chỉ đọc. Không thể thay đổi hay xóa các ứng dụng được tin tưởng của chính sách cha.
7. Chọn hộp kiểm **Cho phép sử dụng các ứng dụng được tin tưởng cục bộ** nếu bạn muốn cho phép người dùng tạo danh sách ứng dụng cục bộ được tin tưởng. Bằng cách này, người dùng có thể tạo danh sách ứng dụng cục bộ được tin tưởng của riêng họ ngoài danh sách ứng dụng chung được tin tưởng được tạo trong chính sách. Quản trị viên có thể sử dụng Kaspersky Security Center để xem, thêm, chỉnh sửa hoặc xóa các mục danh sách trong thuộc tính máy tính.
Nếu hộp kiểm bị xóa, người dùng chỉ có thể truy cập danh sách ứng dụng chung được tin tưởng được tạo trong chính sách.
8. Nhấn vào **Thêm**.
9. Trong cửa sổ mở ra, hãy nhập đường dẫn đến tập tin thực thi của ứng dụng được tin tưởng. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự * cùng ? khi nhập tên đại diện.

Kaspersky Endpoint Security không hỗ trợ biến môi trường %userprofile% khi tạo một danh sách các ứng dụng được tin tưởng trên bảng điều khiển Kaspersky Security Center. Để áp dụng mục cho tất cả các tài khoản người dùng, bạn có thể sử dụng ký tự * (ví dụ: C:\Users*\Documents\File.exe).

Bất cứ khi nào thêm một biến môi trường mới, bạn cần khởi động lại ứng dụng.
10. Cấu hình thiết lập nâng cao cho ứng dụng được tin tưởng (xem bảng bên dưới).
11. Bạn có thể sử dụng hộp kiểm để [loại trừ một ứng dụng khỏi vùng tin tưởng](#) bất kỳ lúc nào.
12. Lưu các thay đổi của bạn.

Cách thêm một ứng dụng vào danh sách được tin tưởng trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Mối đe dọa và loại trừ**.
3. Trong mục **Loại trừ**, hãy nhấn liên kết **Chỉ định ứng dụng được tin tưởng**.
4. Trong cửa sổ mở ra, hãy nhấn vào nút **Thêm**.
5. Chọn tập tin thực thi của ứng dụng được tin tưởng.

Bạn cũng có thể nhập đường dẫn theo cách thủ công. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự * cùng ? khi nhập tên đại diện.

Kaspersky Endpoint Security hỗ trợ các biến môi trường và chuyển đổi đường dẫn trong giao diện cục bộ của ứng dụng. Nói cách khác, nếu bạn nhập đường dẫn tập tin %userprofile%\Documents\File.exe thì một bản ghi C:\Users\Fred123\Documents\File.exe sẽ được thêm vào giao diện cục bộ của ứng dụng cho người dùng Fred123. Theo đó, Kaspersky Endpoint Security sẽ bỏ qua chương trình được tin tưởng File.exe cho những người dùng khác. Để áp dụng mục cho tất cả các tài khoản người dùng, bạn có thể sử dụng ký tự * (ví dụ: C:\Users*\Documents\File.exe).

Bất cứ khi nào thêm một biến môi trường mới, bạn cần khởi động lại ứng dụng.

6. Trong cửa sổ thuộc tính ứng dụng được tin tưởng, hãy cấu hình thiết lập nâng cao (xem bảng bên dưới).
7. Bạn có thể sử dụng nút bật/tắt để [loại trừ ứng dụng khỏi vùng tin tưởng](#) bất kỳ lúc nào.
8. Lưu các thay đổi của bạn.


Thiết lập ứng dụng được tin tưởng

Tham số	Mô tả
Không quét tập tin trước khi mở	Kaspersky Endpoint Security sẽ không quét các tập tin được mở bởi ứng dụng đó. Ví dụ: nếu bạn đang sử dụng các ứng dụng để sao lưu tập tin, tính năng này giúp giảm mức sử dụng tài nguyên bởi Kaspersky Endpoint Security.
Không giám sát hoạt động ứng dụng	Kaspersky Endpoint Security sẽ không giám sát hoạt động mạng và tập tin của ứng dụng trong hệ điều hành. Hoạt động ứng dụng được giám sát bởi các thành phần sau: Phát hiện hành vi , Phòng chống khai thác , Phòng chống xâm nhập máy chủ , Công cụ khắc phục và Tường lửa .
Không kế thừa các hạn chế từ tiến trình cha (ứng dụng)	Các hạn chế được cấu hình cho tiến trình cha sẽ không được Kaspersky Endpoint Security áp dụng cho tiến trình con. Tiến trình cha được khởi chạy bởi một ứng dụng mà các quyền ứng dụng (Phòng chống xâm nhập máy chủ) và quy tắc mạng ứng dụng (Tường lửa) được cấu hình.
Không giám sát hoạt động của ứng dụng con	Kaspersky Endpoint Security sẽ không giám sát hoạt động mạng và hoạt động tập tin của các ứng dụng được khởi chạy bởi ứng dụng này.

Cho phép tương tác với giao diện ứng dụng	Thành phần Tự bảo vệ của Kaspersky Endpoint Security sẽ chặn mọi nỗ lực quản lý các dịch vụ ứng dụng trên máy tính từ xa. Nếu hộp kiểm này được chọn, ứng dụng truy cập từ xa sẽ được phép quản lý cấu hình của Kaspersky Endpoint Security thông qua giao diện Kaspersky Endpoint Security.
Không chặn tương tác với thành phần Bảo vệ AMSI	Kaspersky Endpoint Security sẽ không giám sát các yêu cầu của ứng dụng được tin tưởng đối với các đối tượng được quét bởi thành phần Bảo vệ AMSI .
Không quét lưu lượng mạng	Lưu lượng mạng bắt nguồn từ ứng dụng này sẽ được Kaspersky Endpoint Security loại trừ khỏi tác vụ quét. Bạn có thể loại trừ tất cả lưu lượng hoặc chỉ lưu lượng được mã hóa khỏi tác vụ quét. Bạn cũng có thể loại trừ các địa chỉ IP và mã hiệu cổng riêng lẻ khỏi tác vụ quét.
Bình luận	Nếu cần, bạn có thể cung cấp chú thích ngắn gọn cho ứng dụng được tin tưởng. Nhận xét giúp đơn giản hóa việc tìm kiếm và sắp xếp các ứng dụng được tin tưởng.
Trạng thái	Trạng thái của ứng dụng được tin tưởng: <ul style="list-style-type: none"> • Trạng thái Hoạt động có nghĩa là ứng dụng đang ở trong vùng tin tưởng. • Trạng thái Không hoạt động có nghĩa là ứng dụng bị loại trừ khỏi vùng tin tưởng.

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. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Mối đe dọa và loại trừ**.
3. Trong mục **Loại trừ**, hãy nhấn liên kết **Chỉ định ứng dụng được tin tưởng**.
4. Trong danh sách các ứng dụng được tin tưởng, chọn ứng dụng được tin tưởng cần thiết.
5. Sử dụng nút bật/tắt trong cột **Trạng thái** để thêm hoặc loại trừ ứng dụng được tin tưởng vào/khỏi phạm vi quét.
6. Lưu các thay đổi của bạn.

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. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Mối đe dọa và loại trừ**.
3. Trong danh sách thả xuống **Kho chứng chỉ hệ thống tin tưởng**, hãy chọn kho hệ thống sẽ được Kaspersky Endpoint Security coi là tin tưởng.
4. Lưu các thay đổi của bạn.

Quản lý Sao lưu

Sao lưu sẽ lưu trữ bản sao lưu của các tập tin đã bị xóa hoặc sửa đổi trong quá trình khử mã độc. *Bản sao lưu* là một bản sao của tập tin được tạo trước khi tập tin đó được khử nhiễm hay xóa. Các bản sao lưu của tập tin được lưu trữ trong một định dạng đặc biệt và không gây ra mối đe dọa.

Những bản sao lưu này được lưu trữ trong thư mục C:\ProgramData\Kaspersky Lab\KES\QB.

Người dùng trong nhóm Quản trị viên được cấp quyền truy cập toàn diện vào thư mục này. Quyền truy cập giới hạn vào thư mục này được cấp cho người dùng có tài khoản được sử dụng để cài đặt Kaspersky Endpoint Security.

Kaspersky Endpoint Security không có khả năng cấu hình quyền truy cập của người dùng vào các bản sao lưu tập tin.


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 tập tin từ bản sao lưu đến thư mục gốc của nó.

Nếu Kaspersky Endpoint Security đang được quản lý bởi Kaspersky Security Center, các bản sao lưu tập tin có thể được truyền tải đến Kaspersky Security Center Administration Server. Để biết thêm chi tiết về việc quản lý các bản sao lưu tập tin trong Kaspersky Security Center, vui lòng tham khảo hệ thống Trợ giúp của Kaspersky Security Center.

Cấu hình thời gian lưu trữ tối đa cho các tập tin trong Sao lưu

Thời gian lưu trữ tối đa mặc định cho các tập tin trong Sao lưu là 30 ngày. Sau khi thời gian lưu trữ tối đa đã kết thúc, Kaspersky Endpoint Security sẽ xóa các tập tin cũ nhất khỏi Sao lưu.


Để cấu hình thời gian lưu trữ tối đa cho các tập tin trong Sao lưu:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn mục **Thiết lập tổng quát** → **Các báo cáo và lưu trữ**.
3. Nếu bạn muốn giới hạn thời gian lưu trữ cho các bản sao của tập tin trong Sao lưu, hãy chọn hộp kiểm **Lưu trữ đối tượng trong N ngày** trong mục **Sao lưu**. Nhập thời gian lưu trữ tối đa cho các bản sao tập tin trong Sao lưu.
4. Lưu các thay đổi của bạn.

Cấu hình kích cỡ tối đa của Sao lưu

Bạn có thể chỉ định dung lượng tối đa của Sao lưu. Theo mặc định, kích cỡ của Sao lưu là không giới hạn. Sau khi đạt được kích cỡ tối đa, Kaspersky Endpoint Security sẽ tự động xóa các tập tin cũ nhất khỏi Sao lưu.

Để cấu hình kích cỡ tối đa của Sao lưu:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn mục **Thiết lập tổng quát** → **Các báo cáo và lưu trữ**.
3. Nếu bạn muốn giới hạn dung lượng của Sao lưu, hãy chọn hộp kiểm **Giới hạn dung lượng của bản Sao lưu ở mức N MB** trong mục **Sao lưu**. Quy định dung lượng tối đa của Sao lưu.
4. Lưu các thay đổi của bạn.

Khôi phục các tập tin từ Sao lưu

Nếu một mã độc được phát hiện trong một tập tin, Kaspersky Endpoint Security sẽ chặn tập tin đó, gán trạng thái *Nhiễm mã độc* cho nó, 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 lưu của tập tin sẽ được chuyển thành *Được khử mã độc*. 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 lưu đến thư mục gốc của nó.

Không thể khôi phục các tập tin có trạng thái *Sẽ được khử mã độc khi khởi động lại máy tính*. Hãy khởi động lại máy tính, khi đó trạng thái tập tin sẽ đổi thành *Được khử mã độc* hoặc *Bị xóa*. Bạn cũng có thể khôi phục tập tin đó từ bản sao lưu đến thư mục gốc của tập tin.

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).

Danh sách các bản sao lưu của tập tin được trình bày dưới dạng bảng. Đối với bản sao lưu của một tập tin, đường dẫn đến thư mục gốc của tập tin đó sẽ được hiển thị. Đường dẫn đến thư mục gốc của tập tin có thể chứa dữ liệu cá nhân.

Nếu nhiều tập tin có tên giống nhau và nội dung khác nhau được đặt trong cùng một thư mục được di chuyển đến Sao lưu, chỉ tập tin có vị trí cuối cùng trong Sao lưu mới có thể được khôi phục.

Để khôi phục các tập tin từ Sao lưu:

1. Trong cửa sổ chính của ứng dụng, trong mục **Giám sát**, hãy nhấn vào ô **Sao lưu**.
2. Thao tác này sẽ mở danh sách các tập tin trong Sao lưu; trong danh sách đó, hãy chọn các tập tin mà bạn muốn khôi phục và nhấn vào **Khôi phục**.

Kaspersky Endpoint Security sẽ khôi phục tất cả tập tin từ bản sao lưu được chọn đến thư mục gốc của chúng.

Xóa bản sao lưu của tập tin khỏi Sao lưu

Kaspersky Endpoint Security sẽ tự động xóa các bản sao lưu của các tập tin thuộc bất cứ trạng thái nào khỏi Sao lưu sau khi thời hạn lưu trữ được cấu hình 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.

Để xóa bản sao lưu của tập tin khỏi Sao lưu:

1. Trong cửa sổ chính của ứng dụng, trong mục **Giám sát**, hãy nhấn vào ô **Sao lưu**.
2. Thao tác này sẽ mở ra danh sách các tập tin trong Sao lưu; trong danh sách này, hãy chọn các tập tin mà bạn muốn xóa khỏi Sao lưu và nhấn vào **Xóa**.

Kaspersky Endpoint Security sẽ xóa các bản sao lưu được chọn của tập tin khỏi Sao lưu.

Dịch vụ thông báo

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 các 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.

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.

Cấu hình cấu hình nhật ký sự kiện

Để thiết lập cấu hình nhật ký sự kiện:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, chọn **Thiết lập tổng quát** → **Giao diện**.
3. Trong mục **Thông báo**, hãy nhấn nút **Thiết lập 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.


Các sự kiện có thể chứa dữ liệu người dùng sau:

- Đường dẫn đến các tập tin được quét bởi Kaspersky Endpoint Security.
- Đường dẫn đến các khóa registry được sửa đổi trong quá trình hoạt động của Kaspersky Endpoint Security.
- Tên người dùng Microsoft Windows.
- Địa chỉ của các trang web được mở bởi người dùng.

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 trong báo cáo cục bộ** và **Lưu trong nhật ký sự kiện của Windows**.
Các sự kiện có hộp kiểm được chọn trong cột **Lưu trong báo cáo cục bộ** sẽ được hiển thị trong [nhật ký ứng dụng](#). Các sự kiện có hộp kiểm trong cột **Lưu trong nhật ký sự kiện của Windows** được chọn sẽ được hiển thị trong Nhật ký Windows và trong kênh Application.
6. Lưu các thay đổi của bạn.

Cấu hình việc hiển thị và truyền tải thông báo

Để thiết lập việc hiển thị và truyền tải thông báo:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, chọn **Thiết lập tổng quát** → **Giao diện**.
3. Trong mục **Thông báo**, hãy nhấn nút **Thiết lập 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.
Các sự kiện có thể chứa dữ liệu người dùng sau:
 - Đường dẫn đến các tập tin được quét bởi Kaspersky Endpoint Security.
 - Đường dẫn đến các khóa registry được sửa đổi trong quá trình hoạt động của Kaspersky Endpoint Security.
 - Tên người dùng Microsoft Windows.
 - Địa chỉ của các trang web được mở bởi người dùng.
4. Ở phần bên trái của cửa sổ, chọn thành phần hoặc tác vụ mà bạn muốn cấu hình phương thức thông báo.
5. Trong cột **Thông báo trên màn hình**, hãy chọn các hộp kiểm cạnh các sự kiện liên quan.
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 qua email**, hãy chọn các hộp kiểm cạnh các sự kiện liên quan.
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 **OK**.
8. Nếu bạn đã bật thông báo qua email, hãy cấu hình thiết lập để gửi email:
 - a. Nhấn vào **Thiết lập thông báo email**.
 - b. Chọn hộp kiểm **Thông báo về các sự kiện** để cho phép gửi thông tin về các sự kiện Kaspersky Endpoint Security được chọn trong cột **Thông báo qua email**.

c. Quy định cấu hình gửi thông báo qua email.


Kaspersky Endpoint Security chỉ hỗ trợ xác thực SMTP cơ bản. Thiết lập ứng dụng không cung cấp tùy chọn để cấu hình sử dụng TLS. Bạn có thể cấu hình thông báo trong thuộc tính của Máy chủ quản trị Kaspersky Security Center. Kaspersky Security Center hỗ trợ sử dụng TLS cho máy chủ SMTP.



d. Nhấn **OK**.

9. Lưu các thay đổi của bạn.

Cấu hình việc hiển thị cảnh báo về trạng thái ứng dụng trong khu vực thông báo

Để cấu hình việc hiển thị cảnh báo về trạng thái ứng dụng trong khu vực thông báo:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, chọn **Thiết lập tổng quát** → **Giao diện**.
3. Trong mục **Hiển thị trạng thái của ứng dụng trong khu vực thông 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. Lưu các thay đổi của bạn.

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.

Nhắn tin giữa người dùng và quản trị viên

Các thành phần [Kiểm soát ứng dụng](#), [Kiểm soát thiết bị](#), [Kiểm soát Web](#) và [Kiểm soát thích ứng sự cố](#) 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 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 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 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 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 Endpoint Security, 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 Endpoint Security, các tin nhắn tiêu chuẩn sẽ được gửi đến Máy chủ quản trị 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 (xem chỉ dẫn bên dưới). 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 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.

Để xem tin nhắn của người dùng trong kho lưu trữ sự kiện của Kaspersky Security Center:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong nút **Administration Server** của cây Bảng điều khiển quản trị, chọn thẻ **Events**. 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 **Event selections**, chọn **User requests**.
4. Chọn tin nhắn để gửi đến quản trị viên.
5. Nhấn vào nút **Open event properties window** ở phần bên phải của không gian làm việc của Bảng điều khiển quản trị.


Quản lý báo cáo

Thông tin về hoạt động của mỗi thành phần Kaspersky Endpoint Security, sự kiện mã hóa dữ liệu, hiệu quả của mỗi tác vụ quét, tác vụ cập nhật và tác vụ kiểm tra tính toàn vẹn cùng với hoạt động tổng thể của ứng dụng sẽ được ghi trong báo cáo.

Các bản báo cáo được lưu trữ trong thư mục C:\ProgramData\Kaspersky Lab\KES\Report.

Bản báo cáo có thể chứa các dữ liệu người dùng sau:

- Đường dẫn đến các tập tin được quét bởi Kaspersky Endpoint Security.
- Đường dẫn đến các khóa registry được sửa đổi trong quá trình hoạt động của Kaspersky Endpoint Security.
- Tên người dùng Microsoft Windows.
- Địa chỉ của các trang web được mở bởi người dùng.


Dữ liệu trong báo cáo được trình bày dưới dạng bảng. 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, hãy nhấn nút  cạnh tên của cột. Các sự kiện được ghi lại trong quá trình hoạt động của các thành phần khác nhau hoặc trong quá trình thực hiện các 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 về hoạt động của các thành phần của Kaspersky Endpoint Security.
- Báo cáo tác vụ của Kaspersky Endpoint Security.
- Báo cáo **Mã hóa dữ liệu**. 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:


 **Informational messages**. Các sự kiện tham khảo thường không chứa thông tin quan trọng.

 **Cảnh báo**. Các sự kiện cần được chú ý bởi chúng phản ánh các tình huống quan trọng trong hoạt động của Kaspersky Endpoint Security.

 **Critical events**. Các sự kiện có tầm quan trọng thiết yếu thể hiện các vấn đề trong hoạt động của Kaspersky Endpoint Security, hoặc lỗi hỏng 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 nhóm theo bộ lọc sự kiện bằng nút .
- 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.

Nếu Kaspersky Endpoint Security đang chạy dưới sự quản lý của Kaspersky Security Center, thông tin về các sự kiện có thể được chuyển tiếp đến Máy chủ quản trị Kaspersky Security Center (để biết thêm chi tiết, vui lòng tham khảo [Trợ giúp của Kaspersky Security Center](#)).

Xem báo cáo

Nếu một người dùng có thể xem báo cáo, người dùng đó cũng có thể xem tất cả các sự kiện được phản ánh trong báo cáo.

Để xem báo cáo:


1. Trong cửa sổ chính của ứng dụng, trong mục **Giám sát**, hãy nhấn vào ô **Báo cáo**.
2. Trong danh sách thành phần và tác vụ, hãy chọn một thành phần hoặc tác vụ.
Bên phải của cửa sổ hiển thị một báo cáo chứa một danh sách các sự kiện phát sinh từ hoạt động của thành phần được chọn hoặc tác vụ được chọn của Kaspersky Endpoint Security. Bạn có thể sắp xếp các sự kiện trong báo cáo dựa trên giá trị trong các ô của một cột.
3. Để xem thông tin chi tiết về một sự kiện, hãy chọn sự kiện trong báo cáo.

Một mục chứa thông tin tóm tắt sự kiện sẽ được hiển thị ở phần dưới của cửa sổ.

Cấu hình 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.


Để thay đổi thời gian lưu trữ báo cáo tối đa:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn mục **Thiết lập tổng quát** → **Các báo cáo và lưu trữ**.
3. Nếu bạn muốn giới hạn thời hạn lưu trữ báo cáo, hãy chọn hộp kiểm **Lưu trữ báo cáo không quá N ngày** trong mục **Báo cáo**. Xác định thời gian lưu trữ báo cáo tối đa.
4. Lưu các thay đổi của bạn.

Cấu hình 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 tập tin báo cáo tối đa, Kaspersky Endpoint Security sẽ tự động xóa các mục cũ nhất từ tập tin báo cáo khi đạt đến kích cỡ tập tin báo cáo tối đa.

Để thiết lập kích cỡ tối đa của tập tin báo cáo:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn mục **Thiết lập tổng quát** → **Các báo cáo và lưu trữ**.
3. Trong mục **Báo cáo**, hãy chọn hộp kiểm **Giới hạn dung lượng của tập tin báo cáo ở mức N MB** nếu bạn muốn giới hạn dung lượng của tập tin báo cáo. Xác định dung lượng tối đa của tập tin báo cáo.
4. Lưu các thay đổi của bạn.

Lưu một báo cáo ra tập tin

Người dùng có trách nhiệm đảm bảo sự bảo mật của thông tin từ một báo cáo được lưu ra tập tin, cụ thể là kiểm soát và hạn chế truy cập đến thông tin này.

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. Trong cửa sổ chính của ứng dụng, trong mục **Giám sát**, hãy nhấn vào ô **Báo cáo**.
2. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ này, hãy chọn 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.
3. 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
4. Nhấn vào nút **Lưu báo cáo** ở góc phải trên của cửa sổ.

5. Trong cửa sổ mở ra, hãy chỉ định thư mục đích để lưu tập tin báo cáo.
6. Nhập tên của tập tin báo cáo.
7. Chọn định dạng tập tin báo cáo cần thiết: TXT hoặc CSV.
8. Lưu các thay đổi của bạn.

Xóa nội dung báo cáo

Để xem thông tin từ báo cáo:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn mục **Thiết lập tổng quát** → **Các báo cáo và lưu trữ**.
3. Trong mục **Báo cáo**, hãy nhấn nút **Xóa**.
4. Nếu [Bảo vệ bằng mật khẩu được bật](#), Kaspersky Endpoint Security có thể nhắc bạn nhập thông tin đăng nhập tài khoản người dùng. Ứng dụng sẽ nhắc nhập thông tin đăng nhập tài khoản nếu người dùng đó không có các quyền cần thiết.

Kaspersky Endpoint Security sẽ xóa mọi các báo cáo cho tất cả các thành phần và tác vụ của ứng dụng.

Tự bảo vệ cho Kaspersky Endpoint Security

Tính năng Tự bảo vệ ngăn các ứng dụng khác thực hiện các hành động có thể cản trở hoạt động của Kaspersky Endpoint Security, ví dụ như gỡ bỏ Kaspersky Endpoint Security khỏi máy tính. Nhóm công nghệ Tự bảo vệ khả dụng dành cho Kaspersky Endpoint Security phụ thuộc vào việc hệ điều hành có kiến trúc 32 bit hay 64 bit (tham khảo bảng bên dưới).


Các công nghệ Tự bảo vệ cho Kaspersky Endpoint Security

Công nghệ	Mô tả	Máy tính x86	Máy tính x64
Cơ chế Tự bảo vệ	Công nghệ này sẽ chặn quyền truy cập vào các thành phần sau của ứng dụng: <ul style="list-style-type: none">• các tập tin trong thư mục cài đặt Kaspersky Endpoint Security và các tập tin khác của ứng dụng;• các khóa Registry có bản ghi thuộc về ứng dụng;• các tiến trình mà ứng dụng chạy.	✓	✓
AM-PPL (Antimalware Protected Process Light)	Công nghệ này sẽ bảo vệ các tiến trình của Kaspersky Endpoint Security trước các hành động độc hại. Để biết thêm chi tiết về công nghệ AM-PPL, vui lòng truy cập website Microsoft . Công nghệ AM-PPL có sẵn trên hệ điều hành Windows 10 phiên bản 1703 (RS2) hoặc mới hơn và Windows Server 2019.	✓	✓
Cơ chế bảo vệ quản lý bên ngoài	Công nghệ này ngăn các ứng dụng quản trị từ xa (ví dụ: TeamViewer hoặc RemotelyAnywhere) lấy quyền truy cập vào Kaspersky Endpoint Security.	✓	- (trừ Windows 7)

Bật và tắt Tự bảo vệ

Cơ cấu Tự bảo vệ của Kaspersky Endpoint Security được bật theo mặc định.

Để bật hoặc tắt Tự bảo vệ:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Thiết lập ứng dụng**.
3. Sử dụng hộp kiểm **Bật Tự bảo vệ** để bật hoặc tắt cơ chế Tự bảo vệ.
4. Lưu các thay đổi của bạn.

Bật và tắt hỗ trợ AM-PPL

Kaspersky Endpoint Security hỗ trợ công nghệ Antimalware Protected Process Light (sau đây gọi là "AM-PPL") từ Microsoft. AM-PPL sẽ bảo vệ các tiến trình của Kaspersky Endpoint Security trước các hành động độc hại (ví dụ: chấm dứt ứng dụng). AM-PPL chỉ cho phép các tiến trình đáng tin cậy chạy. Các tiến trình của Kaspersky Endpoint Security được ký theo các yêu cầu bảo mật của Windows và do đó chúng đáng tin cậy. Để biết thêm chi tiết về công nghệ AM-PPL, vui lòng truy cập [website Microsoft](#). Công nghệ AM-PPL được bật theo mặc định.

Kaspersky Endpoint Security cũng có các cơ chế tích hợp để bảo vệ các tiến trình ứng dụng. Hỗ trợ AM-PPL cho phép bạn ủy quyền các chức năng bảo mật tiến trình cho hệ điều hành. Do đó, bạn có thể tăng tốc độ của ứng dụng và giảm mức tiêu thụ tài nguyên máy tính.

Công nghệ AM-PPL có sẵn trên hệ điều hành Windows 10 phiên bản 1703 (RS2) hoặc mới hơn và Windows Server 2019.

Để bật hoặc tắt công nghệ AM-PPL:

1. [Tắt cơ chế Tự bảo vệ của ứng dụng.](#)

Cơ chế Tự bảo vệ sẽ chặn hoạt động sửa đổi và xóa các tiến trình ứng dụng trong bộ nhớ máy tính, bao gồm thay đổi trạng thái AM-PPL.

2. Chạy trình thông dịch dòng lệnh (cmd.exe) với tư cách quản trị viên.

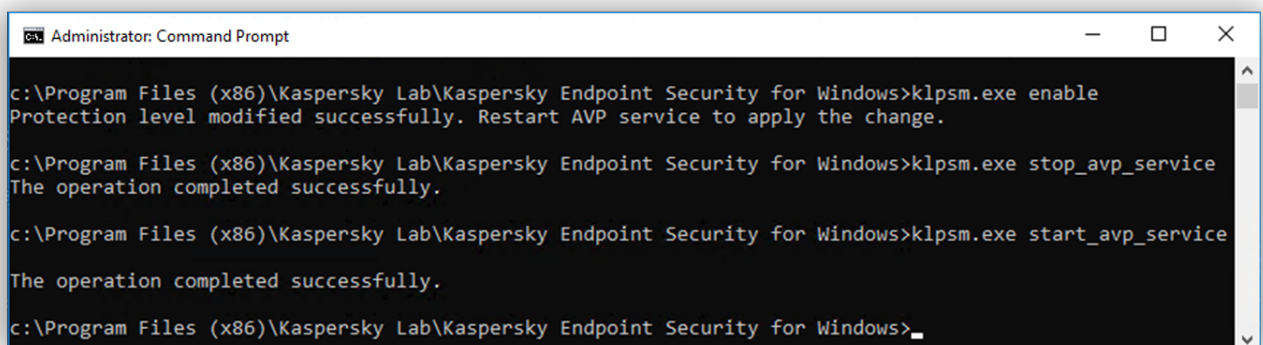
3. Tới thư mục chứa tập tin thực thi Kaspersky Endpoint Security.

4. Hãy nhập chuỗi sau vào dòng lệnh:

- `klpsm.exe enable` – bật hỗ trợ cho công nghệ AM-PPL (xem hình bên dưới).
- `klpsm.exe disable` – tắt hỗ trợ cho công nghệ AM-PPL.

5. Khởi động lại Kaspersky Endpoint Security.

6. [Khôi phục cơ cấu Tự bảo vệ.](#)



```
Administrator: Command Prompt
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe enable
Protection level modified successfully. Restart AVP service to apply the change.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe stop_avp_service
The operation completed successfully.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe start_avp_service
The operation completed successfully.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>
```

Bật hỗ trợ cho công nghệ AM-PPL


Bật và tắt bảo vệ quản lý bên ngoài

Bảo vệ quản lý bên ngoài ngăn các ứng dụng quản trị từ xa (ví dụ: TeamViewer hoặc RemotelyAnywhere) giành quyền truy cập vào Kaspersky Endpoint Security. Công nghệ này bao gồm các tính năng bảo vệ quản lý bên ngoài sau:

- Bảo vệ chống lại hoạt động sửa đổi thiết lập của Kaspersky Endpoint Security.
- Bảo vệ các dịch vụ của Kaspersky Endpoint Security (ví dụ như dịch vụ avp).
- Bảo vệ các tiến trình của ứng dụng.

Bảo vệ chống lại hoạt động quản lý bên ngoài chỉ khả dụng với các máy tính chạy hệ điều hành 32 bit, trừ Windows 7. Đối với Windows 7, công nghệ này khả dụng cho hệ điều hành 32 bit và 64 bit.

Để bật hoặc tắt bảo vệ trước hoạt động quản lý từ bên ngoài:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Thiết lập ứng dụng**.
3. Sử dụng hộp kiểm **Cho phép quản lý thiết lập của Kaspersky Endpoint Security thông qua các ứng dụng kiểm soát từ xa** để bật hoặc tắt tính năng bảo vệ quản lý bên ngoài.

Nếu hộp kiểm được chọn, bạn có thể sử dụng các ứng dụng quản trị từ xa để cấu hình Kaspersky Endpoint Security và quản lý các dịch vụ và tiến trình của ứng dụng.

Nếu hộp kiểm bị xóa, tính năng bảo vệ quản lý bên ngoài sẽ ngăn các ứng dụng quản trị từ xa truy cập vào Kaspersky Endpoint Security. Bạn có thể cho phép cấu hình Kaspersky Endpoint Security bằng cách sử dụng các ứng dụng quản trị từ xa cụ thể. Để thực hiện, bạn phải [thêm ứng dụng quản trị từ xa vào danh sách được tin tưởng](#). Trong trường hợp này, tính năng bảo vệ quản trị từ xa sẽ vẫn ngăn ứng dụng quản trị từ xa truy cập vào các dịch vụ và tiến trình của Kaspersky Endpoint Security.

4. Sử dụng hộp kiểm **Bật quản lý bên ngoài các dịch vụ hệ thống** để bật hoặc tắt tính năng bảo vệ của các dịch vụ Kaspersky Endpoint Security trước sự quản lý từ bên ngoài.

Để thoát ứng dụng khỏi dòng lệnh, hãy tắt tính năng bảo vệ của các dịch vụ Kaspersky Endpoint Security trước sự quản lý từ bên ngoài.


5. Lưu các thay đổi của bạn.

Kết quả là khi tính năng bảo vệ quản lý bên ngoài được bật, Kaspersky Endpoint Security sẽ ngăn con trỏ chuột trở vào cửa sổ ứng dụng. Khi người dùng từ xa cố gắng tắt một dịch vụ ứng dụng, một cửa sổ hệ thống chứa thông báo lỗi sẽ xuất hiện.

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 quản lý bên ngoài được bật.

Để cho phép hoạt động của các ứng dụng quản trị từ xa:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Mối đe dọa và loại trừ**.
3. Trong mục **Loại trừ**, hãy nhấn liên kết **Chỉ định ứng dụng được tin tưởng**.
4. Trong cửa sổ mở ra, hãy nhấn vào nút **Thêm**.
5. Chọn tập tin thực thi của ứng dụng quản trị từ xa.
Bạn cũng có thể nhập đường dẫn theo cách thủ công. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự * cùng ? khi nhập tên đại diện.
6. Chọn hộp kiểm **Không giám sát hoạt động ứng dụng**.
7. Lưu các thay đổi của bạn.

Kết quả hoạt động và tính tương thích với các ứng dụng khác của Kaspersky Endpoint Security

Hiệu suất 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 bạn 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 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

Mức sử dụng tài nguyên máy tính của Kaspersky Endpoint Security khi quét máy tính có thể làm tăng mức tải cho CPU và các hệ thống con của ổ cứng cũng như 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 nhường tài nguyên cho các ứng dụng khác.

Sử dụng Công nghệ khử mã độc nâng cao

Các ứng dụng 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. Sau khi phát hiện hoạt động độc hại trong hệ điều hành, Kaspersky Endpoint Security sẽ thực hiện một quy trình khử mã độc triệt để bằng công nghệ khử mã độc nâng cao đặc biệt. *Công nghệ khử mã độc nâng cao* nhằm tẩy sạch các ứng dụng độc hại ra khỏi hệ điều hành. Đó là các ứng dụng độc hại đã khởi chạy tiến trình của chúng ở trong RAM, khiến Kaspersky Endpoint Security không thể loại trừ chúng bằng các phương thức khác. Kết quả là mỗi 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 mã độc nâng cao 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 toàn bộ "nhẹ" trên toàn máy tính.

Không thể nhắc khởi động lại trên một máy tính chạy Microsoft Windows cho máy chủ do các đặc trưng của Kaspersky Endpoint Security. 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 mã độc nâng cao 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 mã độc tình trạng nhiễm mã độc hiện hoạt trên một máy chủ, hãy bật công nghệ Khử mã độc chủ động cho máy chủ và khởi chạy một tác vụ nhóm *Quét virus* vào thời điểm thuận lợi cho những người dùng máy chủ.

Bật hoặc tắt chế độ tiết kiệm năng lượng

Để bật hoặc tắt chế độ tiết kiệm năng lượng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Thiết lập ứng dụng**.
3. Trong mục **Hiệu năng**, hãy sử dụng hộp kiểm **Hoãn các tác vụ theo lịch trong khi đang sử dụng nguồn pin** để bật hoặc tắt chế độ tiết kiệm 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 Kiểm tra tính toàn vẹn.

4. Lưu các thay đổi của bạn.

Bật hoặc tắt tính năng nhường tài nguyên cho các ứng dụng khác

Mức sử dụng tài nguyên máy tính của Kaspersky Endpoint Security khi quét máy tính có thể làm tăng mức tải cho CPU và các hệ thống con của ổ cứng. Điều này có thể làm chậm các ứng dụng khác. Để tối ưu hóa hiệu năng, Kaspersky Endpoint Security cung cấp một *chế độ chuyển tài nguyên sang các ứng dụng khác*. Ở chế độ này, hệ điều hành có thể giảm mức độ ưu tiên của các luồng tác vụ quét của Kaspersky Endpoint Security khi CPU có mức tải cao. Điều này cho phép phân phối lại tài nguyên hệ điều hành cho các ứng dụng khác. Nhờ vậy, tác vụ quét sẽ nhận được ít thời gian CPU hơn. Kết quả là Kaspersky Endpoint Security sẽ mất nhiều thời gian hơn để quét máy tính. Theo mặc định, ứng dụng được thiết lập để nhường tài nguyên cho các ứng dụng khác.

Để bật hoặc tắt tính năng nhường tài nguyên cho các ứng dụng khác:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Thiết lập ứng dụng**.
3. Trong mục **Hiệu năng**, hãy sử dụng hộp kiểm **Nhường tài nguyên cho các ứng dụng khác** để bật hoặc tắt việc nhường tài nguyên cho các ứng dụng khác.
4. Lưu các thay đổi của bạn.

Các phương pháp tốt nhất để tối ưu hóa hiệu năng của Kaspersky Endpoint Security

Khi triển khai Kaspersky Endpoint Security cho Windows, bạn có thể sử dụng các đề xuất sau để cấu hình bảo vệ máy tính và tối ưu hóa hiệu năng.

Tổng quát

Cấu hình thiết lập tổng quát của ứng dụng theo các khuyến nghị sau:

1. [Nâng cấp Kaspersky Endpoint Security lên phiên bản mới nhất](#).

Các phiên bản mới hơn của ứng dụng đã được sửa lỗi, nâng cao độ ổn định và tối ưu hóa hiệu năng.

2. Bật các thành phần bảo vệ theo thiết lập mặc định.

Thiết lập mặc định được coi là tối ưu. Thiết lập này được khuyến nghị bởi các chuyên gia Kaspersky. Thiết lập mặc định cung cấp mức bảo vệ được đề xuất và sử dụng tài nguyên tối ưu. Nếu cần, bạn có thể [khôi phục thiết lập ứng dụng mặc định](#).

3. Bật các tính năng tối ưu hóa hiệu năng ứng dụng.

Ứng dụng có các tính năng tối ưu hóa hiệu năng: [chế độ tiết kiệm năng lượng](#) và [nhường tài nguyên cho các ứng dụng khác](#). Đảm bảo rằng các tùy chọn này được bật.

Quét virus trên máy trạm

Bạn nên bật [Quét trong nền](#) để đối với tác vụ Quét virus các máy trạm. *Quét trong nền* là một chế độ quét của Kaspersky Endpoint Security không hiển thị thông báo cho người dùng. Quét trong nền yêu cầu ít tài nguyên máy tính hơn các loại quét khác (ví dụ như quét toàn bộ). Trong chế độ này, Kaspersky Endpoint Security sẽ quét các đối tượng khởi động, sector khởi động, bộ nhớ hệ thống và phân vùng hệ thống. Thiết lập quét trong nền được coi là tối ưu. Thiết lập này được khuyến nghị bởi các chuyên gia Kaspersky. Vì vậy, để thực hiện một tác vụ Quét virus cho máy tính, bạn có thể chỉ cần sử dụng chế độ quét trong nền mà không cần sử dụng các tác vụ quét khác.

Nếu tính năng quét trong nền không phù hợp với nhu cầu của bạn, hãy cấu hình tác vụ *Quét virus* phù hợp theo các khuyến nghị sau:

1. [Cấu hình lịch quét máy tính tối ưu.](#)

Bạn có thể cấu hình tác vụ để chạy khi máy tính đang hoạt động dưới mức tải tối thiểu. Ví dụ: bạn có thể cấu hình tác vụ để chạy vào ban đêm hoặc vào cuối tuần.

Nếu người dùng tắt máy tính của họ vào cuối ngày, bạn có thể cấu hình tác vụ quét như sau:

- Bật tính năng Wake-on-LAN. Tính năng Wake-on-LAN cho phép bật nguồn máy tính từ xa bằng cách gửi một tín hiệu đặc biệt qua mạng cục bộ. Để sử dụng tính năng này, bạn phải bật Wake-on-LAN trong thiết lập BIOS. Bạn cũng có thể để máy tính tự động tắt sau khi tác vụ quét kết thúc.
- Tắt tính năng "Chạy các tác vụ đã bị bỏ lỡ". Kaspersky Endpoint Security sẽ bỏ qua các tác vụ bị bỏ lỡ khi người dùng bật máy tính. Việc chạy các tác vụ sau khi máy tính được bật có thể gây bất tiện cho người dùng vì quá trình quét đòi hỏi lượng lớn tài nguyên.

Nếu bạn không thể cấu hình lịch quét tối ưu, hãy thiết lập để các tác vụ chỉ chạy khi máy tính không hoạt động. Kaspersky Endpoint Security sẽ bắt đầu tác vụ quét nếu máy tính bị khóa hoặc nếu trình bảo vệ màn hình được bật. Nếu bạn đã làm gián đoạn việc thực thi tác vụ, chẳng hạn như bằng cách mở khóa máy tính, Kaspersky Endpoint Security sẽ tự động chạy tác vụ, tiếp tục từ thời điểm tác vụ bị gián đoạn.

2. [Xác định phạm vi quét.](#)

Chọn các đối tượng sau để quét:

- Bộ nhớ kernel
- Tiến trình đang chạy và Các đối tượng khởi động
- Sector khởi động
- Ổ đĩa hệ thống (%systemdrive%).

3. [Bật công nghệ iSwift và công nghệ iChecker.](#)

- Công nghệ iSwift.

Công nghệ này cho phép tăng tốc độ quét bằng cách loại trừ một số tập tin nhất định khỏi quá trình quét. Các tập tin được loại trừ khỏi quá trình quét bằng một thuật toán đặc biệt có tính đến ngày phát hành cơ sở dữ liệu Kaspersky Endpoint Security, ngày mà tập tin được quét lần cuối cùng và mọi thay đổi được thực hiện với thiết lập quét. Công nghệ iSwift được cải tiến từ công nghệ iChecker cho hệ thống tập tin NTFS.

- Công nghệ iChecker.

Công nghệ này cho phép tăng tốc độ quét bằng cách loại trừ một số tập tin nhất định khỏi quá trình quét. Các tập tin được loại trừ khỏi quá trình quét bằng một thuật toán đặc biệt có tính đến ngày phát hành cơ sở dữ liệu Kaspersky Endpoint Security, ngày khi tập tin được quét lần cuối cùng và mọi thay đổi được thực hiện với thiết lập quét. Công nghệ iChecker có một số hạn chế: công nghệ này không hoạt động với tập tin lớn và chỉ áp dụng cho các tập tin có cấu trúc mà ứng dụng nhận dạng được (ví dụ như EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP và RAR).

Bạn chỉ có thể bật công nghệ iSwift và công nghệ iChecker trong Bảng điều khiển quản trị (MMC) và giao diện Kaspersky Endpoint Security. Bạn không thể bật các công nghệ này trong Bảng điều khiển web của Kaspersky Security Center.

4. Tắt tính năng quét các tập tin nén được bảo vệ bằng mật khẩu.

Nếu bật tính năng quét các tập tin nén được bảo vệ bằng mật khẩu, một lời nhắc mật khẩu sẽ hiển thị trước khi quét tập tin nén. Vì chúng tôi khuyến nghị bạn lên lịch chạy tác vụ ngoài giờ hành chính nên người dùng không thể nhập mật khẩu. Bạn có thể [quét tập tin nén có mật khẩu bảo vệ theo cách thủ công](#).

Quét virus trên máy chủ

Cấu hình tác vụ *Quét virus* theo các khuyến nghị sau:

1. Cấu hình lịch quét máy tính tối ưu.

Bạn có thể cấu hình tác vụ để chạy khi máy tính đang hoạt động dưới mức tải tối thiểu. Ví dụ: bạn có thể cấu hình tác vụ để chạy vào ban đêm hoặc vào cuối tuần.

2. Bật công nghệ iSwift và công nghệ iChecker.

- Công nghệ iSwift.

Công nghệ này cho phép tăng tốc độ quét bằng cách loại trừ một số tập tin nhất định khỏi quá trình quét. Các tập tin được loại trừ khỏi quá trình quét bằng một thuật toán đặc biệt có tính đến ngày phát hành cơ sở dữ liệu Kaspersky Endpoint Security, ngày mà tập tin được quét lần cuối cùng và mọi thay đổi được thực hiện với thiết lập quét. Công nghệ iSwift được cải tiến từ công nghệ iChecker cho hệ thống tập tin NTFS.

- Công nghệ iChecker.

Công nghệ này cho phép tăng tốc độ quét bằng cách loại trừ một số tập tin nhất định khỏi quá trình quét. Các tập tin được loại trừ khỏi quá trình quét bằng một thuật toán đặc biệt có tính đến ngày phát hành cơ sở dữ liệu Kaspersky Endpoint Security, ngày khi tập tin được quét lần cuối cùng và mọi thay đổi được thực hiện với thiết lập quét. Công nghệ iChecker có một số hạn chế: công nghệ này không hoạt động với tập tin lớn và chỉ áp dụng cho các tập tin có cấu trúc mà ứng dụng nhận dạng được (ví dụ như EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP và RAR).

Bạn chỉ có thể bật công nghệ iSwift và công nghệ iChecker trong Bảng điều khiển quản trị (MMC) và giao diện Kaspersky Endpoint Security. Bạn không thể bật các công nghệ này trong Bảng điều khiển web của Kaspersky Security Center.

3. Tắt tính năng quét các tập tin nén được bảo vệ bằng mật khẩu.

Nếu bật tính năng quét các tập tin nén được bảo vệ bằng mật khẩu, một lời nhắc mật khẩu sẽ hiển thị trước khi quét tập tin nén. Vì chúng tôi khuyến nghị bạn lên lịch chạy tác vụ ngoài giờ hành chính nên người dùng không thể nhập mật khẩu. Bạn có thể [quét tập tin nén có mật khẩu bảo vệ theo cách thủ công](#).

Kaspersky Security Network

Để bảo vệ máy tính của bạn một cách hiệu quả hơn, Kaspersky Endpoint Security sẽ sử dụng dữ liệu được nhận từ người dùng trên khắp thế giới. Kaspersky Security Network được thiết kế để lấy 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. Nếu bạn đang tham gia vào Kaspersky Security Network, các dịch vụ KSN sẽ cung cấp cho Kaspersky Endpoint Security thông tin về danh mục và danh tiếng của các tập tin được quét, cũng như thông tin về danh tiếng của các địa chỉ trang web được quét.

Chỉnh sửa thiết lập Kaspersky Security Network theo các khuyến nghị sau:

1. Tắt chế độ KSN mở rộng.

Chế độ KSN mở rộng là chế độ trong đó Kaspersky Endpoint Security sẽ gửi dữ liệu bổ sung đến Kaspersky.

2. Cấu hình KSN Riêng.

KSN Riêng là một giải pháp cho phép người dùng máy tính lưu trữ Kaspersky Endpoint Security hoặc các ứng dụng khác của Kaspersky để có quyền truy cập cơ sở dữ liệu danh tiếng của Kaspersky Security Network và truy cập các dữ liệu thống kê khác mà không cần gửi dữ liệu cho KSN từ máy tính của riêng họ.

3. Bật chế độ đám mây.

Chế độ đám mây chỉ chế độ hoạt động của ứng dụng trong đó Kaspersky Endpoint Security sử dụng phiên bản nhẹ của cơ sở dữ liệu diệt virus. Kaspersky Security Network hỗ trợ hoạt động của ứng dụng khi cơ sở dữ liệu diệt virus nhẹ đang được sử dụng. Phiên bản nhẹ của cơ sở dữ liệu diệt virus cho phép bạn sử dụng khoảng một nửa dung lượng RAM của máy tính so với dung lượng RAM được sử dụng với cơ sở dữ liệu thông thường. Nếu bạn không tham gia vào Kaspersky Security Network hoặc nếu chế độ đám mây bị tắt, Kaspersky Endpoint Security sẽ tải về phiên bản đầy đủ của cơ sở dữ liệu diệt virus từ các máy chủ của Kaspersky.

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 nội 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. Kaspersky Endpoint Security sử dụng thuật toán mã hóa Tiêu chuẩn mã hóa nâng cao (AES).

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 ứng dụng được kích hoạt bằng 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, khóa giấy phép, Kaspersky Endpoint Security hoặc thành phần mã hóa đã bị xóa/gỡ bỏ thì 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 mức độ tập tin trên các ổ đĩa máy tính cục bộ.** 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 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.
- **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 di động. Sau khi đã bật chế độ di 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.

- **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 gói 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 toàn bộ ổ đĩa.** Bạn có thể chọn một công nghệ mã hóa: Kaspersky Disk Encryption hoặc BitLocker Drive Encryption (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 Tin tưởng (TPM), BitLocker sẽ sử dụng nó để lưu các khóa phục hồi cho phép truy cập đến một ổ cứng được mã hóa. Khi máy tính được khởi động, BitLocker sẽ yêu cầu khóa phục hồi ổ cứng từ Mô-đun Nền tảng Tin tưởng 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 phục hồi.

Bạn có thể quy định quy tắc mã hóa toàn bộ ổ đĩa 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 toàn bộ ổ đĩa 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 logic của ổ cứng cùng một lúc.

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 [Manage Authentication Agent accounts](#). 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 cũng có thể [sử dụng công nghệ Single Sign-On \(SSO\)](#), cho phép bạn tự động đăng nhập vào hệ điều hành bằng 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 lưu 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 Trợ giúp Kaspersky Security Center.

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 toàn bộ ổ đĩa. 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 có thể truy xuất.

Trước khi bắt đầu mã hóa, Kaspersky Endpoint Security sẽ nhận bản đồ các khu vực của hệ thống tập tin. Lướt mã hóa đầu tiên bao gồm các khu vực chứa tập tin tại thời điểm mã hóa được bắt đầu. Lướt 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 được ghi vào một thiết bị mới và thiết bị thường xuyên được mã hóa với chức năng **Chỉ mã hóa dung lượng ổ đĩa được sử dụng** được bật, 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 Kaspersky Security Center Administration Server kiểm soát máy tính tại thời điểm mã hóa. Nếu vì lý do nào đó, máy tính có các đối tượng được mã hóa được quản lý bởi một Máy chủ quản trị khác thì bạn có thể lấy quyền truy cập tới dữ liệu mã hóa theo các cách sau:

- Các máy chủ quản trị có cùng cấp bậc:
 - Bạn không cần thực hiện thêm hành động nào. Người dùng sẽ tiếp tục giữ quyền truy cập với các đối tượng được mã hóa. Khóa mã hóa được phân phối đến tất cả các Máy chủ quản trị.
- Máy chủ quản trị tách biệt:
 - 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 Kaspersky Security Center đã kiểm soát máy tính tại thời điểm mã hóa từ một bản sao lưu 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.

Nếu không có quyền truy cập vào dữ liệu được mã hóa, hãy làm theo các hướng dẫn đặc biệt để làm việc với dữ liệu được mã hóa ([Khôi phục quyền truy cập vào các tập tin được mã hóa](#), [Làm việc với các thiết bị được mã hóa khi không có truy cập đến chúng](#)).

Hạn chế của chức năng mã hóa

Tính năng Mã hóa dữ liệu có các hạn chế sau:

- Ứng dụng sẽ tạo các tập tin dịch vụ trong quá trình mã hóa. Cần khoảng 0,5% dung lượng trống không bị phân mảnh trên ổ đĩa cứng để lưu trữ chúng. Nếu không có đủ dung lượng trống không bị phân mảnh trên ổ đĩa cứng, quá trình mã hóa sẽ không bắt đầu cho đến khi giải phóng đủ dung lượng trống.
- Bạn có thể quản lý tất cả các thành phần mã hóa dữ liệu trong Bảng điều khiển quản trị Kaspersky Security Center và Bảng điều khiển web Kaspersky Security Center. Trong Bảng điều khiển đám mây Kaspersky Security Center, bạn chỉ có thể quản lý BitLocker.
- Mã hóa dữ liệu chỉ khả dụng khi sử dụng Kaspersky Endpoint Security với hệ thống quản trị Kaspersky Security Center hoặc Bảng điều khiển đám mây Kaspersky Security Center (chỉ BitLocker). Không thể Mã hóa dữ liệu khi sử dụng Kaspersky Endpoint Security ở chế độ ngoại tuyến vì Kaspersky Endpoint Security lưu trữ các khóa mã hóa trong Kaspersky Security Center.
- Nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy [Microsoft Windows cho Máy chủ](#) thì bạn chỉ có thể sử dụng chức năng mã hóa toàn bộ ổ đĩa bằng công nghệ BitLocker Drive

Encryption. Nếu Kaspersky Endpoint Security được cài đặt trên máy tính chạy Windows cho Máy trạm thì bạn có thể sử dụng toàn bộ tính năng mã hóa dữ liệu.

Mã hóa toàn bộ ổ đĩa 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.

Khả năng tương thích giữa chức năng mã hóa toàn bộ đĩa của Kaspersky Endpoint Security và Kaspersky Anti-Virus cho UEFI không được hỗ trợ. Kaspersky Anti-Virus cho UEFI khởi chạy trước khi nạp hệ điều hành. Khi sử dụng mã hóa toàn bộ đĩa, ứng dụng sẽ phát hiện ra rằng máy tính không được cài đặt hệ điều hành. Kết quả là hoạt động của Kaspersky Anti-Virus cho UEFI sẽ kết thúc kèm theo một lỗi. Mã hóa mức độ tập tin (FLE) không ảnh hưởng đến hoạt động của Kaspersky Anti-Virus cho UEFI.

Kaspersky Endpoint Security hỗ trợ các cấu hình sau:

- Ổ cứng HDD, SSD và USB.

Công nghệ Kaspersky Disk Encryption (FDE) hỗ trợ làm việc với ổ SSD trong khi vẫn duy trì hiệu năng và tuổi thọ của các ổ SSD.

- Các ổ được kết nối qua bus: SCSI, ATA, IEEE1394, USB, RAID, SAS, SATA, NVME.
- Các ổ đĩa cố định được kết nối qua bus SD hoặc MMC.
- Các ổ đĩa có các sector 512 byte.
- Các ổ đĩa có các sector 4096 byte mô phỏng 512 byte.
- Các ổ đĩa có loại phân vùng sau: GPT, MBR, and VBR (removable drives).
- Phần mềm nhúng của tiêu chuẩn UEFI 64 và BIOS chuẩn cũ.
- Phần mềm nhúng của tiêu chuẩn UEFI có hỗ trợ Secure Boot.

Secure Boot là một công nghệ được thiết kế để xác minh chữ ký số cho các ứng dụng và trình điều khiển của bộ nạp UEFI. Secure Boot sẽ chặn khởi động các ứng dụng và trình điều khiển UEFI chưa được ký hoặc ký bởi các nhà phát hành không xác định. Kaspersky Disk Encryption (FDE) hỗ trợ đầy đủ công nghệ Secure Boot. Authentication Agent được ký bằng chứng chỉ Nhà phát hành Trình điều khiển Microsoft Windows UEFI.

Trên một số thiết bị (ví dụ: Microsoft Surface Pro và Microsoft Surface Pro 2), danh sách chứng chỉ xác minh chữ ký số đã cũ có thể được cài đặt theo mặc định. Trước khi mã hóa ổ đĩa, bạn cần cập nhật danh sách chứng chỉ.

- Phần mềm nhúng tiêu chuẩn UEFI có hỗ trợ Fast Boot.

Fast Boot là công nghệ giúp máy tính khởi động nhanh hơn. Khi bật công nghệ Fast Boot, thông thường máy tính chỉ nạp bộ trình điều khiển UEFI tối thiểu, cần thiết để khởi động hệ điều hành. Khi công nghệ Fast Boot được bật, bàn phím USB, chuột, mã thông báo USB, bàn di chuột và màn hình cảm ứng có thể không hoạt động khi Authentication Agent đang chạy.

Để sử dụng Kaspersky Disk Encryption (FDE), bạn nên tắt công nghệ Fast Boot. Bạn có thể sử dụng [Tiện ích kiểm tra FDE](#) để kiểm tra hoạt động của Kaspersky Disk Encryption (FDE).

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.
 - Hệ thống có 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 có trên 10 phân vùng mở rộng.
 - Hệ thống có tập tin swap được đặt trên một ổ đĩa không phải ổ đĩa hệ thống.
 - Hệ thống nhiều mục khởi động có nhiều hệ điều hành được cài đặt đồng thời.
 - Các phân vùng động (chỉ các phân vùng chính mới được hỗ trợ).
 - Các ổ đĩa có dưới 0,5% không gian ổ đĩa không phân mảnh tự do.
 - Các ổ đĩa có kích cỡ sector khác với 512 byte hoặc 4096 byte giả lập 512 byte.
 - Các ổ đĩa lai.
 - Hệ thống có bộ nạp của bên thứ ba.
 - Các ổ đĩa có thư mục NTFS được nén.
 - Công nghệ Kaspersky Disk Encryption (FDE) không tương thích với các công nghệ mã hóa toàn bộ ổ đĩa khác (như BitLocker, McAfee Drive Encryption và WinMagic SecureDoc).
 - Công nghệ Kaspersky Disk Encryption (FDE) không tương thích với công nghệ ExpressCache.
 - Không hỗ trợ tạo, xóa và sửa đổi phân vùng trên ổ đĩa được mã hóa. Bạn có thể mất dữ liệu.
 - Không hỗ trợ định dạng hệ thống tập tin. Bạn có thể mất dữ liệu.
- Nếu bạn cần định dạng ổ đĩa đã được mã hóa bằng công nghệ Kaspersky Disk Encryption (FDE), hãy định dạng ổ đĩa trên máy tính không có Kaspersky Endpoint Security cho Windows và chỉ sử dụng chế độ mã hóa toàn bộ đĩa.
- Ổ đĩa mã hóa được định dạng bằng tùy chọn định dạng nhanh có thể bị nhận dạng nhầm là được mã hóa trong lần kết nối tiếp theo với máy tính đã cài đặt Kaspersky Endpoint Security cho Windows. Dữ liệu người dùng sẽ không khả dụng.
- Authentication Agent hỗ trợ tối đa 100 tài khoản.
 - Công nghệ Single Sign-On không tương thích với các công nghệ khác của nhà phát triển bên thứ ba.
 - Công nghệ Kaspersky Disk Encryption (FDE) không được hỗ trợ trên các mẫu thiết bị sau:
 - Dell Latitude E6410 (chế độ UEFI)
 - HP Compaq nc8430 (chế độ BIOS chuẩn cũ)
 - Lenovo Think Center 8811 (chế độ BIOS chuẩn cũ)
 - Authentication Agent không hỗ trợ hoạt động với mã thông báo USB khi Hỗ trợ USB chuẩn cũ được bật. Chỉ có phương thức xác thực bằng mật khẩu mới khả dụng trên máy tính.
 - Khi mã hóa ổ đĩa ở chế độ BIOS chuẩn cũ, bạn nên bật Hỗ trợ USB chuẩn cũ trên các kiểu thiết bị sau:
 - Acer Aspire 5560G

- Acer Aspire 6930
- Acer TravelMate 8572T
- Dell Inspiron 1420
- Dell Inspiron 1545
- Dell Inspiron 1750
- Dell Inspiron N4110
- Dell Latitude E4300
- Dell Studio 1537
- Dell Studio 1569
- Dell Vostro 1310
- Dell Vostro 1320
- Dell Vostro 1510
- Dell Vostro 1720
- Dell Vostro V13
- Dell XPS L502x
- Fujitsu Celsius W370
- Fujitsu LifeBook A555
- HP Compaq dx2450 Microtower PC
- Lenovo G550
- Lenovo ThinkPad L530
- Lenovo ThinkPad T510
- Lenovo ThinkPad W540
- Lenovo ThinkPad X121e
- Lenovo ThinkPad X200s (74665YG)
- Samsung R530
- Toshiba Satellite A350
- Toshiba Satellite U400 100
- MSI 760GM-E51 (bo mạch chủ)

Thay đổi độ dài của khóa mã hóa (AES56 / AES256)

Kaspersky Endpoint Security sử dụng thuật toán mã hóa Tiêu chuẩn mã hóa nâng cao (AES). Kaspersky Endpoint Security hỗ trợ thuật toán mã hóa AES với độ dài khóa hiệu quả là 256 hoặc 56 bit. Thuật toán mã hóa dữ liệu phụ thuộc vào thư viện mã hóa AES, được kèm theo gói phân phối: *Mã hóa mạnh (AES256)* hoặc *Mã hóa nhẹ (AES56)*. Thư viện mã hóa AES được cài đặt cùng với ứng dụng.

Việc thay đổi độ dài của khóa mã hóa chỉ khả dụng cho Kaspersky Endpoint Security 11.2.0 trở lên.

Việc thay đổi độ dài khóa mã hóa bao gồm các bước sau:

1. Giải mã các đối tượng được Kaspersky Endpoint Security mã hóa trước khi bạn bắt đầu thay đổi độ dài khóa mã hóa:
 - a. [Giải mã các ổ cứng.](#)
 - b. [Giải mã các tập tin trên ổ đĩa nội bộ.](#)
 - c. [Giải mã ổ đĩa di động.](#)

Sau khi độ dài khóa mã hóa đã được thay đổi, các đối tượng được mã hóa từ trước sẽ không khả dụng.

2. [Gỡ bỏ Kaspersky Endpoint Security.](#)
3. [Cài đặt Kaspersky Endpoint Security](#) từ gói phân phối Kaspersky Endpoint Security chứa một thư viện mã hóa khác.

Bạn cũng có thể thay đổi độ dài khóa mã hóa bằng cách nâng cấp ứng dụng. Bạn chỉ có thể thay đổi độ dài khóa thông qua nâng cấp ứng dụng nếu đáp ứng các điều kiện sau:

- Máy tính phải được cài đặt phiên bản Kaspersky Endpoint Security 10 Service Pack 2 hoặc phiên bản cao hơn.
- Các thành phần mã hóa dữ liệu (Mã hóa mức độ tập tin, Mã hóa toàn bộ ổ đĩa) không được cài đặt trên máy tính.

Theo mặc định, các thành phần mã hóa dữ liệu không được kèm theo Kaspersky Endpoint Security. Thành phần BitLocker Management không ảnh hưởng đến sự thay đổi độ dài của khóa mã hóa.

Để thay đổi độ dài khóa mã hóa, hãy chạy tập tin kes_win.msi hoặc setup_kes.exe từ gói phân phối có chứa thư viện mã hóa cần thiết. Bạn cũng có thể nâng cấp ứng dụng từ xa bằng cách sử dụng gói cài đặt.

Không thể thay đổi độ dài của khóa mã hóa bằng gói phân phối của cùng một phiên bản ứng dụng được cài đặt trên máy tính của bạn nếu không cần gỡ cài đặt ứng dụng trước.

Kaspersky Disk Encryption

Kaspersky Disk Encrypt chỉ khả dụng với các máy tính chạy hệ điều hành Windows cho máy trạm. Đối với máy tính chạy hệ điều hành Windows cho máy chủ, hãy sử dụng công nghệ BitLocker Drive Encryption.

Kaspersky Endpoint Security hỗ trợ mã hóa toàn bộ ổ đĩa trong các hệ thống tập tin FAT32, NTFS và exFat.

Trước khi bắt đầu mã hóa toàn bộ ổ đĩa, ứng dụng sẽ chạy một loạt 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 hoặc 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 toàn bộ ổ đĩa sẽ được bắt đầu sau khi hệ điều hành đã được nạp 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 toàn bộ ổ đĩa 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 toàn bộ ổ đĩa, 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 toàn bộ ổ đĩa 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 mã hóa toàn bộ ổ đĩa, Authentication Agent sẽ được nạp trước lần khởi động hệ điều hành tiếp theo. Kaspersky Endpoint Security sẽ tiếp tục quá trình mã hóa toàn bộ ổ đĩa 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 trong quá trình mã hóa toàn bộ ổ đĩa, 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 toàn bộ ổ đĩa 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 toàn bộ ổ đĩa, Kaspersky Endpoint Security sẽ tiếp tục mã hóa toàn bộ ổ đĩa 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 vào 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.

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.

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](#).

Các tính năng đặc biệt của mã hóa ổ SSD

Ứng dụng hỗ trợ mã hóa ổ SSD, ổ SSHD lai và ổ đĩa có tính năng Intel Smart Response. Ứng dụng này không hỗ trợ mã hóa các ổ đĩa có tính năng Intel Rapid Start. Hãy tắt tính năng Intel Rapid Start trước khi mã hóa ổ đĩa như vậy.

Quá trình mã hóa ổ SSD có các tính năng đặc biệt sau:

- Nếu ổ SSD mới và không chứa dữ liệu bí mật thì chỉ [bật mã hóa phần dung lượng được sử dụng](#). Làm vậy cho phép bạn ghi đè các sector ổ đĩa liên quan.
- Nếu ổ SSD đang được sử dụng và có dữ liệu bí mật, hãy chọn một trong các tùy chọn sau:
 - Xóa hoàn toàn ổ SSD (Xóa bảo mật), cài đặt hệ điều hành và [chạy mã hóa ổ SSD và bật tùy chọn chỉ mã hóa dung lượng được sử dụng](#).
 - Chạy mã hóa ổ SSD khi tắt tùy chọn chỉ mã hóa dung lượng được sử dụng.

Mã hóa ổ SSD yêu cầu 5-10 GB dung lượng trống. Các yêu cầu về dung lượng trống để lưu trữ dữ liệu quản trị mã hóa được cung cấp trong bảng dưới đây.

Yêu cầu về dung lượng trống để lưu trữ dữ liệu quản trị mã hóa

Dung lượng ổ SSD (GB)	Dung lượng trống trên phân vùng chính của ổ SSD (MB)	Dung lượng trống trên phân vùng phụ của ổ SSD (MB)
128	250	64
256	250	640
512	300	128

Khởi chạy Kaspersky Disk Encryption

Trước khi bắt đầu mã hóa toàn bộ ổ đĩa, bạn nên đảm bảo rằng máy tính đang không bị nhiễm virus. Để làm điều này, hãy khởi chạy tác vụ Quét toàn bộ hoặc Quét khu vực quan trọng. Việc mã hóa toàn bộ ổ đĩa của một máy tính bị nhiễm rootkit có thể khiến máy ngừng hoạt động.

Trước khi bắt đầu mã hóa ổ đĩa, bạn phải kiểm tra thiết lập của các tài khoản Authentication Agent. Authentication Agent là thành phần cần thiết để làm việc với các ổ đĩa được bảo vệ bằng công nghệ Kaspersky Disk Encryption (FDE). Trước khi hệ điều hành được nạp, người dùng cần hoàn thành xác thực với Agent. Kaspersky Endpoint Security cho phép bạn tự động tạo tài khoản Authentication Agent trước khi mã hóa ổ đĩa. Bạn có thể bật tự động tạo tài khoản Authentication Agent trong thiết lập chính sách Mã hóa toàn bộ ổ đĩa (xem hướng dẫn bên dưới). Bạn cũng có thể [sử dụng công nghệ Single Sign-On \(SSO\)](#).

Kaspersky Endpoint Security cho phép bạn tự động tạo Authentication Agent cho các nhóm người dùng sau:

- **Tất cả tài khoản trên máy tính.** Tất cả các tài khoản trên máy tính đã hoạt động bất kỳ lúc nào.
- **Tất cả các tài khoản domain trên máy tính.** Tất cả các tài khoản trên máy tính thuộc về một tên miền và đã hoạt động bất kỳ lúc nào.
- **Tất cả tài khoản nội bộ trên máy tính.** Tất cả các tài khoản cục bộ trên máy tính đã hoạt động bất kỳ lúc nào.
- **Tài khoản dịch vụ có mật khẩu dùng một lần.** Cần có tài khoản dịch vụ để có quyền truy cập vào máy tính, như khi người dùng quên mật khẩu. Bạn cũng có thể sử dụng tài khoản dịch vụ như tài khoản dự trữ. Bạn phải nhập tên của tài khoản (mặc định là ServiceAccount). Kaspersky Endpoint Security sẽ tạo mật khẩu tự động. Bạn có thể tìm thấy mật khẩu trong [bảng điều khiển Kaspersky Security Center](#).

- **Quản trị nội bộ.** Kaspersky Endpoint Security sẽ tạo tài khoản người dùng Authentication Agent cho quản trị viên cục bộ của máy tính.
- **Quản lý máy tính.** Kaspersky Endpoint Security sẽ tạo tài khoản người dùng Authentication Agent cho tài khoản của người quản lý máy tính. Bạn có thể xem tài khoản nào có vai trò người quản lý máy tính trong thuộc tính máy tính trong Active Directory. Theo mặc định, vai trò người quản lý máy tính không được định nghĩa, tức là nó không tương ứng với bất kỳ tài khoản nào.
- **Kích hoạt tài khoản.** Kaspersky Endpoint Security sẽ tự động tạo tài khoản Authentication Agent cho tài khoản đang hoạt động tại thời điểm mã hóa ổ đĩa.

Tác vụ [Quản lý tài khoản Authentication Agent](#) được thiết kế để cấu hình thiết lập xác thực người dùng. Bạn có thể sử dụng tác vụ này để thêm tài khoản mới, sửa đổi thiết lập của tài khoản hiện tại hoặc xóa tài khoản nếu cần. Bạn có thể sử dụng tác vụ cục bộ cho các máy tính cá nhân cũng sử dụng tác vụ nhóm cho máy tính từ các nhóm quản trị riêng biệt hoặc một nhóm các máy tính tuyển chọn.

[Cách chạy Kaspersky Disk Encryption thông qua Bảng điều khiển quản trị \(MMC\)](#)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Mã hóa toàn bộ ổ đĩa**.
6. Trong danh sách thả xuống **Công nghệ mã hóa**, hãy chọn **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.

7. Trong danh sách thả xuống **Chế độ mã hóa**, chọn mục **Mã hóa tất cả ổ đĩa cứng**.

Nếu máy tính có cài nhiều hệ điều hành, sau khi mã hóa tất cả các ổ cứng, bạn sẽ chỉ có thể nạp hệ điều hành đã cài đặt ứng dụng.

Nếu bạn muốn loại trừ một số ổ cứng khỏi tác vụ mã hóa, hãy [tạo một danh sách các ổ cứng đó](#).

8. Cấu hình tùy chọn Kaspersky Disk Encryption nâng cao (xem bảng bên dưới).
9. Lưu các thay đổi của bạn.

[Cách chạy Kaspersky Disk Encryption thông qua Bảng điều khiển web và Bảng điều khiển đám mây](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Mã hóa dữ liệu** → **Mã hóa toàn bộ ổ đĩa**.
5. Trong mục **Quản lý mã hóa**, hãy chọn **Kaspersky Disk Encryption**.
6. Nhấn vào liên kết **Kaspersky Disk Encryption**.
Thao tác này sẽ mở cửa sổ thiết lập 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.

7. Trong danh sách thả xuống **Chế độ mã hóa**, chọn mục **Mã hóa tất cả ổ đĩa cứng**.

Nếu máy tính có cài đặt nhiều hệ điều hành, sau khi mã hóa, bạn sẽ chỉ có thể nạp hệ điều hành đã thực hiện việc mã hóa.

Nếu bạn muốn loại trừ một số ổ cứng khỏi tác vụ mã hóa, hãy [tạo một danh sách các ổ cứng đó](#).

8. Cấu hình tùy chọn Kaspersky Disk Encryption nâng cao (xem bảng bên dưới).
9. Lưu các thay đổi của bạn.

Bạn có thể sử dụng công cụ Giám sát mã hóa để kiểm soát quá trình mã hóa hoặc giải mã ổ đĩa trên máy tính của người dùng. Bạn có thể chạy công cụ Giám sát mã hóa từ [cửa sổ chính của ứng dụng](#).

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.

Thiết lập thành phần Kaspersky Disk Encryption

Tham số	Mô tả
Tự động tạo các tài khoản Authentication Agent cho người dùng trong quá trình mã hóa	Nếu hộp kiểm này được chọn, ứng dụng sẽ tạo tài khoản Authentication Agent dựa trên danh sách tài khoản người dùng Windows trên máy tính. Theo mặc định, Kaspersky Endpoint Security sử dụng tất cả các tài khoản cục bộ và tên miền mà người dùng đã sử dụng để đăng nhập vào hệ điều hành trong 30 ngày qua.
Tự động tạo các tài khoản	Nếu hộp kiểm này được chọn, ứng dụng sẽ kiểm tra thông tin về tài khoản người dùng Windows trên máy tính trước khi khởi chạy Authentication Agent.

<p>Authentication Agent cho mọi người dùng của máy tính này sau khi đăng nhập</p>	<p>Nếu Kaspersky Endpoint Security phát hiện tài khoản người dùng Windows không có tài khoản Authentication Agent, ứng dụng sẽ tạo một tài khoản mới để truy cập các ổ đĩa được mã hóa. Tài khoản Authentication Agent mới sẽ có các thiết lập mặc định sau: chỉ cho phép đăng nhập được bảo vệ bằng mật khẩu và thay đổi mật khẩu trong lần xác thực đầu tiên. Do đó, bạn không cần phải thêm tài khoản Authentication Agent theo cách thủ công bằng cách sử dụng tác vụ <i>Quản lý tài khoản Authentication Agent</i> cho máy tính có ổ đĩa đã được mã hóa.</p>
<p>Lưu tên người dùng đã nhập vào Authentication Agent</p>	<p>Nếu hộp kiểm này được chọn, ứng dụng sẽ lưu lại tên của tài khoản Authentication Agent. Bạn sẽ không được yêu cầu nhập tên tài khoản ở lần nhập thông tin xác thực tiếp theo trong Authentication Agent cho cùng tài khoản.</p>
<p>Chỉ mã hóa dung lượng ổ đĩa được sử dụng (giảm thời gian mã hóa)</p>	<p>Hộp kiểm này bật / tắt tùy chọn chỉ giới hạn khu vực mã hóa đến các phần ổ cứng đang được sử dụng. Giới hạn này sẽ giúp bạn giảm thời gian mã hóa.</p> <div data-bbox="413 658 1493 853" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Việc bật hoặc tắt tính năng Chỉ mã hóa dung lượng ổ đĩa được sử dụng (Windows 8 và các phiên bản mới hơn) sau khi bắt đầu mã hóa sẽ không sửa đổi thiết lập này cho đến khi các ổ cứng được giải mã. Bạn phải chọn hoặc xóa hộp kiểm trước khi bắt đầu mã hóa.</p> </div> <p>Nếu hộp kiểm này được chọn, chỉ các phần của ổ cứng có chứa các tập tin mới được mã hóa. Kaspersky Endpoint Security sẽ tự động mã hóa dữ liệu mới khi chúng được bổ sung.</p> <p>Nếu hộp kiểm này bị xóa, toàn bộ ổ cứng sẽ được mã hóa, bao gồm các phần sót lại của những tập tin đã được sửa đổi hoặc bị xóa trước đó.</p> <div data-bbox="413 1122 1493 1350" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Tùy chọn này được khuyến nghị cho các ổ cứng mới có dữ liệu chưa được sửa đổi hoặc bị xóa. Nếu bạn đang áp dụng mã hóa trên một ổ cứng đang được sử dụng, bạn nên mã hóa toàn bộ ổ cứng. Điều này sẽ đảm bảo toàn bộ dữ liệu được bảo vệ, kể cả những dữ liệu đã bị xóa và có khả năng được phục hồi.</p> </div> <p>Hộp kiểm này được xóa ở chế độ mặc định.</p>
<p>Sử dụng Hỗ trợ USB chuẩn cũ (không khuyến dùng)</p>	<p>Hộp kiểm này bật/tắt chức năng Hỗ trợ USB chuẩn cũ. <i>Hỗ trợ USB chuẩn cũ là</i> một chức năng của BIOS/UEFI, cho phép bạn sử dụng các thiết bị USB (như token bảo mật) trong thời gian khởi động của máy tính trước khi khởi động hệ điều hành (chế độ BIOS). Chức năng Hỗ trợ USB chuẩn cũ không ảnh hưởng đến hỗ trợ cho các thiết bị USB sau khi hệ điều hành đã được khởi động.</p> <p>Nếu hộp kiểm này được chọn, tính năng hỗ trợ cho các thiết bị USB trong quá trình khởi động máy tính ban đầu sẽ được bật.</p> <div data-bbox="413 1767 1493 1962" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0; background-color: #f8d7da;"> <p>Khi chức năng Hỗ trợ USB chuẩn cũ được bật, Authentication Agent ở chế độ BIOS không hỗ trợ làm việc với các token qua USB. Bạn chỉ nên sử dụng tùy chọn này khi có vấn đề về tương thích phần cứng và chỉ dành cho các máy tính gặp phải vấn đề này.</p> </div>

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 Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Mã hóa toàn bộ ổ đĩa**.
6. Trong danh sách thả xuống **Công nghệ mã hóa**, hãy chọn **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.
7. Để thêm ổ cứng vào danh sách các ổ cứng được loại trừ khỏi tác vụ mã hóa:
 - a. Nhấn vào **Thêm**.
 - b. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy chỉnh sửa **Tên thiết bị**, **Tên máy tính**, **Kiểu ổ đĩa**, thiết lập **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 ổ đĩa cứng sau đây**.

8. Lưu các thay đổi của bạn.

Xuất và nhập một danh sách các ổ đĩa cứng được loại trừ khỏi tác vụ mã hóa

Bạn có thể xuất danh sách loại trừ mã hóa ổ đĩa cứng vào một tập tin XML. Sau đó, bạn có thể sửa đổi tập tin, ví dụ như thêm một số lượng lớn các loại trừ cùng loại. Bạn cũng có thể sử dụng chức năng xuất/nhập để sao lưu danh sách các loại trừ hoặc để chuyển loại trừ sang máy chủ khác.

[Cách xuất và nhập danh sách loại trừ mã hóa ổ đĩa cứng trong Bảng điều khiển quản trị \(MMC\)](#)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Mã hóa toàn bộ ổ đĩa**.
6. Trong danh sách thả xuống **Công nghệ mã hóa**, hãy chọn **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**.
7. Để xuất danh sách loại trừ:
 - a. Chọn các loại trừ mà bạn muốn xuất. Để chọn nhiều cổng, hãy sử dụng phím **CTRL** hoặc **SHIFT**.
Nếu bạn không chọn loại trừ nào, Kaspersky Endpoint Security sẽ xuất tất cả các loại trừ.
 - b. Nhấn liên kết **Xuất**.
 - c. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin XML mà bạn muốn xuất danh sách các loại trừ vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
 - d. Lưu tập tin.
Kaspersky Endpoint Security sẽ xuất toàn bộ danh sách các loại trừ vào tập tin XML.
8. Để nhập danh sách quy tắc:
 - a. Nhấn **Nhập**.
 - b. Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách các loại trừ.
 - c. Mở tập tin.
Nếu máy tính đã có danh sách các loại trừ, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.
9. Lưu các thay đổi của bạn.

Cách xuất và nhập danh sách loại trừ mã hóa ổ đĩa cứng trong Bảng điều khiển web 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Mã hóa dữ liệu** → **Mã hóa toàn bộ ổ đĩa**.
5. Chọn công nghệ **Kaspersky Disk Encryption** và điều hướng theo liên kết để cấu hình thiết lập.
Thiết lập mã hóa sẽ mở ra.
6. Nhấn liên kết **Loại trừ**.
7. Để xuất danh sách quy tắc:
 - a. Chọn các loại trừ mà bạn muốn xuất.
 - b. Nhấn vào **Xuất**.
 - c. Xác nhận rằng bạn chỉ muốn xuất các loại trừ đã chọn hoặc xuất toàn bộ danh sách loại trừ.
 - d. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin XML mà bạn muốn xuất danh sách các loại trừ vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
 - e. Lưu tập tin.
Kaspersky Endpoint Security sẽ xuất toàn bộ danh sách các loại trừ vào tập tin XML.
8. Để nhập danh sách quy tắc:
 - a. Nhấn **Nhập**.
 - b. Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách các loại trừ.
 - c. Mở tập tin.
Nếu máy tính đã có danh sách các loại trừ, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.
9. Lưu các thay đổi của bạn.

Bật công nghệ Single Sign-On (SSO)

Công nghệ Single Sign-On (SSO) cho phép bạn tự động đăng nhập vào hệ điều hành bằng thông tin đăng nhập của Authentication Agent.

Khi sử dụng công nghệ Single Sign-On, Authentication Agent sẽ bỏ qua các yêu cầu về độ mạnh mật khẩu được chỉ định trong Kaspersky Security Center. Bạn có thể đặt yêu cầu độ mạnh mật khẩu trong thiết lập của hệ điều hành.

Công nghệ Single Sign-On không tương thích với các nhà cung cấp chứng chỉ tài khoản thuộc bên thứ ba.

Cách bật sử dụng công nghệ Single Sign-On trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Thiết lập mã hóa chung**.
6. Trong mục **Thiết lập mật khẩu**, hãy nhấn nút **Thiết lập**.
7. Trong cửa sổ mở ra, trên thẻ **Authentication Agent**, hãy chọn hộp kiểm **Sử dụng công nghệ Single Sign-On (SSO)**.
8. Lưu các thay đổi của bạn.

Kết quả là người dùng chỉ cần hoàn thành quy trình xác thực một lần với Agent. Không bắt buộc thực hiện Quy trình xác thực để nạp hệ điều hành. Hệ điều hành sẽ nạp tự động.

Cách bật sử dụng Single Sign-On trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Mã hóa dữ liệu** → **Mã hóa toàn bộ ổ đĩa**.
5. Chọn công nghệ **Kaspersky Disk Encryption** và điều hướng theo liên kết để cấu hình thiết lập.
Thiết lập mã hóa sẽ mở ra.
6. Trong mục **Thiết lập mật khẩu**, hãy chọn hộp kiểm **Sử dụng công nghệ Single Sign-On (SSO)**.
7. Lưu các thay đổi của bạn.

Kết quả là người dùng chỉ cần hoàn thành quy trình xác thực một lần với Agent. Không bắt buộc thực hiện Quy trình xác thực để nạp hệ điều hành. Hệ điều hành sẽ nạp tự động.

Để Single Sign-On hoạt động, mật khẩu tài khoản Windows và mật khẩu tài khoản Authentication Agent phải khớp nhau. Nếu mật khẩu không khớp, người dùng cần thực hiện quy trình xác thực hai lần: trong giao diện của Authentication Agent và trước khi nạp hệ điều hành. Sau đó, Kaspersky Endpoint Security sẽ thay thế mật khẩu của tài khoản Authentication Agent bằng mật khẩu của tài khoản Windows.

Quản lý tài khoản Authentication Agent

Authentication Agent là thành phần cần thiết để làm việc với các ổ đĩa được bảo vệ bằng công nghệ Kaspersky Disk Encryption (FDE). Trước khi hệ điều hành được nạp, người dùng cần hoàn thành xác thực với Agent. Tác vụ *Quản lý tài khoản Authentication Agent* được thiết kế để cấu hình thiết lập xác thực người dùng. Bạn có thể sử dụng tác vụ cục bộ cho các máy tính cá nhân cũng sử dụng tác vụ nhóm cho máy tính từ các nhóm quản trị riêng biệt hoặc một nhóm các máy tính tuyển chọn.

Bạn không thể cấu hình lịch để bắt đầu tác vụ *Quản lý tài khoản Authentication Agent*. Bạn cũng không thể buộc dừng một tác vụ.

[Cách tạo tác vụ Quản lý tài khoản Authentication Agent trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Trong Bảng điều khiển quản trị, hãy vào thư mục **Administration Server** → **Tác vụ**.

Danh sách tác vụ sẽ mở.

2. Nhấn nút **New task**.

Trình hướng dẫn Tác vụ sẽ được bắt đầu. Làm theo chỉ dẫn của Trình hướng dẫn.

Bước 1. Chọn loại tác vụ

Chọn **Kaspersky Endpoint Security cho Windows (11.9.0)** → **Quản lý tài khoản Authentication Agent**.

Bước 2. Chọn một lệnh quản lý tài khoản Authentication Agent

Tạo danh sách các lệnh quản lý tài khoản Authentication Agent. Các lệnh quản lý cho phép bạn thêm, sửa đổi và xóa các tài khoản Authentication Agent (xem hướng dẫn bên dưới). Chỉ những người dùng có tài khoản Authentication Agent mới có thể hoàn tất quy trình xác thực, nạp hệ điều hành và có quyền truy cập vào ổ đĩa được mã hóa.

Bước 3. Chọn các thiết bị sẽ được gán tác vụ

Chọn các máy tính sẽ được thực hiện tác vụ trên đó. Các tùy chọn sau có thể được sử dụng:

- Gán tác vụ vào một nhóm quản trị. Trong trường hợp này, tác vụ sẽ được gán cho các máy tính được bao gồm trong một nhóm quản trị đã được tạo trước đó.
- Chọn các máy tính được Máy chủ quản trị phát hiện trong mạng – *các thiết bị chưa được gán*. Các thiết bị được quy định có thể bao gồm các thiết bị trong nhóm quản trị cũng như các thiết bị chưa được gán.
- Nhập vào thủ công địa chỉ của thiết bị, hoặc nhập các địa chỉ từ một danh sách. Bạn có thể quy định tên NetBIOS, địa chỉ IP, và địa chỉ IP mạng con của các thiết bị mà bạn muốn gán tác vụ.

Bước 4. Xác định tên tác vụ

Nhập tên cho tác vụ, ví dụ: *Tài khoản quản trị viên*.

Bước 5. Hoàn tất việc tạo tác vụ

Thoát Trình hướng dẫn. Nếu cần, hãy chọn hộp kiểm **Run the task after the Wizard finishes**. Bạn có thể giám sát tiến độ của tác vụ trong thuộc tính tác vụ.

Do đó, sau khi hoàn thành tác vụ khi máy tính khởi động vào lần tới, người dùng mới có thể hoàn tất quy trình xác thực, nạp hệ điều hành và có quyền truy cập vào ổ đĩa được mã hóa.

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.

Danh sách tác vụ sẽ mở.

2. Nhấn vào nút **Thêm**.

Trình hướng dẫn Tác vụ sẽ được bắt đầu. Làm theo chỉ dẫn của Trình hướng dẫn.

Bước 1. Cấu hình thiết lập tác vụ tổng quát

Cấu hình thiết lập của tác vụ tổng quát:

1. Trong danh sách thả xuống **Ứng dụng**, hãy chọn **Kaspersky Endpoint Security cho Windows (11.9.0)**.
2. Trong danh sách thả xuống **Loại tác vụ**, hãy chọn **Quản lý tài khoản Authentication Agent**.
3. Trong trường **Task name**, hãy nhập một mô tả ngắn, ví dụ như *Tài khoản quản trị viên*.
4. Trong phần **Select devices to which the task will be assigned**, chọn phạm vi tác vụ.

Bước 2. Quản lý tài khoản Authentication Agent

Tạo danh sách các lệnh quản lý tài khoản Authentication Agent. Các lệnh quản lý cho phép bạn thêm, sửa đổi và xóa các tài khoản Authentication Agent (xem hướng dẫn bên dưới). Chỉ những người dùng có tài khoản Authentication Agent mới có thể hoàn tất quy trình xác thực, nạp hệ điều hành và có quyền truy cập vào ổ đĩa được mã hóa.

Bước 3. Hoàn tất việc tạo tác vụ

Thoát Trình hướng dẫn. Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ.

Để thực hiện một tác vụ, chọn hộp kiểm cạnh tác vụ đó và nhấn nút **Bắt đầu**.

Do đó, sau khi hoàn thành tác vụ khi máy tính khởi động vào lần tới, người dùng mới có thể hoàn tất quy trình xác thực, nạp hệ điều hành và có quyền truy cập vào ổ đĩa được mã hóa.

Để thêm tài khoản Authentication Agent, bạn cần thêm một lệnh đặc biệt vào tác vụ *Quản lý tài khoản Authentication Agent*. Sử dụng tác vụ nhóm là cách thuận tiện, ví dụ như để thêm tài khoản quản trị viên vào tất cả các máy tính.

Kaspersky Endpoint Security cho phép bạn tự động tạo tài khoản Authentication Agent trước khi mã hóa ổ đĩa. Bạn có thể bật tự động tạo tài khoản Authentication Agent trong [thiết lập chính sách Mã hóa toàn bộ ổ đĩa](#). Bạn cũng có thể [sử dụng công nghệ Single Sign-On \(SSO\)](#).

[Cách thêm tài khoản Authentication Agent thông qua Bảng điều khiển quản trị \(MMC\)](#) ²

1. Mở thuộc tính của tác vụ *Quản lý tài khoản Authentication Agent*.
2. Trong thuộc tính tác vụ, hãy chọn mục **Thiết lập**.
3. Nhấn vào **Thêm** → **Lệnh thêm tài khoản**.
4. Trong cửa sổ mở ra, trong trường **Tài khoản Windows**, chỉ định tên của tài khoản Microsoft Windows sẽ được sử dụng để tạo tài khoản Authentication Agent.
5. Nếu bạn đã nhập thủ công tên tài khoản Windows, hãy bấm vào nút **Cho phép** để xác định định danh bảo mật tài khoản (SID).
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.

Xác định một định danh bảo mật tài khoản Windows là điều cần thiết để xác minh rằng tên tài khoản Windows đã được nhập chính xác. Nếu tài khoản Windows không tồn tại trên máy tính hoặc trong miền được tin tưởng, tác vụ *Quản lý tài khoản Authentication Agent* sẽ kết thúc kèm theo một lỗi.

6. Chọn hộp kiểm **Thay thế tài khoản hiện tại** nếu bạn muốn tài khoản đã được tạo từ trước cho Authentication Agent được thay thế bởi 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 nhóm tác vụ cho việc quản lý các tài khoản Authentication Agent. Bước này không khả dụng khi bạn bổ sung một lệnh tạo tài khoản Authentication Agent trong thuộc tính của một tác vụ cục bộ *Quản lý tài khoản Authentication Agent*.

7. 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.
8. 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. Đặt mật khẩu cho tài khoản Authentication Agent. Nếu cần, bạn có thể yêu cầu mật khẩu mới từ người dùng sau lần xác thực đầu tiên.
9. Chọn hộp kiểm **Cho phép xác thực dựa trên chứng chỉ** 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. Chọn tập tin chứng chỉ để xác thực bằng thẻ thông minh hoặc token.
10. Nếu cần thiết, trong trường **Mô tả dòng lệnh**, nhập chi tiết tài khoản Authentication Agent mà bạn cần để quản lý lệnh.
11. Trong mục **Truy cập chứng thực trong Authentication Agent**, hãy cấu hình quyền truy cập xác thực trong Authentication Agent cho người dùng sử dụng tài khoản được chỉ định trong lệnh.
12. Lưu các thay đổi của bạn.

[Cách thêm tài khoản Authentication Agent thông qua Bảng điều khiển web](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.

Danh sách tác vụ sẽ mở.

2. Nhấn vào tác vụ **Quản lý tài khoản Authentication Agent** của Kaspersky Endpoint Security.

Cửa sổ thuộc tính tác vụ sẽ được mở ra.

3. Chọn thẻ **Application settings**.

4. Trong danh sách tài khoản Authentication Agent, hãy nhấn nút **Thêm**.

Làm vậy sẽ khởi chạy Trình hướng dẫn quản lý tài khoản Authentication Agent.

5. Chọn loại lệnh **Thêm**.

6. Chọn một tài khoản người dùng. Bạn có thể chọn một tài khoản trong danh sách tài khoản tên miền hoặc nhập tên tài khoản theo cách thủ công. Chuyển sang bước tiếp theo.

Kaspersky Endpoint Security sẽ xác định danh bảo mật tài khoản (SID). Đây là điều cần thiết để xác minh tài khoản. Nếu bạn không nhập đúng tên người dùng, Kaspersky Endpoint Security sẽ kết thúc tác vụ kèm theo một lỗi.

7. Cấu hình thiết lập tài khoản Authentication Agent.

- **Create a new Authentication Agent account to replace the existing account.** Kaspersky Endpoint Security sẽ quét các tài khoản hiện có trên máy tính. Nếu ID bảo mật người dùng trên máy tính và trong tác vụ khớp nhau, Kaspersky Endpoint Security sẽ thay đổi thiết lập tài khoản người dùng theo tác vụ đó.
- **Tên người dùng.** Tên người dùng mặc định của tài khoản Authentication Agent tương ứng với tên miền của người dùng.
- **Cho phép xác thực dựa trên mật khẩu.** Đặt mật khẩu cho tài khoản Authentication Agent. Nếu cần, bạn có thể yêu cầu mật khẩu mới từ người dùng sau lần xác thực đầu tiên. Bằng cách này, mỗi người dùng sẽ có mật khẩu riêng của họ. Bạn cũng có thể đặt yêu cầu về độ mạnh mật khẩu cho tài khoản Authentication Agent trong chính sách.
- **Cho phép xác thực dựa trên chứng chỉ.** Chọn tập tin chứng chỉ để xác thực bằng thẻ thông minh hoặc token. Bằng cách này, người dùng sẽ cần nhập mật khẩu cho thẻ thông minh hoặc token.
- **Account access to encrypted data.** Cấu hình quyền truy cập của người dùng vào ổ đĩa được mã hóa. Ví dụ: bạn có thể tạm thời vô hiệu hóa xác thực người dùng thay vì xóa tài khoản Authentication Agent.
- **Bình luận.** Nếu cần, hãy nhập mô tả tài khoản.

8. Lưu các thay đổi của bạn.

9. Hãy chọn hộp kiểm cạnh tác vụ đó và nhấn nút **Bắt đầu**.

Do đó, sau khi hoàn thành tác vụ khi máy tính khởi động vào lần tới, người dùng mới có thể hoàn tất quy trình xác thực, nạp hệ điều hành và có quyền truy cập vào ổ đĩa được mã hóa.

Để thay đổi mật khẩu và thiết lập khác của tài khoản Authentication Agent, bạn cần thêm một lệnh đặc biệt vào tác vụ *Quản lý tài khoản Authentication Agent*. Sử dụng tác vụ nhóm là cách thuận tiện, ví dụ như để thay thế chứng chỉ token quản trị viên trên tất cả các máy tính.

[Cách thay đổi tài khoản Authentication Agent thông qua Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở thuộc tính của tác vụ *Quản lý tài khoản Authentication Agent*.
2. Trong thuộc tính tác vụ, hãy chọn mục **Thiết lập**.
3. Nhấn vào **Thêm** → **Lệnh chỉnh sửa tài khoản**.
4. Trong cửa sổ mở ra, trong trường **Tài khoản Windows**, hãy chỉ định tên của tài khoản người dùng Microsoft Windows mà bạn muốn thay đổi.
5. Nếu bạn đã nhập thủ công tên tài khoản Windows, hãy bấm vào nút **Cho phép** để xác định định danh bảo mật tài khoản (SID).
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.

Xác định một định danh bảo mật tài khoản Windows là điều cần thiết để xác minh rằng tên tài khoản Windows đã được nhập chính xác. Nếu tài khoản Windows không tồn tại trên máy tính hoặc trong miền được tin tưởng, tác vụ *Quản lý tài khoản Authentication Agent* sẽ kết thúc kèm theo một lỗi.

6. 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.
7. Chọn hộp kiểm **Sửa đổi thiết lập xác thực dựa trên mật khẩu** để có thể sửa cấu hình xác thực bằng mật khẩu.
8. 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. Đặt mật khẩu cho tài khoản Authentication Agent.
9. Chọn hộp kiểm **Chỉnh sửa quy tắc thay đổi mật khẩu khi xác thực trong Authentication Agent** nếu bạn muốn Kaspersky Endpoint Security thay đổi giá trị của thiết lập 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 thiết lập được chỉ định dưới đây.
10. Quy định giá trị của cấu hình thay đổi mật khẩu khi xác thực trong Authentication Agent.
11. Chọn hộp kiểm **Sửa đổi thiết lập xác thực dựa trên chứng chỉ** để có thể sửa cấu hình xác thực dựa trên chứng chỉ điện tử của một token hoặc thẻ thông minh.
12. Chọn hộp kiểm **Cho phép xác thực dựa trên chứng chỉ** 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. Chọn tập tin chứng chỉ để xác thực bằng thẻ thông minh hoặc token.
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 truy cập xác thực trong Authentication Agent** nếu bạn muốn Kaspersky Endpoint Security thay đổi quy tắc truy cập của người dùng vào hộp thoại xác thực trong Authentication Agent thành 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 vào quy tắc để truy cập hộp thoại xác thực trong Authentication Agent.
16. Lưu các thay đổi của bạn.

[Cách thay đổi tài khoản Authentication Agent thông qua Bảng điều khiển web](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.
Danh sách tác vụ sẽ mở.
2. Nhấn vào tác vụ **Quản lý tài khoản Authentication Agent** của Kaspersky Endpoint Security.
Cửa sổ thuộc tính tác vụ sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Trong danh sách tài khoản Authentication Agent, hãy nhấn nút **Thêm**.
Làm vậy sẽ khởi chạy Trình hướng dẫn quản lý tài khoản Authentication Agent.
5. Chọn loại lệnh **Thay đổi**.
6. Chọn một tài khoản người dùng. Bạn có thể chọn một tài khoản trong danh sách tài khoản tên miền hoặc nhập tên tài khoản theo cách thủ công. Chuyển sang bước tiếp theo.
Kaspersky Endpoint Security sẽ xác định danh sách bảo mật tài khoản (SID). Đây là điều cần thiết để xác minh tài khoản. Nếu bạn không nhập đúng tên người dùng, Kaspersky Endpoint Security sẽ kết thúc tác vụ kèm theo một lỗi.
7. Chọn các hộp kiểm cạnh thiết lập bạn muốn chỉnh sửa.
8. Cấu hình thiết lập tài khoản Authentication Agent.
 - **Create a new Authentication Agent account to replace the existing account.** Kaspersky Endpoint Security sẽ quét các tài khoản hiện có trên máy tính. Nếu ID bảo mật người dùng trên máy tính và trong tác vụ khớp nhau, Kaspersky Endpoint Security sẽ thay đổi thiết lập tài khoản người dùng theo tác vụ đó.
 - **Tên người dùng.** Tên người dùng mặc định của tài khoản Authentication Agent tương ứng với tên miền của người dùng.
 - **Cho phép xác thực dựa trên mật khẩu.** Đặt mật khẩu cho tài khoản Authentication Agent. Nếu cần, bạn có thể yêu cầu mật khẩu mới từ người dùng sau lần xác thực đầu tiên. Bằng cách này, mỗi người dùng sẽ có mật khẩu riêng của họ. Bạn cũng có thể đặt yêu cầu về độ mạnh mật khẩu cho tài khoản Authentication Agent trong chính sách.
 - **Cho phép xác thực dựa trên chứng chỉ.** Chọn tập tin chứng chỉ để xác thực bằng thẻ thông minh hoặc token. Bằng cách này, người dùng sẽ cần nhập mật khẩu cho thẻ thông minh hoặc token.
 - **Account access to encrypted data.** Cấu hình quyền truy cập của người dùng vào ổ đĩa được mã hóa. Ví dụ: bạn có thể tạm thời vô hiệu hóa xác thực người dùng thay vì xóa tài khoản Authentication Agent.
 - **Bình luận.** Nếu cần, hãy nhập mô tả tài khoản.
9. Lưu các thay đổi của bạn.
10. Hãy chọn hộp kiểm cạnh tác vụ đó và nhấn nút **Bắt đầu**.

Để xóa tài khoản Authentication Agent, bạn cần thêm một lệnh đặc biệt vào tác vụ *Quản lý tài khoản Authentication Agent*. Sử dụng tác vụ nhóm là cách thuận tiện, ví dụ như để xóa tài khoản của một nhân viên bị sa thải.

Cách xóa tài khoản Authentication Agent thông qua Bảng điều khiển quản trị.(MMC)

1. Mở thuộc tính của tác vụ *Quản lý tài khoản Authentication Agent*.
2. Trong thuộc tính tác vụ, hãy chọn mục **Thiết lập**.
3. Nhấn vào **Thêm** → **Lệnh xóa tài khoản**.
4. Trong cửa sổ mở ra, trong trường **Tài khoản Windows**, hãy chỉ định tên tài khoản Windows đã được sử dụng để tạo tài khoản Authentication Agent mà bạn muốn xóa.
5. Nếu bạn đã nhập thủ công tên tài khoản Windows, hãy bấm vào nút **Cho phép** để xác định định danh bảo mật tài khoản (SID).

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.

Xác định một định danh bảo mật tài khoản Windows là điều cần thiết để xác minh rằng tên tài khoản Windows đã được nhập chính xác. Nếu tài khoản Windows không tồn tại trên máy tính hoặc trong miền được tin tưởng, tác vụ *Quản lý tài khoản Authentication Agent* sẽ kết thúc kèm theo một lỗi.

6. Lưu các thay đổi của bạn.

Cách xóa tài khoản Authentication Agent thông qua Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.
Danh sách tác vụ sẽ mở.
2. Nhấn vào tác vụ **Quản lý tài khoản Authentication Agent** của Kaspersky Endpoint Security.
Cửa sổ thuộc tính tác vụ sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Trong danh sách tài khoản Authentication Agent, hãy nhấn nút **Thêm**.
Làm vậy sẽ khởi chạy Trình hướng dẫn quản lý tài khoản Authentication Agent.
5. Chọn loại lệnh **Xóa**.
6. Chọn một tài khoản người dùng. Bạn có thể chọn một tài khoản trong danh sách tài khoản tên miền hoặc nhập tên tài khoản theo cách thủ công.
7. Lưu các thay đổi của bạn.
8. Hãy chọn hộp kiểm cạnh tác vụ đó và nhấn nút **Bắt đầu**.

Do đó, sau khi tác vụ được hoàn tất ở lần khởi động máy tính tiếp theo, người dùng sẽ không thể hoàn tất quy trình xác thực và nạp hệ điều hành. Kaspersky Endpoint Security sẽ từ chối quyền truy cập vào dữ liệu được mã hóa.

Để xem danh sách người dùng có thể hoàn tất xác thực với Agent và nạp hệ điều hành, bạn cần truy cập vào phần thuộc tính của máy tính được quản lý.

[Cách xem danh sách tài khoản Authentication Agent thông qua Bảng điều khiển quản trị \(MMC\)](#)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Devices**.
4. Nhấn đúp để mở cửa sổ thuộc tính máy tính.
5. Trong cửa sổ thuộc tính máy tính, chọn phần **Tác vụ**.
6. Trong danh sách tác vụ, hãy chọn **Quản lý tài khoản Authentication Agent** và mở thuộc tính tác vụ bằng cách nhấn đúp.
7. Trong thuộc tính tác vụ, hãy chọn mục **Thiết lập**.

Do đó, bạn sẽ có thể truy cập danh sách tài khoản Authentication Agent trên máy tính này. Chỉ người dùng trong danh sách này mới có thể hoàn tất xác thực với Agent và nạp hệ điều hành.

[Cách xem danh sách tài khoản Authentication Agent thông qua Bảng điều khiển web](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Managed devices**.
2. Nhấn vào tên của máy tính mà bạn muốn xem danh sách tài khoản Authentication Agent.
3. Trong thuộc tính máy tính, hãy chọn thẻ **Tác vụ**.
4. Trong danh sách tác vụ, hãy chọn **Quản lý tài khoản Authentication Agent**.
5. Trong phần thuộc tính tác vụ, hãy chọn thẻ **Application settings**.

Do đó, bạn sẽ có thể truy cập danh sách tài khoản Authentication Agent trên máy tính này. Chỉ người dùng trong danh sách này mới có thể hoàn tất xác thực với Agent và nạp hệ điều hành.

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 thực hiện, bạn phải thêm tập tin chứng chỉ điện tử của một token hoặc thẻ thông minh vào tác vụ *Quản lý 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.

Kaspersky Endpoint Security hỗ trợ các loại token, đầu đọc thẻ thông minh và thẻ thông minh sau:

- SafeNet eToken PRO 64K (4.2b);
- SafeNet eToken PRO 72K Java;
- SafeNet eToken 4100-72K Java;
- SafeNet eToken 5100;
- SafeNet eToken 5105;
- SafeNet eToken 7300;
- EMC RSA SID 800;
- Gemalto IDPrime.NET 510;
- Gemalto IDPrime.NET 511;
- Rutoken ECP;
- Rutoken ECP Flash;
- Athena IDProtect Laser;
- SafeNet eToken PRO 72K Java;
- Aladdin-RD JaCarta PKI.

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.
- 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 các yêu cầu này, bạn không thể tải tập tin chứng chỉ vào lệnh để tạo tài khoản Authentication Agent.

Tham số KeyUsage của chứng chỉ phải có giá trị keyEncipherment hoặc dataEncipherment. Tham số KeyUsage xác định mục đích của chứng chỉ. Nếu tham số có một giá trị khác, Kaspersky Security Center sẽ tải về tập tin chứng chỉ nhưng sẽ hiển thị một cảnh báo.

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 [tiếp nhận quyền truy cập các thiết bị được mã hóa hoặc khôi phục dữ liệu trên các thiết bị được mã hóa](#).

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 Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Mã hóa toàn bộ ổ đĩa**.
6. Trong danh sách thả xuống **Công nghệ mã hóa**, chọn công nghệ đã được sử dụng để mã hóa ổ cứng.
7. Thực hiện một trong các thao tác sau:
 - Trong danh sách thả xuống **Chế độ mã hóa**, chọn mục **Giải mã 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.

8. Lưu các thay đổi của bạn.

Bạn có thể sử dụng công cụ Giám sát mã hóa để kiểm soát quá trình mã hóa hoặc giải mã ổ đĩa trên máy tính của người dùng. Bạn có thể chạy công cụ Giám sát mã hóa từ [cửa sổ chính của ứng dụng](#).

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.

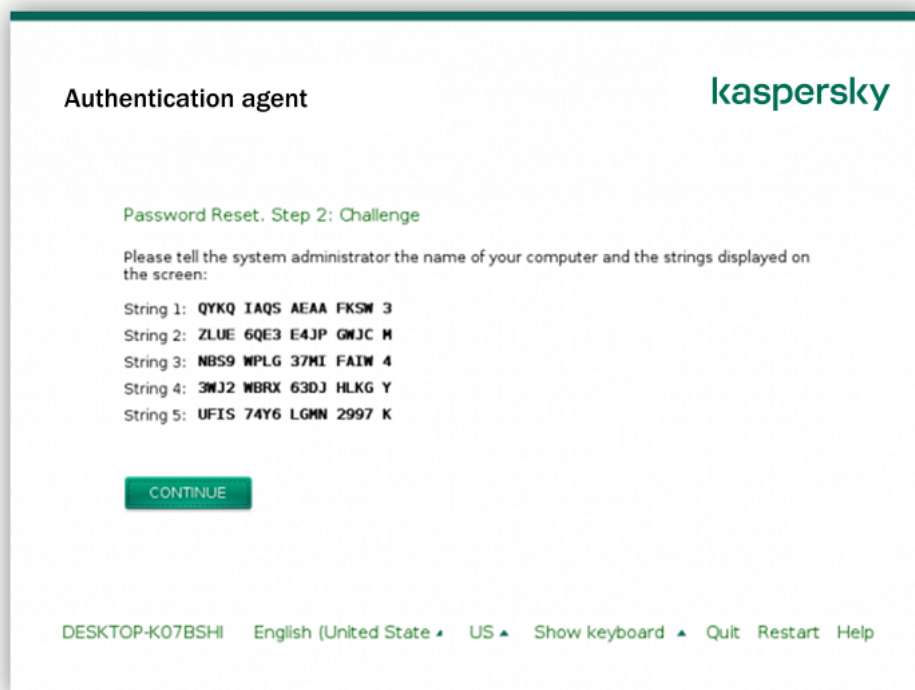
Khôi phục quyền truy cập vào ổ đĩa được bảo vệ bởi công nghệ Kaspersky Disk Encryption

Nếu người dùng quên mật khẩu để truy cập ổ cứng được bảo vệ bởi công nghệ Kaspersky Disk Encryption, bạn cần bắt đầu quy trình khôi phục (Yêu cầu-Phản hồi). Bạn cũng có thể sử dụng [tài khoản dịch vụ](#) để lấy quyền truy cập ổ đĩa cứng nếu tính năng này được bật trong thiết lập mã hóa ổ đĩa.

Khôi phục quyền truy cập vào ổ đĩa cứng hệ thống

Việc khôi phục quyền truy cập vào ổ đĩa cứng hệ thống được bảo vệ bởi công nghệ Kaspersky Disk Encryption bao gồm các bước sau:

1. Người dùng thông báo cáo khối yêu cầu cho quản trị viên (xem hình bên dưới).
2. Quản trị viên nhập các khối yêu cầu vào Kaspersky Security Center, nhận các khối phản hồi và thông báo các khối phản hồi cho người dùng.
3. Người dùng nhập các khối phản hồi trong giao diện Authentication Agent và nhận quyền truy cập vào ổ đĩa cứng.



Khôi phục quyền truy cập vào ổ đĩa cứng hệ thống được bảo vệ bởi công nghệ Kaspersky Disk Encryption

Để bắt đầu quy trình khôi phục, người dùng cần nhấn vào nút **Forgot your password** trong giao diện Authentication Agent.

[Cách nhận khối phản hồi cho ổ đĩa cứng hệ thống được bảo vệ bởi công nghệ Kaspersky Disk Encryption trong Bảng điều khiển quản trị \(MMC\)](#)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Devices**.
4. Trên thẻ **Devices**, hãy chọn máy tính của người dùng yêu cầu truy cập vào dữ liệu được mã hóa và nhấn chuột phải để mở menu ngữ cảnh.
5. Trong menu ngữ cảnh, chọn **Cấp quyền truy cập trong chế độ ngoại tuyến**.
6. Trong cửa sổ mở ra, hãy chọn thẻ **Authentication Agent**.
7. Trong mục **Thuật toán mã hóa được sử dụng**, hãy chọn thuật toán mã hóa: **AES56** hoặc **AES256**.
Thuật toán mã hóa dữ liệu phụ thuộc vào thư viện mã hóa AES, được kèm theo gói phân phối: *Mã hóa mạnh (AES256)* hoặc *Mã hóa nhẹ (AES56)*. Thư viện mã hóa AES được cài đặt cùng với ứng dụng.
8. Trong danh sách thả xuống **Tài khoản**, hãy chọn tên của tài khoản Authentication Agent của người dùng đã yêu cầu khôi phục quyền truy cập vào ổ đĩa.
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.

Kết quả là nội dung của các khối phản hồi đến 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**. Truyền nội dung của các khối phản hồi đến người dùng.

[Cách nhận khối phản hồi cho ổ đĩa cứng hệ thống được bảo vệ bởi công nghệ Kaspersky Disk Encryption trong Bảng điều khiển web](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Managed devices**.
2. Chọn hộp kiểm cạnh tên của máy tính có ổ đĩa mà bạn muốn khôi phục quyền truy cập.
3. Nhấn nút **Grant access to the device in offline mode**.
4. Trong cửa sổ mở ra, hãy chọn mục **Authentication Agent**.
5. 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.
6. Nhập các khối yêu cầu được truyền bởi người dùng.

Nội dung của các khối phản hồi yêu cầu khôi phục tên người dùng và mật khẩu của một tài khoản Authentication Agent sẽ được hiển thị ở cuối cửa sổ. Truyền nội dung của các khối phản hồi đến người dùng.

Sau khi hoàn thành quy trình khôi phục, Authentication Agent sẽ nhắc người dùng thay đổi mật khẩu.

Khôi phục quyền truy cập vào ổ cứng không thuộc hệ thống

Việc khôi phục quyền truy cập vào ổ đĩa cứng không thuộc hệ thống được bảo vệ bởi công nghệ Kaspersky Disk Encryption bao gồm các bước sau:

1. Người dùng gửi cho quản trị viên một tập tin yêu cầu truy cập.
2. Quản trị viên thêm tập tin yêu cầu truy cập vào Kaspersky Security Center, tạo tập tin khóa truy cập và gửi tập tin đó cho người dùng.
3. Người dùng thêm tập tin khóa truy cập vào Kaspersky Endpoint Security và nhận quyền truy cập vào ổ đĩa cứng.

Để bắt đầu quy trình khôi phục, người dùng cần cố gắng truy cập vào ổ đĩa cứng. Kết quả là Kaspersky Endpoint Security sẽ tạo một tập tin yêu cầu truy cập (tập tin có phần mở rộng là KESDC) mà người dùng cần gửi cho quản trị viên, ví dụ như gửi qua email.

Cách lấy tập tin khóa truy cập cho ổ đĩa cứng không thuộc hệ thống được mã hóa trong Bảng điều khiển quản trị (MMC) ²

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Devices**.
4. Trên thẻ **Devices**, hãy chọn máy tính của người dùng yêu cầu truy cập vào dữ liệu được mã hóa và nhấn chuột phải để mở menu ngữ cảnh.
5. Trong menu ngữ cảnh, chọn **Cấp quyền truy cập trong chế độ ngoại tuyến**.
6. Trong cửa sổ mở ra, hãy chọn thẻ **Mã hóa dữ liệu**.
7. Trên thẻ **Mã hóa dữ liệu**, hãy nhấn nút **Duyệt**.
8. Trong cửa sổ để chọn tập tin yêu cầu truy cập, hãy chỉ định đường dẫn đến tập tin nhận được từ người dùng.

Bạn sẽ thấy thông tin về yêu cầu của người dùng. Kaspersky Security Center sẽ tạo một tập tin khóa. Hãy gửi tập tin khóa truy cập dữ liệu mã hóa được tạo ra cho người dùng qua email. Hoặc lưu tập tin truy cập và sử dụng bất kỳ phương thức có sẵn nào để truyền gửi tập tin đó.

Cách lấy tập tin khóa truy cập ổ đĩa cứng không thuộc hệ thống được mã hóa trong Bảng điều khiển web ²

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Managed devices**.
2. Chọn hộp kiểm bên cạnh tên của máy tính có dữ liệu bạn muốn khôi phục quyền truy cập.
3. Nhấn nút **Grant access to the device in offline mode**.
4. Chọn mục **Mã hóa dữ liệu**.
5. Nhấn vào nút **Select file** và chọn tập tin yêu cầu truy cập mà bạn nhận được từ người dùng (tập tin có phần mở rộng là KESDC).
Bảng điều khiển Web sẽ hiển thị thông tin về yêu cầu. Thông tin này sẽ bao gồm tên của máy tính mà người dùng đang yêu cầu quyền truy cập vào tập tin.
6. Nhấn vào nút **Save key** và chọn thư mục để lưu tập tin khóa truy cập dữ liệu được mã hóa (tập tin có phần mở rộng là KESDR).

Kết quả là bạn có thể lấy được khóa truy cập dữ liệu được mã hóa cần để truyền gửi cho người dùng.

Đăng nhập bằng tài khoản dịch vụ Authentication Agent

Kaspersky Endpoint Security cho phép bạn thêm tài khoản dịch vụ Authentication Agent khi [mã hóa ổ đĩa](#). Cần có tài khoản dịch vụ để có quyền truy cập vào máy tính, như khi người dùng quên mật khẩu. Bạn cũng có thể sử dụng tài khoản dịch vụ như tài khoản dự trữ. Để thêm tài khoản, hãy chọn một tài khoản dịch vụ trong [thiết lập mã hóa ổ đĩa](#) và nhập tên của tài khoản người dùng (mặc định là ServiceAccount). Để xác thực bằng tác nhân, bạn sẽ cần mật khẩu dùng một lần.

[Cách tìm mật khẩu dùng một lần trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Devices**.
4. Nhấn đúp để mở cửa sổ thuộc tính máy tính.
5. Trong cửa sổ thuộc tính máy tính, chọn phần **Tác vụ**.
6. Trong danh sách tác vụ, hãy chọn **Quản lý tài khoản Authentication Agent** và mở thuộc tính tác vụ bằng cách nhấn đúp.
7. Trong cửa sổ thuộc tính tác vụ, hãy chọn mục **Thiết lập**.
8. Trong danh sách tài khoản, hãy chọn tài khoản dịch vụ Authentication Agent (ví dụ: WIN10-USER\ServiceAccount).
9. Trong danh sách thả xuống **Hành động**, hãy chọn **Xem tài khoản**.
10. Trong thuộc tính tài khoản, hãy chọn hộp kiểm **Hiển thị mật khẩu ban đầu**.
11. Sao chép mật khẩu dùng một lần để đăng nhập bằng tài khoản dịch vụ.

Cách tìm mật khẩu dùng một lần trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Managed devices**.
2. Nhấn vào tên của máy tính mà bạn muốn xem danh sách tài khoản Authentication Agent. Việc này sẽ mở ra thuộc tính máy tính.
3. Trong thuộc tính máy tính, hãy chọn thẻ **Tác vụ**.
4. Trong danh sách tác vụ, hãy chọn **Quản lý tài khoản Authentication Agent**.
5. Trong phần thuộc tính tác vụ, hãy chọn thẻ **Application settings**.
6. Trong danh sách tài khoản, hãy chọn tài khoản dịch vụ Authentication Agent (ví dụ: WIN10-USER\ServiceAccount).
7. Trong thuộc tính tài khoản, hãy chọn hộp kiểm **Hiển thị mật khẩu ban đầu**.
8. Sao chép mật khẩu dùng một lần để đăng nhập bằng tài khoản dịch vụ.

Kaspersky Endpoint Security tự động cập nhật mật khẩu mỗi khi người dùng xác thực bằng tài khoản dịch vụ. Sau khi xác thực bằng tác nhân, bạn phải nhập mật khẩu tài khoản Windows. Khi đăng nhập bằng tài khoản dịch vụ, bạn không thể sử dụng công nghệ SSO.

Cập nhật hệ điều hành

Có một số lưu ý đặc biệt khi cập nhật hệ điều hành của máy tính được bảo vệ bằng chế độ Mã hóa toàn bộ ổ đĩa (FDE). Hãy cập nhật hệ điều hành như sau: trước tiên, cập nhật HĐH trên một máy tính, sau đó cập nhật HĐH trên số lượng nhỏ máy tính, sau đó cập nhật HĐH trên tất cả các máy tính của mạng.

Nếu bạn đang sử dụng công nghệ Kaspersky Disk Encryption, Authentication Agent sẽ được nạp trước khi hệ điều hành được khởi động. Khi sử dụng Authentication Agent, người dùng có thể đăng nhập vào hệ thống và nhận quyền truy cập vào các ổ đĩa được mã hóa. Sau đó, hệ điều hành bắt đầu nạp.

Nếu bạn tiến hành cập nhật hệ điều hành trên máy tính được bảo vệ bằng công nghệ Kaspersky Disk Encryption, Trình hướng dẫn cập nhật HĐH sẽ gỡ bỏ Authentication Agent. Kết quả là máy tính có thể bị khóa do chương trình nạp HĐH sẽ không thể truy cập vào ổ đĩa được mã hóa.

Để biết chi tiết về việc cập nhật hệ điều hành một cách an toàn, vui lòng tham khảo [Cơ sở kiến thức Hỗ trợ kỹ thuật](#).

Tự động cập nhật hệ điều hành sẽ khả dụng trong các điều kiện sau:

1. Hệ điều hành được cập nhật thông qua WSUS (Windows Server Update Services).
2. Máy tính được cài đặt phiên bản Windows 10 1607 (RS1) hoặc cao hơn.
3. Máy tính được cài đặt Kaspersky Endpoint Security version 11.2.0 hoặc mới hơn.

Nếu đáp ứng tất cả các điều kiện này, bạn có thể cập nhật hệ điều hành theo cách thông thường.

Nếu bạn đang sử dụng công nghệ Kaspersky Disk Encryption (FDE) và Kaspersky Endpoint Security cho Windows phiên bản 11.1.0 hoặc 11.1.1 được cài đặt trên máy tính, bạn không cần phải giải mã ổ đĩa cứng để cập nhật Windows 10.

Để cập nhật hệ điều hành, bạn cần làm như sau:

1. Trước khi cập nhật hệ thống, hãy sao chép các trình điều khiển có tên cm_km.inf, cm_km.sys, klfde.cat, klfde.inf, klfde.sys, klfdefsf.cat, klfdefsf.inf và klfdefsf.sys vào một thư mục cục bộ. Ví dụ:
C:\fde_drivers.
2. Chạy cài đặt cập nhật hệ thống bằng công tắc `/ReflectDrivers` và chỉ định thư mục chứa trình điều khiển đã lưu:

```
setup.exe /ReflectDrivers C:\fde_drivers
```

Nếu bạn đang sử dụng công nghệ BitLocker Drive Encryption, bạn không cần giải mã các ổ đĩa cứng để cập nhật Windows 10. Để biết thêm chi tiết về công nghệ BitLocker, vui lòng truy cập [website Microsoft](#).

Loại trừ lỗi của bản cập nhật chức năng mã hóa

Tính năng Mã hóa toàn bộ ổ đĩa được cập nhật khi phiên bản trước đây của ứng dụng được nâng cấp lên Kaspersky Endpoint Security cho Windows 11.9.0.

Khi bắt đầu cập nhật cho chức năng Mã hóa toàn bộ ổ đĩa, các lỗi sau đây có thể xảy ra:

- Không thể khởi chạy cập nhật.

- Thiết bị không tương thích với Authentication Agent.

Để loại trừ các lỗi xảy ra khi bạn bắt đầu tiến trình cập nhật cho chức năng Mã hóa toàn bộ ổ đĩa trong phiên bản mới của ứng dụng:

1. [Giải mã các ổ cứng](#).
2. [Mã hóa các ổ cứng](#) một lần nữa.

Trong quá trình cập nhật chức năng Mã hóa toàn bộ ổ đĩa, các lỗi sau đây có thể xảy ra:

- Không thể hoàn tất cập nhật.
- Quá trình nâng cấp Mã hóa toàn bộ ổ đĩa bị hoàn tác với một lỗi.

Để loại trừ các lỗi xảy ra trong quá trình cập nhật chức năng Mã hóa toàn bộ ổ đĩa,

[khôi phục quyền truy cập đến các thiết bị được mã hóa sử dụng Tiện ích khôi phục](#).

Chọn cấp độ truy 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.

Để chọn mức độ truy 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 mức độ truy vết trong cửa sổ thiết lập của Authentication Agent:
 - **Disable debug logging (default)**. Nếu chọn tùy chọn này, ứng dụng sẽ không ghi lại thông tin về các sự kiện Authentication Agent trong tập tin dấu vết.
 - **Enable debug logging**. 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.
 - **Enable verbose logging**. 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 **Enable debug logging**. Một cấp độ chi tiết cao có thể làm chậm việc khởi động của Authentication Agent và hệ điều hành.

- **Enable debug logging and select serial port**. 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.

- **Enable verbose debug logging and select serial port.** 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 **Enable debug logging and select serial port**. 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 toàn bộ ổ đĩa.

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, bạn có thể gửi thủ công tập tin dấu vết Authentication Agent đến Kaspersky để phân tích.

Chỉnh sửa văn bản trợ giúp 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 (xem bên dưới).

Để sửa thông điệp trợ giúp của Authentication Agent:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Thiết lập mã hóa chung**.
6. Trong mục **Mẫu**, hãy chọn nút **Trợ giúp**.
7. Trong cửa sổ mở ra, hãy thực hiện như 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 **Phục hồi 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.
8. Sửa thông điệp trợ giúp.

Nếu bạn muốn khôi phục văn bản gốc, nhấn nút **Theo mặc định**.

Bạn có thể nhập văn bản trợ giúp chứa 16 dòng hoặc ngắn hơn. Độ dài tối đa của một dòng là 64 ký tự.

9. Lưu các thay đổi của bạn.

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.

Xóa các đối tượng và dữ liệu còn lại sau khi kiểm tra hoạt động 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 các cách sau:

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

nhập lệnh `avp pbatestreset` vào dòng lệnh.

Quản lý BitLocker

BitLocker là một công nghệ mã hóa được tích hợp trong các hệ điều hành Windows. Kaspersky Endpoint Security cho phép bạn kiểm soát và quản lý BitLocker bằng Kaspersky Security Center. BitLocker mã hóa các phân vùng luận lý. Không thể sử dụng BitLocker để mã hóa các ổ đĩa di động. Để biết thêm chi tiết về BitLocker, hãy tham khảo [tài liệu của Microsoft](#).

BitLocker cung cấp ổ lưu trữ an toàn các khóa truy cập bằng mô-đun nền tảng được tin tưởng. *Mô-đun Nền tảng Tin tưởng (TPM)* là một vi mạch được phát triển để cung cấp các chức năng cơ bản liên quan đến bảo mật (ví dụ: để lưu trữ khóa mã hóa). Mô-đun nền tảng được tin tưởng thường được cài đặt trên bảng mạch chủ máy tính và tương tác với tất cả các thành phần hệ thống khác thông qua bus phần cứng. Sử dụng TPM là cách an toàn nhất để lưu trữ khóa truy cập BitLocker, vì TPM cung cấp xác minh tính toàn vẹn của hệ thống trước khi khởi động. Bạn vẫn có thể mã hóa ổ đĩa trên máy tính mà không cần có TPM. Trong trường hợp này, khóa truy cập sẽ được mã hóa bằng mật khẩu. BitLocker sử dụng các phương thức xác thực sau:

- TPM.
- TPM và mã PIN.
- Mật khẩu.

Sau khi mã hóa ổ đĩa, BitLocker sẽ tạo khóa chủ. Kaspersky Endpoint Security sẽ gửi khóa chủ đến Kaspersky Security Center để bạn có thể [khôi phục quyền truy cập vào ổ đĩa](#), ví dụ như nếu người dùng quên mật khẩu.

Nếu người dùng mã hóa ổ đĩa bằng BitLocker, Kaspersky Endpoint Security sẽ gửi [thông tin về mã hóa ổ đĩa đến Kaspersky Security Center](#). Tuy nhiên, Kaspersky Endpoint Security sẽ không gửi khóa chủ tới Kaspersky Security Center, do đó sẽ không thể khôi phục quyền truy cập vào đĩa bằng Kaspersky Security Center. Để BitLocker hoạt động chính xác với Kaspersky Security Center, [hãy giải mã ổ đĩa](#) và [mã hóa lại ổ đĩa](#) bằng một chính sách. Bạn có thể giải mã ổ đĩa một cách cục bộ hoặc sử dụng một chính sách.

Sau khi mã hóa ổ cứng hệ thống, người dùng cần thực hiện xác thực BitLocker để khởi động hệ điều hành. Sau quy trình xác thực, BitLocker sẽ cho phép người dùng đăng nhập. BitLocker không hỗ trợ công nghệ đăng nhập một lần (SSO).

Nếu bạn đang sử dụng các chính sách nhóm của Windows, hãy tắt quản lý BitLocker trong thiết lập chính sách. Thiết lập chính sách của Windows có thể xung đột với thiết lập chính sách của Kaspersky Endpoint Security. Lỗi có thể xảy ra khi mã hóa một ổ đĩa.

Khởi chạy BitLocker Drive Encryption

Trước khi bắt đầu mã hóa toàn bộ ổ đĩa, bạn nên đảm bảo rằng máy tính đang không bị nhiễm virus. Để làm điều này, hãy khởi chạy tác vụ Quét toàn bộ hoặc Quét khu vực quan trọng. Việc mã hóa toàn bộ ổ đĩa của một máy tính bị nhiễm rootkit có thể khiến máy ngừng hoạt động.

Để sử dụng BitLocker Drive Encryption trên các máy tính chạy hệ điều hành Windows cho máy chủ, bạn có thể cần phải cài đặt thành phần BitLocker Drive Encryption. Cài đặt thành phần bằng các công cụ hệ điều hành (Trình hướng dẫn Bổ sung vai trò và thành phần). Để biết thêm thông tin về việc cài đặt BitLocker Drive Encryption, hãy tham khảo [tài liệu của Microsoft](#).

Cách chạy BitLocker Drive Encryption thông qua Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Mã hóa toàn bộ ổ đĩa**.
6. Trong danh sách thả xuống **Công nghệ mã hóa**, chọn **BitLocker Drive Encryption**.
7. Trong danh sách thả xuống **Chế độ mã hóa**, hãy chọn mục **Mã hóa tất cả ổ đĩa cứng**.

Nếu máy tính có cài đặt nhiều hệ điều hành, sau khi mã hóa, bạn sẽ chỉ có thể nạp hệ điều hành đã thực hiện việc mã hóa.

8. Cấu hình tùy chọn BitLocker Drive Encryption nâng cao (xem bảng bên dưới).
9. Lưu các thay đổi của bạn.

Cách chạy BitLocker Drive Encryption thông qua Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Mã hóa dữ liệu** → **Mã hóa toàn bộ ổ đĩa**.
5. Trong mục **Quản lý mã hóa**, hãy chọn **BitLocker Drive Encryption**.
6. Nhấn vào liên kết **BitLocker Drive Encryption**.
Thao tác này sẽ mở cửa sổ thiết lập BitLocker Drive Encryption.
7. Trong danh sách thả xuống **Chế độ mã hóa**, chọn mục **Mã hóa tất cả ổ đĩa cứng**.

Nếu máy tính có cài đặt nhiều hệ điều hành, sau khi mã hóa, bạn sẽ chỉ có thể nạp hệ điều hành đã thực hiện việc mã hóa.

8. Cấu hình tùy chọn BitLocker Drive Encryption nâng cao (xem bảng bên dưới).
9. Lưu các thay đổi của bạn.

Bạn có thể sử dụng công cụ Giám sát mã hóa để kiểm soát quá trình mã hóa hoặc giải mã ổ đĩa trên máy tính của người dùng. Bạn có thể chạy công cụ Giám sát mã hóa từ [cửa sổ chính của ứng dụng](#).

Sau khi chính sách được áp dụng, ứng dụng sẽ hiển thị các truy vấn sau, tùy thuộc vào thiết lập xác thực:

- Chỉ TPM. Không cần người dùng nhập vào. Ổ đĩa sẽ được mã hóa khi máy tính khởi động lại.
- TPM + PIN / Mật khẩu. Nếu một mô-đun TPM khả dụng, một cửa sổ yêu cầu nhập mã PIN sẽ xuất hiện. Nếu một mô-đun TPM không khả dụng, bạn sẽ thấy một cửa sổ nhắc mật khẩu để xác thực tiền khởi động.
- Chỉ mật khẩu. Bạn sẽ thấy một cửa sổ yêu cầu mật khẩu để xác thực trước khi khởi động.

Nếu chế độ tương thích tiêu chuẩn Xử lý thông tin liên bang được bật cho hệ điều hành máy tính, thì trong Windows 8 và các hệ điều hành cũ hơn, một yêu cầu kết nối thiết bị lưu trữ sẽ được hiển thị để lưu tập tin khóa phục hồi. Bạn có thể lưu nhiều tập tin khóa phục hồi trên một thiết bị lưu trữ duy nhất.

Sau khi đặt mật khẩu hoặc mã PIN, BitLocker sẽ yêu cầu bạn khởi động lại máy tính để hoàn thành quá trình mã hóa. Tiếp theo, người dùng cần thực hiện thủ tục xác thực của BitLocker. Sau thủ tục xác thực, người dùng phải đăng nhập vào hệ thống. Sau khi hệ điều hành được nạp, BitLocker sẽ hoàn thành quá trình mã hóa.

Nếu không có quyền truy cập các khóa mã hóa, người dùng có thể [yêu cầu quản trị viên mạng cục bộ cung cấp một khóa phục hồi](#) (nếu trước đó khóa phục hồi đã không được lưu lên thiết bị lưu trữ hoặc đã bị mất).

Tham số	Mô tả
<p>Cần nhập liệu bàn phím trong quá trình tiền khởi động để bật xác thực BitLocker trên máy tính bảng</p>	<p>Hộp kiểm này bật / tắt quá trình xác thực đòi hỏi nhập liệu trong một môi trường tiền khởi động, kể cả khi nền tảng này không có khả năng nhập liệu trong môi trường tiền khởi động (ví dụ, máy tính bảng có bàn phím cảm ứng).</p> <div data-bbox="470 331 1493 488" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Màn hình cảm ứng của máy tính bảng không khả dụng trong môi trường tiền khởi động. Để hoàn tất xác thực BitLocker trên máy tính bảng, người dùng phải kết nối một bàn phím USB.</p> </div> <p>Nếu hộp kiểm này được chọn, việc sử dụng quá trình xác thực đòi hỏi nhập liệu tiền khởi động sẽ được cho phép. Bạn chỉ nên sử dụng thiết lập này cho các thiết bị có công cụ nhập liệu thay thế trong một môi trường tiền khởi động, ví dụ như bàn phím USB ngoài bàn phím cảm ứng.</p> <p>Nếu hộp kiểm bị xóa thì BitLocker Drive Encryption không khả dụng trên máy tính bảng.</p>
<p>Sử dụng mã hóa phần cứng (Windows 8 và các phiên bản mới hơn)</p>	<p>Nếu hộp kiểm này được chọn, ứng dụng sẽ áp dụng mã hóa phần cứng. Việc này cho phép bạn tăng tốc độ mã hóa và sử dụng ít tài nguyên máy tính hơn.</p>
<p>Chỉ mã hóa dung lượng ổ đĩa được sử dụng (Windows 8 và các phiên bản mới hơn)</p>	<p>Hộp kiểm này bật / tắt tùy chọn chỉ giới hạn khu vực mã hóa đến các phần ổ cứng đang được sử dụng. Giới hạn này sẽ giúp bạn giảm thời gian mã hóa.</p> <div data-bbox="470 1093 1493 1283" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Việc bật hoặc tắt tính năng Chỉ mã hóa dung lượng ổ đĩa được sử dụng (Windows 8 và các phiên bản mới hơn) sau khi bắt đầu mã hóa sẽ không sửa đổi thiết lập này cho đến khi các ổ cứng được giải mã. Bạn phải chọn hoặc xóa hộp kiểm trước khi bắt đầu mã hóa.</p> </div> <p>Nếu hộp kiểm này được chọn, chỉ các phần của ổ cứng có chứa các tập tin mới được mã hóa. Kaspersky Endpoint Security sẽ tự động mã hóa dữ liệu mới khi chúng được bổ sung.</p> <p>Nếu hộp kiểm này bị xóa, toàn bộ ổ cứng sẽ được mã hóa, bao gồm các phần sót lại của những tập tin đã được sửa đổi hoặc bị xóa trước đó.</p> <div data-bbox="470 1552 1493 1783" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Tùy chọn này được khuyến nghị cho các ổ cứng mới có dữ liệu chưa được sửa đổi hoặc bị xóa. Nếu bạn đang áp dụng mã hóa trên một ổ cứng đang được sử dụng, bạn nên mã hóa toàn bộ ổ cứng. Điều này sẽ đảm bảo toàn bộ dữ liệu được bảo vệ, kể cả những dữ liệu đã bị xóa và có khả năng được phục hồi.</p> </div> <p>Hộp kiểm này được xóa ở chế độ mặc định.</p>
<p>Thiết lập xác thực</p>	<p>Sử dụng mật khẩu (Windows 8 và các phiên bản mới hơn)</p> <p>Nếu tùy chọn này được sử dụng, Kaspersky Endpoint Security sẽ nhắc người dùng nhập mật khẩu khi người dùng cố gắng truy cập một ổ đĩa được mã hóa.</p> <p>Tùy chọn này có thể được chọn khi một Mô-đun Nền tảng Tin tưởng (TPM) không được sử dụng.</p> <p>Sử dụng Mô-đun Nền tảng Tin tưởng (TPM)</p>

Nếu tùy chọn này được chọn, BitLocker sẽ sử dụng một Mô-đun Nền tảng Tin tưởng (TPM).

Mô-đun Nền tảng Tin tưởng (TPM) là một vi mạch được phát triển để cung cấp các chức năng cơ bản liên quan đến bảo mật (ví dụ: để lưu trữ khóa mã hóa). Một Mô-đun Nền tảng Tin tưởng 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.

Đối với các máy tính chạy Windows 7 hoặc Windows Server 2008 R2, chỉ có tính năng mã hóa bằng mô-đun TPM là khả dụng. Nếu một mô-đun TPM không được cài đặt thì không thể mã hóa bằng BitLocker. Việc sử dụng mật khẩu trên các máy tính này không được hỗ trợ.

Một thiết bị được trang bị Mô-đun Nền tảng Tin tưởng có thể tạo ra các khóa mã hóa chỉ có thể được giải mã với thiết bị đó. Một Mô-đun Nền tảng Tin tưởng sẽ mã hóa các khóa mã hóa với khóa lưu trữ root của nó. Khóa lưu trữ root được lưu trong Mô-đun Nền tảng Tin tưởng. Điều này tạo nên một cấp độ bảo vệ bổ sung chống lại các nỗ lực hack khóa mã hóa.

Hành động này được chọn theo mặc định.

Bạn có thể đặt một lớp bảo vệ bổ sung để truy cập khóa mã hóa và mã hóa khóa đó bằng một mật khẩu hoặc mã PIN:

- **Use PIN for TPM.** Nếu hộp kiểm này được chọn, người dùng có thể sử dụng một mã PIN để lấy quyền truy cập một khóa mã hóa được lưu trữ trong Mô-đun Nền tảng Tin tưởng (TPM). Nếu hộp kiểm này bị xóa, người dùng bị cấm sử dụng mã PIN. Để truy cập khóa mã hóa, người dùng phải nhập mật khẩu. Bạn có thể cho phép người dùng sử dụng mã PIN cải tiến. *Mã PIN cải tiến* cho phép sử dụng các ký tự khác ngoài ký tự số: chữ cái Latinh viết hoa và viết thường, ký tự đặc biệt và dấu cách.
- **Sử dụng Mô-đun Nền tảng Tin tưởng (TPM); nếu không khả dụng thì sử dụng mật khẩu.** Nếu hộp kiểm này được chọn, người dùng có thể sử dụng một mật khẩu để nhận quyền truy cập đến các khóa mã hóa khi một Mô-đun Nền tảng Tin tưởng (TPM) không khả dụng.

Nếu hộp kiểm bị xóa và TPM không khả dụng, tác vụ mã hóa toàn bộ đĩa sẽ không bắt đầu.

Giải mã ổ cứng được bảo vệ bằng BitLocker

Người dùng có thể giải mã một đĩa bằng hệ điều hành (chức năng *Tắt BitLocker*). Sau đó, Kaspersky Endpoint Security sẽ nhắc người dùng mã hóa lại ổ đĩa. Kaspersky Endpoint Security sẽ nhắc mã hóa đĩa trừ khi bạn bật giải mã đĩa trong chính sách.

[Cách giải mã ổ cứng được bảo vệ bằng BitLocker thông qua Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Mã hóa toàn bộ ổ đĩa**.
6. Trong danh sách thả xuống **Công nghệ mã hóa**, chọn **BitLocker Drive Encryption**.
7. Trong danh sách thả xuống **Chế độ mã hóa**, hãy chọn mục **Giải mã tất cả đĩa cứng**.
8. Lưu các thay đổi của bạn.

Cách giải mã ổ cứng được mã hóa bằng BitLocker thông qua Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Mã hóa dữ liệu** → **Mã hóa toàn bộ ổ đĩa**.
5. Chọn công nghệ **BitLocker Drive Encryption** và điều hướng theo liên kết để cấu hình thiết lập.
Thiết lập mã hóa sẽ mở ra.
6. Trong danh sách thả xuống **Chế độ mã hóa**, hãy chọn mục **Giải mã tất cả đĩa cứng**.
7. Nhấn **OK**.

Bạn có thể sử dụng công cụ Giám sát mã hóa để kiểm soát quá trình mã hóa hoặc giải mã ổ đĩa trên máy tính của người dùng. Bạn có thể chạy công cụ Giám sát mã hóa từ [cửa sổ chính của ứng dụng](#).

Khôi phục quyền truy cập ổ đĩa được bảo vệ bằng BitLocker

Nếu người dùng quên mật khẩu cần để truy cập ổ đĩa cứng được mã hóa bằng BitLocker, bạn cần bắt đầu quy trình khôi phục (Yêu cầu-Phản hồi).

Nếu hệ điều hành của máy tính bật chế độ tương thích với Tiêu chuẩn Xử lý thông tin liên bang (FIPS) thì tập tin khóa phục hồi của hệ điều hành Windows 8 và cũ hơn được lưu vào ổ đĩa di động trước khi mã hóa. Để phục hồi quyền truy cập ổ đĩa đó, hãy cắm ổ đĩa di động và làm theo hướng dẫn trên màn hình.

Quá trình khôi phục quyền truy cập một ổ đĩa được mã hóa bằng BitLocker bao gồm các bước sau:

1. Người dùng thông báo ID khóa khôi phục cho quản trị viên (xem hình bên dưới).
2. Quản trị viên xác minh ID khóa khôi phục trong thuộc tính máy tính trong Kaspersky Security Center. ID mà người dùng cung cấp phải khớp với ID được hiển thị trong thuộc tính máy tính.
3. Nếu ID khóa khôi phục khớp, quản trị viên sẽ cung cấp khóa khôi phục hoặc gửi tập tin khóa khôi phục cho người dùng.

Tập tin khóa khôi phục được sử dụng cho các máy tính chạy các hệ điều hành sau:

- Windows 7;
- Windows 8;
- Windows Server 2008;
- Windows Server 2011;
- Windows Server 2012.

Đối với tất cả các hệ điều hành khác, khóa khôi phục sẽ được sử dụng.

4. Người dùng nhập khóa khôi phục và nhận quyền truy cập vào ổ đĩa cứng.



Khôi phục quyền truy cập vào ổ đĩa cứng được mã hóa bằng BitLocker

Khôi phục quyền truy cập vào ổ đĩa hệ thống

Để bắt đầu quy trình khôi phục, người dùng cần nhấn phím **Esc** ở giai đoạn xác thực tiền khởi động.

[Cách xem khóa khôi phục cho ổ đĩa hệ thống được mã hóa bằng BitLocker trong Bảng điều khiển quản trị \(MMC\)](#)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Devices**.
4. Trên thẻ **Devices**, hãy chọn máy tính của người dùng yêu cầu truy cập vào dữ liệu được mã hóa và nhấn chuột phải để mở menu ngữ cảnh.
5. Trong menu ngữ cảnh, chọn **Cấp quyền truy cập trong chế độ ngoại tuyến**.
6. Trong cửa sổ mở ra, hãy 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.

Kết quả là bạn sẽ có quyền truy cập vào khóa khôi phục hoặc tập tin khóa khôi phục, là thông tin cần được chuyển cho người dùng.

[Cách xem khóa khôi phục cho ổ đĩa hệ thống được mã hóa bằng BitLocker trong Bảng điều khiển web và Bảng điều khiển đám mây](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Managed devices**.
2. Chọn hộp kiểm cạnh tên của máy tính có ổ đĩa mà bạn muốn khôi phục quyền truy cập.
3. Nhấn nút **Grant access to the device in offline mode**.
4. Trong cửa sổ mở ra, hãy chọn mục **BitLocker**.
5. Xác minh ID khóa khôi phục. ID do người dùng cung cấp phải khớp với ID được hiển thị trong phần thiết lập của máy tính.

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.

6. Nhấn nút **Receive key**.

Kết quả là bạn sẽ có quyền truy cập vào khóa khôi phục hoặc tập tin khóa khôi phục, là thông tin cần được chuyển cho người dùng.

Sau khi hệ điều hành được nạp, Kaspersky Endpoint Security sẽ nhắc người dùng thay đổi mật khẩu hoặc mã PIN. Sau khi bạn đặt mật khẩu hoặc mã PIN mới, BitLocker sẽ tạo một khóa chính mới và gửi khóa đến Kaspersky Security Center. Kết quả là khóa phục hồi và tập tin khóa phục hồi sẽ được cập nhật. Nếu người dùng không thay đổi mật khẩu, bạn có thể sử dụng khóa khôi phục cũ vào lần tiếp theo khi hệ điều hành nạp.

Các máy tính chạy Windows 7 không cho phép thay đổi mật khẩu hoặc mã PIN. Sau khi khóa phục hồi được nhập và hệ điều hành được nạp, Kaspersky Endpoint Security sẽ không nhắc người dùng thay đổi mật khẩu hoặc mã PIN. Do đó, bạn không thể đặt mật khẩu mới hoặc mã PIN. Sự cố này bắt nguồn từ các đặc điểm riêng của hệ điều hành. Để tiếp tục, bạn cần mã hóa lại ổ đĩa cứng.

Khôi phục quyền truy cập vào ổ đĩa không thuộc hệ thống

Để bắt đầu quy trình khôi phục, người dùng cần nhấn vào liên kết **Forgot your password** trong cửa sổ cung cấp quyền truy cập vào ổ đĩa. Sau khi có quyền truy cập vào ổ đĩa được mã hóa, người dùng có thể kích hoạt tự động mở khóa ổ đĩa trong khi xác thực Windows trong thiết lập của BitLocker.

[Cách xem khóa khôi phục cho ổ đĩa không thuộc hệ thống được mã hóa bằng BitLocker trong Bảng điều khiển quản trị \(MMC\)](#)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây Bảng điều khiển quản trị, chọn thư mục **Bổ sung** → **Data encryption and protection** → **Encrypted drives**.
3. Trong không gian làm việc, hãy chọn thiết bị được mã hóa mà bạn muốn tạo tập tin khóa truy cập, sau đó trong menu ngữ cảnh của thiết bị, hãy nhấn vào **Nhận quyền truy cập đến thiết bị trong Kaspersky Endpoint Security cho Windows**.
4. 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.

5. Gửi đến người dùng khóa được ghi trong trường **Khóa phục hồi**.

[Cách xem khóa khôi phục cho ổ đĩa không phải của hệ thống được mã hóa bằng BitLocker trong Bảng điều khiển web và Bảng điều khiển đám mây](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Hoạt động** → **Data encryption and protection** → **Encrypted drives**.

2. Chọn hộp kiểm cạnh tên của máy tính có ổ đĩa mà bạn muốn khôi phục quyền truy cập.

3. Nhấn nút **Grant access to the device in offline mode**.

Thao tác này sẽ khởi chạy Trình hướng dẫn để cấp quyền truy cập cho một thiết bị.

4. Làm theo hướng dẫn của Trình hướng dẫn để cấp quyền truy cập cho một thiết bị:

a. Chọn tiện ích **Kaspersky Endpoint Security cho Windows**.

b. Xác minh ID khóa khôi phục. ID do người dùng cung cấp phải khớp với ID được hiển thị trong phần thiết lập của máy tính.

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.

c. Nhấn nút **Receive key**.

Kết quả là bạn sẽ có quyền truy cập vào khóa khôi phục hoặc tập tin khóa khôi phục, là thông tin cần được chuyển cho người dùng.

Tạm dừng bảo vệ BitLocker để cập nhật phần mềm

Có một số lưu ý đặc biệt khi cập nhật hệ điều hành, cài đặt gói cập nhật cho hệ điều hành hoặc cập nhật phần mềm khác khi bật tính năng bảo vệ BitLocker. Việc cài đặt các bản cập nhật có thể yêu cầu khởi động lại máy tính nhiều lần. Sau mỗi lần khởi động lại, người dùng phải hoàn tất xác thực BitLocker. Để đảm bảo các bản cập nhật được cài đặt đúng cách, bạn có thể tạm thời tắt xác thực BitLocker. Trong trường hợp này, ổ đĩa vẫn được mã hóa và người dùng có quyền truy cập dữ liệu sau khi đăng nhập vào hệ thống. Để quản lý xác thực BitLocker, bạn có thể sử dụng tác vụ *Quản lý bảo vệ bằng BitLocker*. Bạn có thể sử dụng tác vụ này để chỉ định số lần khởi động lại máy tính mà không yêu cầu xác thực BitLocker. Bằng cách này, sau khi các bản cập nhật được cài đặt và tác vụ *Quản lý bảo vệ bằng BitLocker* hoàn tất thì xác thực BitLocker sẽ tự động được bật. Bạn có thể bật xác thực BitLocker bất kỳ lúc nào.

[Cách tạm dừng bảo vệ bằng BitLocker bằng Bảng điều khiển quản trị \(MMC\)](#) 

1. Trong Bảng điều khiển quản trị, hãy vào thư mục **Administration Server** → **Tác vụ**.

Danh sách tác vụ sẽ mở.

2. Nhấn nút **New task**.

Trình hướng dẫn Tác vụ sẽ được bắt đầu. Làm theo chỉ dẫn của Trình hướng dẫn.

Bước 1. Chọn loại tác vụ

Chọn **Kaspersky Endpoint Security cho Windows (11.9.0)** → **Quản lý bảo vệ bằng BitLocker**.

Bước 2. Quản lý bảo vệ bằng BitLocker

Cấu hình xác thực BitLocker. Để tạm dừng bảo vệ bằng BitLocker, hãy chọn **Tạm thời cho phép bỏ qua xác thực BitLocker** và nhập số lần khởi động lại mà không cần xác thực BitLocker (1 đến 15 lần). Nếu cần, hãy nhập ngày và giờ hết hạn cho tác vụ. Tại thời điểm được chỉ định, tác vụ sẽ tự động bị tắt và người dùng phải hoàn tất xác thực BitLocker khi máy tính được khởi động lại.

Bước 3. Chọn các thiết bị sẽ được gán tác vụ

Chọn các máy tính sẽ được thực hiện tác vụ trên đó. Các tùy chọn sau có thể được sử dụng:

- Gán tác vụ vào một nhóm quản trị. Trong trường hợp này, tác vụ sẽ được gán cho các máy tính được bao gồm trong một nhóm quản trị đã được tạo trước đó.
- Chọn các máy tính được Máy chủ quản trị phát hiện trong mạng – *các thiết bị chưa được gán*. Các thiết bị được quy định có thể bao gồm các thiết bị trong nhóm quản trị cũng như các thiết bị chưa được gán.
- Nhập vào thủ công địa chỉ của thiết bị, hoặc nhập các địa chỉ từ một danh sách. Bạn có thể quy định tên NetBIOS, địa chỉ IP, và địa chỉ IP mạng con của các thiết bị mà bạn muốn gán tác vụ.

Bước 4. Xác định tên tác vụ

Nhập tên của tác vụ, ví dụ: *Cập nhật lên Windows 10*.

Bước 5. Hoàn tất việc tạo tác vụ

Thoát Trình hướng dẫn. Nếu cần, hãy chọn hộp kiểm **Run the task after the Wizard finishes**. Bạn có thể giám sát tiến độ của tác vụ trong thuộc tính tác vụ.

[Cách tạm dừng bảo vệ bằng BitLocker bằng Bảng điều khiển web](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.

Danh sách tác vụ sẽ mở.

2. Nhấn vào nút **Thêm**.

Trình hướng dẫn Tác vụ sẽ được bắt đầu. Làm theo chỉ dẫn của Trình hướng dẫn.

Bước 1. Cấu hình thiết lập tác vụ tổng quát

Cấu hình thiết lập của tác vụ tổng quát:

1. Trong danh sách thả xuống **Ứng dụng**, hãy chọn **Kaspersky Endpoint Security cho Windows (11.9.0)**.

2. Trong danh sách thả xuống **Loại tác vụ**, hãy chọn **Quản lý bảo vệ bằng BitLocker**.

3. Trong trường **Task name**, nhập một mô tả ngắn, ví dụ như *Cập nhật lên Windows 10*.

4. Trong phần **Select devices to which the task will be assigned**, chọn phạm vi tác vụ.

Bước 2. Quản lý bảo vệ bằng BitLocker

Cấu hình xác thực BitLocker. Để tạm dừng bảo vệ bằng BitLocker, hãy chọn **Tạm thời cho phép bỏ qua xác thực BitLocker** và nhập số lần khởi động lại mà không cần xác thực BitLocker (1 đến 15 lần). Nếu cần, hãy nhập ngày và giờ hết hạn cho tác vụ. Tại thời điểm được chỉ định, tác vụ sẽ tự động bị tắt và người dùng phải hoàn tất xác thực BitLocker khi máy tính được khởi động lại.

Bước 3. Hoàn tất việc tạo tác vụ

Thoát Trình hướng dẫn. Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ.

Để thực hiện một tác vụ, chọn hộp kiểm cạnh tác vụ đó và nhấn nút **Bắt đầu**.

Kết quả là, khi tác vụ đang chạy, sau lần khởi động lại máy tính tiếp theo, BitLocker sẽ không nhắc người dùng xác thực. Sau mỗi lần khởi động lại máy tính mà không cần xác thực BitLocker, Kaspersky Endpoint Security sẽ tạo một sự kiện tương ứng và ghi lại số lần khởi động lại còn lại. Khi đó Kaspersky Endpoint Security sẽ gửi sự kiện đến Kaspersky Security Center để quản trị viên giám sát. Bạn cũng có thể tìm hiểu số lần khởi động lại còn lại trong thuộc tính máy tính, trong bảng điều khiển Kaspersky Security Center.

Khi đạt đến số lần khởi động lại được chỉ định hoặc thời gian hết hạn của tác vụ, xác thực BitLocker sẽ tự động được bật. Để có quyền truy cập dữ liệu, người dùng phải hoàn thành xác thực BitLocker.

Trên máy tính chạy Windows 7, BitLocker không thể đếm số lần khởi động lại máy tính. Việc đếm số lần khởi động lại trên máy tính Windows 7 do Kaspersky Endpoint Security xử lý. Do đó, để tự động bật xác thực BitLocker sau mỗi lần khởi động lại, Kaspersky Endpoint Security phải được khởi động.

Để bật xác thực BitLocker trước thời hạn, hãy mở thuộc tính tác vụ *Quản lý bảo vệ bằng BitLocker* và chọn **Yêu cầu xác thực mỗi lần trước khi khởi động**.

Mã hóa mức độ tập tin trên các ổ đĩa máy tính cục bộ

Thành phần này khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows dành cho máy trạm. Thành phần này không khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows cho máy chủ.

Mã hóa tập tin có các tính năng đặc biệt sau:

- 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 hoặc 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 hoặc các thư mục được chuyển hướng.
- Kaspersky Endpoint Security sẽ không mã hóa các tập tin nếu việc sửa đổi chúng có thể gây hại cho 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% và %PROGRAMFILES(X86)%;
 - Các tập tin registry của Windows.

Danh sách loại trừ mã hóa không thể được xem hoặc sửa. Mặc dù bạn có thêm các tập tin và thư mục trong danh sách loại trừ mã hóa vào danh sách mã hóa, nhưng bạn sẽ không thể mã hóa chúng trong quá trình mã hóa tập tin.

Mã hóa các tập tin trên ổ đĩa nội bộ của máy tính

Kaspersky Endpoint Security không mã hóa các tập tin nằm trong ổ lưu trữ đám mây OneDrive hoặc trong các thư mục khác có tên là OneDrive. Kaspersky Endpoint Security cũng chặn sao chép các tập tin được mã hóa vào thư mục OneDrive nếu các tập tin đó không được thêm vào [quy tắc giải mã](#).

Để mã hóa các tập tin trên ổ đĩa nội bộ:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Mã hóa mức độ tập tin**.
6. Trong danh sách thả xuống **Chế độ mã hóa**, hãy chọn **Theo các quy tắc**.

7. 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.
- **Documents.** Các tập tin trong thư mục *Documents* tiêu chuẩn của hệ điều hành và các thư mục con.
 - **Favorites.** Các tập tin trong thư mục *Favorites* tiêu chuẩn của hệ điều hành và các thư mục con.
 - **Desktop.** Các tập tin trong thư mục *Desktop* tiêu chuẩn của hệ điều hành và các thư mục con.
 - **Các tập tin tạm.** Các tập tin tạm thời liên quan đến hoạt động của các ứng dụng được cài đặt trên máy tính. Ví dụ: các ứng dụng Microsoft Office tạo các tập tin tạm thời chứa các bản sao lưu của tài liệu.
 - **Các tập tin Outlook.** Các tập tin liên quan đến hoạt động của ứng dụng trình khách Outlook: tập tin dữ liệu (PST), tập tin dữ liệu ngoại tuyến (OST), tập tin sổ địa chỉ ngoại tuyến (OAB) và tập tin sổ địa chỉ cá nhân (PAB).
- b. Chọn đề mục **Thư mục tùy chỉnh** để thêm một đường dẫn thư mục được nhập thủ công vào quy tắc mã hóa.

Khi thêm một đường dẫn thư mục, hãy tuân thủ các quy tắc sau:

- Sử dụng một biến môi trường (ví dụ như %FOLDER%\UserFolder\). Bạn chỉ có thể sử dụng một biến môi trường một lần duy nhất và chỉ ở đầu đường dẫn.
- Không sử dụng đường dẫn tương đối.
- Không sử dụng ký tự * và ?.
- Không sử dụng đường dẫn UNC.
- Sử dụng ; hoặc , làm ký tự phân cách.

c. Chọn mục **Các tập tin theo phần mở rộng** để thêm các phần mở rộng của từng 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 nội bộ của máy tính.

d. Chọn mục **Các tập tin theo nhóm phần mở rộng** để thêm các nhóm phần mở rộng tập tin vào quy tắc mã hóa (ví dụ như *tài liệu Microsoft Office*). 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 nội bộ của máy tính.

8. Lưu các thay đổi của bạn.

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](#).

Mã hóa tập tin có các tính năng đặc biệt sau:

- Nếu cùng một tập tin được thêm vào cả quy tắc mã hóa và quy tắc giải mã, thì Kaspersky Endpoint Security sẽ thực hiện các hành động sau:
 - Nếu tập tin không được mã hóa thì Kaspersky Endpoint Security sẽ không mã hóa tập tin này.

- Nếu tập tin được mã hóa thì Kaspersky Endpoint Security sẽ giải mã tập tin này.
- Kaspersky Endpoint Security sẽ tiếp tục mã hóa các tập tin mới nếu các tập tin này đáp ứng các tiêu chí của quy tắc mã hóa. Ví dụ: khi bạn thay đổi các thuộc tính của một tập tin không được mã hóa (đường dẫn hoặc phần mở rộng), thì tập tin đó sẽ đáp ứng các tiêu chí của quy tắc mã hóa. Kaspersky Endpoint Security sẽ mã hóa tập tin này.
- 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.
- Kaspersky Endpoint Security sẽ hoãn việc mã hóa các tập tin đang mở cho đến khi chúng đã được đóng.
- Nếu bạn di chuyển một tập tin được mã hóa đến một thư mục khác trên ổ đĩa nội 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.
- Nếu bạn giải mã một tập tin và sao chép nó vào một thư mục cục bộ khác không có trong quy tắc giải mã thì một bản sao của tập tin có thể được mã hóa. Để tập tin được sao chép không bị mã hóa, hãy tạo quy tắc giải mã cho thư mục đích.

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 Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Mã hóa mức độ tập tin**.
6. Trong danh sách thả xuống **Chế độ mã hóa**, hãy chọn **Theo các quy tắc**.

Quy tắc truy cập sẽ chỉ được áp dụng khi trong chế độ **Theo các quy tắc**. Sau khi đã áp dụng quy tắc truy cập trong chế độ **Theo các quy tắc**, nếu bạn chuyển sang chế độ **Giữ nguyên**, 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.

7. Ở phần bên phải của cửa sổ, chọn thẻ **Quy tắc cho ứng dụng**.
8. 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**.
 - 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**.
 - c. Bảng này liệt kê các ứng dụng khớp với bộ lọc được áp dụng.

- d. 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.
- e. 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.
- f. 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.

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**.

- 9. 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**.
 - 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.

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. Lưu các thay đổi của bạn.

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 Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Mã hóa mức độ tập tin**.

6. Trong danh sách thả xuống **Chế độ mã hóa**, hãy chọn **Theo các quy tắc**.

Quy tắc mã hóa sẽ chỉ được áp dụng trong chế độ **Theo các quy tắc**. Sau khi đã áp dụng quy tắc mã hóa trong chế độ **Theo các quy tắc**, nếu bạn chuyển sang chế độ **Giữ nguyên**, 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.

7. Ở phần bên phải của cửa sổ, chọn thẻ **Quy tắc cho ứng dụng**.

8. 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**.

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**, hãy chọn hộp kiểm cạnh các ứng dụng có các tập tin được tạo mà bạn muốn 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.

Thông tin về quy tắc mã hóa cho các tập tin được tạo hoặc được sửa đổi bởi các ứng dụng được chọn sẽ được hiển thị trong bảng trên thẻ **Quy tắc cho ứng dụng**.

9. 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**.

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**.

Thông tin về quy tắc mã hóa cho các tập tin được tạo hoặc được sửa đổi bởi các ứng dụng được chọn sẽ được hiển thị trong bảng trên thẻ **Quy tắc cho ứng dụng**.

10. Lưu các thay đổi của bạn.

Tạo một quy tắc giải mã

Để tạo một quy tắc giải mã:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.

- Trong thư mục **Managed devices** của cây Bảng điều khiển quản trị, mở thư mục với tên của nhóm quản trị chứa máy khách liên quan.
- Trong không gian làm việc, chọn thẻ **Policies**.
- Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
- Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Mã hóa mức độ tập tin**.
- Trong danh sách thả xuống **Chế độ mã hóa**, hãy chọn **Theo các quy tắc**.
- Trên thẻ **Giải mã**, nhấn nút **Thêm**, và trong danh sách thả xuống chọn một trong các đề mục sau:
 - 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.
 - Chọn đề mục **Thư mục tùy chỉnh** để thêm một đường dẫn thư mục được nhập thủ công vào quy tắc giải mã.
 - Chọn mục **Các tập tin theo phần mở rộng** để thêm các phần mở rộng của từng 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 nội bộ của máy tính.
 - Chọn mục **Các tập tin theo nhóm phần mở rộng** để thêm các nhóm phần mở rộng tập tin vào quy tắc giải mã (ví dụ như *tài liệu Microsoft Office*). 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 nội bộ của máy tính đó.
- Lưu các thay đổi của bạn.

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 nội bộ trên máy tính

Để giải mã các tập tin trên ổ đĩa nội bộ:

- Mở Bảng điều khiển quản trị Kaspersky Security Center.
- Trong thư mục **Managed devices** của cây Bảng điều khiển quản trị, mở thư mục với tên của nhóm quản trị chứa máy khách liên quan.
- Trong không gian làm việc, chọn thẻ **Policies**.
- Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
- Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Mã hóa mức độ tập tin**.
- Ở phần bên phải của cửa sổ, chọn thẻ **Mã hóa**.
- 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**.

Các tập tin và thư mục được xóa khỏi danh sách mã hóa sẽ tự động được thêm vào danh sách giải mã.

8. [Tạo một danh sách giải mã tập tin.](#)

9. Lưu các thay đổi của bạn.

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 mã hóa

Để bảo vệ dữ liệu của bạn khi gửi các tập tin cho người dùng bên ngoài mạng doanh nghiệp, bạn có thể sử dụng các gói mã hóa. Việc chuyển các tập tin lớn trên ổ di động có thể thuận tiện nhờ các gói mã hóa, vì các trình khách email có giới hạn kích thước tập tin.

Trước khi tạo các gói mã hóa, Kaspersky Endpoint Security sẽ nhắc người dùng nhập mật khẩu. Để bảo vệ dữ liệu một cách đáng tin cậy, bạn có thể bật tính năng kiểm tra độ mạnh mật khẩu và chỉ định yêu cầu về độ mạnh của mật khẩu. Điều này sẽ ngăn người dùng sử dụng mật khẩu ngắn và đơn giản như: 1234.

[Cách bật kiểm tra độ mạnh mật khẩu khi tạo một các tập tin nén được mã hóa trong Bảng điều khiển quản trị \(MMC\)](#)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Thiết lập mã hóa chung**.
6. Trong mục **Thiết lập mật khẩu**, hãy nhấn nút **Thiết lập**.
7. Trong cửa sổ mở ra, hãy chọn thẻ **Gói mã hóa**.
8. Cấu hình cài đặt độ phức tạp của mật khẩu khi tạo các gói mã hóa.

[Cách bật kiểm tra độ mạnh mật khẩu khi tạo các tập tin nén được mã hóa mới trong Bảng điều khiển web](#)


1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Mã hóa dữ liệu** → **Mã hóa mức độ tập tin**.
5. Trong mục **Thiết lập mật khẩu gói mã hóa**, hãy cấu hình tiêu chí độ mạnh mật khẩu cần thiết khi tạo các gói được mã hóa.

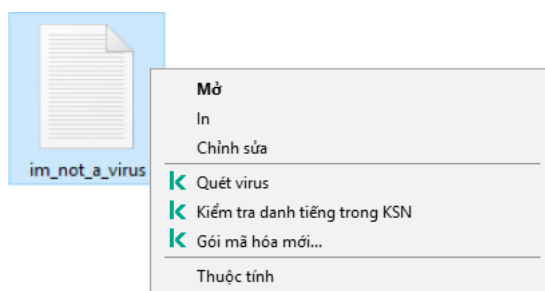
Bạn có thể tạo các gói mã hóa trên các máy tính được cài đặt Kaspersky Endpoint Security khi có tính năng Mã hóa mức độ tập tin.

Khi bổ sung một tập tin vào gói mã hóa có nội dung được lưu trữ trong ổ lưu trữ đám mây OneDrive, Kaspersky Endpoint Security sẽ tải về nội dung của tập tin này và tiến hành mã hóa.

Để tạo một gói mã hóa:

1. Trong bất kỳ trình quản lý tập tin nào, hãy chọn các tập tin hoặc thư mục mà bạn muốn thêm vào gói mã hóa. Nhấn phải chuột để mở menu ngữ cảnh.
2. Trong menu ngữ cảnh, hãy chọn **Gói mã hóa mới** (xem hình bên dưới).
3. Trong cửa sổ mở ra, hãy chọn một vị trí trên ổ đĩa di động để lưu gói mã hóa → chỉ định tên gói và nhấn vào nút **Lưu**.
4. Trong cửa sổ mở ra, hãy chỉ định và xác nhận mật khẩu.
Mật khẩu phải đáp ứng các tiêu chí độ phức tạp được chỉ định trong chính sách.
5. Nhấn nút **Tạo**.

Tiến trình tạo gói mã hóa sẽ được bắt đầu. Kaspersky Endpoint Security sẽ không nén tập tin khi nó tạo một gói mã hóa. Khi quá trình này kết thúc, gói mã hóa tự giải nén, được bảo vệ bằng mật khẩu (một tập tin thực thi có phần mở rộng là .exe - ) được tạo trong thư mục đích đã chọn.



Tạo một gói mã hóa

Để truy cập các tập tin trong gói mã hóa, hãy nhấn đúp vào tập tin đó để khởi chạy Trình hướng dẫn giải nén, sau đó nhập mật khẩu. Nếu bạn quên hoặc mất mật khẩu, bạn sẽ không thể khôi phục mật khẩu và truy cập các tập tin trong gói mã hóa. Bạn có thể tạo lại gói mã hóa đó.

Khôi phục quyền truy cập vào các tập tin được mã hóa

Khi các tập tin được mã hóa, Kaspersky Endpoint Security sẽ nhận một khóa mã hóa cần thiết 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.

Bạn có thể không truy cập được các tập tin được mã hóa 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.

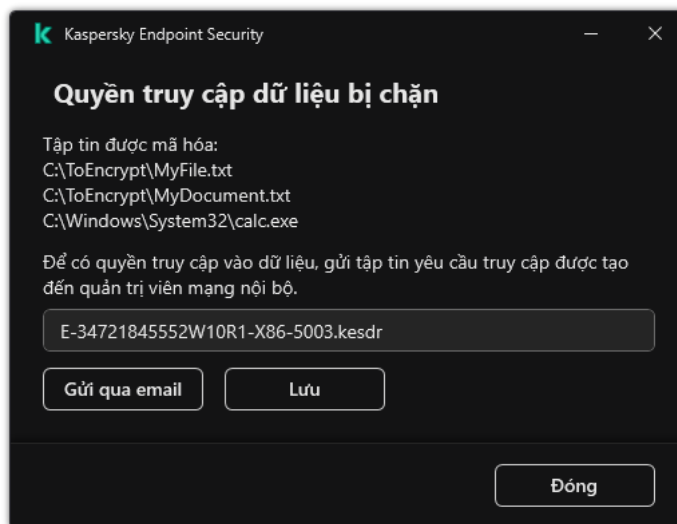
Người dùng có thể làm việc với các tập tin được mã hóa trong các trường hợp sau đây:

- 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 di động](#).

Để có quyền truy cập vào các tập tin được mã hóa, người dùng cần bắt đầu quy trình khôi phục (Yêu cầu-Phản hồi).

Quá trình khôi phục quyền truy cập vào các tập tin được mã hóa bao gồm các bước sau:

1. Người dùng gửi cho quản trị viên một tập tin yêu cầu truy cập (xem hình bên dưới).
2. Quản trị viên thêm tập tin yêu cầu truy cập vào Kaspersky Security Center, tạo tập tin khóa truy cập và gửi tập tin đó cho người dùng.
3. Người dùng thêm tập tin khóa truy cập vào Kaspersky Endpoint Security và nhận quyền truy cập vào các tập tin.



Khôi phục quyền truy cập vào các tập tin được mã hóa

Để bắt đầu quy trình khôi phục, người dùng cần cố truy cập vào một tập tin. Kết quả là Kaspersky Endpoint Security sẽ tạo một tập tin yêu cầu truy cập (tập tin có phần mở rộng là KESDC) mà người dùng cần gửi cho quản trị viên, ví dụ như gửi qua email.

Kaspersky Endpoint Security sẽ tạo một tập tin yêu cầu truy cập để truy cập vào tất cả các tập tin mã hóa được lưu trữ trên ổ đĩa của máy tính (ổ đĩa cục bộ hoặc ổ đĩa di động).

[Cách lấy tập tin khóa truy cập dữ liệu được mã hóa trong Bảng điều khiển quản trị \(MMC\)](#)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Devices**.
4. Trên thẻ **Devices**, hãy chọn máy tính của người dùng yêu cầu truy cập vào dữ liệu được mã hóa và nhấn chuột phải để mở menu ngữ cảnh.
5. Trong menu ngữ cảnh, chọn **Cấp quyền truy cập trong chế độ ngoại tuyến**.
6. Trong cửa sổ mở ra, hãy chọn thẻ **Mã hóa dữ liệu**.
7. Trên thẻ **Mã hóa dữ liệu**, hãy nhấn nút **Duyệt**.
8. Trong cửa sổ để chọn tập tin yêu cầu truy cập, hãy chỉ định đường dẫn đến tập tin nhận được từ người dùng.

Bạn sẽ thấy thông tin về yêu cầu của người dùng. Kaspersky Security Center sẽ tạo một tập tin khóa. Hãy gửi tập tin khóa truy cập dữ liệu mã hóa được tạo ra cho người dùng qua email. Hoặc lưu tập tin truy cập và sử dụng bất kỳ phương thức có sẵn nào để truyền gửi tập tin đó.

[Cách lấy tập tin khóa truy cập dữ liệu được mã hóa trong Bảng điều khiển web](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Managed devices**.
2. Chọn hộp kiểm bên cạnh tên của máy tính có dữ liệu bạn muốn khôi phục quyền truy cập.
3. Nhấn nút **Grant access to the device in offline mode**.
4. Chọn mục **Mã hóa dữ liệu**.
5. Nhấn vào nút **Select file** và chọn tập tin yêu cầu truy cập mà bạn nhận được từ người dùng (tập tin có phần mở rộng là KESDC).
Bảng điều khiển Web sẽ hiển thị thông tin về yêu cầu. Thông tin này sẽ bao gồm tên của máy tính mà người dùng đang yêu cầu quyền truy cập vào tập tin.
6. Nhấn vào nút **Save key** và chọn thư mục để lưu tập tin khóa truy cập dữ liệu được mã hóa (tập tin có phần mở rộng là KESDR).

Kết quả là bạn có thể lấy được khóa truy cập dữ liệu được mã hóa cần để truyền gửi cho người dùng.

Sau khi nhận được tập tin khóa truy cập dữ liệu được mã hóa, người dùng cần chạy tập tin đó bằng cách nhấp đúp vào nó. Kết quả là Kaspersky Endpoint Security sẽ cấp quyền truy cập vào tất cả các tập tin mã hóa được lưu trữ trên ổ đĩa. Để truy cập các tập tin được lưu trữ trên các ổ đĩa khác, bạn phải nhận được một tập tin khóa truy cập riêng biệt cho mỗi ổ đĩa.

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 khi dữ liệu được mã hóa.

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.

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 Kaspersky Security Center.

2. Trong thư mục **Managed devices** 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 **Policies**.

4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

5. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Thiết lập mã hóa chung**.

6. Trong mục **Mẫu**, hãy chọn nút **Mẫu**.

7. Trong cửa sổ mở ra, hãy thực hiện như sau:

- Nếu bạn muốn sửa mẫu thông điệp của người dùng, chọn thẻ **Thông điệp của người dùng**. Cửa sổ **Quyền truy cập dữ liệu bị chặn** sẽ 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 các tập tin được mã hóa. Nhấn vào nút **Gửi qua email** trong cửa sổ **Quyền truy cập dữ liệu bị chặn** để tự động tạo một tin nhắn 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 bạn nhấn nút **Gửi qua email** trong cửa sổ **Yêu cầu truy cập vào tập tin mã hóa** và được gửi đến người dùng sau khi người dùng được cấp quyền truy cập đến các tập tin được mã hóa.

8. Sửa mẫu thông điệp.

9. Lưu các thay đổi của bạn.

Mã hóa ổ đĩa di động

Thành phần này khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows dành cho máy trạm. Thành phần này không khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows cho máy chủ.

Kaspersky Endpoint Security hỗ trợ mã hóa các tập tin trong hệ thống tập tin FAT32 và NTFS. Nếu một ổ đĩa di động có hệ thống tập tin không tương thích được kết nối với máy tính, tác vụ mã hóa cho ổ đĩa di động này sẽ kết thúc với một lỗi và Kaspersky Endpoint Security sẽ gán trạng thái chỉ đọc cho ổ đĩa di động đó.

Để bảo vệ dữ liệu trên các ổ đĩa di động, bạn có thể sử dụng các loại mã hóa sau:

- Mã hóa toàn bộ ổ đĩa (FDE).

Mã hóa toàn bộ ổ đĩa di động, bao gồm cả hệ thống tập tin.

Không thể truy cập dữ liệu được mã hóa bên ngoài mạng doanh nghiệp. Bạn cũng không thể truy cập dữ liệu được mã hóa trong mạng doanh nghiệp nếu máy tính không được kết nối với Kaspersky Security Center (ví dụ: trên một máy tính khách).

- Mã hóa mức độ tập tin (FLE).

Chỉ mã hóa các tập tin trên ổ đĩa di động. Hệ thống tập tin được giữ nguyên.

Mã hóa các tập tin trên ổ đĩa di động cho phép truy cập dữ liệu bên ngoài mạng doanh nghiệp bằng cách sử dụng một chế độ đặc biệt gọi là [chế độ di động](#).

Trong quá trình mã hóa, Kaspersky Endpoint Security sẽ tạo một khóa chủ. Kaspersky Endpoint Security sẽ lưu khóa chủ trong các kho lưu trữ sau:

- Kaspersky Security Center.

- Máy tính của người dùng.

Khóa chủ được mã hóa bằng khóa bí mật của người dùng.

- Ổ đĩa di động.

Khóa chủ được mã hóa bằng khóa công khai của Kaspersky Security Center.

Sau khi quá trình mã hóa hoàn tất, dữ liệu trên ổ đĩa di động có thể truy cập được trong mạng doanh nghiệp như thể chúng được lưu trữ trên một ổ đĩa di động thông thường, chưa được mã.

Truy cập dữ liệu được mã hóa

Khi kết nối một ổ đĩa di động có dữ liệu được mã hóa, Kaspersky Endpoint Security sẽ thực hiện các hành động sau:

1. Kiểm tra khóa chủ trong ổ lưu trữ cục bộ trên máy tính của người dùng.

Nếu tìm thấy khóa chủ, người dùng sẽ có quyền truy cập vào dữ liệu trên ổ đĩa di động.

Nếu không tìm thấy khóa chủ, Kaspersky Endpoint Security sẽ thực hiện các hành động sau:

- a. Gửi một yêu cầu đến Kaspersky Security Center.

Sau khi nhận được yêu cầu, Kaspersky Security Center sẽ gửi một phản hồi có chứa khóa chủ.

- b. Kaspersky Endpoint Security lưu khóa chủ trong ổ lưu trữ cục bộ trên máy tính của người dùng cho các hoạt động tiếp theo với ổ đĩa di động được mã hóa.

2. Giải mã dữ liệu.

Các tính năng đặc biệt của mã hóa ổ đĩa di động

Quá trình mã hóa ổ đĩa di động có các tính năng đặc biệt sau:

- Chính sách 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 áp dụng chính sách Kaspersky Security Center đã được cấu hình cho mã hóa / giải mã các 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 chỉ cho phép đọc, được lưu trữ trên ổ đĩa di động.

- 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

Bắt đầu mã hóa ổ đĩa di động

Bạn có thể sử dụng một chính sách để giải mã một ổ đĩa di động. Một chính sách với thiết lập được xác định để mã hóa ổ đĩa di động sẽ được tạo cho một nhóm quản trị 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.

Kaspersky Endpoint Security hỗ trợ mã hóa trong các hệ thống tập tin FAT32 và NTFS. Nếu một ổ đĩa di động có hệ thống tập tin không tương thích được kết nối với máy tính, mã hóa ổ đĩa di động này sẽ kết thúc với một lỗi và Kaspersky Endpoint Security sẽ gán quyền truy cập chỉ đọc cho ổ đĩa di động đó.

Để mã hóa ổ đĩa di động:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Mã hóa ổ đĩa di động**.
6. Trong danh sách thả xuống của **Chế độ mã hóa**, hãy chọn hành động mặc định bạn muốn Kaspersky Endpoint Security thực hiện đối với ổ đĩa di động:
 - **Mã hóa toàn bộ ổ đĩa di động (FDE)**. Kaspersky Endpoint Security mã hóa nội dung của ổ đĩa di động lần lượt theo từng sector. Kết quả là ứng dụng không chỉ mã hóa các tập tin được lưu trữ trên ổ đĩa di động mà còn mã hóa các hệ thống tập tin của ổ đĩa, bao gồm tên tập tin và cấu trúc thư mục trên ổ đĩa di động.
 - **Mã hóa tất cả các tập tin (FLE)**. Kaspersky Endpoint Security mã hóa tất cả các tập tin được lưu trữ trên các ổ đĩa di động. 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.
 - **Chỉ mã hóa các tập tin mới (FLE)**. Kaspersky Endpoint Security sẽ chỉ mã hóa các tập tin đã được thêm vào ổ đĩa di động hoặc được lưu trữ trên các ổ đĩa di động và đã được sửa đổi sau lần áp dụng chính sách Kaspersky Security Center gần nhất.

Kaspersky Endpoint Security sẽ không mã hóa ổ đĩa di động đã được mã hóa từ trước.

7. Nếu bạn muốn [sử dụng chế độ di động](#) cho để mã hóa ổ đĩa di động, hãy chọn hộp kiểm **Chế độ di động**.

Chế độ di động là chế độ mã hóa tập tin (FLE) trên các ổ đĩa di động, cho phép truy cập dữ liệu bên ngoài mạng công ty. Chế độ di động cũng cho phép bạn làm việc với dữ liệu được mã hóa trên các máy tính chưa cài đặt Kaspersky Endpoint Security.

8. Nếu bạn muốn mã hóa một ổ đĩa di động mới, chúng tôi khuyến cáo bạn chọn hộp kiểm **Chỉ mã hóa dung lượng ổ đĩa được sử dụng**. Nếu hộp kiểm này không được chọn, Kaspersky Endpoint Security sẽ mã hóa tất cả các tập tin, bao gồm các phần còn sót lại của các tập tin bị xóa hoặc bị sửa đổi.
9. Nếu bạn muốn cấu hình mã hóa cho từng ổ đĩa di động, [hãy xác định quy tắc mã hóa](#).
10. Nếu bạn muốn sử dụng tính năng mã hóa toàn bộ ổ đĩa di động ở chế độ ngoại tuyến, hãy chọn hộp kiểm **Cho phép mã hóa ổ đĩa di động ở chế độ ngoại tuyến**.

Chế độ mã hóa ngoại tuyến là tính năng mã hóa ổ đĩa di động (FDE) khi không có kết nối đến Kaspersky Security Center. Trong quá trình mã hóa, Kaspersky Endpoint Security chỉ lưu các khóa chủ trên máy tính của người dùng. Kaspersky Endpoint Security sẽ gửi khóa chủ đến Kaspersky Security Center trong phiên đồng bộ hóa tiếp theo.

Nếu máy tính có khóa chủ được lưu bị hỏng và dữ liệu không được gửi đến Kaspersky Security Center thì không thể truy cập được ổ đĩa di động.

Nếu hộp kiểm **Cho phép mã hóa ổ đĩa di động ở chế độ ngoại tuyến** bị xóa và không có kết nối đến Kaspersky Security Center thì không thể mã hóa ổ đĩa di động.

11. Lưu các thay đổi của bạn.

Sau khi áp dụng chính sách, khi người dùng kết nối một ổ đĩa di động hoặc nếu ổ đĩa di động đã được kết nối, Kaspersky Endpoint Security sẽ yêu cầu người dùng xác nhận thực hiện hoạt động mã hóa (xem hình bên dưới).

Ứng dụng sẽ cho phép bạn thực hiện các hành động sau:

- Nếu người dùng xác nhận yêu cầu mã hóa, Kaspersky Endpoint Security sẽ mã hóa dữ liệu.
- Nếu người dùng từ chối yêu cầu mã hóa, Kaspersky Endpoint Security sẽ giữ nguyên dữ liệu và gán quyền truy cập chỉ đọc cho ổ đĩa di động này.
- Nếu người dùng không phản hồi yêu cầu mã hóa, Kaspersky Endpoint Security sẽ giữ nguyên dữ liệu và gán quyền truy cập chỉ đọc cho ổ đĩa di động này. Ứng dụng yêu cầu xác nhận lại cho lần áp dụng chính sách tiếp theo hoặc khi ổ đĩa di động này được kết nối vào lần tiếp theo.

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. Quá trình mã hóa dữ liệu sẽ được tiếp tục khi ổ đĩa di động được kết nối với máy tính này vào lần tới.

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.



Yêu cầu mã hóa ổ đĩa di động

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 Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Mã hóa ổ đĩa di động**.
6. Nhấn nút **Thêm**, và trong danh sách thả xuống chọn một trong các 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 được tin tưởng của chính sách này**.
 - 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**.
7. 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.
8. Chọn hộp kiểm **Chế độ di 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 di động.
Chế độ di 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.

9. 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.

10. 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 bằng một quy tắc mới, hãy chọn **Làm mới**.

11. Lưu các thay đổi của bạn.

Các quy tắc mã hóa được thêm dành cho các ổ đĩa di động sẽ được áp dụng cho các ổ đĩa di động được kết nối với bất kỳ máy tính nào trong tổ chức.

Xuất và nhập danh sách các quy tắc mã hóa cho ổ đĩa di động

Bạn có thể xuất danh sách các quy tắc mã hóa ổ đĩa di động vào một tập tin XML. Sau đó, bạn có thể sửa đổi tập tin, ví dụ như thêm một số lượng lớn các quy tắc cho cùng loại ổ đĩa di động. Bạn cũng có thể sử dụng chức năng xuất/nhập để sao lưu danh sách các quy tắc hoặc để chuyển quy tắc sang máy chủ khác.

[**Cách xuất và nhập danh sách quy tắc mã hóa ổ đĩa di động trong Bảng điều khiển quản trị \(MMC\)**](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Mã hóa ổ đĩa di động**.
6. Để xuất danh sách các quy tắc mã hóa cho ổ đĩa di động:
 - a. Chọn các quy tắc mà bạn muốn xuất. Để chọn nhiều cổng, hãy sử dụng phím **CTRL** hoặc **SHIFT**. Nếu bạn không chọn quy tắc nào, Kaspersky Endpoint Security sẽ xuất tất cả các quy tắc.
 - b. Nhấn liên kết **Xuất**.
 - c. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin XML mà bạn muốn xuất danh sách các quy tắc vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
 - d. Lưu tập tin.
Kaspersky Endpoint Security sẽ xuất danh sách các quy tắc vào tập tin XML.
7. Để nhập danh sách các quy tắc mã hóa cho ổ đĩa di động:
 - a. Nhấn liên kết **Nhập**.
Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách các quy tắc.
 - b. Mở tập tin.
Nếu máy tính đã có danh sách các quy tắc, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.
8. Lưu các thay đổi của bạn.

[Cách xuất và nhập danh sách quy tắc mã hóa ổ đĩa di động trong Bảng điều khiển web](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Mã hóa dữ liệu** → **Mã hóa ổ đĩa di động**.
5. Trong mục **Quy tắc mã hóa cho các thiết bị đã được chọn**, hãy nhấn liên kết **Quy tắc mã hóa**.
Thao tác này sẽ mở ra danh sách các quy tắc mã hóa cho ổ đĩa di động.
6. Để xuất danh sách các quy tắc mã hóa cho ổ đĩa di động:
 - a. Chọn các quy tắc mà bạn muốn xuất.
 - b. Nhấn vào **Xuất**.
 - c. Xác nhận rằng bạn chỉ muốn xuất các quy tắc đã chọn hoặc xuất toàn bộ danh sách.
 - d. Lưu tập tin.
Kaspersky Endpoint Security sẽ xuất danh sách các quy tắc vào tập tin XML trong thư mục tải xuống mặc định.
7. Để nhập danh sách quy tắc:
 - a. Nhấn liên kết **Nhập**.
Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách các quy tắc.
 - b. Mở tập tin.
Nếu máy tính đã có danh sách các quy tắc, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin XML.
8. Lưu các thay đổi của bạn.

Chế độ di động để truy cập các tập tin được mã hóa trên ổ đĩa di động

Chế độ di động là chế độ mã hóa tập tin (FLE) trên các ổ đĩa di động, cho phép truy cập dữ liệu bên ngoài mạng công ty. Chế độ di động cũng cho phép bạn làm việc với dữ liệu được mã hóa trên các máy tính chưa cài đặt Kaspersky Endpoint Security.

Chế độ di động là cách thuận tiện để sử dụng trong các trường hợp sau:

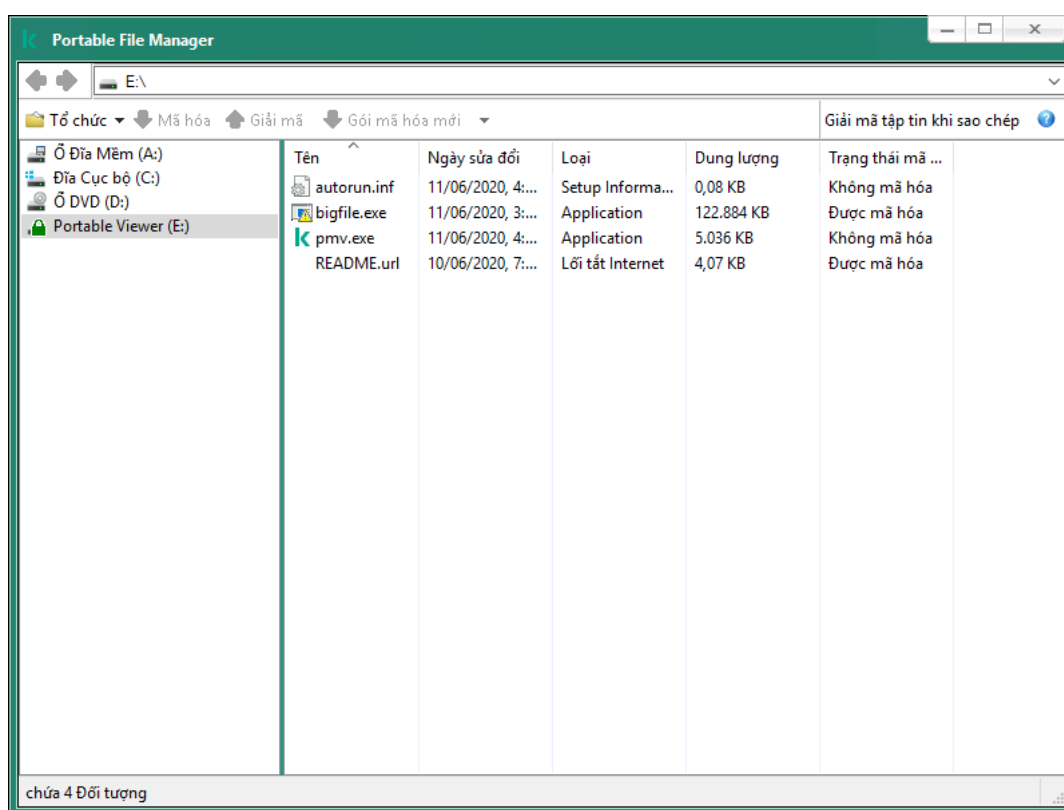
- Không có kết nối giữa máy tính và Máy chủ quản trị Kaspersky Security Center.
- Cơ sở hạ tầng đã thay đổi với sự thay đổi của Máy chủ quản trị Kaspersky Security Center.
- Kaspersky Endpoint Security không được cài đặt trên máy tính.

Trình quản lý tập tin di động

Để hoạt động ở chế độ di động, Kaspersky Endpoint Security sẽ cài đặt một mô-đun mã hóa đặc biệt có tên *Trình quản lý tập tin di động* trên một ổ đĩa di động. Trình quản lý tập tin di động cung cấp giao diện để làm việc với dữ liệu được mã hóa nếu Kaspersky Endpoint Security không được cài đặt trên máy tính (xem hình bên dưới). Nếu Kaspersky Endpoint Security được cài đặt trên máy tính của bạn thì bạn có thể làm việc với các ổ đĩa di động được mã hóa bằng trình quản lý tập tin thông thường (ví dụ: Explorer).

Trình quản lý tập tin di động lưu trữ một khóa để mã hóa các tập tin trên một ổ đĩa di động. Khóa này được mã hóa bằng mật khẩu người dùng. Người dùng sẽ đặt mật khẩu trước khi mã hóa tập tin trên một ổ đĩa di động.

Trình quản lý tập tin di động sẽ tự động khởi chạy khi ổ đĩa di động được kết nối với máy tính không cài đặt Kaspersky Endpoint Security. Nếu máy tính đó tắt chức năng tự động khởi động ứng dụng, hãy khởi động Trình quản lý tập tin di động theo cách thủ công. Để thực hiện, hãy chạy tập tin có tên *pmv.exe* được lưu trữ trên ổ đĩa di động.



Trình quản lý tập tin di động

Hỗ trợ chế độ di động để làm việc với các tập tin được mã hóa

[Cách bật hỗ trợ chế độ di động để làm việc với các tập tin được mã hóa trên các ổ đĩa di động trong Bảng điều khiển quản trị \(MMC\)](#)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Mã hóa ổ đĩa di động**.
6. Trong danh sách thả xuống **Chế độ mã hóa cho thiết bị đã được chọn**, hãy chọn **Mã hóa tất cả các tập tin** hoặc **Chỉ mã hóa các tập tin mới**.

Chế độ di động chỉ khả dụng với Mã hóa mức độ tập tin (FLE). Không thể bật hỗ trợ chế độ di động cho Mã hóa toàn bộ ổ đĩa (FDE).

7. Chọn hộp kiểm **Chế độ di động**.
8. Nếu cần, [hãy thêm quy tắc mã hóa cho từng ổ đĩa di động](#).
9. Lưu các thay đổi của bạn.
10. Sau khi áp dụng chính sách, hãy kết nối ổ đĩa di động với máy tính.
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 Trình quản lý tập tin di động.
12. Nhập vào một mật khẩu đáp ứng được yêu cầu về độ bảo mật và xác nhận nó.
13. Lưu các thay đổi của bạn.

Kaspersky Endpoint Security sẽ mã hóa các tập tin trên ổ đĩa di động. Trình quản lý tập tin di động được sử dụng để làm việc với các tập tin mã hóa cũng sẽ được thêm vào ổ đĩa di động. Nếu đã có các tập tin được mã hóa trên ổ đĩa di động, Kaspersky Endpoint Security sẽ mã hóa lại chúng bằng khóa riêng. Điều này cho phép người dùng truy cập tất cả các tập tin trên ổ đĩa di động ở chế độ di động.

[Cách bật hỗ trợ chế độ di động để làm việc với các tập tin được mã hóa trên các ổ đĩa di động trong Bảng điều khiển web](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Mã hóa dữ liệu** → **Mã hóa ổ đĩa di động**.
5. Trong mục **Quản lý mã hóa**, hãy chọn **Mã hóa tất cả các tập tin** hoặc **Chỉ mã hóa các tập tin mới**.

Chế độ di động chỉ khả dụng với Mã hóa mức độ tập tin (FLE). Không thể bật hỗ trợ chế độ di động cho Mã hóa toàn bộ ổ đĩa (FDE).

6. Chọn hộp kiểm **Chế độ di động**.
7. Nếu cần, [hãy thêm quy tắc mã hóa cho từng ổ đĩa di động](#).
8. Lưu các thay đổi của bạn.
9. Sau khi áp dụng chính sách, hãy kết nối ổ đĩa di động với máy tính.
10. 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 Trình quản lý tập tin di động.
11. Nhập vào một mật khẩu đáp ứng được yêu cầu về độ bảo mật và xác nhận nó.
12. Lưu các thay đổi của bạn.

Kaspersky Endpoint Security sẽ mã hóa các tập tin trên ổ đĩa di động. Trình quản lý tập tin di động được sử dụng để làm việc với các tập tin mã hóa cũng sẽ được thêm vào ổ đĩa di động. Nếu đã có các tệp được mã hóa trên ổ đĩa di động, Kaspersky Endpoint Security sẽ mã hóa lại chúng bằng khóa riêng. Điều này cho phép người dùng truy cập tất cả các tập tin trên ổ đĩa di động ở chế độ di động.

Truy cập các tập tin được mã hóa trên ổ đĩa di động

Sau khi mã hóa tập tin trên ổ đĩa di động có hỗ trợ chế độ di động, các phương thức truy cập tập tin sau đây sẽ khả dụng:

- Nếu Kaspersky Endpoint Security không được cài đặt trên máy tính, Trình quản lý tập tin di động sẽ nhắc bạn nhập mật khẩu. Bạn sẽ cần nhập mật khẩu mỗi lần bạn khởi động lại máy tính hoặc kết nối lại ổ đĩa di động.
- Nếu máy tính được đặt bên ngoài mạng doanh nghiệp và Kaspersky Endpoint Security được cài đặt trên máy tính, ứng dụng sẽ nhắc bạn nhập mật khẩu hoặc gửi cho quản trị viên yêu cầu truy cập các tập tin. Sau khi có quyền truy cập vào các tập tin trên ổ đĩa di động, Kaspersky Endpoint Security sẽ lưu khóa bí mật vào ổ lưu trữ khóa của máy tính. Điều này sẽ cho phép bạn truy cập vào các tập tin về sau này mà không cần nhập mật khẩu hoặc hỏi quản trị viên.

- Nếu máy tính được đặt bên trong mạng doanh nghiệp và Kaspersky Endpoint Security được cài đặt trên máy tính, bạn sẽ có quyền truy cập vào thiết bị mà không cần nhập mật khẩu. Kaspersky Endpoint Security sẽ nhận khóa bí mật từ Máy chủ quản trị Kaspersky Security Center mà máy tính được kết nối với.

Khôi phục mật khẩu để làm việc ở chế độ di động

Nếu bạn quên mật khẩu để làm việc ở chế độ di động, bạn cần kết nối ổ đĩa di động với máy tính được cài đặt Kaspersky Endpoint Security bên trong mạng công ty. Bạn sẽ có quyền truy cập vào các tập tin vì khóa bí mật được lưu trữ trong ổ lưu trữ khóa của máy tính hoặc trên Máy chủ quản trị. Hãy giải mã và mã hóa lại các tập tin bằng mật khẩu mới.

Các tính năng của chế độ di động khi kết nối ổ đĩa di động với máy tính từ một mạng khác

Nếu máy tính được đặt bên ngoài mạng doanh nghiệp và Kaspersky Endpoint Security được cài đặt trên máy tính, bạn có thể truy cập tập tin theo các cách sau:

• Truy cập dựa trên mật khẩu

Sau khi nhập mật khẩu, bạn có thể xem, sửa đổi và lưu tập tin lên ổ đĩa di động (*truy cập thẳng*). Kaspersky Endpoint Security có thể đặt quyền truy cập chỉ cho phép đọc đối với một ổ đĩa di động nếu các tham số sau được cấu hình trong thiết lập chính sách để mã hóa ổ đĩa di động:

- Hỗ trợ chế độ di động bị tắt.
- Chế độ **Mã hóa tất cả các tập tin** hoặc **Chỉ mã hóa các tập tin mới** được chọn.

Trong tất cả các trường hợp khác, bạn sẽ có toàn quyền truy cập vào ổ đĩa di động (quyền đọc/ghi). Bạn có thể thêm và xóa các tập tin.

Bạn có thể thay đổi quyền truy cập ổ đĩa di động ngay cả khi ổ đĩa di động đang được kết nối với máy tính. Nếu quyền truy cập ổ đĩa di động bị thay đổi, Kaspersky Endpoint Security sẽ chặn quyền truy cập vào các tập tin và nhắc bạn nhập lại mật khẩu.

Sau khi nhập mật khẩu, bạn không thể áp dụng thiết lập chính sách mã hóa cho ổ đĩa di động. Trong trường hợp này, bạn không thể giải mã hoặc mã hóa lại các tập tin trên ổ đĩa di động.

• Yêu cầu quản trị viên cấp quyền truy cập vào các tập tin

Nếu bạn quên mật khẩu để làm việc ở chế độ di động, hãy yêu cầu quản trị viên cấp quyền truy cập tập tin. Để truy cập các tập tin, người dùng cần gửi cho quản trị viên một tập tin yêu cầu truy cập (một tập tin có phần mở rộng là KESDC). Ví dụ: người dùng có thể gửi tập tin yêu cầu truy cập qua email. Quản trị viên sẽ gửi một tập tin truy cập dữ liệu được mã hóa (một tập tin có phần mở rộng là KESDR).

Sau khi bạn hoàn thành quy trình Yêu cầu-Phản hồi để khôi phục mật khẩu, bạn sẽ nhận được quyền truy cập thẳng vào các tập tin trên ổ đĩa di động và toàn quyền truy cập vào ổ đĩa di động (quyền đọc/ghi).

Ví dụ: bạn có thể áp dụng chính sách mã hóa ổ đĩa di động và giải mã các tập tin. Sau khi khôi phục mật khẩu hoặc khi chính sách được cập nhật, Kaspersky Endpoint Security sẽ nhắc bạn xác nhận các thay đổi.

[Cách nhận tập tin truy cập dữ liệu được mã hóa trong Bảng điều khiển quản trị \(MMC\)](#) 

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Devices**.
4. Trên thẻ **Devices**, hãy chọn máy tính của người dùng yêu cầu truy cập vào dữ liệu được mã hóa và nhấn chuột phải để mở menu ngữ cảnh.
5. Trong menu ngữ cảnh, chọn **Cấp quyền truy cập trong chế độ ngoại tuyến**.
6. Trong cửa sổ mở ra, hãy chọn thẻ **Mã hóa dữ liệu**.
7. Trên thẻ **Mã hóa dữ liệu**, hãy nhấn nút **Duyệt**.
8. Trong cửa sổ để chọn tập tin yêu cầu truy cập, hãy chỉ định đường dẫn đến tập tin nhận được từ người dùng.

Bạn sẽ thấy thông tin về yêu cầu của người dùng. Kaspersky Security Center sẽ tạo một tập tin khóa. Hãy gửi tập tin khóa truy cập dữ liệu mã hóa được tạo ra cho người dùng qua email. Hoặc lưu tập tin truy cập và sử dụng bất kỳ phương thức có sẵn nào để truyền gửi tập tin đó.

Cách nhận tập tin truy cập dữ liệu được mã hóa trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Managed devices**.
2. Chọn hộp kiểm bên cạnh tên của máy tính có dữ liệu bạn muốn khôi phục quyền truy cập.
3. Nhấn nút **Grant access to the device in offline mode**.
4. Chọn mục **Mã hóa dữ liệu**.
5. Nhấn vào nút **Select file** và chọn tập tin yêu cầu truy cập mà bạn nhận được từ người dùng (tập tin có phần mở rộng là KESDC).
Bảng điều khiển Web sẽ hiển thị thông tin về yêu cầu. Thông tin này sẽ bao gồm tên của máy tính mà người dùng đang yêu cầu quyền truy cập vào tập tin.
6. Nhấn vào nút **Save key** và chọn thư mục để lưu tập tin khóa truy cập dữ liệu được mã hóa (tập tin có phần mở rộng là KESDR).

Kết quả là bạn có thể lấy được khóa truy cập dữ liệu được mã hóa cần để truyền gửi cho người dùng.

Giải mã ổ đĩa di động

Bạn có thể sử dụng một chính sách để giải mã một ổ đĩa di động. Một chính sách với thiết lập được xác định để mã hóa ổ đĩa di động sẽ được tạo cho một nhóm quản trị 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.

Để giải mã ổ đĩa di động:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Mã hóa ổ đĩa di động**.
6. 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**.
7. 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.
 - c. Trong menu ngữ cảnh của **Thiết lập quy tắc** nút, hãy nhấn **Giải mã toàn bộ ổ đĩa di động**.
8. Lưu các thay đổi của bạn.

Kết quả là nếu một người dùng kết nối ổ đĩa di động hoặc nếu ổ đĩa đó đã được kết nối, Kaspersky Endpoint Security sẽ giải mã ổ đĩa di động. Ứng dụng sẽ cảnh báo người dùng rằng tiến trình giải mã sẽ mất một khoảng thời gian. 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. Quá trình giải mã dữ liệu sẽ được tiếp tục khi ổ đĩa di động được kết nối với máy tính đó vào lần tới.

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.

Xem chi tiết mã hóa dữ liệu

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 mã hóa chưa được định nghĩa.* Một chính sách mã hóa Kaspersky Security Center chưa được định nghĩa cho máy tính.
- *Áp dụng chính sách.* 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.* Tiến trình mã hóa dữ liệu trên máy tính đã được hoàn tất sử dụng thiết lập 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.

Xem trạng thái mã hóa

Để xem trạng thái mã hóa của dữ liệu máy tính:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Devices**.
4. Trên thẻ **Devices** trong không gian làm việc, vuốt thanh cuộn sang tận cùng bên phải.
5. Nếu cột **Trạng thái mã hóa** không được hiển thị:
 - a. Nhấn phải chuột để mở menu ngữ cảnh cho đầu mục bảng.
 - b. Trong menu ngữ cảnh, trong danh sách thả xuống **Xem**, chọn **Add/Remove columns**.
 - c. Trong cửa sổ mở ra, hãy đánh dấu hộp **Trạng thái mã hóa**.
 - d. Nhấn **OK**.

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 nội bộ của máy tính, và về mã hóa toàn bộ ổ đĩa.

Xem thống kê mã hóa trên các bảng điều khiển của Kaspersky Security Center

Để xem trạng thái mã hóa trên các bảng điều khiển của Kaspersky Security Center:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây điều khiển, chọn nút **Administration Server**.
3. Trong không gian làm việc ở bên phải của cây Bảng điều khiển quản trị, chọn thẻ **Statistics**.
4. Tạo một trang mới với khung chi tiết chứa số liệu mã hóa dữ liệu. Để làm điều này:
 - a. Trên thẻ **Statistics**, nhấn nút **Customize view**.

- b. Trong cửa sổ mở ra, hãy nhấn vào nút **Thêm**.
- c. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, trong mục **Tổng quát**, hãy nhập tên của trang.
- d. Trong mục **Information panels**, hãy nhấn nút **Add**.
- e. Trong cửa sổ mở ra trong nhóm **Protection status**, hãy chọn mục **Encryption of devices**.
- f. Nhấn **OK**.
- g. Nếu cần, hãy chỉnh sửa thiết lập của bảng chi tiết. Để thực hiện, hãy sử dụng các mục **View** và **Devices**.
- h. Nhấn **OK**.
- i. Lặp lại các bước d – h của chỉ dẫn, sử dụng mục **Encryption of removable drives** trong mục **Protection status**.
Các bảng chi tiết được thêm sẽ hiện ra trong danh sách **Information panels**.
- j. Nhấn **OK**.
Tên của trang với khung chi tiết được tạo ở bước trước sẽ xuất hiện trong danh sách **Pages**.
- k. Nhấn vào nút **Đóng**.

5. Trên thẻ **Statistics**, 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 nội bộ trên máy tính

Để xem lỗi mã hóa tập tin trên các ổ đĩa nội bộ trên máy tính:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Devices**.
4. Chọn tên của máy tính trong danh sách và nhấn phải chuột để mở menu ngữ cảnh.
5. Trong menu ngữ cảnh của máy tính, chọn **Properties**. Trong cửa sổ mở ra, hãy chọn mục **Bảo vệ**.
6. Nhấn vào liên kết **View data encryption errors** để mở cửa sổ **Data encryption errors**.

Cửa sổ này sẽ hiển thị chi tiết các lỗi mã hóa tập tin trên các ổ đĩa nội bộ trên máy tính. Khi một lỗi được sửa, Kaspersky Security Center sẽ xóa chi tiết của lỗi đó khỏi cửa sổ **Data encryption errors**.

Xem báo cáo mã hóa dữ liệu

Để xem báo cáo mã hóa dữ liệu:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong nút **Administration Server** của cây Bảng điều khiển quản trị, chọn thẻ **Reports**.
3. Nhấn nút **New report template**.
Trình hướng dẫn tạo mẫu báo cáo mới sẽ khởi chạy.
4. Làm theo chỉ dẫn của Trình hướng dẫn Mẫu Báo cáo. Trong cửa sổ **Selecting the report template type** trong mục **Other**, chọn một trong các đề mục sau:
 - **Report on encryption status of managed devices.**
 - **Report on encryption status of mass storage devices.**
 - **Report on file encryption errors.**
 - **Report on blockage of access to encrypted files.**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 **Reports**.
5. Chọn mẫu báo cáo được tạo ở các bước trước của chỉ dẫn.
6. Trong menu ngữ cảnh của khuôn mẫu, chọn **Show report**.
Tiến trình tạo báo cáo sẽ được bắt đầu. Báo cáo sẽ được hiển thị trong một cửa sổ mới.

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 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 có 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 khóa truy cập có 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 có 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 khóa truy cập có 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.

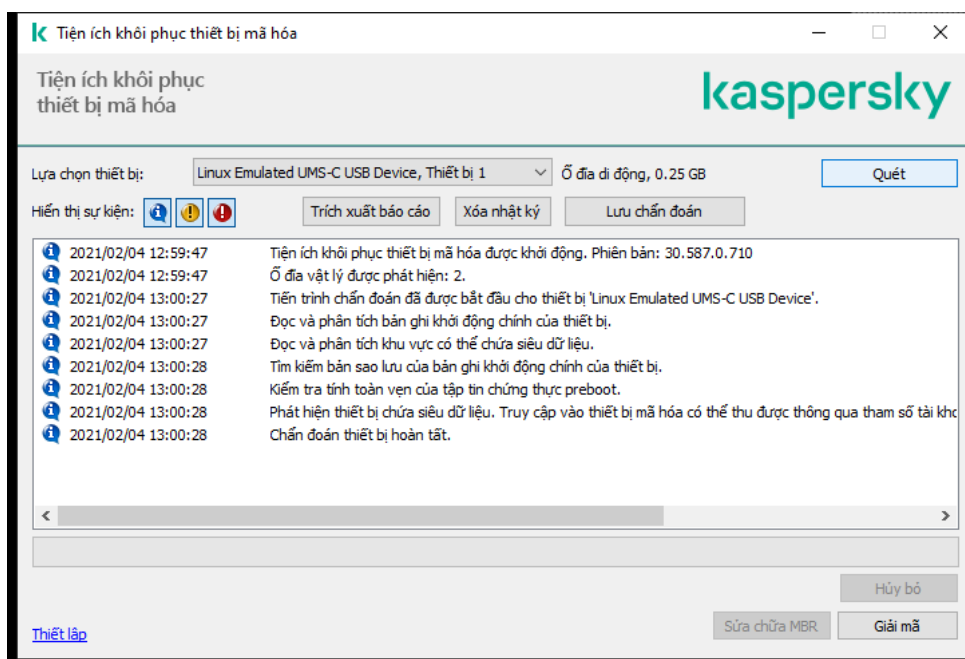
Trước khi khôi phục dữ liệu trên các thiết bị được mã hóa, bạn nên hủy bỏ chính sách Kaspersky Security Center hoặc tắt mã hóa trong thiết lập chính sách Kaspersky Security Center trên máy tính được thực hiện hoạt động này. Điều này sẽ ngăn thiết bị được mã hóa lại một lần nữa.

Khôi phục dữ liệu bằng cách sử dụng Tiện ích khôi phục FDERT

Nếu ổ cứng bị lỗi, hệ thống tập tin có thể bị hỏng. Nếu trường hợp này xảy ra, dữ liệu được bảo vệ bởi công nghệ Kaspersky Disk Encryption sẽ không khả dụng. Bạn có thể giải mã dữ liệu và sao chép dữ liệu vào một ổ đĩa mới.

Việc phục hồi dữ liệu trên ổ đĩa được bảo vệ bởi công nghệ Kaspersky Disk Encryption bao gồm các bước sau:


1. Tạo một Tiện ích khôi phục độc lập (xem hình bên dưới).
2. Kết nối ổ đĩa với máy tính chưa được cài đặt các thành phần mã hóa của Kaspersky Endpoint Security.
3. Chạy Tiện ích khôi phục và chẩn đoán ổ đĩa cứng.
4. Truy cập dữ liệu trên ổ đĩa. Để thực hiện, hãy nhập thông tin đăng nhập của Authentication Agent hoặc bắt đầu quy trình khôi phục (Yêu cầu-Phản hồi).



Tiện ích khôi phục FDERT

Tạo một tiện ích khôi phục độc lập

Để tạo tập tin thực thi của Tiện ích Khôi phục:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ mở ra, hãy nhấn nút **Khôi phục thiết bị mã hóa**.
Tiện ích khôi phục thiết bị mã hóa sẽ được bắt đầu.
3. Nhấn nút **Tạo Tiện ích khôi phục độc lập** trong cửa sổ Tiện ích khôi phục.
4. Lưu Tiện ích khôi phục độc lập vào bộ nhớ máy tính.

Kết quả là tập tin thực thi của Tiện ích khôi phục (fdert.exe) sẽ được lưu vào thư mục được chỉ định. Sao chép Tiện ích khôi phục vào máy tính không có các thành phần mã hóa của Kaspersky Endpoint Security. Điều này sẽ ngăn ổ đĩa được mã hóa lại một lần nữa.

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.

Phục hồi dữ liệu trên ổ đĩa cứng

Để khôi phục truy cập đến thiết bị được mã hóa sử dụng Tiện ích Khôi phục:

1. Chạy tập tin có tên fdert.exe, là tập tin thực thi của Tiện ích khôi phục. Tập tin này được tạo bởi Kaspersky Endpoint Security.
2. Trong cửa sổ Tiện ích khôi phục, hãy chọn thiết bị được mã hóa mà bạn muốn khôi phục quyền truy cập.

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. Nếu bạn muốn nhập thông tin chẩn đoán, hãy nhấn vào nút **Lưu chẩn đoán**.

Tiện ích sẽ lưu tập tin nén trong đó có các tập tin chứa thông tin chẩn đoán.

5. 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.

6. Nhấn nút **Mở khóa** hay **Giải mã** tùy thuộc vào kết quả của chẩn đoán.

7. Nếu bạn muốn khôi phục dữ liệu bằng tài khoản Authentication Agent, hãy chọn tùy chọn **Sử dụng thiết lập của tài khoản Authentication Agent** và nhập thông tin đăng nhập của 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.

8. Nếu bạn muốn bắt đầu quy trình phục hồi, hãy làm như sau:

a. Chọn mục **Chỉ định khóa truy cập thiết bị theo cách thủ công**.

b. Nhấn vào nút **Nhận khóa truy cập** và lưu tập tin yêu cầu truy cập vào bộ nhớ máy tính (tập tin có phần mở rộng là FDERTC).

c. 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.

d. Nhận và lưu tập tin truy cập (tập tin có phần mở rộng là FDERTR) được quản trị viên LAN công ty tạo và gửi cho bạn (xem hướng dẫn bên dưới).

e. Tải về tập tin truy cập trong cửa sổ **Nhận khóa truy cập thiết bị**.

9. Nếu bạn đang giải mã một thiết bị, bạn phải cấu hình thiết lập giải mã bổ sung:

- Chỉ định 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, hãy chọn mục **Giải mã khu vực riêng của thiết bị** và chỉ 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 **Giải mã đến một tập tin ảnh ổ đĩa**.
- Nếu bạn muốn lưu dữ liệu được giải mã tách riêng khỏi dữ liệu mã hóa gốc, chọn hộp kiểm **Giải mã đến một tập tin ảnh ổ đĩa** và sử dụng nút **Duyệt** để quy định đường dẫn lưu tập tin VHD.

10. Nhấn **OK**.

Tiến trình mở khóa / giải mã thiết bị sẽ được bắt đầu.

Cách tạo tập tin truy cập dữ liệu được mã hóa trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây Bảng điều khiển quản trị, chọn thư mục **Bổ sung** → **Data encryption and protection** → **Encrypted drives**.
3. Trong không gian làm việc, hãy chọn thiết bị được mã hóa mà bạn muốn tạo tập tin khóa truy cập, sau đó trong menu ngữ cảnh của thiết bị, hãy nhấn vào **Nhận quyền truy cập đến thiết bị trong Kaspersky Endpoint Security cho Windows**.

Nếu bạn không chắc chắn tập tin yêu cầu truy cập được tạo cho máy tính nào, trong cây Bảng điều khiển quản trị, hãy chọn thư mục **Bổ sung** → **Mã hóa và bảo vệ dữ liệu** và nhấn vào liên kết **Nhận khóa mã hóa thiết bị trong Kaspersky Endpoint Security cho Windows** trong không gian làm việc.

4. Trong cửa sổ mở ra, hãy chọn thuật toán mã hóa để sử dụng: **AES256** hoặc **AES56**.
Thuật toán mã hóa dữ liệu phụ thuộc vào thư viện mã hóa AES, được kèm theo gói phân phối: *Mã hóa mạnh (AES256)* hoặc *Mã hóa nhẹ (AES56)*. Thư viện mã hóa AES được cài đặt cùng với ứng dụng.
5. Nhấn vào **Duyệt** để mở một cửa sổ; trong cửa sổ này, hãy chỉ định đường dẫn đến tập tin yêu cầu có phần mở rộng là `fdertc` nhận được từ người dùng.
6. Nhấn nút **Mở**.

Bạn sẽ thấy thông tin về yêu cầu của người dùng. Kaspersky Security Center sẽ tạo một tập tin khóa. Hãy gửi tập tin khóa truy cập dữ liệu mã hóa được tạo ra cho người dùng qua email. Hoặc lưu tập tin truy cập và sử dụng bất kỳ phương thức có sẵn nào để truyền gửi tập tin đó.

Cách tạo tập tin truy cập dữ liệu được mã hóa trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Hoạt động** → **Data encryption and protection** → **Encrypted drives**.

2. Chọn hộp kiểm bên cạnh tên của máy tính mà bạn muốn khôi phục dữ liệu.

3. Nhấn nút **Grant access to the device in offline mode**.

Thao tác này sẽ khởi chạy Trình hướng dẫn để cấp quyền truy cập cho một thiết bị.

4. Làm theo hướng dẫn của Trình hướng dẫn để cấp quyền truy cập cho một thiết bị:

a. Chọn tiện ích **Kaspersky Endpoint Security cho Windows**.

b. Chọn thuật toán mã hóa để sử dụng: **AES256** hoặc **AES56**.

Thuật toán mã hóa dữ liệu phụ thuộc vào thư viện mã hóa AES, được kèm theo gói phân phối: *Mã hóa mạnh (AES256)* hoặc *Mã hóa nhẹ (AES56)*. Thư viện mã hóa AES được cài đặt cùng với ứng dụng.

c. Nhấn vào nút **Select file** và chọn tập tin yêu cầu truy cập nhận được từ người dùng (tập tin có phần mở rộng là FDERTC).

d. Nhấn vào nút **Save key** và chọn thư mục để lưu tập tin khóa được dùng để truy cập dữ liệu được mã hóa (tập tin có phần mở rộng là FDERTR).

Kết quả là bạn có thể lấy được khóa truy cập dữ liệu được mã hóa cần để truyền gửi cho người dùng.

Tạo một đĩa cứu hộ cho hệ điều hành

Đĩa cứu hộ 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 bản sao của hệ điều hành Windows bằng cách sử dụng đĩa cứu hộ và khôi phục truy cập đến ổ cứng được mã hóa sử dụng Tiện ích Khôi phục được bao gồm trong bản sao hệ điều hành.

Để tạo một đĩa cứu hộ cho hệ điều hành:

1. [Tạo một tập tin thực thi cho Tiện ích khôi phục thiết bị mã hóa](#).

2. Tạo một bản sao tùy chỉnh của môi trường tiền khởi động Windows. Trong khi tạo một bản sao tùy chỉnh của môi trường tiền khởi động Windows, bổ sung tập tin thực thi của Tiện ích Khôi phục vào bản sao.

3. Lưu bản sao 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 bản sao tùy chỉnh của môi trường tiền khởi động Windows (ví dụ, trong [tài nguyên của Microsoft TechNet](#)).

Các giải pháp Detection and Response

Kaspersky Endpoint Security hỗ trợ các giải pháp Detection and Response bằng một tác nhân được tích hợp. Để sử dụng Detection and Response, bạn phải bật tích hợp với các giải pháp này khi cài đặt ứng dụng. Tác nhân được tích hợp hỗ trợ:

- Kaspersky Managed Detection and Response (MDR);
- Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum);
- Kaspersky Endpoint Detection and Response Expert (EDR Expert);
- Kaspersky Sandbox 2.0.

Bạn có thể sử dụng Kaspersky Endpoint Security với giải pháp Detection and Response trong các cấu hình khác nhau, ví dụ như [MDR+EDR Optimum 2.0+Kaspersky Sandbox 2.0].

Kaspersky Endpoint Agent hỗ trợ các giải pháp Detection and Response mà Kaspersky Endpoint Security tích hợp không hỗ trợ (ví dụ: Kaspersky Sandbox 1.0).

Trong Kaspersky Endpoint Security 11.9.0, gói phân phối Kaspersky Endpoint Agent không còn thuộc gói phân phối Kaspersky Endpoint Security. Bạn phải tải xuống gói phân phối Kaspersky Endpoint Agent riêng.

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent hỗ trợ tương tác giữa ứng dụng và các giải pháp khác của Kaspersky để phát hiện các mối đe dọa nâng cao (ví dụ: Kaspersky Sandbox). Các giải pháp của Kaspersky tương thích với các phiên bản cụ thể của Kaspersky Endpoint Agent.

Để sử dụng Kaspersky Endpoint Agent thuộc các giải pháp của Kaspersky, bạn phải kích hoạt các giải pháp đó bằng khóa giấy phép tương ứng.

Để biết thông tin đầy đủ về Kaspersky Endpoint Agent for Windows có trong giải pháp phần mềm bạn đang sử dụng và để biết thông tin đầy đủ về giải pháp độc lập, vui lòng tham khảo Hướng dẫn sử dụng của sản phẩm liên quan:

- *Trợ giúp của Kaspersky Anti Targeted Attack Platform*
- *Trợ giúp của Kaspersky Sandbox*
- *Trợ giúp của Kaspersky Endpoint Detection and Response Optimum*
- *Trợ giúp của Managed Detection and Response của Kaspersky*

Trong Kaspersky Endpoint Security 11.9.0, gói phân phối Kaspersky Endpoint Agent không còn thuộc gói phân phối Kaspersky Endpoint Security. Bạn phải tải xuống gói phân phối Kaspersky Endpoint Agent riêng.

Kaspersky Endpoint Security cho Windows	Kaspersky Endpoint Agent
11.8.0	3.11.0.216.mr1
11.7.0	3,11
11.6.0	3,10
11.5.0	3,9
11.4.0	3,9
11.3.0	3,9
11.2.0	3,9

Chuyển đổi chính sách và tác vụ cho Kaspersky Endpoint Agent

Kaspersky Endpoint Security 11.7.0 đã có một trình hướng dẫn chuyển đổi từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security. Bạn có thể chuyển đổi thiết lập chính sách và tác vụ cho các giải pháp sau:

- Kaspersky Sandbox;
- Kaspersky Endpoint Detection and Response Optimum (EDR Optimum);
- Kaspersky Managed Detection and Response (MDR).

Bạn nên bắt đầu với việc chuyển Kaspersky Endpoint Agent sang Kaspersky Endpoint Security trên một máy tính, sau đó thực hiện công việc này trên một nhóm các máy tính, và sau đó hoàn tất chuyển đổi trên tất cả các máy tính của tổ chức.

Để chuyển thiết lập chính sách và tác vụ từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security,

trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Hoạt động** → **Chuyển từ Kaspersky Endpoint Agent**.

Thao tác này sẽ chạy Trình hướng dẫn chuyển đổi chính sách và tác vụ. Làm theo chỉ dẫn của Trình hướng dẫn.

Bước 1. Chuyển đổi chính sách

Trình hướng dẫn chuyển đổi sẽ tạo một chính sách mới để gộp thiết lập của các chính sách Kaspersky Endpoint Security và Kaspersky Endpoint Agent. Trong danh sách chính sách, hãy chọn các chính sách Kaspersky Endpoint Agent có thiết lập mà bạn muốn gộp với chính sách Kaspersky Endpoint Security. Nhấn vào một chính sách Kaspersky Endpoint Agent để chọn Kaspersky Endpoint Security mà bạn muốn gộp thiết lập mới. Đảm bảo rằng bạn đã chọn đúng các chính sách và chuyển sang bước tiếp theo.

Bước 2. Chuyển đổi tác vụ

Trình hướng dẫn chuyển đổi sẽ tạo các tác vụ mới cho Kaspersky Endpoint Security. Trong danh sách tác vụ, hãy chọn các tác vụ Kaspersky Endpoint Agent mà bạn muốn tạo cho chính sách Kaspersky Endpoint Security. Trình hướng dẫn hỗ trợ các tác vụ dành cho Kaspersky Endpoint Detection and Response và Kaspersky Sandbox. Chuyển sang bước tiếp theo.

Bước 3. Hoàn tất Trình hướng dẫn

Thoát Trình hướng dẫn. Kết quả là trình hướng dẫn:

- Sẽ tạo một chính sách Kaspersky Endpoint Security mới.

Chính sách sẽ gộp thiết lập từ Kaspersky Endpoint Security và Kaspersky Endpoint Agent. Chính sách được gọi là <tên chính sách Kaspersky Endpoint Security> & <tên chính sách Kaspersky Endpoint Agent>. Chính sách mới có trạng thái *Không hoạt động*. Để tiếp tục, hãy thay đổi trạng thái của chính sách Kaspersky Endpoint Agent và Kaspersky Endpoint Security thành *Không hoạt động* và kích hoạt chính sách mới được gộp.

Sau khi chuyển đổi từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security cho Windows, vui lòng đảm bảo thiết lập chính sách mới có [chức năng dành cho việc truyền dữ liệu đến Máy chủ quản trị](#) (dữ liệu tập tin trong khu vực cách ly và dữ liệu chuỗi phát triển mới đe dọa). Các giá trị thông số truyền dữ liệu không được chuyển từ một chính sách của Kaspersky Endpoint Agent.

- Sẽ tạo các tác vụ Kaspersky Endpoint Security mới.

Các tác vụ mới là các bản sao của tác vụ Kaspersky Endpoint Agent dành cho Kaspersky Endpoint Detection and Response và Kaspersky Sandbox. Đồng thời, Trình hướng dẫn sẽ giữ nguyên các tác vụ của Kaspersky Endpoint Agent.

Chuyển cấu hình [KES+KEA] sang cấu hình [KES+built-in agent]

Bây giờ Kaspersky Endpoint Security 11.7.0 đã có các tác nhân tích hợp dành cho giải pháp Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum) và Kaspersky Sandbox 2.0. Bạn không còn cần một ứng dụng Kaspersky Endpoint Agent riêng để hoạt động với các giải pháp này. Khi bạn nâng cấp Kaspersky Endpoint Security lên phiên bản 11.7.0 thì các giải pháp EDR Optimum và Kaspersky Sandbox sẽ tiếp tục hoạt động với Kaspersky Endpoint Security. Ngoài ra, Kaspersky Endpoint Agent sẽ được gỡ bỏ khỏi máy tính.

Trong Kaspersky Endpoint Security 11.9.0, gói phân phối Kaspersky Endpoint Agent không còn thuộc gói phân phối Kaspersky Endpoint Security. Bạn phải tải xuống gói phân phối Kaspersky Endpoint Agent riêng.

Việc chuyển cấu hình [KES+KEA] sang [KES+built-in agent] liên quan đến các bước sau:

1 Nâng cấp Kaspersky Security Center

Nâng cấp tất cả các thành phần của Kaspersky Security Center lên phiên bản 13.2, bao gồm Administration Agent trên máy tính của người dùng và Bảng điều khiển web.

2 Nâng cấp tiện ích web Kaspersky Endpoint Security

Trong Bảng điều khiển web Kaspersky Security Center, hãy nâng cấp tiện ích web Kaspersky Endpoint Security lên phiên bản 11.7.0. Bạn phải sử dụng Bảng điều khiển web để quản lý các thành phần EDR Optimum và Kaspersky Sandbox.

3 Chuyển chính sách và các tác vụ

Hãy sử dụng [Trình hướng dẫn chuyển đổi chính sách và tác vụ của Kaspersky Endpoint Agent](#) để chuyển thiết lập Kaspersky Endpoint Agent sang Kaspersky Endpoint Security cho Windows.

Việc này sẽ tạo một chính sách Kaspersky Endpoint Security mới. Chính sách mới có trạng thái *Không hoạt động*. Để áp dụng chính sách, hãy mở các thuộc tính chính sách, chấp nhận Tuyên bố Kaspersky Security Network và đặt trạng thái thành *Hoạt động*.

4 Chức năng cấp giấy phép

Nếu bạn sử dụng một giấy phép Kaspersky Endpoint Detection and Response Optimum hoặc Kaspersky Optimum Security chung để kích hoạt Kaspersky Endpoint Security cho Windows và Kaspersky Endpoint Agent thì chức năng EDR Optimum sẽ được kích hoạt tự động sau khi nâng cấp lên phiên bản 11.7.0. Bạn không cần phải làm gì khác.

Nếu bạn sử dụng giấy phép Kaspersky Endpoint Detection and Response Optimum Add-on độc lập để kích hoạt chức năng EDR Optimum thì bạn phải đảm bảo rằng khóa EDR Optimum được thêm vào kho của Kaspersky Security Center và [chức năng phân phối khóa giấy phép tự động được bật](#). Sau khi bạn nâng cấp ứng dụng lên phiên bản 11.7.0 thì chức năng EDR Optimum sẽ được kích hoạt tự động.

Nếu bạn sử dụng giấy phép Kaspersky Endpoint Detection and Response Optimum hoặc Kaspersky Optimum Security để kích hoạt Kaspersky Endpoint Agent, và sử dụng một giấy phép khác để kích hoạt Kaspersky Endpoint Security cho Windows thì bạn phải thay thế khóa Kaspersky Endpoint Security cho Windows bằng khóa dùng chung của Kaspersky Endpoint Detection and Response Optimum hoặc Kaspersky Optimum Security. Bạn có thể thay thế khóa bằng tác vụ [Thêm khóa](#).

Bạn không cần kích hoạt chức năng Kaspersky Sandbox. Chức năng Kaspersky Sandbox sẽ khả dụng ngay sau khi nâng cấp và kích hoạt Kaspersky Endpoint Security cho Windows.

5 Nâng cấp ứng dụng Kaspersky Endpoint Security

Để nâng cấp ứng dụng và chuyển đổi chức năng EDR Optimum và Kaspersky Sandbox chúng tôi khuyến nghị chạy [tác vụ cài đặt từ xa](#).

Để nâng cấp ứng dụng bằng tác vụ cài đặt từ xa, bạn phải chỉnh sửa các thiết lập sau:

- Chọn các thành phần Endpoint Detection and Response Optimum hoặc Kaspersky Sandbox trong gói cài đặt.
- Loại trừ thành phần Kaspersky Endpoint Agent trong thiết lập của gói cài đặt.

Bạn cũng có thể nâng cấp ứng dụng từ bằng các phương thức sau:

- Sử dụng dịch vụ cập nhật của Kaspersky (Seamless Update - SMU).
- Cục bộ bằng cách sử dụng Trình hướng dẫn cài đặt.

Trong trường hợp này, bạn phải kiểm tra cấu hình của Kaspersky Endpoint Agent được cài đặt trên máy tính. Nếu Kaspersky Endpoint Agent được cài đặt có thành phần Endpoint Detection and Response Expert (KATA EDR) thì hãy gỡ bỏ thành phần đó trước khi bạn nâng cấp ứng dụng. Nếu bạn không thể gỡ bỏ thành phần Endpoint Detection and Response Expert (KATA EDR) thì Kaspersky Endpoint Security sẽ bỏ qua các thành phần EDR Optimum và Kaspersky Sandbox khi nâng cấp ứng dụng. Bạn có thể cài đặt các thành phần bằng tác vụ [Thay đổi thành phần ứng dụng](#) sau khi nâng cấp ứng dụng.

Kaspersky Endpoint Security hỗ trợ tự động chọn các thành phần khi nâng cấp ứng dụng trên máy tính được cài đặt ứng dụng Kaspersky Endpoint Agent. Việc tự động chọn các thành phần sẽ phụ thuộc vào quyền của tài khoản người dùng đang nâng cấp ứng dụng.

Nếu bạn đang nâng cấp Kaspersky Endpoint Security bằng tập tin EXE hoặc MSI bằng tài khoản hệ thống (SYSTEM) thì Kaspersky Endpoint Security có quyền truy cập các giấy phép đang hoạt động của các giải pháp Kaspersky. Do đó, giả sử nếu máy tính được cài đặt Kaspersky Endpoint Agent và giải pháp EDR Optimum được kích hoạt thì bộ cài đặt Kaspersky Endpoint Security sẽ tự động cấu hình bộ thành phần và chọn thành phần EDR Optimum. Điều này khiến Kaspersky Endpoint Security chuyển sang sử dụng tác nhân tích hợp và gỡ bỏ Kaspersky Endpoint Agent. Việc chạy bộ cài đặt MSI bằng tài khoản hệ thống (SYSTEM) thường được thực hiện khi nâng cấp thông qua dịch vụ cập nhật của Kaspersky (SMU) hoặc khi triển khai gói cài đặt thông qua Kaspersky Security Center.

Nếu bạn đang nâng cấp Kaspersky Endpoint Security bằng một tập tin MSI bằng tài khoản người dùng không có đặc quyền thì Kaspersky Endpoint Security không có quyền truy cập các giấy phép đang hoạt động của các giải pháp Kaspersky. Trong trường hợp này, Kaspersky Endpoint Security tự động chọn các thành phần dựa trên cấu hình của Kaspersky Endpoint Agent như sau:

- Nếu thành phần Endpoint Detection and Response Expert (KATA EDR) được cài đặt, Kaspersky Endpoint Security sẽ chọn thành phần Endpoint Agent. Kaspersky Endpoint Security sẽ chỉ chọn thành phần Endpoint Agent, ngay cả khi Kaspersky Endpoint Agent có các thành phần khác được cài đặt, ví dụ như cấu hình [KATA EDR+KSB].
- Nếu thành phần Kaspersky Sandbox, EDR Optimum, hoặc cấu hình [Kaspersky Sandbox+EDR Optimum] được cài đặt thì Kaspersky Endpoint Security sẽ chọn các thành phần liên quan. Điều này khiến Kaspersky Endpoint Security chuyển sang sử dụng tác nhân tích hợp và gỡ bỏ Kaspersky Endpoint Agent.

6 Khởi động lại máy tính

Khởi động lại máy tính của bạn để hoàn tất nâng cấp ứng dụng với tác nhân tích hợp. Khi nâng cấp ứng dụng, trình cài đặt sẽ gỡ bỏ Kaspersky Endpoint Agent trước khi máy tính được khởi động lại. Sau khi máy tính được khởi động lại, trình cài đặt sẽ thêm tác nhân tích hợp. Điều này có nghĩa là Kaspersky Endpoint Security không thực hiện các chức năng của EDR và Kaspersky Sandbox cho đến khi máy tính được khởi động lại.

7 Kiểm tra tình trạng của Kaspersky Endpoint Detection and Response Optimum và Kaspersky Sandbox

Nếu sau khi nâng cấp, máy tính có trạng thái *Nghiêm trọng* trong bảng điều khiển Kaspersky Security Center:

- Đảm bảo rằng máy tính được cài đặt Administration Agent 13.2.
- Kiểm tra trạng thái hoạt động của thành phần EDR Optimum và Kaspersky Sandbox bằng cách xem *Báo cáo trạng thái thành phần ứng dụng*. Nếu một thành phần có trạng thái *Chưa được cài đặt* thì hãy cài đặt thành phần bằng tác vụ [Thay đổi thành phần ứng dụng](#).
- Đảm bảo rằng bạn chấp nhận Tuyên bố Kaspersky Security Network trong chính sách mới của Kaspersky Endpoint Security cho Windows.

Đảm bảo rằng chức năng EDR Optimum được kích hoạt bằng *Báo cáo trạng thái thành phần ứng dụng*. Nếu một thành phần có trạng thái *Không được giấy phép hỗ trợ* thì hãy đảm bảo rằng [chức năng phân phối khóa giấy phép tự động của EDR Optimum được bật](#).

Nâng cấp ứng dụng thuộc KATA EDR

Nếu bạn có Kaspersky Endpoint Agent được cài đặt để tích hợp với Kaspersky Anti Targeted Attack Platform (thành phần Endpoint Detection and Response Expert (KATA EDR)) thì bạn có thể nâng cấp Kaspersky Endpoint Security cho Windows theo bất kỳ cách nào sau đây:

- Sử dụng một tác vụ cài đặt từ xa.

Để thực hiện, bạn cần chỉnh sửa các thiết lập sau:

- Loại trừ các thành phần Endpoint Detection and Response Optimum và Kaspersky Sandbox trong gói cài đặt.
- Chọn thành phần Kaspersky Endpoint Agent trong thiết lập của gói cài đặt. Nếu máy tính đã có Kaspersky Endpoint Agent được cài đặt thì ứng dụng sẽ được nâng cấp lên 3.11.
- Sử dụng dịch vụ cập nhật của Kaspersky (SMU).
Để thực hiện, bạn phải xác nhận nâng cấp ứng dụng. Kaspersky Endpoint Security sẽ loại trừ Endpoint Detection and Response Optimum và Kaspersky Sandbox khỏi quá trình cài đặt. Nâng cấp Kaspersky Endpoint Agent không được hỗ trợ. Bạn có thể nâng cấp Kaspersky Endpoint Agent theo cách thủ công.
- Cục bộ bằng cách sử dụng Trình hướng dẫn cài đặt.
Kaspersky Endpoint Security sẽ loại trừ Endpoint Detection and Response Optimum và Kaspersky Sandbox khỏi quá trình cài đặt. Nếu máy tính đã có Kaspersky Endpoint Agent được cài đặt thì ứng dụng sẽ được nâng cấp lên 3.11.

Managed Detection and Response



Kaspersky Endpoint Security 11.6.0 giới thiệu tác nhân tích hợp cho giải pháp Managed Detection and Response. Giải pháp *Managed Detection and Response (MDR)* của Kaspersky sẽ tự động phát hiện và phân tích các sự cố bảo mật trong cơ sở hạ tầng của bạn. Để thực hiện, MDR sử dụng dữ liệu đo từ xa nhận được từ các điểm cuối và công nghệ máy học. MDR sẽ gửi dữ liệu sự cố cho các chuyên gia của Kaspersky. Sau đó, các chuyên gia có thể xử lý sự cố, ví dụ như thêm một mục mới vào Cơ sở dữ liệu chống virus. Ngoài ra, các chuyên gia có thể đưa ra các khuyến nghị về cách xử lý sự cố, ví dụ như đề xuất cách ly máy tính khỏi mạng. Để biết thông tin chi tiết về cách hoạt động của giải pháp này, vui lòng tham khảo [Trợ giúp của Managed Detection and Response của Kaspersky](#).²

Tích hợp với MDR

Để thiết lập tích hợp với Kaspersky Managed Detection and Response, bạn phải bật thành phần Managed Detection and Response và cấu hình Kaspersky Endpoint Security.

Bạn phải bật các thành phần sau để Managed Detection and Response hoạt động:

- [Kaspersky Security Network \(chế độ mở rộng\)](#).
- [Phát hiện hành vi](#).

Bắt buộc phải bật các thành phần này. Nếu không Kaspersky Managed Detection and Response không thể hoạt động bởi vì thành phần này sẽ không nhận được dữ liệu đo lường từ xa cần thiết.

Ngoài ra, thành phần Managed Detection and Response của Kaspersky còn sử dụng dữ liệu nhận được từ các thành phần khác của ứng dụng. Không bắt buộc phải bật các thành phần đó. Các thành phần cung cấp dữ liệu bổ sung gồm có:

- [Bảo vệ mỗi đe dọa web](#).
- [Bảo vệ mỗi đe dọa thư điện tử](#).

- [Tường lửa](#).

Để Kaspersky Managed Detection and Response hoạt động với Máy chủ quản trị thông qua Bảng điều khiển web Kaspersky Security Center, bạn cũng phải thiết lập một kết nối bảo mật mới, một *kết nối trong nền*. Kaspersky Managed Detection and Response sẽ nhắc bạn thiết lập một kết nối trong nền khi bạn triển khai giải pháp này. Đảm bảo rằng kết nối trong nền được thiết lập. Để biết chi tiết về việc tích hợp Kaspersky Security Center với các giải pháp khác của Kaspersky, hãy tham khảo [Trợ giúp của Kaspersky Security Center](#).

Việc tích hợp với thành phần Managed Detection and Response của Kaspersky bao gồm các bước sau:

1 Cấu hình Kaspersky Security Network Riêng

Bỏ qua bước này nếu bạn đang sử dụng Bảng điều khiển đám mây Kaspersky Security Center. Bảng điều khiển đám mây Kaspersky Security Center sẽ tự động cấu hình Kaspersky Security Network cục bộ khi cài đặt tiện ích MDR.

KSN Riêng hỗ trợ trao đổi dữ liệu giữa các máy tính và máy chủ chuyên dụng của Kaspersky Security Network, nhưng không hỗ trợ KSN Toàn cầu.

Tải lên tập tin cấu hình Kaspersky Security Network trong thuộc tính Máy chủ quản trị. Tập tin cấu hình Kaspersky Security Network nằm trong tập tin nén ZIP của tập tin cấu hình MDR. Bạn có thể lấy tập tin nén ZIP trong Bảng điều khiển Managed Detection and Response của Kaspersky. Để biết chi tiết về cách cấu hình máy chủ proxy của Kaspersky Security Network Riêng, vui lòng tham khảo [Trợ giúp của Kaspersky Security Network](#). Bạn cũng có thể tải tập tin cấu hình Kaspersky Security Network lên máy tính từ dòng lệnh (xem hướng dẫn bên dưới).

[Cách cấu hình Kaspersky Security Network Riêng từ dòng lệnh](#)

1. Chạy trình thông dịch dòng lệnh (cmd.exe) với tư cách quản trị viên.
2. Tới thư mục chứa tập tin thực thi Kaspersky Endpoint Security.
3. Chạy dòng lệnh sau:

```
avp.com KSN /private <tên tập tin>
```

trong đó <tên tập tin> là tên của tập tin cấu hình chứa thiết lập KSN Riêng (định dạng tập tin PKCS7 hoặc PEM).

Ví dụ:

```
avp.com KSN /private C:\kpsn_config.pkcs7
```

Kết quả là, Kaspersky Endpoint Security sẽ sử dụng KSN Riêng để xác định danh tiếng của các tập tin, ứng dụng và trang web. Thiết lập chính sách trong mục **Kaspersky Security Network** sẽ hiển thị trạng thái hoạt động sau: *Mạng KSN: KSN Riêng*.

Bạn phải [bật chế độ KSN mở rộng](#) để Managed Detection and Response hoạt động.

2 Bật thành phần Managed Detection and Response

Tải tập tin cấu hình BLOB trong chính sách Kaspersky Endpoint Security (xem hướng dẫn bên dưới). Tập tin BLOB chứa ID ứng dụng khách và thông tin về giấy phép cho thành phần Managed Detection and Response của Kaspersky. Tập tin BLOB nằm bên trong tập tin nén ZIP của tập tin cấu hình MDR. Bạn có thể lấy tập tin nén ZIP trong Bảng điều khiển Managed Detection and Response của Kaspersky. Để biết thông tin chi tiết về tập tin BLOB, vui lòng tham khảo [Trợ giúp của Managed Detection and Response của Kaspersky](#).

Cách bật thành phần Managed Detection and Response trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong thư mục **Managed devices** 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 **Policies**.
4. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
5. Trong cửa sổ chính sách, hãy chọn **Detection and Response** → **Managed Detection and Response**.
6. Chọn hộp kiểm **Managed Detection and Response**.
7. Trong mục **Thiết lập**, hãy nhấn **Nhập** và chọn tập tin BLOB nhận được trong Bảng điều khiển Managed Detection and Response của Kaspersky. Tập tin có đuôi mở rộng P7.
8. Lưu các thay đổi của bạn.

Cách bật thành phần Managed Detection and Response trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Detection and Response** → **Managed Detection and Response**.
5. Bật nút bật/tắt **Managed Detection and Response**.
6. Nhấn vào **Nhập** và chọn tập tin BLOB được lấy trong Bảng điều khiển Managed Detection and Response của Kaspersky. Tập tin có đuôi mở rộng P7.
7. Lưu các thay đổi của bạn.

Cách bật thành phần Managed Detection and Response từ dòng lệnh

1. Chạy trình thông dịch dòng lệnh (cmd.exe) với tư cách quản trị viên.

2. Tới thư mục chứa tập tin thực thi Kaspersky Endpoint Security.

3. Chạy dòng lệnh sau:

```
avp.com MDRLICENSE /ADD <tên tập tin> /login=<tên người dùng> /password=<mật khẩu>
```

Để thực thi lệnh này, [Bảo vệ bằng mật khẩu phải được bật](#). Người dùng phải có quyền **Cấu hình thiết lập của ứng dụng**.

Kết quả là Kaspersky Endpoint Security sẽ xác minh tập tin BLOB. Quá trình xác minh tập tin BLOB bao gồm kiểm tra chữ ký số và thời hạn giấy phép. Nếu tập tin BLOB được xác minh thành công, Kaspersky Endpoint Security sẽ tải tập tin đó lên và gửi tập tin đến máy tính trong lần đồng bộ hóa tiếp theo với Kaspersky Security Center. Kiểm tra trạng thái hoạt động của thành phần bằng cách xem *Báo cáo trạng thái thành phần ứng dụng*. Bạn cũng có thể xem trạng thái hoạt động của một thành phần trong mục báo cáo trong giao diện cục bộ của Kaspersky Endpoint Security. Thành phần **Managed Detection and Response** sẽ được thêm vào danh sách các thành phần của Kaspersky Endpoint Security.

Chuyển sang từ Kaspersky Endpoint Agent

Kaspersky Endpoint Security phiên bản 11 và mới hơn hỗ trợ giải pháp MDR. Kaspersky Endpoint Security phiên bản 11 – 11.5.0 chỉ gửi dữ liệu đo lường từ xa đến thành phần Managed Detection and Response của Kaspersky để bật tính năng phát hiện mối đe dọa. Kaspersky Endpoint Security phiên bản 11.6.0 có tất cả các chức năng của tác nhân tích hợp (Kaspersky Endpoint Agent).

Nếu bạn đang sử dụng Kaspersky Endpoint Security 11 – 11.5.0 thì bạn phải cập nhật cơ sở dữ liệu lên phiên bản mới nhất để hoạt động với giải pháp MDR. Bạn cũng phải cài đặt Kaspersky Endpoint Agent.

Nếu bạn đang sử dụng Kaspersky Endpoint Security 11.6.0 trở lên, bạn không cần cài đặt Kaspersky Endpoint Agent để sử dụng giải pháp MDR.

Để chuyển đổi từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security cho Windows:

1. Hãy cấu hình tích hợp với Kaspersky Managed Detection and Response trong chính sách của Kaspersky Endpoint Security.
2. Tắt thành phần Managed Detection and Response trong chính sách Kaspersky Endpoint Agent.

Nếu chính sách Kaspersky Endpoint Security cũng áp dụng cho các máy tính không được cài đặt Kaspersky Endpoint Security 11 – 11.5.0 thì trước hết bạn phải tạo một chính sách Kaspersky Endpoint Agent riêng cho các máy tính đó. Trong chính sách mới, hãy cấu hình tích hợp với Kaspersky Managed Detection and Response.

Endpoint Detection and Response



Kaspersky Endpoint Security 11.7.0 đã có một tác nhân tích hợp cho giải pháp Kaspersky Endpoint Detection and Response Optimum (sau đây gọi là "EDR Optimum"). Kaspersky Endpoint Security 11.8.0 đã có một tác nhân tích hợp cho giải pháp Kaspersky Endpoint Detection and Response Expert (sau đây gọi là "EDR Expert"). *Kaspersky Endpoint Detection and Response* là một loạt các giải pháp để bảo vệ cơ sở hạ tầng CNTT của doanh nghiệp trước các mối đe dọa mạng nâng cao. Chức năng của các giải pháp này kết hợp tính năng tự động phát hiện các mối đe dọa với khả năng phản ứng trước các mối đe dọa này để chống lại các cuộc tấn công nâng cao, bao gồm các cuộc tấn công khai thác mới, phần mềm tống tiền, các cuộc tấn công không dùng tập tin, cũng như các phương pháp sử dụng các công cụ hệ thống hợp pháp. EDR Expert cung cấp nhiều chức năng giám sát và phản ứng trước mối đe dọa hơn EDR Optimum. Để biết chi tiết về các giải pháp, hãy xem [Trợ giúp của Kaspersky Endpoint Detection and Response Optimum](#) và [Trợ giúp của Kaspersky Endpoint Detection and Response Expert](#).

Kaspersky Endpoint Detection and Response sẽ đánh giá và phân tích sự phát triển của mối đe dọa và cung cấp cho *nhân viên an ninh* hoặc *Quản trị viên* thông tin về cuộc tấn công tiềm ẩn cần thiết để có phản ứng kịp thời. Kaspersky Endpoint Detection and Response sẽ hiển thị thông tin chi tiết về việc phát hiện trong một cửa sổ riêng. *Chi tiết về phát hiện* là một công cụ để xem toàn bộ thông tin thu thập được về một mối đe dọa được phát hiện. Chi tiết về phát hiện bao gồm, ví dụ như lịch sử của các tập tin xuất hiện trên máy tính. Để biết chi tiết về việc quản lý thông tin chi tiết về phát hiện, hãy tham khảo [Trợ giúp của Kaspersky Endpoint Detection and Response Optimum](#) và [Trợ giúp của Kaspersky Endpoint Detection and Response Expert](#).

Kaspersky Endpoint Detection and Response sử dụng các công cụ Threat Intelligence sau:

- Cơ sở hạ tầng dịch vụ đám mây của Kaspersky Security Network (sau đây gọi là "KSN"), cung cấp quyền truy cập vào tập tin, trang web và thông tin danh tiếng phần mềm theo thời gian thực từ cơ sở tri thức của Kaspersky. Việc sử dụng dữ liệu từ Kaspersky Security Network đảm bảo thời gian phản ứng nhanh hơn cho các ứng dụng của Kaspersky 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. EDR Expert sử dụng giải pháp Kaspersky Private Security Network (KPSN), gửi dữ liệu đến các máy chủ khu vực mà không gửi dữ liệu từ các thiết bị đến KSN.
- Tích hợp với cổng thông tin [Kaspersky Threat Intelligence Portal](#), hệ thống này chứa và hiển thị thông tin về danh tiếng của các tập tin và địa chỉ web.
- Cơ sở dữ liệu về [Các mối đe dọa của Kaspersky](#).

Tích hợp với Kaspersky Endpoint Detection and Response

Để tích hợp với Kaspersky Endpoint Detection and Response, bạn phải thêm thành phần Endpoint Detection and Response Optimum (EDR Optimum) hoặc thành phần Endpoint Detection and Response Expert (EDR Expert) và cấu hình Kaspersky Endpoint Security.

Các thành phần EDR Optimum and EDR Expert không tương thích.

Phải đáp ứng các điều kiện sau đây để Endpoint Detection and Response hoạt động:

- Kaspersky Security Center 13.2. Không thể kích hoạt tính năng Endpoint Detection and Response trong các phiên bản trước của Kaspersky Security Center.
- Có thể quản lý EDR Optimum trong Bảng điều khiển web Kaspersky Security Center hoặc Bảng điều khiển đám mây Kaspersky Security Center. Chỉ có thể quản lý các tính năng của EDR Expert bằng

Bảng điều khiển web Kaspersky Security Center. Bạn không thể quản lý chức năng này bằng Bảng điều khiển quản trị (MMC).

- Ứng dụng được kích hoạt và chức năng được giấy phép hỗ trợ.
- Thành phần Endpoint Detection and Response được bật.
- Các thành phần ứng dụng mà Endpoint Detection and Response phụ thuộc sẽ được bật và hoạt động. Endpoint Detection and Response phụ thuộc vào các thành phần sau:
 - [Bảo vệ mối đe dọa tập tin.](#)
 - [Bảo vệ mối đe dọa web.](#)
 - [Bảo vệ mối đe dọa thư điện tử.](#)
 - [Phòng chống khai thác.](#)
 - [Phát hiện hành vi.](#)
 - [Phòng chống xâm nhập máy chủ.](#)
 - [Công cụ khắc phục.](#)
 - [Kiểm soát thích ứng sự cố.](#)

Tích hợp với thành phần Kaspersky Endpoint Detection and Response liên quan tới các bước sau:

1 Cài đặt các thành phần Endpoint Detection and Response

Bạn có thể chọn thành phần EDR Optimum hoặc EDR Expert trong quá trình [cài đặt](#) hoặc [nâng cấp](#), cũng như sử dụng *tác vụ* [Thay đổi thành phần ứng dụng](#).

Bạn phải khởi động lại máy tính của mình để hoàn tất việc nâng cấp ứng dụng với các thành phần mới.

2 Kích hoạt Kaspersky Endpoint Detection and Response

Bạn có thể lấy giấy phép để sử dụng Kaspersky Endpoint Detection and Response theo những cách sau:

- Chức năng Endpoint Detection and Response được kèm theo giấy phép của Kaspersky Endpoint Security cho Windows.

Tính năng này sẽ khả dụng ngay sau khi [kích hoạt Kaspersky Endpoint Security cho Windows](#).

- Mua một giấy phép riêng cho EDR Optimum hoặc EDR Expert (Tiện ích Kaspersky Endpoint Detection and Response).

Tính năng này sẽ khả dụng sau khi bạn thêm một khóa riêng cho Kaspersky Endpoint Detection and Response. Kết quả là hai khóa được cài đặt trên máy tính: một khóa dành cho Kaspersky Endpoint Security và một khóa dành cho Kaspersky Endpoint Detection and Response.

Việc cấp giấy phép cho chức năng Endpoint Detection and Response độc lập cũng giống như việc cấp giấy phép cho Kaspersky Endpoint Security.

Đảm bảo rằng chức năng EDR Optimum hoặc EDR Expert được gộp trong giấy phép và đang chạy trong [giao diện cục bộ của ứng dụng](#).

3 **Bật các thành phần Endpoint Detection and Response**

Bạn có thể bật hoặc tắt thành phần này trong thiết lập chính sách của Kaspersky Endpoint Security cho Windows.

[Cách bật hoặc tắt thành phần Endpoint Detection and Response trong Bảng điều khiển web và Bảng điều khiển đám mây](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Detection and Response** → **Endpoint Detection and Response**.
5. Bật nút bật/tắt **Endpoint Detection and Response**.
6. Lưu các thay đổi của bạn.

Thành phần Kaspersky Endpoint Detection and Response sẽ được bật. Kiểm tra trạng thái hoạt động của thành phần bằng cách xem *Báo cáo trạng thái thành phần ứng dụng*. Bạn cũng có thể xem trạng thái hoạt động của một thành phần trong mục [báo cáo](#) trong giao diện cục bộ của Kaspersky Endpoint Security. Thành phần **Endpoint Detection and Response Optimum** hoặc **Endpoint Detection and Response Expert** sẽ được thêm vào danh sách các thành phần của Kaspersky Endpoint Security.

4 **Cho phép truyền dữ liệu đến Máy chủ quản trị**

Để bật tất cả các tính năng Endpoint Detection and Response bạn phải cho phép truyền các loại dữ liệu sau:

- Dữ liệu của tập tin trong khu vực cách ly.

Đây là dữ liệu phải có để lấy thông tin về các tập tin được cách ly trên máy tính thông qua Bảng điều khiển web và Bảng điều khiển đám mây. Ví dụ: bạn có thể tải về một tập tin từ khu vực cách ly để phân tích trong Bảng điều khiển web và Bảng điều khiển đám mây.

- Dữ liệu chuỗi phát triển mối đe dọa.

Đây là dữ liệu phải có để lấy thông tin về các mối đe dọa được phát hiện trên máy tính trong Bảng điều khiển web và Bảng điều khiển đám mây. Bạn có thể xem chi tiết về phát hiện và thực hiện các hành động ứng phó trong Bảng điều khiển web và Bảng điều khiển đám mây.

[Cách bật truyền dữ liệu đến Máy chủ quản trị trong Bảng điều khiển web và Bảng điều khiển đám mây](#) 

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Thiết lập tổng quát** → **Các báo cáo và lưu trữ**.
5. Vui lòng chọn các ô sau trong mục **Truyền dữ liệu đến Máy chủ quản trị**:
 - **Thông tin về các tập tin trong Khu vực cách ly**
 - **Thông tin về một chuỗi phát triển mới đe dọa**
6. Lưu các thay đổi của bạn.

Chuyển sang từ Kaspersky Endpoint Agent

Nếu bạn đang sử dụng Kaspersky Endpoint Security 11.7.0 hoặc mới hơn với thành phần EDR Optimum (tác nhân tích hợp) được cài đặt thì việc hỗ trợ tích hợp với giải pháp Kaspersky Endpoint Detection and Response Optimum sẽ khả dụng ngay sau khi cài đặt. Thành phần EDR Optimum không tương thích với Kaspersky Endpoint Agent. Nếu Kaspersky Endpoint Agent được cài đặt trên máy tính, khi Kaspersky Endpoint Security được cập nhật lên phiên bản 11.7.0, Kaspersky Endpoint Detection and Response Optimum sẽ tiếp tục hoạt động với Kaspersky Endpoint Security ([chuyển đổi cấu hình \[KES+KEA\] sang \[KES+built-in agent\]](#)). Ngoài ra, Kaspersky Endpoint Agent sẽ bị gỡ bỏ khỏi máy tính. Để hoàn tất chuyển đổi từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security cho Windows, bạn cần chuyển thiết lập chính sách và tác vụ bằng [Trình hướng dẫn chuyển đổi](#).

Nếu bạn đang sử dụng Kaspersky Endpoint Security 11.4.0–11.6.0, để có khả năng tương tác với Kaspersky Endpoint Detection and Response Optimum, ứng dụng này sẽ bao gồm cả Kaspersky Endpoint Agent. Bạn có thể cài đặt Kaspersky Endpoint Agent để chạy cùng Kaspersky Endpoint Security.

Trong Kaspersky Endpoint Security 11.9.0, gói phân phối Kaspersky Endpoint Agent không còn thuộc gói phân phối Kaspersky Endpoint Security. Bạn phải tải xuống gói phân phối Kaspersky Endpoint Agent riêng.

Giải pháp Kaspersky Endpoint Detection and Response Expert không hỗ trợ khả năng tương tác với Kaspersky Endpoint Agent. Giải pháp Kaspersky Endpoint Detection and Response Expert sử dụng Kaspersky Endpoint Security tác nhân tích hợp (phiên bản 11.8.0 trở lên).

Thành phần EDR Optimum thuộc một phần của Kaspersky Endpoint Security sẽ hỗ trợ tương tác với giải pháp Kaspersky Endpoint Detection and Response Optimum 2.0. Tương tác với Kaspersky Endpoint Detection and Response Optimum phiên bản 1.0 không được hỗ trợ.

Quét các dấu hiệu về sự xâm nhập (tác vụ tiêu chuẩn)

Một *Dấu hiệu về sự xâm nhập (IOC)* là một tập hợp dữ liệu về một đối tượng hoặc hoạt động cho biết sự truy cập trái phép vào máy tính (xâm nhập dữ liệu). Ví dụ: nhiều nỗ lực đăng nhập không thành công vào hệ thống có thể cấu thành một Dấu hiệu về sự xâm nhập. Tác vụ *Quét IOC* cho phép tìm các Dấu hiệu về sự xâm nhập trên máy tính và thực hiện các biện pháp ứng phó với mỗi đe dọa.

Kaspersky Endpoint Security sẽ tìm kiếm các dấu hiệu về sự xâm nhập bằng cách sử dụng các tập tin IOC. *Tập tin IOC* là các tập tin chứa các tập hợp dấu hiệu mà ứng dụng cố gắng đối chiếu để đếm một lần phát hiện. Các tập tin IOC phải tuân theo [tiêu chuẩn OpenIOC](#).

Chế độ chạy tác vụ quét IOC

Kaspersky Endpoint Detection and Response cho phép bạn tạo các tác vụ Quét IOC tiêu chuẩn để phát hiện dữ liệu bị xâm nhập. *Tác vụ quét IOC tiêu chuẩn* là một nhóm hoặc tác vụ cục bộ được tạo và cấu hình theo cách thủ công trong Bảng điều khiển web. Các tác vụ được chạy bằng các tập tin IOC do người dùng chuẩn bị. Nếu bạn muốn thêm dấu hiệu về sự xâm nhập theo cách thủ công, vui lòng đọc [yêu cầu đối với các tập tin IOC](#).

Tập tin mà bạn có thể tải về bằng cách nhấn vào liên kết bên dưới, có chứa một bảng kèm danh sách đầy đủ các từ của tiêu chuẩn OpenIOC.

 [TẢI XUỐNG TẬP TIN IOC TERMS.XLSX](#)

Kaspersky Endpoint Security cũng hỗ trợ [tác vụ quét IOC độc lập](#) khi ứng dụng được sử dụng như một phần của giải pháp [Kaspersky Sandbox](#).

Tạo một tác vụ Quét IOC

Bạn có thể tạo các tác vụ *Quét IOC* theo cách thủ công:

- Chi tiết về cảnh báo (chỉ dành cho EDR Optimum).

Chi tiết về phát hiện là một công cụ để xem toàn bộ thông tin thu thập được về một mối đe dọa được phát hiện. Chi tiết về phát hiện bao gồm, ví dụ như lịch sử của các tập tin xuất hiện trên máy tính. Để biết chi tiết về việc quản lý thông tin chi tiết về phát hiện, hãy tham khảo [Trợ giúp của Kaspersky Endpoint Detection and Response Optimum](#) và [Trợ giúp của Kaspersky Endpoint Detection and Response Expert](#).

- Sử dụng Trình hướng dẫn Tác vụ.

Bạn có thể cấu hình tác vụ cho EDR Optimum trong Bảng điều khiển web và Bảng điều khiển đám mây. Thiết lập tác vụ cho EDR Expert chỉ khả dụng trong Bảng điều khiển đám mây.

Để tạo một tác vụ Quét IOC:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.
Danh sách tác vụ sẽ mở.
2. Nhấn vào nút **Thêm**.

Trình hướng dẫn Tác vụ sẽ được bắt đầu.

3. Cấu hình các thiết lập của tác vụ:

- a. Trong danh sách thả xuống **Ứng dụng**, hãy chọn **Kaspersky Endpoint Security cho Windows (11.9.0)**.
- b. Trong danh sách thả xuống **Loại tác vụ**, hãy chọn **Quét IOC**.
- c. Trong trường **Task name**, hãy nhập một mô tả ngắn.
- d. Trong phần **Select devices to which the task will be assigned**, chọn phạm vi tác vụ.

4. Chọn các thiết bị theo phạm vi tác vụ được chọn. Chuyển sang bước tiếp theo.

5. Nhập thông tin đăng nhập tài khoản của người dùng có quyền mà bạn muốn sử dụng để chạy tác vụ. Chuyển sang bước tiếp theo.

Theo mặc định, Kaspersky Endpoint Security sẽ khởi chạy tác vụ dưới quyền tài khoản người dùng hệ thống (SYSTEM).

Tài khoản hệ thống (SYSTEM) không có quyền thực hiện tác vụ *Quét IOC* trên các ổ đĩa mạng. Nếu bạn muốn chạy tác vụ cho một ổ đĩa mạng, hãy chọn tài khoản của người dùng có quyền truy cập vào ổ đĩa đó.

Đối với các tác vụ Quét IOC độc lập trên ổ đĩa mạng, trong thuộc tính của tác vụ, bạn cần chọn thủ công tài khoản người dùng có quyền truy cập vào ổ đĩa này.

6. Thoát Trình hướng dẫn.

Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ.

7. Nhấn tác vụ mới.

Cửa sổ thuộc tính tác vụ sẽ được mở ra.

8. Chọn thẻ **Application settings**.

9. Vào mục **Thiết lập quét IOC**.

10. Tải các tập tin IOC để tìm kiếm các dấu hiệu về sự xâm nhập.

Sau khi tải các tập tin IOC, bạn có thể xem danh sách các chỉ số trong các tập tin IOC.

Không nên thêm hoặc xóa tập tin IOC sau khi chạy tác vụ. Làm vậy có thể khiến kết quả quét IOC hiển thị không chính xác cho các lần chạy tác vụ trước đó. Để tìm kiếm các dấu hiệu về sự xâm nhập bằng các tập tin IOC mới, bạn nên thêm các tác vụ mới.

11. Cấu hình các hành động khi phát hiện IOC:

- **Isolate computer from the network**. Nếu chọn tùy chọn này, Kaspersky Endpoint Security sẽ cách ly máy tính khỏi mạng để ngăn chặn mối đe dọa lây lan. Bạn có thể cấu hình thời gian cách ly trong [thiết lập thành phần Endpoint Detection and Response](#).

- **Di chuyển bản sao vào Khu vực cách ly, xóa đối tượng.** Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ xóa đối tượng độc hại được tìm thấy trên máy tính. Trước khi xóa đối tượng, Kaspersky Endpoint Security sẽ tạo một bản sao lưu trong trường hợp đối tượng cần được khôi phục sau này. Kaspersky Endpoint Security sẽ di chuyển bản sao lưu vào Khu vực cách ly.
- **Chạy tác vụ quét các khu vực quan trọng.** Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ chạy tác vụ [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.

12. Vào mục **Nâng cao**.

13. Chọn loại dữ liệu (tài liệu IOC) cần phải được phân tích thuộc một phần của tác vụ.

Kaspersky Endpoint Security sẽ tự động chọn loại dữ liệu (tài liệu IOC) cho tác vụ *Quét IOC* theo nội dung của các tập tin IOC được nạp. Bạn không nên bỏ chọn các loại dữ liệu.

Bạn có thể cấu hình thêm các phạm vi quét cho các loại dữ liệu sau:

- **Files - FileItem.** Đặt một phạm vi quét IOC trên máy tính sử dụng các phạm vi quét định sẵn. Theo mặc định, Kaspersky Endpoint Security sẽ chỉ quét các IOC trong các khu vực quan trọng của máy tính như thư mục Downloads, thư mục Desktop, thư mục chứa các tập tin tạm thời của hệ điều hành, v.v. Bạn cũng có thể thêm phạm vi quét theo cách thủ công.
- **Windows event logs - EventLogItem.** Nhập khoảng thời gian khi các sự kiện được ghi nhật ký. Bạn cũng có thể lựa chọn nhật ký sự kiện Windows nào phải được sử dụng để quét IOC. Theo mặc định, các nhật ký sự kiện sau sẽ được lựa chọn: nhật ký sự kiện ứng dụng, nhật ký sự kiện hệ thống và nhật ký sự kiện bảo mật.

Với loại dữ liệu **Windows registry - RegistryItem**, Kaspersky Endpoint Security sẽ quét [một tập hợp các khóa registry](#).

14. Trong cửa sổ thuộc tính tác vụ, hãy chọn thẻ **Lịch**.

15. Cấu hình lịch tác vụ.

Wake-on-LAN không khả dụng cho tác vụ này. Đảm bảo rằng máy tính được bật để chạy tác vụ.

16. Lưu các thay đổi của bạn.

17. Chọn hộp kiểm cạnh tác vụ.

18. Nhấn vào nút **Chạy**.

Kết quả là Kaspersky Endpoint Security sẽ chạy lệnh tìm kiếm các dấu hiệu về sự xâm nhập trên máy tính. Bạn có thể xem kết quả tác vụ trong các thuộc tính tác vụ trong mục **Kết quả**. Bạn có thể xem thông tin về các dấu hiệu về sự xâm nhập được phát hiện trong thuộc tính của tác vụ: **Application settings** → **IOC Scan Results**.

Kết quả quét IOC được lưu trong vòng 30 ngày. Sau khoảng thời gian này, Kaspersky Endpoint Security sẽ tự động xóa các mục cũ nhất.

Di chuyển tập tin đến Khu vực cách ly

Khi phản ứng với các mối đe dọa, Kaspersky Endpoint Detection and Response Optimum có thể tạo các tác vụ *Di chuyển tập tin đến Khu vực cách ly*. Đây là điều cần thiết để giảm thiểu hậu quả của mối đe dọa. *Khu vực cách ly* là một kho lưu trữ cục bộ đặc biệt trên máy tính. Người dùng có thể cách ly các tập tin mà người dùng coi là nguy hiểm cho máy tính. Các tập tin cách ly được lưu trữ ở trạng thái mã hóa và không đe dọa đến tính bảo mật của thiết bị. Kaspersky Endpoint Security chỉ sử dụng Khu vực cách ly khi làm việc với các giải pháp Kaspersky Sandbox và Kaspersky Endpoint Detection and Response. Trong các trường hợp khác, Kaspersky Endpoint Security sẽ đặt các tập tin liên quan vào [Sao lưu](#). Để biết chi tiết về quản lý khu vực cách ly làm một phần của các giải pháp, vui lòng tham khảo [Trợ giúp của Kaspersky Sandbox](#), [Trợ giúp của Kaspersky Endpoint Detection and Response Optimum](#) và [Trợ giúp của Kaspersky Endpoint Detection and Response Expert](#).

Bạn có thể tạo các tác vụ *Di chuyển tập tin đến Khu vực cách ly* theo những cách sau:

- Chi tiết về cảnh báo (chỉ dành cho EDR Optimum).

Chi tiết về phát hiện là một công cụ để xem toàn bộ thông tin thu thập được về một mối đe dọa được phát hiện. Chi tiết về phát hiện bao gồm, ví dụ như lịch sử của các tập tin xuất hiện trên máy tính. Để biết chi tiết về việc quản lý thông tin chi tiết về phát hiện, hãy tham khảo [Trợ giúp của Kaspersky Endpoint Detection and Response Optimum](#) và [Trợ giúp của Kaspersky Endpoint Detection and Response Expert](#).

- Sử dụng Trình hướng dẫn Tác vụ.

Bạn phải nhập đường dẫn hoặc giá trị hash (SHA256 hoặc MD5) của tập tin, hoặc cả đường dẫn tập tin và giá trị hash của tập tin.

Tác vụ *Di chuyển tập tin vào Khu vực cách ly* có những hạn chế sau:

1. Kích thước tập tin không được vượt quá 100 MB.
2. Không thể cách ly Đối tượng hệ thống quan trọng (SCO). SCO là các tập tin mà hệ điều hành và ứng dụng Kaspersky Endpoint Security cho Windows phải có để có thể chạy.
3. Bạn có thể cấu hình tác vụ cho EDR Optimum trong Bảng điều khiển web và Bảng điều khiển đám mây. Thiết lập tác vụ cho EDR Expert chỉ khả dụng trong Bảng điều khiển đám mây.

Để tạo một tác vụ *Di chuyển tập tin đến Khu vực cách ly*:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.

Danh sách tác vụ sẽ mở.

2. Nhấn vào nút **Thêm**.

Trình hướng dẫn Tác vụ sẽ được bắt đầu.

3. Cấu hình các thiết lập của tác vụ:

- a. Trong danh sách thả xuống **Ứng dụng**, hãy chọn **Kaspersky Endpoint Security cho Windows (11.9.0)**.

- b. Trong danh sách thả xuống **Loại tác vụ**, hãy chọn **Move file to Quarantine**.

- c. Trong trường **Task name**, hãy nhập một mô tả ngắn.

d. Trong phần **Select devices to which the task will be assigned**, chọn phạm vi tác vụ.

4. Chọn các thiết bị theo phạm vi tác vụ được chọn. Nhấn nút **Tiếp theo**.

5. Nhập thông tin đăng nhập tài khoản của người dùng có quyền mà bạn muốn sử dụng để chạy tác vụ. Nhấn nút **Tiếp theo**.

Theo mặc định, Kaspersky Endpoint Security sẽ khởi chạy tác vụ dưới quyền tài khoản người dùng hệ thống (SYSTEM).

6. Hoàn tất trình hướng dẫn bằng cách nhấn nút **Hoàn tất**.

Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ.

7. Nhấn tác vụ mới.

Cửa sổ thuộc tính tác vụ sẽ được mở ra.

8. Chọn thẻ **Application settings**.

9. Trong danh sách tập tin, hãy nhấn vào **Thêm**.

Trình hướng dẫn thêm tập tin sẽ khởi chạy.

10. Để thêm tập tin, bạn phải nhập đường dẫn đầy đủ đến tập tin hoặc cả giá trị hash và đường dẫn.

Nếu tập tin nằm trên ổ đĩa mạng, hãy nhập đường dẫn tập tin bắt đầu bằng `\\`, không phải bằng ký tự ổ đĩa. Ví dụ: `\\server\shared_folder\file.exe`. Nếu đường dẫn tập tin chứa ký tự ổ đĩa mạng, bạn có thể nhận được lỗi *Không tìm thấy tập tin*.

11. Trong cửa sổ thuộc tính tác vụ, hãy chọn thẻ **Lịch**.

12. Cấu hình lịch tác vụ.

Wake-on-LAN không khả dụng cho tác vụ này. Đảm bảo rằng máy tính được bật để chạy tác vụ.

13. Nhấp vào nút **Lưu**.

14. Chọn hộp kiểm cạnh tác vụ.

15. Nhấn vào nút **Chạy**.

Kết quả là Kaspersky Endpoint Security sẽ di chuyển tập tin đó đến Khu vực cách ly. Nếu tập tin bị khóa bởi một tiến trình khác, tác vụ sẽ được hiển thị dưới dạng *Hoàn thành*, nhưng bản thân tập tin chỉ bị cách ly sau khi máy tính được khởi động lại. Sau khi khởi động lại máy tính, hãy xác nhận rằng tập tin đã bị xóa.

Tác vụ *Di chuyển tập tin đến Khu vực cách ly* có thể hoàn thành với lỗi *Truy cập bị từ chối* nếu bạn đang cố gắng cách ly một tập tin thực thi hiện đang chạy. [Tạo một tác vụ chấm dứt tiến trình](#) cho tập tin và thử lại.

Tác vụ *Di chuyển tập tin đến Khu vực cách ly* có thể thất bại kèm theo lỗi *Không đủ dung lượng trống trong kho lưu trữ của Khu vực cách ly* nếu bạn đang cố cách ly một tập tin quá lớn. Hãy làm trống Khu vực cách ly hoặc [tăng dung lượng lưu trữ của Khu vực cách ly](#). Sau đó thử lại.

Bạn có thể khôi phục tập tin từ Khu vực cách ly hoặc làm trống Khu vực cách ly bằng Bảng điều khiển web. Bạn có thể khôi phục cục bộ các đối tượng trên máy tính bằng cách sử dụng [dòng lệnh](#).

Lấy tập tin

Bạn có thể lấy tập tin từ máy tính của người dùng. Ví dụ: bạn có thể cấu hình để lấy tập tin nhật ký sự kiện do ứng dụng của bên thứ ba tạo. Để lấy tập tin, bạn phải tạo một tác vụ chuyên dụng. Kết quả của việc thực hiện tác vụ là tập tin được lưu trong Khu vực cách ly. Bạn có thể tải tập tin này từ Khu vực cách ly xuống máy tính của mình bằng Bảng điều khiển web. Trên máy tính của người dùng, tập tin vẫn nằm trong thư mục gốc của nó.

Kích thước tập tin không được vượt quá 100 MB.

Bạn có thể cấu hình tác vụ cho EDR Optimum trong Bảng điều khiển web và Bảng điều khiển đám mây. Thiết lập tác vụ cho EDR Expert chỉ khả dụng trong Bảng điều khiển đám mây.

Để tạo tác vụ Lấy tập tin:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.
Danh sách tác vụ sẽ mở.
2. Nhấn vào nút **Thêm**.
Trình hướng dẫn Tác vụ sẽ được bắt đầu.
3. Cấu hình các thiết lập của tác vụ:
 - a. Trong danh sách thả xuống **Ứng dụng**, hãy chọn **Kaspersky Endpoint Security cho Windows (11.9.0)**.
 - b. Trong danh sách thả xuống **Loại tác vụ**, hãy chọn **Lấy tập tin**.
 - c. Trong trường **Task name**, hãy nhập một mô tả ngắn.
 - d. Trong phần **Select devices to which the task will be assigned**, chọn phạm vi tác vụ.
4. Chọn các thiết bị theo phạm vi tác vụ được chọn. Nhấn nút **Tiếp theo**.
5. Nhập thông tin đăng nhập tài khoản của người dùng có quyền mà bạn muốn sử dụng để chạy tác vụ. Nhấn nút **Tiếp theo**.

Theo mặc định, Kaspersky Endpoint Security sẽ khởi chạy tác vụ dưới quyền tài khoản người dùng hệ thống (SYSTEM).

6. Hoàn tất trình hướng dẫn bằng cách nhấn nút **Hoàn tất**.
Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ.
7. Nhấn tác vụ mới.
Cửa sổ thuộc tính tác vụ sẽ được mở ra.

8. Chọn thẻ **Application settings**.

9. Trong danh sách tập tin, hãy nhấn vào **Thêm**.

Trình hướng dẫn thêm tập tin sẽ khởi chạy.

10. Để thêm tập tin, bạn phải nhập đường dẫn đầy đủ đến tập tin hoặc cả giá trị hash và đường dẫn.

Nếu tập tin nằm trên ổ đĩa mạng, hãy nhập đường dẫn tập tin bắt đầu bằng `\\`, không phải bằng ký tự ổ đĩa. Ví dụ: `\\server\shared_folder\file.exe`. Nếu đường dẫn tập tin chứa ký tự ổ đĩa mạng, bạn có thể nhận được lỗi *Không tìm thấy tập tin*.

11. Trong cửa sổ thuộc tính tác vụ, hãy chọn thẻ **Lịch**.

12. Cấu hình lịch tác vụ.

Wake-on-LAN không khả dụng cho tác vụ này. Đảm bảo rằng máy tính được bật để chạy tác vụ.

13. Nhấp vào nút **Lưu**.

14. Chọn hộp kiểm cạnh tác vụ.

15. Nhấn vào nút **Chạy**.

Kết quả là Kaspersky Endpoint Security sẽ tạo một bản sao của tập tin và di chuyển bản sao đó đến Khu vực cách ly. Bạn có thể tải xuống tập tin từ Khu vực cách ly trong Bảng điều khiển web.

Xóa tập tin

Bạn có thể xóa tập tin từ xa bằng cách sử dụng tác vụ *Xóa tập tin*. Ví dụ: bạn có thể xóa từ xa một tập tin khi ứng phó với các mối đe dọa.

Tác vụ *Xóa tập tin* có những hạn chế sau:

- Không thể xóa Đối tượng hệ thống quan trọng (SCO). SCO là các tập tin mà hệ điều hành và ứng dụng Kaspersky Endpoint Security cho Windows phải có để có thể chạy.
- Bạn có thể cấu hình tác vụ cho EDR Optimum trong Bảng điều khiển web và Bảng điều khiển đám mây. Thiết lập tác vụ cho EDR Expert chỉ khả dụng trong Bảng điều khiển đám mây.

Để tạo tác vụ *Xóa tập tin*:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.

Danh sách tác vụ sẽ mở.

2. Nhấn vào nút **Thêm**.

Trình hướng dẫn Tác vụ sẽ được bắt đầu.

3. Cấu hình các thiết lập của tác vụ:

- a. Trong danh sách thả xuống **Ứng dụng**, hãy chọn **Kaspersky Endpoint Security cho Windows (11.9.0)**.

- b. Trong danh sách thả xuống **Loại tác vụ**, hãy chọn **Delete file**.
 - c. Trong trường **Task name**, hãy nhập một mô tả ngắn.
 - d. Trong phần **Select devices to which the task will be assigned**, chọn phạm vi tác vụ.
4. Chọn các thiết bị theo phạm vi tác vụ được chọn. Nhấn nút **Tiếp theo**.
5. Nhập thông tin đăng nhập tài khoản của người dùng có quyền mà bạn muốn sử dụng để chạy tác vụ. Nhấn nút **Tiếp theo**.

Theo mặc định, Kaspersky Endpoint Security sẽ khởi chạy tác vụ dưới quyền tài khoản người dùng hệ thống (SYSTEM).

6. Hoàn tất trình hướng dẫn bằng cách nhấn nút **Hoàn tất**.
Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ.
7. Nhấn tác vụ mới.
Cửa sổ thuộc tính tác vụ sẽ được mở ra.
8. Chọn thẻ **Application settings**.
9. Trong danh sách tập tin, hãy nhấn vào **Thêm**.
Trình hướng dẫn thêm tập tin sẽ khởi chạy.
10. Để thêm tập tin, bạn phải nhập đường dẫn đầy đủ đến tập tin hoặc cả giá trị hash và đường dẫn.

Nếu tập tin nằm trên ổ đĩa mạng, hãy nhập đường dẫn tập tin bắt đầu bằng `\\`, không phải bằng ký tự ổ đĩa. Ví dụ: `\\server\shared_folder\file.exe`. Nếu đường dẫn tập tin chứa ký tự ổ đĩa mạng, bạn có thể nhận được lỗi *Không tìm thấy tập tin*.

11. Trong cửa sổ thuộc tính tác vụ, hãy chọn thẻ **Lịch**.
12. Cấu hình lịch tác vụ.

Wake-on-LAN không khả dụng cho tác vụ này. Đảm bảo rằng máy tính được bật để chạy tác vụ.

13. Nhấp vào nút **Lưu**.
14. Chọn hộp kiểm cạnh tác vụ.
15. Nhấn vào nút **Chạy**.

Kết quả là Kaspersky Endpoint Security sẽ xóa tập tin khỏi máy tính. Nếu tập tin bị khóa bởi một tiến trình khác, tác vụ sẽ được hiển thị dưới dạng *Hoàn thành*, nhưng bản thân tập tin chỉ bị xóa sau khi máy tính được khởi động lại. Sau khi khởi động lại máy tính, hãy xác nhận rằng tập tin đã bị xóa.

Tác vụ *Xóa tập tin* có thể hoàn thành với lỗi *Truy cập bị từ chối* nếu bạn đang cố gắng cách ly một tập tin thực thi hiện đang chạy. [Tạo một tác vụ chấm dứt tiến trình](#) cho tập tin và thử lại.

Khởi chạy tiến trình

Bạn có thể chạy các tập tin từ xa bằng cách sử dụng tác vụ *Khởi chạy tiến trình*. Ví dụ: bạn có thể chạy tiện ích tạo tập tin cấu hình máy tính từ xa. Tiếp theo, bạn có thể sử dụng [tác vụ *Lấy tập tin*](#) để nhận tập tin đã tạo trong Bảng điều khiển web Kaspersky Security Center.

Bạn có thể cấu hình tác vụ cho EDR Optimum trong Bảng điều khiển web và Bảng điều khiển đám mây. Thiết lập tác vụ cho EDR Expert chỉ khả dụng trong Bảng điều khiển đám mây.

Để tạo một tác vụ *Khởi chạy tiến trình*:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.
Danh sách tác vụ sẽ mở.
2. Nhấn vào nút **Thêm**.
Trình hướng dẫn Tác vụ sẽ được bắt đầu.
3. Cấu hình các thiết lập của tác vụ:
 - a. Trong danh sách thả xuống **Ứng dụng**, hãy chọn **Kaspersky Endpoint Security cho Windows (11.9.0)**.
 - b. Trong danh sách thả xuống **Loại tác vụ**, hãy chọn **Process start**.
 - c. Trong trường **Task name**, hãy nhập một mô tả ngắn.
 - d. Trong phần **Select devices to which the task will be assigned**, chọn phạm vi tác vụ.
4. Chọn các thiết bị theo phạm vi tác vụ được chọn. Nhấn nút **Tiếp theo**.
5. Nhập thông tin đăng nhập tài khoản của người dùng có quyền mà bạn muốn sử dụng để chạy tác vụ. Nhấn nút **Tiếp theo**.

Theo mặc định, Kaspersky Endpoint Security sẽ khởi chạy tác vụ dưới quyền tài khoản người dùng hệ thống (SYSTEM).

6. Hoàn tất trình hướng dẫn bằng cách nhấn nút **Hoàn tất**.
Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ.
7. Nhấn tác vụ mới.
8. Cửa sổ thuộc tính tác vụ sẽ được mở ra.
9. Chọn thẻ **Application settings**.
10. Nhập lệnh khởi chạy tiến trình.
Ví dụ: nếu bạn muốn chạy một tiện ích (*utility.exe*) lưu thông tin về cấu hình của máy tính vào một tập tin có tên *conf.txt*, bạn phải nhập các giá trị sau:

- **Executable command** – utility.exe
- **Command-line arguments** – /R conf.txt
- **Path to the working folder** – C:\Users\admin\Diagnostic\

Ngoài ra, trong trường **Executable command** trường, bạn có thể nhập C:\Users\admin\Diagnostic\utility.exe /R conf.txt. Trong trường hợp này, bạn không cần nhập phần còn lại của thiết lập.

11. Trong cửa sổ thuộc tính tác vụ, hãy chọn thẻ **Lịch**.

12. Cấu hình lịch tác vụ.

Wake-on-LAN không khả dụng cho tác vụ này. Đảm bảo rằng máy tính được bật để chạy tác vụ.

13. Nhấp vào nút **Lưu**.

14. Chọn hộp kiểm cạnh tác vụ.

15. Nhấn vào nút **Chạy**.

Kết quả là Kaspersky Endpoint Security sẽ chạy lệnh trong chế độ im lặng và khởi chạy tiến trình. Bạn có thể xem kết quả tác vụ trong các thuộc tính tác vụ trong mục **Kết quả**.

Chấm dứt tiến trình

Bạn có thể chấm dứt các tiến trình từ xa bằng cách sử dụng tác vụ *Chấm dứt tiến trình*. Ví dụ: bạn có thể chấm dứt từ xa tiện ích kiểm tra tốc độ Internet đã được khởi chạy bằng [tác vụ Khởi chạy tiến trình](#).

Nếu bạn muốn cấm chạy một tập tin, bạn có thể cấu hình [thành phần Phòng chống thực thi](#). Bạn có thể cấm thực thi các tập tin thực thi, tập lệnh, tập tin định dạng văn phòng.

Tác vụ *Chấm dứt tiến trình* có những hạn chế sau:

- Không thể chấm dứt các tiến trình của Đối tượng hệ thống quan trọng (SCO). SCO là các tập tin mà hệ điều hành và ứng dụng Kaspersky Endpoint Security cho Windows phải có để có thể chạy.
- Bạn có thể cấu hình tác vụ cho EDR Optimum trong Bảng điều khiển web và Bảng điều khiển đám mây. Thiết lập tác vụ cho EDR Expert chỉ khả dụng trong Bảng điều khiển đám mây.

Để tạo một tác vụ Chấm dứt tiến trình:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.

Danh sách tác vụ sẽ mở.

2. Nhấn vào nút **Thêm**.

Trình hướng dẫn Tác vụ sẽ được bắt đầu.

3. Cấu hình các thiết lập của tác vụ:

- a. Trong danh sách thả xuống **Ứng dụng**, hãy chọn **Kaspersky Endpoint Security cho Windows (11.9.0)**.
 - b. Trong danh sách thả xuống **Loại tác vụ**, hãy chọn **Chấm dứt tiến trình**.
 - c. Trong trường **Task name**, hãy nhập một mô tả ngắn.
 - d. Trong phần **Select devices to which the task will be assigned**, chọn phạm vi tác vụ.
4. Chọn các thiết bị theo phạm vi tác vụ được chọn. Nhấn nút **Tiếp theo**.
 5. Nhập thông tin đăng nhập tài khoản của người dùng có quyền mà bạn muốn sử dụng để chạy tác vụ. Nhấn nút **Tiếp theo**.

Theo mặc định, Kaspersky Endpoint Security sẽ khởi chạy tác vụ dưới quyền tài khoản người dùng hệ thống (SYSTEM).

6. Hoàn tất trình hướng dẫn bằng cách nhấn nút **Hoàn tất**.
Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ.
7. Nhấn tác vụ mới.
Cửa sổ thuộc tính tác vụ sẽ được mở ra.
8. Chọn thẻ **Application settings**.
9. Để hoàn tất tiến trình, bạn phải chọn tập tin mà bạn muốn chấm dứt. Bạn có thể chọn một tập tin theo một trong những cách sau đây:
 - Nhập tên đầy đủ tới tập tin.
 - Nhập giá trị băm của tập tin và đường dẫn đến tập tin.
 - Nhập PID của tiến trình (chỉ dành cho các tác vụ cục bộ).

Nếu tập tin nằm trên ổ đĩa mạng, hãy nhập đường dẫn tập tin bắt đầu bằng `\\`, không phải bằng ký tự ổ đĩa. Ví dụ: `\\server\shared_folder\file.exe`. Nếu đường dẫn tập tin chứa ký tự ổ đĩa mạng, bạn có thể nhận được lỗi *Không tìm thấy tập tin*.

10. Trong cửa sổ thuộc tính tác vụ, hãy chọn thẻ **Lịch**.
11. Cấu hình lịch tác vụ.

Wake-on-LAN không khả dụng cho tác vụ này. Đảm bảo rằng máy tính được bật để chạy tác vụ.

12. Nhấp vào nút **Lưu**.
13. Chọn hộp kiểm cạnh tác vụ.
14. Nhấn vào nút **Chạy**.

Kết quả là Kaspersky Endpoint Security sẽ chấm dứt tiến trình đó trên máy tính. Ví dụ: nếu một ứng dụng 'GAME' đang chạy và bạn muốn chấm dứt tiến trình game.exe thì ứng dụng sẽ bị đóng mà không lưu dữ liệu. Bạn có thể xem kết quả tác vụ trong các thuộc tính tác vụ trong mục **Kết quả**.

Phòng chống thực thi

Phòng chống thực thi cho phép quản lý việc chạy các tập tin thực thi và tập lệnh, cũng như mở các tập tin định dạng văn phòng. Ví dụ, bằng cách này, bạn có thể phòng chống thực thi các ứng dụng mà bạn cho là không bảo mật. Do đó, việc phát tán mối đe dọa có thể được ngăn chặn. Phòng chống thực thi hỗ trợ [một tập hợp các phần mở rộng tập tin văn phòng](#) và [một tập hợp các trình thông dịch tập lệnh](#).

Quy tắc phòng chống thực thi

Phòng chống thực thi quản lý quyền truy cập của người dùng vào các tập tin bằng các quy tắc phòng chống thực thi. *Quy tắc phòng chống thực thi* là một tập hợp các tiêu chí mà ứng dụng xem xét khi phản ứng với hoạt động thực thi đối tượng, ví dụ khi chặn thực thi đối tượng. Ứng dụng xác định các tập tin bằng đường dẫn hoặc giá trị tổng kiểm của chúng được tính bằng thuật toán băm MD5 và SHA256.

Bạn có thể tạo các Quy tắc phòng chống thực thi:

- Chi tiết về cảnh báo (chỉ dành cho EDR Optimum).

Chi tiết về phát hiện là một công cụ để xem toàn bộ thông tin thu thập được về một mối đe dọa được phát hiện. Chi tiết về phát hiện bao gồm, ví dụ như lịch sử của các tập tin xuất hiện trên máy tính. Để biết chi tiết về việc quản lý thông tin chi tiết về phát hiện, hãy tham khảo [Trợ giúp của Kaspersky Endpoint Detection and Response Optimum](#) và [Trợ giúp của Kaspersky Endpoint Detection and Response Expert](#).

- Sử dụng một chính sách nhóm hoặc thiết lập ứng dụng cục bộ.

Bạn phải nhập đường dẫn hoặc giá trị hash (SHA256 hoặc MD5) của tập tin, hoặc cả đường dẫn tập tin và giá trị hash của tập tin.

Bạn cũng có thể quản lý Phòng chống thực thi cục bộ bằng [dòng lệnh](#).

Bạn không nên tạo nhiều hơn 5000 quy tắc ngăn chặn chạy vì điều này có thể khiến hệ thống không ổn định.

Các quy tắc phòng chống không hỗ trợ tập tin trên đĩa CD hoặc trong tập tin ảnh ISO. Ứng dụng không chặn thực thi hoặc mở các tập tin này.

Các chế độ của Quy tắc phòng chống thực thi

Thành phần Phòng chống thực thi có thể hoạt động ở hai chế độ:

- **Chỉ thống kê.**

Trong chế độ này, Kaspersky Endpoint Security sẽ phát hành một sự kiện về nỗ lực chạy các đối tượng thực thi hoặc mở tài liệu đáp ứng với tiêu chí quy tắc ngăn chặn vào nhật ký sự kiện Windows và Kaspersky Security Center, nhưng không chặn nỗ lực chạy hoặc mở đối tượng hoặc tài liệu. Chế độ này được chọn theo mặc định.

- **Hoạt động.**

Trong chế độ này, ứng dụng chặn việc thực thi các đối tượng hoặc mở các tài liệu đáp ứng với tiêu chí quy tắc ngăn chặn. Ứng dụng cũng phát hành một sự kiện về nỗ lực thực thi các đối tượng hoặc mở tài liệu vào nhật ký sự kiện Windows và nhật ký sự kiện của Kaspersky Security Center.

Quản lý phòng chống thực thi

Bạn có thể cấu hình thiết lập của thành phần trong Bảng điều khiển web.

Để phòng chống thực thi:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Detection and Response** → **Endpoint Detection and Response**.
5. Sử dụng nút bật/tắt **Phòng chống thực thi** để bật hoặc tắt thành phần.
6. Trong mục **Action on execution or opening of forbidden object**, hãy chọn chế độ hoạt động của thành phần:
 - **Block and write to report.** Trong chế độ này, ứng dụng chặn việc thực thi các đối tượng hoặc mở các tài liệu đáp ứng với tiêu chí quy tắc ngăn chặn. Ứng dụng cũng phát hành một sự kiện về nỗ lực thực thi các đối tượng hoặc mở tài liệu vào nhật ký sự kiện Windows và nhật ký sự kiện của Kaspersky Security Center.
 - **Log events only.** Trong chế độ này, Kaspersky Endpoint Security sẽ phát hành một sự kiện về nỗ lực chạy các đối tượng thực thi hoặc mở tài liệu đáp ứng với tiêu chí quy tắc ngăn chặn vào nhật ký sự kiện Windows và Kaspersky Security Center, nhưng không chặn nỗ lực chạy hoặc mở đối tượng hoặc tài liệu. Chế độ này được chọn theo mặc định.
7. Tạo danh sách các quy tắc phòng chống thực thi:
 - a. Nhấn vào nút **Thêm**.
 - b. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ này, hãy nhập tên của quy tắc phòng chống thực thi (ví dụ: *Ứng dụng A*).
 - c. Trong danh sách thả xuống **Loại**, hãy chọn đối tượng mà bạn muốn chặn: **Executable file, Tập lệnh, Microsoft Office document**.
Nếu bạn chọn sai loại đối tượng, Kaspersky Endpoint Security sẽ không chặn tập tin hoặc tập lệnh.
 - d. Để thêm tập tin, bạn phải nhập giá trị hash (SHA256 hoặc MD5) của tập tin, đường dẫn đầy đủ đến tập tin hoặc cả giá trị hash và đường dẫn.

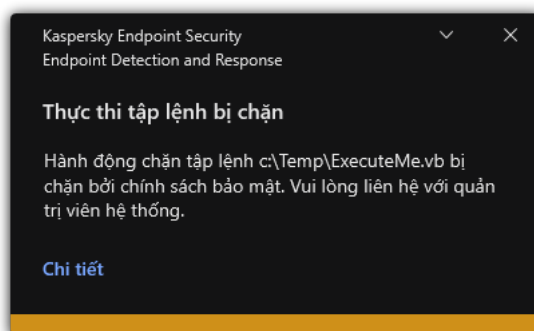
Nếu tập tin nằm trên ổ đĩa mạng, hãy nhập đường dẫn tập tin bắt đầu bằng \\, không phải bằng ký tự ổ đĩa. Ví dụ: \\server\shared_folder\file.exe. Nếu đường dẫn tập tin chứa một chữ cái ổ đĩa mạng, Kaspersky Endpoint Security sẽ không chặn tập tin hoặc tập lệnh.

Phòng chống thực thi hỗ trợ [một tập hợp các phần mở rộng tập tin văn phòng](#) và [một tập hợp các trình thông dịch tập lệnh](#).

e. Nhấn **OK**.

8. Lưu các thay đổi của bạn.

Kết quả là Kaspersky Endpoint Security sẽ chặn hoạt động thực thi của các đối tượng: chạy tập tin thực thi và tập lệnh, mở tập tin định dạng văn phòng. Tuy nhiên, bạn có thể mở tập tin tập lệnh trong trình biên tập văn bản ngay cả khi tập lệnh bị ngăn chặn. Khi chặn thực thi một đối tượng, Kaspersky Endpoint Security sẽ hiển thị một thông báo tiêu chuẩn (xem hình bên dưới) nếu các thông báo [được bật trong thiết lập ứng dụng](#).



Thông báo Phòng chống thực thi

Cách ly mạng máy tính

Cách ly mạng máy tính cho phép tự động cách ly một máy tính khỏi mạng để ứng phó với việc phát hiện một dấu hiệu về sự xâm nhập (IOC) – đây là *chế độ tự động*. Bạn có thể bật tính năng Cách ly mạng theo cách thủ công khi đang điều tra về mối đe dọa được phát hiện – đây là *chế độ thủ công*.

Khi bật chế độ Cách ly mạng, ứng dụng sẽ cắt tất cả các kết nối đang hoạt động và chặn tất cả các kết nối mạng TCP/IP mới trên máy tính, ngoại trừ các kết nối sau:

- Các kết nối được liệt kê trong loại trừ Cách ly mạng.
- Các kết nối được khởi tạo bởi các dịch vụ Kaspersky Endpoint Security.
- Các kết nối được khởi tạo bởi Kaspersky Security Center Network Agent.

Bạn có thể cấu hình thiết lập của thành phần trong Bảng điều khiển web.

Chế độ Cách ly mạng tự động

Bạn có thể cấu hình Cách ly mạng để được bật tự động nhằm ứng phó với việc phát hiện một dấu hiệu IOC. Bạn có thể cấu hình chế độ Cách ly mạng tự động bằng chính sách nhóm.

Cách cấu hình Cách ly mạng để được bật tự động nhằm ứng phó với việc phát hiện một dấu hiệu IOC

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.
Danh sách tác vụ sẽ mở.
2. Nhấn vào tác vụ **IOC Scan** của Kaspersky Endpoint Security.
Cửa sổ thuộc tính tác vụ sẽ được mở ra.
Nếu cần, hãy tạo một tác vụ [Quét IOC](#).
3. Chọn thẻ **Application settings**.
4. Trong mục **Action on IOC detection**, hãy chọn các hộp kiểm **Take response actions after an IOC is found** và **Isolate computer from the network**.
5. Lưu các thay đổi của bạn.

Kết quả là khi phát hiện ra IOC, ứng dụng sẽ cách ly máy tính khỏi mạng để ngăn chặn mối đe dọa lây lan.

Bạn có thể cấu hình Cách ly mạng để bị tắt tự động sau khi kết thúc một khoảng thời gian được chỉ định. Theo mặc định, ứng dụng sẽ tắt Cách ly mạng sau 8 giờ kể từ thời điểm tính năng này được bật. Bạn cũng có thể tắt Cách ly mạng theo cách thủ công (xem hướng dẫn bên dưới). Sau khi tắt Cách ly mạng, máy tính có thể sử dụng Mạng mà không bị hạn chế.

Cách cấu hình thời gian trì hoãn để tắt Cách ly mạng của một máy tính

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Detection and Response** → **Endpoint Detection and Response**.
5. Trong mục **Network isolation**, hãy nhấn vào **Configure computer unlock settings**.
6. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ này, hãy chọn hộp kiểm **Automatically unlock isolated computer in N giờ** và nhập thời gian trì hoãn để tự động tắt Cách ly mạng.
7. Lưu các thay đổi của bạn.

Chế độ Cách ly mạng thủ công

Bạn có thể bật và tắt Cách ly mạng theo cách thủ công. Bạn có thể cấu hình chế độ Cách ly mạng thủ công bằng cách sử dụng các thuộc tính máy tính trong bảng điều khiển Kaspersky Security Center.

Bạn có thể bật Cách ly mạng:

- Chi tiết về cảnh báo (chỉ dành cho EDR Optimum).

Chi tiết về phát hiện là một công cụ để xem toàn bộ thông tin thu thập được về một mối đe dọa được phát hiện. Chi tiết về phát hiện bao gồm, ví dụ như lịch sử của các tập tin xuất hiện trên máy tính. Để biết chi tiết về việc quản lý thông tin chi tiết về phát hiện, hãy tham khảo [Trợ giúp của Kaspersky Endpoint Detection and Response Optimum](#) và [Trợ giúp của Kaspersky Endpoint Detection and Response Expert](#).

- Sử dụng các thiết lập cục bộ của ứng dụng.

Cách bật Cách ly mạng của một máy tính theo cách thủ công

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Managed devices**.
2. Chọn máy tính mà bạn muốn cấu hình thiết lập cục bộ của ứng dụng.
Việc này sẽ mở ra thuộc tính máy tính.
3. Chọn thẻ **Applications**.
4. Nhấn vào **Kaspersky Endpoint Security for Windows**.
Việc này sẽ mở ra thiết lập cục bộ của ứng dụng.
5. Chọn thẻ **Application settings**.
6. Vào **Detection and Response** → **Endpoint Detection and Response**.
7. Trong mục **Network isolation**, hãy nhấn vào **Isolate computer from the network**.

Bạn có thể cấu hình Cách ly mạng để bị tắt tự động sau khi kết thúc một khoảng thời gian được chỉ định. Theo mặc định, ứng dụng sẽ tắt Cách ly mạng sau 8 giờ kể từ thời điểm tính năng này được bật. Sau khi tắt Cách ly mạng, máy tính có thể sử dụng Mạng mà không bị hạn chế.

Cách cấu hình thời gian trì hoãn để tắt Cách ly mạng của một máy tính trong chế độ thủ công

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Managed devices**.
2. Chọn máy tính mà bạn muốn cấu hình thiết lập cục bộ của ứng dụng.
Việc này sẽ mở ra thuộc tính máy tính.
3. Chọn thẻ **Tasks**.
Thao tác này sẽ hiển thị danh sách các tác vụ có sẵn trên máy tính.
4. Chọn tác vụ **Network isolation**.
5. Chọn thẻ **Application settings**.
6. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ này, chọn độ trễ để tắt Cách ly mạng.
7. Lưu các thay đổi của bạn.

Cách tắt Cách ly mạng của một máy tính theo cách thủ công

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Managed devices**.
2. Chọn máy tính mà bạn muốn cấu hình thiết lập cục bộ của ứng dụng.
Việc này sẽ mở ra thuộc tính máy tính.
3. Chọn thẻ **Applications**.
4. Nhấn vào **Kaspersky Endpoint Security for Windows**.
Việc này sẽ mở ra thiết lập cục bộ của ứng dụng.
5. Chọn thẻ **Application settings**.
6. Vào **Detection and Response** → **Endpoint Detection and Response**.
7. Trong mục **Network isolation**, hãy nhấn vào **Unblock computer isolated from the network**.

Bạn cũng có thể tắt Cách ly mạng cục bộ bằng cách sử dụng [dòng lệnh](#).

Network isolation exclusions

Bạn có thể cấu hình các loại trừ Cách ly mạng. Các kết nối mạng phù hợp với quy tắc không bị chặn trên máy tính đó khi chế độ Cách ly mạng được bật.

Để cấu hình các loại trừ Cách ly mạng, bạn có thể sử dụng một danh sách *các cấu hình mạng tiêu chuẩn*. Theo mặc định, các loại trừ bao gồm các cấu hình mạng chứa các quy tắc đảm bảo hoạt động không bị gián đoạn của các thiết bị có máy chủ DNS/DHCP và các vai trò máy khách DNS/DHCP. Bạn cũng có thể sửa đổi thiết lập của các cấu hình mạng tiêu chuẩn hoặc định nghĩa các loại trừ theo cách thủ công (xem hướng dẫn bên dưới).

Các loại trừ được chỉ định trong thuộc tính chính sách chỉ được áp dụng nếu chế độ Cách ly mạng được bật tự động để ứng phó với mối đe dọa được phát hiện. Các loại trừ được chỉ định trong các thuộc tính máy tính chỉ được áp dụng nếu chế độ Cách ly mạng được bật theo cách thủ công trong các thuộc tính máy tính, trong bảng điều khiển của Kaspersky Security Center hoặc trong chi tiết về cảnh báo.

Một chính sách đang hoạt động không ngăn áp dụng các loại trừ Cách ly mạng được cấu hình trong thuộc tính máy tính bởi vì các tham số này có các kịch bản sử dụng khác nhau.

Cách thêm một loại trừ Cách ly mạng trong chế độ tự động

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Detection and Response** → **Endpoint Detection and Response**.
5. Trong mục **Network isolation exclusions**, hãy nhấn vào **Exclusions**.
6. Thao tác này mở ra một cửa sổ; trong cửa sổ này, hãy nhấn vào **Add from profile** và chọn các cấu hình mạng tiêu chuẩn để cấu hình loại trừ.
Các loại trừ Cách ly mạng trong cấu hình được thêm vào danh sách các loại trừ Cách ly mạng. Bạn có thể xem thuộc tính của các kết nối mạng. Nếu cần, bạn có thể sửa đổi thiết lập kết nối mạng.
7. Nếu cần, hãy thêm một loại trừ Cách ly mạng theo cách thủ công. Để thực hiện, trong cửa sổ chứa danh sách loại trừ, hãy nhấn vào **Add** và chỉnh sửa thiết lập kết nối mạng một cách thủ công.
8. Lưu các thay đổi của bạn.

Cách thêm một loại trừ Cách ly mạng trong chế độ thủ công

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Managed devices**.
2. Chọn máy tính mà bạn muốn cấu hình thiết lập cục bộ của ứng dụng.
Việc này sẽ mở ra thuộc tính máy tính.
3. Chọn thẻ **Tasks**.
Thao tác này sẽ hiển thị danh sách các tác vụ có sẵn trên máy tính.
4. Chọn tác vụ **Network isolation**.
5. Chọn thẻ **Application settings**.
6. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ này, hãy nhấn vào **Exclusions**.
7. Thao tác này mở ra một cửa sổ; trong cửa sổ này, hãy nhấn vào **Add from profile** và chọn các cấu hình mạng tiêu chuẩn để cấu hình loại trừ.
Các loại trừ Cách ly mạng trong cấu hình được thêm vào danh sách các loại trừ Cách ly mạng. Bạn có thể xem thuộc tính của các kết nối mạng. Nếu cần, bạn có thể sửa đổi thiết lập kết nối mạng.
8. Nếu cần, hãy thêm một loại trừ Cách ly mạng theo cách thủ công. Để thực hiện, trong cửa sổ chứa danh sách loại trừ, hãy nhấn vào **Add** và chỉnh sửa thiết lập kết nối mạng một cách thủ công.
9. Lưu các thay đổi của bạn.

Bạn cũng có thể xem danh sách loại trừ Cách ly mạng cục bộ bằng cách sử dụng [dòng_lệnh](#). Trong trường hợp này, máy tính phải được cách ly.

Phụ lục 1. Các phần mở rộng tập tin được hỗ trợ cho Phòng chống thực thi

Kaspersky Endpoint Security hỗ trợ phòng chống mở các tập tin định dạng văn phòng trong một số ứng dụng nhất định. Thông tin về các phần mở rộng tập tin và ứng dụng được hỗ trợ được liệt kê trong bảng sau.

Các phần mở rộng tập tin được hỗ trợ cho Phòng chống thực thi

Tên ứng dụng	Tập tin thực thi	Phần mở rộng tập tin
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx

		ppsm sldx sldm
Adobe Acrobat	acrord32.exe	pdf
Foxit PDF Reader	FoxitReader.exe	
STDU Viewer	STDUViewerApp.exe	
Microsoft Edge	MicrosoftEdge.exe	
Google Chrome	chrome.exe	
Mozilla Firefox	firefox.exe	
Yandex Browser	browser.exe	
Tor Browser	tor.exe	

Phụ lục 2. Các trình thông dịch tập lệnh được hỗ trợ

Phòng chống thực thi hỗ trợ các trình thông dịch tập lệnh sau:

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msixexec.exe

- perl.exe
- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplevated.exe
- wscript.exe
- wvahost.exe

Phòng chống thực thi hỗ trợ làm việc với các ứng dụng Java trong môi trường thời gian chạy Java (các tiến trình java.exe và javaw.exe).

Phụ lục 3. Phạm vi quét IOC trong registry (RegistryItem)

Khi bạn thêm loại dữ liệu RegistryItem vào phạm vi quét IOC, Kaspersky Endpoint Security sẽ quét các khóa registry sau:

HKEY_CLASSES_ROOT\htafile

HKEY_CLASSES_ROOT\batfile

HKEY_CLASSES_ROOT\exefile

HKEY_CLASSES_ROOT\comfile

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\Software\Classes\piffile

HKEY_LOCAL_MACHINE\Software\Classes\htafile

HKEY_LOCAL_MACHINE\Software\Classes\exefile

HKEY_LOCAL_MACHINE\Software\Classes\comfile

HKEY_LOCAL_MACHINE\Software\Classes\CLSID

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebg

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Phụ lục 4. Các yêu cầu của tập tin IOC

Khi tạo các tác vụ Quét IOC, hãy xem xét các yêu cầu và hạn chế của [tập tin IOC](#) sau:

- Ứng dụng hỗ trợ các tập tin IOC có phần mở rộng IOC và XML trong phiên bản OpenIOC tiêu chuẩn mở 1.0 và 1.1 để mô tả các dấu hiệu về sự xâm nhập.
- Nếu khi [tạo một tác vụ Quét IOC trên dòng lệnh](#), bạn tải lên các tập tin IOC, một số tập tin trong số đó không được hỗ trợ thì khi tác vụ được chạy, ứng dụng chỉ sử dụng các tập tin IOC được hỗ trợ. Nếu khi tạo một tác vụ *Quét IOC* trên dòng lệnh, tất cả các tập tin IOC mà bạn tải lên hóa ra không được hỗ trợ thì bạn vẫn có thể chạy tác vụ đó, nhưng sẽ không có bất kỳ dấu hiệu về sự xâm nhập nào được phát hiện. Không thể tải lên các tập tin IOC không được hỗ trợ bằng Bảng điều khiển web hoặc Bảng điều khiển đám mây.
- Quá trình thực thi tác vụ vẫn diễn ra thành công dù có các lỗi ngữ nghĩa và các từ và thẻ IOC không được hỗ trợ trong tập tin IOC. Trong các phần như vậy của tập tin IOC, ứng dụng không phát hiện thấy sự trùng khớp nào.

- [Mã định danh của tất cả các tập tin IOC](#) được sử dụng trong một tác vụ Quét IOC phải có tính duy nhất. Nếu có các tập tin IOC có cùng số mã định danh thì điều đó có thể ảnh hưởng đến kết quả thực thi tác vụ.
- Một tập tin IOC không được có kích thước vượt quá 2 MB. Việc sử dụng các tập tin lớn hơn sẽ khiến các tác vụ Quét IOC kết thúc bằng một lỗi. Tổng dung lượng của tất cả các tập tin được thêm vào bộ sưu tập IOC không được vượt quá 10 MB. Nếu tổng dung lượng của tất cả các tập tin vượt quá 10 MB, bạn cần chia bộ sưu tập IOC và tạo vài tác vụ *Quét IOC*.
- Bạn nên tạo một tập tin IOC cho mỗi mối đe dọa. Điều này giúp cho việc phân tích kết quả của tác vụ Quét IOC được dễ dàng hơn.

Tập tin mà bạn có thể tải về bằng cách nhấn vào liên kết bên dưới, có chứa một bảng kèm danh sách đầy đủ các từ của tiêu chuẩn OpenIOC.

[TẢI XUỐNG TẬP TIN IOC TERMS.XLSX](#)

Các tính năng và giới hạn hỗ trợ của ứng dụng đối với tiêu chuẩn OpenIOC được hiển thị trong bảng sau.

Các tính năng và giới hạn của hỗ trợ OpenIOC phiên bản 1.0 và 1.1.

Các điều kiện được hỗ trợ	OpenIOC 1.0: is isnot (là một ngoại lệ của tập hợp) contains containsnot (là một ngoại lệ của tập hợp) OpenIOC 1.1: is contains starts-with ends-with matches greater-than less-than
Các thuộc tính điều kiện được hỗ trợ	OpenIOC 1.1: preserve-case negate
Các toán tử được hỗ trợ	AND OR
Các kiểu dữ liệu được hỗ trợ	"date": ngày tháng (điều kiện áp dụng: is, greater-than, less-than) "int": số nguyên (điều kiện áp dụng: is, greater-than, less-than) "string": chuỗi ký tự (điều kiện áp dụng: is, contains, matches, starts-with, ends-with) "duration": thời lượng tính bằng giây (điều kiện áp dụng: is, greater-than, less-than)
Các tính năng thông dịch kiểu dữ liệu	Các kiểu dữ liệu "boolean string", "restricted string", "md5", "IP", "sha256" và "base64Binary" được thông dịch dưới dạng chuỗi ký tự.

Ứng dụng hỗ trợ thông dịch thiết lập Content cho các kiểu dữ liệu int và date khi nó được đặt theo dạng khoảng thời gian:

OpenIOC 1.0:

Sử dụng toán tử TO trong trường Content:

```
<Content type="int">49600 TO 50700</Content>
```

```
<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>
```

```
<Content type="int">[154192 TO 154192]</Content>
```

OpenIOC 1.1:

Sử dụng các điều kiện greater-than và less-than

Sử dụng toán tử TO trong trường Content

Ứng dụng hỗ trợ thông dịch các kiểu dữ liệu date và duration nếu các dấu hiệu được đặt theo định dạng ISO 8601, Zulu Time Zone, UTC.

Kaspersky Sandbox



Kaspersky Endpoint Security 11.7.0 hiện đã có một tác nhân tích hợp để tích hợp với giải pháp Kaspersky Sandbox. *Giải pháp Kaspersky Sandbox* phát hiện và tự động chặn các mối đe dọa nâng cao trên máy tính. Kaspersky Sandbox sẽ phân tích hành vi của đối tượng để phát hiện hoạt động độc hại và hoạt động đặc trưng của các cuộc tấn công có chủ đích vào cơ sở hạ tầng CNTT của tổ chức. Kaspersky Sandbox sẽ phân tích và quét các đối tượng trên các máy chủ đặc biệt chứa các ảnh máy ảo được triển khai của hệ điều hành Microsoft Windows (máy chủ Kaspersky Sandbox). Để biết chi tiết về giải pháp này, hãy tham khảo [Trợ giúp của Kaspersky Sandbox](#).

Có thể sử dụng các cấu hình sau cho giải pháp Kaspersky Sandbox:

Kaspersky Sandbox 2.0

Kaspersky Sandbox 2.0 hỗ trợ cấu hình [KES+built-in agent].

Yêu cầu tối thiểu:

- Kaspersky Endpoint Security 11.7.0 cho Windows hoặc mới hơn.
- Không cần có Kaspersky Endpoint Agent.
- Kaspersky Security Center 13.2.

Kaspersky Sandbox 1.0

Kaspersky Sandbox 1.0 hỗ trợ cấu hình [KES+KEA].

Yêu cầu tối thiểu:

- Kaspersky Endpoint Security 11.2.0 – 11.6.0 cho Windows.
- Kaspersky Endpoint Agent 3.8.

Bạn có thể cài đặt Kaspersky Endpoint Agent từ gói phân phối Kaspersky Endpoint Security cho Windows.

- Kaspersky Security Center 11.

Tích hợp với Kaspersky Sandbox

Phải thêm thành phần Kaspersky Sandbox để tích hợp với thành phần Kaspersky Sandbox. Bạn có thể chọn thành phần Kaspersky Sandbox trong quá trình [cài đặt](#) hoặc [nâng cấp](#), cũng như sử dụng [tác vụ Thay đổi thành phần ứng dụng](#).

Để sử dụng thành phần này, cần đáp ứng các điều kiện sau:

- Kaspersky Security Center 13.2. Các phiên bản trước của Kaspersky Security Center không cho phép tạo các tác vụ Quét IOC độc lập để ứng phó với mối đe dọa.
- Chỉ có thể quản lý thành phần này bằng Bảng điều khiển web. Bạn không thể quản lý thành phần này bằng Bảng điều khiển quản trị (MMC).
- Ứng dụng được kích hoạt và chức năng được giấy phép hỗ trợ.
- Truyền dữ liệu đến Máy chủ quản trị được bật.

Để sử dụng tất cả các tính năng của Kaspersky Sandbox, đảm bảo rằng truyền dữ liệu tập tin trong khu vực cách ly được bật. Đây là dữ liệu phải có để lấy thông tin về các tập tin được cách ly trên máy tính thông qua Bảng điều khiển web. Ví dụ: bạn có thể tải về một tập tin từ khu vực cách ly để phân tích trong Bảng điều khiển web.

[Cách bật truyền dữ liệu đến Máy chủ quản trị trong Bảng điều khiển web](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Thiết lập tổng quát** → **Các báo cáo và lưu trữ**.
5. Trong mục **Truyền dữ liệu đến Máy chủ quản trị**, hãy chọn hộp kiểm **Thông tin về các tập tin trong Khu vực cách ly**.
6. Lưu các thay đổi của bạn.

- Một kết nối trong nền giữa Bảng điều khiển web Kaspersky Security Center và Máy chủ quản trị được thiết lập

Để Kaspersky Sandbox hoạt động với Máy chủ quản trị thông qua Bảng điều khiển web Kaspersky Security Center, bạn phải thiết lập một kết nối bảo mật mới, một *kết nối nền*. Để biết chi tiết về việc tích hợp Kaspersky Security Center với các giải pháp khác của Kaspersky, hãy tham khảo [Trợ giúp của Kaspersky Security Center](#).

[Thiết lập một kết nối nền trong Bảng điều khiển web](#)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Console settings** → **Tích hợp**.
2. Vào mục **Cross-service integration**.
3. Tắt công tắc bật/tắt **Establish a background connection for cross-service integration**.
4. Lưu các thay đổi của bạn.

Nếu một kết nối nền giữa Bảng điều khiển web Kaspersky Security Center và Máy chủ quản trị không được thiết lập thì các tác vụ quét IOC độc lập có thể không được tạo làm một phần của Threat Response.

- Thành phần Kaspersky Sandbox được bật.

Bạn có thể bật hoặc tắt tích hợp với Kaspersky Sandbox trong Bảng điều khiển web hoặc trên máy bằng cách sử dụng [dòng lệnh](#).

Để bật hoặc tắt tích hợp với Kaspersky Sandbox:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Detection and Response** → **Kaspersky Sandbox**.
5. Sử dụng công tắc bật/tắt **Integration with Kaspersky Sandbox** để bật hoặc tắt thành phần.
6. Lưu các thay đổi của bạn.

Kết quả là thành phần Kaspersky Sandbox được bật. Kiểm tra trạng thái hoạt động của thành phần bằng cách xem *Báo cáo trạng thái thành phần ứng dụng*. Bạn cũng có thể xem trạng thái hoạt động của một thành phần trong mục [báo cáo](#) trong giao diện cục bộ của Kaspersky Endpoint Security. Thành phần **Kaspersky Sandbox** sẽ được thêm vào danh sách các thành phần của Kaspersky Endpoint Security.

Kaspersky Endpoint Security sẽ lưu thông tin về hoạt động của thành phần Kaspersky Sandbox vào một báo cáo. Báo cáo đó cũng chứa thông tin về các lỗi. Nếu bạn gặp lỗi kèm mô tả phù hợp với định dạng Error code: XXX (ví dụ: 0xa67b01f4), hãy liên hệ bộ phận [Hỗ trợ kỹ thuật](#).

Chuyển sang từ Kaspersky Endpoint Agent

Nếu bạn đang sử dụng Kaspersky Endpoint Security 11.7.0 hoặc mới hơn, được cài đặt thành phần Kaspersky Sandbox (tác nhân tích hợp) thì khả năng tương tác với giải pháp Kaspersky Sandbox sẽ khả dụng ngay sau khi cài đặt. Thành phần Kaspersky Sandbox không tương thích với Kaspersky Endpoint Agent. Nếu Kaspersky Endpoint Agent được cài đặt trên máy tính, khi Kaspersky Endpoint Security được cập nhật lên phiên bản 11.7.0, Kaspersky Sandbox sẽ tiếp tục hoạt động với Kaspersky Endpoint Security ([chuyển đổi cấu hình \[KES+KEA\] sang \[KES+built-in agent\]](#)). Ngoài ra, Kaspersky Endpoint Agent sẽ bị gỡ bỏ khỏi máy tính. Để hoàn tất chuyển đổi từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security cho Windows, bạn cần chuyển thiết lập chính sách và tác vụ bằng [Trình hướng dẫn chuyển đổi](#).

Nếu bạn đang sử dụng Kaspersky Endpoint Security 11.4.0–11.6.0, để có khả năng tương tác với Kaspersky Sandbox, ứng dụng này sẽ có cả Kaspersky Endpoint Agent. Bạn có thể cài đặt Kaspersky Endpoint Agent để chạy cùng Kaspersky Endpoint Security.

Trong Kaspersky Endpoint Security 11.9.0, gói phân phối Kaspersky Endpoint Agent không còn thuộc gói phân phối Kaspersky Endpoint Security. Bạn phải tải xuống gói phân phối Kaspersky Endpoint Agent riêng.

Thành phần Kaspersky Sandbox là một phần của Kaspersky Endpoint Security, hỗ trợ khả năng tương tác với giải pháp Kaspersky Sandbox 2.0. Giải pháp Kaspersky Sandbox 1.0 không được hỗ trợ.

Thêm một chứng chỉ TLS

Để cấu hình kết nối được tin tưởng với máy chủ Kaspersky Sandbox, bạn phải chuẩn bị chứng chỉ TLS. Tiếp theo, bạn phải thêm chứng chỉ vào máy chủ Kaspersky Sandbox và chính sách Kaspersky Endpoint Security. Để biết chi tiết về cách chuẩn bị chứng chỉ và thêm chứng chỉ vào máy chủ, hãy tham khảo [Trợ giúp của Kaspersky Sandbox](#).

Bạn có thể thêm chứng chỉ TLS vào Bảng điều khiển web bằng cách sử dụng [dòng lệnh](#).

Để thêm một chứng chỉ TLS vào Bảng điều khiển web:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Detection and Response** → **Kaspersky Sandbox**.
5. Nhấn vào liên kết **Server connection settings**.
Thao tác này sẽ mở ra cửa sổ thiết lập kết nối máy chủ Kaspersky Sandbox.
6. Trong mục **Server TLS certificate**, hãy nhấn vào **Thêm** và chọn tập tin chứng chỉ TLS.
Kaspersky Endpoint Security chỉ có thể có một chứng chỉ TLS cho máy chủ Kaspersky Sandbox. Nếu bạn đã thêm chứng chỉ TLS trước đó, chứng chỉ đó sẽ bị thu hồi. Chỉ chứng chỉ được thêm cuối cùng mới được sử dụng.
7. Cấu hình thiết lập kết nối nâng cao cho máy chủ Kaspersky Sandbox:

- **Thời gian chờ.** Thời gian chờ kết nối cho máy chủ Kaspersky Sandbox. Sau khi hết thời gian chờ đã được cấu hình, Kaspersky Endpoint Security sẽ gửi yêu cầu đến máy chủ tiếp theo. Bạn có thể tăng thời gian chờ kết nối cho Kaspersky Sandbox nếu tốc độ kết nối của bạn thấp hoặc nếu kết nối không ổn định. Thời gian chờ của yêu cầu được khuyến nghị là từ 0.5 giây trở xuống.
- **Kaspersky Sandbox request queue.** Kích thước của thư mục hàng chờ yêu cầu. Khi một đối tượng được truy cập trên máy tính (tệp thực thi được khởi chạy hoặc tài liệu được mở, ví dụ như ở định dạng DOCX hoặc PDF), Kaspersky Endpoint Security cũng có thể gửi đối tượng cần quét bởi Kaspersky Sandbox. Nếu có nhiều yêu cầu, Kaspersky Endpoint Security sẽ tạo một hàng chờ yêu cầu. Theo mặc định, kích thước của thư mục hàng chờ yêu cầu được giới hạn ở 100 MB. Sau khi đạt đến kích thước tối đa, Kaspersky Sandbox ngừng thêm các yêu cầu mới vào hàng chờ và gửi sự kiện tương ứng đến Kaspersky Security Center. Bạn có thể cấu hình kích thước của thư mục hàng đợi yêu cầu tùy thuộc vào cấu hình máy chủ của bạn.

8. Lưu các thay đổi của bạn.

Kết quả là Kaspersky Endpoint Security sẽ xác minh chứng chỉ TLS. Nếu chứng chỉ được xác minh thành công, Kaspersky Endpoint Security sẽ tải tập tin chứng chỉ đó lên máy tính trong lần đồng bộ hóa tiếp theo với Kaspersky Security Center. Nếu bạn đã thêm hai chứng chỉ TLS thì Kaspersky Sandbox sẽ sử dụng chứng chỉ mới nhất để thiết lập kết nối được tin tưởng.

Thêm máy chủ Kaspersky Sandbox

Để kết nối máy tính với máy chủ Kaspersky Sandbox bằng ảnh máy ảo của hệ điều hành, bạn phải nhập địa chỉ máy chủ và cổng. Để biết chi tiết về việc triển khai ảnh máy ảo và cấu hình máy chủ Kaspersky Sandbox, hãy tham khảo [Trợ giúp của Kaspersky Sandbox](#).

Để thêm máy chủ Kaspersky Sandbox vào Bảng điều khiển web:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Detection and Response** → **Kaspersky Sandbox**.
5. Trong mục **Máy chủ Kaspersky Sandbox**, hãy nhấn vào **Thêm**.
6. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy nhập địa chỉ máy chủ Kaspersky Sandbox (IPv4, IPv6, DNS) và cổng.
7. Lưu các thay đổi của bạn.

Quét các dấu hiệu về sự xâm nhập (tác vụ độc lập)

Một *Dấu hiệu về sự xâm nhập (IOC)* là một tập hợp dữ liệu về một đối tượng hoặc hoạt động cho biết sự truy cập trái phép vào máy tính (xâm nhập dữ liệu). Ví dụ: nhiều nỗ lực đăng nhập không thành công vào hệ thống có thể cấu thành một Dấu hiệu về sự xâm nhập. Tác vụ *Quét IOC* cho phép tìm các Dấu hiệu về sự xâm nhập trên máy tính và thực hiện các biện pháp ứng phó với mỗi đe dọa.

Kaspersky Endpoint Security sẽ tìm kiếm các dấu hiệu về sự xâm nhập bằng cách sử dụng các tập tin IOC. *Tập tin IOC* là các tập tin chứa các tập hợp dấu hiệu mà ứng dụng cố gắng khớp để đếm một lần phát hiện. Các tập tin IOC phải tuân theo [tiêu chuẩn OpenIOC](#). Kaspersky Endpoint Security sẽ tự động tạo các tập tin IOC cho Kaspersky Sandbox.

Chế độ chạy tác vụ quét IOC

Ứng dụng sẽ tạo các tác vụ quét IOC độc lập cho Kaspersky Sandbox. *Tác vụ quét IOC độc lập* là một tác vụ nhóm được tạo tự động khi phản ứng với một mối đe dọa được phát hiện bởi Kaspersky Sandbox. Kaspersky Endpoint Security tự động tạo tập tin IOC. Các tập tin IOC tùy chỉnh không được hỗ trợ. Tác vụ sẽ tự động bị xóa sau 30 ngày kể từ thời điểm tạo. Để biết thêm chi tiết về các tác vụ quét IOC độc lập, hãy tham khảo [Trợ giúp của Kaspersky Sandbox](#).

Thiết lập tác vụ quét IOC

Kaspersky Sandbox có thể tự động tạo và chạy tác vụ *Quét IOC* khi phản ứng với các mối đe dọa.

Bạn chỉ có thể cấu hình thiết lập trong Bảng điều khiển web.

Bạn cần Kaspersky Security Center 13.2 để các tác vụ quét IOC độc lập của Kaspersky Sandbox hoạt động.

Để thay đổi thiết lập của tác vụ Quét IOC:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Tasks**.
Danh sách tác vụ sẽ mở.
2. Nhấn vào tác vụ **Quét IOC** của Kaspersky Endpoint Security.
Cửa sổ thuộc tính tác vụ sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào mục **Thiết lập quét IOC**.
5. Cấu hình các hành động khi phát hiện IOC:
 - **Di chuyển bản sao vào Khu vực cách ly, xóa đối tượng.** Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ xóa đối tượng độc hại được tìm thấy trên máy tính. Trước khi xóa đối tượng, Kaspersky Endpoint Security sẽ tạo một bản sao lưu trong trường hợp đối tượng cần được khôi phục sau này. Kaspersky Endpoint Security sẽ di chuyển bản sao lưu vào Khu vực cách ly.
 - **Chạy tác vụ quét các khu vực quan trọng.** Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ chạy tác vụ [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.
6. Cấu hình chế độ chạy tác vụ Quét IOC bằng cách sử dụng hộp kiểm **Chỉ chạy khi máy tính đang rảnh**. Hộp kiểm này bật / tắt chức năng đình chỉ tác vụ *Quét IOC* khi tài nguyên máy tính bị hạn chế. Kaspersky Endpoint Security sẽ tạm ngưng tác vụ *Quét IOC* nếu trình bảo vệ màn hình đang tắt và máy tính đang được mở khóa.

Tùy chọn lịch này cho phép bạn bảo tiết kiệm nguyên máy tính khi máy tính đang được sử dụng.

7. Lưu các thay đổi của bạn.

Bạn có thể xem kết quả tác vụ trong các thuộc tính tác vụ trong mục **Kết quả**. Bạn có thể xem thông tin về các dấu hiệu về sự xâm nhập được phát hiện trong thuộc tính của tác vụ: **Application settings** → **IOC Scan Results**.

Kết quả quét IOC được lưu trong vòng 30 ngày. Sau khoảng thời gian này, Kaspersky Endpoint Security sẽ tự động xóa các mục cũ nhất.

Kaspersky Anti Targeted Attack Platform (KATA EDR)



Kaspersky Endpoint Security 11.9.0 thêm hỗ trợ tích hợp với thành phần Kaspersky Endpoint Detection and Response, là một phần của giải pháp Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* là một giải pháp được thiết kế để phát hiện kịp thời các mối đe dọa tinh vi, chẳng hạn như các cuộc tấn công chủ đích, các mối đe dọa dai dẳng nâng cao (APT), các cuộc tấn công zero-day, v.v. Kaspersky Anti Targeted Attack Platform bao gồm hai khối chức năng: Kaspersky Anti Targeted Attack (sau đây còn được gọi là "KATA") và Kaspersky Endpoint Detection and Response (sau đây còn được gọi là "KEDR"). Bạn có thể mua KEDR riêng. Để biết chi tiết về giải pháp này, vui lòng tham khảo [Trợ giúp của Kaspersky Anti Targeted Attack Platform](#).

Kaspersky Endpoint Detection and Response sử dụng các công cụ Threat Intelligence sau:

- Cơ sở hạ tầng dịch vụ đám mây của Kaspersky Security Network (sau đây gọi là "KSN"), cung cấp quyền truy cập vào tập tin, trang web và thông tin danh tiếng phần mềm theo thời gian thực từ cơ sở tri thức của Kaspersky. Việc sử dụng dữ liệu từ Kaspersky Security Network đảm bảo thời gian phản ứng nhanh hơn cho các ứng dụng của Kaspersky 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.
- Tích hợp với cổng thông tin [Kaspersky Threat Intelligence Portal](#), hệ thống này chứa và hiển thị thông tin về danh tiếng của các tập tin và địa chỉ web.
- Cơ sở dữ liệu về [Các mối đe dọa của Kaspersky](#).

Nguyên lý hoạt động của giải pháp này

Ứng dụng Kaspersky Endpoint Agent được cài đặt trên các máy tính cá nhân, trên cơ sở hạ tầng CNTT của doanh nghiệp và liên tục giám sát các quy trình, kết nối mạng mở và các tập tin đang được sửa đổi. Thông tin về các sự kiện trên máy tính được gửi đến máy chủ của Kaspersky Anti Targeted Attack Platform.

Kaspersky Endpoint Agent có thể tích hợp với Kaspersky Endpoint Security cho Windows. Trong trường hợp này, ứng dụng Kaspersky Endpoint Agent cũng gửi thông tin đến máy chủ của Kaspersky Anti Targeted Attack Platform về các mối đe dọa được phát hiện bởi Kaspersky Endpoint Security cho Windows, bao gồm cả thông tin về kết quả xử lý các mối đe dọa này.

Tích hợp với KATA EDR

Để tích hợp với KATA EDR thì cần phải thêm thành phần Kaspersky Anti Targeted Attack Platform (KATA EDR) và cài đặt Kaspersky Endpoint Agent. Bạn có thể chọn thành phần KATA EDR trong quá trình [cài đặt](#) hoặc [nâng cấp](#), cũng như sử dụng *tác vụ* [Thay đổi thành phần ứng dụng](#).

Thành phần KATA EDR không tương thích với các thành phần EDR Optimum và EDR Expert.

Trong Kaspersky Endpoint Security 11.9.0, gói phân phối không còn gói phân phối Kaspersky Endpoint Agent. Bạn có thể tải xuống gói phân phối Kaspersky Endpoint Agent từ gói phân phối Kaspersky Anti Targeted Attack Platform.

Thành phần KATA EDR sử dụng thông tin nhận được từ các thành phần ứng dụng. Các thành phần sau đảm bảo hoạt động của KATA EDR:

- [Bảo vệ mỗi đe dọa tập tin](#).
- [Bảo vệ mỗi đe dọa web](#).
- [Bảo vệ mỗi đe dọa thư điện tử](#).
- [Phòng chống khai thác](#).
- [Phát hiện hành vi](#).
- [Phòng chống xâm nhập máy chủ](#).
- [Công cụ khắc phục](#).
- [Kiểm soát thích ứng sự cố](#).

Đảm bảo rằng các thành phần này được bật và hoạt động.

Quản lý Khu vực cách ly

Khu vực cách ly là một kho lưu trữ cục bộ đặc biệt trên máy tính. Người dùng có thể cách ly các tập tin mà người dùng coi là nguy hiểm cho máy tính. Các tập tin cách ly được lưu trữ ở trạng thái mã hóa và không đe dọa đến tính bảo mật của thiết bị. Kaspersky Endpoint Security chỉ sử dụng Khu vực cách ly khi làm việc với các giải pháp Kaspersky Sandbox và Kaspersky Endpoint Detection and Response. Trong các trường hợp khác, Kaspersky Endpoint Security sẽ đặt các tập tin liên quan vào [Sao lưu](#). Để biết chi tiết về quản lý khu vực cách ly làm một phần của các giải pháp, vui lòng tham khảo [Trợ giúp của Kaspersky Sandbox](#), [Trợ giúp của Kaspersky Endpoint Detection and Response Optimum](#) và [Trợ giúp của Kaspersky Endpoint Detection and Response Expert](#).

Kaspersky Endpoint Security sử dụng tài khoản hệ thống (SYSTEM) để cách ly các tập tin.

Chỉ có thể cấu hình Khu vực cách ly bằng Bảng điều khiển web. Bạn cũng có thể sử dụng Bảng điều khiển web để quản lý các đối tượng đã cách ly (khôi phục, xóa, thêm, v.v.). Cục bộ, trên máy tính, bạn chỉ có thể [khôi phục đối tượng bằng dòng lệnh](#).

Cấu hình kích thước tối đa cho Khu vực cách ly

Theo mặc định, kích thước của Khu vực cách ly được giới hạn ở 200 MB. Sau khi đạt được kích cỡ tối đa, Kaspersky Endpoint Security sẽ tự động xóa các tập tin cũ nhất khỏi Khu vực cách ly.

Để cấu hình kích thước tối đa của Khu vực cách ly:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Thiết lập tổng quát** → **Các báo cáo và lưu trữ**.
5. Trong mục **Khu vực cách ly**, hãy cấu hình kích thước của Khu vực cách ly:
 - **Giới hạn dung lượng của Khu vực cách ly xuống N MB.** Dung lượng tối đa của Khu vực cách ly tính bằng MB. Ví dụ: bạn có thể đặt dung lượng tối đa của Khu vực cách ly là 200 MB. Khi khu vực cách ly đạt dung lượng tối đa, Kaspersky Endpoint Security sẽ gửi sự kiện tương ứng đến Kaspersky Security Center và phát hành sự kiện này trong Nhật ký sự kiện của Windows. Trong khi đó ứng dụng dừng cách ly các đối tượng mới. Bạn phải xóa Khu vực cách ly theo cách thủ công.
 - **Thông báo khi kho lưu trữ của Khu vực cách ly đạt N phần trăm.** Giá trị ngưỡng của Khu vực cách ly. Ví dụ: bạn có thể đặt ngưỡng Khu vực cách ly thành 50%. Khi khu vực cách ly đạt ngưỡng này, Kaspersky Endpoint Security sẽ gửi sự kiện tương ứng đến Kaspersky Security Center và phát hành sự kiện này trong Nhật ký sự kiện của Windows. Trong khi đó ứng dụng vẫn tiếp tục cách ly các đối tượng mới.
6. Lưu các thay đổi của bạn.

Gửi dữ liệu về các tập tin được cách ly tới Kaspersky Security Center

Để thực hiện các hành động với các đối tượng được cách ly trong Bảng điều khiển web, bạn phải cho phép gửi dữ liệu tập tin được cách ly tới Máy chủ quản trị. Ví dụ: bạn có thể tải về một tập tin từ khu vực cách ly để phân tích trong Bảng điều khiển web. Phải bật gửi dữ liệu tập tin được cách ly phải được bật để tất cả các chức năng của [Kaspersky Sandbox](#) và [Endpoint Detection and Response của Kaspersky Sandbox](#) hoạt động được.

Để cho phép chuyển dữ liệu tập tin được cách ly tới Kaspersky Security Center:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Devices** → **Policies & Profiles**.
2. Nhấn vào tên của chính sách Kaspersky Endpoint Security.
Cửa sổ thuộc tính chính sách sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Vào **Thiết lập tổng quát** → **Các báo cáo và lưu trữ**.
5. Trong mục **Truyền dữ liệu đến Máy chủ quản trị**, hãy chọn hộp kiểm **Thông tin về các tập tin trong Khu vực cách ly**.
6. Lưu các thay đổi của bạn.

Do đó, trong Bảng điều khiển web, bạn có thể xem danh sách các tập tin được cách ly trên máy tính (**Hoạt động** → **Lưu trữ** → **Khu vực cách ly**). Bạn có thể sử dụng Bảng điều khiển web để quản lý các đối tượng đã cách ly (khôi phục, xóa, thêm, v.v.).

Kaspersky Security cho Windows Server



Kaspersky Endpoint Security 11.8.0 hỗ trợ chức năng cơ bản của giải pháp Kaspersky Security cho Windows Server (KSWs). *Kaspersky Security cho Windows Server* bảo vệ các máy chủ chạy hệ điều hành Microsoft Windows và các ổ lưu trữ nối mạng trước virus và các mối đe dọa bảo mật máy tính khác mà các máy chủ và ổ lưu trữ nối mạng gặp phải khi trao đổi tập tin. Để biết thông tin chi tiết về cách thức hoạt động của giải pháp này, vui lòng tham khảo [Trợ giúp của Kaspersky Security cho Windows Server](#). Kể từ Kaspersky Endpoint Security 11.8.0, bạn có thể chuyển từ KSWs sang Kaspersky Endpoint Security cho Windows và sử dụng cùng một giải pháp để bảo vệ máy trạm và máy chủ.

Cài đặt KES trên KSWs

Kaspersky Endpoint Security (KES) hỗ trợ chức năng cơ bản của ứng dụng Kaspersky Security cho Windows Server (KSWs). Kể từ Kaspersky Endpoint Security phiên bản 11.8.0, bạn có thể sử dụng KES thay vì KSWs.

Trước khi cài đặt KES, bạn cần gỡ cài đặt KSWs. Bạn có thể gỡ cài đặt ứng dụng từ xa bằng cách sử dụng tác vụ [Gỡ cài đặt ứng dụng từ xa](#) hoặc [cục bộ trên máy chủ](#). Sau khi gỡ cài đặt KSWs, bạn có thể cần phải khởi động lại máy chủ. Nếu muốn cài đặt Kaspersky Endpoint Security mà không cần khởi động lại máy tính thì bạn nên đảm bảo rằng Kaspersky Security cho Windows Server được gỡ bỏ hoàn toàn. Xem danh sách các tập tin và dịch vụ cần kiểm tra ở bên dưới. Nếu ứng dụng không được gỡ cài đặt hoàn toàn thì lỗi máy chủ có thể xảy ra sau khi cài đặt Kaspersky Endpoint Security. Bạn cũng nên đảm bảo rằng ứng dụng đã được gỡ cài đặt hoàn toàn nếu bạn đã sử dụng tiện ích kavremover. [Tiện ích kavremover](#) không hỗ trợ KSWs.

Sau khi gỡ cài đặt KSWs, [hãy cài đặt Kaspersky Endpoint Security cho Windows](#) bằng bất kỳ phương thức nào khả dụng.

Kiểm tra trạng thái gỡ bỏ Kaspersky Security cho Windows Server

Đảm bảo rằng Kaspersky Security cho Windows Server được gỡ cài đặt hoàn toàn:

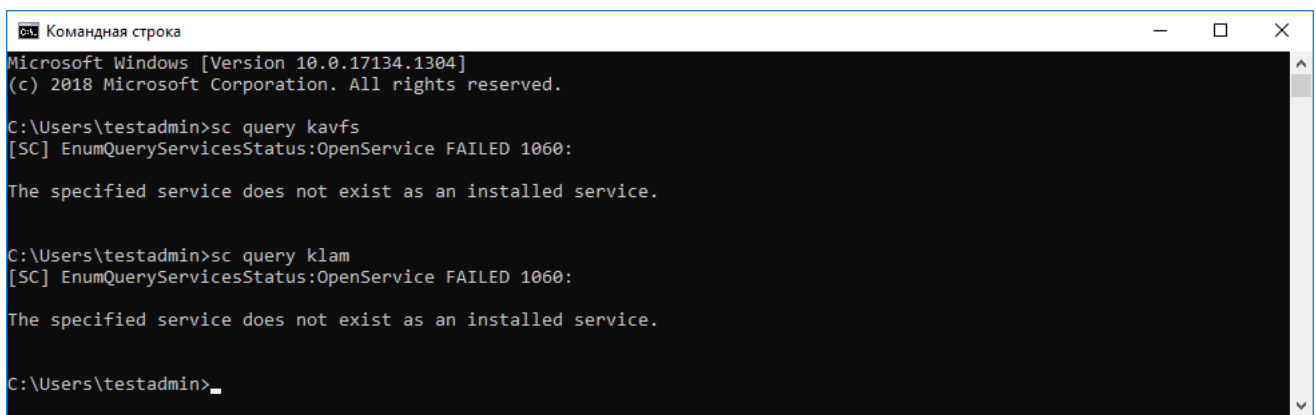
- Thư mục %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\ không tồn tại.
- Các dịch vụ sau đây không chạy:
 - Kaspersky Security Service (KAVFS)
 - Kaspersky Security Management Service (KAVFSGT)
 - Kaspersky Security Exploit Prevention Service (KAVFSSLP)
 - Kaspersky Security Script Checker Service (KAVFSSCS)

Bạn có thể kiểm tra các dịch vụ đang chạy trong Task Manager hoặc bằng cách sử dụng lệnh sc query (xem hình bên dưới).

- Các trình điều khiển sau không được cài đặt:
 - klam.sys

- klflt.sys
- klramdisk.sys
- klelaml.sys
- klfltdev.sys
- klips.sys
- klids.sys
- klwtpee

Bạn có thể kiểm tra các trình điều khiển được cài đặt trong thư mục C:\Windows\System32\drivers hoặc bằng cách sử dụng lệnh `sc query`. Nếu thiếu dịch vụ hoặc trình điều khiển thì bạn sẽ nhận được phản hồi sau đây:



```

Командная строка
Microsoft Windows [Version 10.0.17134.1304]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\testadmin>sc query kavfs
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:
The specified service does not exist as an installed service.

C:\Users\testadmin>sc query klam
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:
The specified service does not exist as an installed service.

C:\Users\testadmin>

```

Kiểm tra trạng thái gỡ bỏ các dịch vụ và trình điều khiển của Kaspersky Security cho Windows Server

Nếu tập tin ứng dụng hoặc trình điều khiển vẫn còn trên máy chủ, hãy xóa chúng theo cách thủ công. Nếu một số dịch vụ của Kaspersky Security cho Windows Server vẫn đang chạy, hãy dừng (`sc stop`) và xóa (`sc delete`) chúng theo cách thủ công. Để dừng trình điều khiển `klam.sys`, hãy sử dụng lệnh `fltmc unload klam`.

Kích hoạt KES bằng khóa KSWs

Sau khi cài đặt ứng dụng, bạn có thể kích hoạt Kaspersky Endpoint Security cho Windows (KES) bằng khóa giấy phép của Kaspersky Security cho Windows Server (KSWs). Quá trình kích hoạt sau khi chuyển đổi phụ thuộc vào phương thức kích hoạt KSWs (xem bảng bên dưới).

Kích hoạt Kaspersky Endpoint Security cho Windows bằng khóa của Kaspersky Security cho Windows Server

Phương thức kích hoạt Kaspersky Security cho Windows Server	Chuyển khóa sang Kaspersky Endpoint Security cho Windows.
Tự động phân phối khóa giấy phép KSWs cho máy tính.	Nếu tính năng phân phối khóa tự động được bật trong thuộc tính khóa giấy phép KSWs, KES sẽ tự động được kích hoạt bằng khóa KSWs.
Khóa KSWs	Nếu KSWs của bạn được kích hoạt bằng tác vụ đó thì khóa giấy phép KSWs sẽ bị

được thêm vào bởi một tác vụ.	xóa trong quá trình chuyển đổi từ KSWs. Bạn phải kích hoạt lại ứng dụng. Ví dụ: bạn có thể thêm khóa giấy phép vào gói cài đặt Kaspersky Endpoint Security cho Windows .
Khóa KSWs được thêm cục bộ trong giao diện ứng dụng.	Nếu KSWs của bạn được kích hoạt cục bộ bằng Trình hướng dẫn kích hoạt ứng dụng, khóa giấy phép KSWs sẽ bị xóa trong quá trình chuyển đổi từ KSWs. Bạn phải kích hoạt lại ứng dụng. Ví dụ: bạn có thể thêm khóa giấy phép vào gói cài đặt Kaspersky Endpoint Security cho Windows .
Khóa KSWs được thêm vào gói cài đặt.	Nếu KSWs của bạn được kích hoạt bằng khóa từ gói cài đặt thì khóa giấy phép KSWs sẽ bị xóa trong quá trình chuyển đổi từ KSWs. Bạn phải kích hoạt lại ứng dụng. Ví dụ: bạn có thể thêm khóa giấy phép vào gói cài đặt Kaspersky Endpoint Security cho Windows .

Quản lý ứng dụng trên máy chủ Chế độ Core

Máy chủ ở Chế độ Core không có giao diện đồ họa. Do đó, bạn chỉ có thể quản lý ứng dụng từ xa bằng bảng điều khiển Kaspersky Security Center hoặc quản lý cục bộ thông qua dòng lệnh.

Quản lý ứng dụng bằng bảng điều khiển Kaspersky Security Center

Cài đặt ứng dụng bằng bảng điều khiển Kaspersky Security Center cũng giống [cài đặt ứng dụng theo cách bình thường](#). Khi [tạo một gói cài đặt](#), bạn có thể thêm khóa giấy phép để kích hoạt ứng dụng. Bạn có thể sử dụng khóa Kaspersky Endpoint Security cho Windows hoặc khóa Kaspersky Security cho Windows.

Trên máy chủ Chế độ Core, các thành phần ứng dụng sau không khả dụng: Bảo vệ mối đe dọa web, Bảo vệ mối đe dọa thư điện, Kiểm soát web, Phòng chống Tấn công BadUSB, Mã hóa mức độ tập tin (FLE), Kaspersky Disk Encryption (FDE).

Không cần khởi động lại khi cài đặt Kaspersky Endpoint Security. Chỉ cần khởi động lại nếu bạn đã 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. Ứng dụng không thể hiển thị cửa sổ để nhắc người dùng khởi động lại máy chủ. Bạn có thể tìm hiểu về sự cần thiết phải khởi động lại máy chủ trong các báo cáo trong bảng điều khiển Kaspersky Security Center.

Quản lý ứng dụng trên máy chủ Chế độ Core cũng giống việc quản lý trên máy tính. Bạn có thể sử dụng các chính sách và tác vụ để cấu hình ứng dụng.

Việc quản lý ứng dụng trên máy chủ Chế độ Core liên quan đến các lưu ý đặc biệt sau:

- Máy chủ Chế độ Core không có giao diện đồ họa, do đó Kaspersky Endpoint Security không hiển thị cảnh báo cho người dùng biết rằng cần Khử mã độc nâng cao. Để khử mã độc một mối đe dọa, bạn cần [bật công nghệ Khử mã độc nâng cao](#) trong thiết lập của ứng dụng và [bật Khử mã độc nâng cao ngay lập tức](#) trong thiết lập tác vụ *Quét virus*. Sau đó bạn cần khởi chạy tác vụ *Quét virus*.
- BitLocker Drive Encryption chỉ khả dụng với Mô-đun nền tảng tin tưởng (TPM). Không thể sử dụng mã PIN / mật khẩu để mã hóa vì ứng dụng không thể hiển thị cửa sổ nhắc mật khẩu để xác thực trước khi khởi động. Nếu hệ điều hành đã bật chế độ tương thích với Tiêu chuẩn Xử lý thông tin liên bang (FIPS), hãy kết nối một ổ đĩa di động để lưu khóa mã hóa trước khi bắt đầu mã hóa ổ đĩa.

Quản lý ứng dụng từ dòng lệnh

Khi bạn không thể sử dụng giao diện đồ họa, bạn có thể [quản lý Kaspersky Endpoint Security từ dòng lệnh](#).

Để cài đặt ứng dụng vào máy chủ Chế độ Core, hãy chạy lệnh sau:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /s
```

Để kích hoạt ứng dụng, hãy chạy lệnh sau:

```
avp.com license /add <mã kích hoạt hoặc tập tin khóa>
```

Để kiểm tra trạng thái hồ sơ ứng dụng, hãy chạy lệnh sau:

```
avp.com status
```

Để xem danh sách các lệnh quản lý ứng dụng, hãy chạy lệnh sau:

```
avp.com help
```

Quản lý ứng dụng từ dòng lệnh

Bạn có thể quản lý Kaspersky Endpoint Security từ dòng lệnh. Bạn có thể xem danh sách các lệnh để quản lý ứng dụng bằng cách thực thi lệnh `HELP`. Để đọc về cú pháp của một lệnh cụ thể, nhập `HELP <lệnh>`.

Phải thoát các ký tự đặc biệt trong dòng lệnh. Để thoát các ký tự `&`, `|`, `(`, `)`, `<`, `>`, `^`, hãy sử dụng ký tự `^` (ví dụ: để sử dụng ký tự `&`, hãy nhập `^&`). Để thoát ký tự `%`, hãy nhập `%%`.

Cài đặt ứng dụng

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`.

Trước khi cài đặt ứng dụng trong chế độ im lặng, vui lòng mở và đọc Thỏa thuận giấy phép người dùng cuối và nội dung văn bản Chính sách quyền riêng tư. Thỏa thuận giấy phép người dùng cuối và nội dung văn bản Chính sách quyền riêng tư được kèm theo [gói phân phối Kaspersky Endpoint Security](#). Bạn chỉ có thể tiếp tục cài đặt ứng dụng nếu bạn đã đọc toàn bộ, hiểu rõ và chấp nhận các điều khoản của Thỏa thuận giấy phép người dùng cuối, bạn hiểu và đồng ý rằng dữ liệu của bạn sẽ được xử lý và truyền tải (bao gồm tới cả các quốc gia bên thứ ba) theo Chính sách quyền riêng tư, và bạn đã đọc toàn bộ và hiểu rõ Chính sách quyền riêng tư. Vui lòng không cài đặt Kaspersky Endpoint Security nếu bạn không chấp nhận các điều khoản của Thỏa thuận giấy phép người dùng cuối và Chính sách quyền riêng tư.

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

1. Chạy trình thông dịch dòng lệnh (cmd.exe) với tư cách quản trị viên.
2. Tới thư mục chứa gói phân phối Kaspersky Endpoint Security.
3. Chạy dòng lệnh sau:

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

hoặc

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

Kết quả là ứng dụng được cài đặt trên máy tính. Bạn có thể xác nhận rằng ứng dụng đã được cài đặt và kiểm tra thiết lập ứng dụng bằng cách thực thi lệnh [status](#).

EULA=1	<p>Chấp nhận 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.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>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.</p> </div>
PRIVACYPOLICY=1	<p>Chấp nhận Chính sách quyền riêng tư. Văn bản của Chính sách quyền riêng tư được bao gồm trong gói phân phối của Kaspersky Endpoint Security.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Để cài đặt ứng dụng hoặc nâng cấp ứng dụng phiên bản ứng dụng, bạn phải chấp nhận Chính sách quyền riêng tư.</p> </div>
KSN	<p>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 khả dụng:</p> <ul style="list-style-type: none"> • 1 – đồng ý tham gia KSN. • 0 – từ chối tham gia KSN (giá trị mặc định). <p>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.</p>
ALLOWREBOOT=1	<p>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.</p> <p>Không cần khởi động lại khi cài đặt Kaspersky Endpoint Security. Chỉ cần khởi động lại nếu bạn đã 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.</p>
SKIPPRODUCTCHECK=1	<p>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.</p>
SKIPPRODUCTUNINSTALL=1	<p>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.</p>

	<p>Không thể bật tính năng tự động gỡ bỏ phần mềm không tương thích khi cài đặt Kaspersky Endpoint Security bằng trình cài đặt msixexec. Hãy sử dụng setup_kes.exe để cho phép tự động gỡ bỏ phần mềm không tương thích.</p>
KLLOGIN	<p>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 KAdmin được sử dụng theo mặc định.</p>
KLPASSWD	<p>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).</p> <p>Nếu bạn quy định một mật khẩu nhưng không quy định tên người dùng với tham số KLLOGIN, tên người dùng mặc định KAdmin sẽ được sử dụng.</p>
KLPASSWDAREA	<p>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 khả dụng:</p> <ul style="list-style-type: none"> • 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. • REMOVE LIC – gỡ bỏ khóa. • REPORTS – xem báo cáo.
ENABLETRACES	<p>Bật hoặc tắt truy vết ứng dụng. Sau khi Kaspersky Endpoint Security khởi chạy, ứng dụng sẽ lưu các tập tin dấu vết vào thư mục %ProgramData%\Kaspersky Lab\KES\Traces. Giá trị khả dụng:</p> <ul style="list-style-type: none"> • 1 – truy vết được bật. • 0 – truy vết bị tắt (giá trị mặc định).
TRACESLEVEL	<p>Cấp chi tiết dấu vết. Giá trị khả dụng:</p> <ul style="list-style-type: none"> • 100 (nghiêm trọng). Chỉ thông báo về các 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 cảnh báo.

	<ul style="list-style-type: none"> • 400 (quan trọng). Tất cả các thông báo lỗi, cảnh báo và thông tin bổ sung. • 500 (bình thường). Thông báo về tất cả các lỗi và cảnh báo, cũng như thông tin chi tiết về hoạt động của ứng dụng trong chế độ bình thường (mặc định). • 600 (thấp). Tất cả các thông báo.
AMPPL	<p>Bật hoặc tắt tính năng bảo vệ các tiến trình Kaspersky Endpoint Security bằng công nghệ AM-PPL (Antimalware Protected Process Light). Để biết thêm chi tiết về công nghệ AM-PPL, vui lòng truy cập website Microsoft.</p> <p>Công nghệ AM-PPL có sẵn trên hệ điều hành Windows 10 phiên bản 1703 (RS2) hoặc mới hơn và Windows Server 2019.</p> <p>Giá trị khả dụng:</p> <ul style="list-style-type: none"> • 1 – Tính năng bảo vệ các tiến trình Kaspersky Endpoint Security bằng công nghệ AM-PPL được bật. • 0 – Tính năng bảo vệ các tiến trình Kaspersky Endpoint Security bằng công nghệ AM-PPL bị tắt.
RESTAPI	<p>Quản lý ứng dụng thông qua REST API. Để quản lý ứng dụng thông qua REST API, bạn phải chỉ định tên người dùng (tham số RESTAPI_User).</p> <p>Giá trị khả dụng:</p> <ul style="list-style-type: none"> • 1 - quản lý thông qua REST API được cho phép. • 0 - quản lý thông qua REST API bị chặn (giá trị mặc định). <p>Để quản lý ứng dụng thông qua REST API, bạn phải cho phép quản lý bằng các hệ thống quản trị. Để thực hiện, hãy đặt tham số AdminKitConnector=1. Nếu bạn quản lý ứng dụng thông qua REST API, bạn không thể quản lý ứng dụng bằng các hệ thống quản trị của Kaspersky.</p>
RESTAPI_User	<p>Tên người dùng của tài khoản miền Windows được sử dụng để quản lý ứng dụng thông qua REST API. Quản lý ứng dụng thông qua REST API chỉ khả dụng cho người dùng này. Nhập tên người dùng theo định dạng <DOMAIN>\<Tên người dùng> (ví dụ: RESTAPI_User=COMPANY\Administrator). Bạn chỉ có thể chọn một người dùng để làm việc với REST API.</p> <p>Thêm tên người dùng là điều kiện tiên quyết để quản lý ứng dụng thông qua REST API.</p>
RESTAPI_Port	<p>Cổng được sử dụng để quản lý ứng dụng thông qua REST API. Cổng 6782 được sử dụng theo mặc định.</p>
RESTAPI_Certificate	<p>Chứng chỉ để xác định các yêu cầu (ví dụ: RESTAPI_Certificate=C:\cert.pem). Tương tác bảo mật của Kaspersky Endpoint Security với máy khách REST yêu cầu định cấu hình nhận dạng yêu cầu. Để thực hiện, bạn phải cài đặt chứng chỉ và sau đó ký vào tải trọng của mỗi yêu cầu.</p>
ADMINKITCONNECTOR	<p>Quản lý ứng dụng bằng các hệ thống quản trị. Kaspersky Security Center là một ví dụ về hệ thống quản trị. Ngoài các hệ thống quản trị</p>

của Kaspersky, bạn có thể sử dụng các giải pháp của bên thứ ba. Kaspersky Endpoint Security cung cấp một API cho mục đích này.

Giá trị khả dụng:

- 1 - cho phép quản lý ứng dụng với sự trợ giúp của các hệ thống quản trị (giá trị mặc định).
- 0 - chỉ cho phép quản lý ứng dụng qua giao diện cục bộ.

Ví dụ:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1  
/pALLOWREBOOT=1
```

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

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

Sau khi Kaspersky Endpoint Security được cài đặt, giấy phép dùng thử sẽ được kích hoạt, trừ khi bạn cung cấp một mã kích hoạt trong [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 cần kích hoạt ứng dụng bằng giấy phép thương mại thông qua [Trình hướng dẫn kích hoạt ứng dụng](#) hoặc một [lệnh đặc biệt](#).

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 tổng quát để cài đặt ứng dụng
- [install.cfg](#) – thiết lập hoạt động 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. Bạn cũng có thể lưu tập tin setup.reg vào một thư mục khác. Nếu làm như vậy, bạn cần chỉ định đường dẫn đến tập tin trong lệnh cài đặt ứng dụng sau: SETUPREG=<đường dẫn đến tập tin setup.reg>.

Kích hoạt ứng dụng

Để kích hoạt ứng dụng từ dòng lệnh,

nhập chuỗi sau vào dòng lệnh:

```
avp.com license /add <mã kích hoạt hoặc tập tin mã khóa> [/login=<tên người dùng>  
/password=<mật khẩu>]
```

Bạn cần nhập thông tin tài khoản người dùng (/login=<tên người dùng> /password=<mật khẩu>) nếu [Mật khẩu bảo vệ được bật](#).

Gỡ bỏ ứng dụng

Bạn có thể gỡ bỏ Kaspersky Endpoint Security từ dòng lệnh bằng một trong các cách 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 gỡ bỏ được bắt đầu trong chế độ im lặng, bạn không cần tham gia vào quá trình gỡ bỏ. Để gỡ bỏ ứng dụng trong chế độ im lặng, sử dụng các tham số chuyển đổi /s và /qn.

Để gỡ bỏ ứng dụng trong chế độ im lặng:

1. Chạy trình thông dịch dòng lệnh (cmd.exe) với tư cách quản trị viên.
2. Tới thư mục chứa gói phân phối Kaspersky Endpoint Security.
3. Chạy dòng lệnh sau:

- Nếu tiến trình gỡ bỏ không [được bảo vệ bằng mật khẩu](#):

```
setup_kes.exe /s /x
```

hoặc

```
msiexec.exe /x <GUID> /qn
```

<GUID> và ID duy nhất của ứng dụng. Bạn có thể tìm ra GUID của ứng dụng bằng lệnh sau:

```
wmic product where "Name like '%Kaspersky Endpoint Security%' " get Name, IdentifyingNumber.
```

- Nếu tiến trình gỡ bỏ [được bảo vệ bằng mật khẩu](#):

```
setup_kes.exe /pKLLLOGIN=<tên người dùng> /pKLPASSWD=<mật khẩu> /s /x
```

hoặc

```
msiexec.exe /x <GUID> KLLLOGIN=<tên người dùng> KLPASSWD=<mật khẩu> /qn
```

Ví dụ:

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLLOGIN=KLAdmin  
KLPASSWD=!Password1 /qn
```

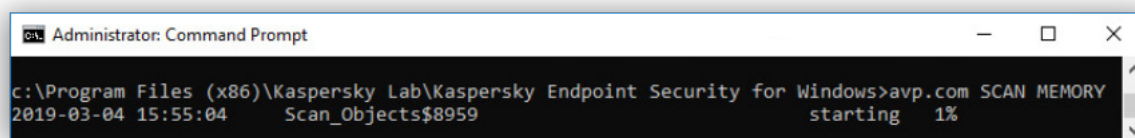
Các lệnh AVP

Để quản lý Kaspersky Endpoint Security từ dòng lệnh:

1. Chạy trình thông dịch dòng lệnh (cmd.exe) với tư cách quản trị viên.
2. Tới thư mục chứa tập tin thực thi Kaspersky Endpoint Security.
3. Để thực thi một lệnh, nhập:

```
avp.com <lệnh> [options]
```

Kết quả là, Kaspersky Endpoint Security sẽ thực thi lệnh đó (xem minh họa dưới đây.)



Quản lý ứng dụng từ dòng lệnh

SCAN. Quét virus

Chạy tác vụ quét virus.

Cú pháp lệnh

```
SCAN [<phạm vi quét>] [<hành động khi phát hiện mỗi đe dọa>] [<loại tập tin>] [<loại trừ quét>] [/R[A]:<tập tin báo cáo>] [<công nghệ quét>] [/C:<tập tin chứa thiết lập quét virus>]
```

Phạm vi quét	
<tập tin để quét>	Một danh sách các tập tin và thư mục được ngăn cách bởi dấu cách. Các đường dẫn dài phải nằm trong dấu ngoặc. Các đường dẫn ngắn (định dạng MS-DOS) không cần nằm trong dấu ngoặc. Ví dụ: <ul style="list-style-type: none">"C:\Program Files (x86)\Example Folder" - đường dẫn dài.C:\PROGRA~2\EXAMPL~1 - đường dẫn ngắn.
/ALL	Chạy tác vụ <i>Quét toàn bộ</i> . Kaspersky Endpoint Security sẽ quét các đối tượng sau: <ul style="list-style-type: none">Bộ nhớ kernelCác đối tượng được nạp lúc khởi động hệ điều hànhSector khởi độngBản sao lưu hệ điều hànhToàn bộ ổ cứng và ổ đĩa di động
/MEMORY	Quét bộ nhớ Kernel
/STARTUP	Quét các đối tượng được nạp lúc khởi động hệ điều hành
/MAIL	Quét hộp thư Outlook

/REMDRIVES	Quét ổ đĩa di động.
/FIXDRIVES	Quét ổ cứng.
/NETDRIVES	Quét ổ đĩa mạng.
/QUARANTINE	Quét các tập tin trong mục Sao lưu của Kaspersky Endpoint Security.
/@:<file list.lst>	<p>Quét các tập tin và thư mục từ một danh sách. Mỗi tập tin trong danh sách phải nằm trên một dòng mới. Các đường dẫn dài phải nằm trong dấu ngoặc. Các đường dẫn ngắn (định dạng MS-DOS) không cần nằm trong dấu ngoặc. Ví dụ:</p> <ul style="list-style-type: none"> "C:\Program Files (x86)\Example Folder" – đường dẫn dài. C:\PROGRA~2\EXAMPL~1 – đường dẫn ngắn.

Hành động khi phát hiện mối đe dọa	
/i0	Thông báo. Nếu tùy chọn này được sử dụng, Kaspersky Endpoint Security sẽ bổ sung thông tin về tập tin nhiễm mã độc vào danh sách các mối đe dọa đang hoạt động khi phát hiện những tập tin này.
/i1	Khử mã độc; chặn nếu không thể khử mã độc. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ tự động khử nhiễm tất cả các tập tin bị nhiễm virus được phát hiện. Nếu không thể khử mã độc, Kaspersky Endpoint Security sẽ bổ sung thông tin về tập tin nhiễm mã độc được phát hiện vào danh sách các mối đe dọa đang hoạt động.
/i2	Khử mã độc; xóa nếu không thể khử mã độc. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ tự động khử nhiễm tất cả các tập tin bị nhiễm virus được phát hiện. Nếu việc khử nhiễm thất bại, Kaspersky Endpoint Security sẽ xóa các tập tin đó. Hành động này được chọn theo mặc định.
/i3	Khử mã độc cho các tập tin nhiễm mã độc được phát hiện. Nếu không thể khử mã độc, xóa các tập tin nhiễm mã độc. Đồng thời xóa các tập tin hỗn hợp (ví dụ các tập nén) nếu tập tin nhiễm mã độc không thể bị khử mã độc hoặc xóa.
/i4	Xóa các tập tin nhiễm mã độc. Đồng thời xóa các tập tin hỗn hợp (ví dụ các tập nén) nếu tập tin nhiễm mã độc không thể bị xóa.

Loại tập tin	
/fe	Quét các tập tin theo phần mở rộng. Nếu thiết lập này được bật, Kaspersky Endpoint Security sẽ chỉ quét các tập tin có thể bị nhiễm virus . Sau đó, định dạng tập tin sẽ được xác định dựa trên phần mở rộng của tập tin.
/fi	Quét các tập tin theo định dạng. Nếu thiết lập này được bật, Kaspersky Endpoint Security sẽ chỉ quét các tập tin có thể bị nhiễm virus . Trước khi quét một tập tin để tìm mã độc, đầu đề nội bộ của tập tin sẽ được phân tích để xác định định dạng của tập tin đó (ví dụ, .txt, .doc, hoặc .exe). Tác vụ quét cũng tìm kiếm các tập tin có đuôi mở rộng tập tin cụ thể.
/fa	Tất cả tập tin. Nếu thiết lập này được bật, Kaspersky Endpoint Security sẽ kiểm tra tất cả các tập tin và không có ngoại lệ (tất cả định dạng và phần mở rộng).

Đây là cấu hình mặc định.

Loại trừ quét	
-e:a	Các tập nén RAR, ARJ, ZIP, CAB, LHA, JAR, và ICE được loại trừ khỏi phạm vi quét.
-e:b	Các cơ sở dữ liệu hộp thư, các e-mail đến và đi được loại trừ khỏi phạm vi quét.
-e:<tên đại diện tập tin>	Các tập tin khớp với tên đại diện tập tin được loại trừ khỏi phạm vi quét. Ví dụ: <ul style="list-style-type: none">Tên đại diện *.exe sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng exe.Tên đại diện example* sẽ bao gồm tất cả đường dẫn đến các tập tin tên là EXAMPLE.
-e:<giờ>	Các tập tin cần nhiều thời gian để quét hơn giới hạn quy định (tính theo giờ) được loại trừ khỏi phạm vi quét.
-es:<megabyte>	Các tập tin có kích cỡ lớn hơn giới hạn quy định (tính theo megabyte) được loại trừ khỏi phạm vi quét.

Lưu sự kiện vào chế độ tập tin báo cáo (chỉ dành cho cấu hình Quét, Trình cập nhật và Khôi phục)	
/R:<tập tin báo cáo>	Chỉ lưu các sự kiện nghiêm trọng đến tập tin báo cáo.
/RA:<tập tin báo cáo>	Lưu tất cả các sự kiện đến một tập tin báo cáo.

Công nghệ quét	
/iChecker=on off	Công nghệ này cho phép tăng tốc độ quét bằng cách loại trừ một số tập tin nhất định khỏi quá trình quét. Các tập tin được loại trừ khỏi quá trình quét bằng một thuật toán đặc biệt có tính đến ngày phát hành cơ sở dữ liệu Kaspersky Endpoint Security, ngày khi tập tin được quét lần cuối cùng và mọi thay đổi được thực hiện với thiết lập quét. Công nghệ iChecker có một số hạn chế: công nghệ này không hoạt động với tập tin lớn và chỉ áp dụng cho các tập tin có cấu trúc mà ứng dụng nhận dạng được (ví dụ như EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP và RAR).
/iSwift=on off	Công nghệ này cho phép tăng tốc độ quét bằng cách loại trừ một số tập tin nhất định khỏi quá trình quét. Các tập tin được loại trừ khỏi quá trình quét bằng một thuật toán đặc biệt có tính đến ngày phát hành cơ sở dữ liệu Kaspersky Endpoint Security, ngày mà tập tin được quét lần cuối cùng và mọi thay đổi được thực hiện với thiết lập quét. Công nghệ iSwift được cải tiến từ công nghệ iChecker cho hệ thống tập tin NTFS.

Thiết lập nâng cao	
/C:<tập tin chứa thiết lập>	Tập tin chứa thiết lập cho tác vụ quét virus. Tập tin này phải được tạo thủ công và lưu trong định dạng TXT. Tập tin này có các nội dung sau: [<phạm vi quét>] [<hành động khi phát hiện mối đe dọa>] [<loại tập tin>] [<loại trừ quét>] [/R[A]:<tập tin báo cáo>] [<công nghệ quét>].

lập quét
virus>

Ví dụ:

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All  
Users\My Documents" "C:\Program Files"
```

UPDATE. Cập nhật cơ sở dữ liệu và các mô-đun phần mềm ứng dụng

Chạy tác vụ *Cập nhật*.

Cú pháp lệnh

```
UPDATE [local] ["<nguồn cập nhật>"] [/R[A]:<tập tin báo cáo>] [/C:<tập tin chứa thiết  
lập cập nhật>]
```

Cấu hình tác vụ cập nhật	
local	<p>Bắt đầu tác vụ <i>Cập nhật</i> được tạo tự động sau khi ứng dụng được cài đặt. Bạn có thể thay đổi thiết lập của tác vụ <i>Cập nhật</i> trong giao diện ứng dụng cục bộ hoặc trong bảng điều khiển của Kaspersky Security Center. Nếu thiết lập này không được cấu hình, Kaspersky Endpoint Security sẽ bắt đầu tác vụ <i>Cập nhật</i> bằng thiết lập mặc định hoặc bằng thiết lập được chỉ định trong lệnh. Bạn có thể cấu hình thiết lập tác vụ <i>Cập nhật</i> như sau:</p> <ul style="list-style-type: none">• UPDATE bắt đầu tác vụ <i>Cập nhật</i> với thiết lập mặc định: nguồn cập nhật là máy chủ cập nhật Kaspersky, tài khoản là Hệ thống và các cài đặt mặc định khác.• UPDATE local bắt đầu tác vụ <i>Cập nhật</i> được tạo tự động sau khi cài đặt (tác vụ được định nghĩa trước).• UPDATE <thiết lập> bắt đầu tác vụ <i>Cập nhật</i> với thiết lập được định nghĩa theo cách thủ công (xem bên dưới).

Nguồn cập nhật	
"<nguồn cập nhật>"	<p>Địa chỉ của một máy chủ HTTP hoặc FTP, hoặc của một thư mục được chia sẻ chứa gói cập nhật. Bạn chỉ có thể xác định một nguồn cập nhật. Nếu nguồn cập nhật không được chỉ định, Kaspersky Endpoint Security sẽ sử dụng nguồn mặc định: các máy chủ cập nhật Kaspersky.</p>

Lưu sự kiện vào chế độ tập tin báo cáo (chỉ dành cho cấu hình Quét, Trình cập nhật và Khôi phục)	
/R:<tập tin báo cáo>	Chỉ lưu các sự kiện nghiêm trọng đến tập tin báo cáo.

/RA:<tập tin báo cáo>

Lưu tất cả các sự kiện đến một tập tin báo cáo.

Thiết lập nâng cao

/C:<tập tin chứa thiết lập cập nhật>

Tập tin chứa thiết lập cho tác vụ *Cập nhật*. Tập tin này phải được tạo thủ công và lưu trong định dạng TXT. Tập tin này có các nội dung sau: ["<nguồn cập nhật>"] [/R[A]:<tập tin báo cáo>].

Ví dụ:

```
avp.com UPDATE local
```

```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. Lần hoàn tác bản cập nhật gần nhất

Hoàn tác cập nhật cơ sở dữ liệu diệt virus gần nhất. Điều này cho phép bạn hoàn tác cơ sở dữ liệu và mô-đun ứng dụng về phiên bản trước đó khi cần thiết, 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.

Cú pháp lệnh

```
ROLLBACK [/R[A]:<tập tin báo cáo>]
```

Lưu sự kiện vào chế độ tập tin báo cáo (chỉ dành cho cấu hình Quét, Trình cập nhật và Khôi phục)

/R:<tập tin báo cáo>

Chỉ lưu các sự kiện nghiêm trọng đến tập tin báo cáo.

/RA:<tập tin báo cáo>

Lưu tất cả các sự kiện đến một tập tin báo cáo.

Ví dụ:

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Truy vết

Bật / tắt truy vết. [Các tập tin dấu vết](#) được lưu trữ trên máy tính của bạn 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, trừ tập tin dấu vết của Authentication Agent, được lưu trữ trong thư mục %ProgramData%\Kaspersky Lab\KES\Traces. Theo mặc định, truy vết được tắt.

Cú pháp lệnh

```
TRACES on|off [<cấp độ truy vết>] [<cấu hình nâng cao>]
```

Tracing level	
< cấp độ truy vết >	<p>Cấp chi tiết dấu vết. Giá trị khả dụng:</p> <ul style="list-style-type: none"> • <code>100</code> (nghiêm trọng). Chỉ thông báo về các lỗi nghiêm trọng. • <code>200</code> (cao). Thông báo về tất cả các lỗi, bao gồm lỗi nghiêm trọng. • <code>300</code> (chẩn đoán). Thông báo về tất cả các lỗi và cảnh báo. • <code>400</code> (quan trọng). Tất cả các thông báo lỗi, cảnh báo và thông tin bổ sung. • <code>500</code> (bình thường). Thông báo về tất cả các lỗi và cảnh báo, cũng như thông tin chi tiết về hoạt động của ứng dụng trong chế độ bình thường (mặc định). • <code>600</code> (thấp). Tất cả các thông báo.

Thiết lập nâng cao	
all	Chạy một lệnh với các tham số <code>dbg</code> , <code>file</code> và <code>mem</code> .
dbg	Sử dụng chức năng <code>OutputDebugString</code> và lưu tập tin dấu vết. Chức năng <code>OutputDebugString</code> gửi một chuỗi ký tự đến trình gỡ lỗi của ứng dụng để hiển thị trên màn hình. Để biết chi tiết, hãy truy cập website MSDN .
file	Lưu một tập tin dấu vết (không có giới hạn kích cỡ).
rot	Lưu dấu vết vào một số tập tin giới hạn với kích cỡ giới hạn và ghi đè lên các tập tin cũ khi kích cỡ tối đa bị vượt quá.
mem	Lưu dấu vết lên các tập tin kết xuất.

Ví dụ:

- `avp.com TRACES on 500`
- `avp.com TRACES on 500 dbg`
- `avp.com TRACES off`
- `avp.com TRACES on 500 dbg mem`
- `avp.com TRACES off file`

START. Bắt đầu hồ sơ

Bắt đầu hồ sơ (ví dụ, để cập nhật cơ sở dữ liệu hoặc bật một thành phần bảo vệ).

Cú pháp lệnh

START <hồ sơ> [/R[A]:<tập tin báo cáo>]

Hồ sơ	
<hồ sơ>	Tên hồ sơ. <i>Hồ sơ</i> là một thành phần, tác vụ hoặc tính năng của Kaspersky Endpoint Security. Bạn có thể xem danh sách các hồ sơ khả dụng bằng cách thực thi lệnh <code>HELP START</code> .

Lưu sự kiện vào chế độ tập tin báo cáo (chỉ dành cho cấu hình Quét, Trình cập nhật và Khôi phục)	
/R:<tập tin báo cáo>	Chỉ lưu các sự kiện nghiêm trọng đến tập tin báo cáo.
/RA:<tập tin báo cáo>	Lưu tất cả các sự kiện đến một tập tin báo cáo.

Ví dụ:

avp.com START Scan_Objects

STOP. Dừng một hồ sơ

Dừng hồ sơ đang chạy (ví dụ, dừng quét, dừng quét ổ đĩa di động, hoặc tắt một thành phần bảo vệ).

Để thực thi lệnh này, [Bảo vệ bằng mật khẩu phải được bật](#). Người dùng phải có quyền **Tắt các thành phần bảo vệ** và **Tắt các thành phần kiểm soát**.

Cú pháp lệnh

STOP <hồ sơ> /login=<tên người dùng> /password=<mật khẩu>

Hồ sơ	
<hồ sơ>	Tên hồ sơ. <i>Hồ sơ</i> là một thành phần, tác vụ hoặc tính năng của Kaspersky Endpoint Security. Bạn có thể xem danh sách các hồ sơ khả dụng bằng cách thực thi lệnh <code>HELP STOP</code> .

Chứng thực	
/login=<tên người dùng> /password=<mật khẩu>	Thông tin đăng nhập vào tài khoản người dùng với các quyền Bảo vệ bằng mật khẩu cần thiết.

STATUS. Trạng thái hồ sơ

Hiển thị thông tin trạng thái cho [hồ sơ ứng dụng](#) (ví dụ, `đang chạy` hoặc `đã hoàn tất`). Bạn có thể xem danh sách các hồ sơ khả dụng bằng cách thực thi lệnh `HELP STATUS`.

Kaspersky Endpoint Security cũng hiển thị thông tin về trạng thái của các hồ sơ bảo dưỡng. Thông tin về trạng thái của hồ sơ bảo dưỡng có thể là cần thiết khi bạn liên hệ với Hỗ trợ kỹ thuật của Kaspersky.

Cú pháp lệnh

```
avp.com STATUS [<hồ sơ>]
```

Nếu bạn nhập lệnh mà không có hồ sơ, Kaspersky Endpoint Security sẽ hiển thị trạng thái cho tất cả các hồ sơ của ứng dụng.

STATISTICS. Thống kê hoạt động của hồ sơ

Xem thông tin thống kê về một [hồ sơ ứng dụng](#) (ví dụ, thời lượng quét hoặc số mối đe dọa được phát hiện.) Bạn có thể xem danh sách các hồ sơ khả dụng bằng cách chạy lệnh `HELP STATISTICS`.

Cú pháp lệnh

```
STATISTICS <hồ sơ>
```

RESTORE. Khôi phục các tập tin từ Sao lưu

Bạn có thể khôi phục một tập tin từ Sao lưu đến thư mục gốc của nó. Nếu một tập tin có cùng tên đã tồn tại ở đường dẫn được chỉ định, ứng dụng sẽ yêu cầu xác nhận để thay thế tập tin. Tập tin đang được khôi phục sẽ được sao chép với tên gốc của nó.

Để thực thi lệnh này, [Bảo vệ bằng mật khẩu phải được bật](#). Bạn phải có quyền **Khôi phục từ Sao lưu**.

Sao lưu sẽ lưu trữ bản sao lưu của các tập tin đã bị xóa hoặc sửa đổi trong quá trình khử mã độc. *Bản sao lưu* là một bản sao của tập tin được tạo trước khi tập tin đó được khử nhiễm hay xóa. Các bản sao lưu của tập tin được lưu trữ trong một định dạng đặc biệt và không gây ra mối đe dọa.

Những bản sao lưu này được lưu trữ trong thư mục `C:\ProgramData\Kaspersky Lab\KES\QB`.

Người dùng trong nhóm Quản trị viên được cấp quyền truy cập toàn diện vào thư mục này. Quyền truy cập giới hạn vào thư mục này được cấp cho người dùng có tài khoản được sử dụng để cài đặt Kaspersky Endpoint Security.

Kaspersky Endpoint Security không có khả năng cấu hình quyền truy cập của người dùng vào các bản sao lưu tập tin.

Cú pháp lệnh

```
RESTORE [/REPLACE] <tên tập tin> /login=<tên người dùng> /password=<mật khẩu>
```

Thiết lập nâng cao	
/REPLACE	Ghi đè lên một tập tin hiện có.
<tên tập tin>	Tên của tập tin được khôi phục.

Chứng thực	
/login=<tên người dùng> /password=<mật khẩu>	Thông tin đăng nhập vào tài khoản người dùng với các quyền Bảo vệ bằng mật khẩu cần thiết.

Ví dụ:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

EXPORT. Xuất thiết lập ứng dụng

Xuất thiết lập của Kaspersky Endpoint Security ra một tập tin. Tập tin này sẽ nằm trong thư mục C:\Windows\SysWOW64.

Cú pháp lệnh

```
EXPORT <hồ sơ> <tên tập tin>
```

Hồ sơ	
<hồ sơ>	Tên hồ sơ. <i>Hồ sơ</i> là một thành phần, tác vụ hoặc tính năng của Kaspersky Endpoint Security. Bạn có thể xem danh sách các hồ sơ khả dụng bằng cách thực thi lệnh <code>HELP EXPORT</code> .

Tập tin để xuất	
<tên tập tin>	Tên của tập tin mà thiết lập ứng dụng sẽ được xuất ra đó. Bạn có thể xuất thiết lập của Kaspersky Endpoint Security ra một tập tin cấu hình DAT hoặc CFG, tập tin văn bản TXT hoặc tài liệu XML.

Ví dụ:

- avp.com EXPORT ids ids_config.dat
- avp.com EXPORT fm fm_config.txt

IMPORT. Nhập thiết lập ứng dụng

Nhập thiết lập cho Kaspersky Endpoint Security từ một tập tin đã được tạo với lệnh `EXPORT`.

Để thực thi lệnh này, [Bảo vệ bằng mật khẩu phải được bật](#). Người dùng phải có quyền **Cấu hình thiết lập của ứng dụng**.

Cú pháp lệnh

```
IMPORT <tên tập tin> /login=<tên người dùng> /password=<mật khẩu>
```

Tập tin để nhập	
<tên tập tin>	Tên của tập tin mà thiết lập ứng dụng sẽ được nhập từ đó. Bạn có thể nhập thiết lập của Kaspersky Endpoint Security từ một tập tin cấu hình DAT hoặc CFG, tập tin văn bản TXT hoặc tài liệu XML.

Chứng thực

```
/login=<tên người dùng>  
/password=<mật khẩu>
```

Thông tin đăng nhập vào tài khoản người dùng với các quyền [Bảo vệ bằng mật khẩu](#) cần thiết.

Ví dụ:

```
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1
```

ADDKEY. Áp dụng một tập tin khóa

Áp dụng tập tin khóa để kích hoạt Kaspersky Endpoint Security. Nếu ứng dụng đã được kích hoạt, khóa sẽ được thêm làm khóa dự trữ.

Cú pháp lệnh

```
ADDKEY <tên tập tin> /login=<tên người dùng> /password=<mật khẩu>
```

Key file

<tên tập tin>	Tên tập tin khóa.
---------------	-------------------

Chứng thực

```
/login=<tên người dùng>  
/password=<mật khẩu>
```

Thông tin tài khoản người dùng. Thông tin tài khoản chỉ cần được nhập nếu [Bảo vệ bằng mật khẩu](#) được bật.

Ví dụ:

```
avp.com ADDKEY file.key
```

LICENSE. Cấp giấy phép

Thực hiện các thao tác với các khóa giấy phép của Kaspersky Endpoint Security hoặc với các khóa của EDR Optimum hoặc EDR Expert (Tiện ích Kaspersky Endpoint Detection and Response).

Để thực thi lệnh này và gỡ bỏ một khóa giấy phép, [Bảo vệ bằng mật khẩu phải được bật](#). Người dùng phải có quyền **Xóa khóa**.

Cú pháp lệnh

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

Hoạt động	
/ADD <tên tập tin>	Áp dụng tập tin khóa để kích hoạt Kaspersky Endpoint Security. Nếu ứng dụng đã được kích hoạt, khóa sẽ được thêm làm khóa dự trữ.
/ADD <mã kích hoạt>	Kích hoạt Kaspersky Endpoint Security bằng một mã kích hoạt. Nếu ứng dụng đã được kích hoạt, khóa sẽ được thêm làm khóa dự trữ.
/REFRESH	Cập nhật trạng thái của giấy phép Kaspersky Endpoint Security. Do đó, ứng dụng nhận được thông tin trạng thái giấy phép cập nhật từ các máy chủ kích hoạt của Kaspersky.
/REFRESH EDR	Cập nhật trạng thái của giấy phép Tiện ích Kaspersky Endpoint Detection and Response. Do đó, ứng dụng nhận được thông tin trạng thái giấy phép cập nhật từ các máy chủ kích hoạt của Kaspersky.
/DEL /login=<tên người dùng> /password=<mật khẩu>	Xóa khóa giấy phép của ứng dụng. Khóa dự trữ cũng sẽ bị xóa.
/DEL EDR /login=<user name> /password=<password>	Xóa khóa giấy phép của Tiện ích Kaspersky Endpoint Detection and Response. Khóa dự trữ cũng sẽ bị xóa.

Chứng thực

```
/login=<tên người dùng>  
/password=<mật khẩu>
```

Thông tin đăng nhập vào tài khoản người dùng với các quyền [Bảo vệ bằng mật khẩu](#) cần thiết.

Ví dụ:

- avp.com LICENSE /ADD file.key
- avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
- avp.com LICENSE /DEL EDR /login=KLAdmin /password=!Password1

RENEW. Mua giấy phép

Mở website Kaspersky để mua hoặc gia hạn giấy phép của bạn.

PBATESTRESET. Đặt lại kết quả kiểm tra ổ đĩa trước khi mã hóa ổ đĩa

Đặt lại kết quả kiểm tra khả năng tương thích cho tính năng Mã hóa toàn bộ ổ đĩa (FDE), bao gồm cả công nghệ Kaspersky Disk Encryption và BitLocker Drive Encryption.

Trước khi chạy Mã hóa toàn bộ ổ đĩa, ứng dụng sẽ thực hiện một số bước kiểm tra để xác minh rằng máy tính có thể được mã hóa. Nếu máy tính không hỗ trợ tính năng Mã hóa toàn bộ ổ đĩa, Kaspersky Endpoint Security sẽ ghi lại thông tin về tình trạng không tương thích. Lần tới bạn cố mã hóa, ứng dụng sẽ không thực hiện kiểm tra này và cảnh báo với bạn rằng việc mã hóa không thể được thực hiện. Nếu cấu hình phần cứng của máy tính đã thay đổi, kết quả kiểm tra khả năng tương thích được ứng dụng ghi từ trước đó phải được đặt lại để có thể tái kiểm tra khả năng tương thích của ổ cứng hệ thống với công nghệ Kaspersky Disk Encryption hoặc BitLocker Drive Encryption.

EXIT. Thoát khỏi ứng dụng

Thoát Kaspersky Endpoint Security. Ứng dụng sẽ bị gỡ khỏi RAM máy tính.

Để thực thi lệnh này, [Bảo vệ bằng mật khẩu phải được bật](#). Người dùng phải có quyền **Thoát khỏi ứng dụng**.

Cú pháp lệnh

```
EXIT /login=<tên người dùng> /password=<mật khẩu>
```

EXITPOLICY. Tắt chính sách

Tắt một chính sách Kaspersky Security Center trên máy tính. Tất cả thiết lập của Kaspersky Endpoint Security đều có thể được cấu hình, bao gồm các thiết lập có khóa đóng trong chính sách (🔒).

Để thực thi lệnh này, [Bảo vệ bằng mật khẩu phải được bật](#). Người dùng phải có quyền **Tắt chính sách Kaspersky Security Center**.

Cú pháp lệnh

```
EXITPOLICY /login=<tên người dùng> /password=<mật khẩu>
```

STARTPOLICY. Bật chính sách

Bật một chính sách Kaspersky Security Center trên máy tính. Thiết lập ứng dụng phải được cấu hình theo chính sách.

DISABLE. Tắt bảo vệ

Tắt Bảo vệ mỗi đe dọa tập tin trên một máy tính có giấy phép Kaspersky Endpoint Security đã hết hạn. Bạn không thể chạy lệnh này trên một máy tính có ứng dụng chưa được kích hoạt hoặc có một giấy phép hợp lệ.

SPYWARE. Phát hiện phần mềm gián điệp

Bật / tắt phát hiện phần mềm gián điệp. Theo mặc định, tính năng phát hiện phần mềm gián điệp được bật.

Cú pháp lệnh

```
SPYWARE on|off
```

KSN. Chuyển đổi KSN Toàn cầu/Riêng

Chọn một giải pháp Kaspersky Security Network để xác định danh tiếng của các tập tin hoặc trang web. Kaspersky Endpoint Security hỗ trợ các giải pháp hạ tầng KSN sau đây:

- *KSN Toàn cầu* là giải pháp được hầu hết các ứng dụng Kaspersky sử dụng. Người tham gia vào KSN sẽ nhận thông tin từ Kaspersky Security Network và gửi cho Kaspersky thông tin về các đối tượng được xóa trên máy tính của người dùng. Đây là những đối tượng sẽ được các chuyên gia phân tích của Kaspersky phân tích thêm và sẽ được đưa vào cơ sở dữ liệu danh tiếng và thống kê của Kaspersky Security Network.
- *KSN Riêng* là một giải pháp cho phép người dùng máy tính lưu trữ Kaspersky Endpoint Security hoặc các ứng dụng khác của Kaspersky để có quyền truy cập cơ sở dữ liệu danh tiếng của Kaspersky Security Network và truy cập các dữ liệu thống kê khác mà không cần gửi dữ liệu cho KSN từ máy tính của riêng họ. KSN Riêng được thiết kế dành cho khách hàng doanh nghiệp không thể tham gia vào Kaspersky Security Network vì bất kỳ lý do nào dưới đây:
 - Các máy trạm cục bộ không được kết nối vào mạng Internet.
 - Việc truyền tải bất kỳ dữ liệu nào bên ngoài quốc gia hoặc bên ngoài mạng LAN của doanh nghiệp đều bị cấm theo luật pháp hoặc bị hạn chế bởi các chính sách bảo mật của doanh nghiệp.

Cú pháp lệnh

```
KSN /global | /private <tên tập tin>
```

Tập tin cấu hình KSN Riêng	
<tên tập tin>	Tên của tập tin cấu hình chứa thiết lập máy chủ proxy KSN. Tập tin này có đuôi mở rộng là PKCS7 hoặc PEM.
Ví dụ:	

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

Các lệnh KESCLI

Các lệnh KESCLI cho phép bạn nhận thông tin về trạng thái bảo vệ máy tính bằng thành phần OPSWAT, và cho phép bạn thực hiện các tác vụ tiêu chuẩn như quét virus và cập nhật cơ sở dữ liệu.

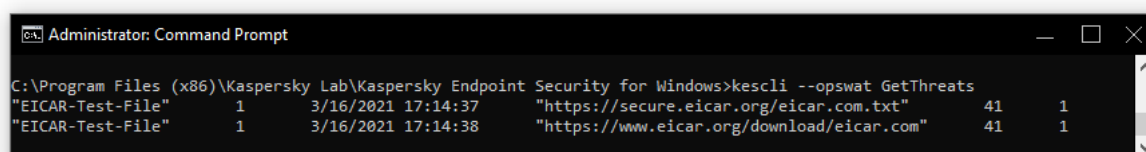
Bạn có thể xem danh sách các lệnh KESCLI bằng cách sử dụng lệnh `--help` hoặc bằng cách sử dụng lệnh viết tắt `-h`.

Để quản lý Kaspersky Endpoint Security từ dòng lệnh:

1. Chạy trình thông dịch dòng lệnh (cmd.exe) với tư cách quản trị viên.
2. Tới thư mục chứa tập tin thực thi Kaspersky Endpoint Security.
3. Để thực thi một lệnh, nhập:

```
kescli <lệnh> [tùy chọn]
```

Kết quả là, Kaspersky Endpoint Security sẽ thực thi lệnh đó (xem minh họa dưới đây.)



```
Administrator: Command Prompt
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>kescli --opswat GetThreats
"EICAR-Test-File" 1 3/16/2021 17:14:37 "https://secure.eicar.org/eicar.com.txt" 41 1
"EICAR-Test-File" 1 3/16/2021 17:14:38 "https://www.eicar.org/download/eicar.com" 41 1
```

Quản lý ứng dụng từ dòng lệnh

Quét. Quét virus

Chạy tác vụ quét virus.

Để chạy tác vụ, quản trị viên phải [Cho phép sử dụng tác vụ cục bộ trong chính sách](#).

Cú pháp lệnh

```
kescli --opswat Scan "<phạm vi quét>" <hành động khi phát hiện mối đe dọa>
```

Bạn có thể kiểm tra trạng thái hoàn thành của tác vụ *Quét toàn bộ* bằng lệnh [GetScanState](#) và xem ngày tháng và thời gian khi tác vụ được hoàn thành gần đây nhất bằng lệnh [GetLastScanTime](#).

Phạm vi quét	
<tập tin để quét>	Một danh sách các tập tin và thư mục được ngăn cách bởi dấu <code>;</code> . Ví dụ: <code>"C:\Program Files (x86)\Example Folder"</code> .

Hành động khi phát hiện mối đe dọa	
0	Thông báo. Nếu tùy chọn này được sử dụng, Kaspersky Endpoint Security sẽ bổ sung thông tin về tập tin nhiễm mã độc vào danh sách các mối đe dọa đang hoạt động khi phát hiện những tập tin này.
1	Khử mã độc; xóa nếu không thể khử mã độc. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ tự động khử nhiễm tất cả các tập tin bị nhiễm virus được phát hiện. Nếu việc khử nhiễm thất bại, Kaspersky Endpoint Security sẽ xóa các tập tin đó. Hành động này được chọn theo mặc định.

Ví dụ:

```
kescli --opswat Scan "C:\Documents and Settings\All Users\My Documents;C:\Program Files" 1
```

GetScanState. Trạng thái hoàn thành tác vụ quét

Nhận thông tin về trạng thái hoàn thành tác vụ *Quét toàn bộ*:

- 1 – tác vụ đang diễn ra.
- 0 – tác vụ đang không chạy.

Cú pháp lệnh

```
--opswat GetScanState
```

Ví dụ:

```
kescli --opswat GetScanState
```

GetLastScanTime. Xác định thời gian hoàn thành tác vụ quét

Nhận thông tin về ngày tháng và thời gian hoàn thành tác vụ *Quét toàn bộ* gần đây nhất.

Cú pháp lệnh

```
kescli --opswat GetLastScanTime
```

GetThreats. Nhận dữ liệu về các mối đe dọa được phát hiện

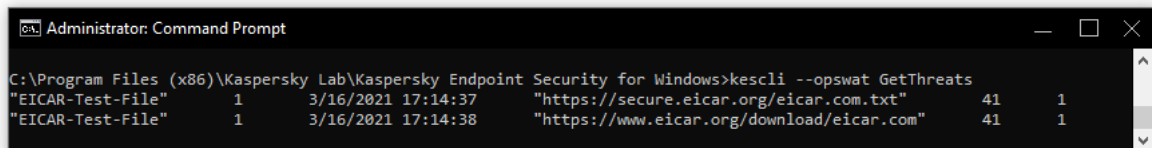
Nhận một danh sách các mối đe dọa được phát hiện (*Báo cáo về các mối đe dọa*). Báo cáo này chứa thông tin về các mối đe dọa và hoạt động của virus trong vòng 30 ngày gần đây nhất, trước khi tạo báo cáo.

Cú pháp lệnh

```
--opswat GetThreats
```

Khi lệnh này được thực thi, Kaspersky Endpoint Security sẽ gửi một phản hồi theo định dạng sau:

<tên của đối tượng được phát hiện> <loại đối tượng> <ngày tháng và thời gian phát hiện>
<đường dẫn đến tập tin> <hành động khi phát hiện mối đe dọa> <mức độ nguy hiểm của mối đe dọa>



```
Administrator: Command Prompt
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>kescli --opswat GetThreats
"EICAR-Test-File" 1 3/16/2021 17:14:37 "https://secure.eicar.org/eicar.com.txt" 41 1
"EICAR-Test-File" 1 3/16/2021 17:14:38 "https://www.eicar.org/download/eicar.com" 41 1
```

Quản lý ứng dụng từ dòng lệnh

Object type	
0	Chưa biết (Unknown).
1	Virus (Virware).
2	Chương trình Trojan (Trojware).
3	Chương trình độc hại (Malware).
4	Chương trình quảng cáo (Adware).
5	Chương trình quay số tự động (Pornware).
6	Các ứng dụng có thể được sử dụng bởi tội phạm mạng để gây hại cho máy tính hoặc dữ liệu của người dùng (Riskware).
7	Đối tượng được đóng gói mà phương thức đóng gói có thể được sử dụng để bảo vệ các mã độc hại (Packed).
20	Các đối tượng không xác định (Xfiles).
21	Các ứng dụng đã biết (Software).
22	Các tập tin bị ẩn (Hidden).
23	Các ứng dụng cần lưu ý (Pupware).
24	Hành vi bất thường (Anomaly).

30	Chưa được xác định (Undetect).
40	Bảng quảng cáo (Banner).
50	Tấn công mạng (Attack).
51	Truy cập Registry (Registry).
52	Hành động đáng ngờ (Suspicion).
60	Lỗi hỏng bảo mật (Vulnerability).
70	Phishing.
80	Tập tin đính kèm email không mong muốn (Attachment).
90	Phần mềm độc hại được phát hiện bởi Kaspersky Security Network (Urgent).
100	Liên kết không xác định (Suspicious URL).
110	Phần mềm độc hại khác (Behavioral).

Hành động khi phát hiện mối đe dọa	
0	Chưa biết (unknown).
1	Mối đe dọa đã được khắc phục (ok).
2	Đối tượng đã bị nhiễm mã độc và chưa được khử mã độc (infected).
5	Đối tượng là một tập tin nén và chưa bị nhiễm mã độc (archive).
9	Đối tượng đã được khử mã độc (disinfected).
10	Đối tượng chưa được khử mã độc (not disinfected).
11	Đối tượng đã bị xóa (deleted).
13	Một bản sao lưu của đối tượng được tạo ra (backupped).
15	Đối tượng đã được chuyển vào mục Sao lưu (quarantined).
23	Đối tượng đã bị xóa khi máy tính khởi động lại (delete on reboot).
25	Đối tượng đã được khử mã độc khi máy tính khởi động lại (disinfect on reboot).
29	Đối tượng đã được người dùng chuyển vào mục Sao lưu (added by user).
30	Đối tượng đã được thêm vào loại trừ (added to exclude).
31	Đối tượng đã được chuyển vào mục Sao lưu khi máy tính khởi động lại (quarantine on reboot).
36	Báo động giả (false alarm).
38	Tiến trình đã bị chấm dứt (terminated).
40	Đối tượng không được phát hiện (not found).
41	Không thể khắc phục mối đe dọa (untreatable).
42	Đối tượng đã được khôi phục (rolled back).
43	Đối tượng đã được tạo do kết quả của hoạt động của mối đe dọa (produced by threat).

44	Đối tượng đã được khôi phục khi máy tính khởi động lại (roll back on reboot).
0xffffffff	Đối tượng chưa được xử lý (discarded).

Mức độ nguy hiểm của mỗi đe dọa	
0	Chưa biết
1	Cao
2	quét vừa
4	Thấp
8	Thông tin (ít hơn <i>Thấp</i>)

UpdateDefinitions. Cập nhật cơ sở dữ liệu và các mô-đun phần mềm ứng dụng

Chạy tác vụ *Cập nhật*. Kaspersky Endpoint Security sử dụng nguồn mặc định: máy chủ cập nhật của Kaspersky.

Để chạy tác vụ, quản trị viên phải [Cho phép sử dụng tác vụ cục bộ trong chính sách](#).

Cú pháp lệnh

```
kescli --opswat UpdateDefinitions
```

Bạn có thể xem ngày tháng và thời gian phát hành của cơ sở dữ liệu chống virus hiện hành bằng lệnh [GetDefinitionsetState](#).

GetDefinitionState. Xác định thời gian hoàn thành tác vụ cập nhật

Nhận thông tin về ngày tháng và thời gian phát hành cơ sở dữ liệu chống virus đang được sử dụng.

Cú pháp lệnh

```
kescli --opswat GetDefinitionState
```

EnableRTP. Bật bảo vệ

Bật các thành phần bảo vệ của Kaspersky Endpoint Security trên máy tính: Bảo vệ mối đe dọa tập tin, Bảo vệ mối đe dọa web, Bảo vệ mối đe dọa thư điện tử, Bảo vệ mối đe dọa mạng, Phòng chống xâm nhập máy chủ.

Để bật các thành phần bảo vệ, quản trị viên phải đảm bảo rằng có thể sửa đổi thiết lập chính sách liên quan (🔒 thuộc tính được mở).

Cú pháp lệnh

```
kescli --opswat EnableRTP
```

Do đó, các thành phần bảo vệ được bật ngay cả khi bạn đã cấm sửa đổi thiết lập ứng dụng bằng [Bảo vệ bằng mật khẩu](#).

Bạn có thể kiểm tra trạng thái hoạt động của thành phần Bảo vệ mối đe dọa tập tin bằng lệnh [GetRealTimeProtectionState](#).

GetRealTimeProtectionState. Trạng thái của thành phần Bảo vệ mối đe dọa tập tin

Nhận thông tin về trạng thái hoạt động của thành phần Bảo vệ mối đe dọa tập tin:

- 1 – thành phần đang được bật.
- 0 – thành phần đang bị tắt.

Cú pháp lệnh

```
kescli --opswat GetRealTimeProtectionState
```

Phiên bản. Xác định phiên bản của ứng dụng

Xác định phiên bản của Kaspersky Endpoint Security cho Windows.

Cú pháp lệnh

```
--Version
```

Bạn cũng có thể sử dụng lệnh viết tắt `-v`.

Ví dụ:
`kescli -v`

Lệnh quản lý Detection and Response

Bạn có thể sử dụng dòng lệnh để quản lý chức năng tích hợp của các giải pháp Detection and Response (ví dụ: Kaspersky Sandbox hoặc Kaspersky Endpoint Detection and Response Optimum). Bạn có thể quản lý các giải pháp Detection and Response nếu không thể quản lý bằng bảng điều khiển Kaspersky Security Center. Bạn có thể xem danh sách các lệnh để quản lý ứng dụng bằng cách thực thi lệnh `HELP`. Để đọc về cú pháp của một lệnh cụ thể, nhập `HELP <lệnh>`.

Để quản lý các tính năng tích hợp của giải pháp Detection and Response bằng dòng lệnh:

1. Chạy trình thông dịch dòng lệnh (cmd.exe) với tư cách quản trị viên.
2. Tới thư mục chứa tập tin thực thi Kaspersky Endpoint Security.
3. Để thực thi một lệnh, nhập:

```
avp.com <lệnh> [options]
```

Kết quả là, Kaspersky Endpoint Security sẽ thực thi lệnh đó (xem minh họa dưới đây.)

SANDBOX. Quản lý Kaspersky Sandbox

Các lệnh để quản lý thành phần Kaspersky Sandbox:

- **Bật hoặc tắt thành phần Kaspersky Sandbox.**
Thành phần Kaspersky Sandbox cho phép tương tác với giải pháp Kaspersky Sandbox.
- **Cấu hình thành phần Kaspersky Sandbox:**
 - **Kết nối máy tính với máy chủ Kaspersky Sandbox.**
Các máy chủ sử dụng ảnh máy ảo đã triển khai của hệ điều hành Microsoft Windows để chạy các đối tượng cần được quét. Bạn có thể nhập địa chỉ IP (IPv4 hoặc IPv6) hoặc tên miền đầy đủ. Để biết chi tiết về việc triển khai ảnh máy ảo và cấu hình máy chủ Kaspersky Sandbox, hãy tham khảo [Trợ giúp của Kaspersky Sandbox](#).
 - **Cấu hình thời gian chờ kết nối cho máy chủ Kaspersky Sandbox.**
Thời gian chờ nhận phản hồi cho yêu cầu quét đối tượng từ máy chủ Kaspersky Sandbox. Sau khi hết thời gian chờ, Kaspersky Sandbox sẽ chuyển hướng yêu cầu đến máy chủ tiếp theo. Giá trị thời gian chờ phụ thuộc vào tốc độ và độ ổn định của kết nối. Giá trị mặc định là 5 giây.
 - **Cấu hình kết nối được tin tưởng giữa máy tính và máy chủ Kaspersky Sandbox.**
Để cấu hình kết nối được tin tưởng với máy chủ Kaspersky Sandbox, bạn phải chuẩn bị chứng chỉ TLS. Tiếp theo, bạn phải thêm chứng chỉ vào máy chủ Kaspersky Sandbox và chính sách Kaspersky Endpoint Security. Để biết chi tiết về cách chuẩn bị chứng chỉ và thêm chứng chỉ vào máy chủ, hãy tham khảo [Trợ giúp của Kaspersky Sandbox](#).
- **Hiển thị thiết lập hiện tại của thành phần.**

Cú pháp lệnh

```
stop sandbox [/login=<tên người dùng> /password=<mật khẩu>]
start sandbox
sandbox /set [--tls=yes|no] [--servers=<địa chỉ máy chủ>:<port>] [--timeout=<thời gian>
```

```
chờ kết nối máy chủ Kaspersky Sandbox (ms)>] [--pinned-certificate=<đường dẫn đến chứng chỉ TLS>][/login=<tên người dùng> /password=<mật khẩu>] sandbox /show
```

Hoạt động	
stop	Tắt thành phần Kaspersky Sandbox.
start	Bật thành phần Kaspersky Sandbox.
set	Cấu hình thành phần Kaspersky Sandbox. Bạn có thể sửa đổi các thiết lập sau: <ul style="list-style-type: none">• Sử dụng kết nối được tin tưởng (--tls);• Thêm một chứng chỉ TLS (--pinned-certificate);• Đặt thời gian chờ kết nối máy chủ Kaspersky Sandbox (--timeout);• Thêm máy chủ Kaspersky Sandbox (--servers).
show	Hiển thị thiết lập hiện tại của thành phần. Bạn nhận được phản hồi sau: sandbox.timeout=<thời gian chờ kết nối máy chủ Kaspersky Sandbox (ms)> sandbox.tls=<trạng thái kết nối được tin tưởng> sandbox.servers=<danh sách máy chủ Kaspersky Sandbox>

Chứng thực	
/login=<tên người dùng> /password=<mật khẩu>	Thông tin đăng nhập vào tài khoản người dùng với các quyền Bảo vệ bằng mật khẩu cần thiết.

Ví dụ:

```
avp.com start sandbox  
avp.com sandbox /set --tls=yes --pinned-certificate="C:\Users\Admin\certificate.pem"  
avp.com sandbox /set --servers=10.10.111.0:147
```

PHÒNG CHỐNG. Quản lý phòng chống thực thi

Tắt Phòng chống thực thi hoặc hiển thị thiết lập thành phần hiện tại, bao gồm danh sách các quy tắc phòng chống thực thi.

Cú pháp lệnh

```
prevention disable  
prevention /show
```

Sau khi thực thi lệnh `prevention /show`, bạn sẽ nhận phản hồi sau:

```
prevention.enable=true|false
```

```
prevention.mode=audit|prevent
```

prevention.rules

id: <rule ID>

target: script|process|document

md5: <giá trị băm MD5 của tập>

sha256: <giá trị băm SHA256 của tập>

pattern: <đường dẫn đến đối tượng>

case-sensitive: true|false

Các giá trị trả về của lệnh:

- -1 có nghĩa là lệnh không được hỗ trợ bởi phiên bản của ứng dụng được cài đặt trên máy tính.
- 0 có nghĩa là lệnh đã được thực thi thành công.
- 1 có nghĩa là một đối số bắt buộc không được truyền vào cho lệnh.
- 2 có nghĩa là một lỗi chung đã xảy ra.
- 4 có nghĩa là đã xảy ra lỗi cú pháp.
- 9 - hoạt động sai (ví dụ: cố gắng tắt thành phần khi thành phần đã bị tắt).

CÁCH LY. Quản lý cách ly mạng

Tắt Cách ly mạng của máy tính hoặc hiển thị thiết lập hiện tại của thành phần. Thiết lập thành phần cũng bao gồm danh sách kết nối mạng được thêm vào mục loại trừ.

Cú pháp lệnh:

```
isolation /OFF /login=<tên người dùng> /password=<mật khẩu>  
isolation /STAT
```

Kết quả của việc chạy lệnh `stat` là bạn nhận được phản hồi sau: `Network isolation on|off`.

RESTORE. Khôi phục các tập tin từ Khu vực cách ly

Bạn có thể khôi phục một tập tin từ Khu vực cách ly đến thư mục gốc của nó. Nếu thư mục đích đã bị xóa, ứng dụng sẽ đặt tập tin đó vào một thư mục đặc biệt trên máy tính. Sau đó bạn phải di chuyển tập tin vào thư mục đích theo cách thủ công. *Khu vực cách ly* là một kho lưu trữ cục bộ đặc biệt trên máy tính. Người dùng có thể cách ly các tập tin mà người dùng coi là nguy hiểm cho máy tính. Các tập tin cách ly được lưu trữ ở trạng thái mã hóa và không đe dọa đến tính bảo mật của thiết bị. Kaspersky Endpoint Security chỉ sử dụng Khu vực cách ly khi làm việc với các giải pháp Kaspersky Sandbox và Kaspersky Endpoint Detection and Response. Trong các trường hợp khác, Kaspersky Endpoint Security sẽ đặt các tập tin liên quan vào [Sao lưu](#). Để biết chi tiết về quản lý khu vực cách ly làm một phần của các giải pháp, vui lòng tham khảo [Trợ giúp của Kaspersky Sandbox](#), [Trợ giúp của Kaspersky Endpoint Detection and Response Optimum](#) và [Trợ giúp của Kaspersky Endpoint Detection and Response Expert](#).

Để thực thi lệnh này, [Bảo vệ bằng mật khẩu phải được bật](#). Bạn phải có quyền **Khôi phục từ Sao lưu**.

Đối tượng được cách ly dưới quyền tài khoản hệ thống (SYSTEM).

Cú pháp lệnh

```
avp.com RESTORE [/REPLACE] <tên tập tin> /login=<tên người dùng> /password=<mật khẩu>
```

Thiết lập nâng cao	
/REPLACE	Ghi đè lên một tập tin hiện có.
<tên tập tin>	Tên của tập tin được khôi phục.

Chứng thực	
/login=<tên người dùng> /password=<mật khẩu>	Thông tin đăng nhập vào tài khoản người dùng với các quyền Bảo vệ bằng mật khẩu cần thiết.

Ví dụ:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

Các giá trị trả về của lệnh:

- -1 có nghĩa là lệnh không được hỗ trợ bởi phiên bản của ứng dụng được cài đặt trên máy tính.
- 0 có nghĩa là lệnh đã được thực thi thành công.
- 1 có nghĩa là một đối số bắt buộc không được truyền vào cho lệnh.
- 2 có nghĩa là một lỗi chung đã xảy ra.
- 4 có nghĩa là đã xảy ra lỗi cú pháp.

IOCSCAN. Quét các dấu hiệu về sự xâm nhập (IOC)

Chạy tác vụ Quét các dấu hiệu về sự xâm nhập (IOC). Một *Dấu hiệu về sự xâm nhập (IOC)* là một tập hợp dữ liệu về một đối tượng hoặc hoạt động cho biết sự truy cập trái phép vào máy tính (xâm nhập dữ liệu). Ví dụ: nhiều nỗ lực đăng nhập không thành công vào hệ thống có thể cấu thành một Dấu hiệu về sự xâm nhập. Tác vụ *Quét IOC* cho phép tìm các Dấu hiệu về sự xâm nhập trên máy tính và thực hiện các biện pháp ứng phó với mỗi đe dọa.

Cú pháp lệnh

```
IOCSCAN <đường dẫn đầy đủ đến tập tin IOC> [/path=<đường dẫn đến thư mục tập tin IOC>  
[/process=on|off] [/hint=<đường dẫn đầy đủ đến tập tin thực thi của một tiến trình|  
đường dẫn tập tin đầy đủ>] [/registry=on|off] [/dnsentry=on|off] [/arpentry=on|off]  
[/ports=on|off] [/services=on|off] [/system=on|off] [/users=on|off] [/volumes=on|off]  
[/eventlog=on|off] [/datetime=<event publication date>] [/channels=<list of channels>]  
[/files=on|off] [/drives=<tất cả|hệ thống|quan trọng|tùy chỉnh>] [/excludes=<danh sách  
loại trừ>] [/scope=<danh sách thư mục cần quét>]
```

IOC files	
<đường dẫn đầy đủ đến tập tin IOC>	Đường dẫn đầy đủ đến tập tin IOC mà bạn muốn sử dụng để quét. Bạn có thể chỉ định nhiều tập tin IOC được phân tách bằng dấu cách. Đường dẫn đầy đủ đến tập tin IOC phải được nhập mà không có đối số /path. Ví dụ: C:\Users\Admin\Desktop\IOC\file1.ioc
/path=<đường dẫn đến thư mục có tập tin IOC>	Đường dẫn đến thư mục có tập tin IOC mà bạn muốn sử dụng để quét. <i>Tập tin IOC</i> là các tập tin chứa các tập hợp dấu hiệu mà ứng dụng cố gắng đối chiếu để đếm một lần phát hiện. Các tập tin IOC phải tuân theo tiêu chuẩn OpenIOC . Ví dụ: C:\Users\Admin\Desktop\IOC

Loại dữ liệu để quét IOC	
/process=on off	Phân tích dữ liệu tiến trình khi thực hiện quét IOC (từ ProcessItem). Nếu giá trị của đối số là off thì Kaspersky Endpoint Security sẽ không phân tích các tiến trình đang chạy trên máy tính khi thực hiện quét. Nếu tập tin IOC chứa các từ IOC của tài liệu IOC ProcessItem, chúng sẽ bị bỏ qua (được phát hiện là không khớp). Nếu đối số không được chỉ định, Kaspersky Endpoint Security chỉ phân tích dữ liệu tiến trình nếu tài liệu IOC ProcessItem được mô tả trong tập tin IOC được cung cấp cho tác vụ quét.
/hint=<đường dẫn đầy đủ đến tập tin thực thi của tiến trình đường dẫn đầy đủ của tập tin>	Phân tích dữ liệu tập tin khi thực hiện quét IOC (từ ProcessItem và FileItem). Bạn có thể chọn một tập tin theo một trong những cách sau đây: <ul style="list-style-type: none"> • <đường dẫn đầy đủ đến tập tin thực thi của tiến trình> - ProcessItem; • <đường dẫn đầy đủ đến tập tin> - FileItem.
/registry=on off	Phân tích dữ liệu registry của Windows khi thực hiện quét IOC (từ RegistryItem). Nếu giá trị của đối số là off thì Kaspersky Endpoint Security sẽ không quét registry của Windows. Nếu tập tin IOC chứa các từ tài liệu IOC RegistryItem, chúng sẽ bị bỏ qua (được phát hiện là không khớp). Nếu đối số không được chỉ định, Kaspersky Endpoint Security chỉ phân tích registry của Windows nếu tài liệu IOC RegistryItem được mô tả trong tập tin IOC được cung cấp cho tác vụ quét. Với loại dữ liệu RegistryItem, Kaspersky Endpoint Security sẽ quét một tập hợp các khóa registry .
/dnsentry=on off	Phân tích dữ liệu về các bản ghi trong bộ đệm DNS cục bộ khi thực hiện quét IOC (từ DnsEntryItem). Nếu giá trị của đối số là off thì Kaspersky Endpoint Security sẽ không quét bộ đệm DNS cục bộ. Nếu tập tin IOC chứa các từ tài liệu IOC DnsEntryItem, chúng sẽ bị bỏ qua (được phát hiện là không khớp).

	<p>Nếu đối số không được chỉ định, Kaspersky Endpoint Security chỉ phân tích bộ đệm DNS cục bộ nếu tài liệu IOC DnsEntryItem được mô tả trong tập tin IOC được cung cấp cho tác vụ quét.</p>
/arpentry=on off	<p>Phân tích dữ liệu về các bản ghi trong bảng ARP khi thực hiện quét IOC (từ ArpEntryItem).</p> <p>Nếu giá trị của đối số là off, Kaspersky Endpoint Security không quét bảng ARP. Nếu tập tin IOC chứa các từ tài liệu IOC ArpEntryItem, chúng sẽ bị bỏ qua (được phát hiện là không khớp).</p> <p>Nếu đối số không được chỉ định, Kaspersky Endpoint Security chỉ phân tích bảng ARP nếu tài liệu IOC ArpEntryItem được mô tả trong tập tin IOC được cung cấp cho tác vụ quét.</p>
/ports=on off	<p>Phân tích dữ liệu về các cổng mở để nghe khi thực hiện quét IOC (từ PortItem).</p> <p>Nếu giá trị của đối số là off, Kaspersky Endpoint Security không quét bảng các kết nối đang hoạt động trên thiết bị. Nếu tập tin IOC chứa các từ tài liệu PortItem, chúng sẽ bị bỏ qua (được phát hiện là không khớp).</p> <p>Nếu đối số không được chỉ định, Kaspersky Endpoint Security chỉ phân tích bảng các kết nối đang hoạt động nếu tài liệu IOC PortItem được mô tả trong tập tin IOC được cung cấp cho tác vụ quét.</p>
/services=on off	<p>Phân tích dữ liệu về các dịch vụ được cài đặt trên thiết bị khi thực hiện quét IOC (từ ServiceItem).</p> <p>Nếu giá trị của đối số là off, Kaspersky Endpoint Security không quét dữ liệu về các dịch vụ được cài đặt trên thiết bị. Nếu tập tin IOC chứa các từ tài liệu IOC ServiceItem, chúng sẽ bị bỏ qua (được phát hiện là không khớp).</p> <p>Nếu đối số không được chỉ định, Kaspersky Endpoint Security chỉ phân tích dữ liệu dịch vụ nếu tài liệu IOC ServiceItem được mô tả trong tập tin IOC được cung cấp cho tác vụ quét.</p>
/system=on off	<p>Phân tích dữ liệu môi trường khi thực hiện quét IOC (từ SystemInfoItem).</p> <p>Nếu giá trị của đối số là off, Kaspersky Endpoint Security không phân tích dữ liệu môi trường. Nếu tập tin IOC chứa các từ tài liệu IOC SystemInfoItem, chúng sẽ bị bỏ qua (được phát hiện là không khớp).</p> <p>Nếu đối số không được chỉ định, Kaspersky Endpoint Security chỉ phân tích dữ liệu môi trường nếu tài liệu IOC SystemInfoItem được mô tả trong tập tin IOC được cung cấp cho tác vụ quét.</p>
/users=on off	<p>Phân tích dữ liệu về người dùng khi thực hiện quét IOC (từ UserItem).</p> <p>Nếu giá trị của đối số là off, Kaspersky Endpoint Security không phân tích dữ liệu về người dùng được tạo trong hệ thống. Nếu tập tin IOC chứa các từ tài liệu IOC UserItem, chúng sẽ bị bỏ qua (được phát hiện là không khớp).</p> <p>Nếu đối số không được chỉ định, Kaspersky Endpoint Security chỉ phân tích dữ liệu về người dùng được tạo trong hệ thống nếu tài liệu IOC UserItem được mô tả trong tập tin IOC được cung cấp để quét.</p>
/volumes=on off	<p>Phân tích dữ liệu về phân vùng khi thực hiện quét IOC (từ VolumeItem).</p>

	<p>Nếu giá trị của đối số là <code>off</code>, Kaspersky Endpoint Security không quét dữ liệu về các phân vùng trên thiết bị. Nếu tập tin IOC chứa các thuật ngữ tài liệu IOC VolumeItem, chúng sẽ bị bỏ qua (được phát hiện là không khớp).</p> <p>Nếu đối số không được chỉ định, Kaspersky Endpoint Security chỉ phân tích dữ liệu phân vùng nếu tài liệu IOC VolumeItem được mô tả trong tập tin IOC được cung cấp cho tác vụ quét.</p>
<code>/eventlog=on off</code>	<p>Phân tích dữ liệu về các bản ghi trong nhật ký sự kiện Windows khi thực hiện quét IOC (từ EventLogItem).</p> <p>Nếu giá trị của đối số là <code>off</code>, Kaspersky Endpoint Security không quét các bản ghi trong nhật ký sự kiện Windows. Nếu tập tin IOC chứa các từ tài liệu IOC EventLogItem, chúng sẽ bị bỏ qua (được phát hiện là không khớp).</p> <p>Nếu đối số không được chỉ định, Kaspersky Endpoint Security chỉ phân tích nhật ký sự kiện Windows nếu tài liệu IOC EventLogItem được mô tả trong tập tin IOC được cung cấp cho tác vụ quét.</p>
<code>/datetime=<ngày phát hành sự kiện></code>	<p>Hãy cân nhắc ngày phát hành sự kiện trong nhật ký sự kiện Windows khi xác định phạm vi quét IOC cho tài liệu IOC tương ứng.</p> <p>Khi thực hiện quét IOC, Kaspersky Endpoint Security sẽ quét các mục nhật ký sự kiện Windows được phát hành trong khoảng thời gian từ ngày và giờ được chỉ định đến thời điểm tác vụ được chạy.</p> <p>Kaspersky Endpoint Security cho phép chỉ định ngày phát hành sự kiện làm giá trị của đối số. Tác vụ quét chỉ được thực hiện cho các sự kiện được phát hành trong nhật ký sự kiện Windows sau ngày được chỉ định và trước khi tác vụ quét được chạy.</p> <p>Nếu đối số không được chỉ định, Kaspersky Endpoint Security sẽ quét các sự kiện với bất kỳ ngày phát hành nào. Không thể chỉnh sửa thiết lập TaskSettings::BaseSettings::EventLogItem::datetime.</p> <p>Thiết lập này chỉ được sử dụng nếu tài liệu IOC EventLogItem được mô tả trong tập tin IOC được cung cấp cho quá trình quét.</p>
<code>/channel=<danh sách kênh></code>	<p>Danh sách tên kênh (nhật ký) mà bạn muốn thực hiện quét IOC.</p> <p>Nếu đối số được chỉ định, Kaspersky Endpoint Security sẽ quét các bản ghi được phát hành trong các nhật ký được chỉ định. Tài liệu IOC phải có từ EventLogItem được mô tả.</p> <p>Tên của nhật ký được chỉ định dưới dạng một chuỗi phù hợp với tên của nhật ký (kênh) được chỉ định trong các thuộc tính của nhật ký (tham số Tên đầy đủ) hoặc trong các thuộc tính sự kiện (tham số <Channel> </Channel> trong lược đồ xml của sự kiện). Bạn có thể chỉ định nhiều kênh được phân tách bằng dấu cách.</p> <p>Nếu đối số không được chỉ định, Kaspersky Endpoint Security sẽ quét các bản ghi cho các kênh Application, System, Security.</p>
<code>/files=on off</code>	<p>Phân tích dữ liệu tập tin khi thực hiện quét IOC (từ FileItem).</p> <p>Nếu giá trị của đối số là <code>off</code>, Kaspersky Endpoint Security không phân tích dữ liệu tập tin. Nếu tập tin IOC chứa các từ tài liệu FileItem, chúng sẽ bị bỏ qua (được phát hiện là không khớp).</p> <p>Nếu đối số không được chỉ định, Kaspersky Endpoint Security chỉ phân tích dữ liệu tập tin nếu tài liệu IOC FileItem được mô tả trong tập tin IOC được cung cấp cho tác vụ quét.</p>
<code>/drives=<tất cả hệ thống quan trọng tùy chỉnh></code>	<p>Đặt phạm vi quét IOC khi phân tích dữ liệu cho tài liệu IOC FileItem.</p> <p>Bạn có thể đặt các giá trị sau cho phạm vi quét:</p> <ul style="list-style-type: none"> • <code><a11></code> cho tất cả các phạm vi tập tin khả dụng.

	<ul style="list-style-type: none"> • <system> cho các tập tin trong thư mục nơi hệ điều hành được cài đặt. • <critical> cho các tập tin tạm thời trong thư mục người dùng và hệ thống. • <custom> cho các tập tin trong phạm vi do người dùng xác định (/scope=<danh sách thư mục cần quét>). <p>Nếu đối số không được chỉ định, tác vụ quét sẽ được thực hiện cho các khu vực quan trọng.</p>
/excludes=<danh sách loại trừ>	Đặt phạm vi loại trừ khi phân tích dữ liệu cho tài liệu IOC FileItem. Bạn có thể chỉ định nhiều đường dẫn được phân tách bằng dấu cách.
/scope=<danh sách thư mục cần quét>	Phạm vi quét IOC do người dùng định nghĩa khi phân tích dữ liệu cho tài liệu IOC FileItem (/drives=custom). Bạn có thể chỉ định nhiều đường dẫn được phân tách bằng dấu cách.

Các giá trị trả về của lệnh:

- -1 có nghĩa là lệnh không được hỗ trợ bởi phiên bản của ứng dụng được cài đặt trên máy tính.
- 0 có nghĩa là lệnh đã được thực thi thành công.
- 1 có nghĩa là một đối số bắt buộc không được truyền vào cho lệnh.
- 2 có nghĩa là một lỗi chung đã xảy ra.
- 4 có nghĩa là đã xảy ra lỗi cú pháp.

Nếu lệnh được thực thi thành công (giá trị trả về 0) và các dấu hiệu về sự xâm phạm đã được phát hiện trong quá trình thực hiện, Kaspersky Endpoint Security xuất thông tin kết quả tác vụ sau đây cho dòng lệnh:

Uuid	ID của tập tin IOC trong tiêu đề của cấu trúc tập tin IOC (thẻ <ioc id="">)
Tên	Mô tả tập tin IOC trong tiêu đề của cấu trúc tập tin IOC (thẻ <description></description>)
Matched Indicator Items	Danh sách ID của tất cả các dấu hiệu được đối chiếu.
Matched objects	Dữ liệu cho từng tài liệu IOC có một sự trùng khớp.

MDRLICENSE. Kích hoạt MDR

Thực hiện các thao tác với tập tin cấu hình BLOB để kích hoạt Managed Detection and Response. Tập tin BLOB chứa ID ứng dụng khách và thông tin về giấy phép cho thành phần Managed Detection and Response của Kaspersky. Tập tin BLOB nằm bên trong tập tin nén ZIP của tập tin cấu hình MDR. Bạn có thể lấy tập tin nén ZIP trong Bảng điều khiển Managed Detection and Response của Kaspersky. Để biết thông tin chi tiết về tập tin BLOB, vui lòng tham khảo [Trợ giúp của Managed Detection and Response của Kaspersky](#).

Phải có đặc quyền của quản trị viên để thực hiện các thao tác với tập tin BLOB. Thiết lập Managed Detection and Response trong chính sách cũng phải có sẵn để chỉnh sửa (🔧).

Cú pháp lệnh

```
MDRLICENSE <hoạt động> [/login=<tên người dùng> /password=<mật khẩu>]
```

Hoạt động	
/ADD <tên tập tin>	Áp dụng tập tin cấu hình BLOB để tích hợp với Managed Detection and Response của Kaspersky (định dạng tập tin P7). Bạn chỉ có thể áp dụng một tập tin BLOB. Nếu tập tin BLOB đã được thêm vào máy tính, tập tin đó sẽ được thay thế.
/DEL	Xóa tập tin cấu hình BLOB.

Chứng thực	
/login=<tên người dùng> /password=<mật khẩu>	Thông tin đăng nhập vào tài khoản người dùng với các quyền Bảo vệ bằng mật khẩu cần thiết.

Ví dụ:

- avp.com MDRLICENSE /ADD file.key
- avp.com MDRLICENSE /DEL /login=KLAdmin /password=!Password1

Các mã lỗi

Các lỗi có thể xảy ra khi làm việc với ứng dụng thông qua dòng lệnh. Khi xảy ra các lỗi, Kaspersky Endpoint Security sẽ hiển thị một thông báo lỗi, ví dụ Lỗi: Không thể khởi chạy tác vụ 'EntAppControl'. Kaspersky Endpoint Security cũng có thể hiển thị thông tin bổ sung dưới dạng mã, ví dụ như `lỗi = 8947906D` (xem bảng bên dưới).

Các mã lỗi

Mã lỗi	Mô tả
09479001	Khóa giấy phép cho Kaspersky Endpoint Security đã được sử dụng trên máy tính này.
0947901D	Giấy phép đã hết hạn. Không thể cập nhật cơ sở dữ liệu.
89479002	Không tìm thấy khóa.
89479003	Chữ ký số bị mất hoặc hư hỏng.
89479004	Dữ liệu bị hư hỏng.
89479005	Tập tin khóa bị hư hỏng.
89479006	Giấy phép đã hết hạn hoặc khóa giấy phép đã hết hạn.
89479007	Tập tin khóa không được chỉ định.

89479008	Không thể áp dụng tập tin khóa.
89479009	Lưu dữ liệu thất bại.
8947900A	Đọc dữ liệu thất bại.
8947900B	Lỗi I/O.
8947900C	Không tìm thấy cơ sở dữ liệu.
8947900E	Thư viện cấp giấy phép không được nạp.
8947900F	Cơ sở dữ liệu bị hư hỏng hoặc cập nhật thủ công.
89479010	Cơ sở dữ liệu bị hỏng.
89479011	Không thể sử dụng tập tin khóa không hợp lệ để thêm một khóa dự trữ.
89479012	Lỗi hệ thống.
89479013	Hỏng danh sách các khóa không được phép.
89479014	Chữ ký số của tập tin không khớp với chữ ký số của Kaspersky.
89479015	Không thể sử dụng khóa của giấy phép phi thương mại như khóa của giấy phép thương mại.
89479016	Phải có giấy phép beta để sử dụng phiên bản beta của ứng dụng.
89479017	Tập tin khóa không tương thích với ứng dụng này.
89479018	Khóa bị chặn bởi Kaspersky.
89479019	Ứng dụng đã được sử dụng thông qua một giấy phép dùng thử. Không thể thêm khóa dùng thử một lần nữa.
8947901A	Tập tin khóa bị hư hỏng.
8947901B	Chữ ký điện tử bị mất, hư hỏng hoặc không phù hợp với chữ ký điện tử của Kaspersky.
8947901C	Không thể thêm khóa nếu giấy phép phi thương mại tương ứng đã hết hạn.
8947901E	Ngày tạo hoặc ngày sử dụng tập tin khóa không hợp lệ. Kiểm tra ngày của hệ thống.
8947901F	Không thể thêm khóa của giấy phép dùng thử: một khóa khác của giấy phép dùng thử đã được kích hoạt.
89479020	Hỏng hoặc thiếu danh sách các khóa không được phép.
89479021	Mô tả cập nhật bị mất hoặc hư hỏng.
89479022	Lỗi trong dữ liệu dịch vụ khóa giấy phép.
89479023	Không thể sử dụng tập tin khóa không hợp lệ để thêm một khóa dự trữ.
89479025	Xảy ra lỗi khi gửi yêu cầu đến máy chủ kích hoạt. Có thể do: Lỗi kết nối Internet hoặc sự cố tạm thời trên máy chủ kích hoạt. Hãy thử kích hoạt ứng dụng sau này bằng mã kích hoạt sau. Nếu lỗi này vẫn xảy ra, liên hệ với nhà cung cấp dịch vụ Internet của bạn.
89479026	Lỗi trong phản hồi từ máy chủ kích hoạt.
89479027	Không thể có được trạng thái phản ứng.
89479028	Đã xảy ra lỗi khi lưu tập tin tạm.
89479029	Mã kích hoạt đã được nhập không đúng cách hoặc ngày hệ thống không chính xác. Kiểm tra ngày hệ thống trên máy tính.
8947902A	Tập tin khóa không tương thích với ứng dụng này hoặc giấy phép đã hết hạn. Bạn

	không thể kích hoạt Kaspersky Endpoint Security bằng cách sử dụng tập tin khóa dành cho một ứng dụng khác.
8947902B	Không nhận được tập tin khóa. Đã nhập mã kích hoạt sai.
8947902C	Máy chủ kích hoạt trả về lỗi 400.
8947902D	Máy chủ kích hoạt trả về lỗi 401.
8947902E	Máy chủ kích hoạt trả về lỗi 403.
8947902F	Máy chủ kích hoạt trả về lỗi 404.
89479030	Máy chủ kích hoạt trả về lỗi 405.
89479031	Máy chủ kích hoạt trả về lỗi 406.
89479032	Phải có xác thực trên máy chủ proxy. Hãy kiểm tra các tùy chọn mạng.
89479033	Đã hết hạn thời gian chờ của yêu cầu.
89479034	Máy chủ kích hoạt trả về lỗi 409.
89479035	Máy chủ kích hoạt trả về lỗi 410.
89479036	Máy chủ kích hoạt trả về lỗi 411.
89479037	Máy chủ kích hoạt trả về lỗi 412.
89479038	Máy chủ kích hoạt trả về lỗi 413.
89479039	Máy chủ kích hoạt trả về lỗi 414.
8947903A	Máy chủ kích hoạt trả về lỗi 415.
8947903C	Lỗi máy chủ nội bộ.
8947903D	Chức năng không được hỗ trợ.
8947903E	Phản hồi không hợp lệ từ cổng. Hãy kiểm tra các tùy chọn mạng.
8947903F	Dịch vụ không khả dụng (Lỗi HTTP 503).
89479040	Đã hết hạn thời gian chờ phản hồi từ cổng. Hãy kiểm tra các tùy chọn mạng.
89479041	Giao thức không hỗ trợ bởi máy chủ.
89479043	Lỗi HTTP.
89479044	ID nguồn tài nguyên không hợp lệ.
89479046	URL không hợp lệ.
89479047	Thư mục đích không hợp lệ.
89479048	Lỗi phân bổ bộ nhớ.
89479049	Xảy ra lỗi khi chuyển đổi các tham số thành chuỗi ANSI (URL, thư mục, tác nhân).
8947904A	Xảy ra lỗi khi tạo luồng thực hiện.
8947904B	Luồng làm việc đang chạy.
8947904C	Luồng làm việc không chạy.
8947904D	Không tìm thấy tập tin khóa trên máy chủ kích hoạt.
8947904E	Khóa đã bị chặn.
8947904F	Lỗi nội bộ của máy chủ kích hoạt.

89479050	Không đủ dữ liệu trong yêu cầu kích hoạt.
89479053	Khóa giấy phép đã hết hạn.
89479054	Máy tính được thiết lập ngày hệ thống không chính xác.
89479055	Giấy phép dùng thử đã hết hạn.
89479056	Giấy phép đã hết hạn.
89479057	Đã vượt quá số lần kích hoạt cho ứng dụng của mã được chỉ định.
89479058	Quy trình kích hoạt kết thúc với một lỗi hệ thống.
89479059	Không thể sử dụng khóa của giấy phép phi thương mại như khóa của giấy phép thương mại.
8947905C	Cần có mã kích hoạt.
89479062	Không thể kết nối đến máy chủ kích hoạt.
89479064	Máy chủ kích hoạt không khả dụng. Vui lòng kiểm tra thiết lập kết nối Internet của bạn và thử kích hoạt lại.
89479065	Ngày phát hành cơ sở dữ liệu ứng dụng vượt quá ngày hết hạn giấy phép.
89479066	Không thể thay thế khóa hiện hoạt bằng khóa đã hết hạn.
89479067	Không thể thêm khóa dự trữ nếu khóa hết hạn trước giấy phép hiện tại.
89479068	Cập nhật khóa đăng ký bị mất.
8947906A	Mã kích hoạt không chính xác (tổng kiểm tra không khớp).
8947906B	Khóa đã được kích hoạt.
8947906C	Các loại giấy phép tương ứng với các khóa hiện hoạt và khóa dự trữ không khớp nhau.
8947906D	Thành phần không được hỗ trợ bởi giấy phép.
8947906E	Không thể thêm khóa gói đăng ký làm khóa dự trữ.
89479213	Lỗi chung liên quan đến lớp truyền tải.
89479214	Kết nối đến máy chủ thất bại.
89479215	Định dạng URL không hợp lệ.
89479216	Chuyển đổi địa chỉ máy chủ proxy thất bại.
89479217	Chuyển đổi địa chỉ máy chủ thất bại. Kiểm tra thiết lập kết nối Internet.
89479218	Kết nối đến máy chủ kích hoạt hoặc máy chủ proxy thất bại.
89479219	Truy cập từ xa bị từ chối.
8947921A	Thời gian phản hồi đã hết hạn.
8947921B	Lỗi gửi yêu cầu HTTP.
8947921C	Lỗi kết nối SSL.
8947921D	Hoạt động bị gián đoạn bằng cách gọi lại.
8947921E	Quá nhiều nỗ lực chuyển tiếp.
8947921F	Kiểm tra người nhận thất bại.
89479220	Không có phản hồi từ máy chủ kích hoạt.

89479221	Lỗi gửi dữ liệu.
89479222	Lỗi nhận dữ liệu.
89479223	Lỗi chứng chỉ SSL cục bộ.
89479224	Lỗi mã hóa SSL.
89479225	Lỗi chứng chỉ SSL máy chủ.
89479226	Gói tin mạng chứa nội dung không hợp lệ.
89479227	Truy cập của người dùng bị từ chối.
89479228	Tập tin chứng chỉ SSL không hợp lệ.
89479229	Không thể thiết lập kết nối SSL.
8947922A	Gửi hoặc nhận gói tin mạng thất bại. Vui lòng thử lại sau.
8947922B	Tập tin với chứng chỉ thu hồi không hợp lệ.
8947922C	Lỗi yêu cầu chứng chỉ SSL.
89479401	Lỗi máy chủ không xác định.
89479402	Lỗi máy chủ nội bộ.
89479403	Không có khóa giấy phép khả dụng cho mã kích hoạt được nhập.
89479404	Khóa hiện hoạt bị khóa.
89479405	Thiếu các tham số cần thiết của yêu cầu kích hoạt ứng dụng.
89479406	Tên người dùng hoặc mật khẩu không chính xác.
89479407	Mã kích hoạt không đúng được gửi đến máy chủ.
89479408	Mã kích hoạt không hợp lệ đối với Kaspersky Endpoint Security. Bạn không thể kích hoạt Kaspersky Endpoint Security bằng cách sử dụng tập tin khóa dành cho một ứng dụng không xác định.
89479409	Yêu cầu bị thiếu mã kích hoạt.
8947940B	Giấy phép đã hết hạn (theo dữ liệu từ máy chủ kích hoạt).
8947940C	Đã vượt quá số lần kích hoạt cho mã kích hoạt này.
8947940D	ID yêu cầu có định dạng không hợp lệ.
8947940E	Mã kích hoạt không hợp lệ đối với Kaspersky Endpoint Security. Mã kích hoạt được dành cho một ứng dụng Kaspersky khác.
8947940F	Không thể cập nhật khóa giấy phép.
89479410	Mã kích hoạt không hợp lệ đối với khu vực này.
89479411	Mã kích hoạt không hợp lệ cho phiên bản ngôn ngữ Kaspersky Endpoint Security.
89479412	Cần có quyền truy cập bổ sung đến máy chủ kích hoạt.
89479413	Máy chủ kích hoạt trả về lỗi 643.
89479414	Máy chủ kích hoạt trả về lỗi 644.
89479415	Máy chủ kích hoạt trả về lỗi 645.
89479416	Máy chủ kích hoạt trả về lỗi 646.
89479417	Định dạng mã kích hoạt không được hỗ trợ bởi máy chủ kích hoạt.

89479418	Mã kích hoạt có định dạng không hợp lệ.
89479419	Máy tính được cài đặt sai thời gian hệ thống.
8947941A	Mã kích hoạt không hợp lệ cho phiên bản Kaspersky Endpoint Security.
8947941B	Gói đăng ký đã hết hạn.
8947941C	Vượt quá lượt kích hoạt của giấy phép này.
8947941D	Khóa giấy phép có chữ ký số không hợp lệ.
8947941E	Cần thêm dữ liệu bổ sung.
8947941F	Xác minh dữ liệu người dùng thất bại.
89479420	Gói đăng ký không hoạt động.
89479421	Máy chủ kích hoạt đang bảo trì.
89479501	Lỗi không xác định của Kaspersky Endpoint Security.
89479502	Tham số được chuyển không hợp lệ (ví dụ, danh sách địa chỉ máy chủ kích hoạt trống).
89479503	Mã kích hoạt không chính xác.
89479504	Tên người dùng không hợp lệ.
89479505	Mật khẩu người dùng không hợp lệ.
89479506	Phản hồi từ máy chủ kích hoạt không hợp lệ.
89479507	Yêu cầu kích hoạt bị gián đoạn.
89479509	Máy chủ kích hoạt trả về danh sách chuyển tiếp trống.

Phụ lục. Hồ sơ ứng dụng

Hồ sơ là một thành phần, tác vụ hoặc tính năng của Kaspersky Endpoint Security. Các hồ sơ được sử dụng để quản lý ứng dụng từ dòng lệnh. Bạn có thể sử dụng các hồ sơ để thực thi lệnh `START`, `STOP`, `STATUS`, `STATISTICS`, `EXPORT`, và `IMPORT`. Bạn có thể cấu hình thiết lập ứng dụng (ví dụ, `STOP DeviceControl`) hoặc chạy các tác vụ (ví dụ, `START Scan_My_Computer`) sử dụng hồ sơ.

Các hồ sơ sau đây có thể được sử dụng:

- `AdaptiveAnomaliesControl` – Kiểm soát thích ứng sự cố.
- `AMSI` – Bảo vệ AMSI.
- `BehaviorDetection` – Phát hiện hành vi.
- `DeviceControl` – Kiểm soát thiết bị.
- `EntAppControl` – Kiểm soát ứng dụng.
- `File_Monitoring` hoặc `FM` – Bảo vệ mối đe dọa tập tin.
- `Firewall` hoặc `FW` – Tường lửa.
- `HIPS` – Phòng chống xâm nhập máy chủ.

- IDS – Bảo vệ mối đe dọa mạng.
- IntegrityCheck – Kiểm tra tính toàn vẹn.
- Mail_Monitoring hoặc EM – Bảo vệ mối đe dọa thư điện tử.
- Rollback – hoàn tác bản cập nhật.
- Scan_ContextScan – Quét từ menu ngữ cảnh.
- Scan_IdleScan – Quét trong nền.
- Scan_Memory – Quét bộ nhớ kernel.
- Scan_My_Computer – Quét toàn bộ.
- Scan_Objects – Quét tùy chỉnh.
- Scan_Qscan – Quét các đối tượng được nạp khi khởi động hệ điều hành.
- Scan_Removable_Drive – Quét ổ đĩa di động.
- Scan_Startup hoặc STARTUP – Quét khu vực quan trọng.
- Updater – Cập nhật.
- Web_Monitoring hoặc WM – Bảo vệ mối đe dọa web.
- WebControl – Kiểm soát Web.

Kaspersky Endpoint Security cũng hỗ trợ các hồ sơ bảo dưỡng. Hồ sơ bảo dưỡng có thể là cần thiết khi bạn liên hệ với Hỗ trợ kỹ thuật của Kaspersky.

Quản lý ứng dụng thông qua REST API

Kaspersky Endpoint Security cho phép bạn cấu hình thiết lập của ứng dụng, chạy tác vụ quét, cập nhật cơ sở dữ liệu diệt virus và thực hiện các tác vụ khác bằng các giải pháp của bên thứ ba. Kaspersky Endpoint Security cung cấp một API cho mục đích này. REST API của Kaspersky Endpoint Security hoạt động trên HTTP và có một bộ các phương thức yêu cầu/phản hồi. Nói cách khác, bạn có thể quản lý Kaspersky Endpoint Security thông qua giải pháp của bên thứ ba chứ không phải giao diện ứng dụng cục bộ hay Bảng điều khiển quản trị Kaspersky Security Center.

Để bắt đầu sử dụng REST API, bạn cần [cài đặt Kaspersky Endpoint Security hỗ trợ REST API](#). Ứng dụng khách REST và Kaspersky Endpoint Security phải được cài đặt trên cùng một máy tính.

Để đảm bảo tương tác an toàn giữa Kaspersky Endpoint Security và trình khách REST:

- Cấu hình tính năng bảo vệ ứng dụng khách REST để không truy cập trái phép theo khuyến nghị của nhà phát triển trình khách REST. Cấu hình tính năng bảo vệ thư mục ứng dụng khách REST để không cho ghi với sự trợ giúp của Danh sách kiểm soát truy cập theo ý muốn - DACL.
- Để chạy ứng dụng khách REST, hãy sử dụng tài khoản riêng có các quyền quản trị viên. Từ chối đăng nhập tương tác vào hệ thống cho tài khoản này.

Ứng dụng được quản lý thông qua REST API tại <http://127.0.0.1> hoặc <http://localhost>. Không thể quản lý Kaspersky Endpoint Security từ xa thông qua REST API.



[MỞ TÀI LIỆU REST API](#)

Cài đặt ứng dụng với REST API

Để quản lý ứng dụng thông qua REST API, bạn cần cài đặt Kaspersky Endpoint Security hỗ trợ REST API. Nếu bạn quản lý Kaspersky Endpoint Security thông qua REST API, bạn không thể quản lý ứng dụng bằng Kaspersky Security Center.

Chuẩn bị cài đặt ứng dụng có hỗ trợ REST API

Tương tác bảo mật của Kaspersky Endpoint Security với máy khách REST yêu cầu định cấu hình nhận dạng yêu cầu. Để thực hiện, bạn phải cài đặt chứng chỉ và sau đó ký vào tải trọng của mỗi yêu cầu.

Để tạo chứng chỉ, bạn có thể sử dụng ví dụ: OpenSSL.

Ví dụ:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

Sử dụng thuật toán mã hóa RSA với độ dài khóa từ 2048 bit trở lên.

Kết quả là bạn sẽ nhận được một chứng chỉ `cert.pem` và một khóa riêng `key.pem`.

Cài đặt ứng dụng có hỗ trợ REST API

Để cài đặt Kaspersky Endpoint Security hỗ trợ REST API:

1. Chạy trình thông dịch dòng lệnh (cmd.exe) với tư cách quản trị viên.
2. Vào thư mục chứa gói phân phối cho Kaspersky Endpoint Security version 11.2.0 trở lên.
3. Cài đặt Kaspersky Endpoint Security với các thiết lập sau:

- RESTAPI=1

- RESTAPI_User=<Tên người dùng>

Tên người dùng để quản lý ứng dụng thông qua REST API. Nhập tên người dùng theo định dạng <DOMAIN>\<Tên người dùng> (ví dụ: RESTAPI_User=COMPANY\Administrator). Bạn chỉ có thể quản lý ứng dụng thông qua REST API trong tài khoản này. Bạn chỉ có thể chọn một người dùng để làm việc với REST API.

- RESTAPI_Port=<Cổng>

Cổng được sử dụng để trao đổi dữ liệu. Tham số tùy chọn. Cổng 6782 được chọn theo mặc định.

- RESTAPI_Certificate=<Đường dẫn đến chứng chỉ>

Chứng chỉ để xác định các yêu cầu (ví dụ: RESTAPI_Certificate=C:\cert.pem).

Bạn có thể cài đặt chứng chỉ sau khi cài đặt ứng dụng hoặc cập nhật chứng chỉ sau khi chứng chỉ hết hạn.

Cách cài đặt chứng chỉ để nhận dạng yêu cầu API REST

1. Tắt [Tự bảo vệ cho Kaspersky Endpoint Security](#)

Cơ chế Tự bảo vệ ngăn chặn việc sửa đổi hoặc xóa các tập tin ứng dụng trên ổ đĩa cứng, tiến trình trong bộ nhớ và các mục trong registry hệ thống.

2. Truy cập khóa registry chứa thiết lập REST API:

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\Rest

3. Nhập đường dẫn đến chứng chỉ, ví dụ: Certificate = C:\Folder\cert.pem.

4. Bật [Tự bảo vệ cho Kaspersky Endpoint Security](#).

5. [Khởi động lại ứng dụng](#).

- AdminKitConnector=1

Quản lý ứng dụng bằng các hệ thống quản trị. Khả năng quản lý được cho phép theo mặc định.

Bạn cũng có thể sử dụng [tập tin setup.ini](#) để xác định thiết lập để làm việc với REST API.

Ví dụ:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1  
/pAdminKitConnector=1 /pRESTAPI=1 /pRESTAPI_User=COMPANY\Administrator  
/pRESTAPI_Certificate=C:\cert.pem /s
```

Do đó, bạn có thể quản lý ứng dụng thông qua REST API. Để kiểm tra hoạt động của ứng dụng, hãy mở tài liệu REST API bằng yêu cầu GET.

Ví dụ:

```
GET http://localhost:6782/kes/v1/api-docs
```

Nếu bạn đã cài đặt ứng dụng có hỗ trợ REST API thì Kaspersky Endpoint Security sẽ tự động tạo quy tắc cho phép trong thiết lập Kiểm soát Web để truy cập tài nguyên web (*Quy tắc dịch vụ cho REST API*). Đây là quy tắc cần thiết để cho phép trình khách REST truy cập Kaspersky Endpoint Security mọi lúc. Ví dụ: nếu bạn đã hạn chế quyền truy cập của người dùng vào tài nguyên web thì điều này sẽ không ảnh hưởng đến việc quản lý ứng dụng thông qua REST API. Chúng tôi khuyến nghị bạn không xóa quy tắc hoặc thay đổi thiết lập *Quy tắc dịch vụ cho REST API*. Nếu bạn xóa quy tắc này thì Kaspersky Endpoint Security sẽ khôi phục lại quy tắc sau khi khởi động lại ứng dụng.

Làm việc với API

Không thể hạn chế quyền truy cập vào ứng dụng thông qua REST API bằng tính năng [Bảo vệ bằng mật khẩu](#). Ví dụ: không thể chặn người dùng tắt bảo vệ thông qua REST API. Bạn có thể cấu hình Bảo vệ bằng mật khẩu thông qua REST API và hạn chế quyền truy cập của người dùng vào ứng dụng thông qua giao diện cục bộ.

Để quản lý ứng dụng thông qua REST API, bạn cần chạy ứng dụng khách REST qua tài khoản mà bạn đã chỉ định khi [cài đặt ứng dụng hỗ trợ REST API](#). Bạn chỉ có thể chọn một người dùng để làm việc với REST API.



[MỞ TÀI LIỆU REST API](#)

Quản lý ứng dụng thông qua REST API bao gồm các bước sau:

1. Lấy các giá trị hiện tại của thiết lập ứng dụng. Để thực hiện, hãy gửi một yêu cầu GET.

Ví dụ:

```
GET http://localhost:6782/kes/v1/settings/ExploitPrevention
```

2. Ứng dụng sẽ gửi phản hồi kèm cấu trúc và giá trị của thiết lập. Kaspersky Endpoint Security hỗ trợ các định dạng XML và JSON.

Ví dụ:

```
{
  "action": 0,
  "enableSystemProcessesMemoryProtection": true,
  "enabled": true
}
```

3. Chỉnh sửa thiết lập chính sách. Sử dụng cấu trúc thiết lập nhận được để phản hồi yêu cầu GET.

Ví dụ:

```
{
  "action": 0,
  "enableSystemProcessesMemoryProtection": false,
  "enabled": true
}
```

4. Lưu thiết lập ứng dụng (tải trọng) trong một tập tin JSON (payload.json).
5. Ký tập tin JSON ở định dạng PKCS7.

Ví dụ:

```
$ openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -binary -outform pem -out signed_payload.pem
```

Kết quả là bạn nhận được một tập tin đã ký chứa tải trọng của yêu cầu (`signed_payload.pem`).

6. Chỉnh sửa thiết lập chính sách. Để thực hiện, hãy gửi yêu cầu POST và đính kèm tập tin đã ký chứa tải trọng yêu cầu (`signed_payload.pem`).

Ứng dụng sẽ áp dụng thiết lập mới và gửi phản hồi có chứa kết quả cấu hình ứng dụng (phản hồi có thể trống). Bạn có thể xác minh rằng thiết lập được cập nhật bằng cách sử dụng yêu cầu GET.

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 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 Kiến thức cơ bản

Kiến thức cơ bản là một phần trên website Hỗ trợ kỹ thuật.

Trên [trang Kaspersky Endpoint Security trong Kiến thức cơ bản](#), 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 Kiến thức cơ bản cũng có thể chứa tin tức từ nhóm Hỗ trợ Kỹ thuật.

Thảo luận về ứng dụng Kaspersky trong cộng đồng người dùng

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 trong [Cộng đồng](#) của chúng tôi.

Trong Cộng đồng này, bạn có thể xem các chủ đề hiện tại, đăng ý kiến của chính bạn và tạo chủ đề thảo luận mới.

Liên hệ với Hỗ trợ kỹ thuật

Nếu bạn không tìm thấy giải pháp cho vấn đề của mình trong tài liệu hoặc trong các [nguồn thông tin về Kaspersky Endpoint Security](#) khác, chúng tôi khuyên bạn nên liên hệ với bộ phận Hỗ trợ kỹ thuật. Bộ phận Hỗ trợ kỹ thuật sẽ giải đáp các thắc mắc của bạn về việc cài đặt và sử dụng Kaspersky Endpoint Security.

Kaspersky sẽ hỗ trợ cho Kaspersky Endpoint Security trong thời gian vòng đời của ứng dụng (tham khảo [trang vòng đời của ứng dụng](#)). 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 [truy cập website Hỗ trợ kỹ thuật](#)
- Gửi yêu cầu đến bộ phận Hỗ trợ kỹ thuật Kaspersky qua [cổng thông tin Kaspersky CompanyAccount](#)

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*. Các tập tin theo dõi cho phép bạn theo dõi quá trình thực hiện lệnh của ứng dụng từng bước và tìm hiểu trên đó giai đoạn hoạt động của ứng dụng một lỗi đã xảy ra.

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.

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 các chức năng nhận thông tin chẩn đoán mở rộng.
- Đặt thiết lập từng thành phần của ứng dụng bằng cách thay đổi các thiết lập đặc biệt không thể truy cập qua giao diện người dùng chuẩn.
- Thay đổi thiết lập lưu trữ thông tin chẩn đoán.
- Cấu hình 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 sử dụng vì mục đích gỡ lỗi. Thông tin chẩn đoán mở rộng sẽ được lưu trên máy tính của người dùng. Dữ liệu không tự động được truyền tải đến Kaspersky.

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. Việc tự ý thay đổi thiết lập ứng dụng theo những cách không được mô tả trong Trợ giúp Trực tuyến hoặc trong các khuyến nghị của bộ phận Hỗ trợ kỹ thuật có thể làm chậm và treo hệ điều hành, giảm mức độ bảo vệ của máy tính và làm tổn hại đến tính khả dụng và tính toàn vẹn của thông tin đang được xử lý.

Nội dung và bộ nhớ của tập tin truy vết

Bạn là cá nhân phải chịu trách nhiệm đảm bảo tính bảo mật của dữ liệu được lưu trữ trên máy tính của mình, đặc biệt là để giám sát và hạn chế truy cập dữ liệu cho đến khi nó được gửi đến Kaspersky.

Các tập tin dấu vết được lưu trữ trên máy tính của bạn 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, trừ tập tin dấu vết của Authentication Agent, được lưu trữ trong thư mục %ProgramData%\Kaspersky Lab\KES\Traces.

Các tập tin dấu vết được đặt tên như sau: KES<số phiên bản dịch vụ_ngàyXX.XX_giờXX.XX_pidXXX.><loại tập tin dấu vết>.log.

Bạn có thể xem dữ liệu được lưu trong các tập tin dấu vết.

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.

Kaspersky Endpoint Security chỉ lưu mật khẩu người dùng vào một tập tin dấu vết dưới dạng mã hóa.

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.
- Dữ liệu trên phần cứng được cài đặt trên máy tính (như dữ liệu vi chương trình BIOS/UEFI). Dữ liệu này được ghi vào các tập tin dấu vết khi thực hiện Kaspersky Disk Encryption.
- 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.
- 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.
- Dữ liệu lưu lượng mạng. Dữ liệu này được ghi vào các tập tin dấu vết nếu các thành phần giám sát lưu lượng được bật (ví dụ như Kiểm soát Web).
- Dữ liệu nhận được từ các máy chủ của Kaspersky (như phiên bản của cơ sở dữ liệu diệt virus).
- Trạng thái của các thành phần Kaspersky Endpoint Security và dữ liệu vận hành của chúng.
- Dữ liệu về hoạt động của người dùng trong ứng dụng.
- Các sự kiện của hệ điều hành.

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 còn 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 còn 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 còn 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 còn 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 còn 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 hiệu năng

Các tập tin dấu vết hiệu năng được đặt tên như sau: KES<số phiên bản_ngàyXX.XX_giờXX.XX_pidXXX.>PERF.HAND.etl.

Ngoài dữ liệu chung, các tập tin dấu vết hiệu năng còn chứa thông tin về mức tải lên bộ vi xử lý, thông tin về thời gian tải của hệ điều hành và các ứng dụng, và thông tin về các tiến trình đang chạy.

Nội dung của tập tin dấu vết của thành phần Bảo vệ AMSI

Ngoài dữ liệu chung, tập tin dấu vết AMSI.log chứa thông tin về kết quả của tác vụ quét được thực hiện theo yêu cầu từ các ứng dụng thuộc bên thứ ba.

Nội dung của tập tin dấu vết của thành phần Bảo vệ mỗi đe dọa thư điện tử

Tập tin dấu vết mcou.OUTLOOK.EXE.log có thể chứa các phần của email, bao gồm địa chỉ email, ngoài dữ liệu chung.

Nội dung của tập tin dấu vết của thành phần Quét từ Menu ngữ cảnh

Tập tin dấu vết shelllex.dll.log chứa thông tin về việc hoàn thành tác vụ quét và dữ liệu cần thiết để gỡ lỗi cho ứng dụng, ngoài thông tin chung.

Nội dung của các tập tin dấu vết của tiện ích web ứng dụng

Các tập tin dấu vết của tiện ích web ứng dụng được lưu trữ trên máy tính có cài đặt Bảng điều khiển web Kaspersky Security Center, trong thư mục Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs.

Các tập tin dấu vết của tiện ích web ứng dụng được đặt tên như sau: logs-kes_windows-<loại tập tin dấu vết>.DESKTOP-<ngày cập nhật tập tin>.log. Bảng điều khiển web bắt đầu ghi dữ liệu sau khi cài đặt và xóa các tập tin dấu vết sau khi Bảng điều khiển web bị gỡ bỏ.

Các tập tin dấu vết của tiện ích web ứng dụng chứa những thông tin sau, ngoài dữ liệu chung:

- Mật khẩu người dùng KLAdmin để mở khóa giao diện Kaspersky Endpoint Security ([Bảo vệ bằng mật khẩu](#)).
- Mật khẩu tạm thời để mở khóa giao diện Kaspersky Endpoint Security ([Bảo vệ bằng mật khẩu](#)).
- Tên người dùng và mật khẩu cho máy chủ email SMTP ([Thông báo qua email](#)).
- Tên người dùng và mật khẩu cho máy chủ proxy Internet ([Máy chủ proxy](#)).
- Tên người dùng và mật khẩu cho [tác vụ Thay đổi thành phần ứng dụng](#).
- Chứng chỉ tài khoản và các đường dẫn được quy định trong các tác vụ và thuộc tính chính sách của Kaspersky Endpoint Security.

Nội dung của tập tin dấu vết cho Authentication Agent

Tập tin dấu vết của Authentication Agent được lưu trữ trong thư mục System Volume Information và được đặt tên như sau: KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin.


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.

Truy vết hoạt động của ứng dụng

Truy vết ứng dụng là một bản ghi chi tiết về các hành động được thực thi bởi ứng dụng và thông báo về các sự kiện xảy ra trong quá trình hoạt động của ứng dụng.

Nên thực hiện truy vết ứng dụng dưới sự giám sát của bộ phận Hỗ trợ kỹ thuật Kaspersky.

Để tạo một tập tin dấu vết ứng dụng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ mở ra, hãy nhấn nút **Công cụ hỗ trợ**.
3. Sử dụng nút bật/tắt **Bật truy vết ứng dụng** để bật hoặc tắt truy vết hoạt động của ứng dụng.
4. Trong danh sách thả xuống **Truy vết**, hãy chọn một chế độ truy vết ứng dụng:
 - **Có luân phiên**. Lưu dấu vết vào một số tập tin giới hạn với kích cỡ giới hạn và ghi đè lên các tập tin cũ khi kích cỡ tối đa bị vượt quá. Nếu chế độ này được chọn, bạn có thể xác định số lượng tập tin tối đa để luân phiên và dung lượng tối đa cho mỗi tập tin.
 - **Ghi vào một tập tin**. Lưu một tập tin dấu vết (không có giới hạn kích cỡ).
5. Trong danh sách thả xuống **Mức độ**, hãy chọn cấp độ truy vết:

Bạn nên xác định rõ mức độ truy vết cần thiết với chuyên gia Hỗ trợ kỹ thuật. Nếu không có hướng dẫn từ Hỗ trợ kỹ thuật, hãy đặt mức độ truy vết là **Bình thường (500)**.
6. Khởi động lại Kaspersky Endpoint Security.
7. Để dừng truy vết tiến trình, hãy quay lại cửa sổ **Công cụ hỗ trợ** và tắt truy vết.

Bạn cũng có thể sử dụng tập tin dấu vết khi cài đặt ứng dụng từ [dòng lệnh](#), bao gồm bằng cách sử dụng [tập tin setup.ini](#).

Kết quả là tập tin dấu vết hiệu năng sẽ được tạo trong thư mục %ProgramData%\Kaspersky Lab\KES\Traces. Sau khi tập tin dấu vết được tạo, hãy gửi tập tin đó đến bộ phận Hỗ trợ kỹ thuật của Kaspersky.


Kaspersky Endpoint Security sẽ tự động xóa các tập tin dấu vết khi ứng dụng được gỡ bỏ. Bạn cũng có thể xóa các tập tin này theo cách thủ công. Để thực hiện, bạn phải tắt truy vết và [dừng ứng dụng](#).

Truy vết hiệu năng của ứng dụng

Kaspersky Endpoint Security cho phép bạn nhận thông tin về các sự cố vận hành máy tính trong quá trình sử dụng ứng dụng. Ví dụ như bạn có thể nhận thông tin về các khoảng trễ trong quá trình tải hệ điều hành sau khi ứng dụng được cài đặt. Để thực hiện điều đó, Kaspersky Endpoint Security sẽ tạo [các tập tin dấu vết hiệu năng](#). *Truy vết hiệu năng* chỉ việc lưu ký các hành động được thực hiện bởi ứng dụng dành cho mục đích chẩn đoán các sự cố hiệu năng của Kaspersky Endpoint Security. Để nhận thông tin, Kaspersky Endpoint Security sẽ sử dụng dịch vụ Truy vết sự kiện cho Windows (ETW). Bộ phận Hỗ trợ kỹ thuật của Kaspersky chịu trách nhiệm chẩn đoán các sự cố của Kaspersky Endpoint Security và xác lập lý do cho các sự cố đó.

Nên thực hiện truy vết ứng dụng dưới sự giám sát của bộ phận Hỗ trợ kỹ thuật Kaspersky.

Để tạo một tập tin dấu vết hiệu năng:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ mở ra, hãy nhấn nút **Công cụ hỗ trợ**.
3. Sử dụng nút bật/tắt **Bật truy vết hiệu năng** để bật hoặc tắt truy vết hiệu năng ứng dụng.
4. Trong danh sách thả xuống **Truy vết**, hãy chọn một chế độ truy vết ứng dụng:
 - **Có luân phiên**. Lưu dấu vết vào một số tập tin giới hạn với kích cỡ giới hạn và ghi đè lên các tập tin cũ khi kích cỡ tối đa bị vượt quá. Nếu chế độ này được chọn, bạn có thể xác định dung lượng tối đa cho mỗi tập tin.
 - **Ghi vào một tập tin**. Lưu một tập tin dấu vết (không có giới hạn kích cỡ).
5. Trong danh sách thả xuống **Mức độ**, hãy chọn cấp độ truy vết:
 - **Nhanh**. Kaspersky Endpoint Security sẽ phân tích các tiến trình quan trọng nhất của hệ điều hành liên quan đến hiệu năng.
 - **Chi tiết**. Kaspersky Endpoint Security sẽ phân tích tất cả các tiến trình của hệ điều hành liên quan đến hiệu năng.
6. Trong danh sách thả xuống **Loại truy vết**, hãy chọn loại truy vết:
 - **Thông tin cơ bản**. Kaspersky Endpoint Security sẽ phân tích các tiến trình khi hệ điều hành đang chạy. Sử dụng loại truy vết này nếu một vấn đề vẫn tiếp tục xuất hiện sau khi hệ điều hành được nạp, ví dụ như vấn đề liên quan đến truy cập Internet trong trình duyệt.
 - **Khi khởi động lại**. Kaspersky Endpoint Security sẽ chỉ phân tích các tiến trình khi hệ điều hành đang nạp. Sau khi hệ điều hành được nạp, Kaspersky Endpoint Security sẽ dừng truy vết. Sử dụng loại truy vết này nếu vấn đề liên quan đến quá trình tải hệ điều hành bị chậm trễ.
7. Khởi động lại máy tính và thử tạo lại vấn đề.
8. Để dừng truy vết tiến trình, hãy quay lại cửa sổ **Công cụ hỗ trợ** và tắt truy vết.

Kết quả là tập tin dấu vết hiệu năng sẽ được tạo trong thư mục %ProgramData%\Kaspersky Lab\KES\Traces. Sau khi tập tin dấu vết được tạo, hãy gửi tập tin đó đến bộ phận Hỗ trợ kỹ thuật của Kaspersky.


Ghi kết xuất

Một tập tin kết xuất chứa tất cả thông tin về bộ nhớ làm việc của các tiến trình Kaspersky Endpoint Security tại thời điểm khi tập tin kết xuất được tạo.

Các tập tin kết xuất được lưu có thể chứa dữ liệu bí mật. Để kiểm soát truy cập dữ liệu, bạn phải tự mình đảm bảo sự bảo mật của các tập tin kết xuất.

Các tập tin kết xuất được lưu trữ trên máy tính của bạn chừng nào ứng dụng còn đang được sử dụng, và sẽ bị xóa vĩnh viễn khi ứng dụng bị gỡ bỏ. Các tập tin kết xuất được lưu trữ trong thư mục %ProgramData%\Kaspersky Lab\KES\Traces.

Để bật và tắt ghi tập tin kết xuất:

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Thiết lập ứng dụng**.
3. Trong mục **Thông tin gỡ lỗi**, sử dụng hộp kiểm **Cho phép ghi tập tin dump** để bật hoặc tắt ghi tập tin kết xuất của ứng dụng.
4. Lưu các thay đổi của bạn.


Bảo vệ 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, và cũng có thể chứa [dữ liệu 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. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát** → **Thiết lập ứng dụng**.
3. Trong mục **Thông tin gỡ lỗi**, hãy sử dụng hộp kiểm **Bật bảo vệ các tập tin kết xuất và dấu vết** để bật hoặc tắt bảo vệ tập tin.
4. Lưu các thay đổi của bạn.

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.

Hạn chế và cảnh báo

Kaspersky Endpoint Security có một số hạn chế nhưng không nghiêm trọng đối với hoạt động của ứng dụng.

[Cài đặt ứng dụng](#) 

- Để biết thêm chi tiết về việc hỗ trợ cho hệ điều hành Microsoft Windows 10, Microsoft Windows Server 2016 và Microsoft Windows Server 2019, vui lòng tham khảo [Cơ sở tri thức Hỗ trợ kỹ thuật](#).
- Để biết thêm chi tiết về việc hỗ trợ cho hệ điều hành Microsoft Windows Server 11 và Microsoft Windows 2022, vui lòng tham khảo [Kiến thức cơ bản của Hỗ trợ kỹ thuật](#).
- Sau khi được cài đặt vào một máy tính bị nhiễm, ứng dụng không thông báo cho người dùng về việc cần phải chạy tác vụ quét máy tính. Bạn có thể gặp sự cố khi [kích hoạt ứng dụng](#). Để giải quyết những vấn đề này, [hãy khởi chạy tác vụ Quét khu vực quan trọng](#).
- Nếu các ký tự không phải ASCII (ví dụ: chữ cái tiếng Nga) được sử dụng trong tập tin setup.ini và setup.reg, bạn nên chỉnh sửa tập tin bằng notepad.exe và lưu tập tin ở dạng mã hóa UTF-16LE. Các bảng mã khác không được hỗ trợ.
- Ứng dụng không hỗ trợ sử dụng các ký tự không phải ASCII khi chỉ định đường dẫn cài đặt ứng dụng trong [thiết lập gói cài đặt](#).
- Khi [thiết lập ứng dụng được nhập từ tập tin CFG](#), giá trị của thiết lập xác định việc tham gia vào Kaspersky Security Network sẽ không được áp dụng. Sau khi nhập các thiết lập, vui lòng đọc văn bản Tuyên bố Kaspersky Security Network và xác nhận sự đồng ý của bạn để tham gia vào Kaspersky Security Network. Bạn có thể đọc nội dung của Tuyên bố trong giao diện ứng dụng hoặc trong tập tin ksn_*.txt trong thư mục chứa gói phân phối ứng dụng.
- Nếu muốn gỡ bỏ và sau đó cài đặt lại mã hóa (FLE hoặc FDE) hoặc thành phần Kiểm soát thiết bị, bạn phải khởi động lại hệ thống trước khi cài đặt lại.
- Khi sử dụng hệ điều hành Microsoft Windows 10, bạn phải khởi động lại hệ thống sau khi gỡ bỏ thành phần Mã hóa mức độ tập tin (FLE).
- Khi cố gắng cài đặt bất kỳ phiên bản nào của Mô-đun mã hóa AES trên máy tính có Kaspersky Endpoint Security cho Windows 11.9.0 nhưng không có thành phần mã hóa nào được cài đặt, quá trình cài đặt Mô-đun mã hóa sẽ kết thúc với một thông báo lỗi để thông báo rằng phiên bản mới hơn của ứng dụng đã được cài đặt. Kể từ Kaspersky Endpoint Security 10 Service Pack 2 cho Windows (phiên bản 10.3.0.6294), không còn tập tin cài đặt riêng cho Mô-đun mã hóa. Các thư viện mã hóa được kèm theo trong gói phân phối ứng dụng. Kaspersky Endpoint Security 11.9.0 không tương thích với các mô-đun mã hóa AES. Các thư viện cần thiết để mã hóa được cài đặt tự động khi thành phần Mã hóa toàn bộ ổ đĩa (FDE) hoặc Mã hóa mức độ tập tin (FLE) được chọn.
- Quá trình cài đặt ứng dụng có thể kết thúc kèm theo lỗi cho biết *Máy tính của bạn được cài đặt một ứng dụng bị thiếu tên hoặc tên không đọc được*. Điều này có nghĩa là các ứng dụng không tương thích hoặc các phần của chúng vẫn còn trên máy tính của bạn. Để xóa các phần đối tượng còn lại của các ứng dụng không tương thích, hãy gửi yêu cầu kèm theo mô tả chi tiết về tình huống tới bộ phận Hỗ trợ kỹ thuật của Kaspersky thông qua [Kaspersky CompanyAccount](#).
- Nếu bạn đã hủy gỡ bỏ ứng dụng, hãy tiến hành khôi phục ứng dụng sau khi máy tính khởi động lại.
- Trên máy tính chạy Windows 10 phiên bản 1903 và 1909, các bản nâng cấp từ Kaspersky Endpoint Security 10 cho Windows Service Pack 2 Maintenance Release 3 (bản dựng 10.3.3.275), Service Pack 2 Maintenance Release 4 (bản dựng 10.3.3.304), 11.0.0 và 11.0.1 có thành phần Mã hóa mức độ tập tin (FLE) được cài đặt có thể kết thúc kèm theo lỗi. Lý do là bởi vì mã hóa tập tin không được hỗ trợ cho các phiên bản này của Kaspersky Endpoint Security cho Windows trong Windows 10 phiên bản 1903 và 1909. Trước khi cài đặt bản nâng cấp này, bạn nên [gỡ bỏ thành phần mã hóa tập tin](#).

- Ứng dụng yêu cầu Microsoft .NET Framework 4.0 trở lên. Microsoft .NET Framework 4.6.1 có các lỗ hổng bảo mật. Nếu bạn đang sử dụng Microsoft .NET Framework 4.6.1, bạn phải cài đặt các bản cập nhật bảo mật. Để biết chi tiết về các bản cập nhật bảo mật của Microsoft .NET Framework, hãy tham khảo [Trang web Hỗ trợ kỹ thuật của Microsoft](#).
- Nếu ứng dụng không được cài đặt thành công với thành phần Kaspersky Endpoint Agent được chọn trong hệ điều hành máy chủ và cửa sổ *Lỗi bộ điều phối Windows Installer* xuất hiện, hãy tham khảo hướng dẫn trên website hỗ trợ của Microsoft.
- Nếu ứng dụng được cài đặt cục bộ ở chế độ không tương tác, hãy sử dụng [tập tin setup.ini](#) được cung cấp để thay thế các thành phần đã cài đặt.
- Sau khi Kaspersky Endpoint Security cho Windows được cài đặt trong một số cấu hình của Windows 7, Windows Defender sẽ tiếp tục hoạt động. Bạn nên tắt Windows Defender theo cách thủ công để ngăn giảm hiệu năng hệ thống.
- Để cài đặt ứng dụng này trên máy tính chạy Windows 7 hoặc Windows Server 2008 R2 được triển khai phần mềm Veeam Backup & Replication, bạn có thể cần phải khởi động lại máy tính và chạy lại quá trình cài đặt.

Nâng cấp ứng dụng

- Khi nâng cấp từ Kaspersky Endpoint Security 10 Service Pack 2 cho Windows (bản dựng 10.3.0.6294), [thành phần Phòng chống xâm nhập máy chủ sẽ được bật](#).
- Khi cập nhật Kaspersky Endpoint Security 10 Service Pack 2 cho Windows (bản dựng 10.3.0.6294), các tập tin đã được đặt trong Sao lưu hoặc Khu vực cách ly ở phiên bản cũ của ứng dụng sẽ được chuyển sang Sao lưu trong phiên bản mới của ứng dụng. Các tập tin này không được chuyển cho các phiên bản trước Kaspersky Endpoint Security 10 Service Pack 2 cho Windows (bản dựng 10.3.0.6294). Để lưu chúng, bạn phải khôi phục các tập tin từ Khu vực cách ly và Sao lưu trước khi nâng cấp ứng dụng. Sau khi nâng cấp xong, hãy quét lại các tập tin đã khôi phục.
- Kể từ phiên bản 11.0.0 của ứng dụng, bạn có thể cài đặt tiện ích MMC cho Kaspersky Endpoint Security cho Windows đề lên phiên bản tiện ích trước. Để quay lại phiên bản tiện ích trước, hãy xóa tiện ích hiện tại và cài đặt phiên bản trước của tiện ích.
- Khi nâng cấp Kaspersky Endpoint Security 11.0.0 hoặc 11.0.1 cho Windows, [thiết lập lịch tác vụ cục bộ](#) cho tác vụ *Cập nhật*, *Quét khu vực quan trọng*, *Quét tùy chỉnh* và *Kiểm tra tính toàn vẹn* sẽ không được lưu.
- Trên máy tính chạy Windows 10 phiên bản 1903 và 1909, các bản nâng cấp từ Kaspersky Endpoint Security 10 cho Windows Service Pack 2 Maintenance Release 3 (bản dựng 10.3.3.275), Service Pack 2 Maintenance Release 4 (bản dựng 10.3.3.304), 11.0.0 và 11.0.1 có thành phần Mã hóa mức độ tập tin (FLE) được cài đặt có thể kết thúc kèm theo lỗi. Lý do là bởi vì mã hóa tập tin không được hỗ trợ cho các phiên bản này của Kaspersky Endpoint Security cho Windows trong Windows 10 phiên bản 1903 và 1909. Trước khi cài đặt bản nâng cấp này, bạn nên [gỡ bỏ thành phần mã hóa tập tin](#).
- Ứng dụng yêu cầu Microsoft .NET Framework 4.0 trở lên. Microsoft .NET Framework 4.6.1 có các lỗ hổng bảo mật. Nếu bạn đang sử dụng Microsoft .NET Framework 4.6.1, bạn phải cài đặt các bản cập nhật bảo mật. Để biết chi tiết về các bản cập nhật bảo mật của Microsoft .NET Framework, hãy tham khảo [Trang web Hỗ trợ kỹ thuật của Microsoft](#).
- Nếu bạn đang nâng cấp phiên bản trước của ứng dụng lên phiên bản 11.9.0, để cài đặt Kaspersky Endpoint Agent, hãy khởi động lại máy tính và đăng nhập vào hệ thống bằng tài khoản có quyền quản trị viên cục bộ. Nếu không, Kaspersky Endpoint Agent sẽ không được cài đặt trong quá trình nâng cấp.
- Nếu bạn đang nâng cấp Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 cho Windows khi có thành phần Mã hóa mức độ tập tin (FLE) được cài đặt trên các máy tính chạy Windows 10 phiên bản 1809, 1903 và 1909, thì trình điều khiển FDE sẽ không được cài đặt vào ảnh WinRE.
- Khi nâng cấp Kaspersky Endpoint Security, ứng dụng sẽ vô hiệu hóa việc sử dụng KSN đến khi Tuyên bố Kaspersky Security Network được chấp nhận. Ngoài ra, bạn có thể thay đổi trạng thái máy tính thành *Nghiêm trọng* trong Kaspersky Security Center; sự kiện *Máy chủ KSN không khả dụng* được nhận. Nếu sử dụng [Kaspersky Managed Detection and Response](#) thì bạn sẽ nhận được các sự kiện về các vi phạm trong hoạt động của giải pháp. Sử dụng KSN là yêu cầu bắt buộc cho hoạt động của Kaspersky Managed Detection and Response. Kaspersky Endpoint Security [sẽ bật sử dụng KSN](#) sau khi áp dụng chính sách trong đó quản trị viên chấp nhận điều khoản sử dụng KSN. Một khi Tuyên bố Kaspersky Security Network được chấp nhận, Kaspersky Endpoint Security sẽ khôi phục hoạt động của ứng dụng.
- Sau khi ứng dụng được nâng cấp từ các phiên bản cũ hơn Kaspersky Endpoint Security 11 cho Windows, máy tính phải được khởi động lại.

- Hệ thống tập tin ReFS được hỗ trợ với một số hạn chế:
 - Kaspersky Endpoint Security có thể xử lý các sự kiện khử mã độc mối đe dọa không chính xác. Ví dụ: nếu ứng dụng đã xóa tập tin độc hại thì báo cáo có thể có mục Đối tượng chưa được xử lý. Đồng thời, Kaspersky Endpoint Security sẽ khử mã độc các mối đe dọa theo thiết lập ứng dụng. Kaspersky Endpoint Security cũng có thể tạo một mục trùng lặp của sự kiện *Đối tượng sẽ được khử mã độc khi khởi động lại* cho cùng một đối tượng.
 - Bảo vệ mối đe dọa tập tin có thể bỏ qua một số mối đe dọa. Đồng thời, Quét virus hoạt động đúng.
 - Sau khi quá trình kiểm tra chống virus trên máy chủ được khởi chạy, các loại trừ quét được thêm vào bằng iChecker sẽ được đặt lại khi máy chủ khởi động lại.
 - Công nghệ iSwift không được hỗ trợ. Kaspersky Endpoint Security không xem xét các loại trừ quét được thêm vào bằng công nghệ iSwift.
 - Kaspersky Endpoint Security không phát hiện các tập tin eicar.com và susp-eicar.com nếu tập tin meicar.exe đã tồn tại trên máy tính trước khi Kaspersky Endpoint Security được cài đặt.
 - Kaspersky Endpoint Security có thể hiển thị không đúng các thông báo khử mã độc mối đe dọa. Ví dụ: ứng dụng có thể hiển thị thông báo mối đe dọa đối với mối đe dọa đã được khử mã độc trước đó.
 - Công nghệ Mã hóa mức độ tập tin (FLE) và Kaspersky Disk Encryption (FDE) không được hỗ trợ trên các nền tảng máy chủ. Đồng thời, Kaspersky Endpoint Security có thể xử lý không đúng các sự kiện mã hóa dữ liệu.
 - Trong hệ điều hành máy chủ, không có cảnh báo nào được hiển thị về việc cần thiết khử mã độc nâng cao.
 - Microsoft Windows Server 2008 không còn được hỗ trợ. - Không hỗ trợ cài đặt ứng dụng trên máy tính chạy hệ điều hành Microsoft Windows Server 2008.
- Chế độ Core được hỗ trợ với những hạn chế:
 - Giao diện đồ họa người dùng cục bộ không khả dụng, bao gồm thông báo, thông báo nổi và các thành phần điều khiển giao diện khác. Ứng dụng không thể hiển thị các cửa sổ nhắc nhở, bao gồm các cửa sổ sau:
 - Phiên bản ứng dụng và lời nhắc xác nhận nâng cấp mô-đun;
 - Lời nhắc khởi động lại máy tính;
 - Lời nhắc nhập thông tin tài khoản xác thực máy chủ proxy;
 - Nhắc lấy quyền truy cập vào một thiết bị (Kiểm soát thiết bị).
 - Các thành phần sau không khả dụng: Bảo vệ mối đe dọa web, Bảo vệ mối đe dọa thư điện tử, Kiểm soát Web, Phòng chống tấn công BadUSB.
 - Anti-Bridging không khả dụng.
 - Bạn chỉ có thể chấp nhận Tuyên bố Kaspersky Security Network trong chính sách ứng dụng trong bảng điều khiển Kaspersky Security Center.

- BitLocker Drive Encryption chỉ khả dụng với Mô-đun nền tảng tin tưởng (TPM). Không thể sử dụng mã PIN / mật khẩu để mã hóa vì ứng dụng không thể hiển thị cửa sổ nhắc mật khẩu để xác thực trước khi khởi động. Nếu hệ điều hành đã bật chế độ tương thích với Tiêu chuẩn Xử lý thông tin liên bang (FIPS), hãy kết nối một ổ đĩa di động để lưu khóa mã hóa trước khi bắt đầu mã hóa ổ đĩa.

Hỗ trợ các nền tảng ảo [?](#)

- Mã hóa toàn bộ ổ đĩa (FDE) trên máy ảo Hyper-V không được hỗ trợ.
- Mã hóa toàn bộ ổ đĩa (FDE) trên nền tảng ảo Citrix không được hỗ trợ.
- Windows 10 Enterprise đa phiên được hỗ trợ nhưng có các hạn chế:
 - Kaspersky Endpoint Security sẽ khử mã độc các mối đe dọa đang hoạt động mà không cần thông báo cho người dùng, giống như khi [khử mã độc các mối đe dọa đang hoạt động trên máy chủ](#). Vì hệ điều hành tiếp tục chạy ở chế độ đa phiên, những người dùng đang hoạt động khác có thể mất dữ liệu của họ nếu mối đe dọa không được giải quyết ngay.
 - Mã hóa toàn bộ ổ đĩa (FDE) không được hỗ trợ.
 - Quản lý BitLocker không được hỗ trợ.
 - Sử dụng Kaspersky Endpoint Security với ổ đĩa di động không được hỗ trợ. Hạ tầng Microsoft Azure coi ổ đĩa di động là ổ đĩa mạng.
- Không hỗ trợ cài đặt và sử dụng mã hóa mức độ tập tin (FLE) trên nền tảng ảo Citrix.
- Để hỗ trợ khả năng tương thích của Kaspersky Endpoint Security cho Windows với Citrix PVS, hãy thực hiện cài đặt với [tùy chọn Đảm bảo tương thích với Citrix PVS](#) được bật. Bạn có thể bật tùy chọn này trong [Trình hướng dẫn cài đặt](#) hoặc bằng cách sử dụng [tham số dòng lệnh](#) /pCITRIXCOMPATIBILITY=1. Trong trường hợp cài đặt từ xa, phải chỉnh sửa [tập tin KUD](#) bằng cách thêm tham số sau vào tập tin: /pCITRIXCOMPATIBILITY=1.
- Citrix XenDesktop. Trước khi bắt đầu nhân bản, bạn phải [tắt tính năng Tự bảo vệ](#) để nhân bản các máy ảo sử dụng vDisk.
- Khi chuẩn bị máy mẫu cho ảnh chủ Citrix XenDesktop có Kaspersky Endpoint Security cho Windows được cài đặt sẵn và Kaspersky Security Center Network Agent, hãy thêm các kiểu loại trừ sau vào tập tin cấu hình:


```
[Rule-Begin]
Type=File-Catalog-Construction
Action=Catalog-Location-Guest-Modifiable
name="%ALLUSERSPROFILE%\Kaspersky\**\*"
name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
[Rule-End]
```

Để biết chi tiết về Citrix XenDesktop, hãy truy cập [website Hỗ trợ Citrix](#).
- Trong một số trường hợp, nỗ lực ngắt kết nối an toàn ổ đĩa di động có thể không thành công trên máy ảo được triển khai trên VMware ESXi Hypervisor. Cố gắng ngắt kết nối an toàn thiết bị một lần nữa.

Khả năng tương thích với Kaspersky Security Center

- Bạn chỉ có thể quản lý thành phần Kiểm soát thích ứng sự cố trong Kaspersky Security Center phiên bản 11 hoặc mới hơn.
- Báo cáo về mối đe dọa của Kaspersky Security Center 11 có thể không hiển thị thông tin về hành động được thực hiện đối với các mối đe dọa được phát hiện bởi thành phần Bảo vệ AMSI.
- Trạng thái hoạt động của các thành phần Kiểm soát thích ứng sự cố và Bảo vệ AMSI chỉ khả dụng trong Kaspersky Security Center phiên bản 11 trở lên. Bạn có thể xem trạng thái hoạt động trong Bảng điều khiển Kaspersky Security Center trong thuộc tính máy tính, trong mục **Tác vụ**. Báo cáo dành cho các thành phần này cũng chỉ có sẵn trong Kaspersky Security Center phiên bản 11 trở lên.

Cấp giấy phép

- Nếu thông báo hệ thống *Lỗi nhận dữ liệu* được hiển thị, hãy xác minh rằng máy tính mà bạn đang thực hiện kích hoạt có quyền truy cập mạng hoặc bạn hãy cấu hình thiết lập kích hoạt thông qua Proxy kích hoạt của Kaspersky Security Center.
- Không thể kích hoạt ứng dụng bằng gói đăng ký qua Kaspersky Security Center nếu giấy phép đã hết hạn hoặc nếu giấy phép dùng thử đang hoạt động trên máy tính. Để thay thế giấy phép dùng thử hoặc giấy phép sắp hết hạn bằng giấy phép của gói đăng ký, hãy [sử dụng tác vụ phân phối giấy phép](#).
- Trong giao diện ứng dụng, ngày hết hạn giấy phép được hiển thị theo giờ địa phương của máy tính.
- Cài đặt ứng dụng kèm tập tin khóa nhúng trên máy tính có kết nối truy cập Internet không ổn định có thể dẫn đến việc hiển thị tạm thời các sự kiện báo rằng ứng dụng chưa được kích hoạt hoặc giấy phép không cho phép hoạt động của thành phần. Điều này là do ứng dụng cài đặt lần đầu và cố gắng kích hoạt giấy phép dùng thử nhúng. Giấy phép này yêu cầu truy cập Internet để kích hoạt trong quá trình cài đặt.
- Trong thời gian dùng thử, việc cài đặt bất kỳ bản vá hoặc nâng cấp ứng dụng nào trên máy tính có truy cập Internet không ổn định có thể dẫn đến việc hiển thị tạm thời các sự kiện cho biết ứng dụng chưa được kích hoạt. Điều này là do ứng dụng cài đặt và cố gắng kích hoạt giấy phép dùng thử nhúng một lần nữa. Giấy phép này yêu cầu truy cập Internet để kích hoạt khi cài đặt bản nâng cấp.
- Nếu giấy phép dùng thử được tự động kích hoạt trong quá trình cài đặt ứng dụng và sau đó ứng dụng bị xóa mà không lưu thông tin giấy phép thì ứng dụng sẽ không được tự động kích hoạt với giấy phép dùng thử khi được cài đặt lại. Trong trường hợp này, hãy kích hoạt ứng dụng theo cách thủ công.
- Nếu bạn đang sử dụng Kaspersky Security Center phiên bản 11 và Kaspersky Endpoint Security phiên bản 11.9.0, báo cáo hiệu năng của thành phần có thể hoạt động không chính xác. Nếu bạn đã cài đặt các thành phần Kaspersky Endpoint Security không có trong giấy phép của mình, Network Agent có thể gửi lỗi trạng thái thành phần vào Nhật ký Windows Event. Để tránh lỗi, hãy xóa các thành phần không có trong giấy phép của bạn.

Công cụ khắc phục

- Ứng dụng chỉ khôi phục tập tin trên các thiết bị có hệ thống tập tin NTFS hoặc FAT32.
- Ứng dụng có thể khôi phục các tập tin với phần mở rộng sau: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls,xlsx, xlsx, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.
- Bạn không thể khôi phục tập tin trên các ổ đĩa mạng hoặc trên các đĩa CD/DVD ghi lại được.
- Bạn không thể khôi phục các tập tin được mã hóa với Encryption File System (EFS). Để biết thêm chi tiết về hoạt động của EFS, vui lòng truy cập [website Microsoft](#).
- Ứng dụng không giám sát việc sửa đổi các tập tin bởi các tiến trình ở cấp kernel hệ điều hành.
- Ứng dụng không giám sát những sửa đổi lên tập tin qua một giao diện mạng (ví dụ, nếu tập tin được lưu trữ trong một thư mục được chia sẻ và một tiến trình được bắt đầu từ xa trên một máy tính khác).

Tường lửa

- Lọc các gói tin hoặc kết nối theo địa chỉ cục bộ, giao diện vật lý và thời gian tồn tại của gói tin (TTL) được hỗ trợ trong các trường hợp sau:
 - Theo địa chỉ cục bộ cho các gói tin hoặc kết nối gửi đi trong các quy tắc ứng dụng cho TCP và UDP và các quy tắc gói tin.
 - Theo địa chỉ cục bộ cho các gói tin hoặc kết nối đến (ngoại trừ UDP) trong các quy tắc chặn ứng dụng và quy tắc gói tin.
 - Theo thời gian tồn tại của gói tin (TTL) trong quy tắc chặn gói tin đối với các gói tin gửi đến hoặc gửi đi.
 - Theo giao diện mạng cho các gói tin gửi đến và gửi đi hoặc kết nối trong các quy tắc gói tin.
- Trong các phiên bản ứng dụng 11.0.0 và 11.0.1, các địa chỉ MAC đã xác định được áp dụng không chính xác. Thiết lập địa chỉ MAC cho phiên bản 11.0.0, 11.0.1 và 11.1.0 trở lên không tương thích. Sau khi nâng cấp ứng dụng hoặc tiện ích từ các phiên bản này lên phiên bản 11.1.0 trở lên, bạn phải xác minh và cấu hình lại các địa chỉ MAC đã xác định trong Quy tắc tường lửa.
- Khi nâng cấp ứng dụng từ phiên bản 11.1.1 và 11.2.0 lên phiên bản 11.9.0, các trạng thái quyền đối với các quy tắc Tường lửa sau sẽ không được chuyển:
 - Yêu cầu đến máy chủ DNS qua TCP.
 - Yêu cầu đến máy chủ DNS qua UDP.
 - Bất kỳ hoạt động mạng.
 - ICMP không có trả lời từ gói tin vào.
 - Luồng ICMP vào.
- Nếu bạn đã cấu hình bộ điều hợp mạng hoặc thời gian tồn tại của gói tin (TTL) cho quy tắc gói tin cho phép thì mức độ ưu tiên của quy tắc này thấp hơn quy tắc chặn ứng dụng. Nói cách khác, nếu hoạt động mạng bị chặn đối với một ứng dụng (ví dụ: ứng dụng nằm trong nhóm tin tưởng *Hạn chế cao*) thì bạn không thể cho phép hoạt động mạng của ứng dụng bằng cách sử dụng quy tắc gói tin với các thiết lập này. Trong tất cả các trường hợp khác, mức độ ưu tiên của quy tắc gói tin cao hơn quy tắc mạng ứng dụng.
- Khi [nhập quy tắc gói tin Tường lửa](#), Kaspersky Endpoint Security có thể sửa đổi tên quy tắc. Ứng dụng xác định các quy tắc bằng các bộ tham số chung giống nhau: giao thức, hướng, cổng từ xa và cục bộ, thời gian tồn tại của gói tin (TTL). Nếu nhóm tham số chung này giống nhau đối với nhiều quy tắc thì ứng dụng sẽ gán cùng tên cho các quy tắc này và thêm một thẻ tham số vào tên. Bằng cách này, Kaspersky Endpoint Security sẽ nhập tất cả các quy tắc gói tin, nhưng tên của các quy tắc có các tham số chung giống nhau có thể bị thay đổi.
- Nếu bạn [đã bật báo cáo sự kiện ứng dụng trong quy tắc mạng](#) thì khi chuyển ứng dụng sang một nhóm tin tưởng khác, các hạn chế của nhóm tin tưởng này sẽ không được áp dụng. Do đó, nếu ứng dụng nằm trong nhóm tin tưởng Được tin tưởng thì ứng dụng sẽ không có các hạn chế mạng. Khi đó, bạn đã bật báo cáo sự kiện cho ứng dụng này và chuyển ứng dụng vào nhóm tin tưởng Không tin tưởng. Tường lửa sẽ không thực thi các hạn chế mạng cho ứng dụng này. Chúng tôi khuyến nghị bạn nên chuyển ứng dụng vào nhóm tin tưởng phù hợp trước rồi sau đó bật báo cáo sự kiện. Nếu phương pháp này không phù hợp, bạn có thể cấu hình các hạn chế cho ứng dụng theo cách thủ công trong phần thiết lập quy tắc mạng. Hạn chế chỉ áp dụng cho giao diện cục bộ của ứng dụng. Chuyển ứng dụng giữa các nhóm tin tưởng trong chính sách hoạt động đúng.

- Thành phần Tường lửa và thành phần Phòng chống xâm nhập có các thiết lập chung: quyền ứng dụng và tài nguyên được bảo vệ. Nếu bạn thay đổi các thiết lập này cho Tường lửa thì Kaspersky Endpoint Security sẽ tự động áp dụng các thiết lập mới cho Phòng chống xâm nhập. Ví dụ: nếu bạn đã cho phép thay đổi thiết lập chung của chính sách Tường lửa (ổ khóa đang mở) thì thiết lập Phòng chống xâm nhập cũng sẽ chuyển sang trạng thái cho phép chỉnh sửa.
- Khi một [quy tắc gói tin mạng](#) được kích hoạt trong Kaspersky Endpoint Security 11.6.0 trở lên thì cột **Tên ứng dụng** trong báo cáo Tường lửa sẽ luôn hiển thị giá trị *Kaspersky Endpoint Security*. Ngoài ra, Tường lửa sẽ chặn kết nối ở cấp độ gói tin đối với mọi ứng dụng. Hành vi này đã được sửa đổi cho Kaspersky Endpoint Security 11.7.0 trở lên. Cột **Loại quy tắc** đã được thêm vào [Báo cáo tường lửa](#). Khi một quy tắc gói tin mạng được kích hoạt, giá trị trong cột **Tên ứng dụng** sẽ vẫn được để trống.

[Phòng chống Tấn công BadUSB](#)

- Kaspersky Endpoint Security sẽ đặt lại thời gian chờ khóa thiết bị USB khi máy tính bị khóa (ví dụ: hết thời gian chờ của màn hình khóa). Có nghĩa là nếu bạn nhập sai mã cấp phép cho thiết bị USB nhiều lần và ứng dụng khóa thiết bị USB đó thì Kaspersky Endpoint Security sẽ cho phép bạn lặp lại nỗ lực cấp phép khi mở khóa máy tính. Trong trường hợp này, Kaspersky Endpoint Security sẽ không khóa thiết bị USB trong một thời gian được chỉ định trong [thiết lập của thành phần Phòng chống Tấn công BadUSB](#).
- Kaspersky Endpoint Security sẽ đặt lại thời gian chờ khóa thiết bị USB khi [tạm dừng bảo vệ máy tính](#). Có nghĩa là nếu bạn nhập sai mã cấp phép cho thiết bị USB nhiều lần và ứng dụng khóa thiết bị USB đó thì Kaspersky Endpoint Security sẽ cho phép bạn lặp lại nỗ lực cấp phép sau [khôi phục bảo vệ máy tính](#). Trong trường hợp này, Kaspersky Endpoint Security sẽ không khóa thiết bị USB trong một thời gian được chỉ định trong [thiết lập của thành phần Phòng chống Tấn công BadUSB](#).

[Kiểm soát ứng dụng](#)

- Chỉ các tập tin nén ZIP dưới 104 MB mới được hỗ trợ khi quản lý các quy tắc Kiểm soát ứng dụng trong Bảng điều khiển web Kaspersky Security Center. Các tập tin nén ở các định dạng khác như RAR hoặc 7z sẽ không được hỗ trợ. Sẽ không có hạn chế như vậy nếu bạn làm việc với các Quy tắc kiểm soát ứng dụng trong Bảng điều khiển quản trị (MMC).
- Khi làm việc trong Microsoft Windows 10 ở chế độ danh sách ứng dụng không được phép, quy tắc chặn có thể được áp dụng không chính xác, điều này có thể gây ra việc chặn các ứng dụng không được chỉ định trong quy tắc.
- Khi các ứng dụng web lữ tiến (PWA) bị chặn bởi thành phần Kiểm soát ứng dụng, appManifest.xml được chỉ định là ứng dụng bị chặn trong báo cáo.
- Khi thêm ứng dụng Notepad tiêu chuẩn vào Quy tắc kiểm soát ứng dụng cho Windows 11, bạn không nên chỉ định đường dẫn đến ứng dụng. Trên máy tính chạy Windows 11, hệ điều hành sử dụng Metro Notepad có trong thư mục C:\Program Files\WindowsApps\Microsoft.WindowsNotepad*\Notepad\Notepad.exe. Trong các phiên bản trước của hệ điều hành, Notepad có trong các thư mục sau:
 - C:\Windows\notepad.exe
 - C:\Windows\System32\notepad.exe
 - C:\Windows\SysWOW64\notepad.exe

Ví dụ như khi thêm Notepad vào Quy tắc kiểm soát ứng dụng, bạn có thể chỉ định tên ứng dụng và hash tập tin từ các thuộc tính của ứng dụng đang chạy.

Kiểm soát Thiết bị

- Quyền truy cập vào các thiết bị Máy in đã được thêm vào danh sách được tin tưởng bị chặn bởi các quy tắc chặn thiết bị và bus.
- Đối với thiết bị MTP, quyền kiểm soát hoạt động Đọc, Ghi và Kết nối được hỗ trợ nếu bạn đang sử dụng trình điều khiển tích hợp sẵn của hệ điều hành của Microsoft. Nếu người dùng cài đặt trình điều khiển tùy chỉnh để làm việc với một thiết bị (ví dụ: như một phần của iTunes hoặc Android Debug Bridge), quyền kiểm soát các hoạt động Đọc và Ghi có thể không hoạt động.
- Khi làm việc với thiết bị MTP, các quy tắc truy cập được thay đổi sau khi kết nối lại thiết bị.
- Thành phần Kiểm soát thiết bị ghi lại các sự kiện liên quan đến các thiết bị được giám sát, chẳng hạn như việc kết nối và ngắt kết nối của thiết bị, đọc tập tin từ thiết bị, ghi tập tin vào thiết bị và các sự kiện khác. Kaspersky Endpoint Security chỉ đăng ký các sự kiện ngắt kết nối cho các loại thiết bị sau: Thiết bị di động (MTP), Ổ đĩa di động, Ổ đĩa mềm, Ổ đĩa CD/DVD. Đối với các loại thiết bị khác, ứng dụng không đăng ký các sự kiện ngắt kết nối. Ứng dụng đăng ký hoạt động kết nối thiết bị với máy tính cho tất cả các loại thiết bị.
- Nếu bạn đang thêm một thiết bị vào danh sách được tin tưởng dựa trên tên đại diện mẫu máy và sử dụng các ký tự có trong ID nhưng không có trong tên mẫu máy, thì những thiết bị này sẽ không được thêm vào. Trên máy trạm, các thiết bị này sẽ được thêm vào danh sách được tin tưởng dựa trên tên đại diện ID.

Kiểm soát Web

- Các định dạng OGV và WEBM không được hỗ trợ.
- Giao thức RTMP không được hỗ trợ.

Kiểm soát thích ứng sự cố

- Bạn nên tự động tạo các loại trừ dựa trên sự kiện. Khi [thêm một loại trừ theo cách thủ công](#), hãy thêm ký tự `*` vào đầu đường dẫn khi chỉ định đối tượng đích.
- [Không thể tạo báo cáo quy tắc Kiểm soát thích ứng sự cố](#) nếu mẫu có dù chỉ một sự kiện có tên dài hơn 260 ký tự.
- Việc thêm các mục loại trừ từ kho lưu trữ Kích hoạt quy tắc Kiểm soát thích ứng sự cố sẽ không được hỗ trợ nếu các thuộc tính của một đối tượng hay tiến trình có giá trị chứa nhiều hơn 256 ký tự (ví dụ: đường dẫn đến đối tượng mục tiêu). Bạn có thể [thêm một mục loại trừ theo cách thủ công trong phần thiết lập Chính sách](#). Bạn cũng có thể thêm một mục loại trừ trong [Báo cáo về các quy tắc Kiểm soát thích ứng sự cố được kích hoạt](#).

Mã hóa ổ đĩa (FDE)

- Sau khi cài đặt ứng dụng, bạn phải khởi động lại hệ điều hành để mã hóa ổ cứng hoạt động đúng.
- Authentication Agent không hỗ trợ chữ tượng hình hoặc các ký tự đặc biệt `[]` và `\`.
- Để có hiệu năng máy tính tối ưu sau khi mã hóa, bộ vi xử lý phải hỗ trợ tập lệnh AES-NI (Intel Advanced Encryption Standard New Instructions). Nếu bộ vi xử lý không hỗ trợ tập lệnh AES-NI thì hiệu năng máy tính có thể bị giảm.
- Khi có các tiến trình cố gắng truy cập vào các thiết bị được mã hóa trước khi ứng dụng cấp quyền truy cập vào các thiết bị đó, ứng dụng sẽ hiển thị cảnh báo cho biết rằng phải chấm dứt các tiến trình đó. Nếu không thể chấm dứt tiến trình, hãy kết nối lại các thiết bị đã mã hóa.
- ID duy nhất của ổ cứng được hiển thị trong phần thống kê mã hóa thiết bị ở định dạng đảo ngược.
- Bạn không nên định dạng thiết bị khi chúng đang được mã hóa.
- Khi nhiều ổ đĩa di động được kết nối đồng thời với một máy tính, chính sách mã hóa chỉ có thể được áp dụng cho một ổ đĩa di động. Khi các thiết bị di động được kết nối lại, chính sách mã hóa sẽ được áp dụng đúng.
- Quá trình mã hóa có thể không bắt đầu trên ổ cứng bị phân mảnh nặng. Chống phân mảnh ổ cứng.
- Khi ổ cứng được mã hóa, chế độ ngủ đông sẽ bị chặn từ thời điểm bắt đầu tác vụ mã hóa cho đến lần khởi động lại đầu tiên của máy tính chạy Microsoft Windows 7/8/8.1/10 và sau khi cài đặt mã hóa ổ cứng cho đến lần khởi động lại đầu tiên của hệ điều hành Microsoft Windows 8/8.1/10. Khi ổ đĩa cứng được giải mã, chế độ ngủ đông sẽ bị chặn từ khi ổ đĩa khởi động được giải mã hoàn toàn cho đến lần khởi động lại hệ điều hành đầu tiên. Khi tùy chọn **Bắt đầu nhanh** được bật trong Microsoft Windows 8/8.1/10, việc chặn chế độ ngủ đông sẽ ngăn bạn tắt hệ điều hành.
- Các máy tính Windows 7 không cho phép thay đổi mật khẩu trong quá trình khôi phục khi ổ đĩa được mã hóa bằng công nghệ BitLocker. Sau khi khóa phục hồi được nhập và hệ điều hành được nạp, Kaspersky Endpoint Security sẽ không nhắc người dùng thay đổi mật khẩu hoặc mã PIN. Do đó, bạn không thể đặt mật khẩu mới hoặc mã PIN. Sự cố này bắt nguồn từ các đặc điểm riêng của hệ điều hành. Để tiếp tục, bạn cần mã hóa lại ổ đĩa cứng.
- Bạn không nên sử dụng công cụ xbootmgr.exe khi có các nhà cung cấp bổ sung được bật. Ví dụ: Bộ điều phối, Mạng hoặc Trình điều khiển.
- Định dạng ổ đĩa di động được mã hóa không được hỗ trợ trên máy tính đã cài đặt Kaspersky Endpoint Security cho Windows.
- Không hỗ trợ định dạng ổ đĩa di động được mã hóa có hệ thống tập tin FAT32 (ổ đĩa được hiển thị là đã mã hóa). Để định dạng ổ đĩa, hãy định dạng lại ổ đĩa đó thành hệ thống tập tin NTFS.
- Để biết chi tiết về cách khôi phục hệ điều hành từ bản sao lưu sang thiết bị GPT được mã hóa, hãy truy cập [Cơ sở kiến thức Hỗ trợ kỹ thuật](#).
- Nhiều tác nhân tải xuống không thể cùng tồn tại trên một máy tính được mã hóa.
- Không thể truy cập vào ổ đĩa di động đã được mã hóa trước đó trên một máy tính khác khi đồng thời đáp ứng tất cả các điều kiện sau:
 - Không có kết nối với máy chủ Kaspersky Security Center.

- Người dùng đang cố gắng cấp phép bằng mã thông báo hoặc mật khẩu mới.

Nếu trường hợp tương tự xảy ra, hãy khởi động lại máy tính. Sau khi máy tính được khởi động lại, quyền truy cập vào ổ đĩa di động được mã hóa sẽ được cấp.

- Có thể không hỗ trợ việc khám phá thiết bị USB của Authentication Agent khi chế độ xHCI cho USB được bật trong thiết lập BIOS.
- Đối với ổ đĩa lai SSHD, tính năng Kaspersky Disk Encryption (FDE) sẽ không hỗ trợ cho phần SSD của thiết bị được sử dụng để lưu vào bộ nhớ đệm dữ liệu hay dùng nhất.
- Không hỗ trợ mã hóa ổ cứng trong hệ điều hành Microsoft Windows 8/8.1/10 32-bit chạy ở chế độ UEFI.
- Hãy khởi động lại máy tính trước khi mã hóa lại ổ cứng đã được giải mã.
- Mã hóa ổ cứng không tương thích với Kaspersky Anti-Virus cho UEFI. Không nên sử dụng mã hóa ổ cứng trên máy tính đã cài đặt Kaspersky Anti-Virus cho UEFI.
- Hỗ trợ [Việc tạo tài khoản Authentication Agent](#) dựa trên tài khoản Microsoft nhưng có các hạn chế sau:
 - Công nghệ [Single Sign-On](#) không được hỗ trợ.
 - Không hỗ trợ tự động tạo tài khoản Authentication Agent nếu chọn tùy chọn tạo tài khoản cho người dùng đăng nhập vào hệ thống trong N ngày qua.
- Nếu tên của tài khoản Authentication Agent có định dạng <tên miền>/<tên tài khoản windows>, sau khi thay đổi tên máy tính, bạn cũng cần thay đổi tên của tài khoản đã được tạo cho người dùng cục bộ của máy tính này. Ví dụ: hãy hình dung có một người dùng cục bộ Ivanov trên máy tính Ivanov và tài khoản Authentication Agent tên là Ivanov/Ivanov đã được tạo cho người dùng này. Nếu tên máy tính Ivanov đã được đổi thành Ivanov-PC, bạn cần thay đổi tên tài khoản Authentication Agent cho người dùng Ivanov từ Ivanov/Ivanov thành Ivanov-PC/Ivanov. Bạn có thể thay đổi tên tài khoản bằng tác vụ quản lý tài khoản cục bộ của Authentication Agent. Trước khi tên của tài khoản đã được thay đổi, bạn có thể xác thực trong môi trường tiền khởi động bằng tên cũ (ví dụ: Ivanov/Ivanov).
- Nếu người dùng được phép truy cập vào máy tính được mã hóa bằng công nghệ Kaspersky Disk Encryption chỉ bằng cách sử dụng mã thông báo và người dùng này cần hoàn tất quy trình khôi phục quyền truy cập, hãy đảm bảo rằng người dùng này được cấp quyền truy cập bằng mật khẩu vào máy tính này sau khi truy cập vào máy tính được mã hóa đã được khôi phục. Mật khẩu mà người dùng đặt khi khôi phục quyền truy cập có thể không được lưu. Trong trường hợp này, người dùng sẽ phải hoàn tất quy trình khôi phục lại quyền truy cập vào máy tính được mã hóa trong lần khởi động lại máy tính tiếp theo.
- Khi giải mã ổ cứng bằng [FDE Recovery Tool](#), quá trình giải mã có thể kết thúc kèm theo lỗi nếu dữ liệu trên thiết bị nguồn bị ghi đè bằng dữ liệu đã giải mã. Một phần dữ liệu trên ổ cứng sẽ vẫn được mã hóa. Bạn nên chọn tùy chọn để lưu dữ liệu được giải mã vào một tập tin trong thiết lập giải mã thiết bị khi sử dụng FDE Recovery Tool.
- Nếu mật khẩu của Authentication Agent đã được thay đổi thì sẽ một thông báo chứa nội dung *Mật khẩu của bạn đã được thay đổi thành công. Thông báo Nhấn OK* sẽ xuất hiện và người dùng khởi động lại máy tính, mật khẩu mới không được lưu. Phải dùng mật khẩu cũ cho lần xác thực tiếp theo trong môi trường tiền khởi động.
- Mã hóa ổ đĩa không tương thích với công nghệ Intel Rapid Start.

- Mã hóa ổ đĩa không tương thích với công nghệ ExpressCache.
- Trong một số trường hợp, khi cố gắng giải mã ổ đĩa được mã hóa bằng [FDE Recovery Tool](#), công cụ này sẽ phát hiện nhầm trạng thái thiết bị là "không được mã hóa" sau khi hoàn tất quy trình "Yêu cầu-Phản hồi". Nhật ký của công cụ sẽ hiển thị một sự kiện cho biết thiết bị đã được giải mã thành công. Trong trường hợp này, bạn phải khởi động lại quy trình khôi phục dữ liệu để giải mã thiết bị.
- Sau khi tiện ích Kaspersky Endpoint Security cho Windows được cập nhật trong Bảng điều khiển web, các thuộc tính máy khách không hiển thị khóa khôi phục BitLocker đến khi khởi động lại dịch vụ Bảng điều khiển web.
- Để xem các hạn chế khác của hỗ trợ mã hóa toàn bộ ổ đĩa và danh sách các thiết bị hỗ trợ mã hóa ổ cứng với các hạn chế, vui lòng tham khảo [Cơ sở Kiến thức Hỗ trợ Kỹ thuật](#).

[Mã hóa mức độ tập tin \(FLE\)](#)

- Mã hóa tập tin và thư mục không được hỗ trợ trong các hệ điều hành thuộc dòng Microsoft Windows Embedded.
- Một khi bạn đã cài đặt ứng dụng, bạn phải khởi động lại hệ điều hành để quá trình mã hóa tập tin và thư mục hoạt động đúng.
- Nếu tập tin được mã hóa được lưu trữ trên máy tính có sẵn chức năng mã hóa và bạn truy cập tập tin từ máy tính không có mã hóa, bạn sẽ được cấp quyền truy cập trực tiếp vào tập tin này. Tập tin mã hóa được lưu trữ trong thư mục mạng trên máy tính có sẵn chức năng mã hóa sẽ được sao chép ở dạng đã giải mã sang máy tính không có sẵn chức năng mã hóa.
- Bạn nên giải mã các tập tin đã được mã hóa bằng Hệ thống tệp mã hóa trước khi mã hóa tập tin bằng Kaspersky Endpoint Security cho Windows.
- Sau khi tập tin được mã hóa, dung lượng của tập tin sẽ tăng thêm 4 kB.
- Sau khi tập tin được mã hóa, thuộc tính *Lưu trữ* sẽ được đặt trong thuộc tính tập tin.
- Nếu một tập tin được giải nén từ tập tin nén mã hóa có cùng tên với một tập tin có sẵn trên máy tính của bạn thì tập tin có sẵn sẽ bị ghi đè bởi tập tin mới được giải nén từ tập tin nén mã hóa. Người dùng không được thông báo về hoạt động ghi đè.
- Trước khi bạn giải nén một tập tin nén được mã hóa, đảm bảo rằng bạn có đủ dung lượng đĩa trống để chứa các tập tin được giải nén. Nếu bạn không có đủ dung lượng đĩa, quá trình giải nén tập tin nén có thể hoàn tất nhưng các tập tin đó có thể bị hỏng. Trong trường hợp này, Kaspersky Endpoint Security có thể không hiển thị bất kỳ thông báo lỗi nào.
- Giao diện [Trình quản lý tập tin di động](#) không hiển thị thông báo về lỗi xảy ra trong quá trình hoạt động.
- Kaspersky Endpoint Security cho Windows không khởi động [Trình quản lý tập tin di động](#) trên máy tính đã cài đặt thành phần Mã hóa mức độ tập tin.
- Bạn không thể sử dụng [Trình quản lý tập tin di động](#) để truy cập vào một ổ đĩa di động nếu các điều kiện sau là đều đúng đồng thời:
 - Không có kết nối với Kaspersky Security Center;
 - Kaspersky Endpoint Security cho Windows được cài đặt trên máy tính;
 - Mã hóa dữ liệu (FDE hoặc FLE) không được thực hiện trên máy tính.

Không thể lấy quyền truy cập cho dù bạn biết mật khẩu cho Trình quản lý tập tin di động.

- Khi sử dụng mã hóa tập tin, ứng dụng không tương thích với ứng dụng thư Sylpheed.
- Kaspersky Endpoint Security cho Windows không hỗ trợ [các quy tắc giới hạn quyền truy cập các tập tin được mã hóa](#) đối với một số ứng dụng. Đây là do một số hoạt động tập tin được thực hiện bởi ứng dụng của bên thứ ba. Ví dụ: sao chép tập tin được thực hiện bởi trình quản lý tập tin, không phải bởi ứng dụng. Theo đó, nếu quyền truy cập vào các tập tin được mã hóa bị từ chối đối với ứng dụng thư Outlook, Kaspersky Endpoint Security sẽ cho phép ứng dụng thư khách truy cập vào tập tin được mã hóa, nếu người dùng đã sao chép tập tin vào thư email qua khay nhớ tạm hoặc sử dụng chức năng kéo và thả. Thao tác sao chép được thực hiện bởi trình quản lý tập tin, trong đó các quy tắc hạn chế quyền truy cập vào tập tin được mã hóa không được chỉ định, tức là quyền truy cập được cho phép.

- Khi ổ đĩa di động được mã hóa kèm [hỗ trợ chế độ di động](#), bạn không thể tắt tính năng kiểm soát thời gian tồn tại của mật khẩu.
- Không hỗ trợ thay đổi thiết lập tập tin page. Hệ điều hành sử dụng các giá trị mặc định thay vì các giá trị tham số được chỉ định.
- Sử dụng tính năng xóa an toàn khi làm việc với các ổ đĩa di động được mã hóa. Chúng tôi không thể đảm bảo tính toàn vẹn của dữ liệu nếu ổ đĩa di động không được ngắt kết nối an toàn.
- Sau khi các tập tin được mã hóa, các bản gốc không được mã hóa của chúng sẽ bị xóa một cách an toàn.
- Không hỗ trợ đồng bộ hóa tập tin ngoại tuyến bằng cách sử dụng Client-Side Caching (CSC). Chúng tôi khuyến nghị cấm quản lý ngoại tuyến các tài nguyên được chia sẻ ở cấp chính sách nhóm. Có thể chỉnh sửa các tập tin ở chế độ ngoại tuyến. Sau khi đồng bộ hóa, các thay đổi được thực hiện đối với tập tin ngoại tuyến có thể bị mất. Để biết chi tiết về hỗ trợ Client-Side Caching (CSC) khi sử dụng mã hóa, vui lòng tham khảo [Cơ sở kiến thức Hỗ trợ kỹ thuật](#).
- Không hỗ trợ [Tạo tập tin nén được mã hóa](#) trong thư mục gốc của ổ cứng hệ thống.
- Bạn có thể gặp sự cố khi truy cập các tập tin được mã hóa qua mạng. Bạn nên di chuyển các tập tin đó sang một nguồn khác hoặc đảm bảo rằng máy tính đang được sử dụng làm máy chủ tập tin được quản lý bởi cùng một Máy chủ quản trị Kaspersky Security Center.
- Thay đổi bố cục bàn phím có thể làm cho cửa sổ nhập mật khẩu cho tập tin nén tự giải nén được mã hóa bị treo. Để khắc phục vấn đề này, hãy đóng cửa sổ nhập mật khẩu, chuyển sang bố cục bàn phím trong hệ điều hành của bạn và nhập lại mật khẩu cho tập tin nén được mã hóa.
- Khi mã hóa tập tin được sử dụng trên các hệ thống có nhiều phân vùng trên một ổ đĩa, bạn nên sử dụng tùy chọn tự động xác định dung lượng của tập tin pagefile.sys. Sau khi máy tính khởi động lại, tập tin pagefile.sys có thể di chuyển giữa các phân vùng đĩa.
- Sau khi áp dụng các quy tắc mã hóa tập tin, bao gồm các tập tin trong thư mục My Documents, hãy đảm bảo rằng người dùng được áp dụng mã hóa có thể truy cập thành công các tập tin được mã hóa. Để thực hiện, hãy yêu cầu mỗi người dùng đăng nhập vào hệ thống khi có kết nối với Kaspersky Security Center. Nếu người dùng cố gắng truy cập các tập tin được mã hóa mà không có kết nối với Kaspersky Security Center, hệ thống có thể bị treo.
- Nếu bằng cách nào đó, các tập tin hệ thống được đưa vào phạm vi mã hóa mức độ tập tin thì những sự kiện liên quan đến lỗi khi mã hóa các tập tin này có thể xuất hiện trong báo cáo. Các tập tin được đề cập trong những sự kiện này không thực sự được mã hóa.
- Các tiến trình Pico không được hỗ trợ.
- Đường dẫn phân biệt chữ hoa chữ thường không được hỗ trợ. Khi áp dụng quy tắc mã hóa hoặc quy tắc giải mã, đường dẫn trong các sự kiện sản phẩm được hiển thị bằng chữ thường.
- Không nên mã hóa các tập tin được hệ thống sử dụng khi khởi động. Nếu các tập tin này được mã hóa, việc cố gắng truy cập các tập tin được mã hóa mà không có kết nối với Kaspersky Security Center có thể khiến hệ thống bị treo hoặc làm xuất hiện lời nhắc truy cập vào các tập tin không được mã hóa.
- Nếu người dùng cùng làm việc với tập tin qua mạng theo quy tắc FLE thông qua các ứng dụng sử dụng phương pháp ánh xạ tập tin vào bộ nhớ (như WordPad hoặc FAR) và các ứng dụng được thiết kế để làm việc với tập tin lớn (như Notepad ++) thì tập tin ở dạng không được mã hóa có thể bị chặn vô thời hạn mà không có khả năng truy cập tập tin đó từ máy tính đang lưu.

- Kaspersky Endpoint Security không mã hóa các tập tin nằm trong ổ lưu trữ đám mây OneDrive hoặc trong các thư mục khác có tên là OneDrive. Kaspersky Endpoint Security cũng chặn sao chép các tập tin được mã hóa vào thư mục OneDrive nếu các tập tin đó không được thêm vào [quy tắc giải mã](#).
- Khi thành phần Mã hóa mức độ tập tin được cài đặt, việc quản lý người dùng và nhóm sẽ không hoạt động ở chế độ WSL (Hệ thống phụ của Windows dành cho Linux).
- Khi thành phần Mã hóa mức độ tập tin được cài đặt, POSIX (Giao diện Hệ điều hành di động) để đổi tên và xóa tập tin không được hỗ trợ.
- Không nên mã hóa các tập tin tạm, vì làm vậy có thể gây mất dữ liệu. Ví dụ: Microsoft Word tạo các tập tin tạm khi xử lý tài liệu. Nếu các tập tin tạm được mã hóa, nhưng tập tin gốc thì không, người dùng có thể nhận được lỗi *Quyền truy cập bị từ chối* khi cố gắng lưu tài liệu. Ngoài ra, Microsoft Word có thể lưu tập tin, nhưng sẽ không thể mở tài liệu vào lần sau, nghĩa là dữ liệu sẽ bị mất. Để tránh mất dữ liệu, bạn cần [loại trừ thư mục tập tin tạm khỏi các quy tắc mã hóa](#).
- Sau khi cập nhật Kaspersky Endpoint Security cho Windows phiên bản 11.0.1 trở xuống, để truy cập các tập tin được mã hóa sau khi khởi động lại máy tính, hãy đảm bảo rằng Network Agent đang chạy. Network Agent có chế độ khởi động chậm, vì vậy bạn không thể truy cập các tập tin được mã hóa ngay sau khi nạp hệ điều hành. Không cần đợi Network Agent khởi chạy sau lần khởi động máy tính tiếp theo.

[Các hạn chế khác](#)

- Nếu ứng dụng trả về 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 diệt virus hoặc áp dụng các bản cập nhật cho mô-đun ứng dụng.
- Các địa chỉ web được [thêm vào danh sách được tin tưởng](#) có thể bị xử lý không chính xác.
- Trong bảng điều khiển Kaspersky Security Center, bạn không thể lưu tập tin vào đĩa từ thư mục **Advanced** → **Repositories** → **Active threats**. Để lưu tập tin, bạn phải khử mã độc tập tin bị nhiễm. Khi khử mã độc, ứng dụng sẽ lưu bản sao của tập tin vào Sao lưu. Bây giờ bạn có thể lưu tập tin vào đĩa từ thư mục **Advanced** → **Repositories** → **Backup**.
- Việc kế thừa thiết lập truyền dữ liệu đến Máy chủ quản trị (**Thiết lập tổng quát** → **Các báo cáo và lưu trữ** → **Truyền dữ liệu đến Máy chủ quản trị**) khác với việc kế thừa của các thiết lập khác. Nếu bạn đã cho phép thay đổi thiết lập truyền dữ liệu trong chính sách ("ổ khóa" được mở), các thiết lập này sẽ được đặt lại về giá trị mặc định trong thuộc tính máy tính cục bộ trong bảng điều khiển nếu chúng chưa được định nghĩa từ trước. Nếu các thiết lập này đã được định nghĩa từ trước thì giá trị của chúng sẽ được khôi phục. Khi xóa một chính sách, các thiết lập sẽ được kế thừa theo cách tương tự. Trong những trường hợp này, các thiết lập khác trong thuộc tính máy tính cục bộ sẽ được kế thừa từ chính sách.
- Kaspersky Endpoint Security sẽ theo dõi lưu lượng HTTP tuân theo các tiêu chuẩn RFC 2616, RFC 7540, RFC 7541, RFC 7301. Nếu Kaspersky Endpoint Security phát hiện định dạng trao đổi dữ liệu khác trong lưu lượng HTTP thì ứng dụng sẽ chặn kết nối này để ngăn tải về các tập tin độc hại từ Internet.
- Kaspersky Endpoint Security ngăn giao tiếp qua giao thức QUIC. Các trình duyệt sử dụng giao thức truyền gửi tiêu chuẩn (TLS hoặc SSL) bất kể hỗ trợ QUIC có được bật trong trình duyệt hay không.
- Giám sát hệ thống. Thông tin đầy đủ về các tiến trình không được hiển thị.
- Khi Kaspersky Endpoint Security cho Windows được khởi động lần đầu tiên, ứng dụng có chữ ký số có thể tạm thời bị xếp vào nhóm sai. Về sau, ứng dụng có chữ ký số sẽ được đưa vào nhóm đúng.
- Khi quét thư bằng [Phần mở rộng Bảo vệ mỗi đe dọa thư điện tử cho Microsoft Outlook](#), bạn nên sử dụng chế độ Cached Exchange Mode (tùy chọn Sử dụng Cached Exchange Mode).
- [Tác vụ Quét virus](#) không hỗ trợ phiên bản Microsoft Outlook 64 bit. Điều này có nghĩa là Kaspersky Endpoint Security sẽ không quét các tập tin MS Outlook (tập tin PST và OST) nếu phiên bản 64 bit của MS Outlook được cài đặt trên máy tính, ngay cả khi bạn thêm [thư vào trong phạm vi quét](#).
- Trong Kaspersky Security Center, khi chuyển từ sử dụng Kaspersky Security Network Toàn cầu sang sử dụng một Kaspersky Security Network Riêng hoặc ngược lại, [tùy chọn tham gia Kaspersky Security Network sẽ bị tắt](#) trong chính sách của sản phẩm cụ thể. Sau khi chuyển đổi, hãy đọc kỹ văn bản của Tuyên bố Kaspersky Security Network và xác nhận sự đồng ý của bạn để tham gia vào KSN. Bạn có thể đọc nội dung của Tuyên bố trong giao diện ứng dụng hoặc khi chỉnh sửa chính sách sản phẩm.

- Trong quá trình quét lại đối tượng độc hại đã bị phần mềm của bên thứ ba chặn, người dùng không được thông báo khi phát hiện lại mối đe dọa. Sự kiện phát hiện lại mối đe dọa được hiển thị trong báo cáo ứng dụng và trong báo cáo Kaspersky Security Center.
- Không thể cài đặt thành phần [Endpoint Sensor](#) trong Microsoft Windows Server 2008.
- Báo cáo của Kaspersky Security Center về mã hóa thiết bị sẽ không bao gồm thông tin về các thiết bị đã được mã hóa bằng Microsoft BitLocker trên nền máy chủ hoặc trên các máy trạm không cài đặt thành phần Kiểm soát thiết bị.
- Không thể bật hiển thị tất cả các mục báo cáo trong Bảng điều khiển web Kaspersky Security Center. Trong Bảng điều khiển web, bạn chỉ có thể thay đổi số lượng mục được hiển thị trong báo cáo. Theo mặc định, Bảng điều khiển web Kaspersky Security Center sẽ hiển thị 1000 mục báo cáo. Bạn có thể cho phép hiển thị tất cả các mục báo cáo trong Bảng điều khiển quản trị (MMC).
- Không thể đặt giá trị hiển thị nhiều hơn 1000 mục báo cáo trong Bảng điều khiển Kaspersky Security Center. Nếu bạn đặt giá trị cao hơn 1000, Bảng điều khiển Kaspersky Security Center sẽ chỉ hiển thị 1000 mục báo cáo.
- Khi sử dụng cây cấp bậc chính sách, bạn có thể truy cập thiết lập của mục Mã hóa ổ đĩa di động trong chính sách con để chỉnh sửa nếu chính sách cha cấm sửa đổi các cài thiết lập.
- Bạn phải bật Audit Logon trong thiết lập hệ điều hành để đảm bảo hoạt động chính xác của các [loại trừ nhằm bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài](#).
- Nếu [bảo vệ thư mục chia sẻ được bật](#), Kaspersky Endpoint Security cho Windows sẽ giám sát nỗ lực mã hóa các thư mục được chia sẻ cho mỗi phiên truy cập từ xa đã được khởi chạy trước khi khởi động Kaspersky Endpoint Security cho Windows, kể cả nếu máy tính nơi bắt nguồn phiên truy cập từ xa được thêm vào các loại trừ. Nếu bạn không muốn Kaspersky Endpoint Security cho Windows giám sát nỗ lực mã hóa các thư mục được chia sẻ cho các phiên truy cập từ xa được khởi chạy từ một máy tính đã được thêm vào loại trừ và được khởi chạy trước khi khởi động Kaspersky Endpoint Security cho Windows, hãy chấm dứt và tái lập phiên truy cập từ xa hoặc khởi động lại máy tính đã cài đặt Kaspersky Endpoint Security cho Windows.
- Nếu [tác vụ cập nhật được chạy với quyền của một tài khoản người dùng cụ thể](#), các bản vá sản phẩm sẽ không được tải xuống khi cập nhật từ nguồn yêu cầu ủy quyền.
- Ứng dụng có thể không khởi động được do hệ thống không đủ hiệu năng. Để giải quyết sự cố này, hãy sử dụng tùy chọn Ready Boot hoặc tăng thời gian chờ của hệ điều hành để khởi động dịch vụ.
- Ứng dụng không thể hoạt động ở chế độ Safe Mode.
- Để đảm bảo rằng Kaspersky Endpoint Security cho Windows phiên bản 11.5.0 và 11.6.0 có thể hoạt động đúng với phần mềm Cisco AnyConnect, bạn phải cài đặt Mô-đun Tuân thủ phiên bản 4.3.183.2048 trở lên. Hãy tìm hiểu thêm về khả năng tương thích với Cisco Identity Services Engine trong [tài liệu của Cisco](#).
- Chúng tôi không thể đảm bảo rằng Audio Control sẽ hoạt động trước lần khởi động lại đầu tiên, sau khi cài đặt ứng dụng.
- Trong Bảng điều khiển quản trị (MMC), trong thiết lập Phòng chống xâm nhập trong cửa sổ dùng để cấu hình quyền ứng dụng, nút **Xóa** sẽ không khả dụng. Bạn có thể xóa ứng dụng khỏi nhóm tin tưởng thông qua menu ngữ cảnh của ứng dụng.
- Trong giao diện cục bộ của ứng dụng, trong thiết lập Phòng chống xâm nhập, các quyền của ứng dụng và tài nguyên được bảo vệ sẽ không khả dụng để xem nếu máy tính được quản lý bởi một chính sách. Chức năng cuộn, tìm kiếm, lọc và các chức năng điều khiển khác của cửa sổ không

khả dụng. Bạn có thể xem quyền của ứng dụng trong thuộc tính chính sách trong Bảng điều khiển Kaspersky Security Center.

- Khi các tập tin theo dõi luân phiên được bật, không có dấu vết nào được tạo cho thành phần AMSI và tiện ích của Outlook.
- Không thể thu thập dấu vết hiệu năng theo cách thủ công trong Windows Server 2008.
- Dấu vết hiệu năng cho loại dấu vết "Khởi động lại" không được hỗ trợ.
- Ghi nhật ký kết xuất không được hỗ trợ cho các tiến trình pico.
- Tác vụ kiểm tra tính khả dụng của KSN không còn được hỗ trợ.
- Tắt tùy chọn "Tắt quản lý dịch vụ hệ thống từ bên ngoài" sẽ không cho phép bạn dừng dịch vụ của ứng dụng đã được cài đặt với tham số AMPPL=1 (theo mặc định, giá trị tham số được đặt thành 1 kể từ phiên bản hệ điều hành Windows 10RS2). Tham số AMPPL với giá trị 1 cho phép sử dụng công nghệ Tiến trình Bảo vệ cho dịch vụ sản phẩm.
- Để chạy tác vụ quét tùy chỉnh thư mục, người dùng bắt đầu tác vụ quét tùy chỉnh phải có quyền đọc các thuộc tính của thư mục này. Nếu không, người dùng đó sẽ không thể thực hiện tác vụ quét thư mục tùy chỉnh và sẽ kết thúc kèm theo lỗi.
- Khi quy tắc quét được định nghĩa trong chính sách chứa một đường dẫn không có ký tự \ ở cuối, ví dụ: C:\folder1\folder2 thì tác vụ quét sẽ được chạy cho đường dẫn C:\folder1\.
- Khi nâng cấp ứng dụng từ phiên bản 11.1.0 lên 11.9.0, thiết lập Bảo vệ AMSI sẽ được đặt lại về giá trị mặc định của chúng.
- Nếu bạn đang sử dụng các chính sách hạn chế phần mềm (SRP) thì máy tính có thể không nạp thành công (màn hình đen). Bạn nên thay đổi thiết lập SRP như sau: đặt giá trị **Tất cả các tập tin phần mềm ngoại trừ các thư viện (như DLL)** cho tham số **Áp dụng các chính sách hạn chế phần mềm cho các đối tượng sau** và thêm quy tắc với mức độ bảo mật **Không hạn chế** cho đường dẫn đến tập tin của ứng dụng (C:\Program Files\Common Files\Kaspersky Lab và C:\Program Files\Kaspersky Lab). Để biết chi tiết về việc sử dụng SRP, hãy tham khảo [tài liệu của Microsoft](#).
- Nếu máy tính thuộc một miền trong Windows Group Policy Object (GPO) với tham số DriverLoadPolicy được đặt thành 8 (chỉ Tốt), khởi động lại máy tính được cài đặt Kaspersky Endpoint Security sẽ gây ra BSOD. Để ngăn lỗi này, tham số Early Launch Antimalware (ELAM) trong Group Policy phải được đặt thành 1 (Tốt và không xác định). Thiết lập ELAM nằm trong chính sách trong mục: **Computer Configuration** → **Administrative Templates** → **System** → **Early Launch Antimalware**.
- Không hỗ trợ quản lý thiết lập tiện ích của Outlook qua API Rest.
- Không thể chuyển thiết lập chạy tác vụ cho một người dùng cụ thể giữa các thiết bị thông qua tập tin cấu hình. Sau khi thiết lập được áp dụng từ tập tin cấu hình, hãy chỉ định thủ công tên người dùng và mật khẩu.
- Sau khi cài đặt bản cập nhật, tác vụ kiểm tra tính toàn vẹn không hoạt động cho đến khi hệ thống được khởi động lại để áp dụng bản cập nhật.
- Khi cấp độ truy vết luân phiên được thay đổi thông qua tiện ích chẩn đoán từ xa, Kaspersky Endpoint Security cho Windows sẽ hiển thị sai giá trị trống cho cấp độ dấu vết. Tuy nhiên, các tập tin dấu vết được ghi theo đúng cấp độ dấu vết. Khi cấp độ truy vết luân phiên được thay đổi thông qua giao diện cục bộ của ứng dụng, cấp độ dấu vết được sửa đổi chính xác nhưng tiện ích

chẩn đoán từ xa hiển thị đúng cấp độ dấu vết được tiện ích định nghĩa lần cuối. Điều này có thể khiến quản trị viên không có thông tin cập nhật về cấp độ dấu vết hiện tại và thông tin liên quan có thể không có trong dấu vết nếu người dùng thay đổi cấp độ truy vết theo cách thủ công trong giao diện cục bộ của ứng dụng.

- Trong giao diện cục bộ, Thiết lập bảo vệ bằng mật khẩu không cho phép thay đổi tên của tài khoản quản trị viên (KLAdmin theo mặc định). Để thay đổi tên của tài khoản quản trị viên, bạn cần tắt Bảo vệ bằng mật khẩu, sau đó bật Bảo vệ bằng mật khẩu và chỉ định tên mới của tài khoản quản trị viên.
- Bạn không thể quét một đối tượng bị cách ly do kết quả của tác vụ [Di chuyển tập tin đến Khu vực cách ly](#).
- Kaspersky Endpoint Security không chạy các tác vụ [Quét IOC](#) trên ổ đĩa mạng nếu đường dẫn thư mục trong thuộc tính tác vụ bắt đầu bằng ký tự ổ đĩa. Kaspersky Endpoint Security chỉ hỗ trợ định dạng đường dẫn UNC cho các tác vụ [Quét IOC](#) trên ổ đĩa mạng. Ví dụ: \\server\shared_folder.
- [Quá trình nhập tập tin cấu hình ứng dụng](#) sẽ kết thúc bằng một lỗi nếu thiết lập [tích hợp với Kaspersky Sandbox](#) được bật trong tập tin cấu hình. Hãy tắt Kaspersky Sandbox trước khi xuất thiết lập ứng dụng. Sau đó thực hiện quy trình xuất/nhập. Sau khi nhập tập tin cấu hình, hãy bật Kaspersky Sandbox.
- Khi phát hiện một dấu hiệu về sự xâm nhập trong khi chạy tác vụ [Quét IOC](#), ứng dụng chỉ cách ly một tập tin cho từ FileItem. Không hỗ trợ cách ly một tập tin cho các từ khác.
- Không thể cách lý một Luồng dữ liệu thay thế (ADS) lớn hơn 4 MB. Kaspersky Endpoint Security sẽ bỏ qua bất kỳ ADS nào lớn như vậy mà không thông báo cho người dùng.
- Bắt buộc phải có tiện ích web Kaspersky Endpoint Security cho Windows 11.7.0 trở lên để quản lý thông tin chi tiết về cảnh báo. Cần thông tin chi tiết về cảnh báo khi làm việc với các giải pháp [Endpoint Detection and Response](#) (EDR Optimum và EDR Expert). Chi tiết về phát hiện chỉ có trong Bảng điều khiển web Kaspersky Security Center và Bảng điều khiển đám mây Kaspersky Security Center.
- Ứng dụng Kaspersky Endpoint Security khi được cài đặt trên máy chủ Windows Server 2019 sẽ không tương thích với Docker. Triển khai các bộ chứa Docker trên máy tính có Kaspersky Endpoint Security sẽ gây lỗi sập hệ thống (BSOD).
- Khả năng tương thích của phần mềm Kaspersky Endpoint Security và Secret Net Studio bị hạn chế:
 - Ứng dụng Kaspersky Endpoint Security không tương thích với thành phần Chống virus của phần mềm Secret Net Studio.
Không thể cài đặt ứng dụng trên máy tính có triển khai Secret Net Studio với thành phần Chống virus. Để tạo khả năng tương tác, bạn phải gỡ bỏ thành phần Chống virus khỏi Secret Net Studio.
 - Secret Net Studio không tương thích với thành phần Mã hóa mức độ tập tin (FLE) của Kaspersky Endpoint Security.
Khi bạn cài đặt Kaspersky Endpoint Security với thành phần Mã hóa mức độ tập tin (FLE), Secret Net Studio có thể hoạt động kèm lỗi. Để đảm bảo khả năng tương tác, bạn phải gỡ bỏ thành phần Mã hóa mức độ tập tin (FLE) khỏi Kaspersky Endpoint Security.
- Chuyển cấu hình [KES+KEA] sang cấu hình [KES+built-in agent] có thể hoàn tất với lỗi gỡ bỏ ứng dụng Kaspersky Endpoint Agent. Lỗi gỡ bỏ ứng dụng được sửa trong phiên bản mới nhất của Kaspersky Endpoint Agent. Để gỡ bỏ Kaspersky Endpoint Agent, hãy khởi động lại máy tính và tạo một tác vụ gỡ bỏ ứng dụng.

Thuật ngữ

Authentication Agent

Giao diện cho phép bạn hoàn tất xác thực để truy cập các ổ cứng được mã hóa và nạp hệ điều hành sau khi ổ cứng khởi động đã được mã hóa.

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.

Chứng nhận giấy phép

Một tài liệu mà Kaspersky chuyển đến người dùng cùng với tập tin khóa hoặc mã kích hoạt. Nó chứa thông tin về giấy phép được cấp cho người dùng.

Cơ sở dữ liệu diệt virus

Cơ sở dữ liệu chứa thông tin về các mối đe dọa về bảo mật máy tính mà Kaspersky biết được từ ngày phát hành cơ sở dữ liệu diệt virus. Các mã nhận diện trong cơ sở dữ liệu diệt 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. Cơ sở dữ liệu được cập nhật thường xuyên và được kèm theo gói phân phối ứng dụng Kaspersky.

Cơ sở dữ liệu về các địa chỉ web lừa đảo

Một danh sách các địa chỉ 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.

Đại diện

Đại diện một tên tập tin và phần mở rộng bằng ký tự đại diện.

Các tên đại diện tập tin có thể chứa bất kỳ ký tự nào được cho phép trong tên tập tin, bao gồm các ký tự đại diện:

- Ký tự * (hoa thị) thay thế bất kỳ nhóm ký tự nào bộ ký tự, ngoại trừ các ký tự \ và / (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ, ký tự đại diện C:**.txt sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng TXT nằm trong các thư mục trên ổ C:, nhưng không phải trong các thư mục con.
- Hai ký tự * liên tiếp thay thế bất kỳ nhóm ký tự nào (bao gồm nhóm rỗng) trong tên tập tin hoặc thư mục, bao gồm các ký tự \ và / (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ, ký tự đại diện C:\Folder***.txt sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng TXT nằm trong thư mục được đặt tên là Folder và các thư mục con. Một đại diện phải có ít nhất một cặp lồng ghép. C:***.txt không phải là một đại diện hợp lệ. Đại diện ** chỉ khả dụng để tạo các mục loại trừ quét.
- Ký tự ? (dấu hỏi) thay thế bất kỳ ký tự đơn nào, ngoại trừ các ký tự \ và / (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ: đại diện C:\Folder\???.txt sẽ bao gồm các đường dẫn đến tất cả các tập tin có trong thư mục Folder có phần mở rộng TXT và tên có ba ký tự.

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 trừ thông tin đăng nhập người dùng, 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).

Liên quan đến hoạt động của các thành phần bảo vệ, 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.

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 chỉ

Trung tâm chứng chỉ đã cấp chứng chỉ.

IOC

Dấu hiệu về sự xâm nhập là Một tập hợp dữ liệu về một đối tượng độc hại hoặc hoạt động độc hại.

Khóa bổ sung

Một khóa chứng chỉ quyền sử dụng ứng dụng nhưng hiện không được sử dụng.

Khóa hiện hoạt

Một khóa hiện đang được sử dụng bởi ứng dụng.

Khử mã độc

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.

Mô-đun Nền tảng Tin tưởng

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 Tin tưởng 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.

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). Đây là thành phần phổ biến trên tất cả các ứng dụng Kaspersky chạy trên hệ điều hành Windows. Các phiên bản chuyên dụng của Network Agent được dành cho các ứng dụng chạy những hệ điều hành khác.

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 nhóm tác vụ cho mỗi ứng dụng được cài đặt trong nhóm này.

OpenIOC

Tiêu chuẩn mở về các mô tả Dấu hiệu về sự xâm nhập (IOC) dựa trên định dạng XML và bao gồm hơn 500 Dấu hiệu về sự xâm nhập khác nhau.

Phạm vi bảo vệ

Các đối tượng liên tục được quét bởi thành phần Bảo vệ mối đe dọa thiết yếu 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.

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 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 có thể gây 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 nguy cơ khá cao về việc xâm nhập của mã độc vào các tập tin như vậy.

Tập tin IOC

Một tập tin chứa một tập hợp các dấu hiệu về sự xâm nhập (IOC) mà ứng dụng cố gắng đối chiếu để đếm một lần phát hiện. Khả năng phát hiện có thể cao hơn nếu tìm thấy nhiều lượt đối chiếu trùng khớp tuyệt đối với nhiều tập tin IOC cho đối tượng nhờ sau khi có kết quả của tác vụ quét.

Tập tin nén

Một hoặc nhiều tập tin được đóng gói vào một tập tin nén duy nhất. Cần phải có một ứng dụng chuyên biệt được gọi là trình nén tập tin để đóng gói và mở gói dữ liệu.

Trình quản lý tập tin di động

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 sẵn có trên máy tính.

Phụ lục

Phần này chứa thông tin bổ sung cho phần thân của tài liệu.

Phụ lục 1. Thiết lập ứng dụng

Bạn có thể sử dụng [chính sách](#), [tác vụ](#) hoặc [giao diện ứng dụng](#) để cấu hình Kaspersky Endpoint Security. Thông tin chi tiết về các thành phần của ứng dụng được cung cấp trong phần tương ứng.

Bảo vệ mỗi đe dọa tập tin

Thành phần Bảo vệ mỗi đe dọa tập tin cho phép bạn ngăn chặn nguy cơ nhiễm mã độc cho hệ thống tập tin của máy tính. Theo mặc định, thành phần Bảo vệ mỗi đe dọa tập tin sẽ chạy thường trực trong RAM của máy tính. Thành phần này quét các tập tin trên tất cả các ổ đĩa của máy tính cũng như trên các ổ đĩa được kết nối. Thành phần này giúp bảo vệ máy tính với sự trợ giúp của cơ sở dữ liệu diệt virus, [dịch vụ đám mây của Kaspersky Security Network](#) và phân tích theo hành vi.

Thành phần này sẽ quét các tập tin được truy cập bởi người dùng hoặc ứng dụng. Nếu phát hiện tập tin độc hại, Kaspersky Endpoint Security sẽ chặn hoạt động của tập tin đó. Sau đó ứng dụng sẽ khử mã độc hoặc xóa tập tin độc hại, tùy thuộc vào thiết lập của thành phần Bảo vệ mỗi đe dọa tập tin.

Khi cố truy cập tập tin có toàn bộ nội dung được lưu trữ trên ổ lưu trữ đám mây OneDrive, Kaspersky Endpoint Security sẽ tải về và quét nội dung tập tin.

Cấu hình thành phần Bảo vệ mỗi đe dọa tập tin

Tham số	Mô tả
Mức độ bảo mật <i>(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)</i>	<p>Đối với thành phần Bảo vệ mỗi đe dọa tập tin, Kaspersky Endpoint Security có thể áp dụng các nhóm thiết lập khác nhau. Các nhóm thiết lập được lưu trữ trong ứng dụng được gọi là <i>mức độ bảo mật</i>:</p> <ul style="list-style-type: none">• Cao. Khi mức độ bảo mật tập tin này được chọn, thành phần Bảo vệ mỗi đe dọa tập tin sẽ áp dụng cấp kiểm soát chặt chẽ nhất cho tất cả các tập tin được mở, lưu lại và khởi động. Thành phần Bảo vệ mỗi đe dọa tập tin quét tất cả các loại tập tin trên tất cả các ổ cứng, ổ đĩa di động và ổ đĩa mạng của máy tính. Thành phần này cũng sẽ quét các tập nén, gói cài đặt và đối tượng OLE nhúng.• Khuyến dùng. Mức độ bảo mật tập tin này được khuyến nghị bởi các chuyên gia của Kaspersky Lab. Thành phần Bảo vệ mỗi đe dọa tập tin chỉ quét các định dạng tập tin cụ thể trên tất cả các ổ cứng, ổ đĩa di động và ổ đĩa mạng của máy tính, và các đối tượng OLE được nhúng. Thành phần Bảo vệ mỗi đe dọa tập tin sẽ không quét các tập nén hay gói cài đặt.• Thấp. Cấu hình bảo mật tập tin này đảm bảo tốc độ quét tối đa. Thành phần Bảo vệ mỗi đe dọa tập tin chỉ quét các tập tin có phần mở rộng cụ thể trên tất cả các ổ cứng, ổ đĩa di động và ổ đĩa mạng của máy tính. Thành phần Bảo vệ mỗi đe dọa tập tin sẽ không quét các tập tin hỗn hợp.
Loại tập tin	Tất cả tập tin. Nếu thiết lập này được bật, Kaspersky Endpoint Security sẽ kiểm tra tất cả các tập tin và không có ngoại lệ (tất cả định dạng và phần mở rộng).

<p>(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)</p>	<p>Quét các tập tin theo định dạng. Nếu thiết lập này được bật, Kaspersky Endpoint Security sẽ chỉ quét các tập tin có thể bị nhiễm virus. Trước khi quét một tập tin để tìm mã độc, đầu đề nội bộ của tập tin sẽ được phân tích để xác định định dạng của tập tin đó (ví dụ, .txt, .doc, hoặc .exe). Tác vụ quét cũng tìm kiếm các tập tin có đuôi mở rộng tập tin cụ thể.</p> <p>Quét các tập tin theo phần mở rộng. Nếu thiết lập này được bật, Kaspersky Endpoint Security sẽ chỉ quét các tập tin có thể bị nhiễm virus. Sau đó, định dạng tập tin sẽ được xác định dựa trên phần mở rộng của tập tin.</p>
<p>Phạm vi bảo vệ</p>	<p>Chứa các đối tượng được quét bởi thành phần Bảo vệ mối đe dọa tập tin. Một đối tượng quét có thể là ổ cứng, ổ đĩa di động, ổ đĩa mạng, thư mục, tập tin hoặc một đại diện tên tập tin.</p> <p>Theo mặc định, thành phần Bảo vệ mối đe dọa tập tin sẽ quét các tập tin được khởi chạy trên bất kỳ ổ cứng, ổ đĩa mạng hoặc ổ đĩa di động nào. Không thể thay đổi hoặc xóa phạm vi bảo vệ dành cho các đối tượng này. Bạn cũng có thể loại trừ một đối tượng (như các ổ đĩa di động) ra khỏi phạm vi quét.</p>
<p>Công nghệ máy học và phân tích dấu hiệu</p> <p>(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)</p>	<p>Phương thức máy học và phân tích dấu hiệu sử dụng cơ sở dữ liệu Kaspersky Endpoint Security chứa mô tả về các mối đe dọa đã biết và các cách để vô hiệu chúng. Tính năng bảo vệ sử dụng phương thức này cho mức độ bảo mật tối thiểu được chấp nhận.</p> <p>Dựa trên khuyến nghị của các chuyên gia Kaspersky, máy học và phân tích dấu hiệu luôn được bật.</p>
<p>Phân tích hành vi</p> <p>(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)</p>	<p>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.</p> <p>Khi quét các tập tin để tìm mã độc, trình phân tích theo hành vi sẽ thực thi các lệnh trong các tập tin thực thi. Số lượng các lệnh được thực thi bởi trình phân tích theo hành vi phụ thuộc vào cấp độ được chỉ định cho trình phân tích theo hành vi. Cấp độ Phân tích hành vi đảm bảo một sự cân bằng giữa việc quét kỹ lưỡng để tìm các mối đe dọa mới, tải lên tài nguyên hệ điều hành, và thời gian phân tích theo hành vi.</p>
<p>Hành động khi phát hiện mối đe dọa</p>	<p>Khử mã độc; xóa nếu không thể khử mã độc. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ tự động khử nhiễm tất cả các tập tin bị nhiễm virus được phát hiện. Nếu việc khử nhiễm thất bại, Kaspersky Endpoint Security sẽ xóa các tập tin đó.</p> <p>Khử mã độc; chặn nếu không thể khử mã độc. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ tự động khử nhiễm tất cả các tập tin bị nhiễm virus được phát hiện. Nếu không thể khử mã độc, Kaspersky Endpoint Security sẽ bổ sung thông tin về tập tin nhiễm mã độc được phát hiện vào danh sách các mối đe dọa đang hoạt động.</p> <p>Chặn. Nếu tùy chọn này được chọn, thành phần Bảo vệ mối đe dọa tập tin sẽ tự động chặn tất cả các tập tin bị nhiễm mà không cố gắng khử nhiễm chúng.</p>

	<p>Trước khi cố gắng khử mã độc hoặc xóa một tập tin bị nhiễm, Kaspersky Endpoint Security sẽ tạo một bản sao lưu của tập tin trong trường hợp bạn cần khôi phục tập tin hoặc nếu nó có thể khử mã độc tập tin trong tương lai.</p>
Chỉ quét các tập tin mới và bị thay đổi	Chỉ quét các tập tin mới và được thay đổi kể từ lần cuối cùng chúng được quét. Điều này giảm thời lượng của một lần quét. Chế độ này được áp dụng cho cả các tập tin đơn và tập tin hỗn hợp.
Quét tập tin nén	Quét định dạng ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE, và các định dạng tập tin nén khác. Kaspersky Endpoint Security quét các tập tin nén không chỉ theo phần mở rộng mà còn theo định dạng. Khi kiểm tra tập tin nén, ứng dụng sẽ thực hiện quy trình giải nén đệ quy. Điều này cho phép phát hiện các mối đe dọa bên trong tập tin nén nhiều cấp (tập tin nén bên trong tập tin nén).
Quét các gói phân phối	Hộp kiểm này bật/tắt tính năng quét các gói phân phối thuộc bên thứ ba.
Quét các tập tin có định dạng Microsoft Office	Quét các tập tin Microsoft Office (DOC, DOCX, XLS, PPT và đuôi mở rộng khác của Microsoft). Các tập tin định dạng Office cũng bao gồm các đối tượng OLE.
Không giải nén các tập tin phức hợp lớn	<p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ không quét các tập tin hỗn hợp nếu dung lượng của chúng vượt quá giá trị được quy định.</p> <p>Nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ quét các tập tin hỗn hợp thuộc mọi kích cỡ.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Kaspersky Endpoint Security sẽ quét các tập tin lớn được trích xuất từ tập tin nén bất kể hộp kiểm này có được chọn hay không.</p> </div>
Giải nén các tập tin hỗn hợp trong nền	<p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ cấp quyền truy cập vào các tập tin tổng hợp lớn hơn giá trị được chỉ định trước khi quét các tập tin này. Trong trường hợp này, Kaspersky Endpoint Security sẽ giải nén và quét các tập tin tổng hợp trong nền.</p> <p>Kaspersky Endpoint Security sẽ chỉ cấp quyền truy cập vào các tập tin tổng hợp nhỏ hơn giá trị này sau khi giải nén và quét các tập tin này.</p> <p>Nếu hộp kiểm này không được chọn, Kaspersky Endpoint Security sẽ chỉ cấp quyền truy cập vào các tập tin tổng hợp sau khi giải nén và quét các tập tin thuộc mọi kích thước.</p>
Chế độ quét	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Kaspersky Endpoint Security quét các tập tin được truy cập bởi người dùng, hệ điều hành hoặc ứng dụng đang chạy trong tài khoản của người dùng.</p> </div> <p>Chế độ thông minh. Ở chế độ này, Bảo vệ mối đe dọa tập tin sẽ quét một đối tượng dựa trên phân tích về hành động đã thực hiện trên đối tượng. Ví dụ: khi làm việc với tài liệu Microsoft Office, 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.</p>

<p><i>(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)</i></p>	<p>Khi truy cập và sửa đổi. Ở chế độ này, Bảo vệ mỗi đe dọa tập tin sẽ quét các đối tượng bất cứ khi nào các đối tượng đó được mở hoặc bị sửa đổi.</p> <p>Khi truy cập. Ở chế độ này, Bảo vệ mỗi đe dọa tập tin sẽ quét các đối tượng chỉ khi các đối tượng đó được mở.</p> <p>Khi thực thi. Ở chế độ này, Bảo vệ mỗi đe dọa tập tin sẽ chỉ quét đối tượng khi chúng được chạy.</p>
<p>Công nghệ iSwift</p> <p><i>(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)</i></p>	<p>Công nghệ này cho phép tăng tốc độ quét bằng cách loại trừ một số tập tin nhất định khỏi quá trình quét. Các tập tin được loại trừ khỏi quá trình quét bằng một thuật toán đặc biệt có tính đến ngày phát hành cơ sở dữ liệu Kaspersky Endpoint Security, ngày mà tập tin được quét lần cuối cùng và mọi thay đổi được thực hiện với thiết lập quét. Công nghệ iSwift được cải tiến từ công nghệ iChecker cho hệ thống tập tin NTFS.</p>
<p>Công nghệ iChecker</p> <p><i>(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)</i></p>	<p>Công nghệ này cho phép tăng tốc độ quét bằng cách loại trừ một số tập tin nhất định khỏi quá trình quét. Các tập tin được loại trừ khỏi quá trình quét bằng một thuật toán đặc biệt có tính đến ngày phát hành cơ sở dữ liệu Kaspersky Endpoint Security, ngày khi tập tin được quét lần cuối cùng và mọi thay đổi được thực hiện với thiết lập quét. Công nghệ iChecker có một số hạn chế: công nghệ này không hoạt động với tập tin lớn và chỉ áp dụng cho các tập tin có cấu trúc mà ứng dụng nhận dạng được (ví dụ như EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP và RAR).</p>
<p>Tạm dừng Bảo vệ mỗi đe dọa tập tin</p> <p><i>(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)</i></p>	<p>Điều này sẽ tạm thời và tự động tạm dừng hoạt động của Bảo vệ mỗi đe dọa tập tin tại thời điểm được chỉ định hoặc khi làm việc với các ứng dụng được chỉ định.</p>

Bảo vệ mỗi đe dọa web

Thành phần Bảo vệ mối đe dọa web ngăn các bản tải xuống tập tin độc hại từ mạng Internet và cũng chặn các website độc hại và lừa đảo. Thành phần này giúp bảo vệ máy tính với sự trợ giúp của cơ sở dữ liệu diệt virus, [dịch vụ đám mây của Kaspersky Security Network](#) và phân tích theo hành vi.

Kaspersky Endpoint Security sẽ quét lưu lượng HTTP, HTTPS và FTP. Kaspersky Endpoint Security sẽ quét các URL và địa chỉ IP. Bạn có thể [chỉ định các cổng mà Kaspersky Endpoint Security sẽ giám sát](#), hoặc chọn tất cả các cổng.

Để giám sát lưu lượng HTTPS, bạn cần [bật quét kết nối được mã hóa](#).

Khi người dùng cố gắng mở một website độc hại hoặc lừa đảo, Kaspersky Endpoint Security sẽ chặn truy cập và hiển thị cảnh báo (xem hình bên dưới).



Thông báo truy cập website bị từ chối

Cấu hình thành phần Bảo vệ mối đe dọa web

Tham số	Mô tả
Mức độ bảo mật (<i>chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security</i>)	<p>Đối với thành phần Bảo vệ mối đe dọa web, Kaspersky Endpoint Security có thể áp dụng các nhóm thiết lập khác nhau. Các nhóm thiết lập được lưu trữ trong ứng dụng được gọi là <i>mức độ bảo mật</i>:</p> <ul style="list-style-type: none">• Cao. Mức độ bảo mật mà theo đó thành phần Bảo vệ mối đe dọa web quét tối đa lưu lượng web mà máy tính tiếp nhận qua giao thức HTTP và FTP. Bảo vệ mối đe dọa web sẽ thực hiện quét chi tiết mọi đối tượng lưu lượng web, sử dụng toàn bộ các cơ sở dữ liệu ứng dụng, và thực hiện phân tích theo hành vi cấp sâu nhất.• Khuyến dùng. Mức độ bảo mật email mang đến sự cân bằng tối ưu giữa hiệu năng của Kaspersky Endpoint Security và bảo mật lưu lượng web. Thành phần Bảo vệ mối đe dọa web thực hiện phân tích theo hành vi ở cấp quét vừa. Mức độ bảo mật lưu lượng web này được khuyến khích bởi các chuyên gia Kaspersky.• Thấp. Thiết lập của mức độ bảo mật lưu lượng web này đảm bảo tốc độ quét lưu lượng web tối đa. Thành phần Bảo vệ mối đe dọa web thực hiện phân tích theo hành vi ở cấp quét vừa.
Hành động khi phát hiện mối đe dọa	Chặn tải về. Nếu mục này được chọn và một đối tượng bị nhiễm mã độc được phát hiện trong lưu lượng web, thành phần Bảo vệ mối đe dọa web sẽ chặn truy cập vào đối tượng đó và hiển thị thông báo trong trình duyệt.

	<p>Thông báo. Nếu mục này được chọn và một đối tượng bị nhiễm mã độc được phát hiện trong lưu lượng web, Kaspersky Endpoint Security cho phép đối tượng này được tải xuống máy tính nhưng sẽ thêm thông tin về đối tượng bị nhiễm mã độc vào danh sách các mối đe dọa đang hoạt động.</p>
<p>Kiểm tra địa chỉ web bằng cách đối chiếu với cơ sở dữ liệu địa chỉ web độc hại <i>(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)</i></p>	<p>Quét các liên kết để xác định xem chúng có được đưa vào trong cơ sở dữ liệu của các địa chỉ web độc hại hay không để cho phép bạn theo dõi các website đã được thêm vào danh sách không được phép. Cơ sở dữ liệu các địa chỉ web độc hại được duy trì bởi Kaspersky, được bao gồm trong gói cài đặt ứng dụng và cập nhật trong quá trình cập nhật cơ sở dữ liệu của Kaspersky Endpoint Security.</p>
<p>Sử dụng phân tích hành vi <i>(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)</i></p>	<p>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.</p> <p>Khi lưu lượng web được quét virus và các ứng dụng khác có mối đe dọa, trình phân tích theo hành vi sẽ thực hiện các lệnh trong các tập tin thực thi. Số lượng các lệnh được thực thi bởi trình phân tích theo hành vi phụ thuộc vào cấp độ được chỉ định cho trình phân tích theo hành vi. Cấp độ Phân tích hành vi đảm bảo một sự cân bằng giữa việc quét kỹ lưỡng để tìm các mối đe dọa mới, tải lên tài nguyên hệ điều hành, và thời gian phân tích theo hành vi.</p>
<p>Kiểm tra địa chỉ web bằng cách đối chiếu với cơ sở dữ liệu địa chỉ web lừa đảo <i>(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)</i></p>	<p>Cơ sở dữ liệu địa chỉ web lừa đảo bao gồm các địa chỉ website đã biết, thường được sử dụng để tạo các cuộc tấn công lừa đảo. Kaspersky bổ sung cho cơ sở dữ liệu về các liên kết lừa đảo này bằng các địa chỉ thu được từ tổ chức quốc tế có tên gọi là Tổ chức toàn cầu về chống lừa đảo trên mạng. Cơ sở dữ liệu các địa chỉ lừa đảo được bao gồm trong gói cài đặt ứng dụng và được bổ sung trong quá trình cập nhật cơ sở dữ liệu của Kaspersky Endpoint Security.</p>
<p>Không quét lưu lượng web từ các địa chỉ web được tin tưởng</p>	<p>Nếu hộp kiểm này được chọn, thành phần Bảo vệ mối đe dọa web sẽ không quét nội dung của các trang web hoặc website có địa chỉ nằm trong danh sách các địa chỉ web được tin tưởng. Bạn có thể thêm cả địa chỉ cụ thể và địa chỉ đại diện của một trang web / website vào danh sách các địa chỉ web được tin tưởng.</p>

Bảo vệ mối đe dọa thư điện tử

Thành phần Bảo vệ mối đe dọa thư điện tử sẽ quét các tập tin đính kèm của email đến và đi để phát hiện virus và các mối đe dọa khác. Thành phần này giúp bảo vệ máy tính với sự trợ giúp của cơ sở dữ liệu diệt virus, [dịch vụ đám mây của Kaspersky Security Network](#) và phân tích theo hành vi.

Bảo vệ mối đe dọa thư điện tử có thể quét cả thư đến và thư đi. Ứng dụng này hỗ trợ POP3, SMTP, IMAP và NNTP trong các ứng dụng thư điện tử sau:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Microsoft Outlook Express
- Windows Mail

Bảo vệ mối đe dọa thư điện tử không hỗ trợ các giao thức và ứng dụng thư điện tử khác.

Bảo vệ mối đe dọa thư điện tử có thể không phải lúc nào cũng có được quyền truy cập *cấp độ giao thức* vào thư (ví dụ: khi sử dụng giải pháp Microsoft Exchange). Do đó, Bảo vệ mối đe dọa thư điện tử có một [phần mở rộng cho Microsoft Office Outlook](#). Phần mở rộng này cho phép quét thư ở *cấp độ của ứng dụng thư điện tử*. Phần mở rộng Bảo vệ mối đe dọa thư điện tử hỗ trợ hoạt động với Outlook 2010, 2013, 2016 và 2019.

Thành phần Bảo vệ mối đe dọa thư điện tử không quét thư nếu ứng dụng thư khách được mở trong trình duyệt.

Khi phát hiện tập tin độc hại trong tập tin đính kèm, Kaspersky Endpoint Security sẽ đổi tên chủ đề thư như sau: [Việc xử lý thư cần sự tham gia của bạn] <chủ đề thư> hoặc [Thư đã được xử lý] <chủ đề thư>.

Cấu hình thành phần Bảo vệ mối đe dọa thư điện tử

Tham số	Mô tả
Mức độ bảo mật (<i>chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security</i>)	<p>Đối với thành phần Bảo vệ mối đe dọa thư điện tử, Kaspersky Endpoint Security sẽ áp dụng các nhóm thiết lập khác nhau. Các nhóm thiết lập được lưu trữ trong ứng dụng được gọi là <i>mức độ bảo mật</i>:</p> <ul style="list-style-type: none">• Cao. Khi mức độ bảo mật email này được chọn, thành phần Bảo vệ mối đe dọa thư điện tử sẽ quét kỹ các email. Thành phần Bảo vệ mối đe dọa thư điện tử sẽ quét các email đến và đi, đồng thời tiến hành phân tích theo hành vi mức độ sâu. Mức độ bảo mật thư điện tử Cao được khuyến nghị cho các môi trường có nguy cơ cao. Một ví dụ về một môi trường như vậy là một kết nối đến một dịch vụ thư điện tử miễn phí từ một mạng gia đình mà không được bảo vệ bởi bảo vệ thư điện tử.• Khuyến dùng. Mức độ bảo mật email mang đến sự cân bằng tối ưu giữa hiệu năng của Kaspersky Endpoint Security và bảo mật email. Thành phần Bảo vệ mối đe dọa thư điện tử sẽ quét các email đến và đi, đồng thời tiến hành phân tích theo hành vi mức độ trung bình. Mức độ bảo mật lưu lượng email này được khuyến khích bởi các chuyên gia Kaspersky.• Thấp. Khi mức độ bảo mật email này được chọn, thành phần Bảo vệ mối đe dọa thư điện tử sẽ chỉ quét các email đến, thực hiện phân tích theo hành vi nhanh và không quét các tập tin đính kèm email. Ở mức độ bảo mật email này, thành phần Bảo vệ mối đe dọa thư điện tử sẽ quét tất cả email ở tốc độ tối đa và sử dụng mức tài nguyên hệ điều hành tối thiểu. Mức độ bảo mật email Thấp được khuyến nghị sử dụng ở các môi trường bảo mật tốt. Một ví dụ về môi trường như vậy có thể là một mạng LAN doanh nghiệp có hệ thống bảo mật email tập trung.

<p>Hành động khi phát hiện mối đe dọa</p>	<p>Khử mã độc; xóa nếu không thể khử mã độc. Khi phát hiện một đối tượng bị nhiễm mã độc trong một thư được gửi đến hoặc thư được gửi đi, Kaspersky Endpoint Security sẽ cố gắng khử mã độc đối tượng được phát hiện. Người dùng có thể truy cập thư có tập tin đính kèm an toàn. Nếu không thể khử mã độc đối tượng, Kaspersky Endpoint Security sẽ xóa đối tượng bị nhiễm. Kaspersky Endpoint Security sẽ thêm thông tin về hành động được thực hiện vào chủ đề thư: [Thư đã được xử lý] <chủ đề thư>.</p> <p>Khử mã độc; chặn nếu không thể khử mã độc. Khi phát hiện một đối tượng bị nhiễm mã độc trong một thư được gửi đến, Kaspersky Endpoint Security sẽ cố gắng khử mã độc đối tượng được phát hiện. Người dùng có thể truy cập thư có tập tin đính kèm an toàn. Nếu không thể khử mã độc đối tượng, Kaspersky Endpoint Security sẽ thêm cảnh báo vào chủ đề thư: [Việc xử lý thư cần sự tham gia của bạn] <chủ đề thư>. Người dùng có thể truy cập thư có tập tin đính kèm ban đầu. Khi phát hiện một đối tượng bị nhiễm mã độc trong một thư được gửi đi, Kaspersky Endpoint Security sẽ cố gắng khử mã độc đối tượng được phát hiện. Nếu không thể khử mã độc đối tượng, Kaspersky Endpoint Security sẽ chặn việc gửi thư và ứng dụng thư điện tử sẽ hiển thị lỗi.</p> <p>Chặn. Nếu phát hiện một đối tượng bị nhiễm mã độc trong thư được gửi đến, Kaspersky Endpoint Security sẽ thêm cảnh báo vào chủ đề thư: [Việc xử lý thư cần sự tham gia của bạn] <chủ đề thư>. Người dùng có thể truy cập thư có tập tin đính kèm ban đầu. Nếu phát hiện một đối tượng bị nhiễm mã độc trong thư được gửi đi, Kaspersky Endpoint Security sẽ chặn gửi thư và ứng dụng thư điện tử sẽ hiển thị lỗi.</p>
<p>Phạm vi bảo vệ</p> <p><i>(Chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)</i></p>	<p><i>Phạm vi bảo vệ</i> bao gồm các đối tượng được thành phần kiểm tra khi nó được chạy: tin nhắn đến và đi hoặc chỉ tin nhắn gửi đến.</p> <p>Để bảo vệ máy tính của mình, bạn chỉ cần quét các thư đến. Bạn có thể bật quét các thư đi để ngăn các tập tin bị nhiễm được gửi trong các tập tin nén. Bạn cũng có thể bật quét các thư đi nếu bạn muốn ngăn các tập tin ở các định dạng cụ thể được gửi, chẳng hạn như các tập tin âm thanh và video chẳng hạn.</p>
<p>Quét lưu lượng POP3, SMTP, NNTP, và IMAP</p>	<p>Hộp kiểm này bật / tắt hoạt động quét lưu lượng được truyền tải qua các giao thức POP3, SMTP, NNTP và IMAP của thành phần Bảo vệ mối đe dọa thư điện tử.</p>
<p>Kết nối phần mở rộng Microsoft Outlook</p>	<p>Nếu hộp kiểm này được chọn, tính năng quét các email được truyền tải qua giao thức POP3, SMTP, NNTP, IMAP sẽ được bật cho từ phía tiện ích mở rộng tích hợp vào Microsoft Outlook.</p> <p>Nếu thư điện tử được quét bằng phần mở rộng dành cho Microsoft Outlook, bạn nên sử dụng Chế độ Exchange đã lưu trong Bộ đệm ẩn. Để biết thêm chi tiết về Cached Exchange Mode và khuyến nghị về việc sử dụng của nó, vui lòng tham khảo Cơ sở tri thức của Microsoft.</p>
<p>Phân tích hành vi</p>	<p>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.</p>

<p>(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)</p>	<p>Khi quét các tập tin để tìm mã độc, trình phân tích theo hành vi sẽ thực thi các lệnh trong các tập tin thực thi. Số lượng các lệnh được thực thi bởi trình phân tích theo hành vi phụ thuộc vào cấp độ được chỉ định cho trình phân tích theo hành vi. Cấp độ Phân tích hành vi đảm bảo một sự cân bằng giữa việc quét kỹ lưỡng để tìm các mối đe dọa mới, tải lên tài nguyên hệ điều hành, và thời gian phân tích theo hành vi.</p>
<p>Quét các tập tin nén đính kèm</p>	<p>Quét định dạng ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE, và các định dạng tập tin nén khác. Kaspersky Endpoint Security quét các tập tin nén không chỉ theo phần mở rộng mà còn theo định dạng.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Nếu trong quá trình quét, Kaspersky Endpoint Security phát hiện mật khẩu cho một tập tin nén trong văn bản của tin nhắn, mật khẩu này sẽ được sử dụng để quét nội dung của tập tin nén để tìm các ứng dụng độc hại. Trong trường hợp này, mật khẩu không được lưu lại. Một tập tin nén được giải nén trong quá trình quét. Nếu xảy ra lỗi ứng dụng trong quá trình giải nén, bạn có thể xóa các tập tin đã giải nén được lưu vào đường dẫn sau theo cách thủ công: %systemroot%\temp. Tập tin có tiền tố PR.</p> </div>
<p>Quét các tập tin đính kèm có định dạng Microsoft Office</p>	<p>Quét các tập tin Microsoft Office (DOC, DOCX, XLS, PPT và đuôi mở rộng khác của Microsoft). Các tập tin định dạng Office cũng bao gồm các đối tượng OLE.</p>
<p>Không quét tập tin nén lớn hơn N MB</p>	<p>Nếu hộp kiểm này được chọn, thành phần Bảo vệ mối đe dọa thư điện tử sẽ loại trừ các tập tin đính kèm email khỏi tác vụ quét nếu kích cỡ của chúng vượt quá giá trị được quy định. Nếu hộp kiểm này bị xóa, thành phần Bảo vệ mối đe dọa thư điện tử sẽ quét các tập tin đính kèm email thuộc mọi kích cỡ.</p>
<p>Giới hạn thời gian kiểm tra các tập tin nén thành N giây</p>	<p>Nếu hộp kiểm này được chọn, thời gian phân bổ cho việc quét các tập tin đính kèm email sẽ bị hạn chế trong khoảng thời gian được quy định.</p>
<p>Lọc tập tin đính kèm</p>	<div style="border: 1px solid black; padding: 10px; margin-bottom: 10px;"> <p>Chức năng bộ lọc tập tin đính kèm không được áp dụng cho các email gửi đi.</p> </div> <p>Vô hiệu lọc. Nếu tùy chọn này được chọn, thành phần Bảo vệ mối đe dọa thư điện tử sẽ không lọc các tập tin được đính kèm email.</p> <p>Đổi tên tập tin nén đính kèm của loại đã chọn. Nếu tùy chọn này được chọn, Bảo vệ mối đe dọa thư điện tử sẽ thay thế ký tự cuối cùng của đuôi mở rộng được tìm thấy trong các tập tin đính kèm của các loại được chỉ định bằng ký tự gạch dưới (ví dụ: attachment.doc_). Vì vậy, để mở tập tin này, người dùng phải đổi tên tập tin.</p>

Xóa tập tin nén đính kèm của loại đã chọn. Nếu tùy chọn này được lựa chọn, thành phần Bảo vệ mỗi đe dọa thư điện tử sẽ xóa tập tin đính kèm thuộc loại được quy định khỏi email.

Trong danh sách tên đại diện tập tin, bạn có thể quy định các loại tập tin đính kèm để đổi tên hoặc xóa khỏi email.

Bảo vệ mỗi đe dọa mạng

Thành phần Bảo vệ mỗi đe dọa mạng sẽ quét lưu lượng mạng vào để phát hiện các hoạt động tương tự với các cuộc tấn công mạng. Khi Kaspersky Endpoint Security phát hiện một nỗ lực tấn công mạng vào máy tính của người dùng, ứng dụng sẽ chặn kết nối mạng với 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 Bảo vệ mỗi đe dọa mạng phát hiện sẽ được cập nhật trong [bản cập nhật cơ sở dữ liệu và mô-đun ứng dụng](#).

Cấu hình thành phần Bảo vệ mỗi đe dọa mạng

Tham số	Mô tả
Coi hoạt động quét cổng và làm nghẽn mạng là các cuộc tấn công	<p><i>Làm nghẽn mạng</i> là một cuộc tấn công vào tài nguyên mạng của một tổ chức (chẳng hạn như máy chủ web). Cuộc tấn công này bao gồm việc gửi một số lượng lớn các yêu cầu làm quá tải băng thông của tài nguyên mạng. Khi điều này xảy ra, người dùng không thể truy cập tài nguyên mạng của tổ chức.</p> <p>Tấn công <i>Quét cổng</i> bao gồm hoạt động quét các cổng UDP, cổng TCP và các dịch vụ mạng trên máy tính. Cuộc tấn công này cho phép kẻ tấn công xác định mức độ lỗ hổng bảo mật của máy tính trước khi tiến hành các kiểu tấn công mạng nguy hiểm hơn. Hoạt động Quét cổng cũng cho phép kẻ tấn công xác định hệ điều hành trên máy tính và lựa chọn các cuộc tấn công mạng thích hợp cho hệ điều hành này.</p> <p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ giám sát lưu lượng mạng để phát hiện các cuộc tấn công này. Nếu phát hiện một cuộc tấn công, ứng dụng sẽ thông báo cho người dùng và gửi sự kiện tương ứng đến Kaspersky Security Center. Ứng dụng sẽ cung cấp thông tin về máy tính tấn công, cần thiết cho các hành động ứng phó kịp thời với mỗi đe dọa.</p> <p>Bạn có thể vô hiệu hóa tính năng phát hiện các loại tấn công này trong trường hợp một số ứng dụng được phép của bạn thực hiện các hoạt động tiêu biểu cho các loại tấn công này. Điều này sẽ giúp tránh cảnh báo nhầm.</p>
Chặn các thiết bị tấn công cho N phút	<p>Nếu hộp kiểm này được chọn, thành phần Bảo vệ mỗi đe dọa mạng sẽ thêm máy tính tấn công vào danh sách chặn. Điều này có nghĩa là thành phần Bảo vệ mỗi đe dọa mạng sẽ chặn kết nối mạng từ máy tính tấn công sau nỗ lực tấn công mạng đầu tiên trong một khoảng thời gian được quy định. Lệnh chặn này sẽ tự động bảo vệ máy tính của người dùng chống lại tất cả các cuộc tấn công mạng có thể có trong tương lai từ cùng một địa chỉ. Thời gian tối thiểu mà máy tính tấn công phải cần trong danh sách chặn là một phút. Thời gian tối đa là 32768 phút.</p> <p>Bạn có thể xem danh sách chặn trong cửa sổ công cụ Giám sát mạng.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"><p>Kaspersky Endpoint Security sẽ xóa danh sách chặn khi ứng dụng được khởi chạy lại và khi thiết lập Bảo vệ mỗi đe dọa mạng bị thay đổi.</p></div>
Loại trừ	<p>Danh sách này chứa các địa chỉ IP mà Bảo vệ mỗi đe dọa mạng sẽ không chặn các cuộc tấn công mạng từ đó.</p>

	Ứng dụng không ghi lại thông tin về các cuộc tấn công mạng từ địa chỉ IP nằm trong danh sách loại trừ.
Chống giả mạo MAC	Một cuộc <i>tấn công giả mạo MAC</i> bao gồm hoạt động thay đổi địa chỉ MAC của một thiết bị mạng (card mạng). Do đó, kẻ tấn công có thể chuyển hướng dữ liệu được gửi đến một thiết bị sang thiết bị khác và chiếm quyền truy cập vào dữ liệu này. Kaspersky Endpoint Security cho phép bạn chặn các cuộc tấn công Giả mạo MAC và nhận thông báo về các cuộc tấn công.

Tường lửa

Tường lửa chặn các kết nối trái phép đến máy tính khi đang làm việc trên Internet hoặc mạng cục bộ. Tường lửa cũng kiểm soát hoạt động mạng của các ứng dụng trên máy tính. Điều này cho phép bạn bảo vệ mạng LAN công ty trước hành vi trộm danh tính và các cuộc tấn công khác. Thành phần này giúp bảo vệ máy tính với sự trợ giúp của cơ sở dữ liệu diệt virus, dịch vụ đám mây của Kaspersky Security Network và các *quy tắc mạng* được xác định trước.

Network Agent được sử dụng để tương tác với Kaspersky Security Center. Tường lửa sẽ tự động tạo quy tắc mạng cần thiết cho ứng dụng và Network Agent để làm việc. Kết quả là Tường lửa sẽ mở vài cổng trên máy tính. Việc cổng nào được mở phụ thuộc vào vai trò của máy tính (ví dụ: điểm phân phối). Để tìm hiểu thêm về các cổng sẽ được mở trên máy tính, hãy tham khảo [Trợ giúp của Kaspersky Security Center](#).

Quy tắc mạng

Bạn có thể cấu hình quy tắc mạng ở các cấp sau:

- *Những quy tắc cho gói tin mạng.* Các quy tắc gói tin mạng áp đặt hạn chế cho các gói tin mạng, bất kể ứng dụng 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. Kaspersky Endpoint Security đã xác định trước các quy tắc gói tin mạng bằng các quyền được khuyến nghị bởi các chuyên gia của Kaspersky.
- *Quy tắc ứng dụng mạng.* 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.

Quyền truy cập được kiểm soát của ứng dụng vào tài nguyên hệ điều hành, tiến trình và dữ liệu cá nhân được cung cấp bởi [thành phần Phòng chống xâm nhập máy chủ](#) bằng cách sử dụng *các quyền của ứng dụng*.

Trong lần khởi động đầu tiên của ứng dụng, Tường lửa sẽ thực hiện các hành động sau:

1. Kiểm tra tính bảo mật của ứng dụng bằng cách cơ sở dữ liệu diệt virus đã tải xuống.
2. Kiểm tra tính bảo mật của ứng dụng trong Kaspersky Security Network.
Bạn nên [tham gia vào Kaspersky Security Network](#) để giúp Tường lửa hoạt động hiệu quả hơn.
3. Đưa ứng dụng vào một trong các *nhóm tin tưởng*: Tin tưởng, Giới hạn mức Thấp, Giới hạn mức Cao, Không tin tưởng.

Một [nhóm tin tưởng quy định các quyền](#) được Kaspersky Endpoint Security áp dụng khi kiểm soát hoạt động của các ứng dụng trong nhóm đó. Kaspersky Endpoint Security sẽ đặt ứng dụng vào một nhóm tin tưởng tùy thuộc vào mức độ nguy hiểm mà ứng dụng này có thể gây ra cho máy tính.

Kaspersky Endpoint Security sẽ đặt ứng dụng vào nhóm tin tưởng cho các thành phần Tường lửa và Phòng chống xâm nhập máy chủ. Bạn chỉ không thể thay đổi nhóm tin tưởng cho Tường lửa hoặc Phòng chống xâm nhập máy chủ.

Nếu bạn từ chối tham gia vào KSN hoặc không có mạng, Kaspersky Endpoint Security sẽ đặt ứng dụng vào một nhóm tin tưởng tùy thuộc vào [thiết lập của thành phần Phòng chống xâm nhập máy chủ](#). Sau khi nhận được danh tiếng của ứng dụng từ KSN, nhóm tin tưởng có thể được thay đổi tự động.

4. Nó sẽ chặn hoạt động mạng của các ứng dụng, tùy thuộc vào nhóm tin tưởng. Ví dụ: các ứng dụng trong nhóm tin tưởng Giới hạn mức Cao không được phép sử dụng bất kỳ kết nối mạng nào.

Khi ứng dụng được khởi chạy vào lần tới, Kaspersky Endpoint Security sẽ kiểm tra tính toàn vẹn của ứng dụng. Nếu ứng dụng không bị thay đổi, thành phần này sử dụng các quy tắc mạng hiện tại cho ứng dụng. Nếu ứng dụng đã bị sửa đổi, Kaspersky Endpoint Security sẽ phân tích ứng dụng đó như khi ứng dụng đó được khởi chạy lần đầu tiên.

Các mức ưu tiên của quy tắc mạng

Mỗi quy tắc có một mức ưu tiên. Quy tắc có vị trí càng cao trên danh sách thì càng có mức ưu tiên cao. Nếu hoạt động mạng được thêm vào một vài quy tắc, Tường lửa sẽ điều chỉnh hoạt động mạng theo quy tắc có mức ưu tiên cao nhất.

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 hành 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.

Các trạng thái kết nối mạng

Tường lửa cho phép bạn kiểm soát hoạt động mạng tùy thuộc vào trạng thái của kết nối mạng. Kaspersky Endpoint Security sẽ nhận trạng thái kết nối mạng từ hệ điều hành của máy tính. Trạng thái của kết nối mạng trong hệ điều hành được người dùng đặt khi thiết lập kết nối. Bạn có thể [thay đổi trạng thái của kết nối mạng trong mục thiết lập của Kaspersky Endpoint Security](#). Tường lửa sẽ giám sát hoạt động mạng tùy thuộc vào trạng thái mạng trong mục thiết lập của Kaspersky Endpoint Security chứ không phải trong hệ điều hành.

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

- **Mạng công cộng.** Mạng không được bảo vệ bởi các ứng dụng diệt virus, tường lửa hoặc bộ lọc (như mạng Wi-Fi trong quán cà phê). 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 cục bộ.** Mạng dành cho người dùng có quyền truy cập hạn chế vào các tập tin và máy in trên máy tính này (ví dụ như mạng LAN công ty hoặc mạng gia đình).
- **Mạng tin tưởng.** Mạng an toàn trong đó máy tính không bị nguy cơ tấn công hay các nỗ lực truy cập dữ liệu trái phép. Tường lửa cho phép mọi hoạt động mạng trong các mạng có trạng thái này.

Cấu hình thành phần Tường lửa

Tham số	Mô tả
Những quy tắc cho gói tin mạng	<p>Bảng với một danh sách các quy tắc gói tin mạng. Các quy tắc gói tin mạng áp đặt hạn chế cho các gói tin mạng, bất kể ứng dụng 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.</p> <p>Bảng này sẽ liệt kê các quy tắc gói tin mạng được thiết lập sẵn và được khuyến nghị bởi Kaspersky để bảo vệ tối ưu lưu lượng mạng trên các máy tính chạy hệ điều hành Microsoft Windows.</p> <p>Tường lửa đặt mức độ ưu tiên thực thi cho mỗi quy tắc gói tin mạng. Tường lửa sẽ xử lý các quy tắc gói tin mạng theo thứ tự xuất hiện trong danh sách quy tắc gói tin mạng, từ trên xuống dưới. Tường lửa xác định quy tắc gói tin mạng trên cùng phù hợp cho kết nối mạng và áp dụng nó bằng cách cho phép hoặc chặn hoạt động mạng. Khi đó, tường lửa sẽ bỏ qua tất cả các quy tắc gói tin mạng sau đó dành cho kết nối mạng cụ thể.</p> <p>Các quy tắc gói tin mạng có ưu tiên cao hơn so với các quy tắc mạng cho ứng dụng.</p>
Kết nối mạng	<p>Bảng này chứa thông tin về các kết nối mạng được Tường lửa phát hiện trên máy tính.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Trạng thái <i>Mạng công cộng</i> sẽ được gán cho Internet ở chế độ mặc định. Bạn không thể thay đổi trạng thái của Internet.</p> </div>
Quy tắc mạng	<p>Ứng dụng</p> <p>Bảng ứng dụng được kiểm soát bởi thành phần Tường lửa. Các ứng dụng được gán vào các nhóm tin tưởng. Một nhóm tin tưởng xác định các quyền được sử dụng bởi Kaspersky Endpoint Security khi kiểm soát hoạt động mạng của các ứng dụng.</p> <p>Bạn có thể chọn một ứng dụng trong một danh sách duy nhất của tất cả các ứng dụng được cài đặt trên máy tính chịu ảnh hưởng của chính sách và thêm ứng dụng đó vào nhóm tin tưởng.</p>

Quy tắc mạng

Bảng quy tắc mạng cho các ứng dụng thuộc một phần của nhóm tin tưởng. Theo các quy tắc này, Tường lửa sẽ quản lý hoạt động mạng của các ứng dụng.

Bảng này sẽ hiển thị các quy tắc mạng xác định trước được khuyến nghị bởi các chuyên gia của Kaspersky. Các quy tắc mạng này đã được thêm vào để bảo vệ tối ưu lưu lượng mạng của các máy tính chạy hệ điều hành Windows. Không thể xóa các quy tắc mạng được xác định trước.

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. Một ví dụ về hậu quả đó là virus có thể thực thi các lệnh dưới quyền tài khoản người dùng của bạn để tải xuống phần mềm độc hại.

Thành phần Phòng chống Tấn công BadUSB sẽ ngăn các thiết bị USB bị nhiễm giả làm một bàn phím khởi kết nối đến máy tính.

Khi một thiết bị USB được kết nối với máy tính và hệ điều hành xác định đó là một bàn phím thì ứng dụng sẽ nhắc người dùng nhập một mã số do ứng dụng tạo ra từ bàn phím này hoặc sử dụng [Bàn phím ảo](#) nếu có (xem hình bên dưới). Thủ tục này được gọi là xác thực bàn phím.

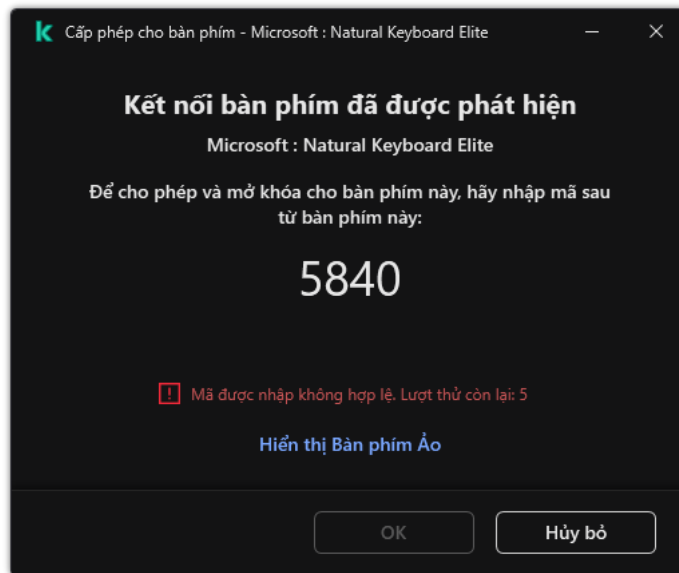
Nếu đã nhập đúng mã, ứng dụng sẽ lưu lại các tham số nhận dạng – VID/PID của bàn phím và số hiệu của cổng kết nối với ứng dụng – trong danh sách các bàn phím được xác thực. Không cần phải lặp lại việc xác thực bàn phím khi kết nối lại bàn phím hoặc sau khi khởi động lại hệ điều hành.

Khi kết nối bàn phím được xác thực với một cổng USB khác của máy tính, thì ứng dụng sẽ hiển thị một lời nhắc để xác thực lại bàn phím này.

Nếu mã số này không được nhập chính xác, ứng dụng sẽ tạo một mã mới. Bạn có thể [cấu hình số lượt thử nhập mã số](#). Nếu mã số được nhập sai vài lần hoặc cửa sổ cấp phép cho bàn phím bị đóng (xem hình bên dưới) thì ứng dụng sẽ chặn nhập vào từ bàn phím này. Khi hết thời gian chặn thiết bị USB hoặc hệ điều hành được khởi động lại, ứng dụng sẽ nhắc người dùng thực hiện lại quy trình cấp phép cho bàn phím.

Ứng dụng sẽ cho phép sử dụng một bàn phím được xác thực và chặn bàn phím không được xác thực.

Thành phần Phòng chống Tấn công BadUSB không được cài đặt theo mặc định. Nếu cần thành phần Phòng chống Tấn công BadUSB, bạn có thể thêm thành phần này trong thuộc tính của [gói cài đặt](#) trước khi cài đặt ứng dụng hoặc [thay đổi các thành phần ứng dụng có sẵn](#) sau khi cài đặt ứng dụng.



Chứng thực bàn phím

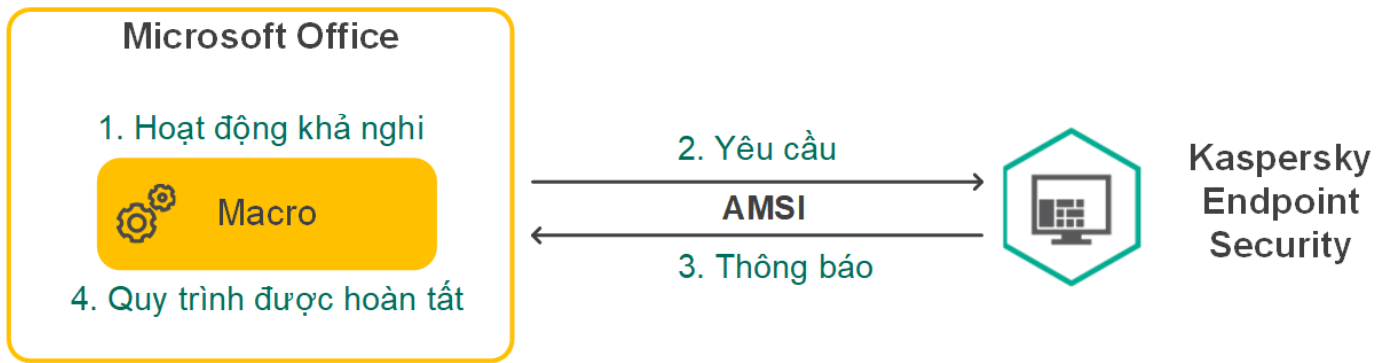
Cấu hình thành phần Phòng chống Tấn công BadUSB

Tham số	Mô tả
Nghiêm cấm việc sử dụng Bàn phím Ảo để xác thực các thiết bị USB	Nếu hộp kiểm này được chọn, ứng dụng sẽ chặn việc sử dụng Bàn phím Ảo để xác thực một thiết bị USB mà từ đó một mã xác thực không thể được nhập.
Số lượng lời nhắc cho phép thiết bị USB tối đa	Tự động chặn thiết bị USB nếu mã cho phép được nhập sai số lần được chỉ định. Giá trị hợp lệ là 1 đến 10. Ví dụ: nếu bạn cho phép 5 lần nhập mã cho phép, thiết bị USB sẽ bị chặn sau lần thứ năm không thành công. Kaspersky Endpoint Security sẽ hiển thị thời lượng chặn cho thiết bị USB. Sau khi hết thời gian này, bạn có thể có 5 lần thử nhập mã cho phép.
Kết thúc thời gian chờ khi đạt số lượng lời nhắc tối đa	Thời gian chặn của thiết bị USB sau số lần nhập mã cho phép không thành công được chỉ định. Giá trị hợp lệ là 1 đến 180 (phút).

Bảo vệ AMSI

Thành phần Bảo vệ AMSI được dành để hỗ trợ Antimalware Scan Interface của Microsoft. *Antimalware Scan Interface (AMSI)* cho phép các ứng dụng thuộc bên thứ ba có hỗ trợ AMSI gửi các đối tượng (ví dụ như kịch bản PowerShell) đến Kaspersky Endpoint Security để quét bổ sung và sau đó nhận kết quả từ việc quét cho các đối tượng này. Các ứng dụng thuộc bên thứ ba ví dụ như các ứng dụng Microsoft Office (xem hình bên dưới). Để biết chi tiết về AMSI, vui lòng tham khảo [tài liệu của Microsoft](#).

Thành phần Bảo vệ AMSI chỉ có thể phát hiện một mối đe dọa và thông báo cho một ứng dụng thuộc bên thứ ba về mối đe dọa được phát hiện. Ứng dụng thuộc bên thứ ba, sau khi nhận được thông báo về mối đe dọa, không cho phép thực hiện các hành động độc hại (ví dụ như chấm dứt).



Ví dụ về hoạt động của AMSI

Thành phần Bảo vệ AMSI có thể từ chối một yêu cầu từ một ứng dụng thuộc bên thứ ba, ví dụ như nếu ứng dụng này vượt quá số yêu cầu tối đa trong một chu kỳ quy định. Kaspersky Endpoint Security sẽ gửi thông tin về một yêu cầu bị từ chối từ ứng dụng thuộc bên thứ ba đến Máy chủ quản trị. Thành phần Bảo vệ AMSI không từ chối các yêu cầu từ các ứng dụng của bên thứ ba có [tích hợp liên tục với thành phần Bảo vệ AMSI](#) được bật.

Bảo vệ AMSI có thể được sử dụng cho các hệ điều hành sau đây cho máy trạm và máy chủ:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise;
- Windows 11;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2022.

Thiết lập Bảo vệ AMSI

Tham số	Mô tả
Quét tập tin nén	Quét định dạng ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE, và các định dạng tập tin nén khác. Kaspersky Endpoint Security quét các tập tin nén không chỉ theo phần mở rộng mà còn theo định dạng. Khi kiểm tra tập tin nén, ứng dụng sẽ thực hiện quy trình giải nén đệ quy. Điều này cho phép phát hiện các mối đe dọa bên trong tập tin nén nhiều cấp (tập tin nén bên trong tập tin nén).
Quét các gói phân phối	Hộp kiểm này bật/tắt tính năng quét các gói phân phối thuộc bên thứ ba.
Quét các tập tin có định dạng Microsoft Office	Quét các tập tin Microsoft Office (DOC, DOCX, XLS, PPT và đuôi mở rộng khác của Microsoft). Các tập tin định dạng Office cũng bao gồm các đối tượng OLE.
Không giải nén các tập tin phức hợp lớn	Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ không quét các tập tin hỗn hợp nếu dung lượng của chúng vượt quá giá trị được quy định. Nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ quét các tập tin hỗn hợp thuộc mọi kích cỡ. Kaspersky Endpoint Security sẽ quét các tập tin lớn được trích xuất từ tập tin nén bất kể hộp kiểm này có được chọn hay không.

Phòng chống khai thác

Thành phần Phòng chống khai thác sẽ phát hiện mã chương trình lợi dụng các lỗ hổng trên máy tính để khai thác quyền của quản trị viên hoặc thực hiện các hoạt động độc hại. Ví dụ như mã khai thác có thể sử dụng một cuộc tấn công tràn bộ đệm. Để thực hiện, mã khai thác sẽ gửi số lượng lớn dữ liệu đến một ứng dụng chứa lỗ hổng. Khi xử lý dữ liệu này, ứng dụng chứa lỗ hổng bảo mật sẽ thực thi mã độc. Kết quả của cuộc tấn công này là mã khai thác có thể tiến hành cài đặt trái phép phần mềm độc hại. Khi có một nỗ lực chạy một tập tin thực thi từ một ứng dụng có lỗ hổng bảo mật không được thực hiện bởi người dùng, Kaspersky Endpoint Security sẽ chặn việc khởi chạy tập tin đó hoặc thông báo cho người dùng.

Cấu hình thành phần Phòng chống khai thác

Tham số	Mô tả
Khi phát hiện khai thác	<p>Chặn hoạt động. Nếu mục này được chọn, khi phát hiện một mã khai thác, Kaspersky Endpoint Security sẽ chặn hoạt động của mã khai thác này và lập một mục nhật ký chứa thông tin về mã khai thác.</p> <p>Thông báo. Nếu mục này được chọn, khi Kaspersky Endpoint Security phát hiện một mã khai thác, ứng dụng sẽ ghi lại một sự kiện chứa thông tin về mã khai thác đó và bổ sung thông tin về mã khai thác vào danh sách các mối đe dọa đang hoạt động.</p>
Bật bảo vệ bộ nhớ tiến trình hệ thống	Nếu công tắc này được bật, Kaspersky Endpoint Security sẽ chặn các tiến trình bên ngoài đang cố gắng truy cập bộ nhớ của tiến trình hệ thống.

Phát hiện hành vi

Thành phần Phát hiện hành vi nhận dữ liệu về hành động của các ứng dụng trên máy tính của bạn và cung cấp thông tin này đến các thành phần bảo vệ khác để cải thiện hiệu quả của chúng. Thành phần Phát hiện hành vi sử dụng Dấu hiệu dòng hành vi (BSS) cho các ứng dụng. Nếu hoạt động của ứng dụng khớp với một dấu hiệu dòng hành vi cụ thể, Kaspersky Endpoint Security sẽ thực hiện hành động phản ứng được chọn. Chức năng của Kaspersky Endpoint Security dựa trên các dấu hiệu dòng hành vi cung cấp chủ động bảo vệ cho máy tính.

Cấu hình thành phần Phát hiện hành vi

Tham số	Mô tả
Khi phát hiện hoạt động của phần mềm độc hại	<ul style="list-style-type: none">• Delete file. Nếu mục này được chọn, khi phát hiện hoạt động độc hại, Kaspersky Endpoint Security sẽ xóa tập tin thực thi của ứng dụng độc hại và tạo một bản sao lưu của tập tin đó trong Sao lưu.• Chấm dứt ứng dụng. Nếu mục này được chọn, khi phát hiện hoạt động độc hại, Kaspersky Endpoint Security sẽ chấm dứt hoạt động của ứng dụng này.• Thông báo. Nếu mục này được lựa chọn và phát hiện hoạt động độc hại của một ứng dụng, Kaspersky Endpoint Security sẽ không chấm dứt ứng dụng này mà thêm thông tin về hoạt động độc hại của ứng dụng này vào danh sách các mối đe dọa đang hoạt động.
Bật tính năng	

<p>bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài</p>	<p>Nếu công tắc này được bật, Kaspersky Endpoint Security sẽ phân tích các hoạt động trong thư mục được chia sẻ. Nếu hoạt động này khớp với một dấu hiệu dòng hành vi giống với hoạt động mã hóa từ bên ngoài, Kaspersky Endpoint Security sẽ thực hiện hành động được chọn.</p> <div data-bbox="424 255 1493 412" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Kaspersky Endpoint Security chỉ ngăn chặn việc mã hóa từ bên ngoài các tập tin nằm trên ổ đĩa có hệ thống tập tin NTFS và không được mã hóa bởi hệ thống EFS.</p> </div> <ul style="list-style-type: none"> • Thông báo. Nếu mục này được lựa chọn, khi phát hiện một nỗ lực sửa đổi các tập tin trong thư mục được chia sẻ, Kaspersky Endpoint Security sẽ bổ sung thông tin về nỗ lực sửa đổi tập tin trong thư mục được chia sẻ đến danh sách các mối đe dọa đang hoạt động. • Chặn kết nối trong N phút. Nếu chọn tùy chọn này, khi Kaspersky Endpoint Security phát hiện nỗ lực sửa đổi tập tin trong thư mục được chia sẻ, ứng dụng sẽ chặn hoạt động mạng của máy tính đang nỗ lực sửa đổi các tập tin và tạo bản sao lưu của các tập tin đã bị sửa đổi. <div data-bbox="424 808 1493 965" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Nếu thành phần Công cụ khắc phục được bật và tùy chọn Chặn kết nối trong N phút được chọn thì các tập tin bị sửa đổi sẽ được khôi phục từ bản sao lưu.</p> </div>
<p>Loại trừ</p>	<p>Danh sách các máy tính sẽ không bị giám sát khi thực hiện mã hóa thư mục được chia sẻ.</p> <div data-bbox="424 1140 1493 1368" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Để áp dụng danh sách loại trừ máy tính khỏi tính năng bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài, bạn phải bật Audit Logon trong chính sách kiểm tra bảo mật của Windows. Audit Logon bị tắt theo mặc định. Để biết thêm về chính sách kiểm tra bảo mật của Windows, vui lòng truy cập website Microsoft.</p> </div>

Phòng chống xâm nhập máy chủ

Thành phần Phòng chống xâm nhập máy chủ 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 cá nhân. Thành phần này giúp bảo vệ máy tính với sự trợ giúp của cơ sở dữ liệu diệt virus và dịch vụ đám mây của Kaspersky Security Network.

Thành phần này kiểm soát hoạt động của các ứng dụng bằng cách sử dụng *các quyền của ứng dụng*. Các quyền của ứng dụng bao gồm các tham số truy cập sau:

- Truy cập vào tài nguyên của hệ điều hành (ví dụ: các tùy chọn khởi động tự động, khóa registry)
- Truy cập vào dữ liệu cá nhân (như các tập tin và ứng dụng)

Hoạt động mạng của các ứng dụng được kiểm soát bởi [Tường lửa](#) bằng cách sử dụng *quy tắc mạng*.

Trong lần khởi động đầu tiên của ứng dụng, thành phần Phòng chống xâm nhập máy chủ sẽ thực hiện các hành động sau:

1. Kiểm tra tính bảo mật của ứng dụng bằng cách cơ sở dữ liệu diệt virus đã tải xuống.
2. Kiểm tra tính bảo mật của ứng dụng trong Kaspersky Security Network.

Bạn nên [tham gia vào Kaspersky Security Network](#) để giúp thành phần Phòng chống xâm nhập máy chủ hoạt động hiệu quả hơn.

3. Đưa ứng dụng vào một trong các *nhóm tin tưởng*: Tin tưởng, Giới hạn mức Thấp, Giới hạn mức Cao, Không tin tưởng.

Một [nhóm tin tưởng quy định các quyền](#) được Kaspersky Endpoint Security áp dụng khi kiểm soát hoạt động của các ứng dụng trong nhóm đó. Kaspersky Endpoint Security sẽ đặt ứng dụng vào một nhóm tin tưởng tùy thuộc vào mức độ nguy hiểm mà ứng dụng này có thể gây ra cho máy tính.

Kaspersky Endpoint Security sẽ đặt ứng dụng vào nhóm tin tưởng cho các thành phần Tường lửa và Phòng chống xâm nhập máy chủ. Bạn chỉ không thể thay đổi nhóm tin tưởng cho Tường lửa hoặc Phòng chống xâm nhập máy chủ.

Nếu bạn từ chối tham gia vào KSN hoặc không có mạng, Kaspersky Endpoint Security sẽ đặt ứng dụng vào một nhóm tin tưởng tùy thuộc vào [thiết lập của thành phần Phòng chống xâm nhập máy chủ](#). Sau khi nhận được danh tiếng của ứng dụng từ KSN, nhóm tin tưởng có thể được thay đổi tự động.

4. Chặn các hành động của ứng dụng tùy thuộc vào nhóm tin tưởng. Ví dụ: các ứng dụng trong nhóm tin tưởng Giới hạn mức Cao bị từ chối truy cập vào các mô-đun hệ điều hành.

Khi ứng dụng được khởi chạy vào lần tới, Kaspersky Endpoint Security sẽ kiểm tra tính toàn vẹn của ứng dụng. Nếu ứng dụng không thay đổi, thành phần sẽ áp dụng các quyền của ứng dụng hiện tại cho nó. Nếu ứng dụng đã bị sửa đổi, Kaspersky Endpoint Security sẽ phân tích ứng dụng đó như khi ứng dụng đó được khởi chạy lần đầu tiên.

Cấu hình thành phần Phòng chống xâm nhập máy chủ

Tham số	Mô tả
Các quyền của ứng dụng	<p>Ứng dụng</p> <p>Bảng các ứng dụng được giám sát bởi thành phần Phòng chống xâm nhập máy chủ. Các ứng dụng được gán vào các nhóm tin tưởng. Một nhóm tin tưởng quy định các quyền được Kaspersky Endpoint Security áp dụng khi kiểm soát hoạt động của các ứng dụng trong nhóm đó.</p> <p>Bạn có thể chọn một ứng dụng trong một danh sách duy nhất của tất cả các ứng dụng được cài đặt trên máy tính chịu ảnh hưởng của chính sách và thêm ứng dụng đó vào nhóm tin tưởng.</p> <p>Quyền truy cập của ứng dụng được trình bày trong các bảng sau:</p> <ul style="list-style-type: none">• Tập tin và registry hệ thống. Bảng này chứa quyền của các ứng dụng trong nhóm tin tưởng để truy cập tài nguyên hệ điều hành và dữ liệu cá nhân.

	<ul style="list-style-type: none"> • Quyền. Cột này chứa quyền của các ứng dụng trong một nhóm tin tưởng để truy cập các tiến trình và tài nguyên của hệ điều hành. • Quy tắc mạng. Bảng quy tắc mạng cho các ứng dụng thuộc một phần của nhóm tin tưởng. Theo các quy tắc này, Trường lửa sẽ quản lý hoạt động mạng của các ứng dụng. Bảng này sẽ hiển thị các quy tắc mạng xác định trước được khuyến nghị bởi các chuyên gia của Kaspersky. Các quy tắc mạng này đã được thêm vào để bảo vệ tối ưu lưu lượng mạng của các máy tính chạy hệ điều hành Windows. Không thể xóa các quy tắc mạng được xác định trước.
Bảo vệ tài nguyên	<p>Tên</p> <p>Bảng chứa các tài nguyên máy tính được phân theo danh mục. Thành phần Phòng chống xâm nhập máy chủ sẽ giám sát các nỗ lực của các ứng dụng khác để truy cập tài nguyên trong bảng này.</p> <p>Một tài nguyên có thể là một danh mục registry, tập tin hoặc thư mục, hoặc khóa registry.</p> <p>Ứng dụng</p> <p>Bảng các ứng dụng được giám sát bởi thành phần Phòng chống xâm nhập máy chủ cho tài nguyên đã chọn. Các ứng dụng được gán vào các nhóm tin tưởng. Một nhóm tin tưởng quy định các quyền được Kaspersky Endpoint Security áp dụng khi kiểm soát hoạt động của các ứng dụng trong nhóm đó.</p>
Nhóm tin tưởng cho các ứng dụng đã được khởi chạy trước khi Kaspersky Endpoint Security cho Windows bắt đầu hoạt động	<p>Một nhóm tin tưởng trong đó Kaspersky Endpoint Security sẽ đặt các ứng dụng được khởi chạy trước Kaspersky Endpoint Security.</p>
Cập nhật quyền cho các ứng dụng trước đây chưa được xác định trong cơ sở dữ liệu KSN	<p>Nếu hộp kiểm này được chọn, thành phần Phòng chống xâm nhập máy chủ sẽ cập nhật các quyền cho các ứng dụng không xác định trước đó bằng cách sử dụng cơ sở dữ liệu của Kaspersky Security Network.</p>
Tin tưởng các ứng dụng được ký số	<p>Nếu hộp kiểm này được chọn, thành phần Phòng chống xâm nhập máy chủ sẽ đặt các ứng dụng có chữ ký điện tử của các nhà cung cấp được tin tưởng vào nhóm Tin tưởng.</p> <p><i>Nhà cung cấp được tin tưởng</i> là các nhà cung cấp phần mềm được Kaspersky tin tưởng. Bạn cũng có thể thêm chứng chỉ nhà cung cấp vào kho chứng chỉ được tin tưởng theo cách thủ công.</p> <p>Nếu hộp kiểm này bị xóa, thành phần Phòng chống xâm nhập máy chủ sẽ không coi các ứng dụng như vậy là được tin tưởng, và sử dụng các tham số khác để xác định nhóm tin tưởng của chúng.</p>
Xóa quy tắc cho các ứng dụng không được khởi động nhiều hơn (ngày, 1 đến 90)	<p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ tự động xóa thông tin về ứng dụng (nhóm tin tưởng và quyền truy cập) nếu các điều kiện sau được đáp ứng:</p> <ul style="list-style-type: none"> • Bạn đặt ứng dụng vào nhóm tin tưởng hoặc cấu hình quyền truy cập của ứng dụng một cách thủ công.

	<ul style="list-style-type: none"> • Ứng dụng chưa khởi chạy trong khoảng thời gian xác định. <p>Nếu nhóm tin tưởng và quyền của ứng dụng được xác định tự động, Kaspersky Endpoint Security sẽ xóa thông tin về ứng dụng này sau 30 ngày. Không thể thay đổi thời hạn lưu trữ cho thông tin ứng dụng hoặc tắt tính năng tự động xóa.</p> <p>Lần tới, khi bạn khởi động ứng dụng này, Kaspersky Endpoint Security sẽ phân tích ứng dụng như thể ứng dụng đang khởi chạy lần đầu tiên.</p>
<p>Nhóm tin tưởng cho các ứng dụng không thể thêm được vào các nhóm có sẵn</p>	<p>Các mục trong danh sách thả xuống này quyết định nhóm tin tưởng được Kaspersky Endpoint Security gán cho một ứng dụng không xác định.</p> <p>Bạn có thể chọn một trong các tùy chọn sau:</p> <ul style="list-style-type: none"> • Giới hạn mức Thấp. • Giới hạn mức Cao. • Không Tin tưởng.

Công cụ khắc phục

Công cụ khắc phục cho phép Kaspersky Endpoint Security có thể hoàn tác các hành động đã được thực hiện bởi phần mềm độc hại trong hệ điều hành.

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 độc hại sau đây:

- **Hoạt động trên tập tin**

Kaspersky Endpoint Security thực hiện các hành động sau:

- Xóa các tập tin thực thi đã được tạo bởi phần mềm độc hại (trên tất cả các ổ đĩa ngoại trừ ổ đĩa mạng).
- Xóa các tập tin thực thi được tạo bởi các chương trình bị xâm nhập bởi phần mềm độc hại.
- Khôi phục các tập tin đã bị sửa đổi hoặc xóa bởi phần mềm độc hại.

Tính năng phục hồi tập tin có [một số giới hạn](#).

- **Hoạt động registry**

Kaspersky Endpoint Security thực hiện các hành động sau:

- Xóa các khóa registry được tạo bởi phần mềm độc hại.
- Không khôi phục các khóa registry đã bị sửa đổi hoặc xóa bởi phần mềm độc hại.

- **Hoạt động hệ thống**

Kaspersky Endpoint Security thực hiện các hành động sau:

- Chấm dứt các tiến trình đã được khởi động bởi một phần mềm độc hại.

- Chấm dứt các tiến trình bị xâm nhập bởi một ứng dụng độc hại.
- Không khôi phục các tiến trình đã bị dừng bởi một phần mềm độc hại.
- **Hoạt động mạng**

Kaspersky Endpoint Security thực hiện các hành động sau:

- Chặn hoạt động mạng của phần mềm độc hại.
- Chặn hoạt động mạng của các tiến trình đã bị phần mềm độc hại xâm nhập.

Việc hoàn tác các hành động của phần mềm độc hại có thể được bắt đầu bởi thành phần [Bảo vệ mối đe dọa tập tin](#) hoặc [Phát hiện hành vi](#), hay 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.

Kaspersky Security Network

Để bảo vệ máy tính của bạn một cách hiệu quả hơn, Kaspersky Endpoint Security sẽ sử dụng dữ liệu được nhận từ người dùng trên khắp thế giới. Kaspersky Security Network được thiết kế để lấy 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. Nếu bạn đang tham gia vào Kaspersky Security Network, các dịch vụ KSN sẽ cung cấp cho Kaspersky Endpoint Security thông tin về danh mục và danh tiếng của các tập tin được quét, cũng như thông tin về danh tiếng của các địa chỉ trang web được quét.

Việc sử dụng Kaspersky Security Network là hoàn toàn tự nguyện. Ứng dụng sẽ nhắc bạn sử dụng KSN trong quá trình cấu hình ban đầu ứng dụng. Người dùng có thể bắt đầu hoặc ngừng tham gia KSN tại bất cứ thời điểm nào.

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 có văn bản của Tuyên bố Kaspersky Security Network cũng được bao gồm trong [gói phân phối](#) ứng dụng.

Để giảm tải cho các máy chủ KSN, các chuyên gia của Kaspersky có thể phát hành các bản cập nhật ứng dụng để tắt tạm thời hoặc hạn chế một phần các yêu cầu được gửi đến Kaspersky Security Network. Trong trường hợp này, trạng thái của kết nối đến KSN trong giao diện cục bộ của ứng dụng sẽ là *Cho phép với hạn chế*.

Hạ tầng KSN

Kaspersky Endpoint Security hỗ trợ các giải pháp hạ tầng KSN sau đây:

- *KSN Toàn cầu* là giải pháp được hầu hết các ứng dụng Kaspersky sử dụng. Người tham gia vào KSN sẽ nhận thông tin từ Kaspersky Security Network và gửi cho Kaspersky thông tin về các đối tượng được xóa trên máy tính của người dùng. Đây là những đối tượng sẽ được các chuyên gia phân tích của

Kaspersky phân tích thêm và sẽ được đưa vào cơ sở dữ liệu danh tiếng và thống kê của Kaspersky Security Network.

- *KSN Riêng* là một giải pháp cho phép người dùng máy tính lưu trữ Kaspersky Endpoint Security hoặc các ứng dụng khác của Kaspersky để có quyền truy cập cơ sở dữ liệu danh tiếng của Kaspersky Security Network và truy cập các dữ liệu thống kê khác mà không cần gửi dữ liệu cho KSN từ máy tính của riêng họ. KSN Riêng được thiết kế dành cho khách hàng doanh nghiệp không thể tham gia vào Kaspersky Security Network vì bất kỳ lý do nào dưới đây:
 - Các máy trạm cục bộ không được kết nối vào mạng Internet.
 - Việc truyền tải bất kỳ dữ liệu nào bên ngoài quốc gia hoặc bên ngoài mạng LAN của doanh nghiệp đều bị cấm theo luật pháp hoặc bị hạn chế bởi các chính sách bảo mật của doanh nghiệp.

Theo mặc định, Kaspersky Security Center sẽ sử dụng KSN Toàn cầu. Bạn có thể cấu hình việc sử dụng KSN Riêng trong Bảng điều khiển quản trị (MMC), trong Bảng điều khiển web Kaspersky Security Center và trong [dòng lệnh](#). Không thể cấu hình việc sử dụng KSN Riêng trong Bảng điều khiển đám mây Kaspersky Security Center.

Để biết thêm chi tiết về KSN Riêng, vui lòng tham khảo tài liệu về Kaspersky Private Security Network.

Proxy KSN

Máy tính của người dùng được quản lý bởi Máy chủ quản trị Kaspersky Security Center có thể tương tác với KSN thông qua dịch vụ Proxy KSN.

Dịch vụ Proxy KSN 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.
- Dịch vụ Proxy KSN sẽ lưu lại dữ liệu được xử lý, qua đó giảm tải cho mạng bên ngoài, kênh truyền thông và tăng tốc độ nhận thông tin được yêu cầu bởi máy tính của người dùng.

Để biết thêm chi tiết về dịch vụ Proxy KSN, vui lòng tham khảo [Trợ giúp của Kaspersky Security Center](#).

Cấu hình của Kaspersky Security Network

Tham số	Mô tả
Bật chế độ KSN mở rộng	<i>Chế độ KSN mở rộng</i> là chế độ trong đó Kaspersky Endpoint Security sẽ gửi dữ liệu bổ sung đến Kaspersky. Kaspersky Endpoint Security sử dụng KSN để phát hiện các mối đe dọa, bất kể vị trí của nút bật/tắt.
Bật chế độ đám mây	<i>Chế độ đám mây</i> chỉ chế độ hoạt động của ứng dụng trong đó Kaspersky Endpoint Security sử dụng phiên bản nhẹ của cơ sở dữ liệu diệt virus. Kaspersky Security Network hỗ trợ hoạt động của ứng dụng khi cơ sở dữ liệu diệt virus nhẹ đang được sử dụng. Phiên bản nhẹ của cơ sở dữ liệu diệt virus cho phép bạn sử dụng khoảng một nửa dung lượng RAM của máy tính so với dung lượng RAM được sử dụng với cơ sở dữ liệu thông thường. Nếu bạn không tham gia vào Kaspersky Security Network hoặc nếu chế độ đám mây bị tắt, Kaspersky Endpoint Security sẽ tải về phiên bản đầy đủ của cơ sở dữ liệu diệt virus từ các máy chủ của Kaspersky. Nếu công tắc này được bật, Kaspersky Endpoint Security sẽ sử dụng phiên bản nhẹ của cơ sở dữ liệu diệt virus, nhằm làm giảm tải cho tài nguyên hệ điều hành.

Kaspersky Endpoint Security sẽ tải về phiên bản nhẹ của cơ sở dữ liệu diệt virus trong lần cập nhật tiếp theo sau khi hộp kiểm này được lựa chọn.

Nếu công tắc này bị tắt, Kaspersky Endpoint Security sẽ sử dụng phiên bản đầy đủ của cơ sở dữ liệu diệt virus.

Kaspersky Endpoint Security sẽ tải về phiên bản đầy đủ của cơ sở dữ liệu diệt virus trong lần cập nhật tiếp theo sau khi hộp kiểm này bị xóa.

**Trạng
thái máy
tính khi
máy chủ
KSN
không
khả dụng**

*(chỉ khả
dụng
trong
Bảng điều
khiển
Kaspersky
Security
Center)*

Các mục trong danh sách thả xuống xác định trạng thái của một máy tính trong Kaspersky Security Center khi các máy chủ KSN không khả dụng.

**Sử dụng
Proxy
KSN**

*(chỉ khả
dụng
trong
Bảng điều
khiển
Kaspersky
Security
Center)*

Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ sử dụng dịch vụ Proxy KSN. Bạn có thể cấu hình thiết lập dịch vụ KSN Proxy trong thuộc tính của Máy chủ quản trị.

**Sử dụng
máy chủ
KSN khi
Proxy
KSN
không có
sẵn**

*(chỉ khả
dụng
trong
Bảng điều
khiển
Kaspersky
Security
Center)*

Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ sử dụng các máy chủ KSN khi dịch vụ KSN Proxy không khả dụng. Máy chủ KSN có thể được đặt trên cả Kaspersky (khi KSN Toàn cầu được sử dụng) và trên một bên thứ ba (nếu KSN Riêng được sử dụng).

Kiểm soát Web

Kiểm soát Web quản lý quyền truy cập của người dùng đối với các tài nguyên web. Điều này giúp giảm lưu lượng và việc sử dụng không hợp lý thời gian làm việc. Khi người dùng cố mở một website bị hạn chế bởi Kiểm soát Web, Kaspersky Endpoint Security sẽ chặn quyền truy cập hoặc hiển thị một cảnh báo (xem hình bên dưới).

Kaspersky Endpoint Security chỉ giám sát lưu lượng HTTP và lưu lượng HTTPS.

Để giám sát lưu lượng HTTPS, bạn cần [bật quét kết nối được mã hóa](#).

Các phương thức quản lý quyền truy cập website

Kiểm soát Web cho phép bạn cấu hình quyền truy cập đến các website bằng các phương thức sau đây:

- **Danh mục website.** Các website được phân loại theo dịch vụ đám mây của Kaspersky Security Network, phân tích theo hành vi và cơ sở dữ liệu của các website đã biết (đã được thêm vào cơ sở dữ liệu của ứng dụng). Ví dụ: bạn có thể hạn chế quyền truy cập của người dùng vào danh mục "Mạng xã hội" hoặc các [danh mục khác](#).
- **Loại dữ liệu.** Bạn có thể hạn chế truy cập của người dùng đến dữ liệu trên một website, ví dụ như ảnh đồ họa. Kaspersky Endpoint Security xác định loại dữ liệu dựa theo định dạng tập tin, không dựa theo phần mở rộng của tập tin.

Kaspersky Endpoint Security không quét các tập tin bên trong tập tin nén. Ví dụ: nếu các tập tin ảnh được đặt trong một tập tin nén thì Kaspersky Endpoint Security sẽ coi đó là dữ liệu "Tập tin nén", không phải là "Tập tin đồ họa".

- **Địa chỉ được chỉ định.** Bạn có thể nhập một địa chỉ web hoặc [sử dụng các đại diện](#).

Bạn có thể sử dụng đồng thời nhiều phương thức để quản lý quyền truy cập đến các website. Ví dụ: bạn có thể hạn chế quyền truy cập loại dữ liệu "Tập tin văn phòng" chỉ với riêng danh mục website "Thư điện tử trên web".


Quy tắc truy cập website

Kiểm soát Web quản lý quyền truy cập của người dùng đến các website thông qua các *quy tắc truy cập*. Bạn có thể thiết lập các cấu hình nâng cao sau đối với một quy tắc truy cập website:

- Những người dùng là đối tượng áp dụng của quy tắc.
Ví dụ như bạn có thể hạn chế truy cập Internet của tất cả người dùng của công ty thông qua một trình duyệt, trừ bộ phận CNTT.
- Lịch quy tắc.
Ví dụ như bạn có thể chỉ hạn chế truy cập Internet thông qua một trình duyệt trong giờ làm việc.

Các mức ưu tiên của quy tắc truy cập

Mỗi quy tắc có một mức ưu tiên. Quy tắc có vị trí càng cao trên danh sách thì càng có mức ưu tiên cao. Nếu một website đã được thêm vào nhiều quy tắc, Kiểm soát Web sẽ quản lý quyền truy cập website đó dựa trên quy tắc có mức ưu tiên cao nhất. Ví dụ như Kaspersky Endpoint Security có thể xác định một cổng thông tin của doanh nghiệp là một mạng xã hội. Để hạn chế truy cập đến các mạng xã hội và cho phép truy cập cổng thông tin web của doanh nghiệp, hãy tạo hai quy tắc: một quy tắc chặn truy cập dành cho danh mục website "Mạng xã hội" và một quy tắc cho phép truy cập dành cho cổng thông tin web của doanh nghiệp. Quy tắc truy cập dành cho cổng thông tin web của doanh nghiệp phải có mức ưu tiên cao hơn so với quy tắc dành cho mạng xã hội.



Trang web yêu cầu không được cung cấp.


Địa chỉ: <http://kaspersky.ru/>.

Trang web bị ngăn chặn bởi quy tắc block.

Lý do: tài nguyên web thuộc về thể loại nội dung Không xác định và thể loại kiểu dữ liệu Không xác định.

Tài nguyên web bị cấm tại công ty. Nếu bạn nghĩ rằng việc ngăn chặn là nhầm lẫn hoặc nếu bạn cần truy cập đến nguồn tài nguyên web này, liên hệ quản trị viên của mạng nội bộ công ty ([Yêu cầu truy cập](#)).

Thư được tạo vào: 29.10.2020 13:09:53



Trang web yêu cầu có thể không an toàn hoặc bị cấm bởi chính sách công ty.

Địa chỉ: <http://kaspersky.com/>.

Trang web bị ngăn chặn bởi quy tắc warn.

Lý do: nguồn tài nguyên web thuộc các thể loại nội dung Không xác định và thể loại kiểu dữ liệu Không xác định.

Nhấn vào liên kết <http://kaspersky.com/> để yêu cầu mở trang web. Nhấn vào liên kết http://kaspersky.com/* để được quyền truy cập vào toàn bộ nội dung của trang web mà trên đó các yêu cầu trang web. Nhấn vào liên kết */*.kaspersky.com/* để được quyền truy cập vào tất cả lĩnh vực có mức độ thấp hơn hoặc bằng với "*".

Truy cập vào các nguồn tài nguyên web được liệt kê ở trên sẽ được cấp trong phiên làm việc hiện tại của Kaspersky Endpoint Security. Trong trường hợp đây là cảnh báo sai, liên hệ quản trị viên của mạng nội bộ công ty ([Yêu cầu truy cập](#)).

Thư được tạo vào: 29.10.2020 13:09:59

Thông báo của Kiểm soát Web

Cấu hình thành phần Kiểm soát Web

Tham số	Mô tả
Quy tắc truy cập tài nguyên web	Danh sách chứa các quy tắc truy cập tài nguyên web. Mỗi quy tắc có một mức ưu tiên. Quy tắc có vị trí càng cao trên danh sách thì càng có mức ưu tiên cao. Nếu một website đã được thêm vào nhiều quy tắc, Kiểm soát Web sẽ quản lý quyền truy cập website đó dựa trên quy tắc có mức ưu tiên cao nhất.
Quy tắc	<i>Quy tắc mặc định</i> là một quy tắc truy cập đến các tài nguyên web không được quản lý bởi bất kỳ quy tắc nào khác. Các tùy chọn sau có thể được sử dụng:

mặc định	<ul style="list-style-type: none"> • Cho phép tất cả, trừ danh sách quy tắc, còn được gọi là chế độ danh sách không được phép dành cho các website bị cấm. • Từ chối tất cả trừ danh sách quy tắc, còn được gọi là chế độ danh sách được phép dành cho các website được phép.
Tin nhắn mẫu	<ul style="list-style-type: none"> • Cảnh báo. Trường nhập liệu này bao gồm một mẫu tin nhắn sẽ được hiển thị nếu một quy tắc cảnh báo về nỗ lực truy cập một tài nguyên web không mong muốn được kích hoạt. • Tin nhắn về hoạt động chặn. Trường nhập liệu này chứa mẫu tin nhắn sẽ được hiển thị nếu một quy tắc chặn truy cập đến một tài nguyên web được kích hoạt. • Thông điệp đến quản trị viên. Mẫu tin nhắn được gửi đến quản trị viên mạng LAN nếu người dùng cho rằng việc chặn là do nhầm lẫn. Sau khi người dùng yêu cầu cung cấp quyền truy cập, Kaspersky Endpoint Security sẽ gửi một sự kiện đến Kaspersky Security Center: Thông báo chặn truy cập trang web gửi đến quản trị viên. Phần mô tả sự kiện chứa một thông báo cho quản trị viên với các biến được thay thế. Bạn có thể xem các sự kiện này trong bảng điều khiển Kaspersky Security Center bằng cách sử dụng lựa chọn sự kiện được định sẵn User requests. Nếu tổ chức của bạn chưa triển khai Kaspersky Security Center hoặc không có kết nối với Máy chủ quản trị thì ứng dụng sẽ gửi một thông báo cho quản trị viên tới địa chỉ email được chỉ định.
Ghi lại việc mở ra các trang được cho phép	<p>Kaspersky Endpoint Security sẽ lưu ký dữ liệu đối với lượt truy cập vào tất cả các website, bao gồm các website được phép. Kaspersky Endpoint Security sẽ gửi các sự kiện đến Kaspersky Security Center, đến nhật ký cục bộ của Kaspersky Endpoint Security, và đến nhật ký Sự kiện của Windows. Để giám sát hoạt động truy cập Internet của người dùng, bạn cần cấu hình thiết lập đối với các sự kiện lưu.</p> <div style="background-color: #f8d7da; padding: 10px; margin: 10px 0;"> <p>Các trình duyệt hỗ trợ chức năng giám sát: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. Chức năng giám hoạt động của người dùng không hoạt động trong các trình duyệt khác.</p> </div> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Việc giám sát hoạt động truy cập Internet của người dùng có thể cần nhiều tài nguyên máy tính hơn khi giải mã lưu lượng HTTPS.</p> </div>

Kiểm soát Thiết bị

Kiểm soát thiết bị quản lý quyền truy cập của người dùng đến các thiết bị được cài đặt trên máy tính hoặc kết nối với máy tính (ví dụ, ổ cứng, camera, hoặc mô-đun Wi-Fi). Việc này cho phép bạn bảo vệ máy tính khỏi bị nhiễm độc khi các thiết bị đó được kết nối, và ngăn thất thoát hoặc rò rỉ dữ liệu.

Các cấp truy cập thiết bị

Kiểm soát thiết bị kiểm soát quyền truy cập ở các cấp độ sau:

- **Loại thiết bị.** Ví dụ, máy in, ổ đĩa di động và ổ CD/DVD.

Bạn có thể cấu hình quyền truy cập thiết bị như sau:

- Cho phép - ✓.
- Chặn - ✗.
- Tùy thuộc vào bus kết nối (ngoại trừ Wi-Fi) - 🌐.
- Chặn với ngoại lệ (chỉ mạng Wi-Fi) - 🌐.

- **Bus kết nối.** Một *bus kết nối* là một giao diện được sử dụng để kết nối các thiết bị đến máy tính (ví dụ: USB hoặc FireWire). Do đó, bạn có thể hạn chế kết nối của tất cả các thiết bị, ví dụ như qua USB.

Bạn có thể cấu hình quyền truy cập thiết bị như sau:

- Cho phép - ✓.
- Chặn - ✗.

- **Thiết bị được tin tưởng.** *Thiết bị được tin tưởng* là các thiết bị mà những người dùng được quy định trong thiết lập thiết bị được tin tưởng có thể truy cập vào bất cứ lúc nào.

Bạn có thể bổ sung các thiết bị được tin tưởng dựa trên dữ liệu sau:

- **Thiết bị bằng ID** Mỗi thiết bị có một mã định danh duy nhất (ID phần cứng hay HWID). Bạn có thể xem ID trong thuộc tính thiết bị bằng cách sử dụng công cụ hệ điều hành. ID thiết bị mẫu: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Thêm thiết bị theo ID là một cách thuận tiện nếu bạn muốn thêm một số thiết bị cụ thể.
- **Thiết bị bằng model** Mỗi thiết bị có một ID nhà cung cấp (VID) và một ID sản phẩm (PID). Bạn có thể xem ID trong thuộc tính thiết bị bằng cách sử dụng công cụ hệ điều hành. Mẫu để nhập VID và PID: `VID_1234&PID_5678`. Thêm thiết bị theo model là cách thuận tiện nếu bạn sử dụng các thiết bị thuộc một model nhất định trong tổ chức của mình. Bằng cách này, bạn có thể thêm tất cả các thiết bị thuộc model này.
- **Thiết bị bằng ID đại diện** Nếu bạn đang sử dụng nhiều thiết bị có ID tương tự, bạn có thể thêm thiết bị vào danh sách được tin tưởng bằng cách sử dụng tên đại diện. Ký tự `*` sẽ thay thế bất kỳ bộ ký tự nào. Kaspersky Endpoint Security không hỗ trợ ký tự `?` khi nhập tên đại diện. Ví dụ: `WDC_C*`.
- **Thiết bị theo model đại diện** Nếu bạn đang sử dụng nhiều thiết bị có VID hoặc PID tương tự (ví dụ: các thiết bị của cùng một nhà sản xuất), bạn có thể thêm thiết bị vào danh sách được tin tưởng bằng cách sử dụng tên đại diện. Ký tự `*` sẽ thay thế bất kỳ bộ ký tự nào. Kaspersky Endpoint Security không hỗ trợ ký tự `?` khi nhập tên đại diện. Ví dụ: `VID_05AC & PID_*`.

Kiểm soát thiết bị điều chỉnh quyền truy cập của người dùng đến các thiết bị thông qua các [quy tắc truy cập](#). Kiểm soát thiết bị cũng cho phép bạn lưu các sự kiện kết nối/ngắt kết nối thiết bị. Để lưu các sự kiện, bạn cần cấu hình việc đăng ký sự kiện trong một chính sách.

Nếu quyền truy cập một thiết bị tùy thuộc vào bus kết nối (trạng thái 🌐), Kaspersky Endpoint Security sẽ không lưu các sự kiện kết nối/ngắt kết nối thiết bị. Để cho phép Kaspersky Endpoint Security lưu các sự kiện kết nối/ngắt kết nối thiết bị, hãy cho phép truy cập đến loại thiết bị tương ứng (trạng thái ✓) hoặc thêm thiết bị vào danh sách tin tưởng.

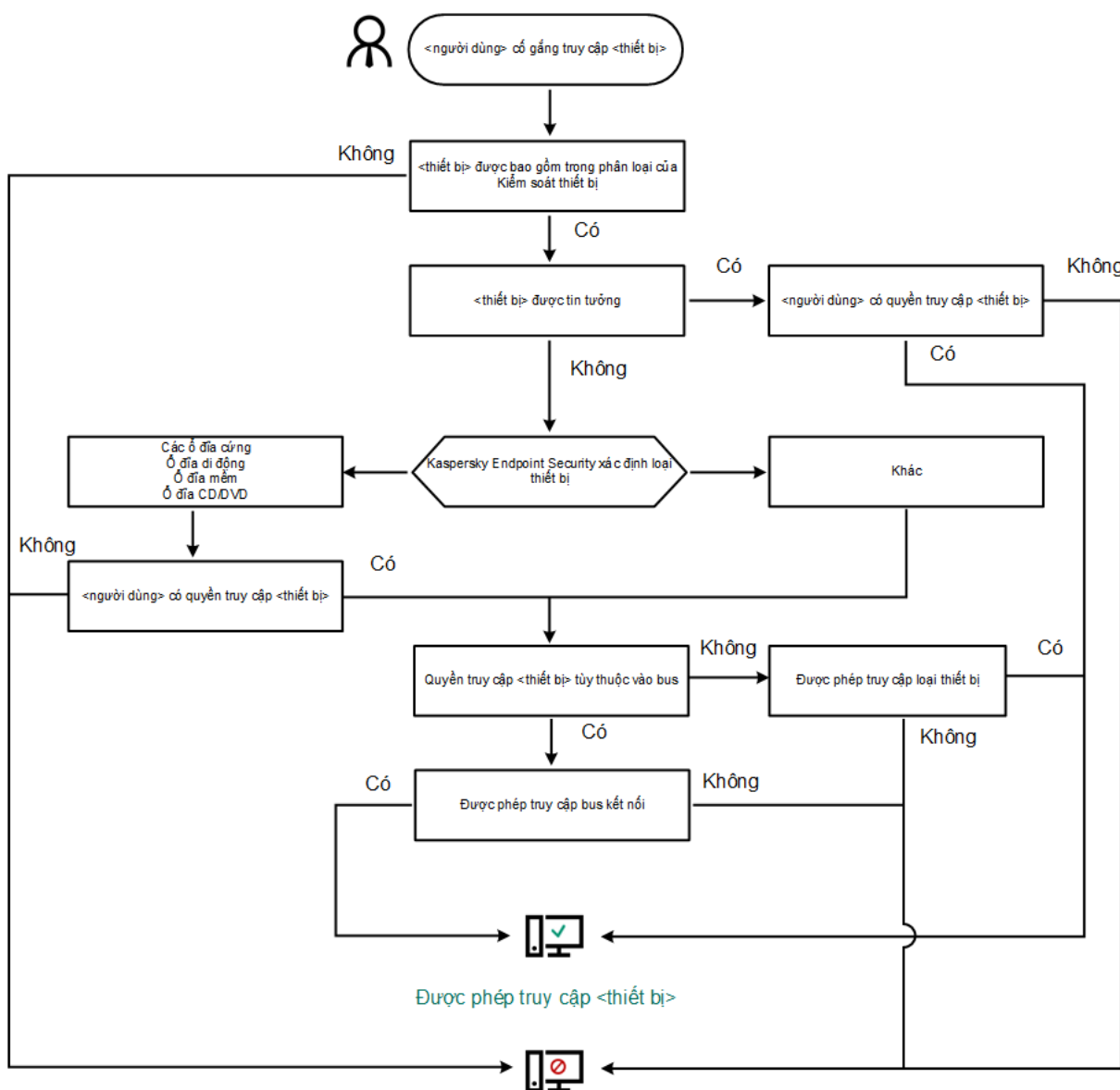
Khi một thiết bị bị chặn bởi Kiểm soát thiết bị được kết nối đến máy tính, Kaspersky Endpoint Security sẽ chặn quyền truy cập và hiển thị một thông báo (xem hình dưới đây).



Thông báo Kiểm soát thiết bị

Thuật toán vận hành Kiểm soát thiết bị

Kaspersky Endpoint Security sẽ đưa ra quyết định về việc cho phép truy cập đến một thiết bị hay không, sau khi người dùng kết nối thiết bị đến máy tính (xem hình bên dưới).



Truy cập vào <thiết bị> bị chặn

Nếu một thiết bị được kết nối và được cho phép truy cập, bạn có thể chỉnh sửa quy tắc truy cập và chặn quyền truy cập. Trong trường hợp này, lần tới, khi có người cố truy cập thiết bị (như xem cây thư mục hoặc thực hiện hoạt động đọc hay ghi) thì Kaspersky Endpoint Security sẽ chặn quyền truy cập. 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](#).

Cấu hình thành phần Kiểm soát thiết bị

Tham số	Mô tả
Allow requests for temporary access <i>(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)</i>	Nếu hộp kiểm được chọn, nút Yêu cầu truy cập sẽ có thể được sử dụng thông qua giao diện cục bộ của Kaspersky Endpoint Security. Nhấn vào nút này để mở ra cửa sổ Yêu cầu truy cập thiết bị . Trong cửa sổ này, người dùng có thể yêu cầu truy cập tạm thời đến một thiết bị bị chặn.
Các thiết bị và mạng Wi-Fi	Bảng này chứa tất cả các loại thiết bị có thể có theo phân loại của thành phần Kiểm soát thiết bị, bao gồm trạng thái truy cập tương ứng của chúng.
Các Bus kết nối	Một danh sách tất cả các bus kết nối có thể sử dụng theo phân loại của thành phần Kiểm soát thiết bị, bao gồm trạng thái truy cập tương ứng của chúng.
Thiết bị được tin tưởng	Danh sách các thiết bị được tin tưởng và người dùng được cấp quyền truy cập các thiết bị này.
Anti-Bridging	<p>Anti-Bridging ngăn tạo các cầu nối mạng bằng cách ngăn thiết lập đồng thời nhiều kết nối mạng cho một máy tính. Tính năng này cho phép bạn bảo vệ mạng doanh nghiệp trước các cuộc tấn công qua mạng không được bảo vệ, mạng phép.</p> <p>Anti-Bridging chặn thiết lập nhiều kết nối theo các mức ưu tiên của thiết bị. Thiết bị có vị trí càng cao trong danh sách thì có mức ưu tiên càng cao.</p> <p>Nếu một kết nối đang hoạt động và một kết nối mới cùng loại (như kết nối Wi-Fi), Kaspersky Endpoint Security sẽ chặn kết nối đang hoạt động và cho phép thiết lập kết nối mới.</p> <p>Nếu một kết nối đang hoạt động và một kết nối mới khác loại (ví dụ như kết nối qua bộ điều hợp mạng và kết nối Wi-Fi), Kaspersky Endpoint Security sẽ chặn kết nối có mức ưu tiên thấp hơn và cho phép kết nối có mức ưu tiên cao hơn.</p> <p>Anti-Bridging hỗ trợ hoạt động với các loại thiết bị sau: bộ điều hợp mạng, Wi-Fi và modem.</p>
Tin nhắn mẫu	Tin nhắn về hoạt động chặn. Mẫu thông báo hiển thị khi người dùng cố truy cập thiết bị bị chặn. Thông báo này cũng sẽ hiển thị khi người dùng cố thực hiện một

hành động lên nội dung thiết bị bị chặn đối với người dùng này.

Thông điệp đến quản trị viên. Một mẫu tin nhắn sẽ được gửi đến quản trị viên mạng LAN khi người dùng tin rằng việc chặn truy cập đến ứng dụng hoặc cấm thao tác với ứng dụng là do nhầm lẫn. Sau khi người dùng yêu cầu cung cấp quyền truy cập, Kaspersky Endpoint Security sẽ gửi một sự kiện đến Kaspersky Security Center: **Thông báo chặn truy cập thiết bị gửi đến quản trị viên.** Phần mô tả sự kiện chứa một thông báo cho quản trị viên với các biến được thay thế. Bạn có thể xem các sự kiện này trong bảng điều khiển Kaspersky Security Center bằng cách sử dụng lựa chọn sự kiện được định sẵn **User requests**. Nếu tổ chức của bạn chưa triển khai Kaspersky Security Center hoặc không có kết nối với Máy chủ quản trị thì ứng dụng sẽ gửi một thông báo cho quản trị viên tới địa chỉ email được chỉ định.

Kiểm soát ứng dụng

Thành phần Kiểm soát ứng dụng quản lý việc khởi động ứng dụng trên máy tính của người dùng. Điều này cho phép bạn thực hiện chính sách bảo mật của công ty khi sử dụng các ứng dụng. Thành phần Kiểm soát ứng dụng cũng làm giảm nguy cơ lây nhiễm máy tính bằng cách hạn chế quyền truy cập vào các ứng dụng.

Việc cấu hình Kiểm soát ứng dụng bao gồm các bước sau:

1. [Tạo danh mục ứng dụng.](#)

Quản trị viên sẽ tạo các danh mục ứng dụng mà quản trị viên muốn quản lý. Các danh mục ứng dụng dành cho tất cả các máy tính trong mạng công ty, bất kể các nhóm quản trị. Để tạo một danh mục, bạn có thể sử dụng các tiêu chí sau: Danh mục KL (ví dụ: *Trình duyệt*), giá trị băm của tập tin, nhà cung cấp ứng dụng và các tiêu chí khác.

2. [Tạo các Quy tắc kiểm soát ứng dụng.](#)

Quản trị viên sẽ tạo các quy tắc Kiểm soát ứng dụng trong chính sách cho nhóm quản trị. Quy tắc bao gồm các danh mục ứng dụng và trạng thái khởi động của các ứng dụng trong các danh mục này: bị chặn hoặc được phép.

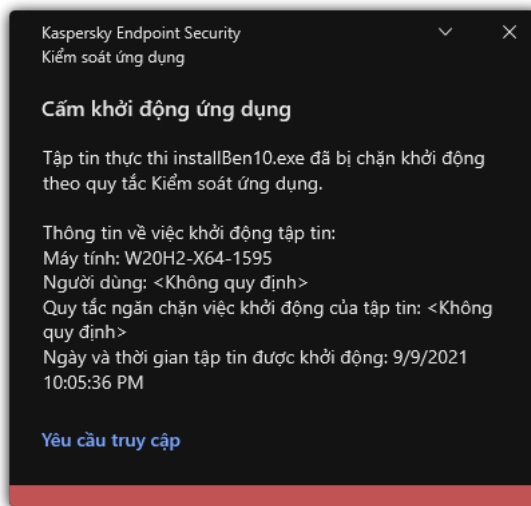
3. [Chọn chế độ Kiểm soát ứng dụng.](#)

Quản trị viên sẽ chọn chế độ làm việc với các ứng dụng không có trong bất kỳ quy tắc nào (danh sách ứng dụng không được phép và được phép).

Khi người dùng cố khởi chạy một ứng dụng bị cấm, Kaspersky Endpoint Security sẽ chặn ứng dụng đó khởi chạy và sẽ hiển thị một thông báo (xem hình bên dưới).

Một *chế độ thử nghiệm* được cung cấp để kiểm tra cấu hình của Kiểm soát ứng dụng. Trong chế độ này, Kaspersky Endpoint Security thực hiện các hoạt động sau:

- Cho phép khởi động ứng dụng, bao gồm cả những ứng dụng bị cấm.
- Hiển thị một thông báo về việc khởi động ứng dụng bị cấm và thêm thông tin vào báo cáo trên máy tính của người dùng.
- Gửi dữ liệu về việc khởi động các ứng dụng bị cấm đến Kaspersky Security Center.



Thông báo của Kiểm soát ứng dụng

Chế độ hoạt động của Kiểm soát ứng dụng

Thành phần Kiểm soát ứng dụng hoạt động ở hai chế độ:

- **Danh sách không được phép** Trong chế độ này, Kiểm soát ứng dụng cho phép người dùng khởi chạy tất cả các ứng dụng ngoại trừ các ứng dụng bị cấm trong Quy tắc kiểm soát ứng dụng.

Chế độ này của thành phần Kiểm soát ứng dụng được bật theo mặc định.

- **Danh sách được phép** Trong chế độ này, Kiểm soát ứng dụng chặn người dùng khởi chạy bất kỳ ứng dụng nào ngoại trừ các ứng dụng được phép và không bị cấm trong Quy tắc kiểm soát ứng dụng.

Nếu quy tắc cho phép của thành phần Kiểm soát ứng dụng được cấu hình đầy đủ, thành phần này sẽ chặn khởi chạy tất cả các ứng dụng mới chưa được xác minh bởi quản trị viên mạng LAN, đồng thời cho phép hoạt động của hệ điều hành và của các ứng dụng được tin tưởng mà người dùng phụ thuộc để thực hiện công việc của họ.

Bạn có thể đọc [các đề xuất về cấu hình Quy tắc kiểm soát ứng dụng trong chế độ danh sách được phép](#).

Bạn có thể cấu hình Kiểm soát ứng dụng để hoạt động ở các chế độ này bằng cả hai cách: sử dụng giao diện cục bộ của Kaspersky Endpoint Security và bằng cách sử dụng Kaspersky Security Center.

Tuy nhiên, Kaspersky Security Center cung cấp các công cụ không có sẵn trong giao diện cục bộ của Kaspersky Endpoint Security, ví dụ như các công cụ cần thiết cho các tác vụ sau:

- [Tạo danh mục ứng dụng](#).

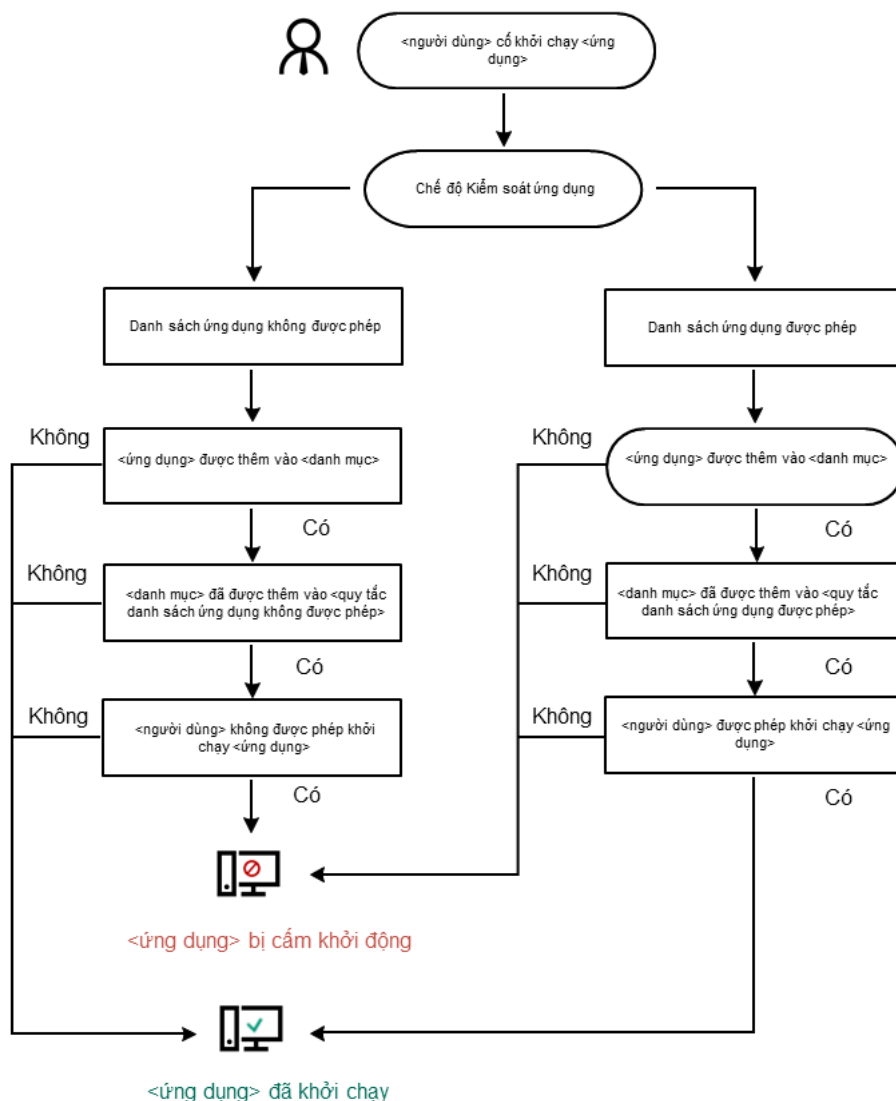
Quy tắc kiểm soát ứng dụng được tạo trong Bảng điều khiển quản trị Kaspersky Security Center dựa trên các danh mục ứng dụng tùy chỉnh của bạn chứ không dựa trên các điều kiện bao gồm và loại trừ như trong trường hợp trong giao diện cục bộ của Kaspersky Endpoint Security.

- [Tiếp nhận thông tin về các ứng dụng được cài đặt trên máy tính trong mạng LAN của công ty](#).

Đây là lý do tại sao bạn nên sử dụng Kaspersky Security Center để cấu hình hoạt động của thành phần Kiểm soát ứng dụng.

Thuật toán hoạt động của Kiểm soát ứng dụng

Kaspersky Endpoint Security sử dụng một thuật toán để đưa ra quyết định về việc khởi chạy một ứng dụng (xem hình bên dưới).



Thuật toán hoạt động của Kiểm soát ứng dụng

Cấu hình thành phần Kiểm soát ứng dụng

Tham số	Mô tả
Test mode	Nếu công tắc này được bật, Kaspersky Endpoint Security sẽ cho phép việc khởi động ứng dụng bị chặn trong chế độ Kiểm soát ứng dụng hiện tại, nhưng ghi lại thông tin về việc khởi động của nó trong báo cáo.
Application Control Mode	Bạn có thể chọn một trong các tùy chọn sau: <ul style="list-style-type: none"> • Danh sách không được phép Nếu mục này được chọn, Kiểm soát ứng dụng sẽ cho phép tất cả người dùng được bắt đầu bất kỳ ứng dụng nào, ngoại trừ các trường hợp thỏa mãn điều kiện trong quy tắc chặn của Kiểm soát ứng dụng. • Danh sách được phép Nếu mục này được chọn, Kiểm soát ứng dụng sẽ chặn tất cả người dùng khỏi việc bắt đầu bất kỳ ứng dụng nào, ngoại trừ trong các

	<p>trường hợp thỏa mãn điều kiện trong quy tắc cho phép của Kiểm soát ứng dụng.</p> <p>Khi chế độ Danh sách được phép được chọn, hai quy tắc Kiểm soát ứng dụng sẽ tự động được tạo:</p> <ul style="list-style-type: none"> • Tập tin ảnh hoàn hảo • Trình cập nhật được tin tưởng <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Bạn không thể sửa các thiết lập của hoặc xóa các quy tắc được tạo tự động. Bạn có thể bật hoặc tắt các quy tắc này.</p> </div>
<p>Control DLL modules load (significantly increases the load on the system)</p>	<p>Khi hộp kiểm này được lựa chọn, Kaspersky Endpoint Security sẽ kiểm soát việc tải các mô-đun DLL khi người dùng cố gắng khởi động ứng dụng. Thông tin về mô-đun DLL và ứng dụng đã tải mô-đun DLL sẽ được ghi lại trong báo cáo.</p> <div style="background-color: #f8d7da; padding: 10px; margin-top: 10px;"> <p>Khi bật chức năng kiểm soát quá trình nạp các mô-đun DLL và trình điều khiển, hãy đảm bảo rằng một trong các quy tắc sau đây được bật trong thiết lập Kiểm soát ứng dụng: quy tắc Tập tin ảnh hoàn hảo mặc định hoặc một quy tắc khác chứa danh mục KL "Chứng chỉ được tin tưởng" và đảm bảo rằng các mô-đun DLL và trình điều khiển được tin tưởng đã được nạp trước khi khởi chạy Kaspersky Endpoint Security. Việc bật tính năng kiểm soát nạp mô-đun DLL và trình điều khiển khi quy tắc Tập tin ảnh hoàn hảo bị tắt có thể gây bất ổn cho hệ điều hành.</p> </div> <p>Kaspersky Endpoint Security chỉ giám sát các mô-đun DLL và trình điều khiển được nạp kể từ khi hộp kiểm được chọn. Sau khi chọn hộp kiểm, bạn nên khởi động lại máy tính để đảm bảo rằng ứng dụng giám sát tất cả các mô-đun DLL và trình điều khiển, bao gồm những mô-đun và trình điều khiển được nạp trước khi Kaspersky Endpoint Security khởi động.</p>
<p>Message templates</p>	<p>Message about blocking Mẫu thông báo được hiển thị khi kích hoạt một quy tắc Kiểm soát ứng dụng chặn ứng dụng khởi chạy.</p> <p>Message to administrator Mẫu tin nhắn mà người dùng có thể gửi cho quản trị viên mạng LAN doanh nghiệp nếu người dùng tin rằng một ứng dụng bị chặn do nhầm lẫn. Sau khi người dùng yêu cầu cung cấp quyền truy cập, Kaspersky Endpoint Security sẽ gửi một sự kiện đến Kaspersky Security Center: Thông báo chặn việc khởi chạy ứng dụng gửi đến quản trị viên. Phần mô tả sự kiện chứa một thông báo cho quản trị viên với các biến được thay thế. Bạn có thể xem các sự kiện này trong bảng điều khiển Kaspersky Security Center bằng cách sử dụng lựa chọn sự kiện được định sẵn User requests. Nếu tổ chức của bạn chưa triển khai Kaspersky Security Center hoặc không có kết nối với Máy chủ quản trị thì ứng dụng sẽ gửi một thông báo cho quản trị viên tới địa chỉ email được chỉ định.</p>

Kiểm soát thích ứng sự cố

Thành phần này khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows dành cho máy trạm. Thành phần này không khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows cho máy chủ.

Thành phần Kiểm soát thích ứng sự cố sẽ giám sát và chặn các hành động mà các máy tính trong mạng công ty ít có khả năng thực hiện. Kiểm soát thích ứng sự cố sử dụng một bộ quy tắc để theo dõi các hành vi khác biệt (ví dụ, quy tắc *Khởi động Microsoft PowerShell từ ứng dụng văn phòng*). Các quy tắc này được tạo bởi các chuyên gia của Kaspersky dựa trên các tình huống hoạt động độc hại thông thường. Bạn có thể cấu hình cách Kiểm soát thích ứng sự cố xử lý từng quy tắc và, chẳng hạn, cho phép thực thi các kịch bản PowerShell tự động hóa một số tác vụ dòng công việc nhất định. Kaspersky Endpoint Security cập nhật ộ quy tắc cùng với các cơ sở dữ liệu ứng dụng. Cập nhật đến các bộ quy tắc phải được [xác nhận thủ công](#).

Thiết lập Kiểm soát thích ứng sự cố

Cấu hình Kiểm soát thích ứng sự cố bao gồm các bước sau:

1. Rèn luyện Kiểm soát thích ứng sự cố.

Sau khi bạn bật Kiểm soát thích ứng sự cố, các quy tắc của nó sẽ hoạt động trong *chế độ rèn luyện*. Trong quá trình rèn luyện, Kiểm soát thích ứng sự cố sẽ theo dõi việc kích hoạt quy tắc và gửi các sự kiện kích hoạt đến Kaspersky Security Center. Mỗi quy tắc đều có thời lượng rèn luyện riêng. Thời lượng của chế độ rèn luyện được quy định bởi các chuyên gia Kaspersky. Thông thường, chế độ rèn luyện sẽ hoạt động trong 2 tuần.

Nếu một quy tắc hoàn toàn không được kích hoạt trong quá trình huấn luyện, Kiểm soát thích ứng sự cố sẽ coi các hành động liên quan đến quy tắc này là ít gặp. Kaspersky Endpoint Security sẽ chặn mọi hành động liên quan đến quy tắc đó.

Nếu một quy tắc được kích hoạt trong quá trình rèn luyện, Kaspersky Endpoint Security sẽ ghi lại sự kiện này trong [báo cáo kích hoạt quy tắc](#) và kho lưu trữ **Triggering of rules in Smart Training state**.

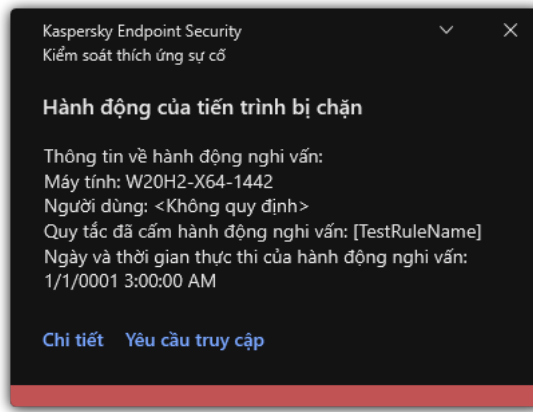
2. Phân tích báo cáo kích hoạt quy tắc.

Quản trị viên sẽ phân tích [báo cáo kích hoạt quy tắc](#) hoặc nội dung của kho lưu trữ **Triggering of rules in Smart Training state**. Sau đó, quản trị viên có thể lựa chọn hành vi của Kiểm soát thích ứng sự cố khi quy tắc này được kích hoạt: chặn hoặc cho phép nó. Quản trị viên cũng có thể tiếp tục giám sát cách hoạt động của quy tắc và kéo dài thời lượng của chế độ rèn luyện. Nếu quản trị viên không có hành động nào, ứng dụng cũng sẽ tiếp tục hoạt động trong chế độ rèn luyện. Thời lượng của chế độ rèn luyện được bắt đầu lại.

Kiểm soát thích ứng sự cố được cấu hình trong thời gian thực. Kiểm soát thích ứng sự cố được cấu hình qua các kênh sau:

- Kiểm soát thích ứng sự cố khởi chạy tự động để chặn các hành động liên kết với các quy tắc không bao giờ được kích hoạt trong chế độ rèn luyện.
- Kaspersky Endpoint Security bổ sung các quy tắc mới hoặc xóa các quy tắc đã lỗi thời.
- Quản trị viên cấu hình hoạt động của Kiểm soát thích ứng sự cố sau khi xem lại báo cáo kích hoạt quy tắc và nội dung của kho lưu trữ **Triggering of rules in Smart Training state**. Bạn nên kiểm tra báo cáo kích hoạt quy tắc và nội dung của kho lưu trữ **Triggering of rules in Smart Training state**.

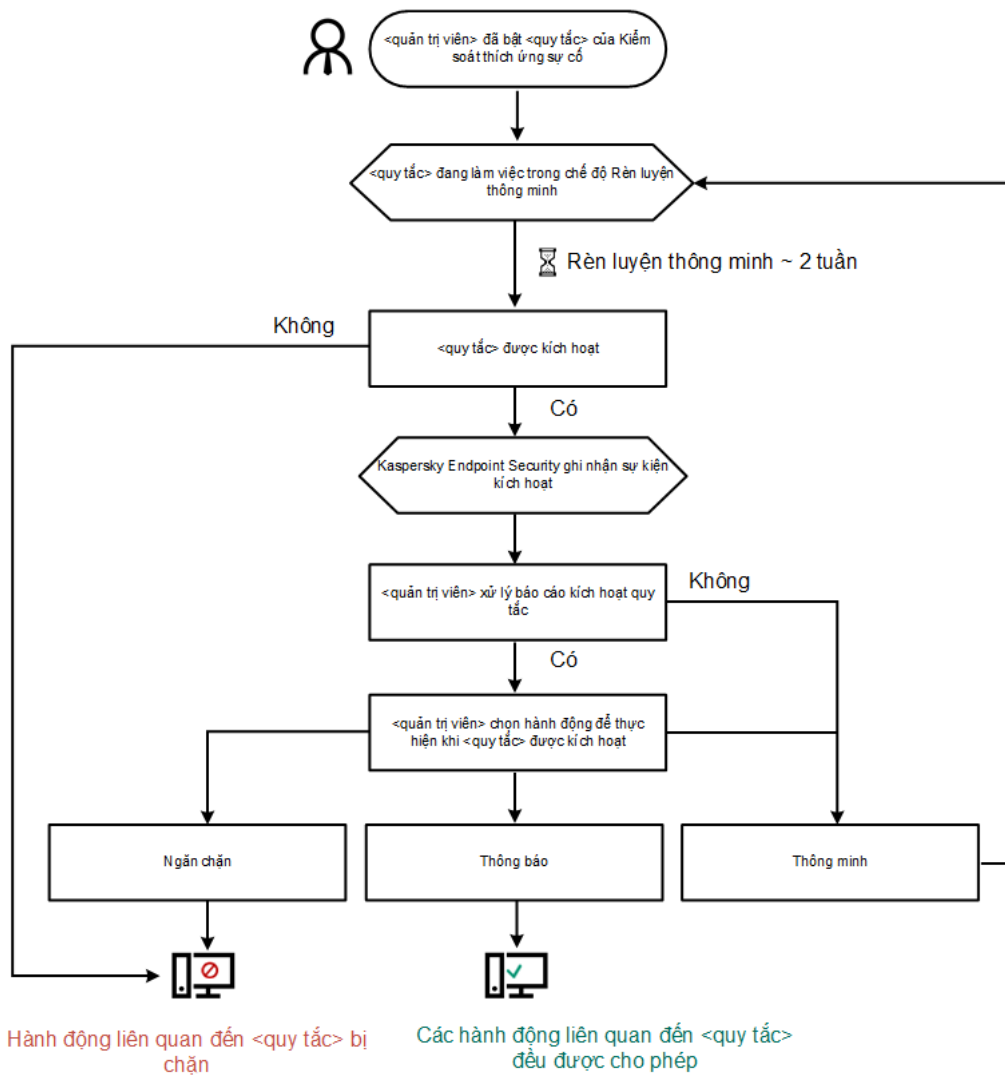
Khi một ứng dụng độc hại cố gắng thực hiện một hành động, Kaspersky Endpoint Security sẽ chặn hành động đó và hiển thị một thông báo (xem hình dưới đây).



Thông báo của Kiểm soát thích ứng sự cố

Thuật toán vận hành Kiểm soát thích ứng sự cố

Kaspersky Endpoint Security quyết định liệu có cho phép hay chặn một hành động liên kết với một quy tắc dựa trên thuật toán sau (xem hình dưới đây).



Thuật toán vận hành Kiểm soát thích ứng sự cố

Cấu hình thành phần Kiểm soát thích ứng sự cố

Tham số	Mô tả
Report	Báo cáo này chứa thông tin về trạng thái của quy tắc phát hiện Kiểm soát thích ứng sự

<p>on Adaptive Anomaly Control rules state</p> <p><i>(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)</i></p>	<p>cố (ví dụ, <i>Tắt</i> hoặc <i>Chặn</i>). Báo cáo này được tạo cho tất cả các nhóm quản trị.</p>
<p>Report on triggered rules of Adaptive Anomaly Control</p> <p><i>(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)</i></p>	<p>Báo cáo này chứa thông tin về các hành động ít gặp được phát hiện bằng cách sử dụng Kiểm soát thích ứng sự cố. Báo cáo này được tạo cho tất cả các nhóm quản trị.</p>
<p>Quy tắc</p>	<p>Bảng quy tắc Kiểm soát thích ứng sự cố. Các quy tắc này được tạo bởi các chuyên gia của Kaspersky dựa trên các tình huống hoạt động độc hại tiềm năng.</p>
<p>Mẫu</p>	<p>Tin nhắn về hoạt động chặn. Mẫu thông báo được hiển thị cho người dùng khi một quy tắc Kiểm soát thích ứng sự cố chặn một hành động ít gặp.</p> <p>Thông điệp đến quản trị viên. Khuôn mẫu thông báo mà người dùng có thể gửi đến quản trị viên mạng doanh nghiệp cục bộ nếu người dùng cho rằng việc chặn là do nhầm lẫn. Sau khi người dùng yêu cầu cung cấp quyền truy cập, Kaspersky Endpoint Security sẽ gửi một sự kiện đến Kaspersky Security Center: Thông báo chặn hoạt động của ứng dụng gửi đến quản trị viên. Phần mô tả sự kiện chứa một thông báo cho quản trị viên với các biến được thay thế. Bạn có thể xem các sự kiện này trong bảng điều khiển Kaspersky Security Center bằng cách sử dụng lựa chọn sự kiện được định sẵn User requests. Nếu tổ chức của bạn chưa triển khai Kaspersky Security Center hoặc không có kết nối với Máy chủ quản trị thì ứng dụng sẽ gửi một thông báo cho quản trị viên tới địa chỉ email được chỉ định.</p>

Cảm biến điểm cuối

Cảm biến điểm cuối không được kèm theo Kaspersky Endpoint Security 11.4.0.

Bạn có thể quản lý Cảm biến điểm cuối trong Bảng điều khiển web Kaspersky Security Center và trong Bảng điều khiển quản trị Kaspersky Security Center. Không thể quản lý Cảm biến điểm cuối trong Bảng điều khiển đám mây Kaspersky Security Center.

Cảm biến điểm cuối được thiết kế để tương tác với Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* là một giải pháp được thiết kế để phát hiện kịp thời các mối đe dọa tinh vi, chẳng hạn như các cuộc tấn công chủ đích, các mối đe dọa dai dẳng nâng cao (APT), các cuộc tấn công zero-day, v.v. Kaspersky Anti Targeted Attack Platform bao gồm hai khối chức năng: Kaspersky Anti Targeted Attack (sau đây còn được gọi là "KATA") và Kaspersky Endpoint Detection and Response (sau đây còn được gọi là "KEDR"). Bạn có thể mua KEDR riêng. Để biết chi tiết về giải pháp này, vui lòng tham khảo [Trợ giúp của Kaspersky Anti Targeted Attack Platform](#).

Việc quản lý Cảm biến điểm cuối có những hạn chế sau:

- Bạn có thể cấu hình thiết lập Cảm biến điểm cuối trong chính sách với điều kiện Kaspersky Endpoint Security phiên bản 11.0.0 đến 11.3.0 được cài đặt trên máy tính. Để biết thêm thông tin về cách cấu hình thiết lập Cảm biến điểm cuối bằng chính sách, hãy tham khảo các [bài viết trợ giúp cho các phiên bản trước của Kaspersky Endpoint Security](#).
- Nếu Kaspersky Endpoint Security phiên bản 11.4.0 trở lên được cài đặt trên máy tính, bạn không thể cấu hình thiết lập Cảm biến điểm cuối trong chính sách.

Cảm biến điểm cuối 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. Cảm biến điểm cuối chuyển tiếp thông tin đến máy chủ KATA.

Chức năng thành phần có thể được sử dụng trong các hệ điều hành sau:

- Windows 7 Service Pack 1 Home / Professional / Enterprise;
- Windows 8.1.1 Professional / Enterprise;
- Windows 10 RS3 Home / Professional / Education / Enterprise;
- Windows 10 RS4 Home / Professional / Education / Enterprise;
- Windows 10 RS5 Home / Professional / Education / Enterprise;
- Windows 10 RS6 Home / Professional / Education / Enterprise;
- Windows Server 2008 R2 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2012 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2012 R2 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2016 Essentials / Standard (64-bit).

Để biết thông tin chi tiết về hoạt động của KATA, hãy tham khảo [Trợ giúp của Kaspersky Anti Targeted Attack Platform](#).

Kaspersky Sandbox

Kaspersky Endpoint Security 11.7.0 hiện đã có một tác nhân tích hợp để tích hợp với giải pháp Kaspersky Sandbox. *Giải pháp Kaspersky Sandbox* phát hiện và tự động chặn các mối đe dọa nâng cao trên máy tính. Kaspersky Sandbox sẽ phân tích hành vi của đối tượng để phát hiện hoạt động độc hại và hoạt động đặc trưng của các cuộc tấn công có chủ đích vào cơ sở hạ tầng CNTT của tổ chức. Kaspersky Sandbox sẽ phân tích và quét các đối tượng trên các máy chủ đặc biệt chứa các ảnh máy ảo được triển khai của hệ điều hành Microsoft Windows (máy chủ Kaspersky Sandbox). Để biết chi tiết về giải pháp này, hãy tham khảo [Trợ giúp của Kaspersky Sandbox](#).

Chỉ có thể quản lý thành phần này bằng Bảng điều khiển web Kaspersky Security Center. Bạn không thể quản lý thành phần này bằng Bảng điều khiển quản trị (MMC).

Thiết lập thành phần Kaspersky Sandbox

Tham số	Mô tả
Server TLS certificate	Để cấu hình kết nối được tin tưởng với máy chủ Kaspersky Sandbox, bạn phải chuẩn bị chứng chỉ TLS. Tiếp theo, bạn phải thêm chứng chỉ vào máy chủ Kaspersky Sandbox và chính sách Kaspersky Endpoint Security. Để biết chi tiết về cách chuẩn bị chứng chỉ và thêm chứng chỉ vào máy chủ, hãy tham khảo Trợ giúp của Kaspersky Sandbox .
Thời gian chờ	Thời gian chờ kết nối cho máy chủ Kaspersky Sandbox. Sau khi hết thời gian chờ đã được cấu hình, Kaspersky Endpoint Security sẽ gửi yêu cầu đến máy chủ tiếp theo. Bạn có thể tăng thời gian chờ kết nối cho Kaspersky Sandbox nếu tốc độ kết nối của bạn thấp hoặc nếu kết nối không ổn định. Thời gian chờ của yêu cầu được khuyến nghị là từ 0.5 giây trở xuống.
Kaspersky Sandbox request queue	Kích thước của thư mục hàng chờ yêu cầu. Khi một đối tượng được truy cập trên máy tính (tệp thực thi được khởi chạy hoặc tài liệu được mở, ví dụ như ở định dạng DOCX hoặc PDF), Kaspersky Endpoint Security cũng có thể gửi đối tượng cần quét bởi Kaspersky Sandbox. Nếu có nhiều yêu cầu, Kaspersky Endpoint Security sẽ tạo một hàng chờ yêu cầu. Theo mặc định, kích thước của thư mục hàng chờ yêu cầu được giới hạn ở 100 MB. Sau khi đạt đến kích thước tối đa, Kaspersky Sandbox ngừng thêm các yêu cầu mới vào hàng chờ và gửi sự kiện tương ứng đến Kaspersky Security Center. Bạn có thể cấu hình kích thước của thư mục hàng đợi yêu cầu tùy thuộc vào cấu hình máy chủ của bạn.
Máy chủ Kaspersky Sandbox	Thiết lập kết nối máy chủ Kaspersky Sandbox. Các máy chủ sử dụng ảnh máy ảo đã triển khai của hệ điều hành Microsoft Windows để chạy các đối tượng cần được quét. Bạn có thể nhập địa chỉ IP (IPv4 hoặc IPv6) hoặc tên miền đầy đủ.
Hành động khi phát hiện mối đe dọa	<p>Di chuyển bản sao vào Khu vực cách ly, xóa đối tượng. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ xóa đối tượng độc hại được tìm thấy trên máy tính. Trước khi xóa đối tượng, Kaspersky Endpoint Security sẽ tạo một bản sao lưu trong trường hợp đối tượng cần được khôi phục sau này. Kaspersky Endpoint Security sẽ di chuyển bản sao lưu vào Khu vực cách ly.</p> <p>Chạy tác vụ quét các khu vực quan trọng. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ chạy tác vụ 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.</p> <p>Tạo một tác vụ Quét IOC. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ tự động tạo tác vụ Quét IOC (tác vụ quét IOC tự động). Đối với tác vụ này, bạn có thể cấu hình chế độ chạy, phạm vi quét và hành động khi phát hiện IOC: xóa đối tượng, chạy tác vụ Quét khu vực quan trọng. Để sửa đổi các thiết lập khác của tác vụ Quét IOC, hãy vào mục thiết lập tác vụ.</p>

Phạm vi quét IOC	<p>Các khu vực tập tin quan trọng. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security chỉ thực hiện quét IOC trong các khu vực tập tin quan trọng của máy tính: bộ nhớ kernel và các sector khởi động.</p> <p>Các khu vực tập tin trên ổ đĩa hệ thống của máy tính. NẾU tùy chọn này được chọn, Kaspersky Endpoint Security sẽ thực hiện quét IOC trên ổ đĩa hệ thống của máy tính.</p>
Chạy tác vụ quét IOC	<p>Thủ công. Chế độ chạy trong đó bạn có thể khởi chạy tác vụ <i>Quét IOC</i> theo cách thủ công tại thời điểm bạn chọn.</p> <p>Sau khi mỗi đe dọa được phát hiện. Chế độ chạy trong đó Kaspersky Endpoint Security sẽ chạy tác vụ <i>Quét IOC</i> tự động bất cứ khi nào một mối đe dọa được phát hiện.</p> <p>Chỉ chạy khi máy tính đang rảnh. Chế độ chạy trong đó Kaspersky Endpoint Security sẽ chạy <i>Quét IOC</i> nếu trình bảo vệ màn hình đang hoạt động hoặc màn hình bị khóa. Nếu người dùng mở khóa máy tính, Kaspersky Endpoint Security sẽ tạm dừng tác vụ. Điều này có nghĩa là tác vụ có thể mất vài ngày để hoàn thành.</p>

Endpoint Detection and Response

Kaspersky Endpoint Security 11.7.0 đã có một tác nhân tích hợp cho giải pháp Kaspersky Endpoint Detection and Response Optimum (sau đây gọi là "EDR Optimum"). Kaspersky Endpoint Security 11.8.0 đã có một tác nhân tích hợp cho giải pháp Kaspersky Endpoint Detection and Response Expert (sau đây gọi là "EDR Expert"). *Kaspersky Endpoint Detection and Response* là một loạt các giải pháp để bảo vệ cơ sở hạ tầng CNTT của doanh nghiệp trước các mối đe dọa mạng nâng cao. Chức năng của các giải pháp này kết hợp tính năng tự động phát hiện các mối đe dọa với khả năng phản ứng trước các mối đe dọa này để chống lại các cuộc tấn công nâng cao, bao gồm các cuộc tấn công khai thác mới, phần mềm tống tiền, các cuộc tấn công không dùng tập tin, cũng như các phương pháp sử dụng các công cụ hệ thống hợp pháp. EDR Expert cung cấp nhiều chức năng giám sát và phản ứng trước mối đe dọa hơn EDR Optimum. Để biết chi tiết về các giải pháp, hãy xem [Trợ giúp của Kaspersky Endpoint Detection and Response Optimum](#) và [Trợ giúp của Kaspersky Endpoint Detection and Response Expert](#).

Kaspersky Endpoint Detection and Response sẽ đánh giá và phân tích sự phát triển của mối đe dọa và cung cấp cho *nhân viên an ninh* hoặc *Quản trị viên* thông tin về cuộc tấn công tiềm ẩn cần thiết để có phản ứng kịp thời. Kaspersky Endpoint Detection and Response sẽ hiển thị thông tin chi tiết về việc phát hiện trong một cửa sổ riêng. *Chi tiết về phát hiện* là một công cụ để xem toàn bộ thông tin thu thập được về một mối đe dọa được phát hiện. Chi tiết về phát hiện bao gồm, ví dụ như lịch sử của các tập tin xuất hiện trên máy tính. Để biết chi tiết về việc quản lý thông tin chi tiết về phát hiện, hãy tham khảo [Trợ giúp của Kaspersky Endpoint Detection and Response Optimum](#) và [Trợ giúp của Kaspersky Endpoint Detection and Response Expert](#).

Bạn có thể cấu hình thành phần EDR Optimum trong Bảng điều khiển web và Bảng điều khiển đám mây. Thiết lập thành phần cho EDR Expert chỉ khả dụng trong Bảng điều khiển đám mây.

Thiết lập Endpoint Detection and Response

Tham số	Mô tả
Cách ly mạng	<p>Tự động cách ly máy tính khỏi mạng để đối phó với các mối đe dọa được phát hiện. Khi bật chế độ cách ly mạng, ứng dụng sẽ cắt tất cả các kết nối đang hoạt động và chặn tất cả các kết nối TCP/IP mới trên máy tính. Ứng dụng chỉ để lại các kết nối sau hoạt động:</p> <ul style="list-style-type: none"> Các kết nối được liệt kê trong loại trừ Cách ly mạng. Các kết nối được khởi tạo bởi các dịch vụ Kaspersky Endpoint Security.

	<ul style="list-style-type: none"> • Các kết nối do Trình khách quản trị Kaspersky Security Center.
Tự động mở khóa máy tính bị cách ly sau N giờ	Tính năng cách ly mạng có thể được tắt tự động sau một thời gian nhất định hoặc theo cách thủ công. Theo mặc định, Kaspersky Endpoint Security sẽ tắt chế độ Cách ly mạng 5 giờ sau khi bắt đầu cách ly.
Network isolation exclusions	<p>Danh sách các quy tắc loại trừ khỏi cách ly mạng. Các kết nối mạng phù hợp với quy tắc không bị chặn trên máy tính khi chế độ Cách ly mạng được bật.</p> <p>Để cấu hình các loại trừ Cách ly mạng, bạn có thể sử dụng một danh sách <i>các cấu hình mạng tiêu chuẩn</i>. Theo mặc định, các loại trừ bao gồm các cấu hình mạng chứa các quy tắc đảm bảo hoạt động không bị gián đoạn của các thiết bị có máy chủ DNS/DHCP và các vai trò máy khách DNS/DHCP. Bạn cũng có thể sửa đổi thiết lập của các cấu hình mạng tiêu chuẩn hoặc định nghĩa các loại trừ theo cách thủ công.</p> <div style="background-color: #f8d7da; padding: 10px; margin-top: 10px;"> <p>Các loại trừ được chỉ định trong thuộc tính chính sách chỉ được áp dụng nếu chế độ Cách ly mạng được bật tự động để ứng phó với mối đe dọa được phát hiện. Các loại trừ được chỉ định trong các thuộc tính máy tính chỉ được áp dụng nếu chế độ Cách ly mạng được bật theo cách thủ công trong các thuộc tính máy tính, trong bảng điều khiển của Kaspersky Security Center hoặc trong chi tiết về cảnh báo.</p> </div>
Phòng chống thực thi	Kiểm soát việc thực thi các tập tin và tập lệnh thực thi và mở các tập tin định dạng văn phòng. Ví dụ: bạn có thể ngăn việc thực thi các ứng dụng được coi là không bảo mật trên máy tính đã chọn. Phòng chống thực thi hỗ trợ một tập hợp các phần mở rộng tập tin văn phòng và một tập hợp các trình thông dịch tập lệnh .
Action on execution or opening of forbidden object	<p>Block and write to report. Trong chế độ này, ứng dụng chặn việc thực thi các đối tượng hoặc mở các tài liệu đáp ứng với tiêu chí quy tắc ngăn chặn. Ứng dụng cũng phát hành một sự kiện về nỗ lực thực thi các đối tượng hoặc mở tài liệu vào nhật ký sự kiện Windows và nhật ký sự kiện của Kaspersky Security Center.</p> <p>Log events only. Trong chế độ này, Kaspersky Endpoint Security sẽ phát hành một sự kiện về nỗ lực chạy các đối tượng thực thi hoặc mở tài liệu đáp ứng với tiêu chí quy tắc ngăn chặn vào nhật ký sự kiện Windows và Kaspersky Security Center, nhưng không chặn nỗ lực chạy hoặc mở đối tượng hoặc tài liệu. Chế độ này được chọn theo mặc định.</p>
Quy tắc phòng chống thực thi	Danh sách các quy tắc phòng chống thực thi đối tượng. <i>Quy tắc phòng chống thực thi</i> là một tập hợp các tiêu chí mà ứng dụng xem xét khi phản ứng với hoạt động thực thi đối tượng, ví dụ khi chặn thực thi đối tượng. Ứng dụng xác định các tập tin bằng đường dẫn hoặc giá trị tổng kiểm của chúng được tính bằng thuật toán băm MD5 và SHA256.

Mã hóa toàn bộ ổ đĩa

Bạn có thể chọn một công nghệ mã hóa: Kaspersky Disk Encryption hoặc BitLocker Drive Encryption (sau đây cũng được gọi tắt là "BitLocker").

Kaspersky Disk Encryption

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 [Manage Authentication Agent accounts](#). 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 cũng có thể [sử dụng công nghệ Single Sign-On \(SSO\)](#), cho phép bạn tự động đăng nhập vào hệ điều hành bằng tên người dùng và mật khẩu của tài khoản Authentication Agent.

Việc xác thực người dùng trong Authentication Agent có thể được thực hiện bằng hai cách:

- Nhập vào 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.

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.

BitLocker Drive Encryption

BitLocker là một công nghệ mã hóa được tích hợp trong các hệ điều hành Windows. Kaspersky Endpoint Security cho phép bạn kiểm soát và quản lý BitLocker bằng Kaspersky Security Center. BitLocker mã hóa các phân vùng luận lý. Không thể sử dụng BitLocker để mã hóa các ổ đĩa di động. Để biết thêm chi tiết về BitLocker, hãy tham khảo [tài liệu của Microsoft](#).

BitLocker cung cấp ổ lưu trữ an toàn các khóa truy cập bằng mô-đun nền tảng được tin tưởng. *Mô-đun Nền tảng Tin tưởng (TPM)* là một vi mạch được phát triển để cung cấp các chức năng cơ bản liên quan đến bảo mật (ví dụ: để lưu trữ khóa mã hóa). Mô-đun nền tảng được tin tưởng thường được cài đặt trên bảng mạch chủ máy tính và tương tác với tất cả các thành phần hệ thống khác thông qua bus phần cứng. Sử dụng TPM là cách an toàn nhất để lưu trữ khóa truy cập BitLocker, vì TPM cung cấp xác minh tính toàn vẹn của hệ thống trước khi khởi động. Bạn vẫn có thể mã hóa ổ đĩa trên máy tính mà không cần có TPM. Trong trường hợp này, khóa truy cập sẽ được mã hóa bằng mật khẩu. BitLocker sử dụng các phương thức xác thực sau:

- TPM.
- TPM và mã PIN.
- Mật khẩu.

Sau khi mã hóa ổ đĩa, BitLocker sẽ tạo khóa chủ. Kaspersky Endpoint Security sẽ gửi khóa chủ đến Kaspersky Security Center để bạn có thể [khôi phục quyền truy cập vào ổ đĩa](#), ví dụ như nếu người dùng quên mật khẩu.

Nếu người dùng mã hóa ổ đĩa bằng BitLocker, Kaspersky Endpoint Security sẽ gửi [thông tin về mã hóa ổ đĩa đến Kaspersky Security Center](#). Tuy nhiên, Kaspersky Endpoint Security sẽ không gửi khóa chủ tới Kaspersky Security Center, do đó sẽ không thể khôi phục quyền truy cập vào đĩa bằng Kaspersky Security Center. Để BitLocker hoạt động chính xác với Kaspersky Security Center, [hãy giải mã ổ đĩa](#) và [mã hóa lại ổ đĩa](#) bằng một chính sách. Bạn có thể giải mã ổ đĩa một cách cục bộ hoặc sử dụng một chính sách.

Sau khi mã hóa ổ cứng hệ thống, người dùng cần thực hiện xác thực BitLocker để khởi động hệ điều hành. Sau quy trình xác thực, BitLocker sẽ cho phép người dùng đăng nhập. BitLocker không hỗ trợ công nghệ đăng nhập một lần (SSO).

Nếu bạn đang sử dụng các chính sách nhóm của Windows, hãy tắt quản lý BitLocker trong thiết lập chính sách. Thiết lập chính sách của Windows có thể xung đột với thiết lập chính sách của Kaspersky Endpoint Security. Lỗi có thể xảy ra khi mã hóa một ổ đĩa.

Thiết lập thành phần Kaspersky Disk Encryption

Tham số	Mô tả
Chế độ mã hóa	<p>Mã hóa tất cả ổ đĩa cứng. Nếu mục này được chọn, ứng dụng sẽ mã hóa tất cả các ổ cứng khi chính sách được áp dụng.</p> <p>Nếu máy tính có cài đặt nhiều hệ điều hành, sau khi mã hóa bạn sẽ chỉ có thể nạp hệ điều hành đã cài đặt ứng dụng.</p> <p>Giải mã tất cả đĩa cứng. Nếu mục này được chọn, ứng dụng sẽ giải mã tất cả các ổ cứng đã được mã hóa từ trước khi chính sách được áp dụng.</p> <p>Giữ nguyên. Nếu mục này được lựa chọn, ứng dụng sẽ để nguyên các ổ đĩa trong trạng thái trước đó của chúng khi chính sách được áp dụng. Nếu ổ đĩa đã được mã hóa, nó vẫn sẽ duy trì tình trạng mã hóa. Nếu ổ đĩa đã được giải mã, nó vẫn sẽ duy trì tình trạng giải mã. Mục này được chọn theo mặc định.</p>
Tự động tạo các tài khoản Authentication Agent cho người dùng Windows trong quá trình mã hóa	<p>Nếu hộp kiểm này được chọn, ứng dụng sẽ tạo tài khoản Authentication Agent dựa trên danh sách tài khoản người dùng Windows trên máy tính. Theo mặc định, Kaspersky Endpoint Security sử dụng tất cả các tài khoản cục bộ và tên miền mà người dùng đã sử dụng để đăng nhập vào hệ điều hành trong 30 ngày qua.</p>
Thiết lập tạo tài khoản Authentication Agent	<p>Tất cả tài khoản trên máy tính. Tất cả các tài khoản trên máy tính đã hoạt động bất kỳ lúc nào.</p> <p>Tất cả các tài khoản domain trên máy tính. Tất cả các tài khoản trên máy tính thuộc về một tên miền và đã hoạt động bất kỳ lúc nào.</p> <p>Tất cả tài khoản nội bộ trên máy tính. Tất cả các tài khoản cục bộ trên máy tính đã hoạt động bất kỳ lúc nào.</p> <p>Tài khoản dịch vụ có mật khẩu dùng một lần. Cần có tài khoản dịch vụ để có quyền truy cập vào máy tính, như khi người dùng quên mật khẩu. Bạn cũng có thể sử dụng tài khoản dịch vụ như tài khoản dự trữ. Bạn phải nhập tên của tài khoản (mặc định là ServiceAccount). Kaspersky Endpoint Security sẽ tạo mật khẩu tự động. Bạn có thể tìm thấy mật khẩu trong bảng điều khiển Kaspersky Security Center.</p> <p>Quản trị nội bộ. Kaspersky Endpoint Security sẽ tạo tài khoản người dùng Authentication Agent cho quản trị viên cục bộ của máy tính.</p> <p>Quản lý máy tính. Kaspersky Endpoint Security sẽ tạo tài khoản người dùng Authentication Agent cho tài khoản của người quản lý máy tính. Bạn có thể xem tài khoản nào có vai trò người quản lý máy tính trong thuộc tính máy tính trong Active Directory. Theo mặc định, vai trò người quản lý máy tính không được định nghĩa, tức là nó không tương ứng với bất kỳ tài khoản nào.</p> <p>Kích hoạt tài khoản. Kaspersky Endpoint Security sẽ tự động tạo tài khoản Authentication Agent cho tài khoản đang hoạt động tại thời điểm mã hóa ổ đĩa.</p>
Tự động tạo các tài khoản Authentication	<p>Nếu hộp kiểm này được chọn, ứng dụng sẽ kiểm tra thông tin về tài khoản người dùng Windows trên máy tính trước khi khởi chạy Authentication Agent. Nếu Kaspersky Endpoint Security phát hiện tài khoản người dùng Windows</p>

<p>Agent cho mọi người dùng của máy tính này sau khi đăng nhập</p>	<p>không có tài khoản Authentication Agent, ứng dụng sẽ tạo một tài khoản mới để truy cập các ổ đĩa được mã hóa. Tài khoản Authentication Agent mới sẽ có các thiết lập mặc định sau: chỉ cho phép đăng nhập được bảo vệ bằng mật khẩu và thay đổi mật khẩu trong lần xác thực đầu tiên. Do đó, bạn không cần phải thêm tài khoản Authentication Agent theo cách thủ công bằng cách sử dụng tác vụ <i>Quản lý tài khoản Authentication Agent</i> cho máy tính có ổ đĩa đã được mã hóa.</p>
<p>Lưu tên người dùng đã nhập vào Authentication Agent</p>	<p>Nếu hộp kiểm này được chọn, ứng dụng sẽ lưu lại tên của tài khoản Authentication Agent. Bạn sẽ không được yêu cầu nhập tên tài khoản ở lần nhập thông tin xác thực tiếp theo trong Authentication Agent cho cùng tài khoản.</p>
<p>Chỉ mã hóa dung lượng ổ đĩa được sử dụng (giảm thời gian mã hóa)</p>	<p>Hộp kiểm này bật / tắt tùy chọn chỉ giới hạn khu vực mã hóa đến các phần ổ cứng đang được sử dụng. Giới hạn này sẽ giúp bạn giảm thời gian mã hóa.</p> <div data-bbox="413 622 1493 817" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Việc bật hoặc tắt tính năng Chỉ mã hóa dung lượng ổ đĩa được sử dụng (Windows 8 và các phiên bản mới hơn) sau khi bắt đầu mã hóa sẽ không sửa đổi thiết lập này cho đến khi các ổ cứng được giải mã. Bạn phải chọn hoặc xóa hộp kiểm trước khi bắt đầu mã hóa.</p> </div> <p>Nếu hộp kiểm này được chọn, chỉ các phần của ổ cứng có chứa các tập tin mới được mã hóa. Kaspersky Endpoint Security sẽ tự động mã hóa dữ liệu mới khi chúng được bổ sung.</p> <p>Nếu hộp kiểm này bị xóa, toàn bộ ổ cứng sẽ được mã hóa, bao gồm các phần sót lại của những tập tin đã được sửa đổi hoặc bị xóa trước đó.</p> <div data-bbox="413 1086 1493 1312" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Tùy chọn này được khuyến nghị cho các ổ cứng mới có dữ liệu chưa được sửa đổi hoặc bị xóa. Nếu bạn đang áp dụng mã hóa trên một ổ cứng đang được sử dụng, bạn nên mã hóa toàn bộ ổ cứng. Điều này sẽ đảm bảo toàn bộ dữ liệu được bảo vệ, kể cả những dữ liệu đã bị xóa và có khả năng được phục hồi.</p> </div> <p>Hộp kiểm này được xóa ở chế độ mặc định.</p>
<p>Sử dụng Hỗ trợ USB chuẩn cũ (không khuyến dùng)</p>	<p>Hộp kiểm này bật/tắt chức năng Hỗ trợ USB chuẩn cũ. <i>Hỗ trợ USB chuẩn cũ là một chức năng của BIOS/UEFI</i>, cho phép bạn sử dụng các thiết bị USB (như token bảo mật) trong thời gian khởi động của máy tính trước khi khởi động hệ điều hành (chế độ BIOS). Chức năng Hỗ trợ USB chuẩn cũ không ảnh hưởng đến hỗ trợ cho các thiết bị USB sau khi hệ điều hành đã được khởi động.</p> <p>Nếu hộp kiểm này được chọn, tính năng hỗ trợ cho các thiết bị USB trong quá trình khởi động máy tính ban đầu sẽ được bật.</p> <div data-bbox="413 1731 1493 1926" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0; background-color: #f8d7da;"> <p>Khi chức năng Hỗ trợ USB chuẩn cũ được bật, Authentication Agent ở chế độ BIOS không hỗ trợ làm việc với các token qua USB. Bạn chỉ nên sử dụng tùy chọn này khi có vấn đề về tương thích phần cứng và chỉ dành cho các máy tính gặp phải vấn đề này.</p> </div>
<p>Thiết lập mật khẩu</p>	<p>Thiết lập độ mạnh của mật khẩu tài khoản Authentication Agent. Bạn cũng có thể bật sử dụng công nghệ Single Sign-On (SSO).</p> <p>Công nghệ SSO cho phép bạn có thể sử dụng cùng một chứng chỉ tài khoản để truy cập các ổ cứng được mã hóa và đăng nhập vào hệ điều hành.</p>

	<p>Nếu hộp kiểm này được chọn, bạn sẽ phải nhập thông tin tài khoản để truy cập các ổ cứng được mã hóa và sau đó tự động đăng nhập vào hệ điều hành.</p> <p>Nếu hộp kiểm này bị xóa, bạn sẽ phải nhập riêng thông tin truy cập vào các ổ cứng được mã hóa và thông tin tài khoản người dùng của hệ điều hành để truy cập vào các ổ cứng được mã hóa và sau đó là đăng nhập vào hệ điều hành.</p>
Help texts	<p>Chứng thực. Văn bản trợ giúp xuất hiện trong cửa sổ Authentication Agent khi nhập thông tin đăng nhập tài khoản.</p> <p>Thay đổi mật khẩu. Văn bản trợ giúp xuất hiện trong cửa sổ Authentication Agent khi thay đổi mật khẩu cho tài khoản Authentication Agent.</p> <p>Phục hồi mật khẩu. Văn bản trợ giúp xuất hiện trong cửa sổ Authentication Agent khi khôi phục mật khẩu cho tài khoản Authentication Agent.</p>

Thiết lập thành phần BitLocker Drive Encryption

Tham số	Mô tả
Chế độ mã hóa	<p>Mã hóa tất cả ổ đĩa cứng. Nếu mục này được chọn, ứng dụng sẽ mã hóa tất cả các ổ cứng khi chính sách được áp dụng.</p> <div style="background-color: #f8d7da; padding: 10px; margin: 10px 0;"> <p>Nếu máy tính có cài đặt nhiều hệ điều hành, sau khi mã hóa bạn sẽ chỉ có thể nạp hệ điều hành đã cài đặt ứng dụng.</p> </div> <p>Giải mã tất cả đĩa cứng. Nếu mục này được chọn, ứng dụng sẽ giải mã tất cả các ổ cứng đã được mã hóa từ trước khi chính sách được áp dụng.</p> <p>Giữ nguyên. Nếu mục này được lựa chọn, ứng dụng sẽ để nguyên các ổ đĩa trong trạng thái trước đó của chúng khi chính sách được áp dụng. Nếu ổ đĩa đã được mã hóa, nó vẫn sẽ duy trì tình trạng mã hóa. Nếu ổ đĩa đã được giải mã, nó vẫn sẽ duy trì tình trạng giải mã. Mục này được chọn theo mặc định.</p>
Cần nhập liệu bàn phím trong quá trình tiền khởi động để bật xác thực BitLocker trên máy tính bảng	<p>Hộp kiểm này bật / tắt quá trình xác thực đòi hỏi nhập liệu trong một môi trường tiền khởi động, kể cả khi nền tảng này không có khả năng nhập liệu trong môi trường tiền khởi động (ví dụ, máy tính bảng có bàn phím cảm ứng).</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Màn hình cảm ứng của máy tính bảng không khả dụng trong môi trường tiền khởi động. Để hoàn tất xác thực BitLocker trên máy tính bảng, người dùng phải kết nối một bàn phím USB.</p> </div> <p>Nếu hộp kiểm này được chọn, việc sử dụng quá trình xác thực đòi hỏi nhập liệu tiền khởi động sẽ được cho phép. Bạn chỉ nên sử dụng thiết lập này cho các thiết bị có công cụ nhập liệu thay thế trong một môi trường tiền khởi động, ví dụ như bàn phím USB ngoài bàn phím cảm ứng.</p> <p>Nếu hộp kiểm bị xóa thì BitLocker Drive Encryption không khả dụng trên máy tính bảng.</p>
Sử dụng mã hóa phần cứng	<p>Nếu hộp kiểm này được chọn, ứng dụng sẽ áp dụng mã hóa phần cứng. Việc này cho phép bạn tăng tốc độ mã hóa và sử dụng ít tài nguyên máy tính hơn.</p>
Chỉ mã hóa dung lượng ổ đĩa được sử dụng (Windows 8 và các phiên bản mới hơn)	<p>Hộp kiểm này bật / tắt tùy chọn chỉ giới hạn khu vực mã hóa đến các phần ổ cứng đang được sử dụng. Giới hạn này sẽ giúp bạn giảm thời gian mã hóa.</p>

Việc bật hoặc tắt tính năng **Chỉ mã hóa dung lượng ổ đĩa được sử dụng (Windows 8 và các phiên bản mới hơn)** sau khi bắt đầu mã hóa sẽ không sửa đổi thiết lập này cho đến khi các ổ cứng được giải mã. Bạn phải chọn hoặc xóa hộp kiểm trước khi bắt đầu mã hóa.

Nếu hộp kiểm này được chọn, chỉ các phần của ổ cứng có chứa các tập tin mới được mã hóa. Kaspersky Endpoint Security sẽ tự động mã hóa dữ liệu mới khi chúng được bổ sung.

Nếu hộp kiểm này bị xóa, toàn bộ ổ cứng sẽ được mã hóa, bao gồm các phần sót lại của những tập tin đã được sửa đổi hoặc bị xóa trước đó.

Tùy chọn này được khuyến nghị cho các ổ cứng mới có dữ liệu chưa được sửa đổi hoặc bị xóa. Nếu bạn đang áp dụng mã hóa trên một ổ cứng đang được sử dụng, bạn nên mã hóa toàn bộ ổ cứng. Điều này sẽ đảm bảo toàn bộ dữ liệu được bảo vệ, kể cả những dữ liệu đã bị xóa và có khả năng được phục hồi.

Hộp kiểm này được xóa ở chế độ mặc định.

Thiết lập xác thực

Sử dụng mật khẩu (Windows 8 và các phiên bản mới hơn)

Nếu tùy chọn này được sử dụng, Kaspersky Endpoint Security sẽ nhắc người dùng nhập mật khẩu khi người dùng cố gắng truy cập một ổ đĩa được mã hóa.

Tùy chọn này có thể được chọn khi một Mô-đun Nền tảng Tin tưởng (TPM) không được sử dụng.

Sử dụng Mô-đun Nền tảng Tin tưởng (TPM)

Nếu tùy chọn này được chọn, BitLocker sẽ sử dụng một Mô-đun Nền tảng Tin tưởng (TPM).

Mô-đun Nền tảng Tin tưởng (TPM) là một vi mạch được phát triển để cung cấp các chức năng cơ bản liên quan đến bảo mật (ví dụ: để lưu trữ khóa mã hóa). Một Mô-đun Nền tảng Tin tưởng 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.

Đối với các máy tính chạy Windows 7 hoặc Windows Server 2008 R2, chỉ có tính năng mã hóa bằng mô-đun TPM là khả dụng. Nếu một mô-đun TPM không được cài đặt thì không thể mã hóa bằng BitLocker. Việc sử dụng mật khẩu trên các máy tính này không được hỗ trợ.

Một thiết bị được trang bị Mô-đun Nền tảng Tin tưởng có thể tạo ra các khóa mã hóa chỉ có thể được giải mã với thiết bị đó. Một Mô-đun Nền tảng Tin tưởng sẽ mã hóa các khóa mã hóa với khóa lưu trữ root của nó. Khóa lưu trữ root được lưu trong Mô-đun Nền tảng Tin tưởng. Điều này tạo nên một cấp độ bảo vệ bổ sung chống lại các nỗ lực hack khóa mã hóa.

Hành động này được chọn theo mặc định.

Bạn có thể đặt một lớp bảo vệ bổ sung để truy cập khóa mã hóa và mã hóa khóa đó bằng một mật khẩu hoặc mã PIN:

- **Use PIN for TPM.** Nếu hộp kiểm này được chọn, người dùng có thể sử dụng một mã PIN để lấy quyền truy cập một khóa mã hóa được lưu trữ trong Mô-đun Nền tảng Tin tưởng (TPM).

Nếu hộp kiểm này bị xóa, người dùng bị cấm sử dụng mã PIN. Để truy cập khóa mã hóa, người dùng phải nhập mật khẩu. Bạn có thể cho phép người dùng sử dụng mã PIN cải tiến. *Mã PIN cải tiến* cho phép sử dụng các ký tự khác ngoài ký tự số: chữ cái Latinh viết hoa và viết thường, ký tự đặc biệt và dấu cách.

- **Sử dụng Mô-đun Nền tảng Tin tưởng (TPM); nếu không khả dụng thì sử dụng mật khẩu.** Nếu hộp kiểm này được chọn, người dùng có thể sử dụng một mật khẩu để nhận quyền truy cập đến các khóa mã hóa khi một Mô-đun Nền tảng Tin tưởng (TPM) không khả dụng.

Nếu hộp kiểm bị xóa và TPM không khả dụng, tác vụ mã hóa toàn bộ đĩa sẽ không bắt đầu.

Mã hóa mức độ tập tin

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 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.

Thành phần này khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows dành cho máy trạm. Thành phần này không khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows cho máy chủ.

Mã hóa tập tin có các tính năng đặc biệt sau:

- 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 hoặc 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 hoặc các thư mục được chuyển hướng.
- Kaspersky Endpoint Security sẽ không mã hóa các tập tin nếu việc sửa đổi chúng có thể gây hại cho 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% và %PROGRAMFILES(X86)%;
 - Các tập tin registry của Windows.

Danh sách loại trừ mã hóa không thể được xem hoặc sửa. Mặc dù bạn có thêm các tập tin và thư mục trong danh sách loại trừ mã hóa vào danh sách mã hóa, nhưng bạn sẽ không thể mã hóa chúng trong quá trình mã hóa tập tin.

Tham số	Mô tả
Chế độ mã hóa	<p>Giữ nguyên. Nếu mục này được chọn, Kaspersky Endpoint Security sẽ để nguyên, không thay đổi các tập tin và thư mục mà không mã hóa hoặc giải mã chúng.</p> <p>Theo các quy tắc. Nếu mục này được chọn, Kaspersky Endpoint Security sẽ mã hóa các tập tin và thư mục theo quy tắc mã hóa, giải mã các tập tin và thư mục theo quy tắc giải mã và điều chỉnh quyền truy cập của ứng dụng vào các tập tin được mã hóa theo quy tắc ứng dụng.</p> <p>Giải mã tất cả. Nếu mục này được chọn, Kaspersky Endpoint Security sẽ giải mã tất cả các tập tin và thư mục đã được mã hóa.</p>
Quy tắc mã hóa	<p>Thẻ này hiển thị quy tắc mã hóa cho các tập tin được lưu trữ trên ổ đĩa nội bộ. Bạn có thể thêm các tập tin như sau:</p> <ul style="list-style-type: none"> Các thư mục được xác định trước. Kaspersky Endpoint Security cho phép bạn thêm các khu vực sau: <ul style="list-style-type: none"> Documents. Các tập tin trong thư mục <i>Documents</i> tiêu chuẩn của hệ điều hành và các thư mục con. Favorites. Các tập tin trong thư mục <i>Favorites</i> tiêu chuẩn của hệ điều hành và các thư mục con. Desktop. Các tập tin trong thư mục <i>Desktop</i> tiêu chuẩn của hệ điều hành và các thư mục con. Các tập tin tạm. Các tập tin tạm thời liên quan đến hoạt động của các ứng dụng được cài đặt trên máy tính. Ví dụ: các ứng dụng Microsoft Office tạo các tập tin tạm thời chứa các bản sao lưu của tài liệu. Các tập tin Outlook. Các tập tin liên quan đến hoạt động của ứng dụng trình khách Outlook: tập tin dữ liệu (PST), tập tin dữ liệu ngoại tuyến (OST), tập tin sổ địa chỉ ngoại tuyến (OAB) và tập tin sổ địa chỉ cá nhân (PAB). Thư mục tùy chỉnh. Bạn có thể nhập đường dẫn đến thư mục. Khi thêm một đường dẫn thư mục, hãy tuân thủ các quy tắc sau: <ul style="list-style-type: none"> Sử dụng một biến môi trường (ví dụ như %FOLDER%\UserFolder\). Bạn chỉ có thể sử dụng một biến môi trường một lần duy nhất và chỉ ở đầu đường dẫn. Không sử dụng đường dẫn tương đối. Không sử dụng ký tự * và ?. Không sử dụng đường dẫn UNC. Sử dụng ; hoặc , làm ký tự phân cách. Các tập tin theo phần mở rộng. Bạn có thể chọn các nhóm mở rộng trong danh sách, ví dụ như nhóm mở rộng <i>Tập tin nén</i>. Bạn cũng có thể thêm phần mở rộng tập tin một cách thủ công.
Quy tắc giải mã	<p>Thẻ này hiển thị quy tắc giải mã cho các tập tin được lưu trữ trên ổ đĩa nội bộ.</p>
Quy tắc cho ứng dụng	<p>Thẻ này hiển thị một bảng chứa các quy tắc truy cập tập tin được mã hóa cho ứng dụng và quy tắc mã hóa cho các tập tin được tạo hoặc sửa đổi bởi các ứng dụng riêng lẻ.</p>
Thiết lập mật khẩu gói mã hóa	<p>Yêu cầu đối với độ mạnh của mật khẩu cần được đáp ứng khi tạo các gói mã hóa.</p>

Mã hóa ổ đĩa di động

Thành phần này khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows dành cho máy trạm. Thành phần này không khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows cho máy chủ.

Kaspersky Endpoint Security hỗ trợ mã hóa các tập tin trong hệ thống tập tin FAT32 và NTFS. Nếu một ổ đĩa di động có hệ thống tập tin không tương thích được kết nối với máy tính, tác vụ mã hóa cho ổ đĩa di động này sẽ kết thúc với một lỗi và Kaspersky Endpoint Security sẽ gắn trạng thái chỉ đọc cho ổ đĩa di động đó.

Để bảo vệ dữ liệu trên các ổ đĩa di động, bạn có thể sử dụng các loại mã hóa sau:

- Mã hóa toàn bộ ổ đĩa (FDE).

Mã hóa toàn bộ ổ đĩa di động, bao gồm cả hệ thống tập tin.

Không thể truy cập dữ liệu được mã hóa bên ngoài mạng doanh nghiệp. Bạn cũng không thể truy cập dữ liệu được mã hóa trong mạng doanh nghiệp nếu máy tính không được kết nối với Kaspersky Security Center (ví dụ: trên một máy tính khách).

- Mã hóa mức độ tập tin (FLE).

Chỉ mã hóa các tập tin trên ổ đĩa di động. Hệ thống tập tin được giữ nguyên.

Mã hóa các tập tin trên ổ đĩa di động cho phép truy cập dữ liệu bên ngoài mạng doanh nghiệp bằng cách sử dụng một chế độ đặc biệt gọi là [chế độ di động](#).

Trong quá trình mã hóa, Kaspersky Endpoint Security sẽ tạo một khóa chủ. Kaspersky Endpoint Security sẽ lưu khóa chủ trong các kho lưu trữ sau:

- Kaspersky Security Center.

- Máy tính của người dùng.

Khóa chủ được mã hóa bằng khóa bí mật của người dùng.

- Ổ đĩa di động.

Khóa chủ được mã hóa bằng khóa công khai của Kaspersky Security Center.

Sau khi quá trình mã hóa hoàn tất, dữ liệu trên ổ đĩa di động có thể truy cập được trong mạng doanh nghiệp như thể chúng được lưu trữ trên một ổ đĩa di động thông thường, chưa được mã.

Truy cập dữ liệu được mã hóa

Khi kết nối một ổ đĩa di động có dữ liệu được mã hóa, Kaspersky Endpoint Security sẽ thực hiện các hành động sau:

1. Kiểm tra khóa chủ trong ổ lưu trữ cục bộ trên máy tính của người dùng.
 Nếu tìm thấy khóa chủ, người dùng sẽ có quyền truy cập vào dữ liệu trên ổ đĩa di động.
 Nếu không tìm thấy khóa chủ, Kaspersky Endpoint Security sẽ thực hiện các hành động sau:
 - a. Gửi một yêu cầu đến Kaspersky Security Center.
 Sau khi nhận được yêu cầu, Kaspersky Security Center sẽ gửi một phản hồi có chứa khóa chủ.
 - b. Kaspersky Endpoint Security lưu khóa chủ trong ổ lưu trữ cục bộ trên máy tính của người dùng cho các hoạt động tiếp theo với ổ đĩa di động được mã hóa.
2. Giải mã dữ liệu.

Các tính năng đặc biệt của mã hóa ổ đĩa di động

Quá trình mã hóa ổ đĩa di động có các tính năng đặc biệt sau:

- Chính sách 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 áp dụng chính sách Kaspersky Security Center đã được cấu hình cho mã hóa / giải mã các 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 chỉ cho phép đọc, được lưu trữ trên ổ đĩa di động.
- 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 thiết lập thành phần ổ đĩa di động

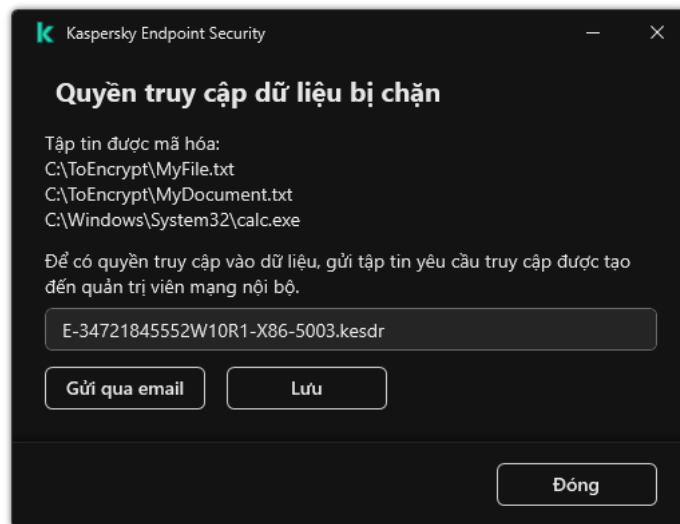
Tham số	Mô tả
Quản lý mã hóa	<p>Mã hóa toàn bộ ổ đĩa di động. Nếu mục này được chọn, khi áp dụng chính sách với thiết lập mã hóa được chỉ định cho các ổ đĩa di động, Kaspersky Endpoint Security sẽ mã hóa ổ đĩa di động theo từng sector, bao gồm cả hệ thống tập tin của chúng.</p> <p>Mã hóa tất cả các tập tin. Nếu mục này được chọn, khi áp dụng chính sách với thiết lập mã hóa được chỉ 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 không mã hóa lại các tập tin đã được mã hóa. Nội dung của hệ thống tập tin của ổ đĩa di động, bao gồm cấu trúc thư mục và tên của các tập tin được mã hóa, sẽ không được mã hóa và bạn vẫn có thể truy cập.</p> <p>Chỉ mã hóa các tập tin mới. Nếu mục này được chọn, khi áp dụng chính sách với thiết lập mã hóa được chỉ định cho các ổ đĩa di động, Kaspersky Endpoint Security sẽ chỉ mã hóa các tập tin đã được bổ sung hoặc sửa đổi trên ổ đĩa di động sau khi chính sách Kaspersky Security Center đã được áp dụng ở lần trước. Chế độ mã hóa này rất tiện lợi khi một ổ đĩa di động được sử dụng cho cả các mục đích cá nhân lẫn công việc. Chế độ mã hóa này cho phép bạn để nguyên, không thay đổi tất cả các tập tin cũ và chỉ mã hóa các tập tin mà người dùng tạo trên một máy tính làm việc có cài đặt Kaspersky Endpoint Security và có bật chức năng mã hóa. Kết quả là, bạn luôn có thể truy cập các tập tin cá nhân, bất kể liệu Kaspersky Endpoint Security có được cài đặt trên máy tính có bật chức năng mã hóa hay không.</p>

	<p>Giải mã toàn bộ ổ đĩa di động. Nếu mục này được chọn, khi áp dụng chính sách với thiết lập mã hóa được chỉ định cho các ổ đĩa di động, Kaspersky Endpoint Security sẽ giải mã tất cả các tập tin được mã hóa được lưu trữ trên các ổ đĩa di động cũng như hệ thống tập tin của ổ đĩa di động nếu trước đó chúng đã được mã hóa.</p> <p>Giữ nguyên. Nếu mục này được lựa chọn, ứng dụng sẽ để nguyên các ổ đĩa trong trạng thái trước đó của chúng khi chính sách được áp dụng. Nếu ổ đĩa đã được mã hóa, nó vẫn sẽ duy trì tình trạng mã hóa. Nếu ổ đĩa đã được giải mã, nó vẫn sẽ duy trì tình trạng giải mã. Mục này được chọn theo mặc định.</p>
<p>Chế độ di động</p>	<p>Hộp kiểm này bật / tắt việc chuẩn bị một ổ đĩa di động, để bạn có thể truy cập các tập tin được lưu trữ trên ổ đĩa di động này trên các máy tính bên ngoài mạng công ty.</p> <p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ nhắc người dùng nhập một mật khẩu trước khi mã hóa các tập tin trên một ổ đĩa di động khi áp dụng chính sách. Bạn cần mật khẩu này để truy cập các tập tin được mã hóa trên một ổ đĩa di động trên các máy tính bên ngoài mạng công ty. Bạn có thể cấu hình độ mạnh của mật khẩu.</p> <p>Chế độ di động khả dụng với chế độ Mã hóa tất cả các tập tin hoặc Chỉ mã hóa các tập tin mới.</p>
<p>Chỉ mã hóa dung lượng ổ đĩa được sử dụng</p>	<p>Hộp kiểm này bật / tắt chế độ mã hóa trong đó chỉ các khu vực ổ đĩa đã được sử dụng mới được mã hóa. Chế độ này được khuyến nghị cho các ổ đĩa mới có dữ liệu chưa được sửa đổi hoặc bị xóa.</p> <p>Nếu hộp kiểm này được chọn, chỉ các phần của ổ đĩa có chứa các tập tin mới được mã hóa. Kaspersky Endpoint Security sẽ tự động mã hóa dữ liệu mới khi chúng được bổ sung.</p> <p>Nếu hộp kiểm này bị xóa, toàn bộ ổ đĩa sẽ được mã hóa, bao gồm các phần sót lại của những tập tin đã được sửa đổi hoặc bị xóa trước đó.</p> <p>Khả năng chỉ mã hóa phần dung lượng được sử dụng chỉ khả dụng với chế độ Mã hóa toàn bộ ổ đĩa di động.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Sau khi quá trình mã hóa được bắt đầu, việc bật / tắt chức năng Chỉ mã hóa dung lượng ổ đĩa được sử dụng sẽ không thay đổi thiết lập này. Bạn phải chọn hoặc xóa hộp kiểm trước khi bắt đầu mã hóa.</p> </div>
<p>Quy tắc mã hóa cho các thiết bị đã được chọn</p>	<p>Bảng này chứa các thiết bị đã được đặt quy tắc mã hóa tùy chỉnh. Bạn có thể tạo quy tắc mã hóa cho từng ổ đĩa di động theo các cách sau:</p> <ul style="list-style-type: none"> • Thêm một ổ đĩa di động trong danh sách các thiết bị được tin tưởng dành cho Kiểm soát thiết bị. • Thêm một ổ đĩa di động theo cách thủ công: <ul style="list-style-type: none"> • Theo ID thiết bị (ID phần cứng hay HWID) • Theo model thiết bị: ID nhà cung cấp (VID) và ID sản phẩm (PID)
<p>Cho phép mã hóa ổ đĩa di động ở chế độ</p>	<p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ mã hóa các ổ đĩa di động khi không thể kết nối đến Kaspersky Security Center. Trong trường hợp này, dữ liệu yêu cầu để giải mã các ổ đĩa di động được lưu trữ trên ổ cứng của máy tính mà ổ đĩa di động kết nối đến, và không được truyền tải đến Kaspersky Security Center.</p> <p>Khi hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ không mã hóa các ổ đĩa di động nếu không có kết nối đến Kaspersky Security Center.</p>

độ ngoại tuyến	
Thiết lập mật khẩu của chế độ di động	Thiết lập độ mạnh mật khẩu cho Trình quản lý tập tin di động.

Mẫu (mã hóa dữ liệu)

Sau khi mã hóa dữ liệu, Kaspersky Endpoint Security có thể hạn chế quyền truy cập vào dữ liệu ví dụ như do sự thay đổi trong cơ sở hạ tầng của tổ chức và thay đổi trong Máy chủ quản trị Kaspersky Security Center. Nếu người dùng không có quyền truy cập vào dữ liệu được mã hóa, người dùng có thể yêu cầu quản trị viên truy cập vào dữ liệu đó. Nói cách khác, người dùng cần gửi cho quản trị viên tập tin yêu cầu truy cập. Sau đó, người dùng cần tải tập tin phản hồi nhận được từ quản trị viên lên Kaspersky Endpoint Security. Kaspersky Endpoint Security sẽ cho phép bạn yêu cầu truy cập dữ liệu từ quản trị viên thông qua email (xem hình bên dưới).



Yêu cầu truy cập vào dữ liệu được mã hóa

Bạn sẽ được cung cấp một mẫu để thông báo rằng bạn không có đủ quyền truy cập dữ liệu. Để thuận tiện cho người dùng, bạn có thể điền vào các trường sau:

- **Người gửi.** Nhập địa chỉ email của nhóm quản trị viên có quyền đối với các tính năng mã hóa dữ liệu.
- **Tiêu đề.** Nhập chủ đề của email có yêu cầu truy cập các tập tin được mã hóa. Ví dụ như bạn có thể thêm thẻ để lọc tin nhắn.
- **Tin nhắn.** Nếu cần, hãy thay đổi nội dung của tin nhắn. Bạn có thể sử dụng các biến để nhận dữ liệu cần thiết (ví dụ như biến %USER_NAME%).

Loại trừ

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.

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 thêm các đối tượng và ứng dụng vào 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. Quản trị viên cũng có thể cho phép người dùng tạo vùng tin tưởng cục bộ của riêng họ cho một máy tính cụ thể. Bằng cách này, người dùng có thể tạo danh sách loại trừ cục bộ của riêng họ và các ứng dụng được tin tưởng ngoài vùng tin tưởng chung trong một chính sách.

Loại trừ quét

Loại trừ quét là một nhóm các điều kiện phải được đáp ứng để Kaspersky Endpoint Security không quét một đối tượng cụ thể 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 làm hỏng 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 bị kẻ xâm nhập khai thác. Để xem chi tiết về các phần mềm hợp pháp có thể bị bọn tội phạm lợi dụng để gây hại cho máy tính hoặc dữ liệu cá nhân của một người dùng, vui lòng tham khảo [trang web Bách khoa toàn thư của Kaspersky IT](#).

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 tên đại diện của ứng dụng được liệt kê trong Bách khoa toàn thư của Kaspersky IT vào vùng tin tưởng. Ví dụ, bạn thường sử dụng ứng dụng Radmin để quản trị từ xa máy tính. 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 tên đại diện của ứng dụng được liệt kê trong Bách khoa toàn thư của Kaspersky IT.

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:

- [Phát hiện hành vi](#).
- [Phòng chống khai thác](#).
- [Phòng chống xâm nhập máy chủ](#).
- [Bảo vệ mối đe dọa tập tin](#).
- [Bảo vệ mối đe dọa web](#).
- [Bảo vệ mối đe dọa thư điện tử](#).
- [Tác vụ quét](#).

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 của ứng dụng và kiểm soát hoạt động của tất cả các ứng dụng và lưu lượng mạng được tạo bởi chúng. Tuy nhiên, một ứng dụng đã được thêm vào danh sách các ứng dụng được tin tưởng sẽ được Kaspersky Endpoint Security loại trừ khỏi các 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 các 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.

Cấu hình loại trừ

Tham số	Mô tả
Loại đối tượng được phát hiện	<p>Bất kể thiết lập ứng dụng có là gì, Kaspersky Endpoint Security sẽ luôn phát hiện và chặn các virus, sâu máy tính và Trojan. Chúng có thể gây thiệt hại đáng kể đến máy tính.</p> <ul style="list-style-type: none">• Virus và sâu 

Danh mục con: virus và sâu (Viruses_and_Worms)

Mức độ mối đe dọa: cao

Các loại virus và sâu truyền thống thực hiện các hành động không được người dùng cho phép. Chúng có thể tự tạo ra bản sao của chính mình, các bản sao đó cũng có thể tự nhân bản.

Virus truyền thống

Khi một virus truyền thống xâm nhập vào máy tính, nó sẽ lây nhiễm vào một tập tin, kích hoạt, thực hiện hành động độc hại, và chèn các bản sao của nó vào những tập tin khác.

Một virus truyền thống sẽ tự sinh sôi trên tài nguyên mạng nội bộ của máy tính; nó không thể tự xâm nhập vào các máy tính khác. Nó chỉ có thể được truyền sang máy tính khác nếu nó chèn bản sao của mình vào một tập tin được lưu trữ trong một thư mục được chia sẻ, hoặc trên một đĩa CD trong máy, hoặc nếu một người dùng chuyển tiếp một email đính kèm tập tin bị nhiễm virus.

Mã virus truyền thống có thể xâm nhập các khu vực khác nhau của máy tính, hệ điều hành và ứng dụng. Tùy thuộc vào môi trường, các virus được chia thành *virus tập tin*, *virus khởi động*, *virus kích bản* và *virus macro*.

Virus có thể lây nhiễm cho các tập tin sử dụng nhiều kỹ thuật khác nhau. *Ghi đè* virus sẽ ghi đè mã của nó lên mã của tập tin bị lây nhiễm và xóa nội dung của tập tin. Tập tin bị lây nhiễm sẽ ngừng hoạt động và không thể được khôi phục. *Ký sinh* virus sẽ sửa nội dung tập tin, để chúng vận hành toàn bộ hoặc một phần chức năng. *Virus đồng hành* không sửa tập tin, nhưng tạo các bản sao. Khi một tập tin nhiễm virus được mở ra, một bản sao của nó (thực chất là một virus) sẽ được khởi chạy. Các loại virus sau cũng có thể được bắt gặp: *virus liên kết*, *virus OBJ*, *virus LIB*, *virus mã nguồn*, v.v...

Sâu

Tương tự như virus truyền thống, mã của sâu, sẽ được kích hoạt và thực hiện các hành động độc hại sau khi nó đã xâm nhập máy tính. Sâu được đặt tên như vậy bởi chúng có thể "bò" từ một máy tính sang máy tính khác và phát tán các bản sao thông qua nhiều kênh dữ liệu mà không có sự cho phép của người dùng.

Tính năng chính phân biệt giữa các loại sâu khác nhau là cách phát tán của chúng. Bảng sau đây cung cấp một cái nhìn tổng quan về các loại sâu khác nhau, được phân loại theo cách phát tán của chúng.

Cách phát tán của sâu

Loại	Tên	Mô tả
Sâu Email	Sâu Email	Phát tán qua email.

		<p>Một email nhiễm virus chứa một tập tin đính kèm với một bản sao của sâu, hoặc một liên kết đến một tập tin được tải lên một website đã bị hack hoặc được tạo vì mục đích cụ thể này. Khi bạn mở tập tin đính kèm ra, sâu sẽ được kích hoạt. Khi bạn nhấn vào liên kết tải về, và mở tập tin, sâu sẽ bắt đầu thực hiện hành động độc hại của nó. Sau đó, nó sẽ tiếp tục phát tán các bản sao, tìm kiếm các địa chỉ email khác và gửi tin nhắn nhiễm virus đến họ.</p>
IM-Worm	Sâu Trình nhắn tin nhanh	<p>Chúng được phát tán qua các ứng dụng nhắn tin nhanh.</p> <p>Thông thường, các loại sâu này gửi tin nhắn chứa liên kết đến một bản sao của sâu trên một website, tập dụng danh bạ của người dùng. Khi người dùng tải về và mở ra tập tin, sâu sẽ được kích hoạt.</p>
IRC-Worm	Sâu trò chuyện Internet	<p>Chúng được phát tán qua các Phòng Tán gẫu IRC, là các hệ thống dịch vụ cho phép giao tiếp với những người khác qua Internet trong thời gian thực.</p> <p>Những loại sâu này sẽ đăng tải một tập tin với bản sao của chúng hoặc một liên kết đến tập tin trong một phòng tán gẫu Internet. Khi người dùng tải về và mở ra tập tin, sâu sẽ được kích hoạt.</p>
Sâu Net	Sâu Mạng	<p>Những loại sâu này phát tán qua mạng máy tính.</p> <p>Khác với những loại sâu khác, một sâu mạng tiêu biểu sẽ phát tán mà không cần sự tham gia của người dùng. Nó sẽ quét mạng nội bộ để tìm các máy tính chứa những chương trình có lỗ hổng bảo mật. Để làm điều này, nó sẽ gửi đi một gói tin mạng đặc biệt (mã khai thác) chứa mã sâu hoặc một phần của nó. Nếu một máy tính có "lỗ hổng bảo mật" nằm trên mạng này, nó sẽ tiếp nhận gói tin mạng đó. Khi sâu đã hoàn thành việc xâm nhập máy tính, nó sẽ kích hoạt.</p>
P2P-Worm	Sâu mạng chia sẻ tập tin	<p>Chúng được phát tán qua các mạng chia sẻ tập tin ngang hàng.</p> <p>Để xâm nhập một mạng P2P, sâu sẽ tự sao chép bản thân nó vào một thư mục chia sẻ tập tin, thường được đặt trên máy tính của người dùng. Mạng P2P sẽ hiển thị thông tin về tập tin này để người dùng có thể "tìm thấy" tập tin nhiễm virus trên mạng như những tập tin khác, sau đó tải về và mở nó ra.</p> <p>Các loại sâu tinh vi hơn sẽ giả lập giao thức mạng của một mạng P2P cụ thể: chúng sẽ gửi trả phản hồi tích cực đến các truy vấn tìm kiếm và cung cấp bản sao của chính mình để tải về.</p>
Sâu	Các loại sâu khác	<p>Các loại sâu khác bao gồm:</p> <ul style="list-style-type: none"> Sâu phát tán bản sao của chúng qua tài nguyên mạng. Bằng cách sử dụng chức năng của hệ điều hành, chúng sẽ quét các thư mục mạng khả dụng, kết nối đến các máy tính trên Internet, và cố gắng nhận quyền truy cập toàn diện đến ổ đĩa của chúng. Khác với những loại sâu được mô tả ở trên, các loại sâu khác không tự kích hoạt được, mà chỉ

khi người dùng mở một tập tin chứa một bản sao của sâu.

- Các loại sâu không sử dụng bất kỳ cách phát tán nào được mô tả ở bảng trước (ví dụ, các loại sâu phát tán qua điện thoại di động).

- **Trojan (bao gồm phần mềm tống tiền)** 

Danh mục con: Trojan

Mức độ mối đe dọa: cao

Khác với sâu và virus, Trojan không tự sinh sôi. Ví dụ, chúng sẽ xâm nhập một máy tính thông qua email hoặc một trình duyệt khi người dùng truy cập một trang web bị nhiễm virus. Trojan được khởi chạy với sự tham gia của người dùng. Chúng sẽ bắt đầu thực hiện hành động độc hại ngay khi được bắt đầu.

Các Trojan khác nhau sẽ hành xử khác nhau trên máy tính bị nhiễm. Chức năng chính của Trojan bao gồm chặn, sửa đổi hoặc phá hủy thông tin, và tắt máy tính hoặc mạng. Trojan cũng có thể nhận hoặc gửi tập tin, thực thi chúng, hiển thị thông báo lên màn hình, yêu cầu trang web, tải về và cài đặt các chương trình, và khởi động lại máy tính.

Tin tặc thường sử dụng "các nhóm" Trojan khác nhau.

Các loại hành vi Trojan được mô tả trong bảng dưới đây.

Loại hành vi Trojan trên một máy tính bị nhiễm

Loại	Tên	Mô tả
Trojan-ArcBomb	Trojan - "bom nén"	<p>Khi giải nén, các tập nén này sẽ tăng kích cỡ đến mức mà hoạt động của máy tính sẽ bị ảnh hưởng.</p> <p>Khi người dùng cố gắng giải nén tập nén này, máy tính có thể bị chậm đến mức treo; ổ cứng có thể bị lấp đầy dữ liệu "trống". "Bom nén" đặc biệt nguy hiểm đối với các máy chủ tập tin và email. Nếu máy chủ sử dụng một hệ thống tự động để xử lý thông tin đến, một "bom nén" có thể ngừng hoạt động của máy chủ.</p>
Backdoor	Trojan quản trị từ xa	<p>Đây được coi là loại Trojan nguy hiểm nhất. Chức năng của chúng cũng tương tự như các ứng dụng quản trị từ xa được cài đặt trên máy tính.</p> <p>Những chương trình này sẽ cài đặt bản thân trên máy tính mà không được người dùng phát hiện, cho phép kẻ xâm nhập có thể quản lý máy tính từ xa.</p>
Trojan	Trojan	<p>Chúng bao gồm các ứng dụng độc hại sau:</p> <ul style="list-style-type: none">• Trojan truyền thống. Những chương trình này chỉ thực hiện chức năng chính của Trojan: chặn, sửa đổi hoặc phá hủy thông tin, và tắt máy tính hoặc mạng. Chúng không có các tính năng cao cấp, khác với những loại Trojan khác được mô tả trong bảng này.• Trojan linh hoạt. Những chương trình này có các tính năng cao cấp giống nhiều loại Trojan khác nhau.
Trojan-	Trojan	Chúng bắt thông tin người dùng "làm con tin",

Ransom	tống tiền	sửa đổi hoặc chặn nó, hoặc ảnh hưởng đến hoạt động của máy tính để người dùng mất khả năng sử dụng thông tin này. Kẻ xâm nhập sẽ đòi tiền chuộc từ người dùng, hứa hẹn sẽ gửi một ứng dụng khôi phục hiệu năng máy tính và dữ liệu đã được lưu trữ trên đó.
Trojan-Clicker	Trojan nhấn chuột	Chúng sẽ truy cập các trang web từ máy tính của người dùng, bằng cách gửi đi lệnh đến trình duyệt hoặc thay đổi các địa chỉ web được quy định trong tập tin hệ điều hành. Bằng cách sử dụng các chương trình này, kẻ xâm nhập có thể gây ra các cuộc tấn công mạng và tăng lượng truy cập website, tăng số lượt hiển thị bằng quảng cáo.
Trojan-Downloader	Trojan tải về	Chúng sẽ truy cập trang web của kẻ xâm nhập, tải về các ứng dụng độc hại khác và cài đặt chúng trên máy tính của người dùng. Chúng có thể chứa tên tập tin của ứng dụng độc hại để tải về, hoặc nhận nó từ trang web được truy cập.
Trojan-Dropper	Trojan đổ bộ	Chúng chứa các Trojan khác sẽ được chúng giải nén trên ổ cứng và cài đặt. Kẻ xâm nhập có thể sử dụng Trojan đổ bộ vì các mục đích sau: <ul style="list-style-type: none"> • Cài đặt một ứng dụng độc hại mà không bị người dùng phát hiện: các chương trình Trojan đổ bộ không hiển thị thông báo nào, hay hiển thị các thông báo giả mạo rằng, ví dụ, có một lỗi trong một tập nén hoặc một phiên bản không tương thích của hệ điều hành. • Bảo vệ một ứng dụng độc hại khác đã được biết khỏi bị phát hiện: không phải phần mềm chống virus nào cũng có thể phát hiện một ứng dụng độc hại trong một ứng dụng Trojan đổ bộ.
Trojan-Notifier	Trojan thông báo	Chúng sẽ thông báo cho kẻ xâm nhập rằng máy tính bị nhiễm có thể được truy cập, gửi thông tin về máy tính đến kẻ xâm nhập: địa chỉ IP, số cổng đang mở, hoặc địa chỉ email. Chúng sẽ kết nối với kẻ xâm nhập qua email, FTP, truy cập trang web của kẻ xâm nhập, hoặc bằng một cách khác. Các chương trình Trojan thông báo thường được sử dụng theo nhóm gồm nhiều Trojan khác nhau. Chúng sẽ thông báo với kẻ xâm nhập rằng các Trojan khác đã được cài đặt thành công trên máy tính của người dùng.
Trojan-Proxy	Trojan proxy	Chúng cho phép kẻ xâm nhập có thể truy cập các trang web một cách ẩn danh sử dụng máy tính của người dùng; chúng thường được sử dụng để gửi thư rác.

Trojan-PSW	Phần mềm đánh cắp mật khẩu	<p>Phần mềm đánh cắp mật khẩu là một loại Trojan đánh cắp tài khoản người dùng, ví dụ như dữ liệu đăng ký phần mềm. Những Trojan này tìm thấy thông tin bí mật trong tập tin hệ thống và trong registry và gửi chúng cho "kẻ tấn công" qua email, qua FTP, qua trang web của kẻ xâm nhập, hoặc bằng một cách khác.</p> <p>Một số loại Trojan này được phân loại vào các kiểu riêng biệt được mô tả trong bảng này. Đó là những Trojan đánh cắp tài khoản ngân hàng (Trojan-Banker), đánh cắp dữ liệu từ ứng dụng nhắn tin nhanh (Trojan-IM), và đánh cắp thông tin của người chơi game trực tuyến (Trojan-GameThief).</p>
Trojan-Spy	Trojan gián điệp	<p>Chúng sẽ theo dõi người dùng, thu thập thông tin về các hành động của người dùng khi làm việc trên máy tính. Chúng có thể đánh cắp dữ liệu mà người dùng nhập vào bằng bàn phím, chụp ảnh màn hình, hoặc thu thập danh sách các ứng dụng đang hoạt động. Sau khi chúng đã nhận được thông tin, chúng sẽ chuyển nó đến kẻ xâm nhập qua email, qua FTP, qua trang web của kẻ xâm nhập, hoặc bằng một cách khác.</p>
Trojan-DDoS	Trojan tấn công mạng	<p>Chúng sẽ gửi nhiều yêu cầu từ máy tính của người dùng đến một máy chủ từ xa. Máy chủ sẽ không đủ tài nguyên để xử lý tất cả các yêu cầu, và sẽ ngừng hoạt động (Từ chối Dịch vụ, hoặc gọi tắt là DoS). Tin tặc thường sẽ lây nhiễm cho nhiều máy tính bằng các chương trình này, để chúng có thể sử dụng máy tính để đồng loạt tấn công một máy chủ.</p> <p>Các chương trình DoS gây ra một cuộc tấn công từ một máy tính với kiến thức của người dùng. Các chương trình DDoS (DoS Phân phối) sẽ phát động tấn công phân phối từ nhiều máy tính mà không được phát hiện bởi người dùng của máy tính bị nhiễm.</p>
Trojan-IM	Trojan đánh cắp thông tin từ người dùng các ứng dụng nhắn tin nhanh	<p>Chúng sẽ đánh cắp tài khoản và mật khẩu của người dùng ứng dụng nhắn tin nhanh. Chúng sẽ truyền dữ liệu đến kẻ xâm nhập qua email, qua FTP, qua trang web của kẻ xâm nhập, hoặc bằng một cách khác.</p>
Rootkit	Rootkit	<p>Chúng sẽ che giấu các ứng dụng độc hại khác và hoạt động của chúng, kéo dài sự tồn tại của những ứng dụng này trong hệ điều hành. Chúng cũng có thể che giấu các tập tin hay tiến trình đang thực hiện các ứng dụng độc hại trong bộ nhớ hoặc khóa registry của máy tính</p>

		bị nhiễm. Rootkit có thể che giấu việc trao đổi dữ liệu giữa các ứng dụng trên máy tính của người dùng và các máy tính khác trên mạng.
Trojan-SMS	Trojan dưới dạng tin nhắn SMS	Chúng có thể lây nhiễm cho điện thoại di động, gửi tin nhắn SMS đến các số điện thoại mất phí.
Trojan-GameThief	Trojan đánh cắp thông tin từ người chơi trò chơi trực tuyến	Chúng sẽ đánh cắp thông tin tài khoản từ người chơi game trực tuyến, sau đó truyền dữ liệu này đến kẻ xâm nhập qua email, qua FTP, qua trang web của kẻ xâm nhập, hoặc bằng một cách khác.
Trojan-Banker	Trojan đánh cắp tài khoản ngân hàng	Chúng sẽ đánh cắp dữ liệu tài khoản ngân hàng hoặc dữ liệu hệ thống tiền điện tử; gửi dữ liệu này đến tin tặc qua email, qua FTP, qua trang web của tin tặc hoặc bằng một cách khác.
Trojan-Mailfinder	Trojan thu thập địa chỉ email	Chúng sẽ thu thập các địa chỉ email được lưu trữ trên một máy tính và gửi thông tin này đến kẻ xâm nhập qua email, qua FTP, qua trang web của kẻ xâm nhập, hoặc bằng một cách khác. Kẻ xâm nhập có thể gửi thư rác đến các địa chỉ mà chúng đã thu thập.

- [Công cụ độc hại](#) 

Danh mục con: Công cụ độc hại

Cấp độ nguy hiểm: trung bình

Khác với các loại phần mềm độc hại khác, công cụ độc hại không thực hiện hành động độc hại ngay khi chúng được khởi chạy. Chúng có thể được lưu trữ và khởi chạy một cách an toàn trên máy tính của người dùng. Kẻ xâm nhập sẽ thường sử dụng các tính năng của những chương trình này để tạo các virus, sâu và Trojan, phát động tấn công mạng trên các máy chủ từ xa, hack máy tính, hoặc thực hiện các hành động độc hại khác.

Các tính năng khác nhau của công cụ độc hại được ghép nhóm theo phân loại được mô tả trong bảng sau.

Tính năng của công cụ độc hại

Loại	Tên	Mô tả
Tiện ích xây dựng	Tiện ích xây dựng	Chúng cho phép tạo ra các virus, sâu và Trojan mới. Một số tiện ích xây dựng có một giao diện cửa sổ tiêu chuẩn trong đó người dùng có thể lựa chọn kiểu ứng dụng độc hại mà họ muốn tạo, cách đối phó với trình gỡ lỗi, và các tính năng khác.
Dos	Tấn công mạng	Chúng sẽ gửi nhiều yêu cầu từ máy tính của người dùng đến một máy chủ từ xa. Máy chủ sẽ không đủ tài nguyên để xử lý tất cả các yêu cầu, và sẽ ngừng hoạt động (Từ chối Dịch vụ, hoặc gọi tắt là DoS).
Khai thác	Mã khai thác	<p><i>Mã khai thác</i> là một bộ dữ liệu hoặc mã chương trình sử dụng lỗ hổng bảo mật của ứng dụng xử lý nó để thực hiện một hành động độc hại trên máy tính. Ví dụ, một mã khai thác có thể ghi hoặc đọc tập tin, hoặc yêu cầu các trang web "bị nhiễm".</p> <p>Các mã khai thác khác nhau sử dụng lỗ hổng bảo mật trong các ứng dụng hoặc dịch vụ mạng khác nhau. Giả dạng dưới dạng một gói tin mạng, mã khai thác sẽ được truyền tải qua mạng đến nhiều máy tính khác nhau, tìm kiếm các máy tính có lỗ hổng bảo mật trong dịch vụ mạng. Một mã khai thác trong một tập tin DOC sử dụng lỗ hổng bảo mật của trình xử lý văn bản. Nó có thể bắt đầu thực hiện hành động đã được lập trình sẵn bởi tin tặc khi người dùng mở tập tin bị nhiễm. Một mã khai thác được nhúng trong một email sẽ tìm kiếm lỗ hổng bảo mật trong một trình khách email bất kỳ. Nó có thể bắt đầu thực thi hành động độc hại ngay khi người dùng mở ra một email bị nhiễm trong trình khách email này.</p> <p>Net-Worm được phát tán qua mạng sử dụng các mã khai thác này. Mã khai thác Nuker là các gói tin mạng làm vô hiệu máy tính.</p>
FileCryptor	Trình mã hóa	Chúng mã hóa các ứng dụng độc hại khác để che giấu các chương trình này khỏi ứng dụng

		chống virus.
Flooder	Chương trình "gây lụt" mạng	Chúng sẽ gửi vô số tin nhắn qua các kênh mạng. Loại công cụ này bao gồm, ví dụ, các chương trình gây lụt Phòng Tấn gấu IRC. Các công cụ kiểu Flooder không chứa các chương trình "gây lụt" các kênh được sử dụng bởi email, ứng dụng nhắn tin nhanh và hệ thống truyền thông di động. Những chương trình này được phân loại là các kiểu riêng biệt được mô tả trong bảng (Email-Flooder, IM-Flooder, và SMS-Flooder).
HackTool	Công cụ hack	Chúng hỗ trợ việc hack máy tính mà chúng được cài đặt trên đó hoặc tấn công một máy tính khác (ví dụ, bằng cách bổ sung các tài khoản hệ thống mới mà không có sự cho phép của người dùng hoặc xóa nhật ký hệ thống để che dấu vết hiện diện của chúng trong hệ điều hành). Loại công cụ này bao gồm một số sniffer có chức năng độc hại, như đánh cắp mật khẩu. Sniffer là các chương trình cho phép xem lưu lượng mạng.
Hoax	Mã lừa đảo	Chúng sẽ cảnh báo người dùng với các tin nhắn giống virus như: chúng có thể "phát hiện một virus" trong một tập tin không bị nhiễm hoặc thông báo với người dùng rằng ổ đĩa đã được định dạng lại, mặc dù thực tế điều này không xảy ra.
Spoof	Công cụ spoof	Chúng sẽ gửi tin nhắn và yêu cầu mạng với địa chỉ người gửi giả mạo. Kẻ xâm nhập có thể sử dụng các công cụ Spoof để giả mạo là người gửi tin nhắn thật.
VirTool	Công cụ sửa đổi các ứng dụng độc hại	Chúng cho phép sửa đổi các phần mềm độc hại khác, che giấu chúng khỏi ứng dụng chống virus.
Email-Flooder	Các chương trình "gây lụt" địa chỉ email	Chúng gửi nhiều tin nhắn đến các địa chỉ email khác nhau, "gây lụt" cho các địa chỉ này. Một lượng lớn thư đến sẽ khiến người dùng không thể xem các email hữu ích trong hộp thư đến của họ.
IM-Flooder	Các chương trình "gây lụt" cho ứng dụng nhắn tin nhanh	Chúng sẽ gửi tin nhắn gây lụt cho người dùng của các ứng dụng nhắn tin nhanh. Một lượng lớn tin nhắn sẽ khiến người dùng không thể xem các tin nhắn đến hữu ích.
SMS-	Các	Chúng sẽ gửi hàng loạt tin nhắn SMS đến điện

Flooder	chương trình "gây lụt" cho tin nhắn SMS	thoại di động.
----------------	---	----------------

- **Phần mềm quảng cáo** 

Danh mục con: phần mềm quảng cáo;

Mức độ mối đe dọa: trung bình

Phần mềm quảng cáo hiển thị thông tin quảng cáo đến người dùng. Các chương trình phần mềm quảng cáo hiển thị bảng quảng cáo trong giao diện của các chương trình khác và điều hướng các truy vấn tìm kiếm đến những trang web quảng cáo. Một số còn thu thập thông tin tiếp thị về người dùng và gửi nó đến nhà phát triển: thông tin này có thể bao gồm tên của các website được truy cập bởi người dùng hoặc nội dung truy vấn tìm kiếm của người dùng. Khác với các chương trình Trojan-Gián điệp, phần mềm quảng cáo gửi thông tin này đến nhà phát triển với sự cho phép của người dùng.

- **Phần mềm quay số tự động** 

Danh mục con: Các phần mềm hợp pháp có thể được sử dụng bởi bạn tội phạm để gây thiệt hại máy tính hoặc dữ liệu cá nhân của bạn.

Cấp độ nguy hiểm: trung bình

Hầu hết các ứng dụng này đều hữu ích, vậy nên có rất nhiều người dùng sử dụng chúng. Các ứng dụng này bao gồm các trình khách IRC, phần mềm tự động quay số, chương trình tải về tập tin, trình giám sát hoạt động hệ thống máy tính, tiện ích mật khẩu, và máy chủ Internet cho FTP, HTTP và Telnet.

Tuy nhiên, nếu kẻ xâm nhập truy cập được vào những chương trình này, hoặc cấy chúng lên máy tính của người dùng, một số tính năng của ứng dụng có thể được sử dụng để phá hoại tính bảo mật.

Các ứng dụng này khác nhau theo chức năng; các phân loại của chúng được mô tả theo bảng dưới đây.

Loại	Tên	Mô tả
Client-IRC	Trình tán gẫu Internet	Người dùng cài đặt các chương trình này để nói chuyện với mọi người trong Phòng Tán gẫu IRC. Kẻ xâm nhập sử dụng chúng để phát tán phần mềm độc hại.
Trình gọi	Phần mềm quay số tự động	Chúng có thể thiết lập kết nối điện thoại qua modem trong chế độ ẩn.
Trình tải về	Chương trình để tải về	Chúng có thể tải về tập tin từ các trang web trong chế độ ẩn.
Giám sát	Chương trình giám sát	Chúng cho phép hoạt động giám sát trên máy tính mà chúng được cài đặt (xem ứng dụng nào đang hoạt động và cách chúng trao đổi dữ liệu với các ứng dụng được cài đặt trên máy tính khác).
PSWTool	Công cụ khôi phục mật khẩu	Chúng cho phép xem và khôi phục mật khẩu bị quên. Kẻ xâm nhập sẽ ngàm cấy chúng trên máy tính của người dùng với mục đích tương tự.
RemoteAdmin	Chương trình quản trị từ xa	Chúng thường được sử dụng bởi quản trị viên hệ thống. Những chương trình này cho phép truy cập đến giao diện của một máy tính từ xa nhằm mục đích giám sát và quản lý nó. Kẻ xâm nhập sẽ ngàm cấy chúng trên máy tính của người dùng với mục đích tương tự: để giám sát và quản lý các máy tính từ xa. Các chương trình quản trị từ xa hợp pháp khác với các Trojan Backdoor cho quản trị từ xa. Trojan có khả năng tự xâm nhập hệ điều hành và tự cài đặt; các chương trình hợp pháp không thể làm điều này.
Server-FTP	Máy	Chúng có chức năng là các máy chủ FTP. Kẻ

	chủ FTP	xâm nhập sẽ cấy chúng lên máy tính của người dùng để truy cập từ xa đến máy tính qua FTP.
Server-Proxy	Máy chủ proxy	Chúng có chức năng là các máy chủ proxy. Kẻ xâm nhập sẽ cấy chúng lên máy tính của người dùng để gửi thư rác với tên của người dùng.
Server-Telnet	Máy chủ Telnet	Chúng có chức năng là các máy chủ Telnet. Kẻ xâm nhập sẽ cấy chúng lên máy tính của người dùng để truy cập từ xa đến máy tính qua Telnet.
Server-Web	Máy chủ web	Chúng có chức năng là các máy chủ web. Kẻ xâm nhập sẽ cấy chúng lên máy tính của người dùng để truy cập từ xa đến máy tính qua HTTP.
RiskTool	Công cụ để làm việc trên máy tính nội bộ	Chúng cung cấp cho người dùng những tính năng bổ sung khi làm việc trên máy tính của người dùng. Các công cụ này cho phép người dùng ẩn tập tin hoặc cửa sổ của các ứng dụng đang hoạt động và chấm dứt các tiến trình đang hoạt động.
NetTool	Công cụ mạng	Chúng cung cấp cho người dùng những tính năng bổ sung khi làm việc với các máy tính khác trên mạng lưới. Các công cụ này cho phép khởi động lại chúng, phát hiện các cổng mở, và bắt đầu các ứng dụng được cài đặt trên máy tính.
Client-P2P	Trình khách mạng P2P	Chúng cho phép làm việc trên các mạng ngang hàng. Chúng có thể được sử dụng bởi kẻ xâm nhập để phát tán phần mềm độc hại.
Client-SMTP	Trình khách SMTP	Chúng gửi email mà không có kiến thức của người dùng. Kẻ xâm nhập sẽ cấy chúng lên máy tính của người dùng để gửi thư rác với tên của người dùng.
WebToolbar	Thanh công cụ web	Chúng bổ sung thanh công cụ vào giao diện của các ứng dụng khác để sử dụng công nghệ tìm kiếm.
FraudTool	Chương trình giả	Chúng giả làm các chương trình khác. Ví dụ, có các chương trình chống virus giả có tác dụng hiển thị thông báo về phát hiện phần mềm độc hại. Tuy nhiên, trong thực tế, chúng không tìm thấy hay khử nhiễm bất cứ thứ gì.

- **Phát hiện các phần mềm khác có thể được sử dụng bởi kẻ xâm nhập để phá hoại máy tính hoặc dữ liệu cá nhân của bạn** 

Danh mục con: Các phần mềm hợp pháp có thể được sử dụng bởi bạn tội phạm để gây thiệt hại máy tính hoặc dữ liệu cá nhân của bạn.

Cấp độ nguy hiểm: trung bình

Hầu hết các ứng dụng này đều hữu ích, vậy nên có rất nhiều người dùng sử dụng chúng. Các ứng dụng này bao gồm các trình khách IRC, phần mềm tự động quay số, chương trình tải về tập tin, trình giám sát hoạt động hệ thống máy tính, tiện ích mật khẩu, và máy chủ Internet cho FTP, HTTP và Telnet.

Tuy nhiên, nếu kẻ xâm nhập truy cập được vào những chương trình này, hoặc cấy chúng lên máy tính của người dùng, một số tính năng của ứng dụng có thể được sử dụng để phá hoại tính bảo mật.

Các ứng dụng này khác nhau theo chức năng; các phân loại của chúng được mô tả theo bảng dưới đây.

Loại	Tên	Mô tả
Client-IRC	Trình tán gẫu Internet	Người dùng cài đặt các chương trình này để nói chuyện với mọi người trong Phòng Tán gẫu IRC. Kẻ xâm nhập sử dụng chúng để phát tán phần mềm độc hại.
Trình gọi	Phần mềm quay số tự động	Chúng có thể thiết lập kết nối điện thoại qua modem trong chế độ ẩn.
Trình tải về	Chương trình để tải về	Chúng có thể tải về tập tin từ các trang web trong chế độ ẩn.
Giám sát	Chương trình giám sát	Chúng cho phép hoạt động giám sát trên máy tính mà chúng được cài đặt (xem ứng dụng nào đang hoạt động và cách chúng trao đổi dữ liệu với các ứng dụng được cài đặt trên máy tính khác).
PSWTool	Công cụ khôi phục mật khẩu	Chúng cho phép xem và khôi phục mật khẩu bị quên. Kẻ xâm nhập sẽ ngàm cấy chúng trên máy tính của người dùng với mục đích tương tự.
RemoteAdmin	Chương trình quản trị từ xa	Chúng thường được sử dụng bởi quản trị viên hệ thống. Những chương trình này cho phép truy cập đến giao diện của một máy tính từ xa nhằm mục đích giám sát và quản lý nó. Kẻ xâm nhập sẽ ngàm cấy chúng trên máy tính của người dùng với mục đích tương tự: để giám sát và quản lý các máy tính từ xa. Các chương trình quản trị từ xa hợp pháp khác với các Trojan Backdoor cho quản trị từ xa. Trojan có khả năng tự xâm nhập hệ điều hành và tự cài đặt; các chương trình hợp pháp không thể làm điều này.
Server-FTP	Máy	Chúng có chức năng là các máy chủ FTP. Kẻ

	chủ FTP	xâm nhập sẽ cấy chúng lên máy tính của người dùng để truy cập từ xa đến máy tính qua FTP.
Server-Proxy	Máy chủ proxy	Chúng có chức năng là các máy chủ proxy. Kẻ xâm nhập sẽ cấy chúng lên máy tính của người dùng để gửi thư rác với tên của người dùng.
Server-Telnet	Máy chủ Telnet	Chúng có chức năng là các máy chủ Telnet. Kẻ xâm nhập sẽ cấy chúng lên máy tính của người dùng để truy cập từ xa đến máy tính qua Telnet.
Server-Web	Máy chủ web	Chúng có chức năng là các máy chủ web. Kẻ xâm nhập sẽ cấy chúng lên máy tính của người dùng để truy cập từ xa đến máy tính qua HTTP.
RiskTool	Công cụ để làm việc trên máy tính nội bộ	Chúng cung cấp cho người dùng những tính năng bổ sung khi làm việc trên máy tính của người dùng. Các công cụ này cho phép người dùng ẩn tập tin hoặc cửa sổ của các ứng dụng đang hoạt động và chấm dứt các tiến trình đang hoạt động.
NetTool	Công cụ mạng	Chúng cung cấp cho người dùng những tính năng bổ sung khi làm việc với các máy tính khác trên mạng lưới. Các công cụ này cho phép khởi động lại chúng, phát hiện các cổng mở, và bắt đầu các ứng dụng được cài đặt trên máy tính.
Client-P2P	Trình khách mạng P2P	Chúng cho phép làm việc trên các mạng ngang hàng. Chúng có thể được sử dụng bởi kẻ xâm nhập để phát tán phần mềm độc hại.
Client-SMTP	Trình khách SMTP	Chúng gửi email mà không có kiến thức của người dùng. Kẻ xâm nhập sẽ cấy chúng lên máy tính của người dùng để gửi thư rác với tên của người dùng.
WebToolbar	Thanh công cụ web	Chúng bổ sung thanh công cụ vào giao diện của các ứng dụng khác để sử dụng công nghệ tìm kiếm.
FraudTool	Chương trình giả	Chúng giả làm các chương trình khác. Ví dụ, có các chương trình chống virus giả có tác dụng hiển thị thông báo về phát hiện phần mềm độc hại. Tuy nhiên, trong thực tế, chúng không tìm thấy hay khử nhiễm bất cứ thứ gì.

- **[Đối tượng được đóng gói mà việc đóng gói có thể được sử dụng để bảo vệ các mã độc hại](#)** 

Kaspersky Endpoint Security sẽ quét các đối tượng nén và mô-đun giải nén trong các tập nén SFX (tự động giải nén).

Để giấu các chương trình nguy hiểm khỏi ứng dụng chống virus, kẻ xâm nhập thường sẽ nén chúng sử dụng các trình nén đặc biệt hoặc tạo các tập tin đóng gói nhiều lớp.

Các chuyên gia phân tích virus của Kaspersky đã xác định các trình nén phổ biến nhất trong giới tin tặc.

Nếu Kaspersky Endpoint Security phát hiện một trình đóng gói như vậy trong một tập tin, tập tin đó có nhiều khả năng sẽ chứa một ứng dụng độc hại hoặc một ứng dụng có thể được sử dụng bởi bọn tội phạm để gây hại cho máy tính hoặc dữ liệu cá nhân của bạn.

Kaspersky Endpoint Security sẽ tập trung vào các loại chương trình sau:

- *Các tập tin được đóng gói có thể gây hại* – sử dụng để đóng gói phần mềm độc hại, ví dụ như virus, sâu và Trojan.
- *Các tập tin đóng gói nhiều lớp* (cấp độ đe dọa trung bình) – đối tượng này đã được đóng gói ba lần bởi một hoặc nhiều trình đóng gói.

• **Các đối tượng đóng gói đa thành phần** 

Kaspersky Endpoint Security sẽ quét các đối tượng nén và mô-đun giải nén trong các tập nén SFX (tự động giải nén).

Để giấu các chương trình nguy hiểm khỏi ứng dụng chống virus, kẻ xâm nhập thường sẽ nén chúng sử dụng các trình nén đặc biệt hoặc tạo các tập tin đóng gói nhiều lớp.

Các chuyên gia phân tích virus của Kaspersky đã xác định các trình nén phổ biến nhất trong giới tin tặc.

Nếu Kaspersky Endpoint Security phát hiện một trình đóng gói như vậy trong một tập tin, tập tin đó có nhiều khả năng sẽ chứa một ứng dụng độc hại hoặc một ứng dụng có thể được sử dụng bởi bọn tội phạm để gây hại cho máy tính hoặc dữ liệu cá nhân của bạn.

Kaspersky Endpoint Security sẽ tập trung vào các loại chương trình sau:

- *Các tập tin được đóng gói có thể gây hại* – sử dụng để đóng gói phần mềm độc hại, ví dụ như virus, sâu và Trojan.
- *Các tập tin đóng gói nhiều lớp* (cấp độ đe dọa trung bình) – đối tượng này đã được đóng gói ba lần bởi một hoặc nhiều trình đóng gói.

Loại trừ

Bảng này chứa thông tin về các mục loại trừ quét.

Bạn có thể loại trừ các đối tượng ra khỏi tác vụ quét bằng các phương thức sau:

- Đặt đường dẫn đến tập tin hoặc thư mục.
- Nhập giá trị băm của đối tượng.

- Sử dụng ký tự đại diện:
 - Ký tự `*` (hoa thị) thay thế bất kỳ nhóm ký tự nào bộ ký tự, ngoại trừ các ký tự `\` và `/` (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ, ký tự đại diện `C:**.txt` sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng TXT nằm trong các thư mục trên ổ C:, nhưng không phải trong các thư mục con.
 - Hai ký tự `*` liên tiếp thay thế bất kỳ nhóm ký tự nào (bao gồm nhóm rỗng) trong tên tập tin hoặc thư mục, bao gồm các ký tự `\` và `/` (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ, ký tự đại diện `C:\Folder***.txt` sẽ bao gồm tất cả đường dẫn đến các tập tin có phần mở rộng TXT nằm trong thư mục được đặt tên là Folder và các thư mục con. Một đại diện phải có ít nhất một cặp lồng ghép. `C:***.txt` không phải là một đại diện hợp lệ.
 - Ký tự `?` (dấu hỏi) thay thế bất kỳ ký tự đơn nào, ngoại trừ các ký tự `\` và `/` (ký tự ngăn cách tên của các tập tin và thư mục trong đường dẫn đến tập tin và thư mục). Ví dụ: đại diện `C:\Folder\???.txt` sẽ bao gồm các đường dẫn đến tất cả các tập tin có trong thư mục Folder có phần mở rộng TXT và tên có ba ký tự.
 - Nhập tên của loại đối tượng theo phân loại của [Bách khoa toàn thư của Kaspersky](#) (ví dụ: Email-Worm, Rootkit hoặc RemoteAdmin). Bạn có thể sử dụng tên đại diện có ký tự `?` (thay thế bất kỳ ký tự đơn nào) và ký tự `*` (thay thế bất kỳ số lượng ký tự nào). Ví dụ: nếu nhập tên đại diện `Client *`, Kaspersky Endpoint Security sẽ loại trừ các đối tượng Client-IRC, Client-P2P và Client-SMTP khỏi quá trình quét.

Ứng dụng được tin tưởng

Bảng này liệt kê các ứng dụng được tin tưởng có hoạt động không được giám sát bởi Kaspersky Endpoint Security trong hoạt động của nó.
Thành phần Kiểm soát ứng dụng quản lý việc khởi chạy của mỗi ứng dụng bất kể ứng dụng đó có được bao gồm trong bảng các ứng dụng được tin tưởng hay không.

Hợp nhất các giá trị khi kế thừa

(Chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)

Thao tác này sẽ gộp danh sách loại trừ quét và ứng dụng được tin tưởng trong chính sách cha và chính sách con của Kaspersky Security Center. Để gộp danh sách, chính sách con phải được cấu hình để kế thừa các thiết lập của chính sách của Kaspersky Security Center.
Nếu hộp kiểm này được chọn, các mục danh sách trong chính sách cha của Kaspersky Security Center sẽ được hiển thị trong chính sách con. Bằng cách này, bạn có thể tạo một danh sách tổng hợp các ứng dụng được tin tưởng cho toàn bộ tổ chức.
Không thể xóa hoặc chỉnh sửa các mục danh sách được kế thừa trong chính sách con. Chỉ có thể xóa và chỉnh sửa các mục trong danh sách loại trừ quét và danh sách ứng dụng được tin tưởng được gộp trong quá trình kế thừa trong chính sách cha. Bạn có thể thêm, chỉnh sửa hoặc xóa các mục danh sách trong các chính sách cấp thấp hơn.
Nếu các mục trong danh sách của chính sách con và chính sách cha khớp với nhau, thì các mục này sẽ được hiển thị dưới dạng cùng một mục của chính sách cha.
Nếu hộp kiểm này không được chọn, các mục danh sách sẽ không được gộp khi kế thừa thiết lập của chính sách Kaspersky Security Center.

Cho phép sử dụng các loại trừ cục bộ / Cho phép sử

Các loại trừ cục bộ và các ứng dụng được tin tưởng cục bộ (vùng tin tưởng cục bộ) - danh sách các đối tượng và ứng dụng do người dùng xác định trong Kaspersky Endpoint Security cho một máy tính cụ thể. Kaspersky Endpoint Security sẽ không giám sát các đối tượng và ứng dụng từ vùng tin tưởng. Bằng cách này, người dùng có thể [tạo danh sách loại trừ cục bộ của riêng họ và các ứng dụng được tin tưởng](#) ngoài vùng tin tưởng chung trong một chính sách.

<p>dụng các ứng dụng được tin tưởng cục bộ (chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)</p>	<p>Nếu hộp kiểm này được chọn, người dùng có thể tạo danh sách cục bộ gồm các loại trừ quét và danh sách các ứng dụng được tin tưởng cục bộ. Quản trị viên có thể sử dụng Kaspersky Security Center để xem, thêm, chỉnh sửa hoặc xóa các mục danh sách trong thuộc tính máy tính.</p> <p>Nếu hộp kiểm bị xóa, người dùng chỉ có thể truy cập danh sách các loại trừ quét chung và các ứng dụng được tin tưởng được tạo trong chính sách.</p>
<p>Kho chứng chỉ hệ thống tin tưởng</p>	<p>Nếu chọn một trong các kho chứng chỉ hệ thống được tin tưởng, Kaspersky Endpoint Security sẽ loại trừ các ứng dụng có chữ ký số được tin tưởng ra khỏi tác vụ quét. Kaspersky Endpoint Security sẽ tự động gán các ứng dụng đó vào nhóm <i>Tin tưởng</i>.</p> <p>Nếu chọn Không sử dụng, Kaspersky Endpoint Security sẽ quét các ứng dụng, bất kể chúng có chữ ký số hay không. Kaspersky Endpoint Security sẽ đặt ứng dụng vào một nhóm tin tưởng tùy thuộc vào mức độ nguy hiểm mà ứng dụng này có thể gây ra cho máy tính.</p>

Thiết lập ứng dụng

Bạn có thể cấu hình các thiết lập tổng quát sau của ứng dụng:

- Chế độ hoạt động
- Tự bảo vệ
- Hiệu suất
- Thông tin gỡ lỗi
- Trạng thái máy tính khi áp dụng các thiết lập

Thiết lập ứng dụng

Tham số	Mô tả
<p>Bắt đầu Kaspersky Endpoint Security cho Windows khi khởi động máy tính</p>	<p>Khi hộp kiểm này được lựa chọn, Kaspersky Endpoint Security sẽ được khởi chạy sau khi hệ điều hành được nạp, bảo vệ máy tính trong toàn phiên sử dụng.</p> <p>Khi hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ không được khởi chạy sau khi hệ điều hành được nạp, người dùng phải khởi chạy thủ công ứng dụng. Bảo vệ máy tính sẽ bị tắt và dữ liệu của người dùng có thể sẽ bị đe dọa.</p>
<p>Sử dụng công nghệ Khử mã độc nâng cao (cần tài</p>	<p>Nếu hộp kiểm được lựa chọn, một thông báo nổi sẽ xuất hiện trên màn hình khi phát hiện hoạt động độc hại trong hệ điều hành. Trong thông báo này, Kaspersky Endpoint Security sẽ đề xuất người dùng thực hiện Khử mã độc nâng cao cho máy tính. Nếu người dùng đồng ý thực hiện quy trình này, Kaspersky Endpoint Security sẽ vô hiệu mối đe dọa đó. Sau khi hoàn tất thủ tục khử nhiễm cao cấp, Kaspersky</p>

<p>nguyên máy tính đáng kể)</p>	<p>Endpoint Security sẽ khởi động lại máy tính. Công nghệ khử mã độc nâng cao sử dụng lượng tài nguyên máy tính đáng kể và có thể làm chậm các ứng dụng khác.</p> <p>Khi ứng dụng đang trong quá trình phát hiện một hoạt động lây nhiễm chủ động, một số chức năng của hệ điều hành có thể không khả dụng. Sự khả dụng của hệ điều hành được khôi phục khi Khử mã độc nâng cao hoàn tất và máy tính được khởi động lại.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Nếu Kaspersky Endpoint Security được cài đặt trên máy tính chạy Windows dành cho Máy chủ thì Kaspersky Endpoint Security sẽ không hiển thị thông báo. Do đó, người dùng không thể chọn hành động để khử mã độc mỗi đe dọa đang hoạt động. Để khử mã độc một mối đe dọa, bạn cần bật công nghệ Khử mã độc nâng cao trong thiết lập của ứng dụng và bật Khử mã độc nâng cao ngay lập tức trong thiết lập tác vụ <i>Quét virus</i>. Sau đó bạn cần khởi chạy tác vụ <i>Quét virus</i>.</p> </div>
<p>Sử dụng Kaspersky Security Center như máy chủ proxy để kích hoạt <i>(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)</i></p>	<p>Nếu hộp kiểm này được chọn, Kaspersky Security Center Administration Server sẽ được sử dụng như một máy chủ proxy khi kích hoạt ứng dụng.</p>
<p>Bật Tự bảo vệ</p>	<p>Khi hộp kiểm này được lựa chọn, Kaspersky Endpoint Security 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.</p>
<p>Cho phép quản lý thiết lập của Kaspersky Endpoint Security thông qua các ứng dụng kiểm soát từ xa</p>	<p>Nếu hộp kiểm này được chọn, các ứng dụng quản trị từ xa được tin tưởng (ví dụ như TeamViewer, LogMeIn Pro và Remotely Anywhere) có thể sửa đổi thiết lập của Kaspersky Endpoint Security.</p> <p>Các ứng dụng quản trị từ xa không được tin tưởng sẽ bị cấm sửa đổi thiết lập của Kaspersky Endpoint Security ngay cả khi hộp kiểm được chọn.</p>
<p>Bật kiểm soát dịch vụ bên ngoài</p>	<p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ cho phép quản lý các dịch vụ ứng dụng từ một máy tính từ xa. Khi một nỗ lực quản lý từ xa các dịch vụ của ứng dụng được thực hiện, một thông báo sẽ được hiển thị trong thanh tác vụ của Microsoft Windows trên biểu tượng ứng dụng (trừ khi dịch vụ thông báo đã bị tắt bởi người dùng).</p>
<p>Hoãn các tác vụ</p>	<p>Nếu hộp kiểm này được chọn, chế độ tiết kiệm năng lượng sẽ được bật. Kaspersky Endpoint Security sẽ tạm hoãn các tác vụ theo lịch. Bạn có thể bắt đầu các tác vụ</p>

theo lịch trong khi đang sử dụng nguồn pin	quét và cập nhật một cách thủ công, nếu cần thiết.
Nhường tài nguyên cho các ứng dụng khác	Mức sử dụng tài nguyên máy tính của Kaspersky Endpoint Security khi quét máy tính có thể làm tăng mức tải cho CPU và các hệ thống con của ổ cứng. Điều này có thể làm chậm các ứng dụng khác. Để tối ưu hóa hiệu năng, Kaspersky Endpoint Security cung cấp một <i>chế độ chuyển tài nguyên sang các ứng dụng khác</i> . Ở chế độ này, hệ điều hành có thể giảm mức độ ưu tiên của các luồng tác vụ quét của Kaspersky Endpoint Security khi CPU có mức tải cao. Điều này cho phép phân phối lại tài nguyên hệ điều hành cho các ứng dụng khác. Nhờ vậy, tác vụ quét sẽ nhận được ít thời gian CPU hơn. Kết quả là Kaspersky Endpoint Security sẽ mất nhiều thời gian hơn để quét máy tính. Theo mặc định, ứng dụng được thiết lập để nhường tài nguyên cho các ứng dụng khác.
Cho phép ghi tập tin dump	Nếu hộp kiểm được chọn, Kaspersky Endpoint Security sẽ ghi kết xuất khi ứng dụng này bị treo. Khi hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ không ghi tập tin kết xuất. Ứng dụng cũng sẽ xóa các tập tin kết xuất hiện có khỏi ổ cứng máy tính.
Bật bảo vệ các tập tin kết xuất và dấu vết	Nếu hộp kiểm này được chọn, quyền truy cập các tập tin kết xuất sẽ được cấp cho quản trị viên hệ thống và nội bộ, cũng như người dùng đã bật tính năng ghi tập tin kết xuất. Chỉ quản trị viên hệ thống và nội bộ mới có thể truy cập các tập tin dấu vết. Nếu hộp kiểm này bị xóa, bất cứ người dùng nào cũng có thể truy cập các tập tin kết xuất và dấu vết.
Trạng thái máy tính khi áp dụng các thiết lập <i>(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)</i>	Các thiết lập hiển thị trạng thái của máy khách có cài đặt Kaspersky Endpoint Security trong Bảng điều khiển web khi có lỗi xảy ra trong quá trình áp dụng một chính sách hoặc thực thi một tác vụ. Có các trạng thái <i>OK</i> , <i>Cảnh báo</i> và <i>Quan trọng</i> .

Các báo cáo và lưu trữ

Báo cáo

Thông tin về hoạt động của mỗi thành phần Kaspersky Endpoint Security, sự kiện mã hóa dữ liệu, hiệu quả của mỗi tác vụ quét, tác vụ cập nhật và tác vụ kiểm tra tính toàn vẹn cùng với hoạt động tổng thể của ứng dụng sẽ được ghi trong báo cáo.

Các bản báo cáo được lưu trữ trong thư mục C:\ProgramData\Kaspersky Lab\KES\Report.

Sao lưu

Sao lưu sẽ lưu trữ bản sao lưu của các tập tin đã bị xóa hoặc sửa đổi trong quá trình khử mã độc. *Bản sao lưu* là một bản sao của tập tin được tạo trước khi tập tin đó được khử nhiễm hay xóa. Các bản sao lưu của tập tin được lưu trữ trong một định dạng đặc biệt và không gây ra mối đe dọa.

Những bản sao lưu này được lưu trữ trong thư mục C:\ProgramData\Kaspersky Lab\KES\QB.

Người dùng trong nhóm Quản trị viên được cấp quyền truy cập toàn diện vào thư mục này. Quyền truy cập giới hạn vào thư mục này được cấp cho người dùng có tài khoản được sử dụng để cài đặt Kaspersky Endpoint Security.

Kaspersky Endpoint Security không có khả năng cấu hình quyền truy cập của người dùng vào các bản sao lưu tập tin.

Khu vực cách ly

Khu vực cách ly là một kho lưu trữ cục bộ đặc biệt trên máy tính. Người dùng có thể cách ly các tập tin mà người dùng coi là nguy hiểm cho máy tính. Các tập tin cách ly được lưu trữ ở trạng thái mã hóa và không đe dọa đến tính bảo mật của thiết bị. Kaspersky Endpoint Security chỉ sử dụng Khu vực cách ly khi làm việc với các giải pháp Kaspersky Sandbox và Kaspersky Endpoint Detection and Response. Trong các trường hợp khác, Kaspersky Endpoint Security sẽ đặt các tập tin liên quan vào [Sao lưu](#). Để biết chi tiết về quản lý khu vực cách ly làm một phần của các giải pháp, vui lòng tham khảo [Trợ giúp của Kaspersky Sandbox](#), [Trợ giúp của Kaspersky Endpoint Detection and Response Optimum](#) và [Trợ giúp của Kaspersky Endpoint Detection and Response Expert](#).

Chỉ có thể cấu hình Khu vực cách ly bằng Bảng điều khiển web. Bạn cũng có thể sử dụng Bảng điều khiển web để quản lý các đối tượng đã cách ly (khôi phục, xóa, thêm, v.v.). Bạn có thể khôi phục cục bộ các đối tượng trên máy tính bằng cách sử dụng [dòng lệnh](#).

Kaspersky Endpoint Security sử dụng tài khoản hệ thống (SYSTEM) để cách ly các tập tin.

Cấu hình các báo cáo và lưu trữ

Tham số	Mô tả
Lưu trữ báo cáo không quá N ngày	Nếu hộp kiểm được chọn, khoảng thời gian lưu trữ báo cáo sẽ bị giới hạn trong khoảng thời gian xác định. Thời gian lưu trữ báo cáo tối đa là 30 ngày ở chế độ mặc định. Sau khoảng thời gian đó, Kaspersky Endpoint Security sẽ tự động xóa các mục cũ nhất từ tập tin báo cáo.
Giới hạn dung lượng của tập tin báo cáo ở mức N MB	Nếu hộp kiểm được chọn, kích thước tối đa của tập tin báo cáo sẽ bị giới hạn theo giá trị mặc định. Theo mặc định, kích cỡ tập tin tối đa là 1024 MB. Để tránh vượt quá kích cỡ tập tin báo cáo tối đa, Kaspersky Endpoint Security sẽ tự động xóa các mục cũ nhất từ tập tin báo cáo khi đạt đến kích cỡ tập tin báo cáo tối đa.
Lưu trữ đối tượng trong N ngày	Nếu hộp kiểm được chọn, khoảng thời gian lưu trữ tập tin sẽ bị giới hạn trong khoảng thời gian xác định. Thời gian lưu trữ tập tin tối đa là 30 ngày ở chế độ mặc định. Sau khi thời gian lưu trữ tối đa đã kết thúc, Kaspersky Endpoint Security sẽ xóa các tập tin cũ nhất khỏi Sao lưu.
Giới hạn dung lượng	Nếu hộp kiểm được chọn, kích thước lưu trữ tối đa sẽ bị giới hạn theo giá trị mặc định. Theo mặc định, kích cỡ tối đa là 100 MB. Để tránh vượt quá kích thước lưu trữ

Lượng của bản Sao lưu ở mức N MB	tối đa, Kaspersky Endpoint Security sẽ tự động xóa các tập tin cũ nhất trong phần lưu trữ khi đạt đến kích thước lưu trữ tối đa.
Giới hạn dung lượng của Khu vực cách ly xuống N MB <i>(chỉ khả dụng trong Bảng điều khiển web)</i>	Dung lượng tối đa của Khu vực cách ly tính bằng MB. Ví dụ: bạn có thể đặt dung lượng tối đa của Khu vực cách ly là 200 MB. Khi khu vực cách ly đạt dung lượng tối đa, Kaspersky Endpoint Security sẽ gửi sự kiện tương ứng đến Kaspersky Security Center và phát hành sự kiện này trong Nhật ký sự kiện của Windows. Trong khi đó ứng dụng dừng cách ly các đối tượng mới. Bạn phải xóa Khu vực cách ly theo cách thủ công.
Thông báo khi kho lưu trữ của Khu vực cách ly đạt N phần trăm <i>(chỉ khả dụng trong Bảng điều khiển web)</i>	Giá trị ngưỡng của Khu vực cách ly. Ví dụ: bạn có thể đặt ngưỡng Khu vực cách ly thành 50%. Khi khu vực cách ly đạt ngưỡng này, Kaspersky Endpoint Security sẽ gửi sự kiện tương ứng đến Kaspersky Security Center và phát hành sự kiện này trong Nhật ký sự kiện của Windows. Trong khi đó ứng dụng vẫn tiếp tục cách ly các đối tượng mới.
Truyền dữ liệu đến Máy chủ quản trị <i>(chỉ khả dụng trong Kaspersky Security Center)</i>	Các danh mục sự kiện trên các máy khách có thông tin phải được gửi đến Máy chủ quản trị.

Thiết lập mạng

Bạn có thể cấu hình máy chủ proxy được sử dụng để kết nối với mạng Internet và cập nhật cơ sở dữ liệu diệt virus, chọn chế độ giám sát công mạng và cấu hình quét kết nối được mã hóa.

Các tùy chọn mạng

Tham số	Mô tả
Hạn chế lưu lượng trên các	Nếu hộp kiểm này được chọn, ứng dụng sẽ giới hạn lưu lượng mạng của mình khi kết nối Internet bị hạn chế. Kaspersky Endpoint Security sẽ xác định một kết nối Internet di động tốc độ cao là kết nối bị hạn chế và xác định một kết nối Wi-Fi là kết nối không giới hạn.

Kết nối tính phí lưu lượng	Tính năng Tối ưu chi phí mạng hoạt động trên máy tính chạy Windows 8 trở lên.
Chèn mã vào lưu lượng web để tương tác với các trang web	<p>Nếu chọn hộp kiểm này, Kaspersky Endpoint Security sẽ chèn một mã tương tác trang web vào lưu lượng web. Mã này đảm bảo rằng thành phần Kiểm soát Web có thể hoạt động chính xác. Mã này cho phép đăng ký các sự kiện Kiểm soát Web. Nếu không có mã này, bạn không thể bật giám sát hoạt động Internet của người dùng.</p> <div style="background-color: #f8d7da; padding: 10px; margin-top: 10px;"> <p>Các chuyên gia Kaspersky khuyên bạn chèn mã tương tác trang web này vào lưu lượng để đảm bảo hoạt động chính xác của Kiểm soát Web.</p> </div>
Máy chủ proxy	<p>Các thiết lập của máy chủ proxy được sử dụng để truy cập Internet cho người dùng máy khách. Kaspersky Endpoint Security sẽ sử dụng các thiết lập này cho một số thành phần bảo vệ nhất định, bao gồm để cập nhật các cơ sở dữ liệu và mô-đun ứng dụng.</p> <p>Để cấu hình tự động máy chủ proxy, Kaspersky Endpoint Security sử dụng giao thức WPAD (Giao thức tự động phát hiện web proxy). Nếu không thể xác định địa chỉ IP của máy chủ proxy bằng giao thức này, Kaspersky Endpoint Security sẽ sử dụng địa chỉ máy chủ proxy được đặt trong thiết lập của trình duyệt Microsoft Internet Explorer.</p>
Bỏ qua máy chủ proxy đối với các địa chỉ cục bộ	<p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ không sử dụng một máy chủ proxy khi thực hiện tác vụ cập nhật từ một thư mục được chia sẻ.</p>
Giám sát các cổng	<p>Giám sát tất cả các cổng mạng. Trong chế độ giám sát cổng mạng này, các thành phần bảo vệ (Bảo vệ mỗi đe dọa tập tin, Bảo vệ mỗi đe dọa web, Bảo vệ mỗi đe dọa thư điện tử) sẽ giám sát dòng dữ liệu được truyền qua bất kỳ cổng mạng mở nào trên máy tính.</p> <p>Chỉ giám sát các cổng mạng được chọn. Trong chế độ giám sát cổng mạng này, các thành phần bảo vệ giám sát các cổng được chọn của máy tính và hoạt động mạng của các ứng dụng được chọn. Danh sách cổng mạng thường được sử dụng để truyền tải email và lưu lượng mạng được cấu hình theo đề xuất của các chuyên gia Kaspersky.</p> <p>Giám sát tất cả các cổng cho ứng dụng từ danh sách được khuyến nghị bởi Kaspersky. Tính năng này sử dụng một danh sách các ứng dụng định sẵn có cổng được Kaspersky Endpoint Security giám sát. Ví dụ: danh sách này bao gồm Google Chrome, Adobe Reader, Java và các ứng dụng khác.</p> <p>Theo dõi tất cả các cổng của những ứng dụng được chỉ định. Tính năng này sử dụng một danh sách các ứng dụng có cổng được Kaspersky Endpoint Security giám sát.</p>
Quét kết nối được mã hóa	<p>Kaspersky Endpoint Security sẽ quét lưu lượng mạng mã hóa được truyền qua các giao thức sau:</p> <ul style="list-style-type: none"> • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. <p>Kaspersky Endpoint Security hỗ trợ các chế độ quét kết nối được mã hóa sau:</p>

	<ul style="list-style-type: none"> • Không quét các kết nối được mã hóa. Kaspersky Endpoint Security sẽ không có quyền truy cập vào nội dung của các trang web có địa chỉ bắt đầu bằng <code>https://</code>. • Quét các kết nối mã hóa khi được yêu cầu bởi các thành phần bảo vệ. Kaspersky Endpoint Security sẽ chỉ quét lưu lượng được mã hóa khi được yêu cầu bởi các thành phần Bảo vệ mối đe dọa tập tin, Bảo vệ mối đe dọa thư điện tử và Kiểm soát Web. • Luôn luôn quét các kết nối mã hóa. Kaspersky Endpoint Security sẽ quét lưu lượng mạng được mã hóa ngay cả khi các thành phần bảo vệ bị tắt. <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Kaspersky Endpoint Security không quét các kết nối được mã hóa được thiết lập bởi các ứng dụng được tin tưởng có tính năng quét lưu lượng bị tắt. Kaspersky Endpoint Security không quét các kết nối được mã hóa trong danh sách website được tin tưởng được xác định trước. Các chuyên gia Kaspersky là những người tạo ra danh sách website được tin tưởng được định nghĩa trước. Danh sách này được cập nhật bằng cơ sở dữ liệu diệt virus của ứng dụng. Bạn chỉ có thể xem danh sách website được tin tưởng được định nghĩa trước trong giao diện Kaspersky Endpoint Security. Bạn không thể xem danh sách này trong Bảng điều khiển Kaspersky Security Center.</p> </div>
<p>Chứng chỉ gốc được tin tưởng</p>	<p>Danh sách chứng chỉ gốc được tin tưởng. Kaspersky Endpoint Security cho phép bạn cài đặt chứng chỉ gốc được tin tưởng trên máy tính của người dùng, ví dụ như nếu bạn cần triển khai một trung tâm chứng thực mới. Ứng dụng cho phép bạn thêm chứng chỉ vào một kho chứng chỉ đặc biệt của Kaspersky Endpoint Security. Trong trường hợp này, chứng chỉ được coi là được tin tưởng cho riêng ứng dụng Kaspersky Endpoint Security. Nói cách khác, người dùng có thể lấy quyền truy cập vào một website bằng chứng chỉ mới trong trình duyệt. Nếu ứng dụng khác cố lấy quyền truy cập vào website đó thì bạn có thể nhận một lỗi kết nối do sự cố chứng chỉ. Để thêm vào kho chứng chỉ hệ thống, bạn có thể sử dụng các chính sách nhóm của Active Directory.</p>
<p>Hành động khi cố truy cập một tên miền có chứng chỉ không được tin tưởng</p>	<ul style="list-style-type: none"> • Cho phép. Khi truy cập một tên miền với một chứng chỉ không được tin tưởng, Kaspersky Endpoint Security sẽ cho phép kết nối mạng. Khi mở một tên miền có chứng chỉ không được tin tưởng trong một trình duyệt, Kaspersky Endpoint Security sẽ hiển thị một trang HTML với cảnh báo và giải thích rằng việc truy cập tên miền cụ thể này là không được khuyến nghị. Người dùng có thể nhấn vào liên kết từ trang cảnh báo HTML để nhận quyền truy cập đến tài nguyên web được yêu cầu. Nếu ứng dụng hoặc dịch vụ của bên thứ ba thiết lập kết nối với tên miền có chứng chỉ không được tin tưởng thì Kaspersky Endpoint Security sẽ tạo chứng chỉ riêng để quét lưu lượng. Chứng chỉ mới có trạng thái <i>Không tin tưởng</i>. Đây là điều cần thiết để cảnh báo ứng dụng của bên thứ ba về kết nối không được tin tưởng vì không thể hiển thị trang HTML trong trường hợp này và kết nối có thể được thiết lập ở chế độ nền. • Chặn kết nối. Khi truy cập một tên miền với một chứng chỉ không được tin tưởng, Kaspersky Endpoint Security sẽ chặn kết nối mạng. Khi mở một tên miền có chứng chỉ không được tin tưởng trong một trình duyệt, Kaspersky Endpoint Security sẽ hiển thị một trang HTML giải thích rằng tên miền này bị chặn.
<p>Khi xảy ra lỗi quét kết nối được mã hóa</p>	<ul style="list-style-type: none"> • Chặn kết nối. Nếu mục này được chọn, khi xảy ra lỗi quét kết nối được mã hóa, Kaspersky Endpoint Security sẽ chặn kết nối mạng.

	<ul style="list-style-type: none"> • Thêm tên miền vào mục loại trừ. Nếu mục này được chọn, khi xảy ra lỗi quét kết nối được mã hóa, Kaspersky Endpoint Security sẽ thêm tên miền đã gây ra lỗi vào danh sách các tên miền có lỗi quét và không giám sát lưu lượng mạng được mã hóa khi truy cập tên miền này. Bạn chỉ có thể xem danh sách các tên miền có lỗi quét kết nối được mã hóa trong giao diện cục bộ của ứng dụng. Để xóa nội dung danh sách, bạn cần chọn Chặn kết nối. Kaspersky Endpoint Security cũng sẽ tạo ra một sự kiện cho lỗi quét kết nối được mã hóa.
Chặn các kết nối SSL 2.0 (khuyến dùng)	<p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ chặn các kết nối mạng được thiết lập qua giao thức SSL 2.0.</p> <p>Nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ không chặn các kết nối mạng được thiết lập qua giao thức SSL 2.0 và không giám sát lưu lượng mạng được truyền tải qua các kết nối này.</p>
Giải mã kết nối mã hóa với các website sử dụng chứng chỉ EV	<p>Các chứng chỉ EV (Chứng chỉ Chứng thực mở rộng) sẽ xác nhận tính xác thực của các website và tăng cường tính bảo mật của kết nối. Các trình duyệt sử dụng biểu tượng ổ khóa trong thanh địa chỉ của chúng để chỉ báo một trang web có chứng chỉ EV. Các trình duyệt cũng có thể tô màu toàn bộ hoặc một phần thanh địa chỉ bằng màu xanh lá cây.</p> <p>Nếu hộp kiểm được chọn, Kaspersky Endpoint Security sẽ giải mã và giám sát các kết nối được mã hóa với các website sử dụng chứng chỉ EV.</p> <p>Nếu hộp kiểm không được chọn, Kaspersky Endpoint Security sẽ không có quyền truy cập nội dung của lưu lượng HTTPS. Vì lý do này, ứng dụng sẽ chỉ giám sát lưu lượng HTTPS dựa trên địa chỉ website mà thôi, ví dụ như https://bing.com.</p> <p>Nếu bạn đang mở một website có chứng chỉ EV lần đầu tiên, kết nối được mã hóa sẽ được giải mã, cho dù hộp kiểm có được chọn hay không.</p>
Địa chỉ được tin tưởng	<p>Tính năng này sử dụng danh sách địa chỉ web mà Kaspersky Endpoint Security không quét kết nối mạng. Bạn có thể nhập một tên miền hoặc địa chỉ IP. Kaspersky Endpoint Security hỗ trợ ký tự * để nhập một tên đại diện trong tên miền.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Kaspersky Endpoint Security không hỗ trợ mặt nạ cho các địa chỉ IP. Bạn có thể nhập một dải địa chỉ IP vào giao diện cục bộ của ứng dụng (ví dụ: 198.51.100.0/24). Bạn không thể nhập một dải địa chỉ IP vào Bảng điều khiển Kaspersky Security Center.</p> </div> <p>Ví dụ:</p> <ul style="list-style-type: none"> • <code>domain.com</code> – bản ghi này gồm các địa chỉ sau: https://domain.com, https://www.domain.com, https://domain.com/page123. Bản ghi không bao gồm các tên miền con (ví dụ: subdomain.domain.com). • <code>subdomain.domain.com</code> – bản ghi bao gồm các địa chỉ sau: https://subdomain.domain.com, https://subdomain.domain.com/page123. Bản ghi không bao gồm tên miền <code>domain.com</code>. • <code>*.domain.com</code> – bản ghi này bao gồm các địa chỉ sau: https://movies.domain.com, https://images.domain.com/page123. Bản ghi không bao gồm tên miền <code>domain.com</code>.
Ứng dụng	<p>Danh sách các ứng dụng có hoạt động không bị giám sát bởi Kaspersky Endpoint Security trong hoạt động của nó. Bạn có thể chọn các loại hoạt động của ứng dụng</p>



<p>được tin tưởng</p>	<p>mà Kaspersky Endpoint Security sẽ không giám sát (ví dụ như không quét lưu lượng mạng). Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự * cùng ? khi nhập tên đại diện.</p>
<p>Sử dụng kho chứng chỉ đã chọn để quét các kết nối được mã hóa trong các ứng dụng Mozilla</p> <p><i>(chỉ khả dụng trong giao diện Kaspersky Endpoint Security)</i></p>	<p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ quét lưu lượng được mã hóa trong trình duyệt Mozilla Firefox và ứng dụng thư điện tử Thunderbird. Quyền truy cập vào một số website thông qua giao thức HTTPS có thể bị chặn.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Để quét lưu lượng trong trình duyệt Mozilla Firefox và ứng dụng thư điện tử Thunderbird, bạn phải bật Quét kết nối được mã hóa. Nếu Quét kết nối được mã hóa bị tắt, Kaspersky Endpoint Security sẽ không quét lưu lượng được mã hóa trong trình duyệt Mozilla Firefox và ứng dụng thư điện tử Thunderbird.</p> </div> <p>Kaspersky Endpoint Security sử dụng chứng chỉ gốc của Kaspersky để giải mã và phân tích lưu lượng được mã hóa. Bạn có thể chọn kho chứng chỉ chứa chứng chỉ gốc của Kaspersky.</p> <ul style="list-style-type: none"> • Sử dụng kho chứng chỉ Windows (khuyến dùng). Chứng chỉ gốc của Kaspersky được thêm vào kho này trong quá trình cài đặt Kaspersky Endpoint Security. • Sử dụng kho chứng chỉ Mozilla. Mozilla Firefox và Thunderbird sử dụng kho chứng chỉ của riêng họ. Nếu chọn kho chứng chỉ của Mozilla, bạn cần thêm chứng chỉ gốc Kaspersky vào kho này theo cách thủ công thông qua các thuộc tính của trình duyệt.

Giao diện

Bạn có thể cấu hình thiết lập của giao diện ứng dụng.

Cấu hình giao diện

Tham số	Mô tả
<p>Tương tác với người dùng</p> <p><i>(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)</i></p>	<p>With simplified interface. Trên một máy khách, cửa sổ chính của ứng dụng không thể truy cập và chỉ có biểu tượng trong khu vực thông báo của Windows khả dụng. Trong menu ngữ cảnh của biểu tượng, thực hiện số lượng giới hạn các hoạt động với Kaspersky Endpoint Security. Kaspersky Endpoint Security cũng sẽ hiển thị các thông báo trên biểu tượng của ứng dụng.</p> <p>With full interface. Trên một máy tính khách, cửa sổ chính của Kaspersky Endpoint Security và biểu tượng trong khu vực thông báo của Windows sẽ khả dụng. Trong menu ngữ cảnh của biểu tượng, người dùng có thể thực hiện các thao tác với Kaspersky Endpoint Security. Kaspersky Endpoint Security cũng sẽ hiển thị các thông báo trên biểu tượng của ứng dụng.</p> <p>Ẩn mục Giám sát hoạt động ứng dụng. Trên máy tính khách, trong cửa sổ chính của Kaspersky Endpoint Security, nút Giám sát hoạt động ứng dụng không khả dụng. <i>Giám sát hoạt động ứng dụng</i> là một công cụ được thiết kế để xem thông tin về hoạt động của các ứng dụng trên máy tính người dùng theo thời gian thực.</p> <p>No interface. Trên một máy khách, không có dấu hiệu hoạt động của Kaspersky Endpoint Security được hiển thị. Biểu tượng trong khu vực thông báo của Windows và các thông báo không khả dụng.</p>
<p>Thiết lập thông báo</p>	<p>Một bảng với cấu hình thông báo về các sự kiện có cấp độ quan trọng khác nhau có thể xảy ra trong quá trình hoạt động của một thành phần, tác vụ hoặc toàn bộ ứng</p>

	dụng. Kaspersky Endpoint Security sẽ hiển thị thông báo về các sự kiện này trên màn hình, gửi chúng qua email, hoặc ghi lại chúng.
Thiết lập thông báo email	Thiết lập máy chủ SMTP để gửi thông báo về các sự kiện được kích hoạt trong quá trình hoạt động của ứng dụng.
Hiển thị trạng thái của ứng dụng trong khu vực thông báo	Các danh mục sự kiện của ứng dụng khiến biểu tượng Kaspersky Endpoint Security thay đổi trong khu vực thông báo trên thanh tác vụ của Microsoft Windows ( hoặc ) và dẫn đến một thông báo nổi.
Thông báo trạng thái cơ sở dữ liệu diệt virus trên máy	Cấu hình thông báo về các cơ sở dữ liệu diệt virus lỗi thời được sử dụng bởi ứng dụng.
Bảo vệ bằng mật khẩu	<p>Nếu công tắc này được bật, Kaspersky Endpoint Security sẽ yêu cầu người dùng nhập mật khẩu khi người dùng cố thực hiện một hoạt động trong phạm vi của Bảo vệ bằng mật khẩu. Phạm vi Bảo vệ bằng mật khẩu bao gồm các hoạt động bị cấm (như tắt các thành phần bảo vệ) và tài khoản của người dùng có phạm vi Bảo vệ bằng mật khẩu được áp dụng.</p> <p>Sau khi bật Bảo vệ bằng mật khẩu, Kaspersky Endpoint Security sẽ yêu cầu bạn đặt một mật khẩu để thực hiện các hoạt động.</p>
Technical Support web resources <i>(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)</i>	Danh sách liên kết đến các tài nguyên web chứa thông tin hỗ trợ kỹ thuật cho Kaspersky Endpoint Security. Các liên kết được bổ sung sẽ được hiển thị trong cửa sổ Hỗ trợ của giao diện cục bộ của Kaspersky Endpoint Security, thay cho các liên kết tiêu chuẩn.
Message to user <i>(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)</i>	Thông báo được hiển thị trong cửa sổ Hỗ trợ của giao diện cục bộ của Kaspersky Endpoint Security.

Quản lý thiết lập

Bạn có thể lưu thiết lập Kaspersky Endpoint Security hiện tại vào một tập tin và sử dụng chúng để nhanh chóng cấu hình ứng dụng trên một máy tính khác. Bạn cũng có thể sử dụng tập tin cấu hình khi triển khai ứng dụng thông qua Kaspersky Security Center bằng một [gói cài đặt](#). Bạn có thể khôi phục thiết lập mặc định bất kỳ lúc nào.

Thiết lập quản lý cấu hình ứng dụng chỉ khả dụng trong giao diện Kaspersky Endpoint Security.

Thiết lập quản lý cấu hình ứng dụng

Cấu hình	Mô tả
Nhập	Giải nén ứng dụng cài đặt từ một tập tin ở định dạng CFG và áp dụng chúng.
Xuất	Lưu các thiết lập ứng dụng hiện tại vào một tập tin ở định dạng CFG.
Khôi phục	Bạn có thể khôi phục các thiết lập mặc định theo khuyến nghị của Kaspersky cho Endpoint Security bất kỳ thời điểm nào. Khi thiết lập được khôi phục, mức độ bảo mật Khuyến dùng được thiết lập cho tất cả các thành phần bảo vệ.

Cập nhật cơ sở dữ liệu và các mô-đun phần mềm 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 mới 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 đang sử dụng một máy chủ proxy, bạn cần cấu hình thiết lập máy chủ proxy.

Các bản cập nhật được tải về qua giao thức HTTPS. Chúng cũng có thể được tải về qua giao thức HTTP khi bạn không thể tải về bản cập nhật qua giao thức HTTPS.

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. 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 lỗi hỏng 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 cửa sổ chính của ứng dụng hoặc chú giải công cụ mà bạn nhìn thấy khi di con trỏ qua biểu tượng của ứng dụng trong vùng thông báo.

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](#).

Thiết lập cập nhật mô-đun ứng dụng và cơ sở dữ liệu

Tham số	Mô tả
Lịch cập nhật cơ sở dữ liệu	<p>Tự động. Trong chế độ này, Kaspersky Endpoint Security sẽ kiểm tra nguồn cập nhật để xác định tình trạng sẵn có của các gói cập nhật mới với tần suất nhất định. Tần suất kiểm tra gói cập nhật sẽ tăng lên trong các kỳ bùng phát virus và giảm khi không có gì. Sau khi phát hiện một gói cập nhật mới, Kaspersky Endpoint Security sẽ tải nó về và cài đặt trên máy tính của bạn.</p> <p>Thủ công. Chế độ chạy tác vụ cập nhật này cho phép bạn khởi chạy thủ công tác vụ cập nhật.</p> <p>Theo lịch. Trong chế độ chạy tác vụ cập nhật này, Kaspersky Endpoint Security sẽ chạy tác vụ cập nhật theo lịch mà bạn đã quy định. Nếu chế độ chạy tác vụ cập nhật này được chọn, bạn cũng có thể khởi động tác vụ cập nhật của Kaspersky Endpoint Security một cách thủ công.</p>
Run missed tasks	<p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ bắt đầu lại tác vụ cập nhật bị bỏ qua ngay khi có thể. Tác vụ cập nhật có thể bị bỏ qua, ví dụ như khi máy tính được tắt vào thời điểm bắt đầu tác vụ cập nhật.</p> <p>Khi hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ không bắt đầu các tác vụ cập nhật đã bị lỡ. Thay vào đó, ứng dụng sẽ chạy tác vụ cập nhật kế tiếp dựa theo lịch hiện tại.</p>
Nguồn cập nhật	<p><i>Nguồn cập nhật</i> là một tài nguyên chứa các bản cập nhật cơ sở dữ liệu và mô-đun ứng dụng của Kaspersky Endpoint Security.</p> <p>Nguồn cập nhật bao gồm máy chủ Kaspersky Security Center và Kaspersky, máy chủ cập nhật của Kaspersky và các thư mục cục bộ hoặc thư mục mạng.</p> <p>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.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"><p>Kaspersky Endpoint Security không hỗ trợ các bản cập nhật từ máy chủ HTTPS, trừ khi chúng là các máy chủ cập nhật của Kaspersky.</p></div>

	<p>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.</p>
<p>Chạy cập nhật cơ sở dữ liệu với quyền</p>	<p>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 một nguồn cập nhật không được cấu hình máy chủ proxy. 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.</p>
<p>Tải xuống các bản cập nhật của mô-đun ứng dụng</p>	<p>Tải xuống các bản cập nhật mô-đun ứng dụng cùng các bản cập nhật cơ sở dữ liệu ứng dụng.</p> <p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ thông báo với người dùng về các bản cập nhật mô-đun ứng dụng khả dụng và bao gồm các bản cập nhật mô-đun ứng dụng trong gói cập nhật trong khi thực thi tác vụ cập nhật. Cách các bản cập nhật mô-đun ứng dụng được áp dụng được xác định bởi thiết lập sau:</p> <ul style="list-style-type: none"> • Cài đặt các bản cập nhật quan trọng và được phê duyệt. Nếu tùy chọn này được lựa chọn, khi có các bản cập nhật mô-đun ứng dụng, Kaspersky Endpoint Security sẽ tự động cài đặt các bản cập nhật thiết yếu, và chỉ cài đặt tất cả các bản cập nhật mô-đun ứng dụng khác sau khi chúng đã được phê duyệt cục bộ thông qua giao diện ứng dụng hoặc qua Kaspersky Security Center. • Chỉ cài đặt các bản cập nhật được phê duyệt. Nếu tùy chọn này được lựa chọn, khi có các bản cập nhật mô-đun ứng dụng, Kaspersky Endpoint Security sẽ chỉ cài đặt chúng sau khi chúng đã được phê duyệt cục bộ thông qua giao diện ứng dụng hoặc qua Kaspersky Security Center. Tùy chọn này được chọn mặc định. <p>Nếu hộp kiểm này được xóa, Kaspersky Endpoint Security sẽ không thông báo với người dùng về các bản cập nhật mô-đun ứng dụng khả dụng và không bao gồm các bản cập nhật mô-đun ứng dụng trong gói cập nhật trong khi thực thi tác vụ cập nhật.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Nếu các bản cập nhật mô-đun ứng dụng yêu cầu việc xem lại và chấp nhận các điều khoản của Thỏa thuận giấy phép người dùng cuối, ứng dụng sẽ chỉ cài đặt các bản cập nhật sau khi các điều khoản của Thỏa thuận giấy phép người dùng cuối đã được chấp nhận.</p> </div> <p>Hộp kiểm này được chọn theo mặc định.</p>
<p>Sao chép các bản cập nhật vào thư mục</p>	<p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ sao chép gói cập nhật đến thư mục được chia sẻ được quy định dưới hộp kiểm. Sau đó, các máy tính khác trên mạng LAN của bạn sẽ có thể nhận gói cập nhật từ thư mục được chia sẻ này. Điều này làm giảm lưu lượng Internet bởi gói cập nhật sẽ chỉ được tải về một lần. Thư mục sau được chỉ định theo mặc định: C:\ProgramData\Kaspersky Lab\KES\Update distribution\.</p>
<p>Máy chủ proxy cho các bản cập nhật</p>	<p>Thiết lập máy chủ proxy để truy cập Internet của người dùng máy khách để cập nhật mô-đun ứng dụng và cơ sở dữ liệu.</p> <p>Để cấu hình tự động máy chủ proxy, Kaspersky Endpoint Security sử dụng giao thức WPAD (Giao thức tự động phát hiện web proxy). Nếu không thể xác định địa chỉ IP của máy chủ proxy bằng giao thức này, Kaspersky Endpoint Security sẽ sử dụng địa chỉ máy chủ proxy được đặt trong thiết lập của trình duyệt Microsoft Internet Explorer.</p>

<p><i>(chỉ khả dụng trong giao diện Kaspersky Endpoint Security)</i></p>	
<p>Bỏ qua máy chủ proxy đối với các địa chỉ cục bộ <i>(chỉ khả dụng trong giao diện Kaspersky Endpoint Security)</i></p>	<p>Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ không sử dụng một máy chủ proxy khi thực hiện tác vụ cập nhật từ một thư mục được chia sẻ.</p>

Phụ lục 2. Các nhóm tin tưởng của ứng dụng

Kaspersky Endpoint Security phân loại tất cả các ứng dụng được khởi động trên máy tính vào các nhóm tin tưởng. Các ứng dụng được phân loại thành các nhóm tin tưởng tùy vào cấp độ đe dọa mà ứng dụng đó có thể gây ra cho hệ điều hành.

Các nhóm tin tưởng được chia như sau:

- **Tin tưởng.** Nhóm này bao gồm các ứng dụng đáp ứng một hoặc nhiều điều kiện sau đây:
 - Các ứng dụng được ký điện tử bởi các nhà cung cấp được tin tưởng.
 - Các ứng dụng được ghi vào cơ sở dữ liệu ứng dụng được tin tưởng của Kaspersky Security Network.
 - Người dùng đã đặt ứng dụng vào trong nhóm Được Tin tưởng.

Không có hoạt động nào bị ngăn cấm cho các ứng dụng này.

- **Giới hạn mức Thấp.** Nhóm này bao gồm các ứng dụng đáp ứng các điều kiện sau đây:
 - Các ứng dụng không được ký điện tử bởi các nhà cung cấp được tin tưởng.
 - Các ứng dụng không được ghi vào cơ sở dữ liệu ứng dụng được tin tưởng của Kaspersky Security Network.
 - Người dùng đã đặt ứng dụng vào trong nhóm "Hạn chế thấp".

Các ứng dụng này phải chịu những hạn chế tối thiểu trong việc truy cập tài nguyên hệ điều hành.

- **Giới hạn mức Cao.** Nhóm này bao gồm các ứng dụng đáp ứng các điều kiện sau đây:
 - Các ứng dụng không được ký điện tử bởi các nhà cung cấp được tin tưởng.

- Các ứng dụng không được ghi vào cơ sở dữ liệu ứng dụng được tin tưởng của Kaspersky Security Network.
- Người dùng đã đặt ứng dụng vào trong nhóm "Giới hạn mức Cao".

Các ứng dụng này phải chịu những hạn chế cao trong việc truy cập tài nguyên hệ điều hành.

- **Không Tin tưởng.** Nhóm này bao gồm các ứng dụng đáp ứng các điều kiện sau đây:
 - Các ứng dụng không được ký điện tử bởi các nhà cung cấp được tin tưởng.
 - Các ứng dụng không được ghi vào cơ sở dữ liệu ứng dụng được tin tưởng của Kaspersky Security Network.
 - Người dùng đã đặt ứng dụng vào trong nhóm Không Tin tưởng.

Với các ứng dụng như vậy, tất cả các hoạt động đều bị chặn.

Phụ lục 3. Phần mở rộng tập tin để quét nhanh ổ đĩa di động

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 Nhóm 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

Ink – 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 – email Microsoft Outlook Express

nws – email mới của Microsoft Outlook Express

msg – email Microsoft Mail

plg – email

mbx – 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;

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, xlsx 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

Phụ lục 4. Các loại tập tin cho bộ lọc đính kèm Bảo vệ mỗi đe dọa thư điện tử

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 tập tin đính kèm email, thành phần Bảo vệ mỗi đe dọa 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 – email Microsoft Outlook Express

nws – email mới của Microsoft Outlook Express

msg – email Microsoft Mail

plg – email

mbx – 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;

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, xlsx 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

Phụ lục 5. Thiết lập mạng để tương tác với các dịch vụ bên ngoài

Kaspersky Endpoint Security sử dụng các thiết lập mạng sau để tương tác với các dịch vụ bên ngoài.

Thiết lập mạng

Địa chỉ	Mô tả
activation- v2.kaspersky.com/activation-service/activation-service.svc Giao thức: HTTPS Cổng: 443	Kích hoạt ứng dụng.
s00.upd.kaspersky.com s01.upd.kaspersky.com s02.upd.kaspersky.com s03.upd.kaspersky.com s04.upd.kaspersky.com	Cập nhật cơ sở dữ liệu và các mô-đun phần mềm ứng dụng.

s05.upd.kaspersky.com
s06.upd.kaspersky.com
s07.upd.kaspersky.com
s08.upd.kaspersky.com
s09.upd.kaspersky.com
s10.upd.kaspersky.com
s11.upd.kaspersky.com
s12.upd.kaspersky.com
s13.upd.kaspersky.com
s14.upd.kaspersky.com
s15.upd.kaspersky.com
s16.upd.kaspersky.com
s17.upd.kaspersky.com
s18.upd.kaspersky.com
s19.upd.kaspersky.com
cm.k.kaspersky-labs.com

Giao thức: HTTPS

Cổng: 443

downloads.upd.kaspersky.com

Giao thức: HTTPS

Cổng: 443

- Cập nhật cơ sở dữ liệu và các mô-đun phần mềm ứng dụng.
- Kiểm tra xem các máy chủ Kaspersky có thể truy cập không. Nếu không thể truy cập các máy chủ bằng DNS hệ thống thì ứng dụng sẽ sử dụng DNS công cộng. Đây là điều cần thiết để đảm bảo cơ sở dữ liệu chống virus được cập nhật và duy trì cấp độ bảo mật cho máy tính. Kaspersky Endpoint Security sử dụng danh sách các máy chủ DNS công cộng sau, theo trình tự sau:
 1. DNS công cộng của Google (8.8.8.8).
 2. Cloudflare DNS (1.1.1.1).
 3. Alibaba Cloud DNS (223.6.6.6).
 4. Quad9 DNS (9.9.9.9).
 5. CleanBrowsing (185.228.168.168).





	<p>Các yêu cầu được ứng dụng đưa ra có thể chứa địa chỉ của các miền và địa chỉ IP công cộng của người dùng vì ứng dụng thiết lập kết nối TCP/UDP với máy chủ DNS. Ví dụ: đây là thông tin cần thiết để xác thực chứng chỉ của tài nguyên web khi sử dụng giao thức HTTPS. Nếu Kaspersky Endpoint Security đang sử dụng máy chủ DNS công cộng, việc xử lý dữ liệu được điều chỉnh bởi chính sách bảo mật của dịch vụ liên quan. Nếu bạn muốn ngăn Kaspersky Endpoint Security sử dụng máy chủ DNS công cộng, hãy liên hệ với bộ phận Hỗ trợ kỹ thuật để có bản vá riêng.</p>
<p>touch.kaspersky.com Giao thức: HTTP</p>	<ul style="list-style-type: none"> • Nhận thời gian được tin tưởng để kiểm tra thời hạn hiệu lực của chứng chỉ (kết nối TLS). • Cảnh báo về quyền truy cập bị từ chối vào một tài nguyên web trong trình duyệt (Bảo vệ mỗi đe dọa web và Kiểm soát Web).
<p>p00.upd.kaspersky.com p01.upd.kaspersky.com p02.upd.kaspersky.com p03.upd.kaspersky.com p04.upd.kaspersky.com p05.upd.kaspersky.com p06.upd.kaspersky.com p07.upd.kaspersky.com p08.upd.kaspersky.com p09.upd.kaspersky.com p10.upd.kaspersky.com p11.upd.kaspersky.com</p>	<p>Cập nhật cơ sở dữ liệu và các mô-đun phần mềm ứng dụng.</p>

<p>p12.upd.kaspersky.com p13.upd.kaspersky.com p14.upd.kaspersky.com p15.upd.kaspersky.com p16.upd.kaspersky.com p17.upd.kaspersky.com p18.upd.kaspersky.com p19.upd.kaspersky.com downloads.kaspersky-labs.com cm.k.kaspersky-labs.com Giao thức: HTTP Cổng: 80</p>	
<p>ds.kaspersky.com Giao thức: HTTPS Cổng: 443</p>	Sử dụng Kaspersky Security Network.
<p>ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com Giao thức: Any Cổng: 443, 1443</p>	Sử dụng Kaspersky Security Network.
<p>click.kaspersky.com redirect.kaspersky.com Giao thức: HTTPS</p>	Theo các liên kết trong giao diện.
<p>cr1.kaspersky.com ocsp.kaspersky.com Giao thức: HTTP Cổng: 80</p>	Cơ sở hạ tầng khóa công khai (PKI).

Phụ lục 6. Các sự kiện ứng dụng

Thông tin về hoạt động của mỗi thành phần Kaspersky Endpoint Security, sự kiện mã hóa dữ liệu, tình trạng hoàn thành của mỗi tác vụ quét, tác vụ cập nhật và tác vụ kiểm tra tính toàn vẹn, và hoạt động tổng thể của ứng dụng sẽ được ghi trong nhật ký sự kiện của Kaspersky Security Center và nhật ký sự kiện của Windows.




Kaspersky Endpoint Security sẽ tạo các loại sự kiện sau: sự kiện chung và sự kiện cụ thể. Các sự kiện cụ thể chỉ được tạo bởi Kaspersky Endpoint Security cho Windows. Các sự kiện cụ thể có một ID đơn giản như 000000cb. Mỗi sự kiện cụ thể chứa các tham số bắt buộc sau:

- GNRL_EA_DESCRIPTION là nội dung của sự kiện.
- GNRL_EA_ID là ID dịch vụ của sự kiện.
- GNRL_EA_SEVERITY là trạng thái của sự kiện. 1 - Thông báo thông tin , 2 - Cảnh báo , 3 - Lỗi chức năng , 4 - Nghiêm trọng .
- EVENT_TYPE_DISPLAY_NAME là tiêu đề của sự kiện.
- TASK_DISPLAY_NAME là tên của thành phần ứng dụng đã khởi tạo sự kiện.



Các sự kiện chung có thể được tạo bởi Kaspersky Endpoint Security cho Windows cũng như các ứng dụng Kaspersky khác (ví dụ: Kaspersky Security cho Windows Server). Các sự kiện chung có ID phức tạp hơn như GNRL_EV_VIRUS_FOUND. Ngoài các thiết lập bắt buộc, các sự kiện chung còn chứa các thiết lập nâng cao.

Sự kiện nghiêm trọng

Thỏa thuận giấy phép người dùng cuối đã bị vi phạm

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	201
ID sự kiện Kaspersky Security Center	GNRL_EV_LICENSE_EXPIRATION
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Giấy phép sắp hết hạn

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	203
ID sự kiện Kaspersky Security Center	000000cb
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	


Cơ sở dữ liệu bị thiếu hoặc hư hỏng

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	206
ID sự kiện Kaspersky Security Center	000000ce
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-



Cơ sở dữ liệu đã cũ

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	207
ID sự kiện Kaspersky Security Center	000000cf
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Chế độ chạy tự động của ứng dụng bị vô hiệu

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	209
ID sự kiện Kaspersky Security Center	000000d1
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	


Lỗi kích hoạt

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	229
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Phát hiện mối đe dọa đang hoạt động. Nên khởi chạy Khử mã độc nâng cao

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	231
ID sự kiện Kaspersky Security Center	000000e7
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Máy chủ KSN không khả dụng

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	2023
ID sự kiện Kaspersky Security Center	000007e7
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Không đủ không gian trống trong ổ lưu trữ của Khu vực cách ly

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	343
ID sự kiện Kaspersky Security Center	00000157
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Đối tượng được khôi phục từ Khu vực cách ly

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	346
ID sự kiện Kaspersky Security Center	0000015a
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Đối tượng không được xóa khỏi Khu vực cách ly

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	348
ID sự kiện Kaspersky Security Center	0000015c
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Đã thiết lập kết nối với một tên miền có chứng chỉ không được tin tưởng 

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	57
ID sự kiện Kaspersky Security Center	00000039
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓




Không thể xác minh một kết nối được mã hóa. Tên miền được thêm vào danh sách loại trừ 

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	60
ID sự kiện Kaspersky Security Center	0000003c
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓




Đã phát hiện đối tượng độc hại (cơ sở cục bộ) 

Trạng thái	
Thành phần	Bảo vệ mối đe dọa tập tin Bảo vệ mối đe dọa web Bảo vệ mối đe dọa thư điện tử Bảo vệ AMSI Phòng chống xâm nhập máy chủ Phát hiện hành vi Phòng chống khai thác Quét virus
ID sự kiện Windows	302
ID sự kiện Kaspersky Security Center	GNRL_EV_VIRUS_FOUND
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 là hash của đối tượng (SHA256). • GNRL_EA_PARAM_2 là tên của đối tượng. • GNRL_EA_PARAM_5 là tên của mối đe dọa phù hợp với phân loại của Kaspersky, ví dụ: EICAR-Test-File. • GNRL_EA_PARAM_7 là tên của người dùng phiên. • GNRL_EA_PARAM_8 là loại mối đe dọa, ví dụ: Trojware. • GNRL_EA_PARAM_9 là thông tin bổ sung về đối tượng được phát hiện: Thành phần ứng dụng (engine). Công nghệ phát hiện mối đe dọa (method). Mối đe dọa được phát hiện bởi KSN Riêng (<code>denylist</code>): true hoặc false. Phiên bản EDR. Định danh mối đe dọa trong EDR. Giá trị hash MD5 của đối tượng.
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓



[Đã phát hiện đối tượng độc hại \(KSN\)](#) 

Trạng thái	
Thành phần	Bảo vệ mối đe dọa tập tin Bảo vệ mối đe dọa web Bảo vệ mối đe dọa thư điện tử Bảo vệ AMSI Phòng chống xâm nhập máy chủ Phát hiện hành vi Phòng chống khai thác Quét virus
ID sự kiện Windows	302
ID sự kiện Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_BY_KSN
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 là hash của đối tượng (SHA256). • GNRL_EA_PARAM_2 là tên của đối tượng. • GNRL_EA_PARAM_5 là tên của mối đe dọa phù hợp với phân loại của Kaspersky, ví dụ: EICAR-Test-File. • GNRL_EA_PARAM_7 là tên của người dùng phiên. • GNRL_EA_PARAM_8 là loại mối đe dọa, ví dụ: Trojware. • GNRL_EA_PARAM_9 là thông tin bổ sung về đối tượng được phát hiện: Thành phần ứng dụng (engine). Công nghệ phát hiện mối đe dọa (method). Mối đe dọa được phát hiện bởi KSN Riêng (<code>denylist</code>): true hoặc false. Phiên bản EDR. Định danh mối đe dọa trong EDR. Giá trị hash MD5 của đối tượng.
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	




Không thể khử mã độc 

Trạng thái	
Thành phần	Bảo vệ mối đe dọa tập tin Bảo vệ mối đe dọa thư điện tử Phòng chống xâm nhập máy chủ Quét virus
ID sự kiện Windows	312
ID sự kiện Kaspersky Security Center	GNRL_EV_OBJECT_NOTCURED
Tham số sự kiện	<ul style="list-style-type: none"> GNRL_EA_PARAM_1 là hash của đối tượng (SHA256). GNRL_EA_PARAM_2 là tên của đối tượng. GNRL_EA_PARAM_5 là tên của mối đe dọa phù hợp với phân loại của Kaspersky, ví dụ: EICAR-Test-File. GNRL_EA_PARAM_7 là tên của người dùng phiên. GNRL_EA_PARAM_8 là loại mối đe dọa, ví dụ: Trojware. GNRL_EA_PARAM_9 là thông tin bổ sung về đối tượng được phát hiện: Thành phần ứng dụng (engine). Công nghệ phát hiện mối đe dọa (method). Mối đe dọa được phát hiện bởi KSN Riêng (denylist): true hoặc false. Phiên bản EDR. Định danh mối đe dọa trong EDR. Giá trị hash MD5 của đối tượng.
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



[Không thể xóa](#)

Trạng thái	
Thành phần	Bảo vệ mối đe dọa tập tin Phòng chống xâm nhập máy chủ Phát hiện hành vi Quét virus
ID sự kiện Windows	313
ID sự kiện Kaspersky Security Center	00000139
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	


[Lỗi xử lý](#)

Trạng thái	
Thành phần	Bảo vệ mối đe dọa tập tin Bảo vệ mối đe dọa web Bảo vệ mối đe dọa thư điện tử Phòng chống xâm nhập máy chủ Bảo vệ AMSI Quét virus
ID sự kiện Windows	317
ID sự kiện Kaspersky Security Center	0000013d
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	




Chăm dứt tiến trình

Trạng thái	
Thành phần	Bảo vệ mối đe dọa tập tin Phòng chống xâm nhập máy chủ Phát hiện hành vi Quét virus
ID sự kiện Windows	452
ID sự kiện Kaspersky Security Center	000001c4
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	




Không thể chăm dứt tiến trình

Trạng thái	
Thành phần	Bảo vệ mối đe dọa tập tin Phòng chống xâm nhập máy chủ Phát hiện hành vi Quét virus
ID sự kiện Windows	453
ID sự kiện Kaspersky Security Center	000001c5
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-




Đã chặn liên kết nguy hiểm

Trạng thái	
Thành phần	Bảo vệ mối đe dọa web
ID sự kiện Windows	362
ID sự kiện Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_BLOCKED
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_2 là đường dẫn đến đối tượng. • GNRL_EA_PARAM_5 là tên của đối tượng theo phân loại của Kaspersky. • GNRL_EA_PARAM_7 là tên của người dùng phiên. • GNRL_EA_PARAM_8 là loại mối đe dọa, ví dụ: Trojware. • GNRL_EA_PARAM_9 là thông tin bổ sung về đối tượng được phát hiện: Thành phần ứng dụng (engine). Công nghệ phát hiện mối đe dọa (method). Mối đe dọa được phát hiện bởi KSN Riêng (denylist): true hoặc false.
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



[Liên kết nguy hiểm đã được mở](#)

Trạng thái	
Thành phần	Bảo vệ mối đe dọa web
ID sự kiện Windows	363
ID sự kiện Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_REPORTED
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_2 là đường dẫn đến đối tượng. • GNRL_EA_PARAM_5 là tên của đối tượng theo phân loại của Kaspersky. • GNRL_EA_PARAM_7 là tên của người dùng phiên. • GNRL_EA_PARAM_8 là loại mối đe dọa, ví dụ: Trojware. • GNRL_EA_PARAM_9 là thông tin bổ sung về đối tượng được phát hiện: Thành phần ứng dụng (engine). Công nghệ phát hiện mối đe dọa (method). Mối đe dọa được phát hiện bởi KSN Riêng (denylist): true hoặc false.
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	




[Phát hiện liên kết nguy hiểm đã được mở ra trước đây](#)

Trạng thái	
Thành phần	Bảo vệ mối đe dọa web
ID sự kiện Windows	1201
ID sự kiện Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_PASSED
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_2 là đường dẫn đến đối tượng. • GNRL_EA_PARAM_5 là tên của đối tượng theo phân loại của Kaspersky. • GNRL_EA_PARAM_7 là tên của người dùng phiên. • GNRL_EA_PARAM_8 là loại mối đe dọa, ví dụ: Trojware. • GNRL_EA_PARAM_9 là thông tin bổ sung về đối tượng được phát hiện: Thành phần ứng dụng (engine). Công nghệ phát hiện mối đe dọa (method). Mối đe dọa được phát hiện bởi KSN Riêng (denylist): true hoặc false.
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Hành động của tiến trình bị chặn

Trạng thái	
Thành phần	Kiểm soát thích ứng sự cố
ID sự kiện Windows	2200
ID sự kiện Kaspersky Security Center	GNRL_EV_ADSEC_DETECT
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 là tên của quy tắc Kiểm soát thích ứng sự cố. • GNRL_EA_PARAM_2 là ID của quy tắc phân tích hành vi. • GNRL_EA_PARAM_3 là tên của người dùng phiên. • GNRL_EA_PARAM_4 là tiến trình nguồn. • GNRL_EA_PARAM_5 là đối tượng nguồn. • GNRL_EA_PARAM_6 là tiến trình đích. • GNRL_EA_PARAM_7 là đối tượng đích. • GNRL_EA_PARAM_8 là thông tin bổ sung về đối tượng được phát hiện: Giá trị băm của tiến trình/đối tượng nguồn và tiến trình/đối tượng đích. Tiến trình bị chặn (verdict_type): true hoặc false. ID bảo mật của người dùng (SID).
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Bàn phím không được cho phép

Trạng thái	
Thành phần	Phòng chống Tấn công BadUSB
ID sự kiện Windows	2051
ID sự kiện Kaspersky Security Center	00000803
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	




Yêu cầu AMSI đã bị chặn

Trạng thái	
Thành phần	Bảo vệ AMSI
ID sự kiện Windows	2200
ID sự kiện Kaspersky Security Center	00000898
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Hoạt động mạng bị ngăn chặn

Trạng thái	
Thành phần	Tường lửa
ID sự kiện Windows	602
ID sự kiện Kaspersky Security Center	00000329
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Đã phát hiện tấn công mạng

Trạng thái	
Thành phần	Bảo vệ mối đe dọa mạng
ID sự kiện Windows	651
ID sự kiện Kaspersky Security Center	GNRL_EV_ATTACK_DETECTED
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 là tên của cuộc tấn công. • GNRL_EA_PARAM_2 là giao thức. • GNRL_EA_PARAM_3 là địa chỉ IP của máy tính đóng vai trò là nguồn tấn công mạng. Địa chỉ IP được chỉ định theo thứ tự byte của máy chủ. Ví dụ: 2886729929 cho 172.16.0.201. • GNRL_EA_PARAM_4 là số cổng. • GNRL_EA_PARAM_5 là địa chỉ IPv6, ví dụ: 12B012B012B012B012B012B012B012B012B012B012B0. • GNRL_EA_PARAM_6 là địa chỉ IP của máy tính bị tấn công mạng. Địa chỉ IP được chỉ định theo thứ tự byte của máy chủ. Ví dụ: 2886729929 cho 172.16.0.201.
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Cấm khởi động ứng dụng

Trạng thái	
Thành phần	Kiểm soát ứng dụng
ID sự kiện Windows	702
ID sự kiện Kaspersky Security Center	GNRL_EV_APPLICATION_LAUNCH_DENIED
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_2 là tên của người dùng phiên. • GNRL_EA_PARAM_3 là định danh của danh mục được tạo theo cách thủ công. • GNRL_EA_PARAM_4 là ID danh mục ứng dụng. • GNRL_EA_PARAM_5 là thông tin về chữ ký số của ứng dụng. • GNRL_EA_PARAM_6 là tên của tập tin thực thi của ứng dụng (ví dụ: chrome.exe). • GNRL_EA_PARAM_7 là đường dẫn đến tập tin thực thi. • GNRL_EA_PARAM_8 là hash của đối tượng (SHA256). • GNRL_EA_PARAM_9 là phiên bản của ứng dụng mà người dùng đang cố chạy.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Tiến trình bị nghiêm cấm được bắt đầu trước khi Kaspersky Endpoint Security khởi động

Trạng thái	
Thành phần	Kiểm soát ứng dụng
ID sự kiện Windows	710
ID sự kiện Kaspersky Security Center	000002c6
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Truy cập bị từ chối (cơ sở nội bộ)

Trạng thái	
Thành phần	Kiểm soát Web
ID sự kiện Windows	752
ID sự kiện Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 là URL. • GNRL_EA_PARAM_2 là tên của người dùng phiên. • GNRL_EA_PARAM_3 là tên của quy tắc Kiểm soát Web.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



[Truy cập bị từ chối \(KSN\)](#)

Trạng thái	
Thành phần	Kiểm soát Web
ID sự kiện Windows	752
ID sự kiện Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED_BY_KSN
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 là URL. • GNRL_EA_PARAM_2 là tên của người dùng phiên. • GNRL_EA_PARAM_3 là tên của quy tắc Kiểm soát Web.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



[Hoạt động với thiết bị bị chặn](#)

Trạng thái	
Thành phần	Kiểm soát Thiết bị
ID sự kiện Windows	802
ID sự kiện Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Tham số sự kiện	<ul style="list-style-type: none"> GNRL_EA_PARAM_1 là ID phần cứng (HWID). GNRL_EA_PARAM_2 là tên của người dùng phiên.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	


Kết nối mạng bị chặn

Trạng thái	
Thành phần	Kiểm soát Thiết bị
ID sự kiện Windows	809
ID sự kiện Kaspersky Security Center	00000329
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Lỗi cập nhật thành phần

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1011
ID sự kiện Kaspersky Security Center	000003f3
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Lỗi phân bổ các bản cập nhật thành phần

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1012
ID sự kiện Kaspersky Security Center	000003f4
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-



Lỗi cập nhật nội bộ

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1014
ID sự kiện Kaspersky Security Center	000003f6
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-



Lỗi cập nhật mạng

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1015
ID sự kiện Kaspersky Security Center	000003f7
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Không thể chạy cùng lúc hai tác vụ

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1017
ID sự kiện Kaspersky Security Center	000003f9
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Lỗi xác nhận cơ sở dữ liệu và mô-đun cho ứng dụng

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1018
ID sự kiện Kaspersky Security Center	000003fa
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Lỗi tương tác với Kaspersky Security Center

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1019
ID sự kiện Kaspersky Security Center	000003fb
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	


Không phải tất cả thành phần đã được cập nhật

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1021
ID sự kiện Kaspersky Security Center	000003fd
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Cập nhật hoàn tất thành công, phân phối các bản cập nhật thất bại

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1023
ID sự kiện Kaspersky Security Center	000003ff
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-


Lỗi tác vụ nội bộ

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	101
ID sự kiện Kaspersky Security Center	00000065
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Cài đặt bản vá thất bại

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	2153
ID sự kiện Kaspersky Security Center	00000869
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	




Hoàn tác bản vá thất bại

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	2156
ID sự kiện Kaspersky Security Center	0000086c
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Lỗi áp dụng quy tắc mã hóa / giải mã tập tin

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	904
ID sự kiện Kaspersky Security Center	00000388
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Lỗi mã hóa / giải mã tập tin

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	912
ID sự kiện Kaspersky Security Center	GNRL_EV_ENCRYPTION_ERROR
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 là đường dẫn đến tập tin. • GNRL_EA_PARAM_2 là nguyên nhân của lỗi. • GNRL_EA_PARAM_3 là loại của thiết bị.
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

[Truy cập tập tin bị chặn](#)

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	940
ID sự kiện Kaspersky Security Center	GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 là đối tượng đích. • GNRL_EA_PARAM_2 là tên của người dùng phiên. • GNRL_EA_PARAM_3 là tên của tập tin thực thi (ví dụ: chrome.exe), đang cố gắng lấy quyền truy cập vào tập tin.
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-


[Lỗi bật chế độ di động](#)

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	951
ID sự kiện Kaspersky Security Center	000003b7
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Lỗi tắt chế độ di động

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	953
ID sự kiện Kaspersky Security Center	000003b9
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Lỗi tạo gói mã hóa

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	931
ID sự kiện Kaspersky Security Center	000003a3
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Lỗi mã hóa / giải mã thiết bị

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1305
ID sự kiện Kaspersky Security Center	00000519
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Không thể nạp mô-đun mã hóa

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1311
ID sự kiện Kaspersky Security Center	0000051f
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Tác vụ để quản lý tài khoản Authentication Agent đã kết thúc với lỗi

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1340
ID sự kiện Kaspersky Security Center	0000053c
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Không thể áp dụng chính sách

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	1312
ID sự kiện Kaspersky Security Center	00000520
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Nâng cấp FDE đã thất bại

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1342
ID sự kiện Kaspersky Security Center	0000053e
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Không thể hoàn tác nâng cấp FDE (để biết thêm thông tin, vui lòng tham khảo Trợ giúp trực tuyến của Kaspersky Endpoint Security cho Windows) 

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1344
ID sự kiện Kaspersky Security Center	00000540
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Máy chủ Kaspersky Anti Targeted Attack Platform không khả dụng

Trạng thái	
Thành phần	Cảm biến điểm cuối
ID sự kiện Windows	2100
ID sự kiện Kaspersky Security Center	00000834
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Không thể xóa đối tượng

Trạng thái	
Thành phần	Kaspersky Sandbox
ID sự kiện Windows	2252
ID sự kiện Kaspersky Security Center	000008cc
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Đối tượng không được cách ly (Kaspersky Sandbox)

Trạng thái	
Thành phần	Kaspersky Sandbox
ID sự kiện Windows	2603
ID sự kiện Kaspersky Security Center	00000a2b
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Đã xảy ra một lỗi bên trong

Trạng thái	
Thành phần	Kaspersky Sandbox
ID sự kiện Windows	2607
ID sự kiện Kaspersky Security Center	00000a2f
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Chứng chỉ máy chủ Kaspersky Sandbox không hợp lệ

Trạng thái	
Thành phần	Kaspersky Sandbox
ID sự kiện Windows	2613
ID sự kiện Kaspersky Security Center	00000a35
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Nốt Kaspersky Sandbox không khả dụng

Trạng thái	
Thành phần	Kaspersky Sandbox
ID sự kiện Windows	2614
ID sự kiện Kaspersky Security Center	00000a36
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Đã xảy ra lỗi khi xử lý đối tượng trong Kaspersky Sandbox

Trạng thái	
Thành phần	Kaspersky Sandbox
ID sự kiện Windows	2617
ID sự kiện Kaspersky Security Center	00000a39
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Đã vượt quá tải lượng tối đa tới Kaspersky Sandbox

Trạng thái	
Thành phần	Kaspersky Sandbox
ID sự kiện Windows	2618
ID sự kiện Kaspersky Security Center	00000a3a
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-


Đã phát hiện IOC

Trạng thái	
Thành phần	Endpoint Detection and Response
ID sự kiện Windows	2651
ID sự kiện Kaspersky Security Center	00000a5b
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓




Không thể xác minh giấy phép Kaspersky Sandbox

Trạng thái	
Thành phần	Kaspersky Sandbox
ID sự kiện Windows	2620
ID sự kiện Kaspersky Security Center	00000a3c
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓




Đã chặn khởi động đối tượng

Trạng thái	
Thành phần	Endpoint Detection and Response
ID sự kiện Windows	2553
ID sự kiện Kaspersky Security Center	000009f9
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓




Khởi động tiến trình bị chặn

Trạng thái	
Thành phần	Endpoint Detection and Response
ID sự kiện Windows	2551
ID sự kiện Kaspersky Security Center	000009f7
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	


Thực thi tập lệnh bị chặn

Trạng thái	
Thành phần	Endpoint Detection and Response
ID sự kiện Windows	2559
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Đối tượng không được cách ly (Endpoint Detection and Response)



Trạng thái	
Thành phần	Endpoint Detection and Response
ID sự kiện Windows	2556
ID sự kiện Kaspersky Security Center	000009fc
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Thay đổi các thành phần ứng dụng



Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	1401
ID sự kiện Kaspersky Security Center	00000579
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Lỗi chức năng

Không thể thực hiện tác vụ



Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	212
ID sự kiện Kaspersky Security Center	000000d4
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Thiết lập tác vụ không hợp lệ. Thiết lập không được áp dụng

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	707
ID sự kiện Kaspersky Security Center	000002c3
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Cảnh báo

Ứng dụng bị lỗi trong phiên trước đó

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	237
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Giấy phép sắp hết hạn

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	204
ID sự kiện Kaspersky Security Center	000000cc
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Cơ sở dữ liệu đã lỗi thời

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	208
ID sự kiện Kaspersky Security Center	000000d0
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Cập nhật tự động bị vô hiệu

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	210
ID sự kiện Kaspersky Security Center	000000d2
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Tự bảo vệ bị vô hiệu

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	211
ID sự kiện Kaspersky Security Center	000000d3
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Thành phần bảo vệ bị vô hiệu

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	214
ID sự kiện Kaspersky Security Center	000000d6
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	


Máy tính đang chạy trong chế độ an toàn

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	215
ID sự kiện Kaspersky Security Center	000000d7
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-


Các tập tin không được xử lý

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	216
ID sự kiện Kaspersky Security Center	000000d8
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Chính sách nhóm được áp dụng

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	219
ID sự kiện Kaspersky Security Center	000000db
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Tác vụ được dừng

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	222
ID sự kiện Kaspersky Security Center	000000de
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Thoát và mở lại ứng dụng để hoàn tất cập nhật

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	224
ID sự kiện Kaspersky Security Center	0000057b
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	


Yêu cầu khởi động lại máy tính

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	225
ID sự kiện Kaspersky Security Center	000000e1
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Giấy phép cho phép việc sử dụng các thành phần chưa được cài đặt

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	226
ID sự kiện Kaspersky Security Center	000000e2
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Khử mã độc nâng cao được bắt đầu

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	232
ID sự kiện Kaspersky Security Center	000000e8
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	


Khử mã độc nâng cao hoàn tất

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	233
ID sự kiện Kaspersky Security Center	000000e9
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Sai khóa dự trữ

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	230
ID sự kiện Kaspersky Security Center	000000e6
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Gói đăng ký sắp hết hạn

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	240
ID sự kiện Kaspersky Security Center	000000f0
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Đã chặn

Trạng thái	
Thành phần	Phát hiện hành vi Phòng chống khai thác Bảo vệ mỗi đe dọa web
ID sự kiện Windows	331
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Không thể khôi phục đối tượng từ Sao lưu

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	336
ID sự kiện Kaspersky Security Center	00000150
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Đã phát hiện các hoạt động mạng khả nghi

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	2001
ID sự kiện Kaspersky Security Center	000007d1
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Đã chấm dứt kết nối được mã hóa

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	250
ID sự kiện Kaspersky Security Center	000007d3
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Đã tắt Tham gia KSN

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	2021
ID sự kiện Kaspersky Security Center	000007e5
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Việc xử lý một số chức năng hệ điều hành đã bị tắt.

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	245
ID sự kiện Kaspersky Security Center	000000f5
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Ổ lưu trữ của Khu vực cách lý sắp hết không gian trống

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	344
ID sự kiện Kaspersky Security Center	00000158
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Kết nối bị chặn

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	809
ID sự kiện Kaspersky Security Center	00000abe
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	


Không thể tạo bản sao lưu

Trạng thái	
Thành phần	Bảo vệ mối đe dọa tập tin Phát hiện hành vi Phòng chống xâm nhập máy chủ Quét virus
ID sự kiện Windows	310
ID sự kiện Kaspersky Security Center	00000136
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Đối tượng chưa được xử lý

Trạng thái	
Thành phần	Bảo vệ mối đe dọa tập tin Bảo vệ mối đe dọa thư điện tử Phòng chống xâm nhập máy chủ Bảo vệ AMSI Quét virus
ID sự kiện Windows	314
ID sự kiện Kaspersky Security Center	GNRL_EV_OBJECT_REPORTED
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 là hash của đối tượng (SHA256). • GNRL_EA_PARAM_2 là tên của đối tượng. • GNRL_EA_PARAM_5 là tên của mối đe dọa phù hợp với phân loại của Kaspersky, ví dụ: EICAR-Test-File. • GNRL_EA_PARAM_7 là tên của người dùng phiên. • GNRL_EA_PARAM_8 là loại mối đe dọa, ví dụ: Trojware. • GNRL_EA_PARAM_9 là thông tin bổ sung về đối tượng được phát hiện: Thành phần ứng dụng (engine). Công nghệ phát hiện mối đe dọa (method). Mối đe dọa được phát hiện bởi KSN Riêng (denylist): true hoặc false. Phiên bản EDR. Định danh mối đe dọa trong EDR. Giá trị hash MD5 của đối tượng.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Đối tượng bị mã hóa

Trạng thái	
Thành phần	Phòng chống xâm nhập máy chủ
ID sự kiện Windows	320
ID sự kiện Kaspersky Security Center	00000140
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-



Đối tượng bị hư hỏng

Trạng thái	
Thành phần	Bảo vệ mối đe dọa tập tin Bảo vệ mối đe dọa web Bảo vệ mối đe dọa thư điện tử Bảo vệ AMSI Phòng chống xâm nhập máy chủ Quét virus
ID sự kiện Windows	321
ID sự kiện Kaspersky Security Center	00000141
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-



Đã phát hiện phần mềm hợp pháp có thể bị kẻ xâm nhập sử dụng làm hư hại máy tính của bạn hoặc dữ liệu cá nhân (cơ sở cục bộ)

Trạng thái	
Thành phần	Bảo vệ mối đe dọa tập tin Bảo vệ mối đe dọa web Bảo vệ mối đe dọa thư điện tử Phòng chống xâm nhập máy chủ Bảo vệ AMSI Phát hiện hành vi Quét virus
ID sự kiện Windows	303
ID sự kiện Kaspersky Security Center	GNRL_EV_SUSPICIOUS_OBJECT_FOUND
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 là hash của đối tượng (SHA256). • GNRL_EA_PARAM_2 là tên của đối tượng. • GNRL_EA_PARAM_5 là tên của mối đe dọa phù hợp với phân loại của Kaspersky, ví dụ: EICAR-Test-File. • GNRL_EA_PARAM_7 là tên của người dùng phiên. • GNRL_EA_PARAM_8 là loại mối đe dọa, ví dụ: Trojware.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



[Đã phát hiện phần mềm hợp pháp có thể bị kẻ xâm nhập sử dụng làm hư hại máy tính hoặc dữ liệu cá nhân của bạn \(KSN\)](#) 

Trạng thái	
Thành phần	Bảo vệ mối đe dọa tập tin Bảo vệ mối đe dọa web Bảo vệ mối đe dọa thư điện tử Phòng chống xâm nhập máy chủ Bảo vệ AMSI Phát hiện hành vi Quét virus
ID sự kiện Windows	303
ID sự kiện Kaspersky Security Center	GNRL_EV_SUSPICIOUS_OBJECT_FOUND
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 là hash của đối tượng (SHA256). • GNRL_EA_PARAM_2 là tên của đối tượng. • GNRL_EA_PARAM_5 là tên của mối đe dọa phù hợp với phân loại của Kaspersky, ví dụ: EICAR-Test-File. • GNRL_EA_PARAM_7 là tên của người dùng phiên. • GNRL_EA_PARAM_8 là loại mối đe dọa, ví dụ: Trojware.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



[Đã xóa đối tượng](#) 

Trạng thái	
Thành phần	Bảo vệ mối đe dọa tập tin Bảo vệ mối đe dọa thư điện tử Phòng chống xâm nhập máy chủ Phòng chống khai thác Phát hiện hành vi Quét virus
ID sự kiện Windows	307
ID sự kiện Kaspersky Security Center	GNRL_EV_OBJECT_DELETED
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 là hash của đối tượng (SHA256). • GNRL_EA_PARAM_2 là tên của đối tượng. • GNRL_EA_PARAM_5 là tên của mối đe dọa phù hợp với phân loại của Kaspersky, ví dụ: EICAR-Test-File. • GNRL_EA_PARAM_7 là tên của người dùng phiên. • GNRL_EA_PARAM_8 là loại mối đe dọa, ví dụ: Trojware. • GNRL_EA_PARAM_9 là thông tin bổ sung về đối tượng được phát hiện: Thành phần ứng dụng (engine). Công nghệ phát hiện mối đe dọa (method). Mối đe dọa được phát hiện bởi KSN Riêng (denylist): true hoặc false. Phiên bản EDR. Định danh mối đe dọa trong EDR. Giá trị hash MD5 của đối tượng.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



[Đối tượng được khử mã độc](#)

Trạng thái	
Thành phần	Bảo vệ mối đe dọa tập tin Bảo vệ mối đe dọa thư điện tử Phòng chống xâm nhập máy chủ Quét virus
ID sự kiện Windows	306
ID sự kiện Kaspersky Security Center	GNRL_EV_OBJECT_CURED
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 là hash của đối tượng (SHA256). • GNRL_EA_PARAM_2 là tên của đối tượng. • GNRL_EA_PARAM_5 là tên của mối đe dọa phù hợp với phân loại của Kaspersky, ví dụ: EICAR-Test-File. • GNRL_EA_PARAM_7 là tên của người dùng phiên. • GNRL_EA_PARAM_8 là loại mối đe dọa, ví dụ: Trojware. • GNRL_EA_PARAM_9 là thông tin bổ sung về đối tượng được phát hiện: Thành phần ứng dụng (engine). Công nghệ phát hiện mối đe dọa (method). Mối đe dọa được phát hiện bởi KSN Riêng (denylist): true hoặc false. Phiên bản EDR. Định danh mối đe dọa trong EDR. Giá trị hash MD5 của đối tượng.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Đối tượng sẽ được khử mã độc khi khởi động lại

Trạng thái	
Thành phần	Phòng chống xâm nhập máy chủ Bảo vệ mối đe dọa tập tin Quét virus
ID sự kiện Windows	324
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-



Đối tượng sẽ bị xóa khi khởi động lại

Trạng thái	
Thành phần	Phát hiện hành vi Phòng chống khai thác Phòng chống xâm nhập máy chủ Bảo vệ mối đe dọa tập tin Quét virus
ID sự kiện Windows	323
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-



Đối tượng bị xóa theo thiết lập

Trạng thái	
Thành phần	Bảo vệ mối đe dọa thư điện tử
ID sự kiện Windows	342
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-




Hoàn tất khôi phục

Trạng thái	
Thành phần	Bảo vệ mối đe dọa tập tin Phát hiện hành vi Phòng chống khai thác Quét virus
ID sự kiện Windows	455
ID sự kiện Kaspersky Security Center	000001c7
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Đã chặn việc tải về đối tượng

Trạng thái	
Thành phần	Bảo vệ mối đe dọa web
ID sự kiện Windows	341
ID sự kiện Kaspersky Security Center	GNRL_EV_OBJECT_BLOCKED
Tham số sự kiện	<ul style="list-style-type: none"> GNRL_EA_PARAM_1 là hash của đối tượng (SHA256). GNRL_EA_PARAM_2 là tên của đối tượng. GNRL_EA_PARAM_5 là tên của mối đe dọa phù hợp với phân loại của Kaspersky, ví dụ: EICAR-Test-File. GNRL_EA_PARAM_7 là tên của người dùng phiên. GNRL_EA_PARAM_8 là loại mối đe dọa, ví dụ: Trojware. GNRL_EA_PARAM_9 là thông tin bổ sung về đối tượng được phát hiện: Thành phần ứng dụng (engine). Công nghệ phát hiện mối đe dọa (method). Mối đe dọa được phát hiện bởi KSN Riêng (denylist): true hoặc false. Phiên bản EDR. Định danh mối đe dọa trong EDR. Giá trị hash MD5 của đối tượng.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Lỗi cấp phép cho bàn phím

Trạng thái	
Thành phần	Phòng chống Tấn công BadUSB
ID sự kiện Windows	2052
ID sự kiện Kaspersky Security Center	00000804
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Kết quả quét đối tượng đã được gửi đến một ứng dụng thuộc bên thứ ba

Trạng thái	
Thành phần	Bảo vệ AMSI
ID sự kiện Windows	1512
ID sự kiện Kaspersky Security Center	GNRL_EV_OBJECT_REPORTED
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 là hash của đối tượng (SHA256). • GNRL_EA_PARAM_2 là tên của đối tượng. • GNRL_EA_PARAM_5 là tên của mối đe dọa phù hợp với phân loại của Kaspersky, ví dụ: EICAR-Test-File. • GNRL_EA_PARAM_7 là tên của người dùng phiên. • GNRL_EA_PARAM_8 là loại mối đe dọa, ví dụ: Trojware. • GNRL_EA_PARAM_9 là thông tin bổ sung về đối tượng được phát hiện: Thành phần ứng dụng (engine). Công nghệ phát hiện mối đe dọa (method). Mối đe dọa được phát hiện bởi KSN Riêng (denylist): true hoặc false. Phiên bản EDR. Định danh mối đe dọa trong EDR. Giá trị hash MD5 của đối tượng.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Thiết lập tác vụ được áp dụng thành công

Trạng thái	
Thành phần	Kiểm soát ứng dụng
ID sự kiện Windows	708
ID sự kiện Kaspersky Security Center	000002c4
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Cảnh báo về nội dung không mong muốn (cơ sở nội bộ)

Trạng thái	
Thành phần	Kiểm soát Web
ID sự kiện Windows	708
ID sự kiện Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 là URL. • GNRL_EA_PARAM_2 là tên của người dùng phiên. • GNRL_EA_PARAM_3 là tên của quy tắc Kiểm soát Web.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Cảnh báo về nội dung không mong muốn (KSN)

Trạng thái	
Thành phần	Kiểm soát Web
ID sự kiện Windows	708
ID sự kiện Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 là URL. • GNRL_EA_PARAM_2 là tên của người dùng phiên. • GNRL_EA_PARAM_3 là tên của quy tắc Kiểm soát Web.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Nội dung không mong muốn đã được truy cập sau một cảnh báo

Trạng thái	
Thành phần	Kiểm soát Web
ID sự kiện Windows	754
ID sự kiện Kaspersky Security Center	000002f2
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-


Truy cập tạm thời vào thiết bị kích hoạt

Trạng thái	
Thành phần	Kiểm soát Thiết bị
ID sự kiện Windows	803
ID sự kiện Kaspersky Security Center	000002f2
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Hành động bị hủy bỏ bởi người dùng

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1016
ID sự kiện Kaspersky Security Center	000003f8
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Người dùng đã chọn không tham gia chính sách mã hóa

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1306
ID sự kiện Kaspersky Security Center	0000051a
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Đã làm gián đoạn áp dụng quy tắc mã hóa / giải mã tập tin

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	903
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

[Đã gián đoạn mã hóa / giải mã tập tin](#)

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	914
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

[Đã gián đoạn mã hóa / giải mã thiết bị](#)

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1303
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

[Không thể cài đặt hoặc nâng cấp các trình điều khiển Kaspersky Disk Encryption trong tập tin ảnh WinRE](#)

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1345
ID sự kiện Kaspersky Security Center	00000541
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

[Kiểm tra chữ ký mô-đun đã thất bại](#)

Trạng thái	
Thành phần	Kiểm tra tính toàn vẹn
ID sự kiện Windows	2002
ID sự kiện Kaspersky Security Center	000007d2
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	


Đã chặn việc khởi động ứng dụng

Trạng thái	
Thành phần	Cảm biến điểm cuối
ID sự kiện Windows	2105
ID sự kiện Kaspersky Security Center	00000839
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Đã chặn việc mở tài liệu

Trạng thái	
Thành phần	Cảm biến điểm cuối
ID sự kiện Windows	2106
ID sự kiện Kaspersky Security Center	0000083a
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Quản trị viên máy chủ Kaspersky Anti Targeted Attack Platform đã chấm dứt tiến trình

Trạng thái	
Thành phần	Cảm biến điểm cuối
ID sự kiện Windows	2112
ID sự kiện Kaspersky Security Center	00000840
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Quản trị viên máy chủ Kaspersky Anti Targeted Attack Platform đã chấm dứt ứng dụng

Trạng thái	
Thành phần	Cảm biến điểm cuối
ID sự kiện Windows	2113
ID sự kiện Kaspersky Security Center	00000841
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Tập tin hoặc luồng dữ liệu đã bị xóa bởi quản trị viên máy chủ Kaspersky Anti Targeted Attack Platform

Trạng thái	
Thành phần	Cảm biến điểm cuối
ID sự kiện Windows	2111
ID sự kiện Kaspersky Security Center	0000083f
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Tập tin đã được quản trị viên khôi phục từ Khu vực cách ly trên máy chủ Kaspersky Anti Targeted Attack Platform

Trạng thái	
Thành phần	Cảm biến điểm cuối
ID sự kiện Windows	2110
ID sự kiện Kaspersky Security Center	0000083e
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Quản trị viên đã cách ly tập tin trên máy chủ Kaspersky Anti Targeted Attack Platform

Trạng thái	
Thành phần	Cảm biến điểm cuối
ID sự kiện Windows	2109
ID sự kiện Kaspersky Security Center	0000083d
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Hoạt động mạng của tất cả các ứng dụng của bên thứ ba đang bị chặn

Trạng thái	
Thành phần	Cảm biến điểm cuối
ID sự kiện Windows	2107
ID sự kiện Kaspersky Security Center	0000083b
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Hoạt động mạng của tất cả các ứng dụng thuộc bên thứ ba được bỏ chặn

Trạng thái	
Thành phần	Cảm biến điểm cuối
ID sự kiện Windows	2108
ID sự kiện Kaspersky Security Center	0000083c
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓




Đối tượng sẽ bị xóa khi khởi động lại (Kaspersky Sandbox)

Trạng thái	
Thành phần	Kaspersky Sandbox
ID sự kiện Windows	2605
ID sự kiện Kaspersky Security Center	00000a2d
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓




Tổng kích cỡ của các tác vụ quét đã vượt quá giới hạn

Trạng thái	
Thành phần	Kaspersky Sandbox
ID sự kiện Windows	2612
ID sự kiện Kaspersky Security Center	00000a34
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓




Khởi động đối tượng được cho phép, sự kiện được ghi nhật ký

Trạng thái	
Thành phần	Endpoint Detection and Response
ID sự kiện Windows	2553
ID sự kiện Kaspersky Security Center	000009fa
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	




Khởi động tiến trình được cho phép, sự kiện được ghi nhật ký

Trạng thái	
Thành phần	Endpoint Detection and Response
ID sự kiện Windows	2554
ID sự kiện Kaspersky Security Center	000009f8
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	




Đối tượng sẽ bị xóa khi khởi động lại (Endpoint Detection and Response)

Trạng thái	
Thành phần	Endpoint Detection and Response
ID sự kiện Windows	2558
ID sự kiện Kaspersky Security Center	000009fe
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	




Cách ly mạng

Trạng thái	
Thành phần	Endpoint Detection and Response
ID sự kiện Windows	2700
ID sự kiện Kaspersky Security Center	00000a8c
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Chăm dứt cách ly mạng

Trạng thái	
Thành phần	Endpoint Detection and Response
ID sự kiện Windows	2701
ID sự kiện Kaspersky Security Center	00000a8d
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Khởi động lại là cần thiết để hoàn tất tác vụ

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	225
ID sự kiện Kaspersky Security Center	0000057b
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Thông báo chặn việc khởi chạy ứng dụng gửi đến quản trị viên

Trạng thái	
Thành phần	Kiểm soát ứng dụng
ID sự kiện Windows	503
ID sự kiện Kaspersky Security Center	GNRL_EV_AC_USER_REQUEST
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_DESCRIPTION là thông báo đến người dùng. • GNRL_EA_PARAM_2 là tên của người dùng phiên. • GNRL_EA_PARAM_6 là tên của tập tin thực thi của ứng dụng (ví dụ: chrome.exe). • GNRL_EA_PARAM_7 là đường dẫn đến tập tin thực thi. • GNRL_EA_PARAM_8 là hash của đối tượng (SHA256). • GNRL_EA_PARAM_9 là phiên bản của ứng dụng mà người dùng đang cố chạy.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



[Thông báo chặn truy cập thiết bị gửi đến quản trị viên](#)

Trạng thái	
Thành phần	Kiểm soát Thiết bị
ID sự kiện Windows	804
ID sự kiện Kaspersky Security Center	GNRL_EV_DC_USER_REQUEST
Tham số sự kiện	<ul style="list-style-type: none"> • c_er_descr là thông báo đến người dùng. • GNRL_EA_PARAM_1 là ID phần cứng (HWID). • GNRL_EA_PARAM_2 là tên của người dùng phiên.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



[Thông báo chặn truy cập trang web gửi đến quản trị viên](#)

Trạng thái	
Thành phần	Kiểm soát Web
ID sự kiện Windows	755
ID sự kiện Kaspersky Security Center	GNRL_EV_WC_USER_REQUEST
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_DESCRIPTION là thông báo đến người dùng. • GNRL_EA_PARAM_1 là URL. • GNRL_EA_PARAM_2 là tên của người dùng phiên.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

[Kết nối đến thiết bị đã bị chặn](#)

Trạng thái	
Thành phần	Kiểm soát Thiết bị
ID sự kiện Windows	807
ID sự kiện Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 là ID phần cứng (HWID). • GNRL_EA_PARAM_2 là tên của người dùng phiên.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

[Thông báo chặn hoạt động của ứng dụng gửi đến quản trị viên](#)

Trạng thái	
Thành phần	Kiểm soát thích ứng sự cố
ID sự kiện Windows	503
ID sự kiện Kaspersky Security Center	GNRL_EV_ADSEC_USER_REQUEST
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_DESCRIPTION là thông báo đến người dùng. • GNRL_EA_PARAM_1 là tên của quy tắc Kiểm soát thích ứng sự cố. • GNRL_EA_PARAM_2 là ID của quy tắc phân tích hành vi. • GNRL_EA_PARAM_3 là tên của người dùng phiên. • GNRL_EA_PARAM_4 là tiến trình nguồn. • GNRL_EA_PARAM_5 là đối tượng nguồn. • GNRL_EA_PARAM_6 là tiến trình đích. • GNRL_EA_PARAM_7 là đối tượng đích. • GNRL_EA_PARAM_8 là thông tin bổ sung về đối tượng được phát hiện: Giá trị băm của tiến trình/đối tượng nguồn và tiến trình/đối tượng đích. Tiến trình bị chặn (verdict_type): true hoặc false. ID bảo mật của người dùng (SID).
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Thông báo thông tin

[Ứng dụng được khởi động](#) 

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	235
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-


Ứng dụng được dừng

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	236
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Hoạt động đến tài nguyên ứng dụng đã bị chặn bởi Tự bảo vệ

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	213
ID sự kiện Kaspersky Security Center	000000d5
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Báo cáo được xóa

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	217
ID sự kiện Kaspersky Security Center	000000d9
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Chính sách nhóm bị vô hiệu

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	220
ID sự kiện Kaspersky Security Center	000000dc
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Thiết lập của ứng dụng bị thay đổi

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	218
ID sự kiện Kaspersky Security Center	000000da
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Tác vụ được bắt đầu

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	221
ID sự kiện Kaspersky Security Center	000000dd
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Tác vụ hoàn tất

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	223
ID sự kiện Kaspersky Security Center	000000df
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Tất cả các thành phần ứng dụng được xác định bởi giấy phép cài đặt và chạy trong chế độ chuẩn 

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	227
ID sự kiện Kaspersky Security Center	000000e3
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Thiết lập của gói đăng ký đã thay đổi

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	238
ID sự kiện Kaspersky Security Center	000000ee
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Gói đăng ký đã được gia hạn

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	239
ID sự kiện Kaspersky Security Center	000000ef
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Đối tượng được khôi phục từ Sao lưu

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	335
ID sự kiện Kaspersky Security Center	0000014f
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Nhập tên người dùng và mật khẩu

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	2000
ID sự kiện Kaspersky Security Center	000007d0
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Đã bật Tham gia KSN

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	2020
ID sự kiện Kaspersky Security Center	000007e4
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Máy chủ KSN khả dụng

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	2022
ID sự kiện Kaspersky Security Center	000007e6
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Ứng dụng sẽ hoạt động và xử lý dữ liệu trong khuôn khổ luật pháp liên quan và sử dụng hạ tầng phù hợp

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	2024
ID sự kiện Kaspersky Security Center	000007e8
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Đối tượng được khôi phục từ Khu vực cách ly

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	345
ID sự kiện Kaspersky Security Center	00000159
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Đối tượng bị xóa khỏi Khu vực cách ly

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	347
ID sự kiện Kaspersky Security Center	0000015b
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Một bản sao lưu của đối tượng được tạo ra

Trạng thái	
Thành phần	Bảo vệ mối đe dọa tập tin Bảo vệ mối đe dọa thư điện tử Phát hiện hành vi Phòng chống xâm nhập máy chủ Kaspersky Sandbox Quét virus
ID sự kiện Windows	308
ID sự kiện Kaspersky Security Center	00000134
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Ghi đè bởi một bản sao đã được khử mã độc trước đó

Trạng thái	ⓘ
Thành phần	Bảo vệ mối đe dọa tập tin Phòng chống xâm nhập máy chủ Quét virus
ID sự kiện Windows	327
ID sự kiện Kaspersky Security Center	00000147
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-


Phát hiện tập tin nén được bảo vệ bằng mật khẩu ⓘ

Trạng thái	ⓘ
Thành phần	Bảo vệ mối đe dọa tập tin Bảo vệ mối đe dọa web Bảo vệ mối đe dọa thư điện tử Bảo vệ AMSI Phòng chống xâm nhập máy chủ Quét virus
ID sự kiện Windows	322
ID sự kiện Kaspersky Security Center	GNRL_EV_PASSWD_ARCHIVE_FOUND
Tham số sự kiện	<ul style="list-style-type: none"> GNRL_EA_PARAM_2 là tên của đối tượng. GNRL_EA_PARAM_3 là ngày tạo đối tượng (không bắt buộc). GNRL_EA_PARAM_7 là tên của người dùng phiên. GNRL_EA_PARAM_9 là thông tin bổ sung về đối tượng được phát hiện: Thành phần ứng dụng (engine ⓘ). Công nghệ phát hiện mối đe dọa (method ⓘ). Mối đe dọa được phát hiện bởi KSN Riêng (denylist): true hoặc false.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Thông tin về các đối tượng được phát hiện ⓘ

Trạng thái	
Thành phần	Bảo vệ mối đe dọa tập tin Bảo vệ mối đe dọa web Bảo vệ mối đe dọa thư điện tử Bảo vệ AMSI Phòng chống xâm nhập máy chủ Quét virus
ID sự kiện Windows	332
ID sự kiện Kaspersky Security Center	0000014c
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓



Đối tượng này nằm trong danh sách được phép của KSN Riêng

Trạng thái	
Thành phần	Bảo vệ mối đe dọa tập tin Bảo vệ mối đe dọa web Bảo vệ mối đe dọa thư điện tử Bảo vệ AMSI Phòng chống xâm nhập máy chủ Quét virus
ID sự kiện Windows	340
ID sự kiện Kaspersky Security Center	00000154
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓



Đổi tên đối tượng

Trạng thái	
Thành phần	Bảo vệ mối đe dọa thư điện tử Phòng chống khai thác Phát hiện hành vi Quét virus
ID sự kiện Windows	329
ID sự kiện Kaspersky Security Center	00000149
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓



Xử lý đối tượng

Trạng thái	
Thành phần	Phòng chống xâm nhập máy chủ Bảo vệ mối đe dọa tập tin Bảo vệ mối đe dọa web Bảo vệ mối đe dọa thư điện tử Quét virus
ID sự kiện Windows	301
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-



Đối tượng được bỏ qua

Trạng thái	
Thành phần	Phòng chống xâm nhập máy chủ Bảo vệ mối đe dọa tập tin Bảo vệ AMSI Quét virus
ID sự kiện Windows	315
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-



Phát hiện tập tin nén

Trạng thái	
Thành phần	Phòng chống xâm nhập máy chủ Bảo vệ mối đe dọa tập tin Bảo vệ mối đe dọa web Bảo vệ mối đe dọa thư điện tử Bảo vệ AMSI Quét virus
ID sự kiện Windows	318
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-



Đã phát hiện đối tượng được gói

Trạng thái	
Thành phần	Phòng chống xâm nhập máy chủ Bảo vệ mối đe dọa tập tin Bảo vệ mối đe dọa web Bảo vệ mối đe dọa thư điện tử Bảo vệ AMSI Quét virus
ID sự kiện Windows	319
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Liên kết đã được xử lý

Trạng thái	
Thành phần	Bảo vệ mối đe dọa web
ID sự kiện Windows	361
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Cho phép ứng dụng khởi động

Trạng thái	
Thành phần	Kiểm soát ứng dụng
ID sự kiện Windows	701
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-


Nguồn cập nhật đã được chọn

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1001
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-


Máy chủ proxy đã được chọn

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1002
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-



Liên kết này nằm trong danh sách được phép của KSN Riêng

Trạng thái	
Thành phần	Bảo vệ mỗi đe dọa web
ID sự kiện Windows	370
ID sự kiện Kaspersky Security Center	00000172
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓



Ứng dụng được đặt trong nhóm Tin tưởng

Trạng thái	
Thành phần	Phòng chống xâm nhập máy chủ
ID sự kiện Windows	401
ID sự kiện Kaspersky Security Center	00000191
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓



Ứng dụng được đặt trong nhóm bị giới hạn

Trạng thái	
Thành phần	Phòng chống xâm nhập máy chủ
ID sự kiện Windows	402
ID sự kiện Kaspersky Security Center	00000192
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Phòng chống xâm nhập máy chủ đã được kích hoạt

Trạng thái	
Thành phần	Phòng chống xâm nhập máy chủ
ID sự kiện Windows	403
ID sự kiện Kaspersky Security Center	00000193
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Tập tin được khôi phục

Trạng thái	
Thành phần	Phát hiện hành vi Phòng chống khai thác Phòng chống xâm nhập máy chủ
ID sự kiện Windows	457
ID sự kiện Kaspersky Security Center	000001c9
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Đã khôi phục giá trị registry

Trạng thái	ⓘ
Thành phần	Phát hiện hành vi Phòng chống khai thác
ID sự kiện Windows	458
ID sự kiện Kaspersky Security Center	000001ca
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-



Xóa giá trị registry ⓘ

Trạng thái	ⓘ
Thành phần	Phát hiện hành vi Phòng chống khai thác
ID sự kiện Windows	459
ID sự kiện Kaspersky Security Center	000001cb
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Hành động của tiến trình bị bỏ qua ⓘ

Trạng thái	
Thành phần	Kiểm soát thích ứng sự cố
ID sự kiện Windows	2201
ID sự kiện Kaspersky Security Center	GNRL_EV_ADSEC_DETECT
Tham số sự kiện	<ul style="list-style-type: none"> GNRL_EA_PARAM_1 là tên của quy tắc Kiểm soát thích ứng sự cố. GNRL_EA_PARAM_2 là ID của quy tắc phân tích hành vi. GNRL_EA_PARAM_3 là tên của người dùng phiên. GNRL_EA_PARAM_4 là tiến trình nguồn. GNRL_EA_PARAM_5 là đối tượng nguồn. GNRL_EA_PARAM_6 là tiến trình đích. GNRL_EA_PARAM_7 là đối tượng đích. GNRL_EA_PARAM_8 là thông tin bổ sung về đối tượng được phát hiện: Giá trị băm của tiến trình/đối tượng nguồn và tiến trình/đối tượng đích. Tiến trình bị chặn (verdict_type): true hoặc false. ID bảo mật của người dùng (SID).
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	



Đã cấp phép cho bàn phím

Trạng thái	
Thành phần	Phòng chống Tấn công BadUSB
ID sự kiện Windows	2050
ID sự kiện Kaspersky Security Center	00000802
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	


Hoạt động mạng cho phép

Trạng thái	
Thành phần	Tường lửa
ID sự kiện Windows	601
ID sự kiện Kaspersky Security Center	00000259
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Cấm khởi động ứng dụng trong chế độ thử nghiệm

Trạng thái	
Thành phần	Kiểm soát ứng dụng
ID sự kiện Windows	703
ID sự kiện Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_DENIED
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_2 là tên của người dùng phiên. • GNRL_EA_PARAM_3 là định danh của danh mục được tạo theo cách thủ công. • GNRL_EA_PARAM_4 là định danh bảo mật tài khoản (SID). • GNRL_EA_PARAM_5 là thông tin về chữ ký số của ứng dụng. • GNRL_EA_PARAM_6 là tên của tập tin thực thi của ứng dụng (ví dụ: chrome.exe). • GNRL_EA_PARAM_7 là đường dẫn đến tập tin thực thi. • GNRL_EA_PARAM_8 là hash của đối tượng (SHA256). • GNRL_EA_PARAM_9 là phiên bản của ứng dụng mà người dùng đang cố chạy.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	


Cho phép ứng dụng khởi động trong chế độ thử nghiệm

Trạng thái	
Thành phần	Kiểm soát ứng dụng
ID sự kiện Windows	704
ID sự kiện Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_ALLOW
Tham số sự kiện	<ul style="list-style-type: none"> GNRL_EA_PARAM_2 là tên của người dùng phiên. GNRL_EA_PARAM_3 là định danh của danh mục được tạo theo cách thủ công. GNRL_EA_PARAM_4 là định danh bảo mật tài khoản (SID). GNRL_EA_PARAM_5 là thông tin về chữ ký số của ứng dụng.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Đã mở một trang được cho phép

Trạng thái	
Thành phần	Kiểm soát Web
ID sự kiện Windows	751
ID sự kiện Kaspersky Security Center	000002f4
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Hoạt động với các thiết bị cho phép

Trạng thái	
Thành phần	Kiểm soát Thiết bị
ID sự kiện Windows	801
ID sự kiện Kaspersky Security Center	00000321
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Thao tác với tập tin đã được thực thi

Trạng thái	?
Thành phần	Kiểm soát Thiết bị
ID sự kiện Windows	808
ID sự kiện Kaspersky Security Center	GNRL_EV_USB_FILE_OPERATION
Tham số sự kiện	<ul style="list-style-type: none"> GNRL_EA_PARAM_1 là hoạt động của tập tin (ghi hoặc xóa). GNRL_EA_PARAM_2 là đường dẫn đến tập tin. GNRL_EA_PARAM_3 là tên của thiết bị. GNRL_EA_PARAM_4 là tên của người dùng phiên. GNRL_EA_PARAM_5 là ID phần cứng (HWID).
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

[Không có cập nhật mới](#) [?](#)

Trạng thái	?
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1020
ID sự kiện Kaspersky Security Center	000003fc
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

[Tác vụ phân phối cập nhật hoàn tất thành công](#) [?](#)

Trạng thái	?
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1022
ID sự kiện Kaspersky Security Center	000003fe
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

[Đang tải tập tin](#) [?](#)

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1003
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-


Tập tin được tải

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1004
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Tập tin được cài đặt

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1005
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Tập tin được cập nhật

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1006
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Tập tin khôi phục do lỗi cập nhật

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1007
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

[Đang cập nhật các tập tin](#)

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1008
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

[Đang phân phối các bản cập nhật](#)

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1009
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

[Đang hoàn tác các tập tin](#)

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1010
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

[Đang tạo danh sách các tập tin để tải về](#)

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	1013
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-


Đang tải về các bản vá

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	2150
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Đang cài đặt bản vá

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	2151
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-



Đã cài đặt bản vá

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	2152
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Đang hoàn tác bản vá

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	2154
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-


Bản vá đã được hoàn tác

Trạng thái	
Thành phần	Cập nhật cơ sở dữ liệu
ID sự kiện Windows	2155
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Đã bắt đầu áp dụng quy tắc mã hóa / giải mã tập tin

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	901
ID sự kiện Kaspersky Security Center	00000385
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Hoàn tất áp dụng quy tắc mã hóa / giải mã tập tin

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	902
ID sự kiện Kaspersky Security Center	00000386
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Tiếp tục áp dụng quy tắc mã hóa / giải mã tập tin

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	905
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

[Đã bắt đầu mã hóa / giải mã tập tin](#)

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	910
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

[Đã hoàn tất mã hóa / giải mã tập tin](#)

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	911
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

[Tập tin không được mã hóa bởi vì nó được loại trừ](#)

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	913
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

[Cho phép chế độ di động](#)

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	950
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Chế độ lưu động bị vô hiệu

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	952
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Đã bắt đầu mã hóa / giải mã thiết bị

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1301
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Đã hoàn tất mã hóa / giải mã thiết bị

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1302
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Đã tiếp tục mã hóa / giải mã thiết bị

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1304
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Thiết bị không được mã hóa

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1307
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Tiến trình mã hóa / giải mã thiết bị được chuyển sang chế độ hoạt động

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1308
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Tiến trình mã hóa / giải mã thiết bị được chuyển sang chế độ thụ động

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1309
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-


Khởi động mô-đun mã hóa

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1310
ID sự kiện Kaspersky Security Center	0000051e
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Tài khoản Authentication Agent mới được tạo

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1330
ID sự kiện Kaspersky Security Center	00000532
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Tài khoản Authentication Agent bị xóa

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1331
ID sự kiện Kaspersky Security Center	00000533
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Mật khẩu tài khoản Authentication Agent đã được thay đổi

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1332
ID sự kiện Kaspersky Security Center	00000534
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Đăng nhập Authentication Agent thành công

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1333
ID sự kiện Kaspersky Security Center	00000535
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-


Cố gắng đăng nhập Authentication Agent không thành công

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1334
ID sự kiện Kaspersky Security Center	00000536
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-


Truy cập vào ổ đĩa cứng bằng cách sử dụng thủ tục yêu cầu quyền truy cập vào thiết bị mã hóa

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1335
ID sự kiện Kaspersky Security Center	00000537
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-


Cố gắng truy cập vào ổ đĩa cứng bằng cách sử dụng thủ tục yêu cầu quyền truy cập vào thiết bị mã hóa không thành công

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1336
ID sự kiện Kaspersky Security Center	00000538
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-


Tài khoản đã không được thêm. Tài khoản này đã tồn tại

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1337
ID sự kiện Kaspersky Security Center	00000539
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-


Tài khoản đã không được sửa đổi. Tài khoản này không tồn tại

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1338
ID sự kiện Kaspersky Security Center	0000053a
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Tài khoản đã không bị xóa. Tài khoản này không tồn tại

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1339
ID sự kiện Kaspersky Security Center	0000053b
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Nâng cấp FDE đã thành công

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1341
ID sự kiện Kaspersky Security Center	0000053d
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Đã khôi phục lại thành công nâng cấp FDE

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1343
ID sự kiện Kaspersky Security Center	0000053f
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Không thể gỡ bỏ các trình điều khiển Kaspersky Disk Encryption khỏi tập tin ảnh WinRE

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1346
ID sự kiện Kaspersky Security Center	00000542
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Khóa phục hồi của BitLocker đã bị thay đổi

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1370
ID sự kiện Kaspersky Security Center	0000055a
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Mật khẩu/mã PIN của BitLocker đã bị thay đổi

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1371
ID sự kiện Kaspersky Security Center	0000055b
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Khóa khôi phục BitLocker đã được lưu vào ổ đĩa di động

Trạng thái	
Thành phần	Mã hóa dữ liệu
ID sự kiện Windows	1372
ID sự kiện Kaspersky Security Center	0000055c
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Chức năng xử lý các tác vụ từ máy chủ Kaspersky Anti Targeted Attack Platform đang không hoạt động

Trạng thái	
Thành phần	Cảm biến điểm cuối
ID sự kiện Windows	2103
ID sự kiện Kaspersky Security Center	00000837
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Endpoint Sensor đã được kết nối với máy chủ

Trạng thái	
Thành phần	Cảm biến điểm cuối
ID sự kiện Windows	2101
ID sự kiện Kaspersky Security Center	00000835
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Kết nối đến máy chủ Kaspersky Anti Targeted Attack Platform đã được khôi phục

Trạng thái	
Thành phần	Cảm biến điểm cuối
ID sự kiện Windows	2102
ID sự kiện Kaspersky Security Center	00000836
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Các tác vụ từ máy chủ Kaspersky Anti Targeted Attack Platform đang được xử lý [?]

Trạng thái	
Thành phần	Cảm biến điểm cuối
ID sự kiện Windows	2104
ID sự kiện Kaspersky Security Center	00000838
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Đã xóa đối tượng [?]

Trạng thái	
Thành phần	Xóa sạch dữ liệu
ID sự kiện Windows	2251
ID sự kiện Kaspersky Security Center	000008cb
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-


Thống kê tác vụ xóa sạch [?]

Trạng thái	
Thành phần	Xóa sạch dữ liệu
ID sự kiện Windows	2253
ID sự kiện Kaspersky Security Center	000008cd
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Đối tượng được cách ly (Kaspersky Sandbox) [?]

Trạng thái	
Thành phần	Kaspersky Sandbox
ID sự kiện Windows	2602
ID sự kiện Kaspersky Security Center	00000a2a
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Đối tượng bị xóa (Kaspersky Sandbox)

Trạng thái	
Thành phần	Kaspersky Sandbox
ID sự kiện Windows	2604
ID sự kiện Kaspersky Security Center	00000a2c
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-


Quét IOC được khởi chạy

Trạng thái	
Thành phần	Endpoint Detection and Response
ID sự kiện Windows	2652
ID sự kiện Kaspersky Security Center	00000a5c
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Quét IOC được hoàn thành

Trạng thái	
Thành phần	Endpoint Detection and Response
ID sự kiện Windows	2653
ID sự kiện Kaspersky Security Center	00000a5d
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Đối tượng được cách ly (Endpoint Detection and Response)


Trạng thái	
Thành phần	Endpoint Detection and Response
ID sự kiện Windows	2555
ID sự kiện Kaspersky Security Center	000009fb
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓


Đối tượng bị xóa (Endpoint Detection and Response)


Trạng thái	
Thành phần	Endpoint Detection and Response
ID sự kiện Windows	2557
ID sự kiện Kaspersky Security Center	000009fd
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Đã thay đổi thành công thành phần ứng dụng

Trạng thái	
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	1402
ID sự kiện Kaspersky Security Center	0000057a
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓



Trạng thái	
Thành phần	Kaspersky Sandbox
ID sự kiện Windows	2606
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Trạng thái	
Thành phần	Kaspersky Sandbox
ID sự kiện Windows	2609
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-



Trạng thái	
Thành phần	Kaspersky Sandbox
ID sự kiện Windows	2610
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-

Trạng thái	
Thành phần	Kaspersky Sandbox
ID sự kiện Windows	2616
ID sự kiện Kaspersky Security Center	-
Nhật ký sự kiện của Windows (mặc định)	
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	-



Phát hiện Kaspersky Sandbox không đồng bộ

Trạng thái	
Thành phần	Kaspersky Sandbox
ID sự kiện Windows	2619
ID sự kiện Kaspersky Security Center	GNRL_EV_APP_INCIDENT_OCCURED
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 là thiết lập của thành phần Kaspersky Sandbox. • GNRL_EA_PARAM_2 là đường dẫn đến đối tượng. • GNRL_EA_PARAM_3 là ID sự cố. • GNRL_EA_PARAM_4 là hash của đối tượng (SHA256).
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Thiết bị được kết nối

Trạng thái	
Thành phần	Kiểm soát Thiết bị
ID sự kiện Windows	805
ID sự kiện Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUGGED
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 là ID phần cứng (HWID). • GNRL_EA_PARAM_2 là tên của người dùng phiên.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

Thiết bị được ngắt kết nối

Trạng thái	
Thành phần	Kiểm soát Thiết bị
ID sự kiện Windows	806
ID sự kiện Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_UNPLUGGED
Tham số sự kiện	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 là ID phần cứng (HWID). • GNRL_EA_PARAM_2 là tên của người dùng phiên.
Nhật ký sự kiện của Windows (mặc định)	-
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	

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 và nhãn hiệu dịch vụ đã đăng ký là tài sản của các chủ sở hữu tương ứng.

Adobe, Acrobat, Flash, Reader và Shockwave là các thương hiệu hoặc thương hiệu đã đăng ký của Adobe Systems Incorporated tại Hoa Kỳ và/hoặc các quốc gia khác.

Apple, FireWire, iTunes và Safari là các thương hiệu của Apple Inc., được đăng ký tại Hoa Kỳ và các quốc gia khác.

AutoCAD là thương hiệu hoặc thương hiệu đã đăng ký của Autodesk, Inc. và/hoặc các chi nhánh và/hoặc công ty chi nhánh của hãng tại Hoa Kỳ và/hoặc các quốc gia khác.

Từ, nhãn hiệu và logo Bluetooth thuộc sở hữu của Bluetooth SIG, Inc.

Borland là thương hiệu hoặc thương hiệu đã đăng ký của Borland Software Corporation.

Android và Google Chrome là các thương hiệu của Google, Inc.

Citrix và Citrix Provisioning Services và XenDesktop là các thương hiệu của Citrix Systems, Inc. và/hoặc một hoặc nhiều công ty con của hãng và có thể được đăng ký tại Cơ quan sáng chế và nhãn hiệu Liên bang Mỹ và ở các quốc gia khác.

Dell là thương hiệu của Dell, Inc. hoặc các công ty con của hãng.

dBase là một thương hiệu của dataBased Intelligence, Inc.

EMC là thương hiệu hoặc thương hiệu đã đăng ký của EMC Corporation tại Hoa Kỳ và/hoặc các khu vực.

Foxit là thương hiệu đã đăng ký của Foxit Corporation.

Radmin là một thương hiệu được đăng ký của Famatech.

IBM là một thương hiệu của International Business Machines Corporation, được đăng ký ở nhiều khu vực tài phán trên thế giới.

Intel là thương hiệu của Intel Corporation tại Hoa Kỳ và/hoặc các quốc gia khác.

IOS, Any Connect là các thương hiệu đã đăng ký của Cisco Systems, Inc. và/hoặc các công ty trực thuộc của Cisco Systems, Inc. ở Hoa Kỳ và các quốc gia khác.

Lenovo và ThinkPad là các thương hiệu của Lenovo tại Hoa Kỳ và/hoặc các nơi khác.

Linux là thương hiệu đã đăng ký của Linus Torvalds tại Hoa Kỳ và các quốc gia khác.

Logitech là thương hiệu đã đăng ký hoặc thương hiệu của Logitech tại Hoa Kỳ và/hoặc các quốc gia khác.

LogMeIn Pro và Remotely Anywhere là các thương hiệu của LogMeIn, Inc.

Mail.ru là thương hiệu đã đăng ký của Mail.Ru, LLC.

McAfee là thương hiệu hoặc thương hiệu đã đăng ký của McAfee, Inc. tại Hoa Kỳ và các quốc gia khác.

Microsoft, Access, Active Directory, ActiveSync, BitLocker, Excel, Internet Explorer, LifeCam Cinema, MSDN, MultiPoint, Outlook, PowerPoint, PowerShell, Visual Basic, Visual FoxPro, Windows, Windows PowerShell, Windows Server, Windows Store, MS-DOS, Surface và Hyper-V là các thương hiệu đã đăng ký của Microsoft Corporation tại Hoa Kỳ và các quốc gia khác.

Mozilla, Firefox, và Thunderbird là các thương hiệu của Mozilla Foundation.

Java và JavaScript là các thương hiệu đã đăng ký của Oracle và/hoặc công ty chi nhánh của hãng.

VERISIGN là thương hiệu đã đăng ký tại Hoa Kỳ và khu vực khác hoặc là thương hiệu chưa đăng ký của VeriSign, Inc. và các công ty chi nhánh của hãng.

VMware, VMware ESX, VMware ESXi và VMware Workstation là các thương hiệu đã đăng ký hoặc thương hiệu của VMware, Inc. tại Hoa Kỳ và/hoặc khu vực tài phán khác của hãng.

Tor là nhãn hiệu đã đăng ký của The Tor Project, Mã số đăng ký tại Hoa Kỳ là 3,465,432.

Thawte là thương hiệu hoặc thương hiệu đã đăng ký của Symantec Corporation hoặc các chi nhánh của hãng tại Hoa Kỳ và các quốc gia khác.

SAMSUNG là thương hiệu của SAMSUNG tại Hoa Kỳ và các quốc gia khác.