kaspersky

Kaspersky Endpoint Security 14.2 cho Windows

© 2026 AO Kaspersky Lab

Nội dung

- Kaspersky Endpoint Security cho Windows Help
  - Có gì mới
  - Đã khắc phục các sự cố
  - Các câu hỏi thường gặp
- Kaspersky Endpoint Security cho Windows
  - Các chế độ của ứng dụng: Tiêu chuẩn, EDR Agent, Light Agent
  - 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
  - Các tiến trình của Kaspersky Endpoint Security cho Windows
  - Thay đổi thành phần ứng dụng
  - Nâng cấp phiên bản trước của ứng dụng
    - Nâng cấp ứng dụng mà không cần khởi động lại
    - Bản cập nhật SMU 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 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
  - Xóa khóa giấy phép
  - Xem thông tin giấy phép
  - Mua giấy phép
  - Gia hạn gói đăng ký

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
- Đang chuẩn bị ứng dụng để sử dụng
- Quản lý chính sách
  - Tạo một chính sách
  - Xuất và nhập chính sách
  - Chỉ báo mức độ bảo mật
- 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
- 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

Quét phần mềm độc hại
- 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 tra 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
- Cập nhật mô-đun ứng dụng
- Sử dụng một máy chủ proxy để cập nhật
- Lần hoàn tác bản cập nhật gần nhất

Công nghệ khử mã độc nâng cao
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
Loại bỏ các mối đe dọa chưa được xử lý
Bảo vệ máy tính
Trạng thái bảo vệ theo thời gian thực
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
Quét container
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
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
Cấp quyền cho đầu quét mã vạch
Bảo vệ AMSI
Bật và tắt Bảo vệ AMSI
Tối ưu hóa quét tập tin bằng Bảo vệ AMSI
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 được 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
- Quét email trong Thunderbird, MyOffice, R7-Office

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 mối đe dọa mạng theo loại

Tường lửa
- Bật hoặc tắt Tường lửa
- Thay đổi kiểu 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
  - Định nghĩa quy tắc gói tin mạng trong XML
- 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 khai thác
- Bật và tắt Phòng chống khai thác
- Bảo vệ bộ nhớ của tiến trình hệ thống

Phát hiện hành vi

Anti-Cryptor
- Bật hoặc tắt bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài
- Cấu hình thời gian chặn của máy tính không được tin tưởng
- Chỉnh sửa phạm vi giám sát
- Thêm máy tính được tin tưởng để mã hóa dữ liệu 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

Công cụ khắc phục

Kaspersky Security Network
- Bật và tắt sử dụng Kaspersky Security Network
- Hạn chế của Kaspersky Private Security Network
- 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
Thêm chứng chỉ Kaspersky vào kho chứng chỉ riêng
Loại trừ các kết nối khỏi tác vụ quét
Chặn truy cập vào các tên miền có chứng chỉ không được tin tưởng
Xóa sạch dữ liệu
Kiểm soát máy tính
Kiểm soát Web
Bổ sung một quy tắc truy cập tài nguyên web
Lọc theo địa chỉ tài nguyên web
Lọc theo nội dung tài nguyên web
Kiểm tra các quy tắc truy cập tài nguyên web
Xuất và nhập các Quy tắc kiểm soát web
Xuất và nhập địa chỉ tài nguyên web của quy tắc Kiểm soát 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
Kiểm soát web cho máy ảo
Các biến trong mẫu thông báo của Kiểm soát web
Kiểm soát Thiết bị
Thông tin về quy tắc truy cập
Lấy thông tin về các thiết bị được lắp đặt
Quản lý quyền truy cập thiết bị theo loại
Quản lý quyền truy cập thiết bị bằng bus kết nối
Phân biệt quyền truy cập của người dùng vào thiết bị
Quản lý quyền truy cập thiết bị di động
Quản lý quyền truy cập thiết bị Bluetooth
Kiểm soát in
Kiểm soát các kết nối Wi-Fi
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
Thêm thiết bị vào danh sách được tin tưởng
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
Rèn luyện 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
- Giám sát hoạt động của Kiểm soát thích ứng sự cố

Kiểm soát ứng dụng

- Giới hạn chức năng của Kiểm soát ứng dụng
- Lấy thông tin về các ứng dụng được cài đặt
- Cách bật chế độ Ứng dụng bị chặn
- Kiểm soát ứng dụng dựa trên máy tính cơ sở
- Quản lý các Quy tắc Kiểm soát ứng dụng
  - Bổ sung một điều kiện kích hoạt cho quy tắc Kiểm soát 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
  - Thêm một Quy tắc kiểm soát ứng dụng
  - 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
  - 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
  - Bật và tắt kiểm tra quy tắc 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 thử nghiệm của thành phần 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
- Các biến trong mẫu thông báo của Kiểm soát ứng dụng
- Các phương pháp tốt nhất để kiểm kê tập tin thực thi
- 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

Kiểm tra nhật ký

- Cấu hình quy tắc định trước
- Thêm quy tắc tùy chỉnh

Giám sát tính toàn vẹn của hệ thống

- Giới thiệu về quy tắc Giám sát tính toàn vẹn của hệ thống
- Giám sát tính toàn vẹn của hệ thống theo thời gian thực
- Kiểm tra tính toàn vẹn của hệ thống theo yêu cầu
- Xuất và nhập quy tắc Giám sát tính toàn vẹn hệ thống
- Xem báo cáo Giám sát tính toàn vẹn của hệ thống
- Đặt lại trạng thái toàn vẹn của hệ thống

Cloud Discovery

Khu vực tin tưởng
Tạo một loại trừ quét
Tạo ngoại lệ dựa trên loại đối tượng được phát hiện
Sửa danh sách các ứng dụng được tin tưởng
Tạo vùng cục bộ được tin tưởng
Xuất và nhập vùng được tin tưởng
Xử lý các ứng dụng có chữ ký số được tin tưởng
Phụ lục. Các loại trừ quét được định sẵn và các ứng dụng được tin tưởng
Microsoft SQL Server
Microsoft Exchange Server
Microsoft System Center Configuration Manager
Citrix
VMware
Khử trùng lặp dữ liệu trong Microsoft Windows Server
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
Bảo vệ các dịch vụ ứng dụng trước hoạt động quản lý bên ngoài
Hỗ trợ các ứng dụng quản trị từ xa
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
Thu hồi mật khẩu tạm thời
Các khía cạnh đặc biệt của quyền truy cập được Bảo vệ bằng mật khẩu
Đặt lại mật khẩu KLAdmin
Bảo vệ kết nối Máy chủ quản trị
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
- 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
- Cấp phép cho MDR và EDR Optimum
- Khả năng tương thích với các giải pháp EDR của bên thứ ba
- Kaspersky Endpoint Agent
  - Chuyển cấu hình [KES+KEA] sang cấu hình [KES+built-in agent]
  - Chuyển đổi chính sách và tác vụ cho Kaspersky Endpoint Agent
- Endpoint Detection and Response Agent (EDR Agent)
  - Cài đặt EDR Agent
  - Tích hợp EDR Agent với MDR
  - Tích hợp EDR Agent với EDR (KATA)
  - Tích hợp EDR Agent với NDR (KATA)
  - Tích hợp Tác nhân EDR với EDR Expert (on-premises)
  - Khả năng tương thích với các ứng dụng EPP của bên thứ ba
- Managed Detection and Response
  - Tích hợp tác nhân tích hợp với MDR
  - Hướng dẫn chuyển KEA sang KES cho MDR
- Endpoint Detection and Response
  - Tích hợp tác nhân tích hợp với EDR Optimum / EDR Expert
  - Quét các dấu hiệu về sự xâm nhập (tác vụ tiêu chuẩn)
  - Thông tin đo từ xa mở rộng cho tác vụ Quét IOC
  - 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
  - Cloud Sandbox
  - Hướng dẫn chuyển KEA sang KES cho EDR Optimum
- Kaspersky Sandbox
  - Tích hợp tác nhân tích hợp với Kaspersky Sandbox
  - Quét các dấu hiệu về sự xâm nhập (tác vụ độc lập)
  - Hướng dẫn chuyển KEA sang KES cho Kaspersky Sandbox
- Kaspersky Anti Targeted Attack Platform
  - Tích hợp tác nhân tích hợp với EDR / NDR (KATA)
  - Cấu hình đo từ xa EDR (KATA)
  - Loại trừ đo lường từ xa EDR (KATA)
    - Ví dụ 1. Các tiến trình được loại trừ
    - Ví dụ 2. Các giao tiếp mạng được loại trừ
    - Ví dụ 3. Các thao tác với tập tin được loại trừ
    - Ví dụ 4. Các sửa đổi registry được loại trừ
  - KATA Sandbox
    - Tích hợp tác nhân tích hợp với KATA Sandbox
    - Cấu hình các hành động Phản hồi với mối đe dọa
  - Hướng dẫn chuyển KEA sang KES cho EDR (KATA)

- Endpoint Detection and Response Expert (on-premises)
  - Tích hợp tác nhân tích hợp với EDR Expert (on-premises)
  - Cấu hình thiết lập đo lường từ xa của EDR Expert (on-premises)
  - Loại trừ đo từ xa của EDR Expert (on-premises)
  - Xuất và nhập bộ lọc sự kiện EDR Expert (on-premises)
  - Những lưu ý đặc biệt khi sử dụng cấu hình chính sách để thiết lập tích hợp với EDR Expert (on-premises) và EDR (KATA)
- Endpoint Detection and Response Expert (cloud)
  - Tích hợp tác nhân tích hợp với EDR Expert (cloud)
  - Cấu hình thiết lập dữ liệu đo lường từ xa của EDR Expert (cloud)
  - Loại trừ dữ liệu đo lường từ xa của EDR Expert (cloud)
  - Các xuất và nhập bộ lọc sự kiện EDR Expert (cloud)
- 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
  - Khôi phục các tập tin từ Khu vực cách ly
- Giám sát các hành động EDR

Kaspersky Unified Monitoring and Analysis Platform (KUMA)
- Tích hợp Kaspersky Endpoint Security với KUMA
  - Chuẩn bị cho tích hợp KES với KUMA
  - Kết nối KES với KUMA
- Lọc các sự kiện được gửi đến KUMA
- Xuất và nhập bộ lọc sự kiện KUMA

Hướng dẫn chuyển từ KSWS sang KES
- Sự tương hợp của thành phần của KSWS và KES
- Sự tương hợp của thiết lập KSWS và KES
- Chuyển các thành phần KSWS
- Chuyển đổi các tác vụ và chính sách của KSWS
- Chuyển vùng được tin tưởng của KSWS
- Chuyển các quy tắc Kiểm soát khởi chạy ứng dụng KSWS
- Cài đặt KES thay vì KSWS
- Chuyển cấu hình [KSWS+KEA] sang cấu hình [KES+built-in agent]
- Đảm bảo rằng Kaspersky Security for Windows Server đã được gỡ bỏ thành công
- Kích hoạt KES bằng khóa KSWS
- Các cân nhắc đặc biệt để chuyển các máy chủ có mức tải cao
- Quản lý ứng dụng trên máy chủ ở chế độ Server Core
- Chuyển từ [KSWS+KEA] sang [KES+tác nhân tích hợp]

Chế độ Light Agent để bảo vệ máy ảo
- Những cân nhắc đặc biệt cho chế độ Light Agent
- Cấu hình sơ bộ của máy ảo
  - Khả năng tương thích với công nghệ Citrix App Layering
  - Khả năng tương thích với công nghệ Citrix Provisioning (Citrix Provisioning Services)
  - Khả năng tương thích với công nghệ Omnissa App Volumes
- Cài đặt Light Agent
- Kết nối Light Agent với SVM
  - Khám phá SVM
  - Cấu hình thuật toán chọn SVM cho Light Agent

Phân phối các kết nối của Light Agents tới SVM (thẻ)
Bảo vệ kết nối giữa Light Agent và SVM
Kích hoạt Light Agent
Hướng dẫn chuyển từ KSVLA Light Agent sang KES Light Agent
Cài đặt KES Light Agent thay vì KSVLA Light Agent
Tính tương ứng của các thành phần KSVLA Light Agent và KES Light Agent
Chuyển các tác vụ và chính sách KSVLA Light Agent
Chuyển cấu hình [KSVLA Light Agent+KEA] sang cấu hình [KES Light Agent+tác nhân tích hợp]
Quản lý ứng dụng từ dòng lệnh
Setup. Cài đặt ứng dụng
Setup /x. Gỡ bỏ ứng dụng
msiexec /i. Phục hồi ứng dụng
Các lệnh AVP
SCAN. Quét phần mềm độc hại
UPDATE. Cập nhật cơ sở dữ liệu và các mô-đun phần mềm ứng dụng
ROLLBACK. Lần hoàn tác bản cập nhật gần nhất
TRACES. Truy vết
START. Bắt đầu một 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 ứng dụng
EXITPOLICY. Tắt chính sách
STARTPOLICY. Bật chính sách
DISABLE. Tắt bảo vệ
SPYWARE. Phát hiện phần mềm gián điệp
KSN. Chuyển qua lại giữa KSN / KPSN
SERVERBINDINGDISABLE. Tắt bảo vệ kết nối máy chủ
Các lệnh KESCLI
Scan. Quét phần mềm độc hại
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 ngày tháng và thời gian cập nhật gần đây nhất của cơ sở dữ liệu
EnableRTP. Bật bảo vệ
GetRealTimeProtectionState. Trạng thái của thành phần Bảo vệ mối đe dọa tập tin
GetEncryptionState. Trạng thái mã hóa ổ đĩa
Version. Xác định phiên bản của ứng dụng

- Lệnh quản lý Detection and Response
  - SANDBOX. Quản lý Sandbox
  - PREVENTION. Quản lý phòng chống thực thi
  - ISOLATION. Quản lý cách ly mạng
  - RESTORE. Khôi phục các tập tin từ Khu vực cách ly
  - IOCSCAN. Quét các dấu hiệu về sự xâm nhập (IOC)
  - MDRLICENSE. Kích hoạt MDR
  - EDRKATA. Tích hợp EDR (KATA)
  - EDRExpertOnPrem. Tích hợp EDR Expert (on-premises)
  - KUMA. Tích hợp KUMA
  - YARA. Chạy Quét YARA
  - BỘ LỌC ĐO LƯỜNG TỪ XA. Lọc các sự kiện được gửi đến KUMA
- Các lệnh quản lý Light Agent
  - KSVLAINFO. Xác định chế độ Light Agent
  - VIISINFO. Trạng thái kết nối Light Agent với Máy chủ tích hợp
  - SVMINFO. Trạng thái kết nối của Light Agent với Máychủ bảo vệ
- 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
- Thu thập dữ liệu hệ điều hành (Kaspersky Get System Info)

Hạn chế và cảnh báo

Thuật ngữ
- Authentication Agent
- Báo động giả
- Chứng nhận giấy phép
- Cloud Discovery
- 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 hiện hoạt
- Khử mã độc
- Light Agent
- Máy chủ tích hợp

- Mô-đun Nền tảng Tin tưởng
- Network Agent
- Nhóm quản trị
- OpenIOC
- Phạm vi bảo vệ
- Phạm vi quét
- SVM
- 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
- Xác thực Kerberos

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 tra nhật ký
  - Anti-Cryptor
  - Kiểm soát Web
  - Kiểm soát Thiết bị
  - Kiểm soát ứng dụng
  - Kiểm soát thích ứng sự cố
  - Giám sát tính toàn vẹn của hệ thống
  - Endpoint Sensor
  - Sandbox
  - Managed Detection and Response
  - Endpoint Detection and Response
  - Endpoint Detection and Response Expert (on-premises)
  - Network Detection and Response (KATA)
  - Tích hợp KUMA
  - 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

- Nghiêm trọng
- Lỗi chức năng
- Cảnh báo
- Thông báo thông tin

Phụ lục 7. Các phần mở rộng tập tin được hỗ trợ cho Phòng chống thực thi

Phụ lục 8. Trình thông dịch tập lệnh được hỗ trợ để Phòng chống thực thi

Phụ lục 9. Phạm vi quét IOC trong registry (RegistryItem)

Phụ lục 10. Các yêu cầu của tập tin IOC

Phụ lục 11. API cho EDR Threat Response

Phụ lục 12. Tài khoản người dùng trong quy tắc thành phần ứng dụng

Thông tin pháp lý

- 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
    - Kaspersky Endpoint Detection and Response Expert (on-premises)
    - Kaspersky Network Detection and Response (KATA)
    - Tích hợp với Kaspersky Unified Monitoring and Analysis Platform (KUMA)
  - Tuân thủ luật của Liên minh châu Âu (GDPR)
- Thông báo thương hiệu
- Thông tin về mã của bên thứ ba

Kaspersky Endpoint Security cho Windows Help

Có gì mới trong phiên bản 14.2

Đã thêm hỗ trợ xác thực dựa trên token dành cho Bảo vệ bằng mật khẩu

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

Cung cấp dữ liệu

Trong mục Thỏa thuận giấy phép người dùng cuối

Khi sử dụng KSN

GDPR

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)

Điều tốt nhất nên làm

Tối ưu hóa hiệu năng ứng dụng

Triển khai Chế độ từ chối mặc định trong Kiểm soát ứng dụng

Chuyển KEA sang KES với tác nhân tích hợp

Sử dụng KES như một phần của các giải pháp khác

Kaspersky EDR

Kaspersky Sandbox

Kaspersky MDR

Có gì mới

Bản cập nhật 14.2

Kaspersky Endpoint Security 14.2 cho Windows có các tính năng và cải tiến sau đây:

1. Đã thay đổi nhóm các thành phần được cài đặt mặc định. Cấu hình ứng dụng mặc định đã có tính năng Phòng chống Tấn công BadUSB, quản lý BitLocker và tác nhân tích hợp EDR Optimum.

2. Đã thêm hỗ trợ cho xác thực dựa trên token (Bảo vệ bằng mật khẩu). Giờ đây, để truy cập ứng dụng, bạn có thể sử dụng tên người dùng và mật khẩu của mình, mật khẩu tạm thời do quản trị viên cấp hoặc token. Ví dụ: phương thức xác thực dựa trên token có thể được sử dụng cho các tài khoản người dùng dịch vụ không yêu cầu mật khẩu.

3. Đã thêm tiêu chí độ mạnh mật khẩu mới cho BitLocker – kiểm tra lịch sử mật khẩu. Ứng dụng ngăn người dùng đặt lại mật khẩu mà họ đã sử dụng trước đó.

4. Đã thêm hỗ trợ thay đổi ngôn ngữ giao diện Kaspersky Endpoint Security khi cập nhật ứng dụng bằng cách sử dụng tác vụ *Cài đặt ứng dụng từ xa*. Giờ đây bạn không cần phải cài đặt lại ứng dụng nếu lỡ chọn sai ngôn ngữ giao diện.

5. Đã thêm các sự kiện đo kiểm từ xa mới dành cho người dùng các giải pháp Kaspersky Endpoint Detection and Response: GPO Change, SCCM Local Config Mismatch, SCCM Config Change, SCCM Deployment Task, Smb Connection Open. Những sự kiện mới này tăng cường khả năng phát hiện mối đe dọa của các giải pháp EDR.

6. Đã bổ sung hỗ trợ cho hành động ứng phó với mối đe dọa mới. *Đặt tập tin*, dành cho người dùng Kaspersky Endpoint Detection and Response Expert (on-premises). Tác vụ này cho phép bạn cung cấp các tập tin cấu hình, kịch bản ứng phó với mối đe dọa, tiện ích để giảm thiểu tác động của các cuộc tấn công, v.v., cho máy tính. Tác vụ *Đặt tập tin* có sẵn trong bảng điều khiển OSMP khi triển khai giải pháp Kaspersky EDR Expert (on-premises) phiên bản 9.0.

7. Đã cải tiến hành vi của các hành động ứng phó với mối đe dọa dành cho người dùng Kaspersky Endpoint Detection and Response Optimum. Giờ đây, trước khi thực hiện hành động (*Xóa tập tin*, *Chuyển tập tin vào Khu vực cách ly* hoặc *Phòng chống thực thi* ứng dụng sẽ kiểm tra xem đối tượng đó có quan trọng đối với hệ thống (System Critical Object, SCO) hay không và cảnh báo về tác động tiềm tàng đến sự ổn định của hệ thống. Không nên áp dụng các hành động này cho các tập tin Đối tượng đặc biệt quan trọng của hệ thống (SCO).

8. Đã thêm hỗ trợ cho người dùng Kaspersky Security for Virtualization Light Agent để vận hành ứng dụng như một phần của cụm Máy chủ tích hợp có tính khả dụng cao. Cụm máy chủ tích hợp có tính khả dụng cao cho phép bảo vệ liên tục cho môi trường ảo nhờ vào cơ chế chuyển đổi dự phòng của SVM và Light Agent sang máy chủ tích hợp dự phòng bất cứ khi nào máy chủ tích hợp chính gặp sự cố.

9. Khi phát triển phiên bản Kaspersky Endpoint Security này, chúng tôi đã tích hợp các thay đổi có trong các bản vá riêng sau: PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF18057, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF20081, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF21062, PF21063, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF22059, PF22065, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF23063, PF23095, PF24005, PF24011, PF24013, PF24014, PF24017, PF24019, PF24037, PF24043, PF24048, PF25013, PF25016, PF25019, PF25030.

Bản cập nhật 14.1

Kaspersky Endpoint Security 14.1 cho Windows có các tính năng và cải tiến sau đây:

1. Đã bổ sung hỗ trợ cho hệ điều hành Windows Server 2025.

2. Đã nâng giới hạn về số lượng quy tắc lọc sự kiện đo từ xa cho Endpoint Detection and Response Expert (on-premises) và Kaspersky Endpoint Detection and Response Expert (cloud). Kaspersky Endpoint Security hiện đã hỗ trợ tổng cộng lên đến 10.000 quy tắc lọc bao gồm và loại trừ.

3. Bây giờ bạn có thể cấu hình để các tác vụ chỉ chạy vào những ngày cụ thể trong tuần, với khoảng thời gian được chỉ định tính bằng tuần. Lịch này khả dụng trong Kaspersky Security Center 16.1 trở lên.

4. Đối với tác vụ *Quét phần mềm độc hại*, giờ đây bạn có thể chỉ định khoảng thời gian mà tác vụ sẽ tạm dừng, ví dụ như để giảm thiểu tác động đến hiệu năng máy tính trong thời gian tải cao.

5. Hiệu năng của hệ thống phụ ổ đĩa cứng trên máy tính được bảo vệ đã được tối ưu hóa bằng cách giảm số lượng thao tác I/O.

6. Khi phát triển phiên bản Kaspersky Endpoint Security này, chúng tôi đã tích hợp các thay đổi có trong các bản vá riêng sau: PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF14071, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF18057, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF20081, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF21062, PF21063, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF22059, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF23063, PF24005, PF24011, PF24013, PF24014, PF24017, PF24019, PF25013, PF25016, PF25019.

Bản cập nhật 14.0

Kaspersky Endpoint Security 14.0 cho Windows có các tính năng và cải tiến sau đây:

1. Máy tính chạy trên kiến trúc ARM hiện đã được hỗ trợ. Bạn có thể cài đặt ứng dụng ở chế độ tiêu chuẩn hoặc chế độ EDR Agent. Tuy nhiên, ứng dụng này có một số hạn chế (ví dụ: trong số các công nghệ mã hóa dữ liệu, chỉ có BitLocker được hỗ trợ).

2. Tính năng kiểm tra chính sách mở rộng được hỗ trợ trong Bảng điều khiển web Kaspersky Security Center phiên bản 15.0 trở lên. Giờ đây, bạn có thể xem các sửa đổi chính sách và lưu chúng vào một tập tin. Một bản *sửa đổi* là một tập hợp các tham số đã được người dùng chỉnh sửa và lưu lại. Các bản sửa đổi cho phép bạn so sánh và hoàn tác các thay đổi đối với các thông số chính sách.

3. Giờ đây, người dùng Kaspersky Endpoint Detection and Response đã có thể xem được các sự kiện đo từ xa mới. Những sự kiện mới này tăng cường khả năng phát hiện mối đe dọa bằng các giải pháp Kaspersky EDR.

4. Khi phát triển phiên bản này của Kaspersky Endpoint Security cho Windows, chúng tôi đã kết hợp các thay đổi có trong các bản vá riêng sau: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

Bản cập nhật 12.12

Kaspersky Endpoint Security 12.12 cho Windows có các tính năng và cải tiến sau đây:

1. Chức năng bảo vệ thư mục chia sẻ trước mã hóa bên ngoài. Trước đây, chức năng này là một phần của thành phần Phát hiện hành vi, nay đã được tách ra thành một thành phần riêng biệt Anti-Cryptor.

2. Đã bổ sung hỗ trợ cho giao thức Kerberos để xác thực ứng dụng thông qua máy chủ proxy để truy cập internet.

3. Giờ đây bạn có thể chỉ định hash tập tin cho ứng dụng tin tưởng chứ không chỉ là một đường dẫn đầy đủ.

4. Thêm nhiều tính năng của tác vụ *Quét IOC* có sẵn cho người dùng giải pháp Endpoint Detection and Response (EDR). Chức năng Quét IOC hồi cứu đã có sẵn. *Quét IOC hồi cứu* là một chế độ của tác vụ *Quét IOC*, trong đó Kaspersky Endpoint Security sẽ quét để tìm dấu hiệu về sự xâm nhập bằng cách sử dụng dữ liệu trong một khoảng thời gian nhất định. Chế độ này được thiết kế để phát hiện các dấu hiệu về sự xâm nhập trong dữ liệu hoạt động mạng của máy tính. Kaspersky Endpoint Security phân tích dữ liệu trong nhật ký hệ điều hành và nhật ký trình duyệt trên máy tính.

5. Người dùng Kaspersky Endpoint Detection and Response (EDR) có thể gỡ bỏ giới hạn kích thước của khu vực cách ly. Đây là điều có thể cần thiết cho quá trình quét YARA vì ứng dụng có thể lưu một tập tin kết xuất bộ nhớ lớn. Bây giờ bạn có thể sử dụng toàn bộ dung lượng ổ đĩa trống của mình cho khu vực cách ly.

6. Hiện tại, tính năng nén HTTPS đã được hỗ trợ để tối ưu hóa việc xuất sự kiện sang Kaspersky Unified Monitoring and Analysis Platform (KUMA). Điều này giúp giảm lưu lượng truy cập chiều ra.

7. Khi phát triển phiên bản này của Kaspersky Endpoint Security cho Windows, chúng tôi đã kết hợp các thay đổi có trong các bản vá riêng sau: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

Bản cập nhật 12.11

Kaspersky Endpoint Security 12.11 cho Windows cung cấp các tính năng và cải tiến sau đây:

1. Ứng dụng sẽ kiểm tra cấu hình của các thành phần điều khiển trước khi lưu thiết lập. Tính năng kiểm tra đã được thêm cho thành phần Kiểm soát ứng dụng, Kiểm soát thiết bị, Giám sát tính toàn vẹn của hệ thống. Bây giờ ứng dụng sẽ hiển thị cảnh báo nếu thiết lập hiện tại của thành phần điều khiển có thể làm tăng mức tải cho máy tính hoặc gây ra lỗi hệ thống. Ví dụ: trong trường hợp thành phần Kiểm soát ứng dụng, nếu bạn chọn chế độ chặn tất cả các ứng dụng ngoại trừ những ứng dụng được phép và bạn không thêm quy tắc cho phép nào, ứng dụng sẽ hiển thị cảnh báo vì cấu hình như vậy có thể gây ra lỗi hệ thống.

2. Đã thêm hỗ trợ tự động gửi tập tin tới KATA Sandbox để đánh giá. *KATA Sandbox* là một thành phần của Kaspersky Anti Targeted Attack Platform, chạy các tập tin trên ảnh ảo của hệ điều hành. 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. 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 (các máy chủ Sandbox). Để KATA Sandbox hoạt động ở chế độ tự động, bạn phải triển khai Kaspersky Anti Targeted Attack Platform 8.0 trở lên.

3. Tối ưu hóa gửi dữ liệu đo từ xa EDR. Bây giờ bạn có thể chỉ định độ dài tối đa của gói tin.

4. Đã nâng cao khả năng chẩn đoán kết nối tới Kaspersky Security Network. Đã mở rộng thông tin chi tiết về lỗi kết nối cho Kaspersky Security Network để giải quyết các sự cố tiềm ẩn.

5. Đã thêm hỗ trợ cho việc cấu hình danh sách sự kiện được gửi đến Kaspersky Unified Monitoring and Analysis Platform (KUMA). Bây giờ, ngoài danh sách sự kiện được xác định trước trong KUMA, bạn có thể thêm sự kiện vào dữ liệu đo từ xa hoặc loại trừ sự kiện theo ID của chúng theo cách thủ công trong Nhật ký sự kiện Windows.

6. Đã cập nhật giao diện chính sách trong Bảng điều khiển web. Bố cục của các phần chính sách đã được thay đổi để truy cập nhanh hơn vào các tính năng cần thiết.

7. Hỗ trợ cho Windows 11 25H2.

8. Khi phát triển phiên bản này của Kaspersky Endpoint Security cho Windows, chúng tôi đã kết hợp các thay đổi có trong các bản vá riêng sau: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF22004, PF22008, PF22014.

Bản cập nhật 12.10

Kaspersky Endpoint Security 12.10 cho Windows cung cấp các tính năng và cải tiến sau đây:

1. Đối với thành phần Phòng chống tấn công BadUSB, tùy chọn đã được thêm vào để cấp quyền cho đầu quét mã vạch đọc mã vạch từ màn hình. Bây giờ bạn không cần phải nhập mã bằng bàn phím trên màn hình để cấp quyền cho máy quét mã vạch.

2. Các tính năng và cải tiến sau đây khả dụng với người dùng giải pháp Endpoint Detection and Response (EDR) của Kaspersky:

   - Bây giờ bạn có thể quản lý Cô lập mạng của máy tính trong phần thông tin chi tiết cảnh báo. Ngoài ra, trong phần chi tiết cảnh báo, bạn có thể chỉ định khoảng thời gian Cô lập mạng của máy tính và thêm loại trừ.

   - Điền thông tin chi tiết cảnh báo bằng dữ liệu mới. Bây giờ thông tin chi tiết cảnh báo đã chứa nhiều thông tin hơn về mối đe dọa, bao gồm cách ứng dụng hoạt động khi phản hồi các mối đe dọa EDR.

   - Việc xử lý tập tin IOC đã được cải thiện. Bây giờ bạn có thể xem và chỉnh sửa nội dung của các tập tin IOC trong giao diện của Bảng điều khiển web Kaspersky Security Center. Sau khi tải tập tin IOC, ứng dụng sẽ hiển thị báo cáo về việc áp dụng thuật ngữ IOC.

   - Cải thiện phản hồi với các IOC được phát hiện. Bây giờ bạn có thể cách ly các tập tin được phát hiện bởi tác vụ *Quét IOC* ngay trong kết quả phát hiện IOC trong thuộc tính của tác vụ. Bạn cũng có thể cô lập máy tính khỏi mạng trong thuộc tính của tác vụ.

   - Bây giờ bạn có thể tạo các tập tin IOC trực tiếp trong thuộc tính của tác vụ *Quét IOC* dựa trên danh sách hash tập tin, địa chỉ IP hoặc tên DNS được tạo trong tập tin TXT.

   - Mở rộng phạm vi quét cho tác vụ *Quét IOC*. Bây giờ bạn có thể xác định phạm vi cho Quét IOC của registry (**Windows Registry – RegistryItem**). Trong các phiên bản trước của ứng dụng, bạn chỉ có thể sử dụng phạm vi Quét IOC được định sẵn trong registry.

3. Đã thêm quyền bảo vệ Mật khẩu mới, *Xuất thiết lập*. Theo mặc định, chỉ người dùng KLAdmin mới có thể tạo tập tin cấu hình với thiết lập Kaspersky Endpoint Security trong giao diện ứng dụng. Để cấp quyền truy cập cho người dùng khác, bạn cần cấp cho họ quyền tương ứng.

4. Khi phát triển phiên bản này của Kaspersky Endpoint Security cho Windows, chúng tôi đã kết hợp các thay đổi có trong các bản vá riêng sau: PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF13120, PF13123, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF15062, PF16052, PF16053, PF16055, PF16056, PF16057, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF21007.

Bản cập nhật 12.9

Kaspersky Endpoint Security 12.9 cho Windows cung cấp các tính năng và cải tiến sau đây:

1. Đã thêm chức năng mới để *quản lý mật khẩu tạm thời*. Mật khẩu tạm thời cho phép bạn cấp quyền truy cập vào Kaspersky Endpoint Security khi bật tính năng Bảo vệ bằng mật khẩu cho một máy tính riêng. Quản lý mật khẩu tạm thời cho phép lưu lịch sử mật khẩu (tối đa 30 ngày), theo dõi trạng thái mật khẩu tạm thời (*Đang hoạt động*, *Hết hạn*, *Đã thu hồi*) và thu hồi mật khẩu tạm thời.

2. Đã thêm tùy chọn chấm dứt kết nối tới các tài nguyên web bị cấm bởi các quy tắc Kiểm soát web ngay sau khi chính sách được áp dụng. Trong các phiên bản trước của ứng dụng, Kiểm soát web chỉ hạn chế các kết nối mới tới các tài nguyên web bị cấm.

3. Đối với người dùng Kaspersky Anti Targeted Attack Platform, đã thêm tùy chọn chạy kiểm tra YARA cục bộ trên máy tính. Để thực hiện việc này, bạn cần tải xuống tập tin có quy tắc YARA và thực hiện lệnh trong CMD.

4. Đã khắc phục hành vi của ứng dụng khi BitLocker được bật trên các máy tính có ổ đĩa đã được BitLocker bảo vệ bằng các công cụ của bên thứ ba. Kaspersky Endpoint Security khởi tạo quy trình khôi phục để gửi khóa khôi phục đến Kaspersky Security Center. Do đó, việc quản lý BitLocker được chuyển đến bảng điều khiển Kaspersky Security Center.

5. Một phần mới, **Response history**, khả dụng với người dùng giải pháp Detection and Response của Kaspersky. Phần này chứa thông tin về các hành động ứng phó mối đe dọa được thực hiện trên máy tính. Ví dụ: các hành động như vậy bao gồm chạy tác vụ *Chấm dứt tiến trình* hoặc cô lập máy tính khỏi mạng. Lịch sử phản hồi chỉ khả dụng với người dùng của các giải pháp Kaspersky sau: MDR, EDR, KATA.

6. Đối với người dùng Kaspersky Unified Monitoring and Analysis Platform, đã có sẵn hỗ trợ cho các hành động ứng phó với mối đe dọa EDR. Khi phản hồi các mối đe dọa, KUMA sẽ chạy các tập lệnh tạo ra các tác vụ EDR tương ứng. Để thực hiện tác vụ EDR, bạn cần tạo quy tắc phản hồi cho tập lệnh tùy chỉnh trong bảng điều khiển KUMA và chọn sự kiện.

7. Khi phát triển phiên bản Kaspersky Endpoint Security cho Windows này, chúng tôi đã kết hợp các thay đổi có trong các bản vá riêng sau: PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF20011, PF20016, PF20017, PF20020, PF20021.

Bản cập nhật 12.8

Kaspersky Endpoint Security 12.8 cho Windows cung cấp các tính năng và cải tiến sau đây:

1. Ứng dụng hiện đã hỗ trợ Chế độ Light Agent để bảo vệ môi trường ảo. Bây giờ bạn có thể triển khai ứng dụng dưới dạng Light Agent như một phần của giải pháp Kaspersky Security for Virtualization Light Agent 6.2.

2. Đã hỗ trợ chặn hoạt động của tập tin trong các container Docker trên máy chủ. *Container* là môi trường biệt lập, trong đó ứng dụng có thể chạy mà không cần tương tác trực tiếp với hệ điều hành. Kaspersky Endpoint Security sẽ quét các tập tin bên trong container mà người dùng có quyền truy cập. Khi phát hiện một mối đe dọa, các ứng dụng sẽ chặn hoạt động độc hại này và cố gắng khử mã độc tập tin bên trong container. Nếu không thể khử mã độc tập tin, ứng dụng sẽ dừng container.

3. Bây giờ bạn có thể xác định phạm vi bảo vệ để bảo vệ các thư mục được chia sẻ chống lại mã hóa từ bên ngoài (thành phần Phát hiện hành vi). Bây giờ bạn có thể chỉ định các thư mục chia sẻ mà ứng dụng phải theo dõi hoạt động đối với tập tin. Bạn cũng có thể loại trừ các tập tin khỏi phạm vi bảo vệ. Trong các phiên bản trước của ứng dụng, thành phần Phát hiện hành vi sẽ theo dõi mọi thư mục được chia sẻ để biết hoạt động đối với tập tin.

4. Bây giờ bạn có thể cấu hình các nhóm thành phần khác nhau cho các loại hệ điều hành khác nhau trong gói cài đặt. Tức là bạn có thể triển khai ứng dụng tới các máy trạm và máy chủ bằng cùng một gói cài đặt. Các thành phần không khả dụng với một loại hệ điều hành nhất định sẽ tự động bị loại trừ trong thuộc tính gói cài đặt.

5. Đã thêm tùy chọn để chọn loại trừ quét được định sẵn và các ứng dụng được tin tưởng. Các loại trừ quét được định sẵn và các ứng dụng được tin tưởng cho phép cấu hình nhanh vùng đáng tin cậy cho ứng dụng trong môi trường ảo (Citrix, VMware). Ví dụ: các loại trừ như vậy bao gồm các tập tin máy ảo VHD và VHDX. Có thể thêm loại trừ khi tạo gói cài đặt ứng dụng, tạo một chính sách hoặc khi cài đặt Kaspersky Endpoint Security.

6. Dữ liệu đo lường từ xa của EDR đã bao gồm các sự kiện cho hoạt động với thiết bị được kết nối USB. Bạn cũng có thể thêm những sự kiện này vào mục loại trừ khỏi dữ liệu đo lường từ xa của EDR.

7. Đã thêm tùy chọn để chặn kết nối mạng qua giao thức TLS 1.0 lỗi thời. TLS 1.0 có mức độ bảo mật thấp, do đó bạn nên tắt giao thức này và sử dụng phiên bản TLS 1.2 hoặc TLS 1.3 mới hơn. Theo mặc định, Kaspersky Endpoint Security sẽ chặn các kết nối TLS 1.0. Sau khi cập nhật phiên bản ứng dụng, hoạt động của các dịch vụ của bên thứ ba sử dụng giao thức TLS 1.0 có thể không thành công. Để tránh các vấn đề về hoạt động của các dịch vụ của bên thứ ba, bạn có thể cho phép sử dụng giao thức TLS 1.0 trong chính sách nhóm trước khi cập nhật phiên bản ứng dụng.

8. Khi phát triển phiên bản Kaspersky Endpoint Security cho Windows này, chúng tôi đã kết hợp các thay đổi có trong các bản vá riêng sau: PF10053, PF10054, PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018.

Bản cập nhật 12.7

Kaspersky Endpoint Security 12.7 cho Windows cung cấp các tính năng và cải tiến sau đây:

1. Bây giờ bạn có thể giới hạn sử dụng tài nguyên CPU cho các tác vụ *Quét phần mềm độc hại*. Để thực hiện, trong thiết lập ứng dụng, hãy chỉ định phần trăm mức tải CPU tối đa cho tất cả các lõi có thể được sử dụng trong khi quét máy tính.

2. Bây giờ bạn có thể gửi tập tin để quét trong KATA Sandbox theo cách thủ công. *KATA Sandbox* là một thành phần của Kaspersky Anti Targeted Attack Platform, chạy các tập tin trên ảnh ảo của hệ điều hành. 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. 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 (các máy chủ Sandbox). Để gửi tập tin cần quét tới KATA Sandbox, hãy chọn lệnh liên quan trong menu ngữ cảnh của tập tin.

3. Bây giờ bạn có thể thiết lập tích hợp với giải pháp bảo vệ mạng LAN của doanh nghiệp, *Kaspersky Network Detection and Response*. Kaspersky Network Detection and Response (NDR) là một phần của Kaspersky Anti Targeted Attack Platform. Bạn có thể cấu hình tương tác với NDR ở chế độ tiêu chuẩn cũng như chế độ EDR Agent.

4. Đã thêm hỗ trợ cho ứng dụng thư Microsoft Office Outlook phiên bản 2021 vào phần mở rộng Bảo vệ mối đe dọa thư điện tử. Phần mở rộng cho phép quét thư ở cấp độ ứng dụng thư điện tử thay vì cấp độ giao thức. Ngoài thư, phần mở rộng cho phép bạn quét các đối tượng nhận được qua giao diện MAPI từ kho lưu trữ Microsoft Exchange (ví dụ: các đối tượng trong Lịch). Quá trình quét này diễn ra trong ứng dụng thư điện tử.

5. Khi phát triển phiên bản Kaspersky Endpoint Security cho Windows này, chúng tôi đã kết hợp các thay đổi có trong các bản vá riêng sau: PF10049, PF10355, PF12114, PF13109, PF14056, PF15038, PF15045, PF16037, PF16042, PF16047, PF17014, PF17018, PF17021, PF17024, PF18006, PF18007.

Bản cập nhật 12.6

Kaspersky Endpoint Security 12.6 cho Windows cung cấp các tính năng và cải tiến sau đây:

1. Chức năng tích hợp với giải pháp Kaspersky SIEM – *Kaspersky Unified Monitoring and Analysis Platform; KUMA* – đã được thêm. Bây giờ có thể gửi sự kiện từ nhật ký sự kiện Windows tới bộ thu thập KUMA. Điều này cho phép KUMA nhận các sự kiện Windows (hỗ trợ một bộ EventID giới hạn) từ tất cả các máy tính được cài đặt Kaspersky Endpoint Security mà không cần cài đặt tác nhân KUMA trên các máy tính này.

2. Đã thêm thành phần mới *Giám sát tính toàn vẹn của hệ thống* để thay thế thành phần Giám sát tính toàn vẹn của tập tin. Thành phần Giám sát tính toàn vẹn của hệ thống bao gồm tất cả chức năng của Giám sát tính toàn vẹn của tập tin và ngoài ra còn cho phép giám sát các thay đổi của registry và kết nối của các thiết bị bên ngoài. Thành phần Giám sát tính toàn vẹn của hệ thống sẽ giám sát những thay đổi trong hệ điều hành, có thể cho biết các hành vi xâm nhập bảo mật máy tính. Khi phát hiện những thay đổi như vậy, Kaspersky Endpoint Security sẽ tạo ra các sự kiện tương ứng và cảnh báo cho quản trị viên. Giám sát tính toàn vẹn của tập tin không còn là một phần của ứng dụng. Cài đặt Giám sát tính toàn vẹn của tập tin sẽ tự động chuyển sang Giám sát tính toàn vẹn của hệ thống khi bạn cập nhật ứng dụng. Để đảm bảo tính năng Giám sát tính toàn vẹn của hệ thống hoạt động đúng, cả ứng dụng Kaspersky Endpoint Security và tiện ích quản lý đều phải được cập nhật lên phiên bản 12.6.

3. Đã thêm trạng thái của Tác nhân EDR tích hợp (KATA) được cài đặt vào thuộc tính máy tính trong bảng điều khiển Kaspersky Security Center. Bây giờ, nếu bạn đã cài đặt Tác nhân EDR (KATA) tích hợp, cột **Trạng thái cảm biến điểm cuối** sẽ hiển thị trạng thái hiện tại của thành phần (ví dụ: *Đang chạy*, *Đã dừng*, *Không được hỗ trợ bởi giấy phép*, v.v.).

4. Đã thêm tùy chọn để chọn loại trừ quét được định sẵn và các ứng dụng được tin tưởng. Các ứng dụng được tin tưởng và loại trừ quét được định sẵn sẽ giúp nhanh chóng cấu hình vùng được tin tưởng khi sử dụng ứng dụng trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager. Ví dụ: các loại trừ như vậy bao gồm các tập tin cơ sở dữ liệu MDF và LDF. Có thể thêm loại trừ khi tạo chính sách mới, sửa đổi chính sách hiện có hoặc khi cài đặt Kaspersky Endpoint Security.

5. Việc hiển thị thông tin chi tiết của cảnh báo cho Kaspersky Endpoint Detection and Response Optimum đã được chuyển từ tiện ích quản lý Kaspersky Endpoint Security sang một tiện ích quản lý Kaspersky Endpoint Detection and Response riêng biệt. Tiện ích quản lý EDR là một tiện ích duy nhất để làm việc với các tác nhân trên hệ điều hành Windows, Mac và Linux. Giờ đây, khi làm việc với EDR Optimum, bạn sẽ cần tiện ích quản lý Kaspersky Endpoint Security để tạo các tác vụ ứng phó với mối đe dọa và tiện ích quản lý EDR để xem thông tin chi tiết của cảnh báo.

6. Hỗ trợ cho Windows 11 24H2.

7. Khi phát triển phiên bản Kaspersky Endpoint Security cho Windows này, chúng tôi đã kết hợp các thay đổi có trong các bản vá riêng sau: pf10048, pf10353, pf12106, pf12107, pf12108, pf13090, pf13100, pf15031, pf15034, pf15036, pf16021, pf16023, pf16029, pf17002.

Bản cập nhật 12.5

Kaspersky Endpoint Security 12.5 cho Windows cung cấp các tính năng và cải tiến sau đây:

1. Tùy chọn để cấu hình loại trừ đo lường từ xa đã được thêm. Dữ liệu *đo từ xa* là danh sách các sự kiện đã xảy ra trên máy tính được bảo vệ. Dữ liệu đo lường từ xa được Kaspersky Anti Targeted Attack Platform (EDR) sử dụng để giám sát và bảo vệ cơ sở hạ tầng CNTT của tổ chức. Cấu hình loại trừ đo lường từ xa giúp nâng cao hiệu năng máy tính và tối ưu hóa việc truyền dữ liệu đến máy chủ thu thập Đo lường từ xa.

2. Giao diện vùng tin tưởng của ứng dụng đã được cải tiến. Giờ đây, Kaspersky Endpoint Security sẽ ẩn các đối tượng của vùng tin tưởng đối với người dùng nếu quản trị viên đã cấm người dùng thêm các tùy chọn loại trừ quét (cục bộ) và các ứng dụng được tin tưởng của họ. Điều này sẽ ngăn kẻ xâm nhập truy cập trái phép vào vùng tin tưởng, tăng mức độ bảo mật máy tính.

3. Đã thêm tùy chọn quét lưu lượng truy cập cho các ứng dụng thư MyOffice Mail và R7-Office Organizer. Thành phần Bảo vệ mối đe dọa thư điện tử giờ đây không chỉ quét các tập tin đính kèm thư khi tải xuống mà còn quét cả các thư được gửi và nhận.

4. Một danh mục tài nguyên web mới *Công cụ AI tạo sinh* đã được thêm. Bạn có thể cấu hình quyền truy cập các trang web từ danh mục mới bằng cách sử dụng Kiểm soát web.

5. Bây giờ bạn có thể chọn vị trí của quy tắc gói mạng trong danh sách Tường lửa. Vị trí của quy tắc gói tin mạng trong danh sách sẽ xác định mức độ ưu tiên của quy tắc đó. Trong các phiên bản trước của ứng dụng, chỉ có thể thêm quy tắc mới vào cuối danh sách, sau đó bạn phải di chuyển quy tắc đó trong danh sách theo cách thủ công để ưu tiên quy tắc đó. Bây giờ, khi thêm quy tắc, bạn có thể chọn đặt quy tắc đó ở đầu, ở cuối danh sách hay bên cạnh quy tắc đã chọn.

6. Trong quy tắc của các thành phần Kaspersky Endpoint Security, giờ đây bạn có thể chọn người dùng không chỉ từ Active Directory mà còn từ danh sách người dùng trong Kaspersky Security Center. Bạn cũng có thể nhập dữ liệu tài khoản người dùng cục bộ theo cách thủ công. Khả năng này đã được thêm vào cho các quy tắc của những thành phần sau: Kiểm soát ứng dụng, Kiểm soát thiết bị, Kiểm soát web, Kiểm soát thích ứng sự cố và Kiểm tra nhật ký.

7. Bây giờ báo cáo phát hiện tấn công mạng đã có một cột có Địa chỉ MAC của máy tính tấn công (thành phần Bảo vệ mối đe dọa mạng). Bên cạnh địa chỉ IP, bây giờ bạn có thể thấy địa chỉ MAC của máy tính tấn công trong báo cáo. Tính năng này rất hữu ích cho việc điều tra sự cố. Các báo cáo chứa địa chỉ MAC của máy tính tấn công cũng sẽ có trong bảng điều khiển Kaspersky Security Center Linux phiên bản 15.1 trở lên.

8. Đã tăng mức độ yêu cầu bảo vệ máy tính. Giờ đây, mức độ bảo vệ cao đã yêu cầu kích hoạt Bảo vệ các dịch vụ ứng dụng trước sự quản lý bên ngoài. Kiểm tra chỉ báo mức độ bảo mật trong phần trên của cửa sổ chính sách. Nếu bạn có mức độ bảo mật trung bình hoặc thấp, bạn có thể bật Bảo vệ dịch vụ ứng dụng trước sự quản lý bên ngoài trong cửa sổ đề xuất chỉ báo mức độ bảo mật.

9. Đã thêm hỗ trợ các sự kiện phát hiện đối tượng mới khi ứng dụng đang chạy trong Cấu hình Endpoint Detection and Response Agent (EDR Agent). Những sự kiện này đã được hỗ trợ trong cấu hình [KES+tác nhân tích hợp].

10. Khi phát triển phiên bản Kaspersky Endpoint Security cho Windows này, chúng tôi đã kết hợp các thay đổi có trong các bản vá riêng sau: pf9640, pf9830, pf9831, pf10047, pf10351, pf12102, pf12105, pf13084, pf13089, pf14040, pf14047, pf15026, pf15028, pf16013.

Bản cập nhật 12.4

Kaspersky Endpoint Security 12.4 cho Windows cung cấp các tính năng và cải tiến sau đây:

1. Đã thêm chức năng mới để bảo vệ kết nối của máy tính với Kaspersky Security Center. Tác vụ *Bảo vệ kết nối Máy chủ quản trị* cho phép đặt mật khẩu để kết nối với máy chủ được tin tưởng. Điều này có nghĩa là không thể kết nối lại máy tính và chạy các lệnh từ máy chủ khác nếu không có mật khẩu này.

2. Đối với thành phần Bảo vệ bằng mật khẩu, đã thêm khả năng chọn người dùng theo cách thủ công chọn ngoài Active Directory. Có nghĩa là bạn có thể chỉ định theo cách thủ công tên người dùng và mật khẩu cũng như gán quyền truy cập Kaspersky Endpoint Security cho tài khoản này. Bằng cách này, bạn không cần chia sẻ mật khẩu KLAdmin của mình với người dùng khác hoặc tạo tài khoản Active Directory mới để kiểm soát quyền truy cập ứng dụng.

3. Hỗ trợ cho Windows 11 23H2.

Bản cập nhật 12.3

Kaspersky Endpoint Security 12.3 cho Windows cung cấp các tính năng và cải tiến sau đây:

1. Bây giờ bạn có thể cài đặt ứng dụng trong cấu hình Endpoint Detection and Response Agent. Cấu hình này cho phép cài đặt ứng dụng với một bộ thành phần được yêu cầu bởi các giải pháp Detection and Response của Kaspersky: Kaspersky Managed Detection and Response và Kaspersky Anti Targeted Attack Platform (EDR). Bạn có thể cài đặt ứng dụng trong cấu hình này cùng với các giải pháp của bên thứ ba (ví dụ: Dr.Web, Dallas Lock, ESET). Điều này cho phép bạn sử dụng các công cụ bảo mật cơ sở hạ tầng của bên thứ ba cùng với tính năng Detection and Response by Kaspersky.

2. Đã cải tiến khả năng hoạt động của Kaspersky Endpoint Security với các thiết bị Bluetooth. Bây giờ bạn có thể cấu hình loại trừ và hạn chế quyền truy cập vào tất cả các thiết bị Bluetooth ngoại trừ thiết bị đầu vào (bàn phím không dây, chuột, v.v.).

3. Đã tối ưu hóa hoạt động của thành phần Kiểm soát ứng dụng với cơ sở dữ liệu các tập tin thực thi. Giờ đây Kaspersky Endpoint Security sẽ tự động xóa thông tin của tập tin khỏi cơ sở dữ liệu nếu tập tin đó bị xóa khỏi máy tính. Điều này cho phép cập nhật cơ sở dữ liệu và tiết kiệm tài nguyên của Kaspersky Security Center.

4. Đã tăng mức độ yêu cầu bảo vệ máy tính. Mức độ bảo vệ cao hiện nay yêu cầu bật Bảo vệ bằng mật khẩu. Kiểm tra chỉ báo mức độ bảo mật trong phần trên của cửa sổ chính sách. Nếu có mức bảo vệ trung bình hoặc thấp, bạn có thể bật Bảo vệ bằng mật khẩu trong cửa sổ đề xuất chỉ báo mức độ bảo mật.

5. Đã thêm hỗ trợ giao thức HTTPS để cho phép ứng dụng hoạt động với Kaspersky Security Network. Cho phép sử dụng HTTPS trong thuộc tính Máy chủ quản trị trong Thiết lập máy chủ proxy KSN.

Bản cập nhật 12.2

Kaspersky Endpoint Security 12.2 cho Windows cung cấp các tính năng và cải tiến sau đây:

1. Đã thêm hỗ trợ giao thức WPA3 vào kiểm soát kết nối với mạng Wi-Fi (Kiểm soát thiết bị). Bây giờ bạn có thể chọn giao thức WPA3 trong thiết lập mạng Wi-Fi được tin tưởng và từ chối kết nối với mạng bằng giao thức kém bảo mật hơn.

2. Bây giờ bạn có thể chọn giao thức và cổng cho các loại trừ của Bảo vệ mối đe dọa mạng. Bây giờ ngoài việc chỉ định địa chỉ IP của các thiết bị được tin tưởng, bạn cũng có thể chọn một cổng và giao thức. Điều này cho phép bạn loại trừ các luồng dữ liệu riêng lẻ và ngăn các cuộc tấn công mạng từ các địa chỉ IP được tin tưởng.

3. Thứ tự khác nhau của các nguồn cập nhật cho tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng cục bộ* nếu một chính sách được áp dụng cho máy tính. Máy chủ Kaspersky Security Center hiện được sử dụng theo mặc định làm nguồn cập nhật đầu tiên thay vì máy chủ Kaspersky. Điều này giúp tiết kiệm lưu lượng khi người dùng chạy tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* cục bộ.

Bản cập nhật 12.1

Kaspersky Endpoint Security 12.1 cho Windows cung cấp các tính năng và cải tiến sau đây:

1. Đã thêm tác nhân tích hợp cho giải pháp Kaspersky Anti Targeted Attack Platform. Bạn không còn cần Kaspersky Endpoint Agent để sử dụng EDR (KATA) nữa. Tất cả các chức năng của Kaspersky Endpoint Agent sẽ được thực hiện bởi Kaspersky Endpoint Security. Để chuyển các chính sách của Kaspersky Endpoint Agent, hãy sử dụng Trình hướng dẫn chuyển đổi. Sau khi cập nhật ứng dụng, Kaspersky Endpoint Security sẽ chuyển sang sử dụng tác nhân tích hợp và gỡ bỏ Kaspersky Endpoint Agent. Đã thêm Kaspersky Endpoint Agent vào danh sách phần mềm không tương thích. Kaspersky Endpoint Security có các tác nhân tích hợp sẵn cho mọi giải pháp Detection and Response, do đó bạn không cần cài đặt Kaspersky Endpoint Agent để tích hợp với các giải pháp đó nữa.

2. Đã hỗ trợ chế độ tương thích Azure WVD. Tính năng này đảm bảo hiển thị chính xác trạng thái máy ảo Azure trong bảng điều khiển Kaspersky Anti Targeted Attack Platform. Chế độ tương thích Azure WVD cho phép gán ID cảm biến duy nhất vĩnh viễn cho các máy ảo này.

3. Bây giờ bạn có thể cấu hình quyền truy cập của người dùng vào thiết bị di động trong iTunes hoặc các ứng dụng tương tự. Ví dụ: bạn có thể cho phép thiết bị di động chỉ được sử dụng trong iTunes và chặn sử dụng thiết bị di động làm ổ đĩa di động. Ứng dụng này cũng hỗ trợ các quy tắc này cho ứng dụng Android Debug Bridge (ADB).

4. Kaspersky Security Center phiên bản 11 không còn được hỗ trợ nữa. Hãy nâng cấp Kaspersky Security Center lên phiên bản mới nhất.

Đã khắc phục các sự cố

Bảng dưới đây liệt kê tất cả các sự cố đã phát hiện trong các phiên bản trước của Kaspersky Endpoint Security và đã được khắc phục trong phiên bản hiện tại.

Danh sách các lỗi đã được khắc phục trong phiên bản 14.2

Mã định danh	Mô tả
10110351	Thành phần Kiểm soát thiết bị cho phép truy cập vào thiết bị MTD (thẻ SD) khi hành động **Chặn** được chọn cho loại thiết bị **Ổ đĩa di động**.
10068496	Trên thiết bị được bảo vệ, chế độ Bảo vệ chống giả mạo địa MAC có thể được thay đổi khi thiết lập Bảo vệ mối đe dọa mạng bị khóa trong chính sách cha.
10095087	Khi bật tính năng quét Kết nối mã hóa, việc truy cập bất kỳ trang web nào thông qua tường lửa thế hệ mới (NGFW) có chứng chỉ bị thu hồi sẽ kích hoạt thông báo về việc bị chuyển hướng đến một tên miền có chứng chỉ không được tin tưởng.
10140912	Sau khi cài đặt ứng dụng, máy tính không nhận diện được thiết bị PDA BHT1100B chạy hệ điều hành Windows Mobile.
10141009	Nếu thành phần Mã hóa tập tin được cài đặt, ứng dụng Anthropic Claude có thể không khởi chạy.

Mã định danh	Mô tả
10610853	Sau khi nâng cấp lên phiên bản mới, không thể mở chính sách vì thiết lập Kiểm soát thiết bị trong phiên bản mới bao gồm các thiết bị không được hỗ trợ trong phiên bản trước.
10720516	Khi cài đặt ứng dụng, các tệp đính kèm trong các tập tin ở định dạng văn phòng có thể không mở được.
10421967	Không thể đăng nhập vào hộp thư dùng chung nếu hộp thư này được thêm vào dưới dạng một tài khoản riêng biệt.

Danh sách sự cố đã được khắc phục trong tiện ích web 14.2.0.8289

Mã định danh	Mô tả
9946286	Khi thêm địa chỉ trang web vào quy tắc Kiểm soát web, không thể sử dụng tên đại diện không có dấu chấm giữa tên miền và vùng tên miền.
10054657 10507166	Sau khi chuyển sang phiên bản mới, không thể quản lý một số thành phần nhất định (chẳng hạn như Kiểm soát thiết bị và Application Control) thông qua chính sách.
10084390	Trong thiết lập thành phần Kiểm soát thiết bị, loại thiết bị **Ổ đĩa cứng** bị trùng lặp, khiến ổ cứng của người dùng bị chặn.
10113718	Trong một số trường hợp, các quy tắc tường lửa tùy chỉnh không được hiển thị.
10311613	Trong thiết lập thành phần Host Intrusion Prevention, không thể thêm tài nguyên được bảo vệ bằng tên đại diện khi sử dụng ký tự `*`.
10391923	Trong Kiểm soát ứng dụng, khi tạo một danh mục ứng dụng dựa trên giá trị hash MD5 của một tập tin, không có cảnh báo nào được hiển thị cho biết danh mục đó không hợp lệ và sẽ không hoạt động.
10571790	Đối với thành phần Application Control, tiêu đề của danh sách quy tắc chặn trong chế độ **Allow all except the rules list** đã được hiệu chỉnh.
10592891 10689065	Trong Khu vực tin tưởng, trường **Comment** không được hiển thị đối với các loại trừ trong phần **Malware Scan exclusions**.
10613015 10689049 10592534	Trong thành phần Kiểm soát thiết bị, trường **Comment** không được hiển thị đối với các thiết bị được tin tưởng.
10645068 10689057	Tác vụ *Remove key* không chạy nếu chọn tập tin khóa giấy phép ở định dạng KEY.
10685370 10685422	Trong thành phần Kiểm soát thiết bị, không thể thêm thiết bị mới vào danh sách thiết bị được tin tưởng nếu đã có thiết bị có tên đó trong danh sách.
10721136	Không thể lưu các tác vụ nhóm nếu không chỉ định ngày hoàn thành trong thiết lập lịch trình.
10753509	Sửa đổi danh sách người dùng và nhóm cho các thiết bị được tin tưởng trong thành phần Kiểm soát thiết bị có thể thay đổi loại bản ghi, khiến các thiết lập không còn áp dụng cho thiết bị đó nữa.
10773402	Trong một số trường hợp, các thay đổi đối với thiết lập chính sách có thể không được lưu do cấu hình bị hỏng.
10822620	Thiết lập của thành phần Anti-Cryptor không được hiển thị trong chính sách và thay đổi đối với thiết lập thông báo không được lưu.
10817035	Trong chính sách con, vẫn cho phép thêm thiết bị được tin tưởng ngay cả khi thiết lập này bị vô hiệu hóa trong chính sách cha (biểu tượng "ổ khóa"). Tuy nhiên, thiết bị được thêm vào lại không được lưu.
10678009	Trong tiện ích web Kaspersky Endpoint Security, không thể thêm quy tắc tường lửa mới vào chính sách nếu trước đây quy tắc đó được tạo bằng dải địa chỉ IP.

Danh sách các lỗi đã được khắc phục trong phiên bản 14.1

Mã định danh	Mô tả
10140523	Việc kích hoạt Native NVMe trong Windows 11 có thể khiến ứng dụng hoạt động không ổn định.
9340076	Trên thiết bị đã cài đặt ứng dụng và bật tính năng Mã hóa tập tin, Windows Explorer sẽ không tự động làm mới nội dung của thư mục mạng sau khi thư mục đó được sửa đổi từ thiết bị khác.
9722863	Báo cáo Kiểm soát thiết bị không bao gồm sự kiện ngắt kết nối token USB.
10006481	Sau khi áp dụng quy tắc từ chối lưu lượng đến, các kết nối TCP đang hoạt động, được kết nối với dịch vụ bên ngoài có thể bị chấm dứt sớm do tính toán sai thời gian chờ.
10140912	Ứng dụng không phát hiện thiết bị PDA BHT1100B.
10157563	Folder Redirection có thể không hoạt động sau khi khởi động lại trên các máy trạm VDI.
10158494	Tính năng Quản lý thiết bị ghi lại nhiều sự kiện kết nối và ngắt kết nối của thiết bị di động mà không cần kết nối lại vật lý.

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?

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 phần mềm độc hại 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?

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?

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.

Ứng dụng này không nhằm mục đích sử dụng trong các quy trình công nghệ liên quan đến hệ thống điều khiển tự động. Để bảo vệ các thiết bị trong các hệ thống như vậy, bạn nên sử dụng ứng dụng Kaspersky Industrial CyberSecurity for Nodes.

Các công nghệ phát hiện mối đe dọa



Máy học

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).



Phân tích đám mây

Kaspersky Endpoint Security sẽ nhận dữ liệu về mối đe dọa từ 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.



Phân tích chuyên gia

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.



Phân tích hành vi

Kaspersky Endpoint Security sẽ phân tích hoạt động của đối tượng theo thời gian thực.



Phân tích tự động

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.



Sandbox

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.



Cloud Sandbox

Kaspersky Endpoint Security sẽ quét các đối tượng trong môi trường cách ly do Kaspersky cung cấp. Công nghệ Cloud Sandbox được bật vĩnh viễn và khả dụng cho tất cả người dùng Kaspersky Security Network bất kể họ đang sử dụng loại giấy phép nào. Nếu đã triển khai giải pháp Endpoint Detection and Response, bạn có thể bật một bộ đếm riêng cho các mối đe dọa được Cloud Sandbox phát hiện.

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.

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 sự lây nhiễm vào hệ thống tập tin máy tính. Theo mặc định, thành phần Bảo vệ mối đe dọa tập tin sẽ nằm vĩnh viễn trong RAM của máy tính và quét tất cả các tập tin đã mở, đã lưu và đã chạy theo thời gian thực. Thành phần này sẽ quét các tập tin trên tất cả các ổ đĩa máy tính, bao gồm cả 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 kết nối đến 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 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 • Windows Mail • MyOffice Mail • R7-Office Organizer Để quét lưu lượng truy cập trong ứng dụng thư Mozilla Thunderbird, MyOffice Mail và R7-Office Organizer, bạn cần phải thêm chứng chỉ Kaspersky vào kho chứng chỉ và chọn kho chứng chỉ riêng. 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 Mail Threat Protection hỗ trợ các phiên bản 32 bit và 64 bit của Outlook 2010, 2013, 2016, 2019, 2021, 2024 và 365. Trên máy tính có kiến trúc Arm, phần mở rộng Mail Threat Protection hỗ trợ các phiên bản 32 bit và 64 bit của Outlook 2016, Outlook 2021, Outlook 2024 và Outlook 365 dành cho Arm64. **Bảo vệ mối đe dọa mạng** Thành phần *Bảo vệ mối đe dọa mạng* (còn được gọi là Intrusion Detection System, IDS) sẽ giám sát lưu lượng truy cập mạng đến để biết hoạt động đặc trưng của các cuộc tấn công mạng. Khi ứng dụng 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 ứng dụng. 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.

Phần	Thành phần
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 tiếng của các địa chỉ web được quét, cũng như thông tin về danh mục và danh tiếng của các tập tin 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 và cung cấp chức năng bảo vệ chủ động cho máy tính. Thành phần Phát hiện hành vi còn giám sát các cổng mạng để tìm các tiến trình của ứng dụng có thể đe dọa đến tính bảo mật của máy tính. Ứng dụng sẽ lấy thông tin về những tiến trình như vậy thông qua cơ sở dữ liệu chống virus. **Chống công cụ mã hóa** Thành phần Anti-Cryptor sẽ 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. **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. Thành phần Phòng chống khai thác còn giám sát các cổng mạng để tìm các tiến trình của ứng dụng có thể đe dọa đến tính bảo mật của máy tính. Ứng dụng sẽ lấy thông tin về những tiến trình như vậy thông qua cơ sở dữ liệu chống virus. **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** Thành phần 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.

Phần	Thành phần
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 mất 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 không điển hình (ví dụ, quy tắc *Khởi chạy Microsoft PowerShell từ ứng dụng office*). 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. **Kiểm tra nhật ký** Kiểm tra nhật ký sẽ giám sát tính toàn vẹn của môi trường được bảo vệ dựa trên phân tích nhật ký sự kiện của Windows. Khi ứng dụng phát hiện các dấu hiệu của hành vi bất thường trong hệ thống, ứng dụng sẽ thông báo cho quản trị viên, vì hành vi này có thể chỉ báo một nỗ lực tấn công mạng. **Giám sát tính toàn vẹn của hệ thống** Thành phần Giám sát tính toàn vẹn của hệ thống sẽ giám sát những thay đổi trong hệ điều hành, có thể cho biết các hành vi xâm nhập bảo mật máy tính. Khi phát hiện những thay đổi như vậy, Kaspersky Endpoint Security sẽ tạo ra các sự kiện tương ứng và cảnh báo cho quản trị viên.
Tác vụ 	**Quét phần mềm độc hại** Kaspersky Endpoint Security sẽ quét máy tính để tìm virus và các mối đe dọa khác. Tác vụ Quét phần mềm độc hại 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 cơ sở dữ liệu và mô-đun ứng dụng** 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 của ứng dụng** 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).

Phần	Thành phần
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. **Endpoint Detection and Response Expert (on-premises)** và **Network Detection and Response (KATA)** Các tác nhân tích hợp để quản lý thành phần Network 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 ba đơn vị chức năng: • Kaspersky Anti Targeted Attack Platform (*KATA*) • Kaspersky Endpoint Detection and Response (*EDR (KATA)*) • Network Detection and Response (*NDR (KATA)*) Bạn có thể mua tất cả các đơn vị chức năng hoặc mua riêng từng đơn vị chức năng. Để biết chi tiết về giải pháp này, vui lòng tham khảo Trợ giúp của Kaspersky Anti Targeted Attack Platform. **Sandbox** Tác nhân tích hợp cho Sandbox. Thành phần *Sandbox* phát hiện và tự động chặn các mối đe dọa nâng cao trên máy tính. 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. 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 (các máy chủ Sandbox). Để biết chi tiết về giải pháp này, vui lòng tham khảo Trợ giúp của Kaspersky Sandbox và Trợ giúp của Kaspersky Anti Targeted Attack Platform. **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.

Các chế độ của ứng dụng: Tiêu chuẩn, EDR Agent, Light Agent

Kaspersky Endpoint Security cho Windows là một phần của nhiều giải pháp Kaspersky. Tùy thuộc vào giải pháp, bạn cần chọn chế độ cho ứng dụng.



Chế độ tiêu chuẩn

Đây là chế độ chính và mặc định của ứng dụng. Bạn có thể cài đặt ứng dụng ở chế độ này như một phần của giải pháp Kaspersky EPP (Endpoint Protection Platform). Ví dụ: Kaspersky Endpoint Security ở Chế độ tiêu chuẩn là một phần của Kaspersky Endpoint Security for Business. Kaspersky Endpoint Security cho phép bảo vệ toàn diện cho máy trạm và máy chủ trước nhiều mối đe dọa, tấn công mạng và lừa đảo. Ở chế độ tiêu chuẩn, các tác nhân tích hợp sẵn cũng có sẵn để tích hợp với các giải pháp Kaspersky Detection and Response, bao gồm EDR, MDR, KUMA và các giải pháp khác.



EDR Agent

Chế độ này cho phép triển khai các giải pháp Kaspersky Detection and Response cùng với các giải pháp EPP của bên thứ ba. Các giải pháp Detection and Response, bao gồm Kaspersky Managed Detection and Response (MDR) và Kaspersky Anti Targeted Attack Platform (KATA). EDR Agent cũng hỗ trợ giải pháp Kaspersky SIEM, Kaspersky Unified Monitoring and Analysis Platform (KUMA).

Ở chế độ này, các thành phần bảo vệ tiêu chuẩn như Bảo vệ chống mối đe dọa tập tin hoặc Bảo vệ chống mối đe dọa web không khả dụng. Giải pháp EPP của bên thứ ba cung cấp khả năng bảo vệ tiêu chuẩn cho máy tính. EDR Agent liên tục giám sát các tiến trình đang chạy trên các máy tính này, các kết nối mạng mở và các tập tin đang được sửa đổi, đồng thời tương tác với các giải pháp Detection and Response.



Light Agent

Chế độ này được sử dụng để bảo vệ môi trường ảo. Kaspersky Endpoint Security ở chế độ Light Agent là một phần của giải pháp Kaspersky Hybrid Cloud Security. Light Agent bảo vệ các máy ảo có hệ điều hành khách cho máy trạm và máy chủ. Các thành phần bảo vệ và kiểm soát có sẵn ở chế độ này giống như ở chế độ Tiêu chuẩn. Sự khác biệt là các đối tượng được quét virus và phần mềm độc hại khác bằng một thành phần giải pháp đặc biệt được cài đặt trên một máy ảo riêng biệt, SVM (Secure Virtual Machine). Do đó, Light Agent sử dụng tài nguyên của SVM để đảm bảo tính bảo mật của cơ sở hạ tầng thay vì tài nguyên của máy ảo.

Gói phân phối

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

- **AES256**

  Gói phân phối này được dùng để cài đặt trên các máy tính có kiến trúc x86/x64. Gói phân phối này chứa các công cụ mật mã để triển khai thuật toán mã hóa AES (Advanced Encryption Standard) với độ dài khóa hiệu quả là 256 bit.

- **AES56**

  Gói phân phối này được dùng để cài đặt trên các máy tính có kiến trúc x86/x64. 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.

- **Arm64**

  Gói phân phối này được thiết kế để cài đặt trên các máy tính chạy trên kiến trúc Arm. Gói phân phối này không được dùng để cài đặt trên máy chủ.

Trước khi cài đặt, hãy đảm bảo gói phân phối phù hợp với kiến trúc bộ xử lý của bạn. Nếu gói phân phối không phù hợp với kiến trúc bộ xử lý, trình cài đặt sẽ dừng quá trình cài đặt và báo lỗi.

Gói phân phối là một tệp lưu trữ tự giải nén ở định dạng EXE. Để xem nội dung của gói phân phối, bạn cần giải nén tệp lưu trữ vào một thư mục riêng. 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 cho tiện tích quản lý ứng dụng trong Bảng điều khiển quản trị Kaspersky Security Center.
`bases.cab`	Các tập tin trong gói cập nhật được sử dụng trong quá trình cài đặt.
`cleaner_v2.cab` `cleanerapi_v2.cab`	Các tập tin để gỡ bỏ phần mềm không tương thích.
`incompatible.txt`	Tập tin chứa danh sách phần mềm có thể gây ra sự cố tương thích với Kaspersky Endpoint Security. Kaspersky không đảm bảo khả năng tương thích của Kaspersky Endpoint Security với phần mềm trong danh sách này.
`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.
`kes.cab`	Các tập tin cho giao diện đồ họa của ứng dụng.
`aes256.cab` / `aes56.cab`	Các tập tin cho thuật toán mã hóa AES (không có trong gói phân phối Arm64).
`package.kcat`	Tập tin chứa các mã nhận diện của gói phân phối ứng dụng. Mã nhận diện số đảm bảo tính xác thực và toàn vẹn của gói phân phối ứng dụng.

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

Bài viết này liệt kê các phiên bản phần mềm mà ứng dụng đã được kiểm thử và được đảm bảo hoạt động đúng chức năng. Ứng dụng này cũng có thể hoạt động với các phiên bản phần mềm khác, nhưng các cấu hình đó chưa trải qua chu kỳ kiểm thử đầy đủ và không được đưa vào danh sách các phiên bản được đảm bảo hỗ trợ.

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:

Để cài đặt ứng dụng, bạn cần có quyền quản trị viên trên máy tính.

Yêu cầu chung tối thiểu

Yêu cầu tối thiểu	Máy trạm (x86/x64)	Máy chủ (x86/x64)	Arm
Lưu trữ	2 GB	2 GB	2 GB
CPU	1 GHz, hỗ trợ tập lệnh SSE2	1.4 GHz, hỗ trợ tập lệnh SSE2	1 GHz, kiến trúc Armv8.1
RAM	Máy trạm (x86): 1 GB Máy trạm (x64): 2 GB	2 GB Lưu ý: Máy chủ cần 8 GB bộ nhớ để cài đặt ứng dụng với tác nhân tích hợp sẵn cho việc tích hợp với Kaspersky Anti Targeted Attack Platform.	4 GB
Microsoft .NET Framework	4 trở lên	4 trở lên	4.8 trở lên

Máy trạm

Các hệ điều hành được hỗ trợ cho máy trạm:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1
- 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 / Enterprise multi-session
- Windows 11 for Arm64 Home / Pro / Pro for Workstations / Education / Enterprise

Hệ điều hành Windows, bắt đầu từ phiên bản 11 24H2, hỗ trợ công nghệ UDP Receive Segment Coalescing Offload (URO). Công nghệ này được bật theo mặc định nếu máy tính có card mạng và trình điều khiển tương thích. Tắt URO trên máy tính của người dùng có thể làm giảm đáng kể hiệu năng của ứng dụng.

Để đảm bảo Kaspersky Endpoint Security hoạt động đúng, dịch vụ Windows Security Center (wscsvc) phải đang chạy trên máy tính của người dùng.

Không thể cài đặt Kaspersky Endpoint Security trên Microsoft Windows 7 nếu không cài đặt bản cập nhật hệ điều hành: KB4490628 (12 tháng 3 năm 2019) và KB4474419 (23 tháng 9 năm 2019). Để biết thông tin chi tiết, hãy 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 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 for Windows thay vì Kaspersky Security for Windows Server trên các máy chủ và cụm máy chủ trong tổ chức của bạn (Cluster Mode). Ứng dụng cũng hỗ trợ Server Core Mode (xem các vấn đề đã biết).

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;
- Windows Web Server 2008 R2 Service Pack 1
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter (bao gồm chế độ Server Core);
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (bao gồm chế độ Server Core);
- Windows Server 2016 Essentials / Standard / Datacenter (bao gồm chế độ Server Core);
- Windows Server 2019 Essentials / Standard / Datacenter (bao gồm chế độ Server Core);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (bao gồm chế độ Core Server);
- Windows Server 2025 Standard / Datacenter.

> Không thể cài đặt Kaspersky Endpoint Security trên Microsoft Windows Server 2008 R2 nếu không cài đặt bản cập nhật hệ điều hành: KB4490628 (12 tháng 3 năm 2019) và KB4474419 (23 tháng 9 năm 2019).

> 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.

Các hệ điều hành cho máy chủ không được hỗ trợ:

- Windows Server 2003 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 2;
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2008 Core Standard / Enterprise / Datacenter Service Pack 2
- Microsoft Small Business Server 2008 Standard / Premium Service Pack 2

Nền tảng ảo

Các nền tảng ảo được hỗ trợ để vận hành ứng dụng ở chế độ tiêu chuẩn:

- VMware Workstation Pro 15.5.2;
- VMware ESXi 7.0 Patch Release ESXi 7.0b
- Windows Hyper-V Server 2019
- Citrix Virtual Apps và Desktops 7 2009;
- Citrix Provisioning 2009;
- Citrix Hypervisor 8.2 LTSR

Ứng dụng hỗ trợ các máy ảo chạy Windows 11 Pro Arm64 được tạo bằng Hyper-V.

Máy ảo để cài đặt Light Agent

Cài đặt Kaspersky Endpoint Security ở chế độ Light Agent trên máy ảo dựa trên kiến trúc Arm hiện không được hỗ trợ.

BIOS trên máy ảo phải hỗ trợ đặc tả SMBIOS phiên bản 2.1 trở lên.

Phải cài đặt các gói phần mềm và tiện ích sau trên máy ảo:

- Khi sử dụng gói Microsoft Hyper-V – Integration Services.
- Khi sử dụng gói VMware vSphere – VMware Tools.
- Khi sử dụng gói XenServer – XenTools.
- Khi sử dụng gói HUAWEI FusionSphere – HUAWEI Tools.
- Khi sử dụng hypervisor dựa trên KVM – QEMU Guest Agent.

Xem Trợ giúp của Kaspersky Security for Virtualization Light Agent đối với các yêu cầu của hạ tầng ảo để chạy ứng dụng ở chế độ Light Agent.

Để ứng dụng hoạt động đúng, hãy sử dụng giao diện mạng ảo hóa với băng thông tối thiểu 100 Mbit/giây.

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;
- Microsoft Remote Desktop Services dựa trên Windows Server 2022;
- Microsoft Remote Desktop Services dựa trên Windows Server 2025;
- Citrix RDSH từ Citrix Virtual Apps và Desktops 7 2507 LTSR

Hỗ trợ Kaspersky Security Center

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

- Kaspersky Security Center 14.2
- Kaspersky Security Center Linux 14.2
- Kaspersky Security Center Linux 15
- Kaspersky Security Center Windows 15.1
- Kaspersky Security Center Linux 15.1
- Kaspersky Security Center Linux 15.2
- Kaspersky Security Center Linux 15.3
- Kaspersky Security Center Linux 15.4
- Kaspersky Security Center Linux 16

- Kaspersky Security Center Linux 16.1
- Kaspersky Security Center Linux 16.2
- Kaspersky Security Center Linux 16.3
- Kaspersky Security Center Linux 17

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).

Kể từ Kaspersky Endpoint Security 12.8 cho Windows, bạn có thể cấu hình các nhóm thành phần khác nhau cho các loại hệ điều hành khác nhau trong gói cài đặt. Tức là bạn có thể triển khai ứng dụng tới các máy trạm và máy chủ bằng cùng một gói cài đặt.

Cài đặt Kaspersky Endpoint Security ở chế độ Light Agent trên máy ảo dựa trên kiến trúc Arm hiện không được hỗ trợ.

So sánh các tính năng của Kaspersky Endpoint Security

Tính năng	Máy trạm	Máy trạm chạy trên Arm	Máy chủ	Chế độ Server Core
Bảo vệ mối đe dọa nâng cao				
Kaspersky Security Network	✓	✓	✓	✓
Phát hiện hành vi	✓	✓	✓	✓
Chống công cụ mã hóa	✓	✓	✓	✓
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 tra nhật ký	–	–	✓	–
Kiểm soát ứng dụng	✓	✓	✓	✓
Kiểm soát thiết bị	✓	✓	✓	✓
Kiểm soát Web	✓	✓	✓	–

Tính năng	Máy trạm	Máy trạm chạy trên Arm	Máy chủ	Chế độ Server Core
Kiểm soát thích ứng sự cố	✓	✓	–	–
Giám sát tính toàn vẹn của hệ thống	–	–	✓	–
Cloud Discovery	✓	✓	–	–
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 (cloud)	✓	✓	✓	✓
Endpoint Detection and Response (KATA)	✓	✓	✓	✓
Network Detection and Response (KATA)	✓	✓	✓	✓
Sandbox	✓	✓	✓	✓
Managed Detection and Response (MDR)	✓	✓	✓	✓
Tích hợp KUMA	✓	✓	✓	✓

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 có thể làm việc với Bảng điều khiển web bằng trình duyệt trên bất kỳ máy tính nào.

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.

Kaspersky Endpoint Security là một phần của giải pháp Kaspersky Next Pro View. Để biết thêm thông tin về các tính năng ứng dụng có sẵn khi nó hoạt động dưới dạng một phần của giải pháp này, hãy xem Trợ giúp Kaspersky Next.

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	✓	✓	✓
Chống công cụ mã hóa			
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 tra nhật ký	✓	✓	✓
Kiểm soát ứng dụng	✓	✓	✓
Kiểm soát thiết bị	✓	✓	✓
Kiểm soát Web	✓	✓	✓
Kiểm soát thích ứng sự cố	✓	✓	✓
Giám sát tính toàn vẹn của hệ thống	✓	✓	✓
Cloud Discovery	–	–	✓
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 (cloud)	–	–	✓
Endpoint Detection and Response (KATA)	✓	✓	–
Network Detection and Response (KATA)	✓	✓	–
Sandbox	–	✓	–
Managed Detection and Response (MDR)	✓	✓	✓
Tích hợp KUMA	✓	✓	✓

Tính năng	Kaspersky Security Center		Kaspersky Security Center
	Bảng điều khiển quản trị	Bảng điều khiển web	Bảng điều khiển đám mây
Tác vụ			
Thêm khóa	✓	✓	✓
Thay đổi thành phần ứng dụng	✓	✓	✓
Kho	✓	✓	✓
Cập nhật	✓	✓	✓
Hoàn tác bản cập nhật	✓	✓	✓
Quét phần mềm độc hại	✓	✓	✓
Kiểm tra tính toàn vẹn của ứng dụng	✓	✓	–
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)	–	✓	✓
Bắt đầu tiến trình (EDR)	–	✓	✓
Chấm dứt tiến trình (EDR)	–	✓	✓

Khả năng tương thích với các ứng dụng khác

Kaspersky Endpoint Security không tương thích với một số ứng dụng của Kaspersky cũng như một số ứng dụng của bên thứ ba. Do đó, trước khi cài đặt, cập nhật phiên bản ứng dụng và thay đổi các thành phần ứng dụng, Kaspersky Endpoint Security sẽ quét máy tính để xem có ứng dụng nào như vậy hay không.

Khả năng tương thích với các ứng dụng của bên thứ ba

Kaspersky Endpoint Security không tương thích với các ứng dụng thuộc hệ thống bảo vệ điểm cuối của bên thứ ba (Endpoint Protection Platform, EPP). Kaspersky Endpoint Security cũng có thể gặp phải sự cố tương thích với các ứng dụng khác. Để xác định khả năng tương thích, Kaspersky Endpoint Security sẽ tham khảo danh sách phần mềm do Kaspersky chuẩn bị. Danh sách này được chứa trong tập tin incompatible.txt. Tập tin này được kèm theo gói phân phối.

Kaspersky không đảm bảo khả năng tương thích của Kaspersky Endpoint Security với phần mềm trong danh sách này. Nếu phát hiện một ứng dụng trong danh sách, trình cài đặt sẽ dừng triển khai Kaspersky Endpoint Security. Trình cài đặt có thể tự động xóa một số ứng dụng khỏi danh sách. Nếu bạn sẵn sàng bỏ qua những rủi ro và muốn cài đặt Kaspersky Endpoint Security cùng một phần mềm trong danh sách trên cùng một máy tính, bạn có thể bỏ qua việc kiểm tra máy tính (xem hướng dẫn bên dưới).

TẢI XUỐNG TẬP TIN INCOMPATIBLE.TXT

Khả năng tính tương thích với các ứng dụng của Kaspersky

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

- Kaspersky Standard | Plus | Premium.
- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Endpoint Sensor như một phần của Kaspersky Anti Targeted Attack Platform và các giải pháp Kaspersky Endpoint Detection and Response.
- Kaspersky Endpoint Agent như một phần của các giải pháp Detection and Response của Kaspersky.

  > Kaspersky đang chuyển tất cả tính năng Detection and Response sang hoạt động với tác nhân tích hợp của Kaspersky Endpoint Security thay vì Kaspersky Endpoint Agent. Kể từ phiên bản 12.1, ứng dụng sẽ hỗ trợ tất cả các giải pháp Detection and Response.

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

  > Kể từ Kaspersky Endpoint Security 12.0, bạn có thể chuyển từ Kaspersky Security for Windows Server sang Kaspersky Endpoint Security cho Windows và sử dụng cùng một giải pháp để bảo vệ máy trạm và máy chủ.

- 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.

Việc bỏ qua kiểm tra phần mềm có thể gây ra sự cố tương thích

Nếu Kaspersky Endpoint Security phát hiện phần mềm trong danh sách incompatible.txt, quá trình cài đặt ứng dụng sẽ bị chấm dứt. Để tiếp tục cài đặt, bạn phải gỡ bỏ ứng dụng đó. Tuy nhiên, nếu nhà cung cấp phần mềm bên thứ ba đã nêu trong tài liệu của họ rằng phần mềm của họ tương thích với Endpoint Protection Platform (EPP), bạn có thể cài đặt Kaspersky Endpoint Security vào máy tính có ứng dụng từ nhà cung cấp này. Ví dụ: nhà cung cấp giải pháp Endpoint Detection and Response (EDR) có thể tuyên bố khả năng tương thích của họ với các hệ thống EPP của bên thứ ba. Nếu đúng như vậy, bạn cần tiến hành cài đặt Kaspersky Endpoint Security mà không cần chạy kiểm tra phần mềm đã cài đặt. Để làm như vậy, hãy truyền các tham số sau vào trình cài đặt:

- `SKIPPRODUCTCHECK=1` Tắt kiểm tra phần mềm đã cài đặt. Danh sách phần mềm có thể gây ra sự cố tương thích có trong tập tin incompatible.txt có trong gói phân phối. Nếu không có giá trị nào được đặt cho tham số này và phần mềm trong danh sách được phát hiện thì quá trình cài đặt Kaspersky Endpoint Security sẽ bị chấm dứt.

- `SKIPPRODUCTUNINSTALL=1` Tắt tính năng tự động gỡ bỏ phần mềm được phát hiện khỏi danh sách incompatible.txt. Nếu không có giá trị nào được đặt cho tham số này, Kaspersky Endpoint Security sẽ cố gắng gỡ bỏ phần mềm có thể gây ra sự cố tương thích.

- `CLEANERSIGNCHECK=0` Tắt xác minh chữ ký số của các ứng dụng được tìm thấy thông qua kiểm tra. Nếu tham số này không được đặt, xác minh chữ ký số sẽ bị tắt khi triển khai ứng dụng thông qua Kaspersky Security Center. Khi ứng dụng được cài đặt cục bộ, xác minh chữ ký số được bật theo mặc định.

Bạn có thể truyền các tham số trong dòng lệnh khi cài đặt ứng dụng cục bộ.

Nếu trong quá trình cài đặt bạn bỏ qua bước quét các phần mềm có thể gây ra vấn đề tương thích, Kaspersky Endpoint Security có thể thực hiện lại bước kiểm tra này khi các thành phần ứng dụng thay đổi. Để bỏ qua quá trình quét phần mềm đã cài đặt, bạn cần cấu hình tác vụ *Thay đổi thành phần ứng dụng*.

Ví dụ:
```
C:\KES\setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0 /s
```

Để cài đặt Kaspersky Endpoint Security từ xa, bạn cần thêm các tham số thích hợp vào tập tin tạo gói cài đặt có tên `kes_win.kud` trong `[Setup]` (xem bên dưới). Các tập tin `kes_win.kud` được kèm theo gói phân phối.

kes_win.kud
```
[Setup]
UseWrapper=1
ExecutableRelPath=EXEC
Params=/s /pAKINSTALL=1 /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0
Executable=setup_kes.exe
RebootDelegated = 1
RebootAllowed=1
ConfigFile=installer.ini
RelPathsToExclude=klcfginst.msi
```

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.
4. Các thiết lập nhận được từ tập tin cấu hình (install.cfg).

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).

Khi cài đặt Kaspersky Endpoint Security, hệ điều hành có thể hiển thị thông báo riêng. Kết nối mạng và Internet cũng có thể bị gián đoạn khi ứng dụng đang được cài đặt.

Lỗi có thể xảy ra khi cài đặt, cập nhật hoặc gỡ bỏ Kaspersky Endpoint Security. Để biết thêm thông tin về cách xử lý các lỗi này, vui lòng tham khảo Cơ sở tri thức hỗ trợ kỹ thuật.

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. Trước khi cài đặt ứng dụng, bạn phải đảm bảo rằng Kaspersky Security Center Network Agent đã được cài đặt trên máy tính. *Network Agent* giúp xúc tiến tương tác giữa Máy chủ quản trị và một máy khách.

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.

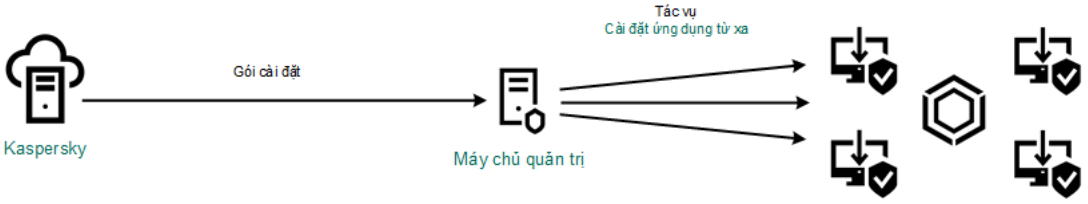
Bản cài đặt tiêu chuẩn của ứng dụng

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 *Install application remotely* thuộc Máy chủ quản trị Kaspersky Security Center.



Triển khai Kaspersky Endpoint Security

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

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Advanced → Remote installation**.
3. 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 nguồn gói cài đặt

Chọn nguồn **Deploy Kaspersky Security Center package**.

Bước 3. 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 4. 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**. Network Agent chịu trách nhiệm phân phối gói cài đặt Kaspersky Endpoint Security đến các máy tính khách. Nếu Network Agent không được cài đặt, tác vụ sẽ kết thúc với một lỗi. Trong trường hợp này, hãy thêm gói cài đặt Network Agent vào tác vụ *Install application remotely* và bật tính năng phân phối tập tin thông qua tài nguyên hệ điều hành. Khi đó, Network Agent sẽ được cài đặt bằng cách sử dụng tài nguyên 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 5. 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 bằng cách sử dụng tác vụ *Add key*.

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. 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 9. Bắt đầu quá trình cài đặt

Hoàn tất 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 bằng cách sử dụng tác vụ *Add key*.

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**. Network Agent chịu trách nhiệm phân phối gói cài đặt Kaspersky Endpoint Security đến các máy tính khách. Nếu Network Agent không được cài đặt, tác vụ sẽ kết thúc với một lỗi. Trong trường hợp này, hãy thêm gói cài đặt Network Agent vào tác vụ *Install application remotely* và bật tính năng phân phối tập tin thông qua tài nguyên hệ điều hành. Khi đó, Network Agent sẽ được cài đặt bằng cách sử dụng tài nguyên 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

Hoàn tất 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** → **Advanced** → **Remote installation** → **Installation packages**.

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

2. Nhấn vào **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 14.2*.

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 của gói cài đặt, bạn có thể chọn các thành phần ứng dụng cho các loại hệ điều hành khác nhau. Tức là gói cài đặt bao gồm hai nhóm thành phần: dành cho máy trạm và dành cho máy chủ. Trước khi triển khai gói cài đặt, trình cài đặt sẽ phát hiện loại hệ điều hành và chỉ cài đặt những thành phần ứng dụng mà bạn đã chọn cho loại hệ điều hành đó. Theo đó, bạn có thể sử dụng cùng một gói cài đặt cho máy trạm và máy chủ.

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.

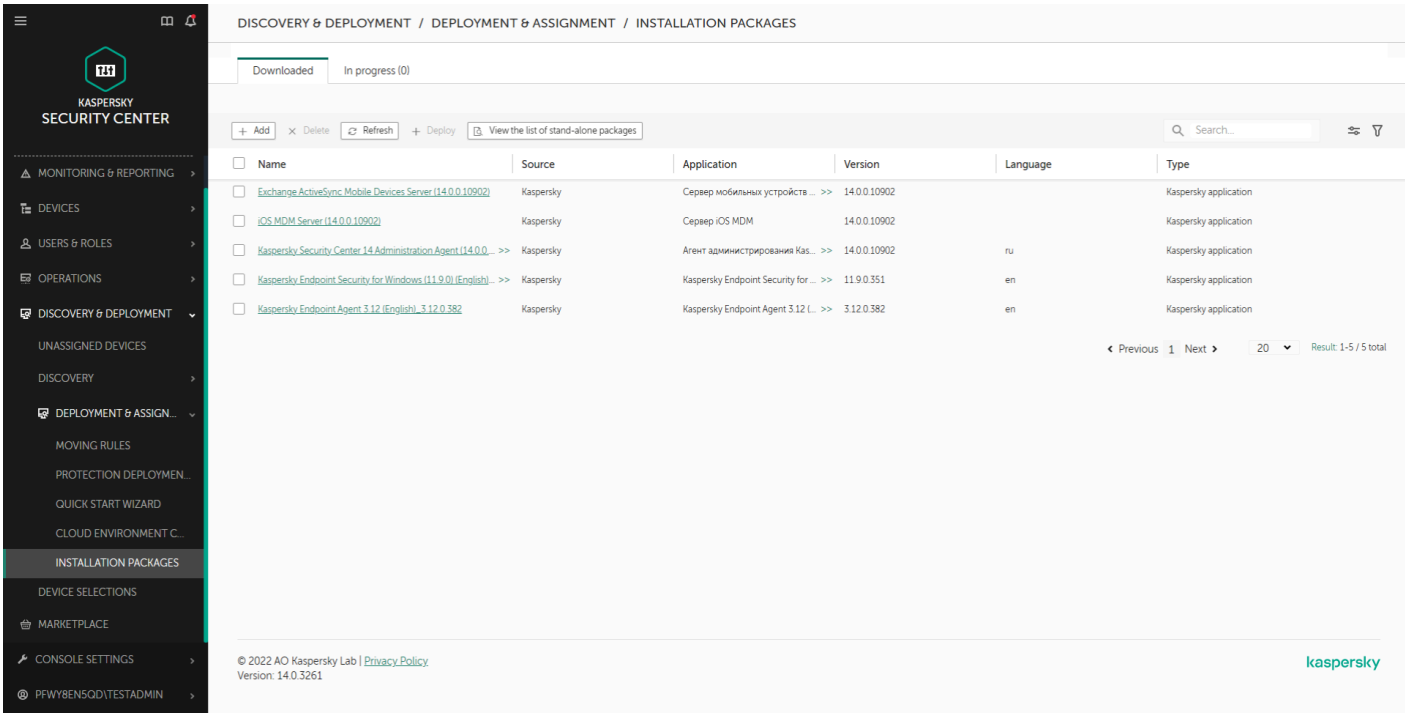
Cách tạo gói cài đặt trong Bảng điều khiển web

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 **Add**.

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



Danh sách gói cài đặt

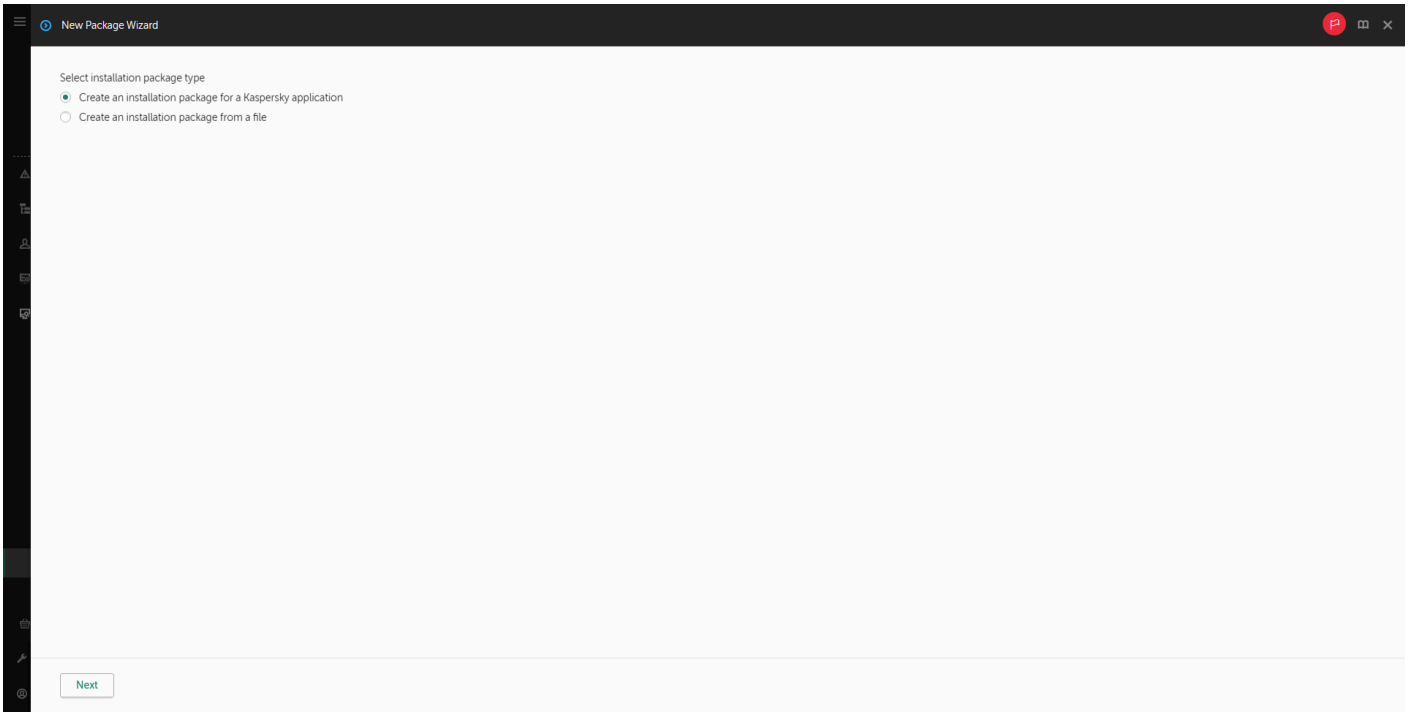
Bước 1. Chọn loại gói cài đặt

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.

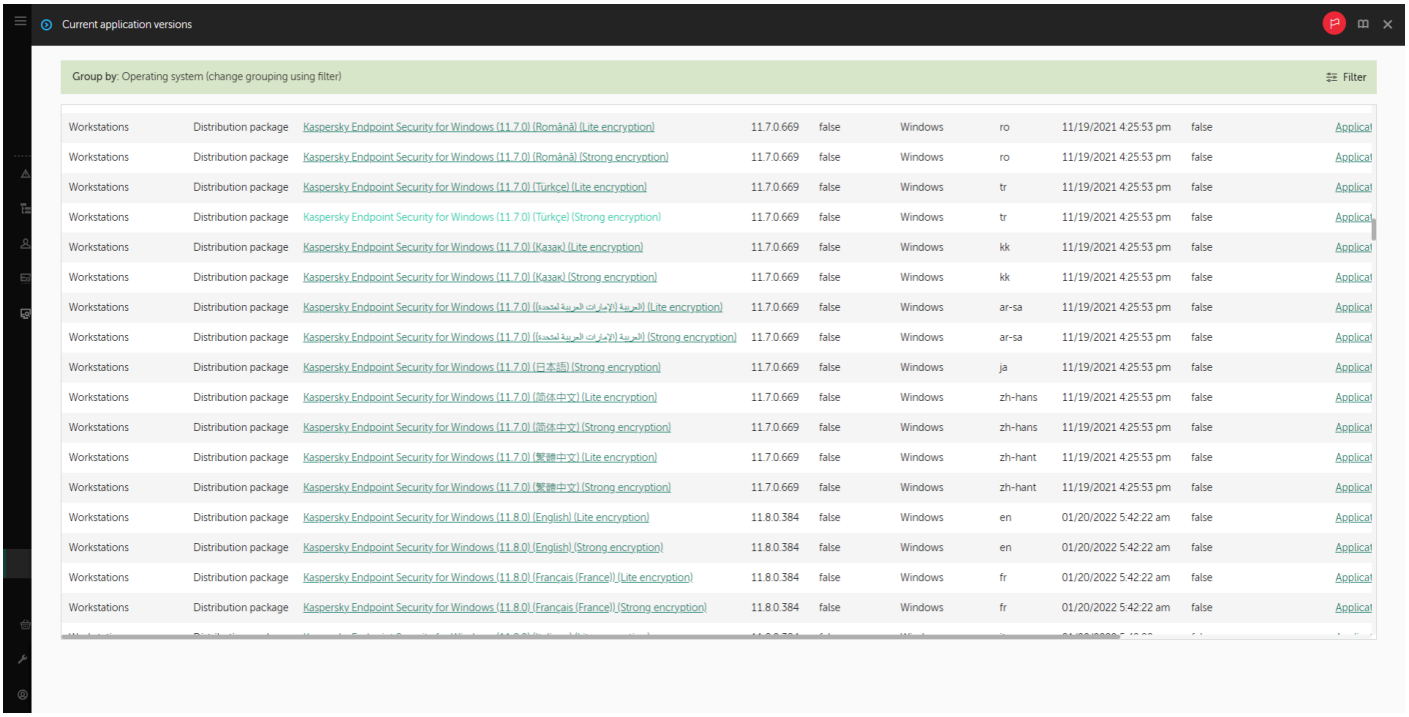
Tính năng tạo gói cài đặt Kaspersky Endpoint Security từ tập tin chỉ khả dụng trong Bảng điều khiển web Kaspersky Security Center.



Các loại gói cài đặt

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.

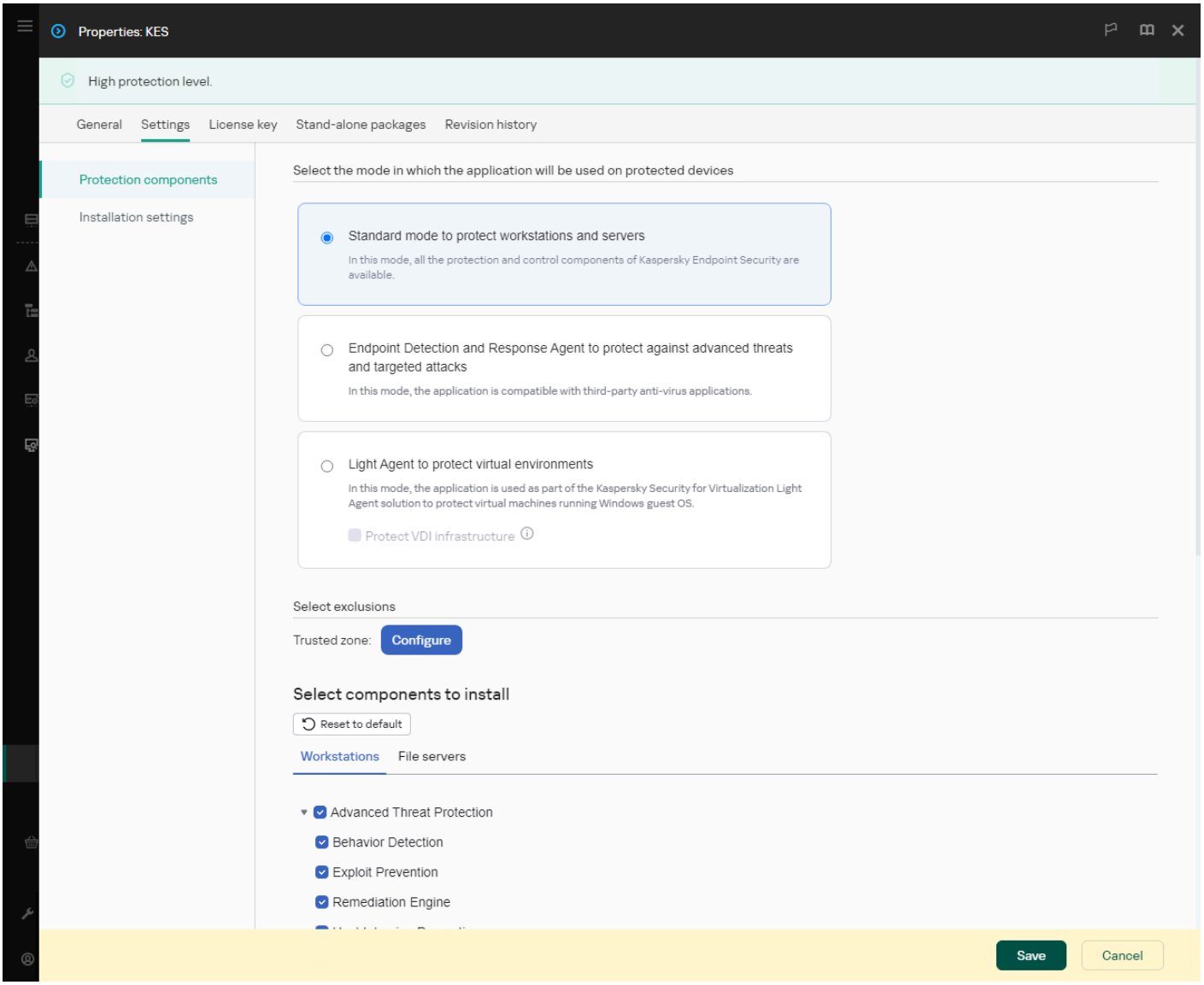


Danh sách gói cài đặt trên máy chủ Kaspersky

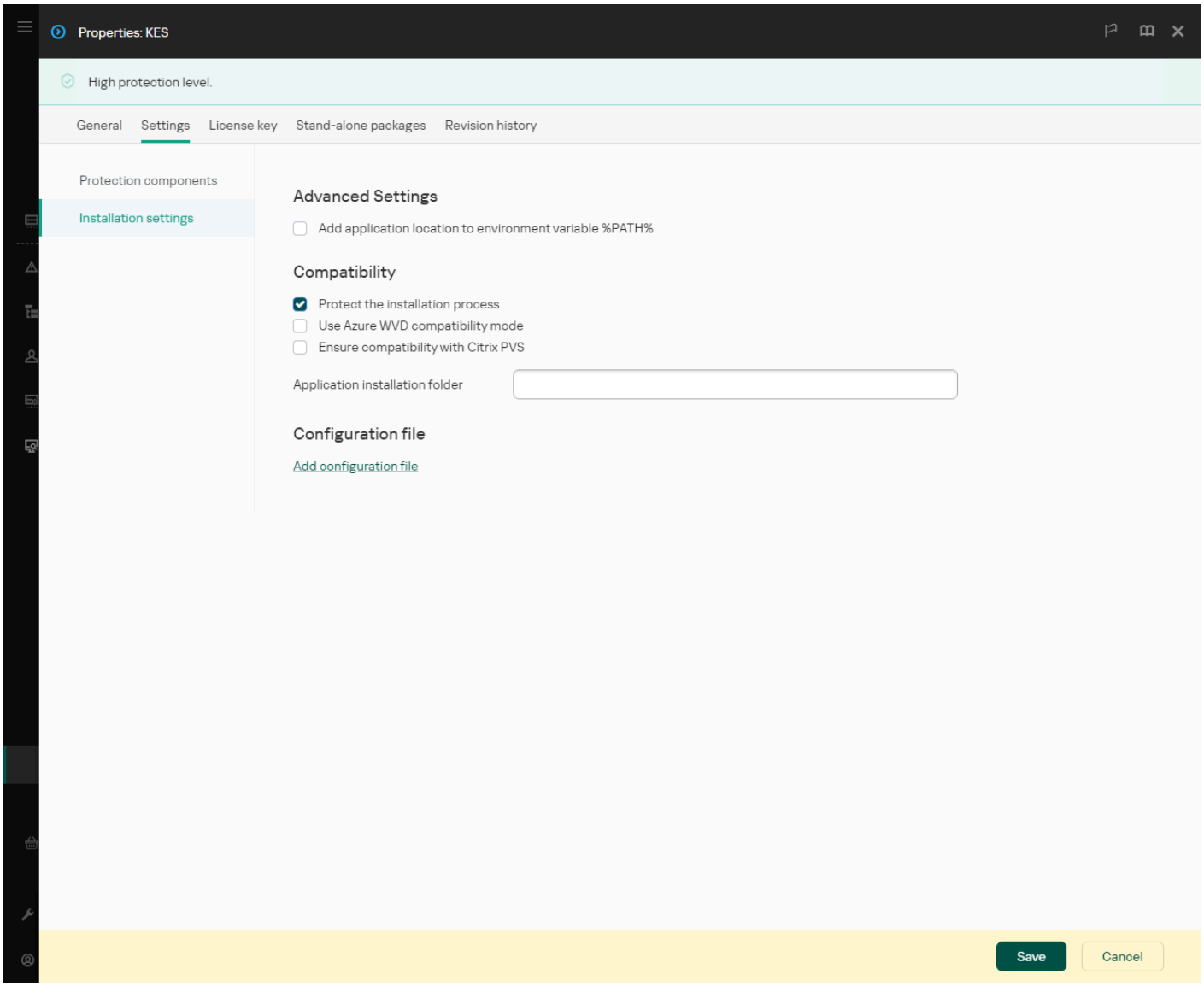
Gói cài đặt sẽ được tạo và được thêm vào Kaspersky Security Center. Sử dụng gói cài đặt, bạn có thể cài đặt Kaspersky Endpoint Security trên các máy tính mạng doanh nghiệp hoặc cập nhật phiên bản ứng dụng.

Trong thiết lập của gói cài đặt, bạn có thể chọn các thành phần ứng dụng cho các loại hệ điều hành khác nhau. Tức là gói cài đặt bao gồm hai nhóm thành phần: dành cho máy trạm và dành cho máy chủ. Trước khi triển khai gói cài đặt, trình cài đặt sẽ phát hiện loại hệ điều hành và chỉ cài đặt những thành phần ứng dụng mà bạn đã chọn cho loại hệ điều hành đó. Theo đó, bạn có thể sử dụng cùng một gói cài đặt cho máy trạm và máy chủ.

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.



Các thành phần có trong gói cài đặt



Thiết lập cài đặt của gói cài đặt

Cấu hình gói cài đặt

Phần	Mô tả
Thành phần bảo vệ	**Chế độ tiêu chuẩn**. Cấu hình mặc định. Cấu hình này cho phép bạn sử dụng tất cả các thành phần của ứng dụng, bao gồm các thành phần cung cấp hỗ trợ cho các giải pháp Detection and Response. Cấu hình này được sử dụng để bảo vệ máy tính toàn diện trước nhiều mối đe dọa, tấn công mạng và gian lận. **Endpoint Detection and Response Agent**. Trong cấu hình này, bạn chỉ có thể cài đặt các thành phần hỗ trợ các giải pháp Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), cũng như KUMA. Đây là cấu hình cần thiết nếu Endpoint Protection Platform (EPP) của bên thứ ba được triển khai trong tổ chức của bạn cùng với giải pháp Kaspersky Detection and Response. Điều này làm cho Kaspersky Endpoint Security trong cấu hình Endpoint Detection and Response Agent tương thích với các ứng dụng EPP của bên thứ ba. **Light Agent để bảo vệ môi trường ảo**. Cấu hình này được dành cho ứng dụng được sử dụng như một phần của giải pháp Kaspersky Security for Virtualization Light Agent. Phải cài đặt Light Agent trên mỗi máy ảo cần được bảo vệ bằng giải pháp này. Trong cấu hình này, bạn không thể sử dụng các thành phần các thành phần Mã hóa dữ liệu hoặc Kiểm soát thích ứng sự cố. Nếu bạn đang cài đặt Light Agent trên một mẫu máy ảo sẽ được sử dụng để tạo *máy ảo không lưu các thay đổi*, hãy chọn hộp kiểm **Bảo vệ hạ tầng VDI** (VDI chữ là viết tắt của Virtual Desktop Infrastructure). Chế độ bảo vệ VDI giúp tối ưu hóa hiệu năng của Kaspersky Endpoint Security trên các máy ảo không lưu các thay đổi. Ở chế độ này, Light Agent từ chối các bản cập nhật ứng dụng đòi hỏi khởi động lại máy ảo. Khi nhận được các bản cập nhật ứng dụng yêu cầu khởi động lại, Light Agent sẽ tạo một sự kiện về việc cần cập nhật mẫu của các máy ảo được bảo vệ.

Phần	Mô tả
Loại trừ	Kể từ Kaspersky Endpoint Security 12.6 cho Windows, loại trừ quét và ứng dụng được tin tưởng được thêm vào khu vực tin tưởng. Các ứng dụng được tin tưởng và loại trừ quét được xác định trước giúp nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager. Điều này có nghĩa là bạn không cần thiết lập khu vực tin tưởng theo cách thủ công cho ứng dụng trên máy chủ. Kể từ Kaspersky Endpoint Security 12.8 cho Windows, bạn có thể cài đặt ứng dụng ở chế độ Light Agent để bảo vệ môi trường ảo. Các loại trừ quét được định sẵn và các ứng dụng được tin tưởng có thể giúp bạn nhanh chóng cấu hình Kaspersky Endpoint Security trong các môi trường máy ảo Citrix và VMware. Bạn cũng có thể cấu hình khu vực tin tưởng sau trong thuộc tính chính sách: loại trừ quét và ứng dụng được tin tưởng.
Lựa chọn thành phần để cài đặt	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 *Thay đổi thành phần ứng dụng* task. Bạn có thể tạo các nhóm thành phần riêng biệt cho máy trạm và máy chủ. Trước khi triển khai gói cài đặt, trình cài đặt sẽ phát hiện loại hệ điều hành và chỉ cài đặt những thành phần ứng dụng mà bạn đã chọn cho loại hệ điều hành đó. Theo đó, bạn có thể sử dụng cùng một gói cài đặt cho máy trạm và máy chủ. Tập hợp các thành phần khả dụng sẽ tùy thuộc vào cấu hình của ứng dụng: **Chế độ tiêu chuẩn** Kaspersky Data Encryption, Mã hóa mức độ tập tin và tất cả các tác nhân tích hợp sẵn, ngoại trừ EDR Optimum, đều không được cài đặt theo mặc định. Bạn có thể thêm các thành phần này trong thiết lập gói cài đặt. **Endpoint Detection and Response Agent** Trong cấu hình này, chỉ có các tác nhân tích hợp cho giải pháp Kaspersky Detection and Response mới khả dụng. **Light Agent để bảo vệ môi trường ảo** Trong cấu hình này, bạn có thể sử dụng hầu hết các thành phần ứng dụng có sẵn trong cấu hình **Chế độ tiêu chuẩn**, ngoại trừ các thành phần mã hóa dữ liệu và Kiểm soát thích ứng sự cố.
License key	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.
Incompatible applications	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.
Installation settings	**Thêm đường dẫn vào tập tin avp.com với biến hệ thống %PATH%**. Bạn có thể thêm đường dẫn cài đặt vào biến số %PATH% để tiện sử dụng giao diện dòng lệnh. **Protect the installation process**. 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 khả năng tương thích với Citrix PVS**. Bạn có thể bật hỗ trợ Citrix Provisioning Services để cài đặt Kaspersky Endpoint Security lên một máy tính ảo. **Sử dụng chế độ tương thích Azure WVD**. Tính năng này đảm bảo hiển thị chính xác trạng thái máy ảo Azure trong bảng điều khiển Kaspersky Anti Targeted Attack Platform. Để theo dõi hiệu năng của máy tính, Kaspersky Endpoint Security sẽ gửi thông tin đo từ xa đến các máy chủ KATA. Thông tin đo từ xa chứa một ID của máy tính (Sensor ID). Chế độ tương thích Azure WVD cho phép gán Sensor ID duy nhất vĩnh viễn cho các máy ảo này. Nếu chế độ tương thích bị tắt thì Sensor ID có thể thay đổi sau khi máy tính được khởi động lại do cách máy ảo Azure hoạt động. Điều này có thể khiến các máy ảo trùng lặp xuất hiện trên bảng điều khiển. **Application installation folder**. 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(x86)%\Kaspersky Lab\KES.14.2.` **Configuration file**. Cài đặt ứng dụng bằng các thiết lập được định sẵn. Để thực hiện, bạn cần tải lên một tập tin định nghĩa thiết lập của Kaspersky Endpoint Security. Bạn có thể tạo một tập tin cấu hình trong giao diện cục bộ của ứng dụng. Trình hướng dẫn gói mới không hỗ trợ các tập tin cấu hình được mã hóa. Khi xuất tập tin cấu hình, hãy bỏ qua bước mã hóa tập tin.

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 *Download updates to the Administration Server repository* 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. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn thư mục **Advanced** → **Remote installation** → **Installation packages**.

   Thao tác này sẽ mở danh sách các gói cài đặt đã được tải về Kaspersky Security Center.
3. Mở thuộc tính của gói cài đặt.
4. Trong mục **General**, hãy nhấn **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 *Install application remotely* được thiết kế để cài đặt Kaspersky Endpoint Security từ xa. Tác vụ *Install application remotely* 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. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Tasks**.
   Danh sách tác vụ sẽ mở.
3. Nhấn vào **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**. Network Agent chịu trách nhiệm phân phối gói cài đặt Kaspersky Endpoint Security đến các máy tính khách. Nếu Network Agent không được cài đặt, tác vụ sẽ kết thúc với một lỗi. Trong trường hợp này, hãy thêm gói cài đặt Network Agent vào tác vụ *Install application remotely* và bật tính năng phân phối tập tin thông qua tài nguyên hệ điều hành. Khi đó, Network Agent sẽ được cài đặt bằng cách sử dụng tài nguyên 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 14.2*.

Bước 10. Hoàn thành tạo tác vụ

Hoàn tất 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 **Asset management** → **Tasks**.
   Danh sách tác vụ sẽ mở.
2. Nhấn vào **Add**.

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 **Application**, hãy chọn **Kaspersky Security Center**.
2. Trong danh sách thả xuống **Task type**, hãy 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 **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 (14.2).
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**. Network Agent chịu trách nhiệm phân phối gói cài đặt Kaspersky Endpoint Security đến các máy tính khách. Nếu Network Agent không được cài đặt, tác vụ sẽ kết thúc với một lỗi. Trong trường hợp này, hãy thêm gói cài đặt Network Agent vào tác vụ *Install application remotely* và bật tính năng phân phối tập tin thông qua tài nguyên hệ điều hành. Khi đó, Network Agent sẽ được cài đặt bằng cách sử dụng tài nguyên 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, hãy 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, hãy 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 **Finish**. 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 **Start**. 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.

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. Đảm bảo rằng tài khoản người dùng mà bạn đang sử dụng để chạy Trình hướng dẫn thiết lập nằm trong nhóm quản trị viên.

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.

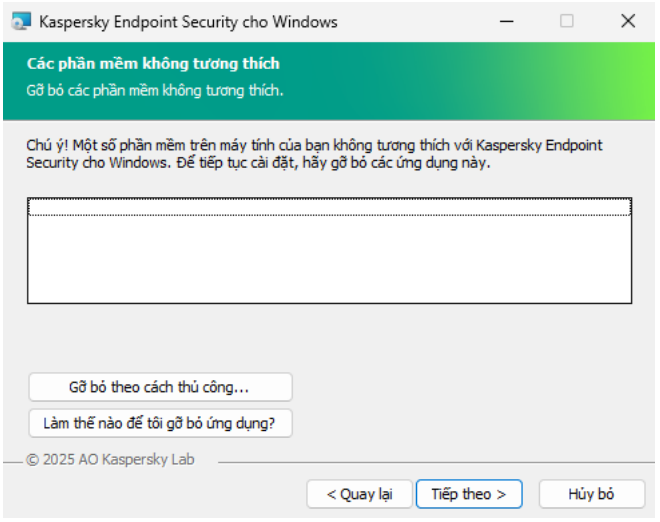
   Trình hướng dẫn cài đặt sẽ được bắt đầu.

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:

- Liệu có phần mềm nào đã được cài đặt có thể gây ra vấn đề tương thích với Kaspersky Endpoint Security hay không (danh sách phần mềm có trong tập tin incompatible.txt đi kèm gói phân phối).
- Liệu các yêu cầu về phần cứng và phần mềm có được đáp ứng hay không.
- Liệu Microsoft .NET Framework đã được cài đặt hay chưa.
- 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. Ví dụ: một thông báo về phần mềm không tương thích (xem hình bên dưới).



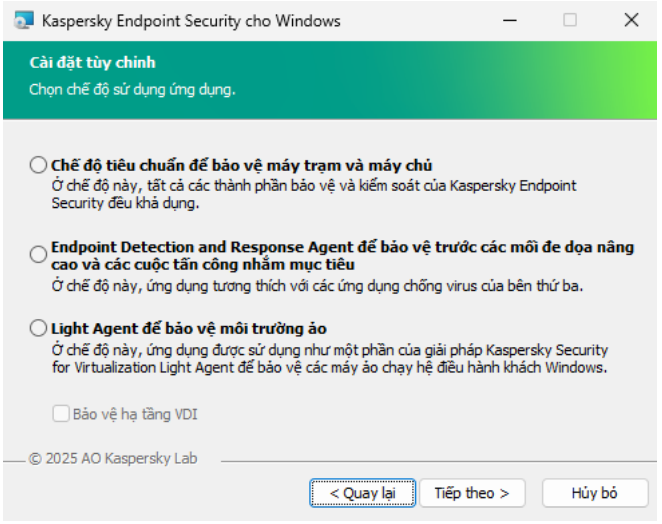
Gỡ bỏ các phần mềm không tương thích

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 14.2 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 12.3 cho Windows (bản dựng 12.3.0.493)
- Kaspersky Endpoint Security 12.4 cho Windows (bản dựng 12.4.0.467)
- Kaspersky Endpoint Security 12.5 cho Windows (bản dựng 12.5.0.539)
- Kaspersky Endpoint Security 12.6 cho Windows (bản dựng 12.6.0.438)
- Kaspersky Endpoint Security 12.7 cho Windows (bản dựng 12.7.0.533)
- Kaspersky Endpoint Security 12.8 cho Windows (bản dựng 12.8.0.505)
- Kaspersky Endpoint Security 12.9 cho Windows (bản dựng 12.9.0.384)
- Kaspersky Endpoint Security 12.10 cho Windows (bản dựng 12.10.0.466)
- Kaspersky Endpoint Security 12.11 cho Windows (bản dựng 12.11.0.637)
- Kaspersky Endpoint Security 12.12 cho Windows (bản dựng 12.12.0.522)
- Kaspersky Endpoint Security 14.0 cho Windows (bản dựng 14.0.0.504)
- Kaspersky Endpoint Security 14.1 cho Windows (bản dựng 14.1.0.423)

Cấu hình của Kaspersky Endpoint Security



Lựa chọn cấu hình ứng dụng

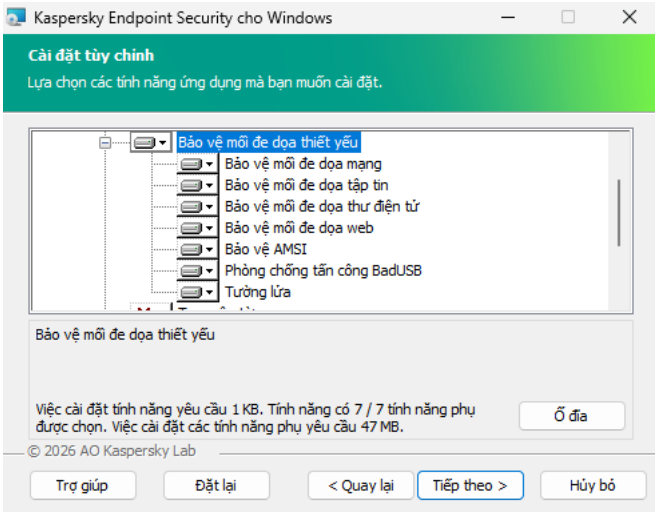
Chế độ tiêu chuẩn. Cấu hình mặc định. Cấu hình này cho phép bạn sử dụng tất cả các thành phần của ứng dụng, bao gồm các thành phần cung cấp hỗ trợ cho các giải pháp Detection and Response. Cấu hình này được sử dụng để bảo vệ máy tính toàn diện trước nhiều mối đe dọa, tấn công mạng và gian lận.

Endpoint Detection and Response Agent. Trong cấu hình này, bạn chỉ có thể cài đặt các thành phần hỗ trợ các giải pháp Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), cũng như KUMA. Đây là cấu hình cần thiết nếu Endpoint Protection Platform (EPP) của bên thứ ba được triển khai trong tổ chức của bạn cùng với giải pháp Kaspersky Detection and Response. Điều này làm cho Kaspersky Endpoint Security trong cấu hình Endpoint Detection and Response Agent tương thích với các ứng dụng EPP của bên thứ ba.

Light Agent để bảo vệ môi trường ảo. Cấu hình này được dành cho ứng dụng được sử dụng như một phần của giải pháp Kaspersky Security for Virtualization Light Agent. Phải cài đặt Light Agent trên mỗi máy ảo cần được bảo vệ bằng giải pháp này. Trong cấu hình này, bạn không thể sử dụng các thành phần các thành phần Mã hóa dữ liệu hoặc Kiểm soát thích ứng sự cố. Nếu bạn đang cài đặt Light Agent trên một mẫu máy ảo sẽ được sử dụng để tạo *máy ảo không lưu các thay đổi*, hãy chọn hộp kiểm **Bảo vệ hạ tầng VDI** (VDI chữ là viết tắt của Virtual Desktop Infrastructure). Chế độ bảo vệ VDI giúp tối ưu hóa hiệu năng của Kaspersky Endpoint Security trên các máy ảo không lưu các thay đổi. Ở chế độ này, Light Agent từ chối các bản cập nhật ứng dụng đòi hỏi khởi động lại máy ảo. Khi nhận được các bản cập nhật ứng dụng yêu cầu khởi động lại, Light Agent sẽ tạo một sự kiện về việc cần cập nhật mẫu của các máy ảo được bảo vệ.

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 (xem hình bên dưới). 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.



Lựa chọn các thành phần ứng dụng để cài đặt

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

- Kaspersky Disk Encryption
- Mã hóa mức độ tập tin
- Endpoint Detection and Response Expert (on-premises)
- Endpoint Detection and Response Expert (cloud)
- Sandbox
- Managed Detection and Response
- Network Detection and Response (KATA)
- Tích hợp với KUMA

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 áp dụng cho Endpoint Detection and Response Optimum
- Chỉ áp dụng cho Endpoint Detection and Response Expert (cloud)
- Chỉ áp dụng cho Endpoint Detection and Response Expert (on-premises)
- Chỉ áp dụng cho Network Detection and Response (KATA)

- Chỉ áp dụng cho Sandbox
- Endpoint Detection and Response Optimum và Sandbox
- Endpoint Detection and Response Expert (cloud) và Sandbox
- Endpoint Detection and Response Expert (on-premises) và Sandbox
- Network Detection and Response (KATA) và Endpoint Detection and Response Expert (on-premises)
- Network Detection and Response (KATA) và Managed Detection and Response

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.

Chọn thư mục để cài đặt ứng dụng

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(x86)%\Kaspersky Lab\KES.14.2.`

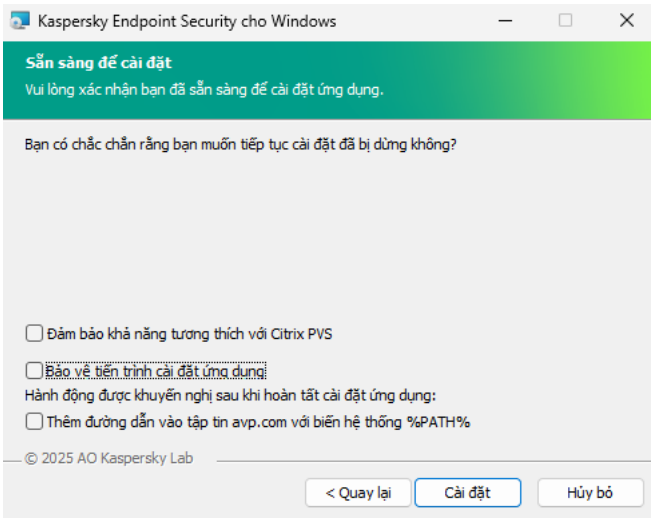
Cấu hình khu vực tin tưởng

Kể từ Kaspersky Endpoint Security 12.6 cho Windows, loại trừ quét và ứng dụng được tin tưởng được thêm vào khu vực tin tưởng. Các ứng dụng được tin tưởng và loại trừ quét được xác định trước giúp nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager. Điều này có nghĩa là bạn không cần thiết lập khu vực tin tưởng theo cách thủ công cho ứng dụng trên máy chủ.

Kể từ Kaspersky Endpoint Security 12.8 cho Windows, bạn có thể cài đặt ứng dụng ở chế độ Light Agent để bảo vệ môi trường ảo. Các loại trừ quét được định sẵn và các ứng dụng được tin tưởng có thể giúp bạn nhanh chóng cấu hình Kaspersky Endpoint Security trong các môi trường máy ảo Citrix và VMware.

Bạn cũng có thể cấu hình khu vực tin tưởng sau trong thuộc tính chính sách: loại trừ quét và ứng dụng được tin tưởng.

Thiết lập nâng cao



Thiết lập cài đặt ứng dụng 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 khả năng tương thích với Citrix PVS. Bạn có thể bật hỗ trợ Citrix Provisioning Services để cài đặt Kaspersky Endpoint Security lên một máy tính ảo.

Thêm đường dẫn vào tập tin avp.com với biến hệ thống %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

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

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.

Chỉ sử dụng tập tin setup.ini khi cài đặt ứng dụng trong chế độ im lặng.

Bạn không thể thêm đường dẫn vào tập tin cấu hình install.cfg trong tập tin setup.ini. Ứng dụng cũng bỏ qua tập tin cấu hình install.cfg nếu tập tin đó được đặt trong cùng thư mục với gói phân phối Kaspersky Endpoint Security. Để áp dụng thiết lập từ tập tin cấu hình install.cfg, bạn cần chỉ định đường dẫn đến tập tin trong lệnh cài đặt ứng dụng sau: `CONFIGPATH=<path to the configuration file>`.

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 ở chế độ Tiêu chuẩn. 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.
- `[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`, `enabled`, và `true`. Các giá trị thay thế cho `0` là các giá trị `no`, `off`, `disable`, `disabled`, và `false`.

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.

Phần	Tham số	Mô tả
	`Eula`	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. Việc chấp nhận các điều khoản của Thỏa thuận giấy phép người dùng cuối là cần thiết để cài đặt ứng dụng hoặc nâng cấp phiên bản ứng dụng.
	`PrivacyPolicy`	Chấp nhận Chính sách quyền riêng tư. Văn bản của Chính sách quyền riêng tư được bao gồm trong gói phân phối của Kaspersky Endpoint Security. Để cài đặt ứng dụng hoặc nâng cấp ứng dụng phiên bản ứng dụng, bạn phải chấp nhận Chính sách quyền riêng tư.
	`KSN`	Đồng ý hoặc từ chối tham gia Kaspersky Security Network (KSN). Nếu không có giá trị nào được thiết lập cho tham số này, Kaspersky Endpoint Security sẽ nhắc bạn xác nhận sự đồng ý hoặc từ chối tham gia KSN khi Kaspersky Endpoint Security được khởi động lần đầu. Giá trị khả dụng: • `1` – đồng ý tham gia KSN. • `0` – từ chối tham gia KSN (giá trị mặc định). Gói phân phối Kaspersky Endpoint Security được tối ưu cho việc sử dụng với Kaspersky Security Network. Nếu bạn không chọn tham gia Kaspersky Security Network, bạn nên cập nhật Kaspersky Endpoint Security ngay sau khi hoàn tất cài đặt.
	`CLEANERSIGNCHECK`	Xác minh chữ ký số của các tập tin phần mềm được phát hiện từ danh sách incompatible.txt. Để gỡ bỏ phần mềm, Kaspersky Endpoint Security sẽ chạy tập tin cài đặt phần mềm. Nếu tập tin bộ cài đặt không có chữ ký số thì Kaspersky Endpoint Security sẽ coi tập tin đó là không được tin tưởng và sẽ tạm dừng việc gỡ bỏ phần mềm để tránh chạy mã độc hại tiềm ẩn. Nếu ứng dụng không thể xác minh chữ ký số của tập tin phần mềm được phát hiện thì quá trình cài đặt Kaspersky Endpoint Security sẽ bị dừng kèm một lỗi. Giá trị mặc định sẽ khác nhau, tùy thuộc vào phương thức cài đặt phần mềm: • `0` có nghĩa là khâu xác minh chữ ký số bị tắt (giá trị mặc định nếu được triển khai thông qua Kaspersky Security Center). • `1` có nghĩa là khâu xác minh chữ ký số được bật (giá trị mặc định nếu ứng dụng đang được cài đặt cục bộ).
	`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 KLAdmin được sử dụng theo mặc định.
	`Password`	Quy định một mật khẩu để truy cập các tính năng và cấu hình của Kaspersky Endpoint Security (mật khẩu được quy định cùng với các tham số `Login` và `PasswordArea`). Nếu bạn quy định một mật khẩu nhưng không quy định tên người dùng với tham số `Login`, tên người dùng mặc định KLAdmin sẽ được sử dụng.
	`PasswordArea`	Quy định phạm vi của mật khẩu để truy cập Kaspersky Endpoint Security. Khi người dùng cố gắng thực hiện một hành động có trong phạm vi này, Kaspersky Endpoint Security sẽ hỏi thông tin tài khoản của người dùng (các tham số `Login` và `Password`). Sử dụng ký tự `;` để nhập nhiều giá trị. Giá trị khả dụng: • `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. • `EXPORT` – xuất thiết lập ứng dụng. Ví dụ: `PasswordArea=SET;PasswordArea=UNINST;PasswordArea=EXIT`.

Phần	Tham số	Mô tả
	`SelfProtection`	Bật hoặc tắt cơ cấu bảo vệ cài đặt ứng dụng. Giá trị khả dụng: • `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. 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.
	`PROTECTOSSERVICES`	Bảo vệ chức năng của dịch vụ hệ điều hành. Tính năng bảo vệ dịch vụ hệ điều hành sẽ ngăn các ứng dụng của bên thứ ba can thiệp vào hoạt động của các dịch vụ hệ điều hành. Ví dụ: các dịch vụ đó bao gồm dịch vụ tự động khởi chạy ứng dụng. • `1` có nghĩa là tính năng bảo vệ dịch vụ hệ điều hành được bật (giá trị mặc định). • `0` có nghĩa là tính năng bảo vệ dịch vụ hệ điều hành bị tắt.
	`EnableAzureSupport`	Bật hoặc tắt chế độ tương thích Azure WVD. Giá trị khả dụng: • `1` – Chế độ tương thích Azure WVD được bật. • `0` – Chế độ tương thích Azure WVD bị tắt (giá trị mặc định). Tính năng này đảm bảo hiển thị chính xác trạng thái máy ảo Azure trong bảng điều khiển Kaspersky Anti Targeted Attack Platform. Để theo dõi hiệu năng của máy tính, Kaspersky Endpoint Security sẽ gửi thông tin đo từ xa đến các máy chủ KATA. Thông tin đo từ xa chứa một ID của máy tính (Sensor ID). Chế độ tương thích Azure WVD cho phép gán Sensor ID duy nhất vĩnh viễn cho các máy ảo này. Nếu chế độ tương thích bị tắt thì Sensor ID có thể thay đổi sau khi máy tính được khởi động lại do cách máy ảo Azure hoạt động. Điều này có thể khiến các máy ảo trùng lặp xuất hiện trên bảng điều khiển.
	`Reboot`	Tự động khởi động lại máy tính nếu cần thiết sau khi cài đặt hoặc nâng cấp ứng dụng. Nếu không có giá trị nào được đặt cho tham số này thì việc tự động khởi động lại máy tính sẽ bị chặn. Không cần khởi động lại khi cài đặt Kaspersky Endpoint Security. Chỉ cần khởi động lại nếu bạn 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.
	`AddEnvironment`	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: • `1` – Biến hệ thống %PATH% sẽ được bổ sung đường dẫn đến các tập tin thực thi trong thư mục cài đặt Kaspersky Endpoint Security. • `0` – Biến hệ thống %PATH% sẽ không được bổ sung đường dẫn đến các tập tin thực thi trong thư mục cài đặt Kaspersky Endpoint Security.
	`AMPPL`	Bật hoặc tắt tính năng bảo vệ 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. Công nghệ AM-PPL có sẵn trên hệ điều hành Windows 10 phiên bản 1703 (RS2) hoặc mới hơn và Windows Server 2019. Giá trị khả dụng: • `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.

Phần	Tham số	Mô tả
	UPGRADEMODE	Chế độ nâng cấp ứng dụng: • Seamless nghĩa là nâng cấp ứng dụng bằng cách khởi động lại máy tính (giá trị mặc định). • Force có nghĩa là nâng cấp ứng dụng mà không cần khởi động lại. Bạn có thể nâng cấp ứng dụng mà không cần khởi động lại kể từ phiên bản 11.10.0. Bạn phải khởi động lại máy tính để nâng cấp phiên bản cũ hơn của ứng dụng. Bạn cũng có thể cài đặt các bản vá mà không cần khởi động lại kể từ phiên bản 11.11.0. Không cần khởi động lại khi cài đặt Kaspersky Endpoint Security. Vì vậy, chế độ nâng cấp của ứng dụng sẽ được chỉ định trong thiết lập ứng dụng. Bạn có thể thay đổi tham số này trong thiết lập ứng dụng hoặc trong chính sách. Khi nâng cấp ứng dụng đã được cài đặt, mức ưu tiên của tham số được chỉ định trong tập tin setup.ini cao hơn mức ưu tiên của tham số được chỉ định trong thiết lập ứng dụng hoặc trong dòng lệnh. Ví dụ: nếu chế độ nâng cấp Force được chỉ định trong tập tin setup.ini và chế độ Seamless được chỉ định trong thiết lập ứng dụng thì bản nâng cấp sẽ được cài đặt mà không khởi động lại máy tính (Force). Nếu bạn đang sử dụng tập tin setup.ini trong đó tham số UPGRADEMODE không được chỉ định thì trình cài đặt sẽ sử dụng giá trị mặc định (Seamless) và sẽ cài đặt bản nâng cấp khi khởi động lại máy tính.
	SetupReg	Cho phép ghi các khóa registry từ tập tin setup.reg vào registry. SetupReg: setup.reg giá trị tham số.
	EnableTraces	Bật hoặc tắt truy vết 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.14.2\Traces. Giá trị khả dụng: • 1 – truy vết được bật. • 0 – truy vết bị tắt (giá trị mặc định).
	TracesLevel	Cấp chi tiết dấu vết. Giá trị khả dụng: • 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). • 600 (thấp). Tất cả các thông báo.
	RESTAPI	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). Giá trị khả dụng: • 1 - quản lý thông qua REST API được cho phép. • 0 - quản lý thông qua REST API bị chặn (giá trị mặc định). 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.
	RESTAPI_User	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>\<UserName> (ví dụ: RESTAPI_User=COMPANY\Administrator). Bạn chỉ có thể chọn một người dùng để làm việc với REST API. Thêm tên người dùng là điều kiện tiên quyết để quản lý ứng dụng thông qua REST API.
	RESTAPI_Port	Cổng được sử dụng để quản lý ứng dụng thông qua REST API. Cổng 6782 được sử dụng theo mặc định. Đảm bảo rằng cổng chưa được sử dụng.
	RESTAPI_Certificate	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.

Phần	Tham số	Mô tả
	`StandaloneMode`	Cài đặt ứng dụng ở chế độ Endpoint Detection and Response Agent (EDR Agent). *Endpoint Detection and Response Agent* là một ứng dụng được cài đặt trên các máy trạm và máy chủ riêng lẻ trong cơ sở hạ tầng CNTT của tổ chức để hỗ trợ các giải pháp Kaspersky Managed Detection and Response và Kaspersky Anti Targeted Attack Platform. EDR Agent tương thích với các ứng dụng EPP của bên thứ ba. Điều này cho phép bạn sử dụng các công cụ bảo mật cơ sở hạ tầng của bên thứ ba cùng với tính năng Detection and Response by Kaspersky. Để cài đặt EDR Agent, trong phần `[Components]`, hãy chọn thành phần `StandaloneKATA, StandaloneNDR` hoặc `StandaloneMDR`. EDR Agent không hỗ trợ các thành phần ứng dụng khác. Giá trị khả dụng: • `1` để cài đặt ứng dụng ở chế độ EDR Agent. • `0` để cài đặt ứng dụng ở chế độ Tiêu chuẩn (mặc định).
	`KSVLAMode`	Cài đặt ứng dụng ở chế độ Light Agent. Cấu hình này được dành cho ứng dụng được sử dụng như một phần của giải pháp Kaspersky Security for Virtualization Light Agent. Phải cài đặt Light Agent trên mỗi máy ảo cần được bảo vệ bằng giải pháp này. Giá trị khả dụng: • `1` để cài đặt ứng dụng ở chế độ Light Agent. • `0` để cài đặt ứng dụng ở chế độ Tiêu chuẩn (mặc định).
	`InstallOnVDI`	Bật chế độ bảo vệ VDI khi cài đặt ứng dụng ở chế độ Light Agent (`KSVLAMode=1`). Chế độ bảo vệ VDI giúp tối ưu hóa hiệu năng của Kaspersky Endpoint Security trên các máy ảo không lưu các thay đổi. Ở chế độ này, Light Agent từ chối các bản cập nhật ứng dụng đòi hỏi khởi động lại máy ảo. Khi nhận được các bản cập nhật ứng dụng yêu cầu khởi động lại, Light Agent sẽ tạo một sự kiện về việc cần cập nhật mẫu của các máy ảo được bảo vệ. Giá trị khả dụng: • `1` để bật chế độ bảo vệ VDI. • `0` để tắt chế độ bảo vệ VDI (mặc định).
	`KESExclusions`	Thêm loại trừ quét định sẵn và ứng dụng được tin tưởng khi cài đặt ứng dụng trên máy chủ. Các ứng dụng được tin tưởng và loại trừ quét được xác định trước giúp nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager. Ví dụ: các loại trừ quét được xác định trước cho máy chủ SQL bao gồm các tập tin cơ sở dữ liệu MDF và LDF. Điều này có nghĩa là bạn không cần thiết lập khu vực tin tưởng theo cách thủ công cho ứng dụng trên máy chủ. Giá trị khả dụng: • `1` bật các loại trừ quét được định sẵn và các ứng dụng được tin tưởng. • `0` tắt các loại trừ quét được định sẵn và các ứng dụng được tin tưởng.
	`LAExclusions`	Thêm loại trừ quét được định sẵn v ứng dụng được tin tưởng khi cài đặt ứng dụng trên máy ảo (chế độ Light Agent). Các loại trừ quét được định sẵn và các ứng dụng được tin tưởng có thể giúp bạn nhanh chóng cấu hình Kaspersky Endpoint Security trong các môi trường máy ảo Citrix và VMware. Giá trị khả dụng: • `1` bật các loại trừ quét được định sẵn và các ứng dụng được tin tưởng. • `0` tắt các loại trừ quét được định sẵn và các ứng dụng được tin tưởng.
	`EnableUniqueSensorID`	Tạo định danh máy tính duy nhất (Sensor ID) trong quá trình cài đặt hoặc cập nhật ứng dụng. Sensor ID được sử dụng trong giải pháp Kaspersky Anti Targeted Attack Platform để xác định các máy tính gửi dữ liệu từ xa đến máy chủ. Khi tạo Sensor ID, ứng dụng sẽ sử dụng một thuật toán có cân nhắc đến cấu hình của máy tính như số sê-ri của bo mạch chủ. Trong một số trường hợp, ví dụ như khi sử dụng ứng dụng trong môi trường ảo, Sensor ID có thể bị trùng lặp. Do đó, Kaspersky Anti Targeted Attack Platform không thể xác định được máy tính nào đã gửi dữ liệu từ xa. Để tạo một Sensor ID duy nhất, bạn cần đặt tham số `EnableUniqueSensorID=1`. Kết quả là ứng dụng sẽ sử dụng một thuật toán khác để tạo Sensor ID, thuật toán này sẽ cân nhắc đến các dữ liệu khác về máy tính. Làm vậy sẽ đảm bảo có một Sensor ID duy nhất. Theo mặc định, tham số này không được đặt. Ứng dụng kế thừa Sensor ID trong các trường hợp sau: • Cập nhật phiên bản của ứng dụng; • chuyển cấu hình [KES+KEA] sang cấu hình [KES+tác nhân tích hợp]. Là một phần của quá trình sửa ứng dụng, do đó trình cài đặt sẽ cố gắng kế thừa Sensor ID. Nếu không thể khôi phục Sensor ID, ứng dụng sẽ tạo ra một Sensor ID mới.

Phần	Tham số	Mô tả
	`CitrixCompatibility`	Bật hỗ trợ Citrix Provisioning Services để cài đặt Kaspersky Endpoint Security lên một máy tính ảo.
`[Components]`	`ALL`	Cài đặt tất cả các thành phần. Nếu giá trị tham số `1` được quy định, tất cả các thành phần sẽ được cài đặt bất kể cấu hình cài đặt của các thành phần riêng lẻ. Do cách thức hỗ trợ các giải pháp Detection and Response, các thành phần Endpoint Detection and Response Optimum và Sandbox được cài đặt trên máy tính. Thành phần Endpoint Detection and Response Expert (cloud) không tương thích với cấu hình này.
	`MailThreatProtection`	Bảo vệ mối đe dọa thư điện tử.
	`WebThreatProtection`	Bảo vệ mối đe dọa web.
	`AMSI`	Bảo vệ AMSI.
	`HostIntrusionPrevention`	Phòng chống xâm nhập máy chủ.
	`BehaviorDetection`	Phát hiện hành vi.
	`ExploitPrevention`	Phòng chống khai thác.
	`RemediationEngine`	Công cụ khắc phục.
	`Firewall`	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.
	`CloudDiscovery`	Cloud Discovery.
	`LogInspector`	Kiểm tra nhật ký
	`AntiCryptor`	Anti-Cryptor
	`FileThreatProtection`	Bảo vệ mối đe dọa tập tin.
	`SystemIntegrityMonitor`	Giám sát tính toàn vẹn của hệ thống.
	`FileEncryption`	Thư viện Mã hóa mức độ tập tin.
	`DiskEncryption`	Thư viện Mã hóa toàn bộ ổ đĩa.
	`MSBitLocker`	Các thư viện quản lý mã hóa BitLocker.
	`BadUSBAttackPrevention`	Phòng chống Tấn công BadUSB.
	`EDR`	Endpoint Detection and Response Optimum Thành phần này không tương thích với các thành phần Endpoint Detection and Response Expert (cloud) (`EDRCloud`) và Endpoint Detection and Response Expert (on-premises) (`AntiAPT`).
	`EDRCloud`	Endpoint Detection and Response Expert (cloud) Thành phần này không tương thích với các thành phần Endpoint Detection and Response Optimum (`EDR`) và Endpoint Detection and Response Expert (on-premises) (`AntiAPT`).

Phần	Tham số	Mô tả
	`AntiAPT`	Endpoint Detection and Response Expert (on-premises) Thành phần này không tương thích với các thành phần Endpoint Detection and Response Expert (cloud) (`EDRCloud`) và Endpoint Detection and Response Optimum (`EDR`).
	`SB`	Kaspersky Sandbox hoặc KATA Sandbox. *Kaspersky Sandbox* là giải pháp Detection and Response solution độc lập của Kaspersky. *KATA Sandbox* là một thành phần của giải pháp Kaspersky Anti Targeted Attack Platform.
	`MDR`	Managed Detection and Response
	`NDR`	Network Detection and Response (KATA) Thành phần này không tương thích với các thành phần Endpoint Detection and Response Expert (cloud) (`EDRCloud`) và Endpoint Detection and Response Optimum (`EDR`).
	`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: • `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.
	`KUMAIntegration`	Tích hợp với KUMA.
	`StandaloneKATA`	Cài đặt ứng dụng ở chế độ Endpoint Detection and Response Agent (EDR Agent) để tích hợp với Kaspersky Anti Targeted Attack Platform (EDR).
	`StandaloneMDR`	Cài đặt ứng dụng ở chế độ Endpoint Detection and Response Agent (EDR Agent) để tích hợp với Kaspersky Managed Detection and Response.
	`StandaloneNDR`	Cài đặt ứng dụng ở chế độ Endpoint Detection and Response Agent (EDR Agent) để tích hợp với Kaspersky Anti Targeted Attack Platform (NDR).
	`StandaloneSiemTelemetry`	Cài đặt ứng dụng ở chế độ Endpoint Detection and Response Agent (EDR Agent) để tích hợp với KUMA.
`[Tasks]`	`ScanMyComputer`	Tác vụ Quét toàn bộ. Giá trị khả dụng: • `1` – Tác vụ này sẽ được bao gồm trong danh sách tác vụ của Kaspersky Endpoint Security. • `0` – Tác vụ này không được bao gồm trong danh sách tác vụ của Kaspersky Endpoint Security.
	`ScanCritical`	Tác vụ Quét khu vực quan trọng. Giá trị khả dụng: • `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`	Tác vụ cập nhật. Giá trị khả dụng: • `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.

Các tiến trình của Kaspersky Endpoint Security cho Windows

Kaspersky Endpoint Security cho Windows khởi chạy các tiến trình được mô tả trong bảng bên dưới.

Các tiến trình của Kaspersky Endpoint Security cho Windows

Tên tập tin	Mục đích
avp.exe	Tiến trình làm việc của Kaspersky Endpoint Security for Windows.
avpsus.exe	Tiến trình này cho phép cài đặt và khôi phục lại các bản cập nhật mô-đun ứng dụng rất quan trọng và đã được phê duyệt.

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.

  > Phương pháp này không khả dụng nếu ứng dụng được cài đặt qua Kaspersky Security Center. Bạn chỉ có thể thay đổi bộ thành phần ứng dụng trong Control Panel sau khi cài đặt ứng dụng cục bộ.

- 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 cân 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.
- Nếu ứng dụng được cài đặt ở chế độ Light Agent trong cơ sở hạ tầng VDI thì việc thay đổi các thành phần thiết lập không được hỗ trợ.

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

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Tasks**.
   Danh sách tác vụ sẽ mở.
2. Nhấn vào **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 (14.2)** → **Lựa chọn thành phần để cài đặt**.

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

Chọn cấu hình của ứng dụng:

- **Chế độ tiêu chuẩn để bảo vệ máy chủ**. Cấu hình mặc định. Cấu hình này cho phép bạn sử dụng tất cả các thành phần của ứng dụng, bao gồm các thành phần cung cấp hỗ trợ cho các giải pháp Detection and Response. Cấu hình này được sử dụng để bảo vệ máy tính toàn diện trước nhiều mối đe dọa, tấn công mạng và gian lận.
- **Endpoint Detection and Response Agent để bảo vệ trước các mối đe dọa nâng cao và các cuộc tấn công nhắm mục tiêu**. Trong cấu hình này, bạn chỉ có thể cài đặt các thành phần hỗ trợ các giải pháp Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), cũng như KUMA. Đây là cấu hình cần thiết nếu Endpoint Protection Platform (EPP) của bên thứ ba được triển khai trong tổ chức của bạn cùng với giải pháp Kaspersky Detection and Response. Điều này làm cho Kaspersky Endpoint Security trong cấu hình Endpoint Detection and Response Agent tương thích với các ứng dụng EPP của bên thứ ba.

  Khi thay đổi cấu hình ứng dụng cho EDR Agent để hoạt động với MDR, hãy đảm bảo rằng các thành phần chịu trách nhiệm nhận dữ liệu đo lường từ xa đã được kích hoạt.

- **Light Agent để bảo vệ môi trường ảo**. Cấu hình này được dành cho ứng dụng được sử dụng như một phần của giải pháp Kaspersky Security for Virtualization Light Agent. Phải cài đặt Light Agent trên mỗi máy ảo cần được bảo vệ bằng giải pháp này. Trong cấu hình này, bạn không thể sử dụng các thành phần các thành phần Mã hóa dữ liệu hoặc Kiểm soát thích ứng sự cố. Nếu bạn đang cài đặt Light Agent trên một mẫu máy ảo sẽ được sử dụng để tạo *máy ảo không lưu các thay đổi*, hãy chọn hộp kiểm **Bảo vệ hạ tầng VDI** (VDI chữ là viết tắt của Virtual Desktop Infrastructure). Chế độ bảo vệ VDI giúp tối ưu hóa hiệu năng của Kaspersky Endpoint Security trên các máy ảo không lưu các thay đổi. Ở chế độ này, Light Agent từ chối các bản cập nhật ứng dụng đòi hỏi khởi động lại máy ảo. Khi nhận được các bản cập nhật ứng dụng yêu cầu khởi động lại, Light Agent sẽ tạo một sự kiện về việc cần cập nhật mẫu của các máy ảo được bảo vệ.

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

Bước 3. Thiết lập nâng cao

Cấu hình thiết lập nâng cao cho tác vụ (xem bảng bên dưới).

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. 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 6. Xác định tên tác vụ

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

Bước 7. Hoàn tất việc tạo tác vụ

Hoàn tất 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 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 **Tasks**.

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **Add**.

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 **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2.0**.
2. Trong danh sách thả xuống **Task type**, hãy 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 **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 phần thuộc tính tác vụ, hãy chọn thẻ **Application settings**. Tiếp theo, hãy chọn cấu hình của ứng dụng:

- **Standard mode to protect workstations and servers**. Cấu hình mặc định. Cấu hình này cho phép bạn sử dụng tất cả các thành phần của ứng dụng, bao gồm các thành phần cung cấp hỗ trợ cho các giải pháp Detection and Response. Cấu hình này được sử dụng để bảo vệ máy tính toàn diện trước nhiều mối đe dọa, tấn công mạng và gian lận.

- **Endpoint Detection and Response Agent to protect against advanced threats and targeted attacks**. Trong cấu hình này, bạn chỉ có thể cài đặt các thành phần hỗ trợ các giải pháp Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), cũng như KUMA. Đây là cấu hình cần thiết nếu Endpoint Protection Platform (EPP) của bên thứ ba được triển khai trong tổ chức của bạn cùng với giải pháp Kaspersky Detection and Response. Điều này làm cho Kaspersky Endpoint Security trong cấu hình Endpoint Detection and Response Agent tương thích với các ứng dụng EPP của bên thứ ba.

  Khi thay đổi cấu hình ứng dụng cho EDR Agent để hoạt động với MDR, hãy đảm bảo rằng các thành phần chịu trách nhiệm nhận dữ liệu đo lường từ xa đã được kích hoạt.

- **Light Agent to protect virtual environments**. Cấu hình này được dành cho ứng dụng được sử dụng như một phần của giải pháp Kaspersky Security for Virtualization Light Agent. Phải cài đặt Light Agent trên mỗi máy ảo cần được bảo vệ bằng giải pháp này. Trong cấu hình này, bạn không thể sử dụng các thành phần các thành phần Mã hóa dữ liệu hoặc Kiểm soát thích ứng sự cố. Nếu bạn đang cài đặt Light Agent trên một mẫu máy ảo sẽ được sử dụng để tạo *máy ảo không lưu các thay đổi*, hãy chọn hộp kiểm **Protect VDI infrastructure** (VDI chữ là viết tắt của Virtual Desktop Infrastructure). Chế độ bảo vệ VDI giúp tối ưu hóa hiệu năng của Kaspersky Endpoint Security trên các máy ảo không lưu các thay đổi. Ở chế độ này, Light Agent từ chối các bản cập nhật ứng dụng đòi hỏi khởi động lại máy ảo. Khi nhận được các bản cập nhật ứng dụng yêu cầu khởi động lại, Light Agent sẽ tạo một sự kiện về việc cần cập nhật mẫu của các máy ảo được bảo vệ.

Chọn các thành phần ứng dụng sẽ khả dụng trên máy tính của người dùng. Cấu hình thiết lập nâng cao cho tác vụ (xem bảng bên dưới).

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.

Lỗi có thể xảy ra khi cài đặt, cập nhật hoặc gỡ bỏ Kaspersky Endpoint Security. Để biết thêm thông tin về cách xử lý các lỗi này, vui lòng tham khảo Cơ sở tri thức hỗ trợ kỹ thuật.

Tham số	Mô tả
Thiết lập tác vụ	**Kiểm tra các ứng dụng không tương thích của bên thứ ba**. Theo mặc định, Kaspersky Endpoint Security sẽ kiểm tra tính tương thích của các ứng dụng đã cài đặt. Danh sách phần mềm có thể gây ra sự cố tương thích có trong tập tin incompatible.txt file. Tập tin này được kèm theo gói phân phối. Nếu bật tác vụ quét các phần mềm đã cài đặt, khi phát hiện một ứng dụng trong danh sách, Kaspersky Endpoint Security sẽ dừng tác vụ. Bạn có thể tắt quét phần mềm đã cài đặt nếu tài liệu của nhà cung cấp phần mềm bên thứ ba khẳng định tính tương thích với Endpoint Protection Platform (EPP). **Gỡ bỏ ứng dụng không tương thích của hãng thứ ba**. Tự động gỡ bỏ các ứng dụng được liệt kê trong tập tin incompatible.txt trước khi thay đổi nhóm thành phần. Nếu chức năng này được bật, Kaspersky Endpoint Security sẽ cố gỡ bỏ các ứng dụng có thể gây ra sự cố tương thích để tiếp tục tác vụ. **Sử dụng chế độ tương thích Azure WVD**. Tính năng này đảm bảo hiển thị chính xác trạng thái máy ảo Azure trong bảng điều khiển Kaspersky Anti Targeted Attack Platform. Để theo dõi hiệu năng của máy tính, Kaspersky Endpoint Security sẽ gửi thông tin đo từ xa đến các máy chủ KATA. Thông tin đo từ xa chứa một ID của máy tính (Sensor ID). Chế độ tương thích Azure WVD cho phép gán Sensor ID duy nhất vĩnh viễn cho các máy ảo này. Nếu chế độ tương thích bị tắt thì Sensor ID có thể thay đổi sau khi máy tính được khởi động lại do cách máy ảo Azure hoạt động. Điều này có thể khiến các máy ảo trùng lặp xuất hiện trên bảng điều khiển.
Loại trừ	Kể từ Kaspersky Endpoint Security 12.6 cho Windows, loại trừ quét và ứng dụng được tin tưởng được thêm vào khu vực tin tưởng. Các ứng dụng được tin tưởng và loại trừ quét được xác định trước giúp nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager. Điều này có nghĩa là bạn không cần thiết lập khu vực tin tưởng theo cách thủ công cho ứng dụng trên máy chủ. Kể từ Kaspersky Endpoint Security 12.8 cho Windows, bạn có thể cài đặt ứng dụng ở chế độ Light Agent để bảo vệ môi trường ảo. Các loại trừ quét được định sẵn và các ứng dụng được tin tưởng có thể giúp bạn nhanh chóng cấu hình Kaspersky Endpoint Security trong các môi trường máy ảo Citrix và VMware. Bạn cũng có thể cấu hình khu vực tin tưởng sau trong thuộc tính chính sách: loại trừ quét và ứng dụng được tin tưởng.
Chế độ riêng / Chế độ kết hợp	Bạn có thể tạo các nhóm thành phần riêng biệt cho máy trạm và máy chủ – **Chế độ riêng**. Trước khi triển khai gói cài đặt, trình cài đặt sẽ phát hiện loại hệ điều hành và chỉ cài đặt những thành phần ứng dụng mà bạn đã chọn cho loại hệ điều hành đó. Theo đó, bạn có thể sử dụng cùng một gói cài đặt cho máy trạm và máy chủ. **Chế độ kết hợp** cung cấp danh sách các thành phần chung cho máy trạm và máy chủ. Tính khả dụng của từng thành phần phụ thuộc vào loại hệ điều hành. Ở chế độ này, bạn nên tạo gói cài đặt riêng cho máy trạm và gói cài đặt riêng cho máy chủ. Bạn chỉ có thể cấu hình danh sách các thành phần chung trong gói cài đặt ở chế độ Tiêu chuẩn.
Sử dụng mật khẩu để chỉnh sửa bộ thành phần ứng dụng	Quản trị viên thường bật Bảo vệ bằng mật khẩu để hạn chế quyền truy cập vào Kaspersky Endpoint Security. Nghĩa là, để sửa đổi lựa chọn các thành phần ứng dụng, bạn phải nhập thông tin đăng nhập của người dùng có quyền **Gỡ bỏ / thay đổi / khôi phục ứng dụng**. Ví dụ: bạn có thể sử dụng tài khoản KLAdmin.
Sử dụng mật khẩu để gỡ cài đặt Kaspersky Endpoint Agent và Kaspersky Security for Windows Server	Quản trị viên thường bật Bảo vệ bằng mật khẩu trong thiết lập của các tác vụ này để hạn chế quyền truy cập vào Kaspersky Endpoint Agent (KEA) và Kaspersky Security for Windows Server (KSWS). Nghĩa là, nếu bạn đang chuyển từ cấu hình [KES+KEA] sang [KES+tác nhân tích hợp] hoặc nếu bạn đang chuyển từ KSWS sang KES thì bạn phải nhập mật khẩu để gỡ bỏ các ứng dụng này.

Nâng cấp 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.
- 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.
- Để thay đổi ngôn ngữ của ứng dụng, trong tác vụ *Install application remotely*, hãy chọn gói cài đặt có ngôn ngữ bản địa hóa mà bạn muốn và cập nhật ứng dụng. Tính năng thay đổi ngôn ngữ ứng dụng lần đầu khả dụng trong Kaspersky Endpoint Security cho Windows 14.2.

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

- Kaspersky Endpoint Security 12.3 cho Windows (bản dựng 12.3.0.493)
- Kaspersky Endpoint Security 12.4 cho Windows (bản dựng 12.4.0.467)
- Kaspersky Endpoint Security 12.5 cho Windows (bản dựng 12.5.0.539)
- Kaspersky Endpoint Security 12.6 cho Windows (bản dựng 12.6.0.438)
- Kaspersky Endpoint Security 12.7 cho Windows (bản dựng 12.7.0.533)
- Kaspersky Endpoint Security 12.8 cho Windows (bản dựng 12.8.0.505)
- Kaspersky Endpoint Security 12.9 cho Windows (bản dựng 12.9.0.384)
- Kaspersky Endpoint Security 12.10 cho Windows (bản dựng 12.10.0.466)
- Kaspersky Endpoint Security 12.11 cho Windows (bản dựng 12.11.0.637)
- Kaspersky Endpoint Security 12.12 cho Windows (bản dựng 12.12.0.522)
- Kaspersky Endpoint Security 14.0 cho Windows (bản dựng 14.0.0.504)
- Kaspersky Endpoint Security 14.1 cho Windows (bản dựng 14.1.0.423)

Lỗi có thể xảy ra khi cài đặt, cập nhật hoặc gỡ bỏ Kaspersky Endpoint Security. Để biết thêm thông tin về cách xử lý các lỗi này, vui lòng tham khảo Cơ sở tri thức hỗ trợ kỹ thuật.

Các phương pháp nâng cấp ứng dụng

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

- Sử dụng dịch vụ cập nhật của Kaspersky (Seamless Update – SMU).
- 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. Khi bạn cập nhật Kaspersky Endpoint Security, hãy cân nhắc các điều sau:

- Bảng điều khiển web 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 tác nhân MDR tích hợp 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.

Nâng cấp ứng dụng mà không cần khởi động lại

Nâng cấp ứng dụng mà không cần khởi động lại cung cho phép máy chủ hoạt động không bị gián đoạn khi phiên bản ứng dụng được cập nhật.

Nâng cấp ứng dụng mà không cần khởi động lại có các hạn chế sau:

- Bạn có thể nâng cấp ứng dụng mà không cần khởi động lại kể từ phiên bản 11.10.0. Bạn phải khởi động lại máy tính để nâng cấp phiên bản cũ hơn của ứng dụng.

- Bạn có thể cài đặt các bản vá mà không cần khởi động lại kể từ phiên bản 11.11.0. Để cài đặt các bản vá cho các phiên bản trước của ứng dụng, bạn có thể phải khởi động lại máy tính.

- Nâng cấp ứng dụng mà không cần khởi động lại không khả dụng trên máy tính đã bật mã hóa dữ liệu (mã hóa của Kaspersky (FDE), BitLocker, Mã hóa mức độ tập tin (FLE)). Để nâng cấp ứng dụng trên các máy tính được bật mã hóa dữ liệu, máy tính phải được khởi động lại.

- Không thể nâng cấp ứng dụng trên máy ảo nếu không khởi động lại. Bạn phải khởi động lại máy ảo để nâng cấp ứng dụng trên máy ảo.

Sau khi nâng cấp ứng dụng, cài đặt bản vá lỗi, thay đổi bộ thành phần ứng dụng hoặc khôi phục, Kaspersky Endpoint Security sẽ khởi động lại để bắt đầu sử dụng phiên bản mới. Quá trình khởi động lại Kaspersky Endpoint Security có thể mất tới một phút. Trong thời gian này, cấp độ bảo vệ máy tính sẽ bị giảm sút. Sau khi khởi động lại ứng dụng, mức độ bảo vệ của máy tính sẽ được khôi phục.

Cách chọn chế độ nâng cấp ứng dụng trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.

2. Trong cây bảng điều khiển, hãy chọn **Policies**.

3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

4. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Thiết lập ứng dụng**.

5. Trong mục **Thiết lập nâng cao**, hãy chọn hoặc xóa hộp kiểm **Cài đặt các bản cập nhật ứng dụng mà không cần khởi động lại** để cấu hình chế độ nâng cấp ứng dụng.

6. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách chọn chế độ nâng cấp ứng dụng trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.

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** → **User Interaction**.

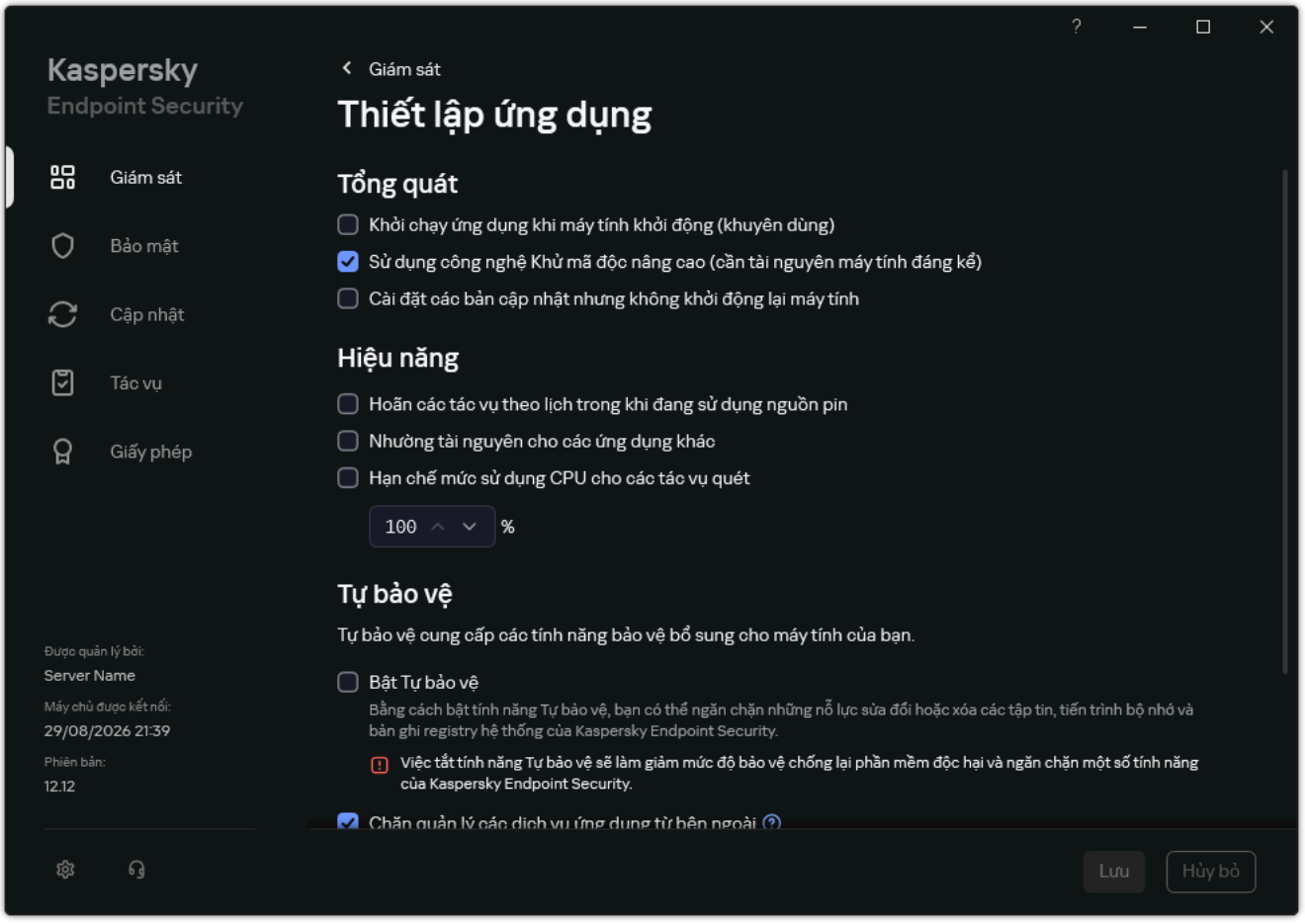
5. Trong mục **Application update settings**, hãy chọn hoặc xóa hộp kiểm **Install application updates without restart** để cấu hình chế độ nâng cấp ứng dụng.

6. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách chọn chế độ nâng cấp 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 **Thiết lập tổng quát** → **Thiết lập ứng dụng**.



Thiết lập Kaspersky Endpoint Security cho Windows

3. Trong mục **Tổng quát**, hãy chọn hoặc xóa hộp kiểm **Cài đặt các bản cập nhật nhưng không khởi động lại máy tính** để cấu hình chế độ nâng cấp ứng dụng.

4. Lưu các thay đổi của bạn.

Bạn cũng có thể chọn chế độ nâng cấp ứng dụng khi cài đặt ứng dụng từ dòng lệnh (sử dụng tùy chọn `UPGRADEMODE`).

Sau khi quy trình nâng cấp ứng dụng mà không cần khởi động lại hoàn tất, phiên bản mới của Kaspersky Endpoint Security sẽ được cài đặt trên máy tính. Phiên bản trước đó của ứng dụng sẽ tự động bị xóa.

Bạn không thể khởi chạy nâng cấp ứng dụng trước khi quá trình nâng cấp trước đó hoàn tất.

Bạn có thể kiểm tra trạng thái nâng cấp Kaspersky Endpoint Security bằng cách sử dụng báo cáo phiên bản ứng dụng Kaspersky trong bảng điều khiển Kaspersky Security Center.

Bản cập nhật SMU của ứng dụng

Để cập nhật ứng dụng bằng dịch vụ cập nhật của Kaspersky (Seamless Update; SMU), bạn không cần phải chạy trình cài đặt, trái với các phương thức cập nhật khác. Kaspersky Endpoint Security tải phiên bản mới của ứng dụng cùng cơ sở dữ liệu diệt virus từ cùng một nguồn.

Bản cập nhật SMU cho phép cập nhật ứng dụng trên tất cả máy tính trong tổ chức của bạn lên phiên bản mới nhất. Trước khi áp dụng bản cập nhật SMU, bạn nên thử nghiệm phiên bản mới của ứng dụng trên một vài máy tính. Để thực hiện, bạn phải cập nhật ứng dụng trên các máy tính này theo cách thủ công (ví dụ: cục bộ bằng Trình hướng dẫn cài đặt). Bạn không thể chọn từng máy tính khi thực hiện cập nhật SMU.

Lịch cập nhật ứng dụng sẽ được nhân viên của Kaspersky quyết định. Để đảm bảo phiên bản mới của ứng dụng chạy trơn tru, Kaspersky sẽ cung cấp các bản cập nhật theo từng bước. Điều này có nghĩa là bạn có thể nhận được bản cập nhật SMU muộn hơn tới hai tháng so với thời điểm phát hành phiên bản mới.

Bạn có thể quản lý bản cập nhật SMU của ứng dụng bằng cách sử dụng tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*. Để phiên bản mới của ứng dụng được kèm theo trong cùng một gói với cơ sở dữ liệu diệt virus, bạn phải cho phép cập nhật *mô-đun ứng dụng* trong thiết lập tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*. Cũng trong thiết lập tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*, bạn có thể cho phép cập nhật ứng dụng mà không cần khởi động lại.

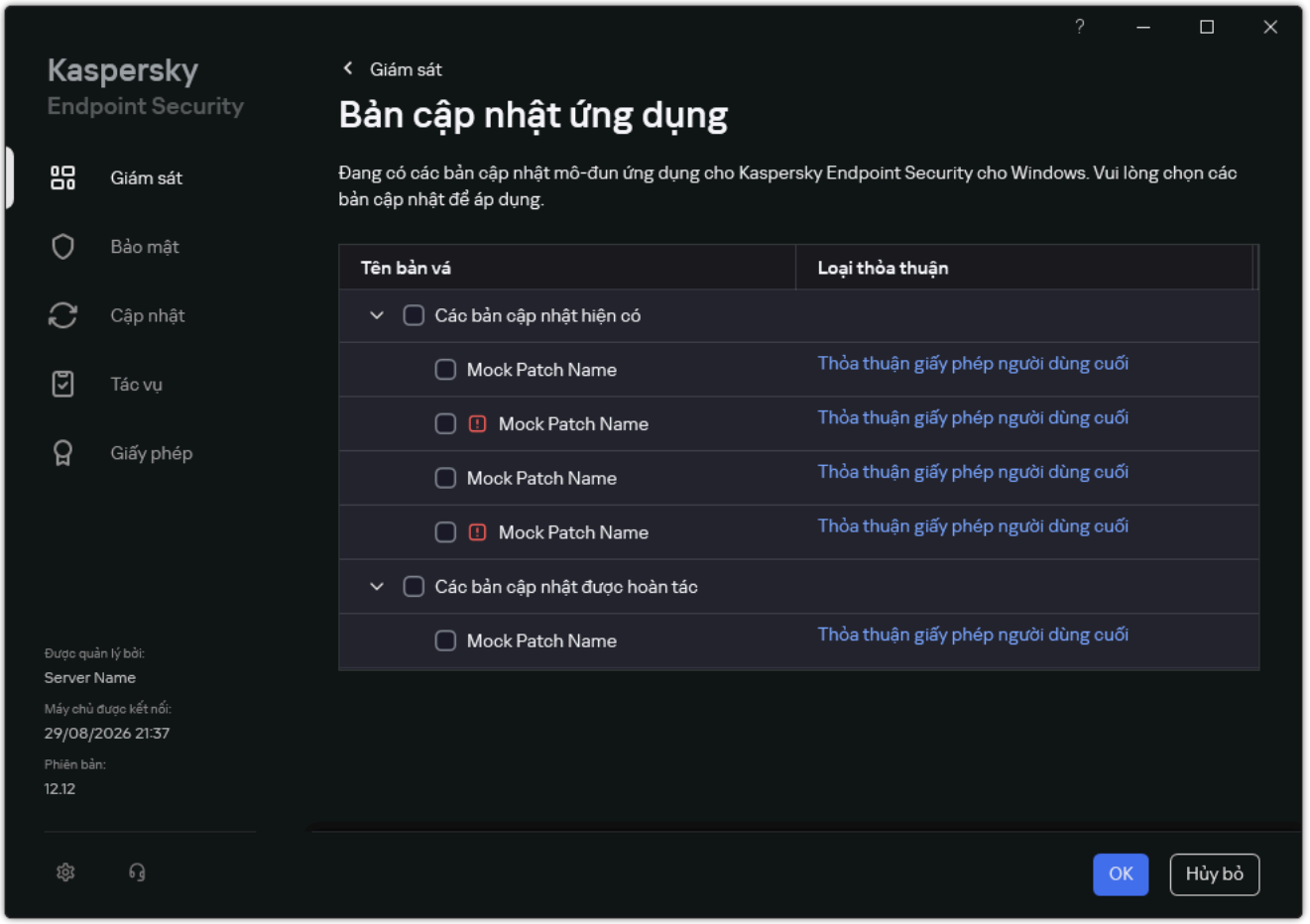
Các bước cập nhật ứng dụng của SMU

1. **Sau khi phiên bản mới của ứng dụng được phát hành, Kaspersky sẽ phân phối bản cập nhật.**
2. **Người dùng chấp thuận cập nhật ứng dụng.**

   Nếu máy tính được kết nối với Kaspersky Security Center, bản cập nhật sẽ khả dụng trong Kaspersky Security Center, trong phần **Update of Kaspersky databases and application modules**. Để biết thêm chi tiết về việc chấp thuận các bản cập nhật, hãy tham khảo Trợ giúp Kaspersky Security Center.

   Nếu máy tính không được kết nối với Kaspersky Security Center, bản cập nhật sẽ khả dụng trong phần thông báo của giao diện ứng dụng: . Để chấp thuận bản cập nhật, hãy chọn phiên bản ứng dụng và chấp nhận các điều khoản và điều kiện của thỏa thuận (xem hình bên dưới).
3. **Kaspersky Endpoint Security sẽ chạy tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* theo đúng lịch được cấu hình.**

Kết quả là Kaspersky Endpoint Security sẽ cập nhật ứng dụng ở chế độ "yên lặng".



Các bản cập nhật ứng dụng khả dụng

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.

Lỗi có thể xảy ra khi cài đặt, cập nhật hoặc gỡ bỏ Kaspersky Endpoint Security. Để biết thêm thông tin về cách xử lý các lỗi này, vui lòng tham khảo Cơ sở tri thức hỗ trợ kỹ thuật.

Gỡ bỏ ứng dụng từ xa thông qua Kaspersky Security Center

Bạn có thể gỡ bỏ ứng dụng từ xa thông qua tác vụ *Uninstall application remotely*. 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. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Tasks**.
   Danh sách tác vụ sẽ mở.
3. Nhấn vào **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 → Advanced → 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 (14.2)**.

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 **Edit**.
3. Nhập mật khẩu của tài khoản KLAdmin.

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 14.2*.

Bước 10. Hoàn thành tạo tác vụ

Hoàn tất 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 **Tasks**.
   Danh sách tác vụ sẽ mở.
2. Nhấn vào **Add**.

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 **Application**, hãy chọn **Kaspersky Security Center**.
2. Trong danh sách thả xuống **Task type**, hãy 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 **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 loại **Uninstall managed application**.
2. Chọn **Kaspersky Endpoint Security for Windows**.

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.

5. Trong trường **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.

6. 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 **Finish**. 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 **Start**. 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 *Uninstall application remotely*. Nếu không có mật khẩu, tác vụ sẽ không được thực hiện.

Để sử dụng mật khẩu của tài khoản KLAdmin trong tác vụ Uninstall application remotely:

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

   Danh sách tác vụ sẽ mở.

2. Nhấn vào tác vụ **Uninstall application remotely** Kaspersky Security Center.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

3. Chọn thẻ **Application settings**.

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

5. Nhập mật khẩu của tài khoản KLAdmin.

6. Lưu các thay đổi của bạn.

Khởi động lại máy tính để hoàn tất quá trình gỡ cài đặt. Để thực hiện, Network Agent sẽ hiển thị một cửa sổ nổi lên.

Gỡ bỏ ứng dụng từ xa thông qua Active Directory

Bạn có thể gỡ bỏ ứng dụng từ xa bằng chính sách nhóm của Microsoft Windows. Để gỡ bỏ ứng dụng, bạn cần mở Bảng điều khiển quản lý Chính sách nhóm (gpmc.msc) và sử dụng Trình chỉnh sửa Chính sách nhóm để tạo một tác vụ gỡ bỏ ứng dụng (để biết thêm chi tiết, vui lòng truy cập Website hỗ trợ kỹ thuật của Microsoft).

Nếu hoạt động gỡ bỏ ứng dụng được bảo vệ bằng mật khẩu, bạn cần làm như sau:

1. Tạo một tập tin BAT chứa nội dung sau:

   ```
   msiexec.exe /x<GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
   ```

   <GUID> và ID duy nhất của ứng dụng. Bạn có thể tìm ra GUID của ứng dụng trong Cơ sở tri thức hỗ trợ kỹ thuật hoặc bằng lệnh sau:

   ```
   wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
   ```

   Ví dụ

   ```
   msiexec.exe /x{6BB76C8F-365E-4345-83ED-6D7AD612AF76} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
   ```

2. Tạo chính sách Microsoft Windows mới cho máy tính trong Bảng điều khiển quản lý Chính sách nhóm (gpmc.msc).

3. Sử dụng chính sách mới để chạy tập tin BAT được tạo trên máy tính.

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.



Lựa chọn hoạt động gỡ bỏ ứng dụng

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 dữ liệu nào, ứng dụng sẽ bị gỡ bỏ hoàn toàn (xem hình bên dưới).



Lưu dữ liệu sau khi xóa

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.

Kaspersky Endpoint Security lưu dữ liệu trong thư mục `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.

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\KES\Doc\<locale>\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. Không thể kích hoạt ứng dụng theo giấy phép dùng thử sau khi ứng dụng đã được kích hoạt bằng giấy phép thương mại.

- *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 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:

- ID 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.
- Lấy tập tin khóa từ Máy chủ quản trị khác.

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 chức năng của ứng dụng tùy thuộc vào loại giấy phép Kaspersky Next, hãy xem trong Trợ giúp của Kaspersky Next.

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	Kaspersky Hybrid Cloud Security Enterprise
Bảo vệ mối đe dọa nâng cao								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Phát hiện hành vi	✓	✓	✓	✓	✓	✓	✓	✓
Chống công cụ mã hóa	✓	✓	✓	✓	✓	✓	✓	✓
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	✓	✓	✓	✓	✓	✓	✓	✓

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	Kaspersky Hybrid Cloud Security Enterprise
Bảo vệ AMSI	✓	✓	✓	✓	✓	✓	✓	✓
Kiểm soát bảo mật								
Kiểm tra nhật ký	–	–	–	–	–	–	–	–
Kiểm soát ứng dụng	✓	✓	✓	✓	✓	✓	✓	✓
Kiểm soát thiết bị	✓	✓	✓	✓	✓	✓	✓	✓
Kiểm soát Web	✓	✓	✓	✓	✓	✓	✓	✓
Kiểm soát thích ứng sự cố	–	✓	✓	✓	✓	✓	–	✓
Giám sát tính toàn vẹn của hệ thống	–	–	–	–	–	–	–	–
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 *(Phải mua giấy phép Kaspersky Sandbox riêng)*	✓	✓	✓	✓	✓	✓	✓	✓

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	Kaspersky Hybrid Cloud Security Enterprise
Tích hợp với KUMA *(Giấy phép để Tích hợp KUMA phải được mua riêng)*	✓	✓	✓	✓	✓	✓	✓	✓
Chế độ Light Agent *(để kích hoạt ứng dụng, bạn phải thêm khóa giấy phép vào SVM mà Light Agent được kết nối)*	–	–	–	–	–	–	✓	✓

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 chức năng của ứng dụng tùy thuộc vào loại giấy phép Kaspersky Next, hãy xem trong Trợ giúp của Kaspersky Next.

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	Kaspersky Hybrid Cloud Security Enterprise
Bảo vệ mối đe dọa nâng cao								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Phát hiện hành vi	✓	✓	✓	✓	✓	✓	✓	✓
Chống công cụ mã hóa	✓	✓	✓	✓	✓	✓	✓	✓
Phòng chống khai thác	✓	✓	✓	✓	✓	✓	✓	✓

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	Kaspersky Hybrid Cloud Security Enterprise
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 tra nhật ký	–	–	–	–	–	–	–	✓
Kiểm soát ứng dụng	–	✓	✓	✓	✓	✓	–	✓
Kiểm soát thiết bị	–	✓	✓	✓	✓	✓	✓	✓
Kiểm soát Web	–	✓	✓	✓	✓	✓	✓	✓
Kiểm soát thích ứng sự cố	–	–	–	–	–	–	–	–
Giám sát tính toàn vẹn của hệ thống	–	–	–	–	–	–	–	✓
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								

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	Kaspersky Hybrid Cloud Security Enterprise
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(Phải mua giấy phép Kaspersky Sandbox riêng)*	✓	✓	✓	✓	✓	✓	✓	✓
Tích hợp với KUMA *(Giấy phép để Tích hợp KUMA phải được mua riêng)*	✓	✓	✓	✓	✓	✓	✓	✓
Chế độ Light Agent *(để kích hoạt ứng dụng, bạn phải thêm khóa giấy phép vào SVM mà Light Agent được kết nối)*	–	–	–	–	–	–	✓	✓

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 bằng cách sử dụng bộ phần mềm Kaspersky Security Center.
  - 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. Bạn có thể thêm cả khóa hiện hoạt và khóa dự trữ bằng cách này.
  - 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.

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

- 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.

- 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.

> Nếu Kaspersky Endpoint Security đang được sử dụng trong Chế độ Light Agent để bảo vệ môi trường ảo thì bạn không cần kích hoạt ứng dụng riêng.

Kích hoạt ứng dụng

Cách kích hoạt ứng dụng trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Tasks**.

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **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 (14.2)** → **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

Hoàn tất 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 **Tasks**.

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **Add**.

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 **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.
2. Trong danh sách thả xuống **Task type**, hãy chọn **Add key**.
3. Trong trường **Task name**, nhập một mô tả ngắn gọn, ví dụ như *Kích hoạt Kaspersky Endpoint Security cho Windows*.
4. Trong phần **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 (**Operations → Licensing**).

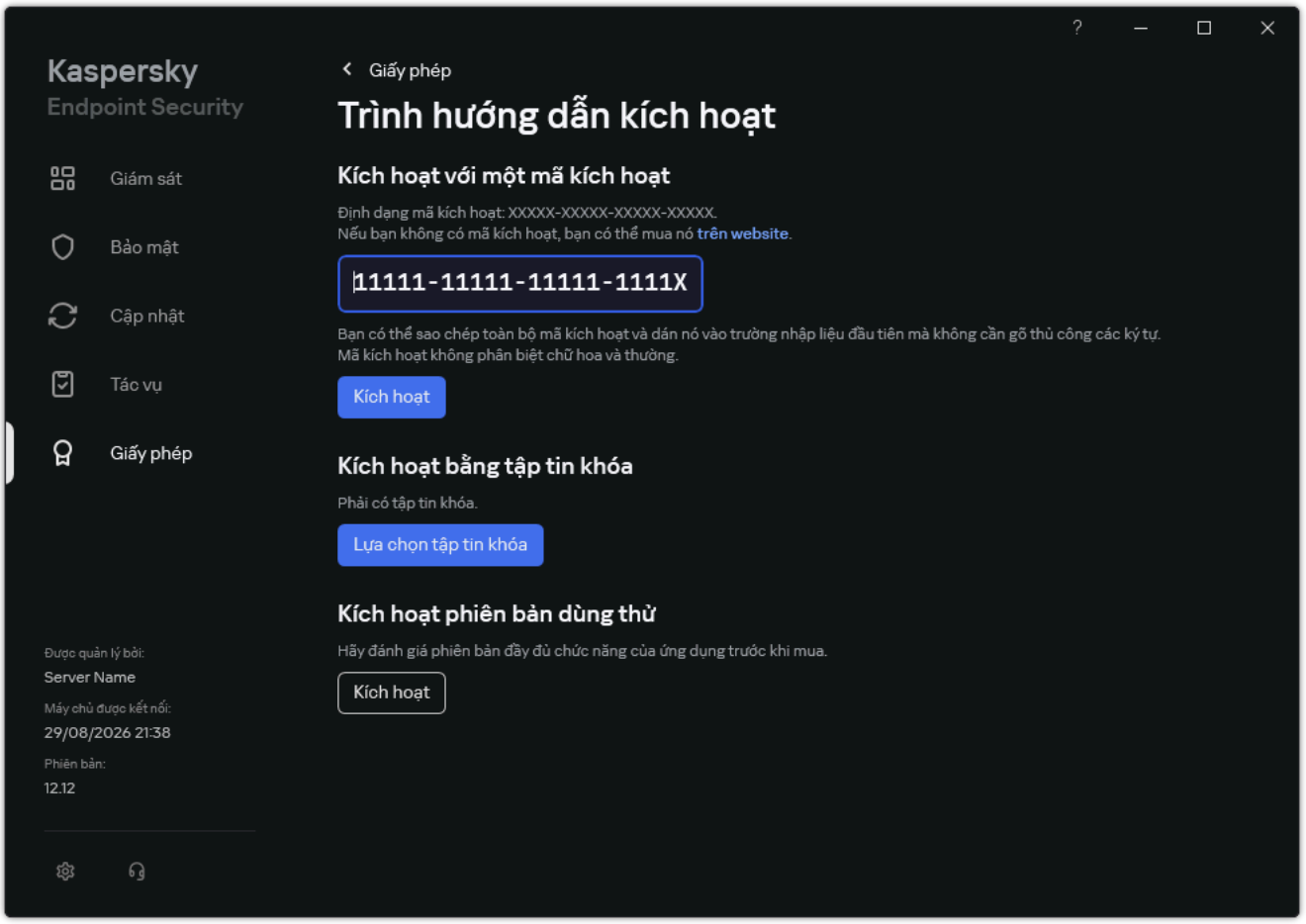
Bước 4. Hoàn tất việc tạo tác vụ

Hoàn tất trình hướng dẫn bằng cách nhấn nút **Finish**. 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 **Start**. 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 giao diện ứng dụng

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.



Kích hoạt ứng dụng

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. 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 **Kaspersky Licenses**.

   Một danh sách khóa giấy phép sẽ mở ra.

2. Mở thuộc tính khóa giấy phép.

3. Trong phần **General**, hãy chọn hộp kiểm **Automatically distribute license key to managed devices**.

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** → **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 **Automatically distribute license key to managed devices**.

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**.

Nếu đang kích hoạt ứng dụng bằng *mã kích hoạt*, bạn cần truy cập internet để kết nối với máy chủ kích hoạt của Kaspersky. Nếu đang kích hoạt ứng dụng bằng *tập tin khóa*, thì bạn không cần truy cập internet. Nếu các máy tính nằm trong một phần mạng bị cô lập và không có quyền truy cập internet, để kích hoạt ứng dụng bằng mã, bạn phải cho phép sử dụng Máy chủ quản trị Kaspersky Security Center làm máy chủ proxy. Có nghĩa là ứng dụng có thể có quyền truy cập vào máy chủ kích hoạt thông qua Máy chủ quản trị có quyền truy cập internet.

Cách cho phép sử dụng Máy chủ quản trị làm máy chủ proxy để kích hoạt ứng dụng trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Thiết lập ứng dụng**.

4. Chọn hộp kiểm **Sử dụng Kaspersky Security Center như máy chủ proxy để kích hoạt**.

5. Lưu các thay đổi của bạn.

Cách cho phép sử dụng Máy chủ quản trị làm máy chủ proxy để 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 **Asset management → Policies**.

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 → KSC Integration**.

5. Chọn hộp kiểm **Use Kaspersky Security Center as proxy server for activation**.

6. Lưu các thay đổi của bạn.

Nếu bạn không thể kích hoạt ứng dụng bằng *mã kích hoạt*, bạn có thể thử lấy một *tập tin khóa* bằng giải pháp Kaspersky và thử kích hoạt lại ứng dụng bằng phương pháp khác.

Giám sát sử dụng giấy phép

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

- Xem *Report on usage of license keys* trong cơ sở hạ tầng của tổ chức (**Monitoring** → **Reports**).
- Xem trạng thái của máy tính trên thẻ **Managed devices** → **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 (**Operations** → **Licensing**).

Chi tiết về việc kích hoạt ứng dụng như một phần của Bảng điều khiển đám mây của Kaspersky Security Center

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.

Xóa khóa giấy phép

Để xóa khóa giấy phép, bạn cần chạy một tác vụ đặc biệt trên máy tính của mình. Ví dụ: bạn có thể xóa khóa giấy phép để sắp xếp lại các đơn vị cấp phép. Ngoài ra, khi giấy phép hết hạn, Kaspersky Endpoint Security sẽ thông báo cho bạn. Nếu bạn đã thêm khóa giấy phép có thời hạn ngắn để dùng thử ứng dụng (ví dụ: Tiện ích bổ trợ EDR Optimum), bạn có thể xóa khóa giấy phép này để thoát khỏi thông báo và khắc phục tình trạng máy tính.

Tác vụ *Xóa khóa* cho phép xóa bất kỳ khóa giấy phép nào khỏi máy tính. Bạn có thể xóa giấy cấp phép đang hoạt động cũng như giữ lại khóa giấy phép. Ngoài khóa giấy phép kích hoạt Kaspersky Endpoint Security, bạn có thể xóa từng khóa giấy phép của giải pháp Kaspersky Detection and Response (ví dụ: Tiện ích bổ trợ EDR Optimum).

Cách xóa khóa giấy phép trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Tasks**.
   Danh sách tác vụ sẽ mở.
2. Nhấn vào **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 (14.2)** → **Xóa khóa**.

Bước 2. Chọn một giấy phép

Chọn khóa giấy phép mà bạn muốn xóa. Bạn có thể chọn khóa giấy phép từ kho khóa của Kaspersky Security Center hoặc chọn tập tin khóa.

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 nhiệm vụ, ví dụ: *Xóa khóa cho beta*.

Bước 6. Hoàn tất việc tạo tác vụ

Hoàn tất 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 xóa khóa giấy phép trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Tasks**.
   Danh sách tác vụ sẽ mở.
2. Nhấn vào **Add**.

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 **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.
2. Trong danh sách thả xuống **Task type**, hãy chọn **Remove key**.
3. Trong trường **Task name**, nhập một mô tả ngắn, ví dụ như *Xóa khóa cho beta*.
4. Trong phần **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

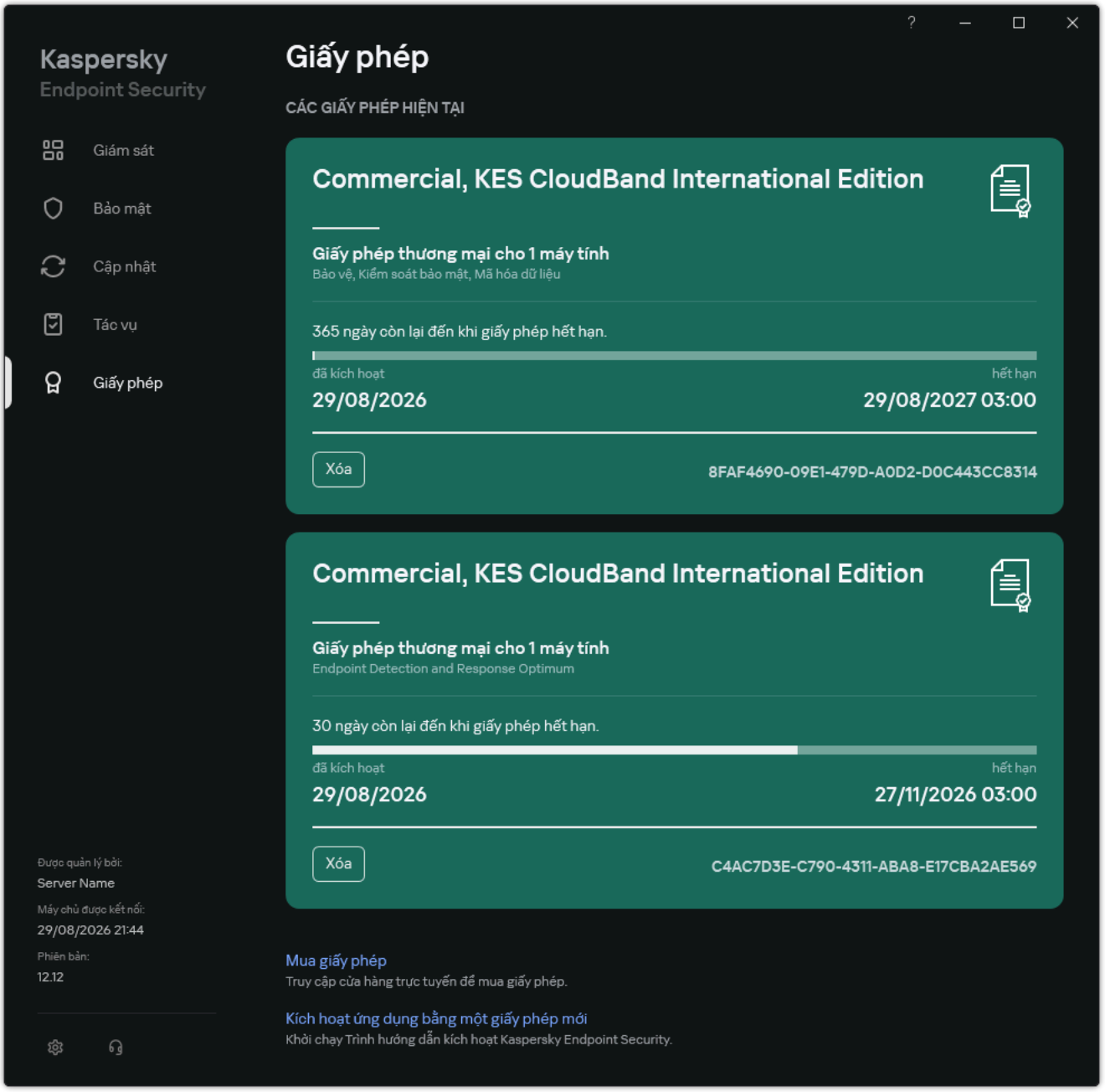
Chọn khóa giấy phép mà bạn muốn xóa. Bạn có thể chọn khóa giấy phép từ kho khóa của Kaspersky Security Center hoặc chọn tập tin khóa. Chuyển sang bước tiếp theo.

Bước 4. Hoàn tất việc tạo tác vụ

Hoàn tất trình hướng dẫn bằng cách nhấn nút **Finish**. 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 **Start**.

Cách xóa khóa giấy phép trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Giấy phép**.
2. Chọn khóa mà bạn muốn xóa và nhấn vào **Xóa**.



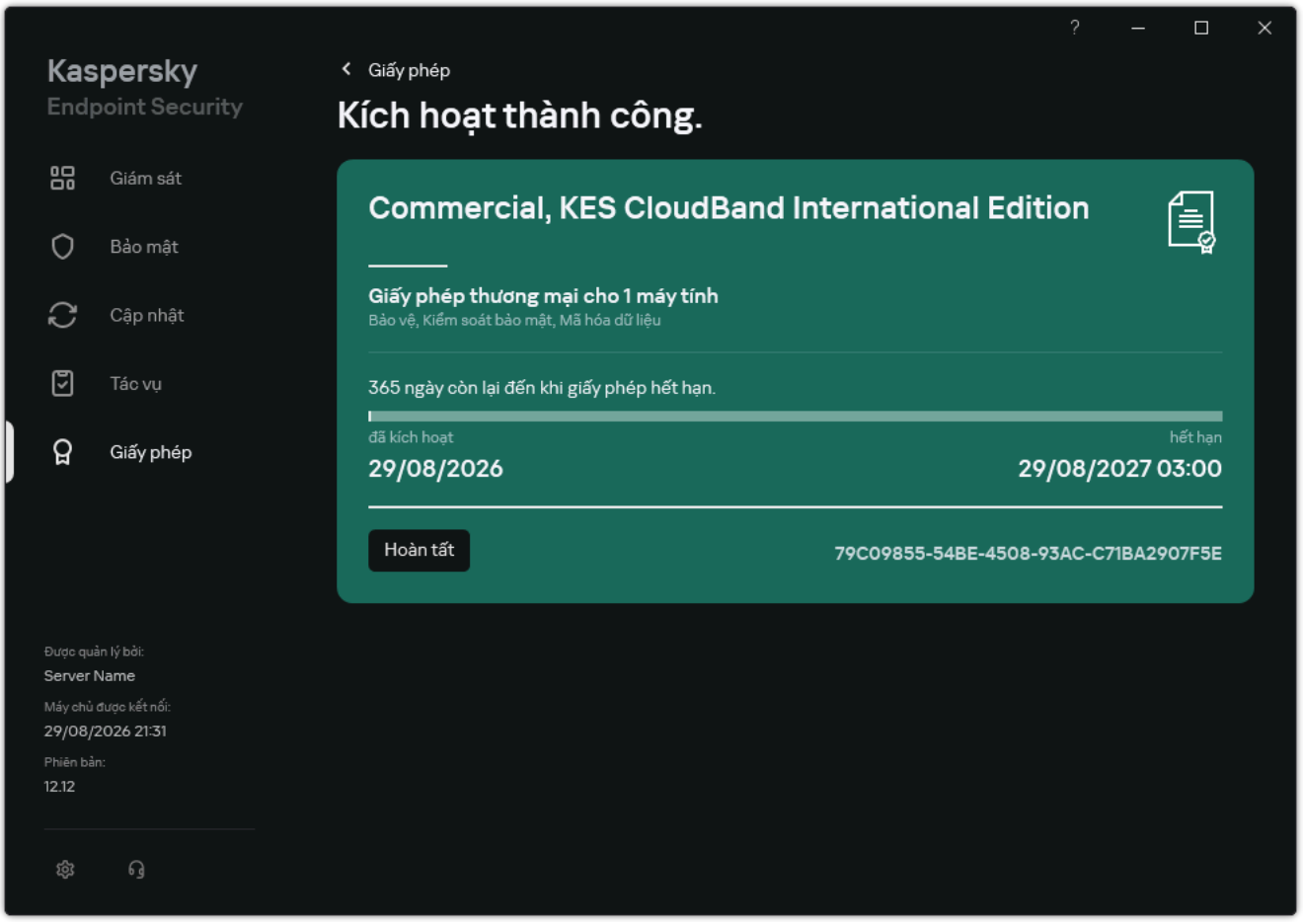
Cửa sổ Cấp giấy phép

Bạn cũng có thể xóa khóa giấy phép trên dòng lệnh.

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 trại 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.

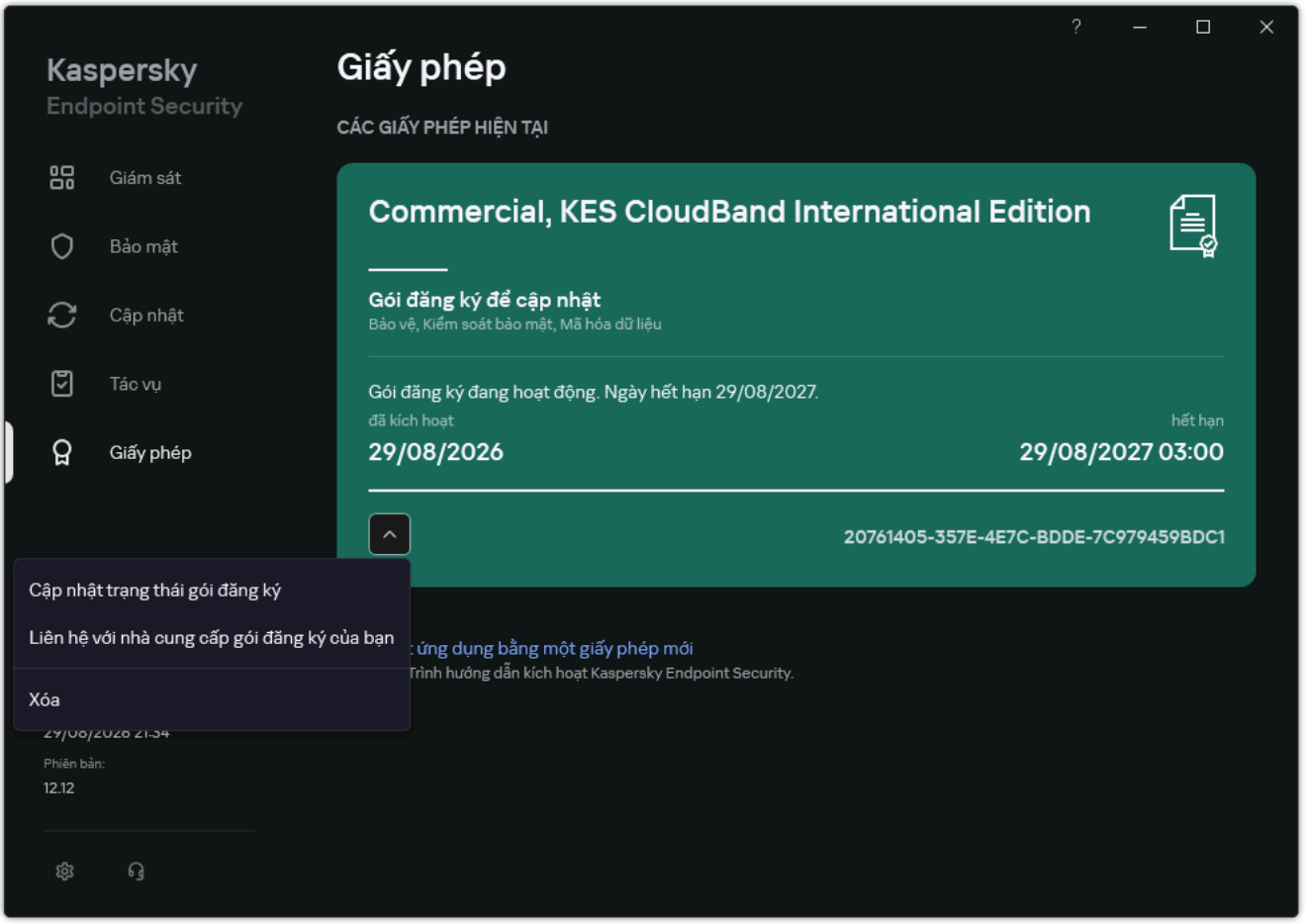
Bạn có thể gia hạn gói đăng ký trên website của nhà cung cấp dịch vụ.

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.



Gia hạn gói đăng ký

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*). Đây là giao diện web để quản lý hệ thống bảo vệ dựa trên các ứng dụng Kaspersky. Bạn có thể làm việc với Bảng điều khiển web Kaspersky Security Center thông qua trình duyệt trên bất kỳ thiết bị nào. 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. Tiện ích web phải được cài đặt trên máy tính đã cài đặt Kaspersky Security Center Web Console. 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**.

Nếu đang sử dụng Kaspersky Endpoint Security là một phần của giải pháp Kaspersky Endpoint Detection and Response Optimum thì bạn phải cài đặt tiện ích quản lý của Kaspersky Endpoint Detection and Response. Bạn cần tiện ích quản lý để hiển thị thông tin chi tiết về cảnh báo. *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. Do đó, để tạo các tác vụ phản hồi trước mối đe dọa, bạn cần có tiện ích quản lý của Kaspersky Endpoint Security và để xem chi tiết cảnh báo, bạn cần có tiện ích quản lý của EDR.

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.

Kể từ Kaspersky Endpoint Security 12.11 cho Windows, quy trình cài đặt tiện ích web đã thay đổi. Gói phân phối đã bao gồm hai tiện ích web: *Kaspersky Endpoint Security for Windows 14.2.0* và *Unified Protection and Management Plug-in*. Đây là do quá trình chuyển đổi sang một tiện web thống nhất duy nhất để quản lý các ứng dụng Kaspersky. Tiện ích web thống nhất cho phép tạo một chính sách duy nhất để quản lý nhiều ứng dụng Kaspersky (ví dụ: Kaspersky Endpoint Security cho Windows, macOS và Linux). Quá trình chuyển đổi sang tiện ích web thống nhất có thể cần vài bản phát hành. Sau khi quá trình chuyển đổi hoàn tất, gói phân phối sẽ chỉ bao gồm *Unified Protection and Management Plug-in*.

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.

Nếu Tiện ích quản lý Kaspersky Endpoint Security 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 lý:

- Các phiên bản cũ của Tiện ích quản lý Kaspersky Endpoint Security sẽ bị gỡ bỏ.
- Phiên bản mới của Tiện ích quản lý Kaspersky Endpoint Security hỗ trợ việc quản lý các phiên bản cũ của Kaspersky Endpoint Security 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.

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.

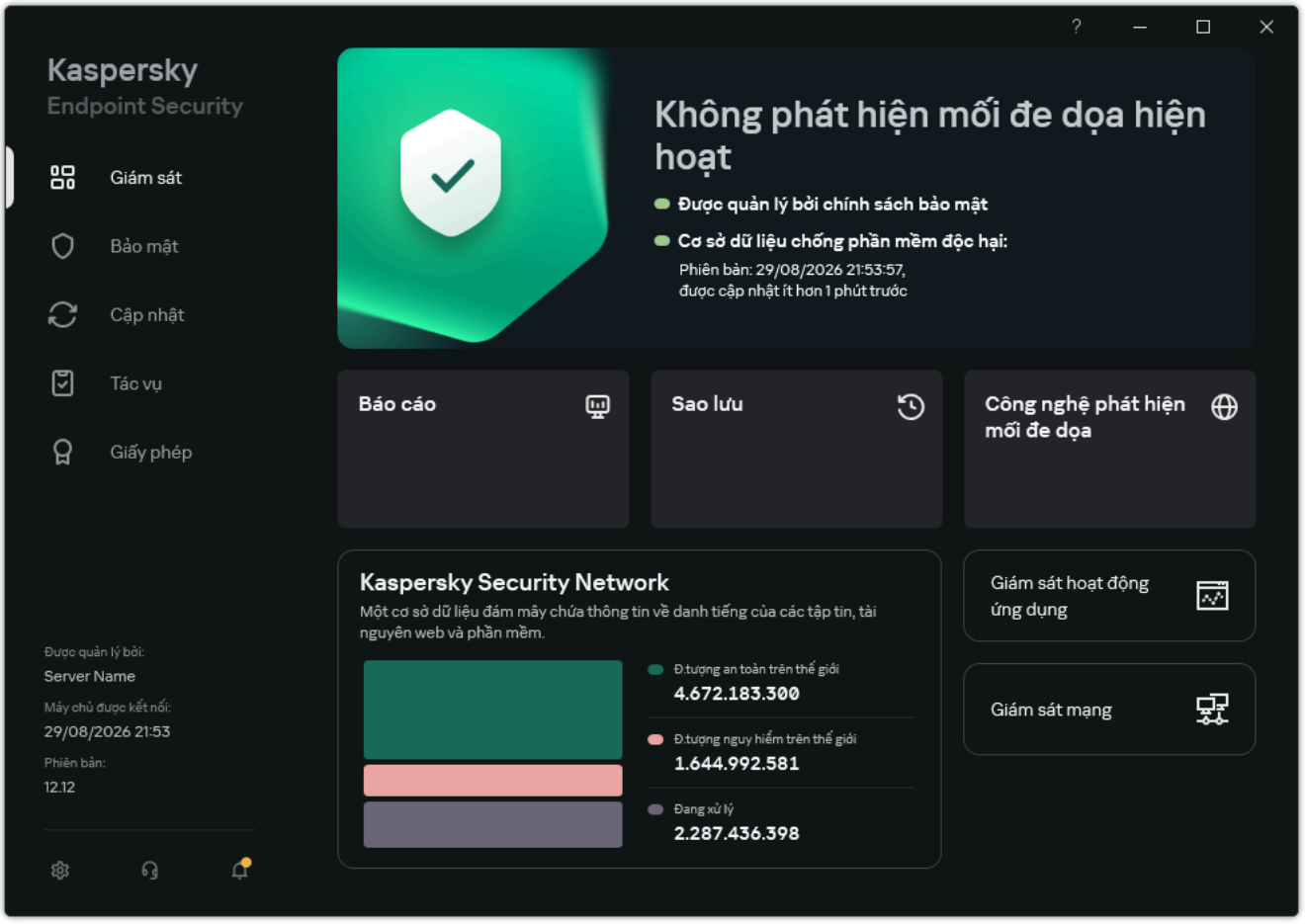
Việc sử dụng TLS bảo mật cho ứng dụng bằng cách cung cấp các tính năng sau:

- 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 một Public Key Infrastructure (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 Self-Signed Certificate. 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 tiếng của các địa chỉ web được quét, cũng như thông tin về danh mục và danh tiếng của các tập tin được quét. • **Giám sát hoạt động ứng dụng**. Xem thông tin về hoạt động của các ứng dụng được cài đặt. Giám sát hoạt động ứng dụng sẽ 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 đó khỏi 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 phần mềm độc hại và kiểm tra tính toàn vẹn của ứng dụng. Quản trị viên có thể ẩn tác vụ khỏi 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.

Nếu biểu tượng ứng dụng trong khu vực thông báo trên thanh tác vụ bị ẩn, quản trị viên có vô hiệu hóa hiển thị giao diện ứng dụng trong chính sách.

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 phần mềm độc hại. Ứng dụng cũng sẽ tiếp tục sử dụng Kaspersky Security Network.

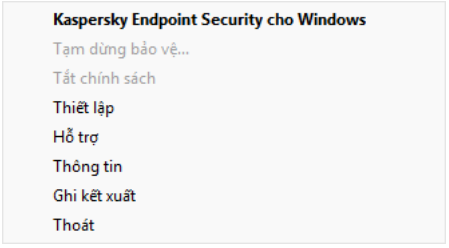
- **Tắt chính sách** / **Bật chính sách**. Tắt chính sách Kaspersky Security Center trên máy tính. Tất cả thiết lập của Kaspersky Endpoint Security đều có thể được cấu hình, bao gồm các thiết lập có khóa đóng trong chính sách (). Nếu chính sách bị tắt, ứng dụng sẽ yêu cầu mật khẩu để truy cập Kaspersky 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 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 của ứng dụng**.

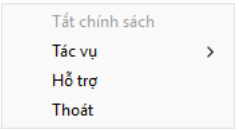
  - **Khôi phục cơ sở dữ liệu về phiên bản trước đây**.

  - **Quét toàn bộ**.

  - **Quét tùy chỉnh**.

- **Quét khu vực quan trọng**.
- **Cập nhật**.

- **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:

- **Simplified**. 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 chỉ hiển thị các thông báo yêu cầu người dùng thao tác phía trên biểu tượng ứng dụng.
- **Full**. 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.
- **Do not display user 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Giao diện**.

4. Trong mục **Tương tác với người dùng**, hãy cấu hình cách hiển thị giao diện ứng dụng:

   - **Hiển thị giao diện người dùng**. 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. Nếu cần, bạn có thể bật chức năng **Ẩn mục Giám sát hoạt động ứng dụng** để ẩn dữ liệu về hoạt động của ứng dụng trên máy tính, qua đó hạn chế quyền truy cập của người dùng vào công cụ Giám sát hoạt động ứng dụng.

   - **Hiển thị giao diện giản lược**. 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 chỉ hiển thị các thông báo yêu cầu người dùng thao tác phía trên biểu tượng ứng dụng.

   - **Không hiển thị giao diện người dùng**. 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.

5. Lưu các thay đổi của bạn.

Cách cấu hình chế độ hiển thị giao diện ứng dụng trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.

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** → **User Interaction**.

5. Trong mục **Visibility for users**, hãy cấu hình cách hiển thị giao diện ứng dụng:

   - **Display user interface**. Nếu chức năng này bị tắt, sẽ không có dấu hiệu nào cho thấy Kaspersky Endpoint Security đang hoạt động trên máy tính của người dùng. Biểu tượng trong khu vực thông báo của Windows và các thông báo không khả dụng.

   - **Simplified**. 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 chỉ hiển thị các thông báo yêu cầu người dùng thao tác phía trên biểu tượng ứng dụng.

   - **Full**. 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.

   - **Hide Application Activity Monitor section**. 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.

6. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Đang chuẩn bị ứng dụng để sử dụng

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 cơ sở dữ liệu và mô-đun ứng dụng* và *Quét phần mềm độc hại*.

  Phải thực hiện tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* để cập nhật khả 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 *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* được tạo tự động bởi trình hướng dẫn sử dụng nhanh Máy chủ quản trị. Để tạo tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*, hãy cài đặt Tiện ích quản lý của Kaspersky Endpoint Security cho Windows khi đang chạy Trình hướng dẫn.

  Tác vụ *Quét phần mềm độc hại* 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 phần mềm độc hại*.

  Cách tạo tác vụ Quét phần mềm độc hại trong Bảng điều khiển quản trị (MMC)

  1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Tasks**.

     Danh sách tác vụ sẽ mở.

  2. Nhấn vào **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 (14.2) → Quét phần mềm độc hại**.

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 chọn tùy chọn này, ứng dụng sẽ tự động cố gắng khử mã độc tập tin bị nhiễm được phát hiện. Nếu không thể khử mã độc, ứng dụng sẽ xóa 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 khử mã độc thất bại, 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.

- **Run only when the computer is idle**. Hoãn bắt đầu tác vụ 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. Tùy chọn lịch này cho phép bạn bảo tiết kiệm nguyên máy tính khi máy tính đang được sử dụng.

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 phần mềm độc hại*. 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

Hoàn tất 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 phần mềm độc hại sẽ được thực thi trên máy tính của người dùng theo lịch được quy định.

Cách tạo tác vụ Quét phần mềm độc hại trong Bảng điều khiển web

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

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **Add**.

   Trình hướng dẫn Tác vụ sẽ được bắt đầu.

3. Cấu hình các thiết lập của tác vụ:

   a. Trong danh sách thả xuống **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.

   b. Trong danh sách thả xuống **Task type**, hãy chọn **Malware Scan**.

   c. Trong trường **Task name**, nhập một mô tả ngắn, ví dụ như *Quét hàng tuần*.

   d. Trong phần **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. Chọn một tài khoản để chạy tác vụ. Theo mặc định, Kaspersky Endpoint Security khởi chạy tác vụ với quyền của tài khoản người dùng cục bộ.

6. Hoàn tất trình hướng dẫn.

   Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ.

7. 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.

8. Chọn hộp kiểm cạnh tác vụ.

9. Nhấn vào **Start**.

   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 phần mềm độc hại sẽ được thực thi trên máy tính của người dùng theo lịch được quy định.

- Tối ưu hóa hiệu năng của Kaspersky Endpoint Security.

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.

Mỗi thiết lập chính sách đều có thuộc tính ("ổ khóa"). Trạng thái của thuộc tính này quyết định liệu thiết lập đó có được truyền đến các thiết bị được quản lý trong nhóm quản trị hay không:

- Nếu "ổ khóa" mở () thì giá trị của thiết lập này sẽ không được truyền đến các thiết bị được quản lý. Bạn có thể chỉnh sửa thiết lập này trong giao diện cục bộ của ứng dụng. Các thiết lập như vậy được gọi là *được mở khóa*.

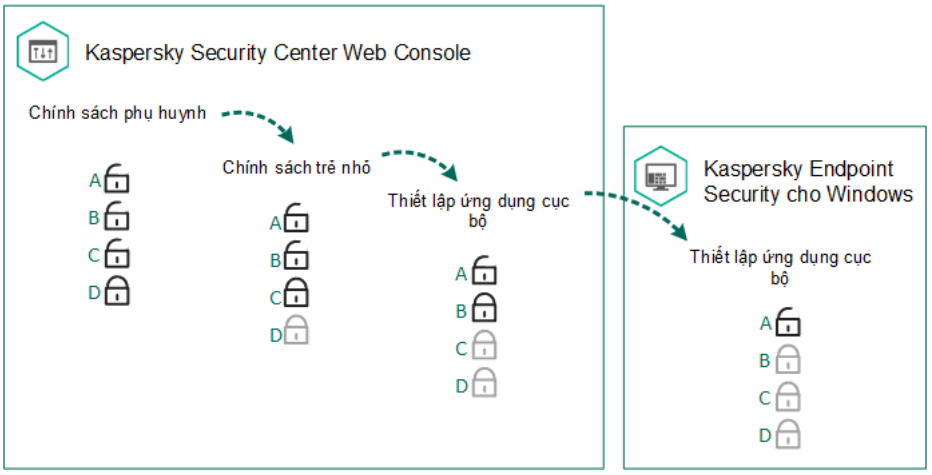
- Nếu "ổ khóa" đóng () thì giá trị của thiết lập này sẽ được truyền và áp dụng cho các thiết bị được quản lý. Các thiết lập như vậy được gọi là *bị khóa*. Không thể chỉnh sửa các thiết lập bị chặn trong giao diện cục bộ của ứng dụng.

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.

Kế thừa thiết lập

Các chính sách, giống như các nhóm quản trị, được sắp xếp theo cấp bậc. *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.

Theo mặc định, chính sách con sẽ kế thừa thiết lập từ chính sách cha. Nếu thiết lập trong chính sách cha có thuộc tính (ổ khóa" bị đóng), thì trong các chính sách con và thiết lập ứng dụng cục bộ, giá trị của thiết lập đó sẽ bị ghi đè theo chính sách cha và thiết lập sẽ bị khóa. Nếu cần, bạn có thể vô hiệu hóa việc kế thừa thiết lập từ chính sách cha. 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 cấu hình quyền truy cập thiết lập chính sách, hãy vào mục **Security** của cửa sổ thuộc tính của Máy chủ quản trị Kaspersky Security Center (theo mặc định, phần này bị ẩn trong giao diện bảng điều khiển).

Sửa đổi chính sách

Kaspersky Security Center theo dõi các thay đổi chính sách và tạo ra các bản sửa đổi. Một bản *sửa đổi* là một tập hợp các tham số đã được người dùng chỉnh sửa và lưu lại. Các bản sửa đổi cho phép bạn so sánh và hoàn tác các thay đổi đối với các thông số chính sách. Ngoài tập hợp các tham số đã được sửa đổi, bản sửa đổi còn bao gồm thông tin về người dùng đã thực hiện các thay đổi, thời gian, địa chỉ IP, chú thích của người dùng và các dữ liệu liên quan khác.

Để xem nhật ký sửa đổi, hãy mở thuộc tính chính sách và vào phần **Revision history**. Để biết thêm chi tiết về thao tác với bản sửa đổi, hãy tham khảo Trợ giúp của Kaspersky Security Center.

Tạo một chính sách

Khi tạo chính sách, trình hướng dẫn sẽ đề xuất các thiết lập liên quan đến chế độ đã chọn. Ví dụ: đối với chế độ Light Agent, bạn phải thêm Máy chủ bảo vệ (SVM). Khi sử dụng ứng dụng để bảo vệ máy chủ SQL, bạn phải thêm các loại trừ quét được định sẵn để đảm bảo hoạt động của máy chủ không bị ảnh hưởng. Trình hướng dẫn sẽ đề xuất các thiết lập chính sách liên quan sau khi chọn chế độ. Khi đó, bạn có thể chỉnh sửa các thiết lập này trong thuộc tính 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, hãy chọn thẻ **Policies**.
4. Nhấn vào **New policy**.
   Trình hướng dẫn Chính sách sẽ được bắt đầu.
5. Làm theo chỉ dẫn của Trình hướng dẫn Chính sách.

Bước 1. Chọn ứng dụng để tạo chính sách nhóm

Chọn ứng dụng **Kaspersky Endpoint Security for Windows (14.2)**.

Bước 2. Đặt tên cho chính sách nhóm

Nhập tên cho chính sách nhóm, ví dụ: *Chính sách cho văn phòng*.

Bạn cũng có thể tạo chính sách mới dựa trên các chính sách hiện có bằng Trình hướng dẫn chính sách. Để thực hiện như vậy, khi chỉ định tên chính sách nhóm, hãy chọn hộp kiểm **Use policy settings for an earlier version of the application**. Trình hướng dẫn cũng cho phép tạo chính sách Kaspersky Endpoint Security (KES) dựa trên chính sách của một giải pháp khác, ví dụ: Kaspersky Security for Windows Server (KSWS) hoặc Kaspersky Security for Virtualization Light Agent cho Windows

Bước 3. Tham gia Kaspersky Security Network

Vui lòng đọc và chấp nhận các điều khoản của Tuyên bố Kaspersky Security Network (KSN).

Bước 4. Chọn chế độ sử dụng ứng dụng trên máy tính

Tùy thuộc vào mục đích sử dụng Kaspersky Endpoint Security, bạn có thể cấu hình chính sách cho các chế độ ứng dụng sau:

- Chế độ tiêu chuẩn để bảo vệ máy chủ

Ở chế độ này, bạn có thể chọn cách cấu hình chính sách theo ý muốn:

- **Tạo một chính sách với 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.

- **Thay đổi thiết lập chính sách trong Trình hướng dẫn**. Phương pháp này cho phép quản lý các thiết lập chính sách từng bước bằng trình hướng dẫn. Bạn cũng có thể quản lý thiết lập chính sách bằng cách sử dụng tập tin cấu hình của ứng dụng (xem bước tiếp theo).

- Endpoint Detection and Response Agent để bảo vệ trước các mối đe dọa nâng cao và các cuộc tấn công nhắm mục tiêu.

  Endpoint Detection and Response Agent là một ứng dụng được cài đặt trên các máy trạm và máy chủ riêng lẻ trong cơ sở hạ tầng CNTT của tổ chức để hỗ trợ các giải pháp Detection and Response của Kaspersky. Bước tiếp theo, bạn cần chọn một giải pháp để tích hợp Tác nhân EDR.

- Light Agent để bảo vệ môi trường ảo.

  Để sử dụng ứng dụng ở chế độ Light Agent, bạn cần cấu hình kết nối với máy ảo SVM. Những thiết lập này là bắt buộc để ứng dụng hoạt động ở chế độ Light Agent.

Kaspersky Endpoint Security cung cấp một chính sách chung cho tất cả chế độ ứng dụng và các loại HĐH. Điều này có nghĩa là chính sách này bao gồm toàn bộ các thiết lập. Tuy nhiên, ứng dụng có thể bỏ qua một số thiết lập chính sách vì Kaspersky Endpoint Security được triển khai ở chế độ mà một số chức năng không khả dụng. Ví dụ: khi sử dụng ứng dụng ở chế độ Endpoint Detection and Response Agent, chỉ những thiết lập liên quan đến tích hợp với các giải pháp Kaspersky Detection and Response và tích hợp với KUMA mới khả dụng.

Bạn nên sử dụng các chính sách khác nhau cho các chế độ và loại hệ điều hành khác nhau.

Bước 5. Nhập thiết lập

Bước này khả dụng nếu bạn chọn cấu hình chính sách thủ công ở bước 4.

Bạn có thể tạo chính sách dựa trên thiết lập Kaspersky Endpoint Security từ tập tin cấu hình CFG. Trình hướng dẫn chính sách mới không hỗ trợ các tập tin cấu hình được mã hóa. Khi xuất tập tin cấu hình, hãy bỏ qua bước mã hóa tập tin.

Khi nhập tập tin cấu hình CFG ứng dụng, không phải tất cả các thiết lập chính sách đều có sẵn cho trình hướng dẫn. Ví dụ: các hồ sơ chính sách bị thiếu trong thiết lập ứng dụng. Nếu bạn muốn chuyển tất cả thiết lập và hồ sơ sang chính sách, bạn có thể nhập một chính sách khác từ tập tin KLP.

Khi nhập tập tin cấu hình, Kaspersky Endpoint Security sẽ không chuyển mật khẩu bộ chứa mã hóa. Nếu bạn sử dụng xác thực hai chiều khi kết nối với máy chủ, bạn cần phải chỉ định mật khẩu của bộ chứa mã hóa lại từ đầu.

Bước 6 - 10. Cấu hình thiết lập chính sách

> Bước này khả dụng nếu bạn chọn cấu hình chính sách thủ công ở bước 4.

Làm theo các bước sau để quản lý thiết lập chính sách.

Bước 11. Cấu hình khu vực tin tưởng

Cấu hình vùng tin tưởng. Bạn có thể thêm loại trừ quét được định sẵn và ứng dụng được tin tưởng. Các ứng dụng được tin tưởng và loại trừ quét được xác định trước giúp nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager. Điều này có nghĩa là bạn không cần thiết lập khu vực tin tưởng theo cách thủ công cho ứng dụng trên máy chủ. Các loại trừ quét được định sẵn và các ứng dụng được tin tưởng cũng có thể giúp bạn nhanh chóng cấu hình Kaspersky Endpoint Security ở chế độ Light Agent trong môi trường ảo Citrix và VMware.

Bước 12. Chọn trạng thái chính sách

- **Active**. Sau lần đồng bộ tiếp theo, chính sách sẽ được sử dụng làm chính sách hoạt động trên máy tính.

  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.

- **Inactive**. Chính sách sao lưu. Nếu cần thiết, một chính sách không hoạt động có thể được chuyển trạng thái thành hoạt động.

  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.

- **Out-of-office**. Chính sách này được kích hoạt khi máy tính rời khỏi mạng doanh nghiệp.

Hoàn tất trình hướng dẫn.

Cách tạo chính sách trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.

2. Nhấn vào **Add**.

   Trình hướng dẫn Chính sách sẽ được bắt đầu.

3. Chọn Kaspersky Endpoint Security và nhấn **Next**.

4. Vui lòng đọc và chấp nhận các điều khoản của Tuyên bố Kaspersky Security Network (KSN) và nhấn **Next**.

5. Chọn chế độ của ứng dụng:

   - Standard mode to protect workstations and servers
   - Endpoint Detection and Response Agent to protect against advanced threats and targeted attacks.

     Nếu chọn chế độ này, bạn có thể tạo chính sách để tích hợp máy tính với các giải pháp Kaspersky Detection and Response. Trình hướng dẫn sẽ nhắc bạn cấu hình tích hợp cho Kaspersky Managed Detection and Response rồi đến Kaspersky Anti Targeted Attack Platform (EDR).
   - Light Agent to protect virtual environments.

     Nếu bạn chọn chế độ này, ở bước tiếp theo, bạn phải cấu hình kết nối với Máy chủ bảo vệ (SVM). Những thiết lập này là bắt buộc để ứng dụng hoạt động ở chế độ Light Agent.

   Kaspersky Endpoint Security cung cấp một chính sách chung cho tất cả chế độ ứng dụng và các loại HĐH. Điều này có nghĩa là chính sách này bao gồm toàn bộ các thiết lập. Tuy nhiên, ứng dụng có thể bỏ qua một số thiết lập chính sách vì Kaspersky Endpoint Security được triển khai ở chế độ mà một số chức năng không khả dụng. Ví dụ: khi sử dụng ứng dụng ở chế độ Endpoint Detection and Response Agent, chỉ những thiết lập liên quan đến tích hợp với các giải pháp Kaspersky Detection and Response và tích hợp với KUMA mới khả dụng.

   > Bạn nên sử dụng các chính sách khác nhau cho các chế độ và loại hệ điều hành khác nhau.

6. Cấu hình vùng tin tưởng. Bạn có thể thêm loại trừ quét được định sẵn và ứng dụng được tin tưởng. Các ứng dụng được tin tưởng và loại trừ quét được xác định trước giúp nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager. Điều này có nghĩa là bạn không cần thiết lập khu vực tin tưởng theo cách thủ công cho ứng dụng trên máy chủ. Các loại trừ quét được định sẵn và các ứng dụng được tin tưởng cũng có thể giúp bạn nhanh chóng cấu hình Kaspersky Endpoint Security ở chế độ Light Agent trong môi trường ảo Citrix và VMware.

7. Trên thẻ **General**, bạn có thể thực hiện những hành động sau:

   - Thay đổi tên chính sách.
   - Chọn trạng thái chính sách:

     - **Active**. Sau lần đồng bộ tiếp theo, chính sách sẽ được sử dụng làm chính sách hoạt động trên máy tính.

       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.
     - **Inactive**. Chính sách sao lưu. Nếu cần thiết, một chính sách không hoạt động có thể được chuyển trạng thái thành hoạt động.

       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.
     - **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.

8. Trên thẻ **Application settings**, bạn có thể cấu hình Cấu hình chính sách Kaspersky Endpoint Security.

9. Hoàn tất trình hướng dẫn.

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.

Xuất và nhập chính sách

Kaspersky Endpoint Security cho phép xuất chính sách cùng với các thiết lập và cấu hình ra tập tin KLP. Sau đó, bạn có thể sử dụng chức năng xuất/nhập chính sách để sao lưu các chính sách, chuyển các chính sách sang máy chủ khác hoặc là để chuyển các chính sách từ Kaspersky Security Center Windows sang Kaspersky Security Center Linux. Để biết chi tiết về việc quản lý chính sách, vui lòng tham khảo Trợ giúp của Kaspersky Security Center.

Cách xuất và nhập 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, mở thư mục với tên của nhóm quản trị chứa máy khách liên quan.

3. Trong không gian làm việc, hãy chọn thẻ **Policies**.

4. Để xuất chính sách:

   a. Nhấn vào chính sách bạn muốn xuất.

   b. Nhấn vào liên kết **Export policy to file** trong phần bên phải của cửa sổ.

   c. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin KLP mà bạn muốn xuất chính sách rồi chọn thư mục để lưu tập tin này.

   d. Lưu tập tin.

5. Để nhập chính sách:

   a. Nhấn vào **Import policy from file**.

   b. Trong cửa sổ mở ra, hãy chọn tập tin chính sách KLP mà bạn muốn nhập.

   c. Mở tập tin.

   Thao tác này sẽ thêm một chính sách mới có trạng thái *Inactive policy*.

Cách xuất và nhập chính sách trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
2. Để xuất chính sách:

   a. Chọn hộp kiểm cạnh chính sách mà bạn muốn xuất.

   b. Nhấn nút **Export**.

   c. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin KLP mà bạn muốn xuất chính sách rồi chọn thư mục để lưu tập tin này.

   d. Lưu tập tin.

3. Để nhập chính sách:

   a. Nhấn vào **Import**.

   b. Chọn tập tin chính sách KLP mà bạn muốn nhập.

   c. Sau khi chính sách được xử lý thành công, hãy chọn nhóm quản trị mà bạn muốn áp dụng chính sách đó.

   d. Nhấn vào nút **Complete** để hoàn tất việc nhập chính sách.

   Thao tác này sẽ thêm một chính sách mới có trạng thái *Inactive*.

Chỉ báo mức độ bảo mật

Chỉ báo mức độ bảo mật được hiển thị trên đầu cửa sổ thuộc tính. 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.

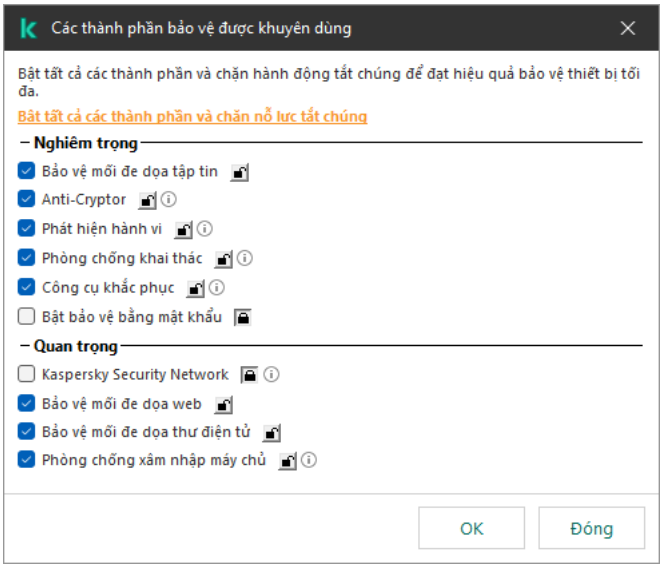
- Công cụ khắc phục.
- Bảo vệ các dịch vụ ứng dụng trước hoạt động quản lý bên ngoài.

- **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.
  - Bảo vệ bằng mật khẩu.

- **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 khuyên dùng** 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.

Sau khi nâng cấp ứng dụng, chỉ báo mức độ bảo vệ có thể cho biết mức độ bảo vệ thấp hơn so với trước khi nâng cấp. Điều này là do phiên bản mới hơn của ứng dụng ra mắt các thành phần hoặc tính năng mới quan trọng đối với bảo mật máy tính. Sau khi nâng cấp ứng dụng, bạn cần quản lý các thiết lập mới để đảm bảo mức độ bảo vệ vẫn cao.



Chỉ báo mức độ bảo mật của chính sách

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 phần mềm độc hại**. 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 phần mềm độc hại* 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.
- **Thay đổi thành phần ứng dụng**. Kaspersky Endpoint Security sẽ cài đặt hoặc gỡ bỏ các thành phần trên máy khách theo danh sách các thành phần được quy định trong cấu hình tác vụ. Thành phần Bảo vệ mối 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 cơ sở dữ liệu và mô-đun ứng dụng**. Kaspersky Endpoint Security sẽ cập nhật các cơ sở dữ liệu và mô-đun ứng dụng. Tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* 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 của ứng dụng**. 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.

Nếu ứng dụng đang hoạt động như một phần của giải pháp Endpoint Detection and Response của Kaspersky, bạn có thể chạy các tác vụ bổ sung như hành động phản hồi phát hiện (responses). Ví dụ: bạn có thể chấm dứt các tiến trình từ xa bằng cách sử dụng tác vụ *Chấm dứt tiến trình*.

Các tác vụ chỉ được thực hiện trên máy tính nếu Kaspersky Endpoint Security đang chạy.

Tạo một tác vụ

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 **Tasks** trong cây Bảng điều khiển quản trị.
3. Nhấn vào **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

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Tasks**.
   Danh sách tác vụ sẽ mở.
2. Nhấn vào **Add**.
   Trình hướng dẫn Tác vụ sẽ được bắt đầu.
3. Cấu hình các thiết lập của tác vụ:
   a. Trong danh sách thả xuống **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.
   b. Trong danh sách thả xuống **Task type**, 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 **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. Chọn một tài khoản để chạy tác vụ. Theo mặc định, Kaspersky Endpoint Security khởi chạy tác vụ với quyền của tài khoản người dùng cục bộ.

6. Hoàn tất 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 **Start**. 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 → 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.

Quản lý quyền 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 **Security** 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Tác vụ cục bộ → Quản lý tác vụ**.

4. Cấu hình chế độ quản lý tác vụ (xem bảng bên dưới).

5. 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 thẻ **Asset management → Policies**.

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 → User Interaction**.

5. Trong mục **Permitted actions**, hãy cấu hình chế độ quản lý tác vụ (xem bảng bên dưới).

6. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cấu hình Quản lý tác vụ

Tham số	Mô tả
Access to local tasks	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. Nếu bỏ chọn hộp kiểm này, các tác vụ cục bộ sẽ bị ẩn trong giao diện ứng dụng. 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. 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.
View group tasks	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. Khi hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ hiển thị một danh sách tác vụ trống.
Manage group tasks	Nếu hộp kiểm được chọn, người dùng có thể khởi chạy và dừng các tác vụ nhóm được chỉ định trong bảng điều khiển 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 giản lược. 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 bảng điều khiển Kaspersky Security Center.

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, hãy chọn thẻ **Devices**.

4. Nhấn đúp để mở cửa sổ thuộc tính máy tính.

5. Trong cửa sổ thuộc tính máy tính, chọn phần **Applications**.

6. Trong danh sách các ứng dụng Kaspersky được cài đặt trên máy tính, hãy chọn **Kaspersky Endpoint Security cho Windows (14.2)** và nhấn đúp để mở thuộc tính ứng dụng.

7. Trong mục **Thiết lập tổng quát**, hãy cấu hình Kaspersky Endpoint Security cũng như Các báo cáo và lưu trữ.

   Các phần còn lại trong cửa sổ thuộc tính ứng dụng là tiêu chuẩn đối với 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**.

8. 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 **Asset management** → **Assets (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 14.2**.
   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)

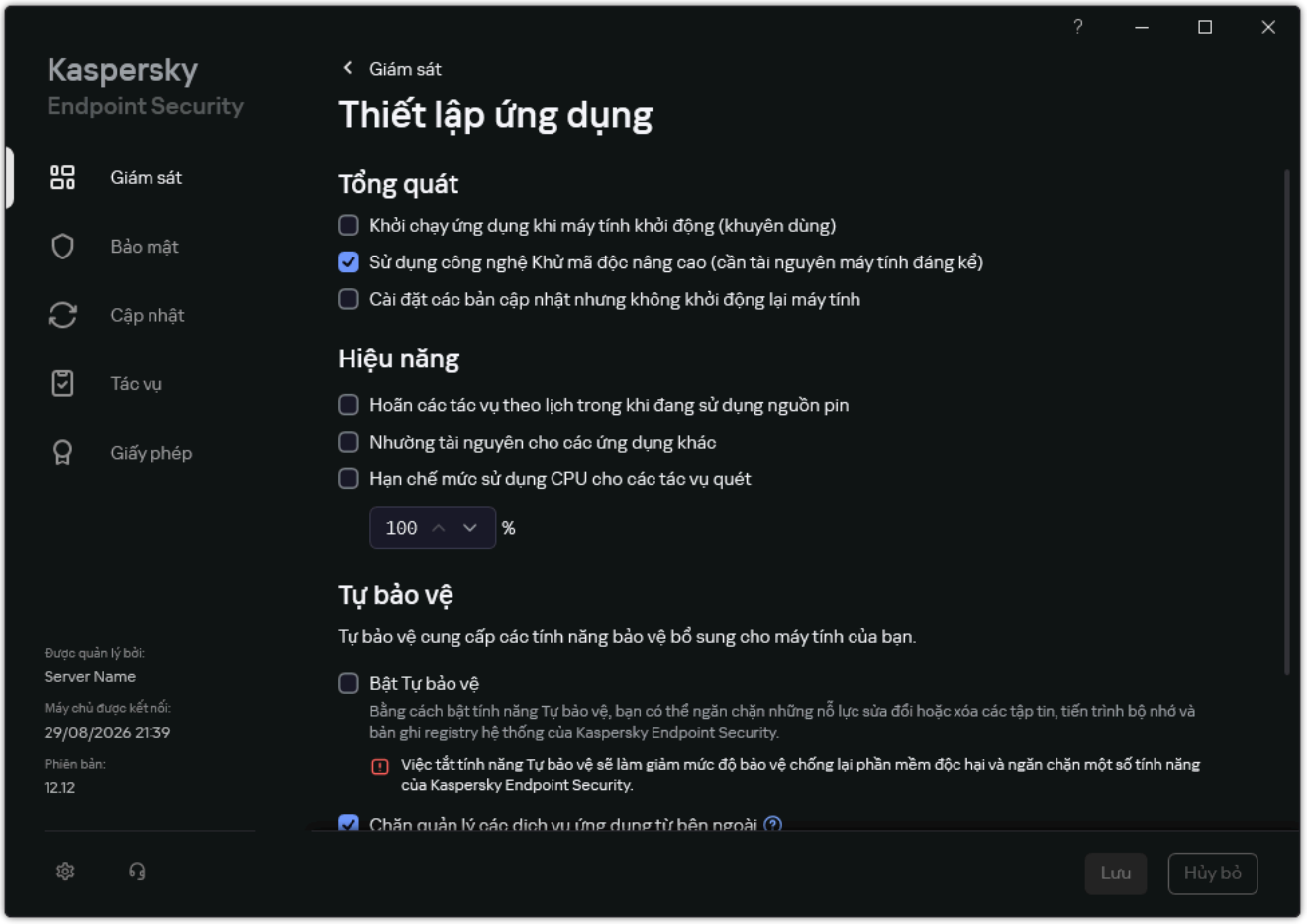
1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Thiết lập ứng dụng**.
4. Sử dụng hộp kiểm **Khởi chạy ứng dụng khi máy tính khởi động (khuyên dùng)** để cấu hình khởi chạy ứng dụng.
5. 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 **Asset management** → **Policies**.
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** → **User Interaction**.
5. Sử dụng hộp kiểm **Start Kaspersky Endpoint Security on computer startup (recommended)** 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**.



Thiết lập Kaspersky Endpoint Security cho Windows

3. Sử dụng hộp kiểm **Khởi chạy ứng dụng khi máy tính khởi động (khuyên dùng)** để cấu hình 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, hãy chọn thẻ **Devices**.

4. Nhấn đúp để mở cửa sổ thuộc tính máy tính.

5. Trong cửa sổ thuộc tính máy tính, chọn phần **Applications**.

6. Trong danh sách các ứng dụng Kaspersky được cài đặt trên máy tính, hãy chọn **Kaspersky Endpoint Security cho Windows (14.2)** và nhấn đúp để mở thuộc tính ứng dụng.

7. Thực hiện một trong các thao tác 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 **Asset management → Assets (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 **Applications**.

4. Chọn hộp kiểm đối diện **Kaspersky Endpoint Security cho Windows**.

5. Nhấn vào nút **Bắt đầu** hoặc **Dừng**.

Cách khởi chạy hoặc dừng Kaspersky Endpoint Security từ dòng lệnh

1. Chạy trình thông dịch dòng lệnh (cmd.exe) với tư cách quản trị viên.

2. Vào thư mục chứa tập tin thực thi klpsm.exe.

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`.

Để dừng ứng dụng từ dòng lệnh, hãy cho phép quản lý các dịch vụ hệ thống từ bên ngoài.



Khởi chạy và dừng ứng dụng từ dòng lệnh

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).

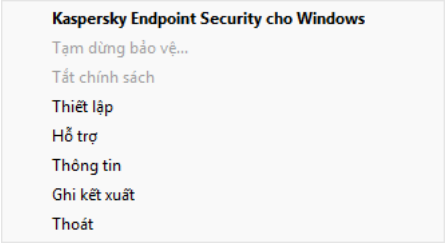
   Mục menu ngữ cảnh này khả dụng nếu Bảo vệ bằng mật khẩu được bật.

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.
- Thực hiện cài đặt từ xa Kaspersky Endpoint Security thông qua Kaspersky Security Center với các cấu hình được thiết lập sẵn.
- Chuyển thiết lập ứng dụng sang một chính sách.
- Di chuyển cấu hình của Kaspersky Endpoint Security từ một máy tính sang máy tính khác (xem các hướng dẫn ở bên dưới).

Xuất tập tin cấu hình

Kể từ Kaspersky Endpoint Security phiên bản 14.2, có thể mã hóa tập tin cấu hình được xuất. Vì tập tin cấu hình có thể chứa thông tin đăng nhập, bạn nên mã hóa tập tin cấu hình. Bạn không thể chỉnh sửa tập tin được mã hóa. Mọi nỗ lực sửa đổi tập tin cấu hình đều làm hỏng tập tin đó.

Mã hóa tập tin cấu hình có các tính năng đặc biệt sau:

- Kaspersky Endpoint Security chỉ cho phép nhập các tập tin được mã hóa thông qua giao diện người dùng của ứng dụng hoặc trên dòng lệnh. Bạn không thể sử dụng tập tin như vậy trong bảng điều khiển Kaspersky Security Center để cấu hình chính sách hoặc cài đặt ứng dụng từ xa. Nếu bạn định thêm tập tin này vào chính sách hoặc gói cài đặt, hãy bỏ qua bước mã hóa tập tin.
- Không thể khôi phục mật khẩu của một tập tin đã được mã hóa.
- Các phiên bản Kaspersky Endpoint Security cũ hơn phiên bản 14.1 không hỗ trợ nhập tập tin cấu hình được mã hóa. Nếu bạn định nhập tập tin vào phiên bản ứng dụng cũ hơn, hãy bỏ qua bước mã hóa tập tin.

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. Để lưu tập tin cấu hình, bạn phải bật Bảo vệ bằng mật khẩu. Người dùng phải có quyền **Xuất thiết lập**.
5. 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.

6. Nếu cần, hãy bật công tắc bật/tắt **Mã hóa tập tin được xuất** và nhập mật khẩu mã hóa cho tập tin cấu hình.

   Lưu mật khẩu vào nơi an toàn. Không thể khôi phục mật khẩu này.

7. Lưu tập tin.

Kết quả là ứng dụng sẽ tạo ra một tập tin cấu hình.

Nhập tập tin cấu hình

Khi nhập tập tin cấu hình, Kaspersky Endpoint Security sẽ không chuyển mật khẩu bộ chứa mã hóa. Nếu bạn sử dụng xác thực hai chiều khi kết nối với máy chủ, bạn cần phải chỉ định mật khẩu của bộ chứa mã hóa lại từ đầu.

Để nhập cấu hình của Kaspersky Endpoint Security từ một tập tin thiết lập:

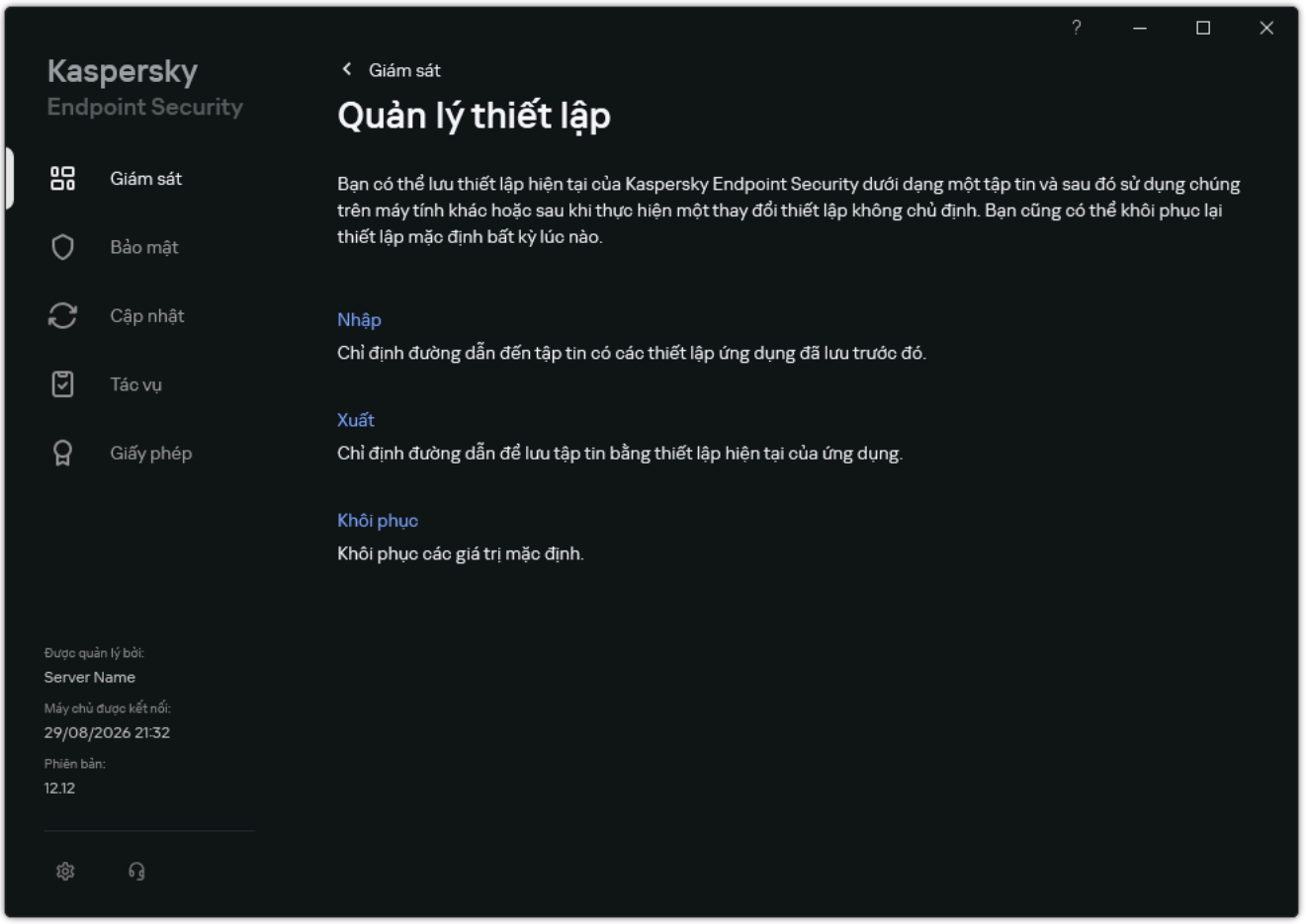
1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát → Quản lý thiết lập**.
3. Nhấn vào **Nhập**.
4. Trong cửa sổ mở ra, hãy nhập đường dẫn đến tập tin cấu hình.

5. Nếu tập tin cấu hình được mã hóa, hãy nhập mật khẩu mà bạn đã chỉ định khi xuất tập tin.

> Nếu quên mật khẩu mã hóa của tập tin cấu hình, bạn không thể khôi phục mật khẩu. Trong trường hợp này, bạn cần lặp lại các bước xuất tập tin cấu hình.

6. Mở tập tin.

Tất cả giá trị của cấu hình Kaspersky Endpoint Security sẽ được đặt theo tập tin thiết lập được chọn.



Quản lý thiết lập ứng dụng

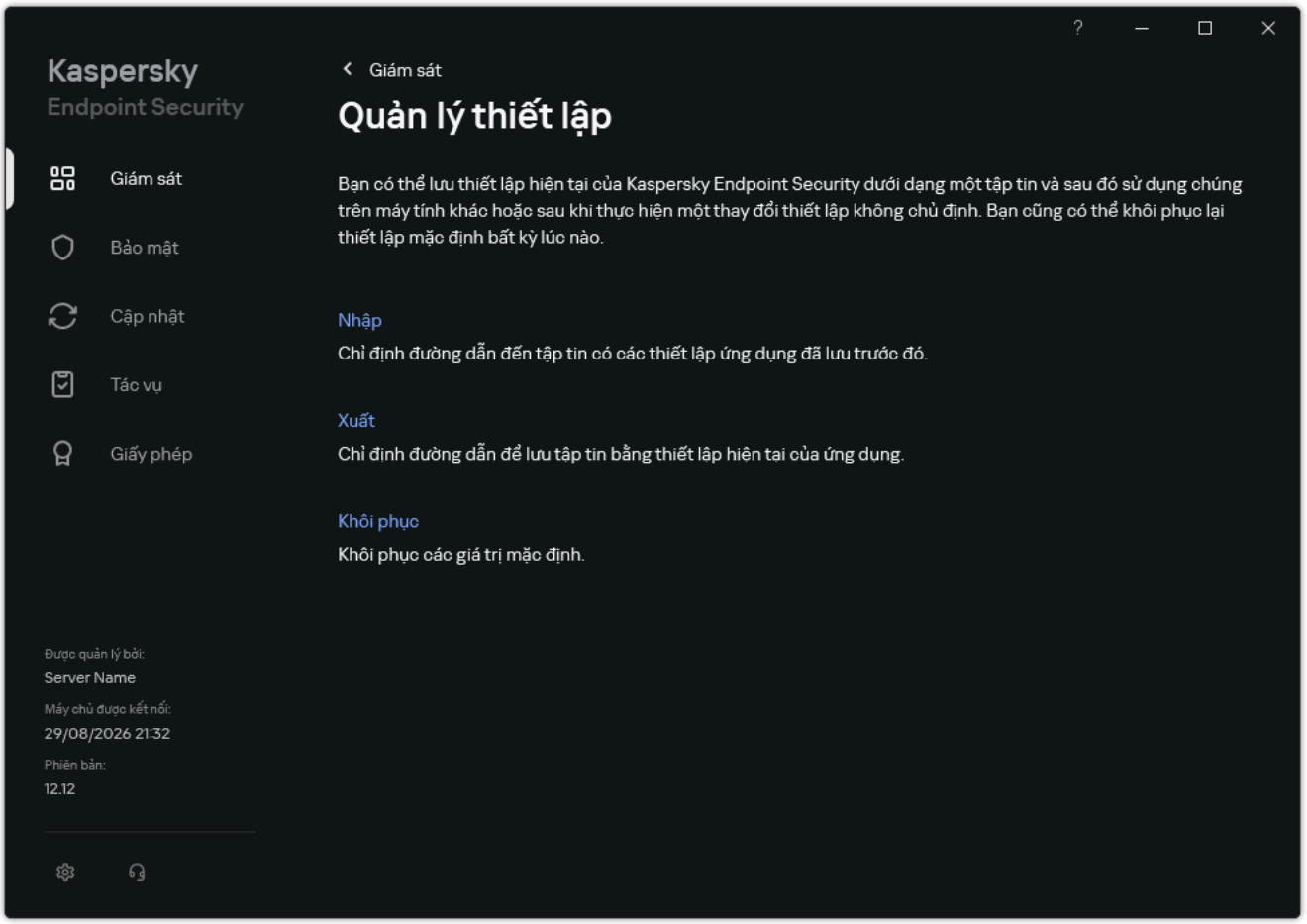
Khôi phục các thiết lập mặc định của ứng dụng

Bạn có thể khôi phục thiết lập ứng dụng theo khuyến nghị của Kaspersky bất kỳ lúc nào. Khi thiết lập được khôi phục, mức độ bảo mật **Khuyên 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.



Quản lý thiết lập ứng dụng

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 bọn tội phạm để phá hoại máy tính hoặc dữ liệu cá nhân của bạn.

Sử dụng chế độ tiết kiệm năng lượng

Mức tiêu thụ năng lượng bởi ứng dụng là một cân nhắc chính cho các máy tính lưu động. Các tác vụ được lập lịch của Kaspersky Endpoint Security thường sử dụng khá nhiều tài nguyên. Khi máy tính đang chạy bằng pin, bạn có thể sử dụng chế độ tiết kiệm năng lượng để tiêu thụ ít công suất hơn.

Trong chế độ tiết kiệm năng lượng, các tác vụ được lập lịch sau sẽ tự động được hoãn:

- Tác vụ 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 khi quét máy tính có thể làm tăng mức tải cho CPU và các hệ thống con của ổ cứng. 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 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 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 mã độc nâng cao. Để khử mã độc tình trạng nhiễm mã độc hiện hoạt trên một máy chủ, hãy bật công nghệ Khử mã độc nâng cao cho máy chủ và khởi chạy một tác vụ nhóm *Quét phần mềm độc hại* vào thời điểm thuận lợi cho những người dùng máy chủ.

Bật hoặc tắt chế độ tiết kiệm năng lượng

Chế độ tiết kiệm pin là một chức năng giúp giảm tải tài nguyên của máy tính xách tay và kéo dài thời lượng pin mà không ảnh hưởng đáng kể đến mức độ bảo mật. Trong chế độ tiết kiệm pin, ứng dụng sẽ hạn chế việc chạy các tác vụ theo lịch. Nhờ đó, chế độ tiết kiệm pin đảm bảo sự cân bằng giữa mức độ bảo mật và thời lượng pin của máy tính xách tay.

Khi chế độ tiết kiệm điện 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:

- *Quét toàn bộ*.
- *Quét khu vực quan trọng*.
- *Quét tùy chỉnh*.
- *Kiểm tra tính toàn vẹn của ứng dụng*.
- *Quét IOC*.
- *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* (chỉ áp dụng cho các bản vá)

Ứng dụng chỉ bỏ qua các bản cập nhật cơ sở dữ liệu theo lịch khi máy tính xách tay đang chạy bằng pin và mức pin dưới 30% (giá trị mặc định). Bạn có thể thay đổi mức sạc pin tối thiểu bằng cách chỉnh sửa registry. Tại mức tối thiểu đó, ứng dụng bắt đầu bỏ qua các bản cập nhật cơ sở dữ liệu chống virus đã lên lịch (xem hướng dẫn bên dưới). Trong tất cả các trường hợp khác, Kaspersky Endpoint Security sẽ cập nhật cơ sở dữ liệu theo lịch, bất kể máy tính xách tay đang cắm nguồn hay chạy bằng pin, hoặc ứng dụng có đang ở chế độ tiết kiệm pin hay không.

Cách bật hoặc tắt chế độ tiết kiệm năng lượng trong Bảng điều khiển quản trị (MMC)

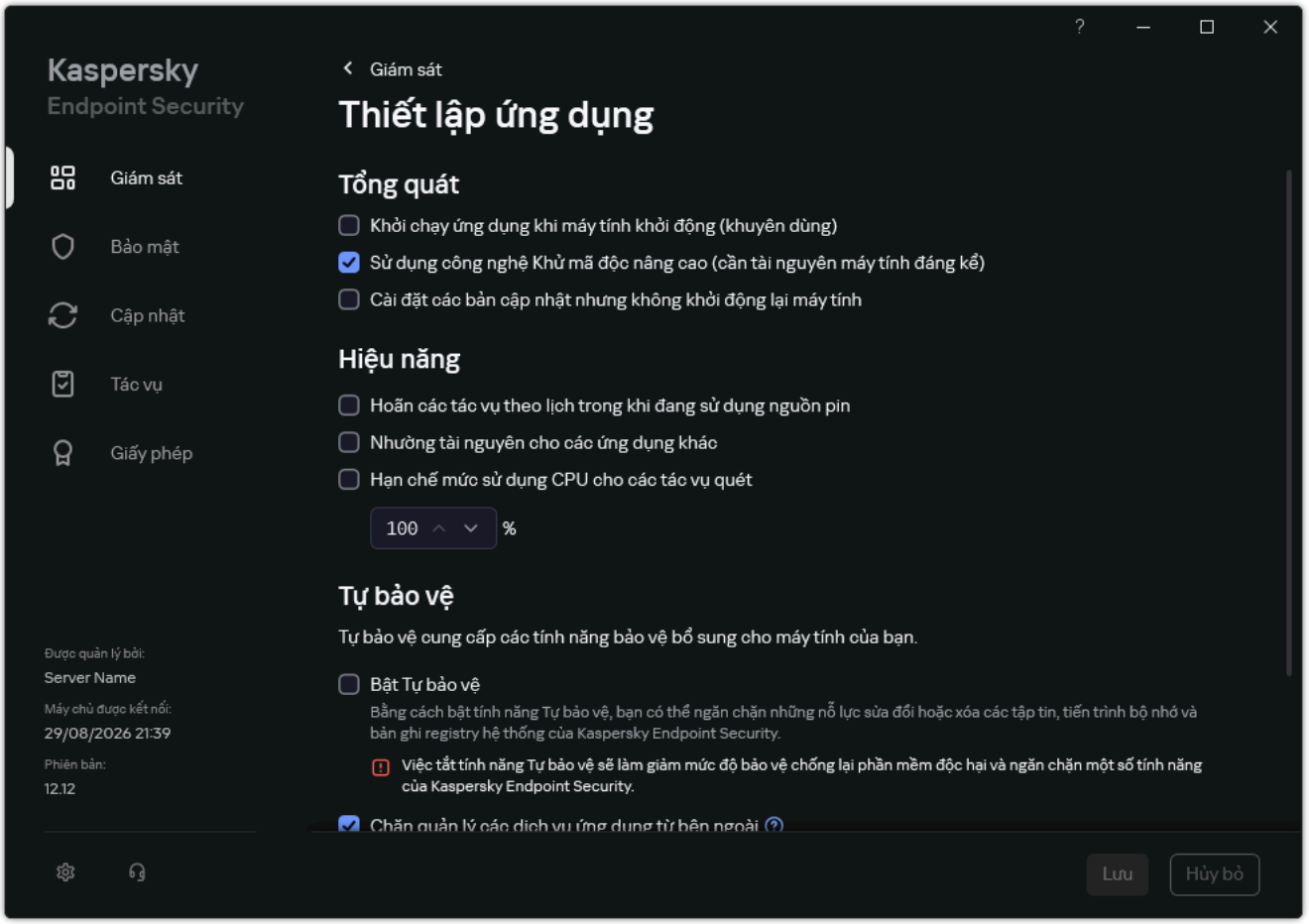
1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Thiết lập ứng dụng**.
5. Trong mục **Hiệu năng**, hãy sử 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.
6. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật hoặc tắt chế độ tiết kiệm năng lượng trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.
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** → **Performance**.
5. Trong mục **Postpone or skip scheduled tasks while running on battery power**, hãy sử dụng hộp kiểm **Postpone or skip scheduled tasks while running on battery power (depends on OS)** để bật hoặc tắt chế độ tiết kiệm pin.
6. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật hoặc tắt chế độ tiết kiệm năng lượng 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**.



Thiết lập Kaspersky Endpoint Security cho Windows

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.
4. Lưu các thay đổi của bạn.

Cách thay đổi mức sạc tối thiểu, và tại mức đó ứng dụng bắt đầu bỏ qua các bản cập nhật cơ sở dữ liệu chống virus đã lên lịch

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.14.2\environment]`
   - Đối với hệ điều hành 32-bit:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES.14.2\environment]`
3. Mở `UpdaterAccumulatorThreshold` để chỉnh sửa.
4. Chỉ định mức sạc tối thiểu, và tại mức đó ứng dụng bắt đầu bỏ qua các bản cập nhật cơ sở dữ liệu chống virus đã lên lịch.

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 cấu hình để nhường tài nguyên cho các ứng dụng khác.

Cách bật hoặc tắt nhường tài nguyên cho các ứng dụng khác trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Thiết lập ứng dụng**.
4. 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.
5. Lưu các thay đổi của bạn.

Cách bật hoặc tắt nhường tài nguyên cho các ứng dụng khác trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Policies**.
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** → **Performance**.

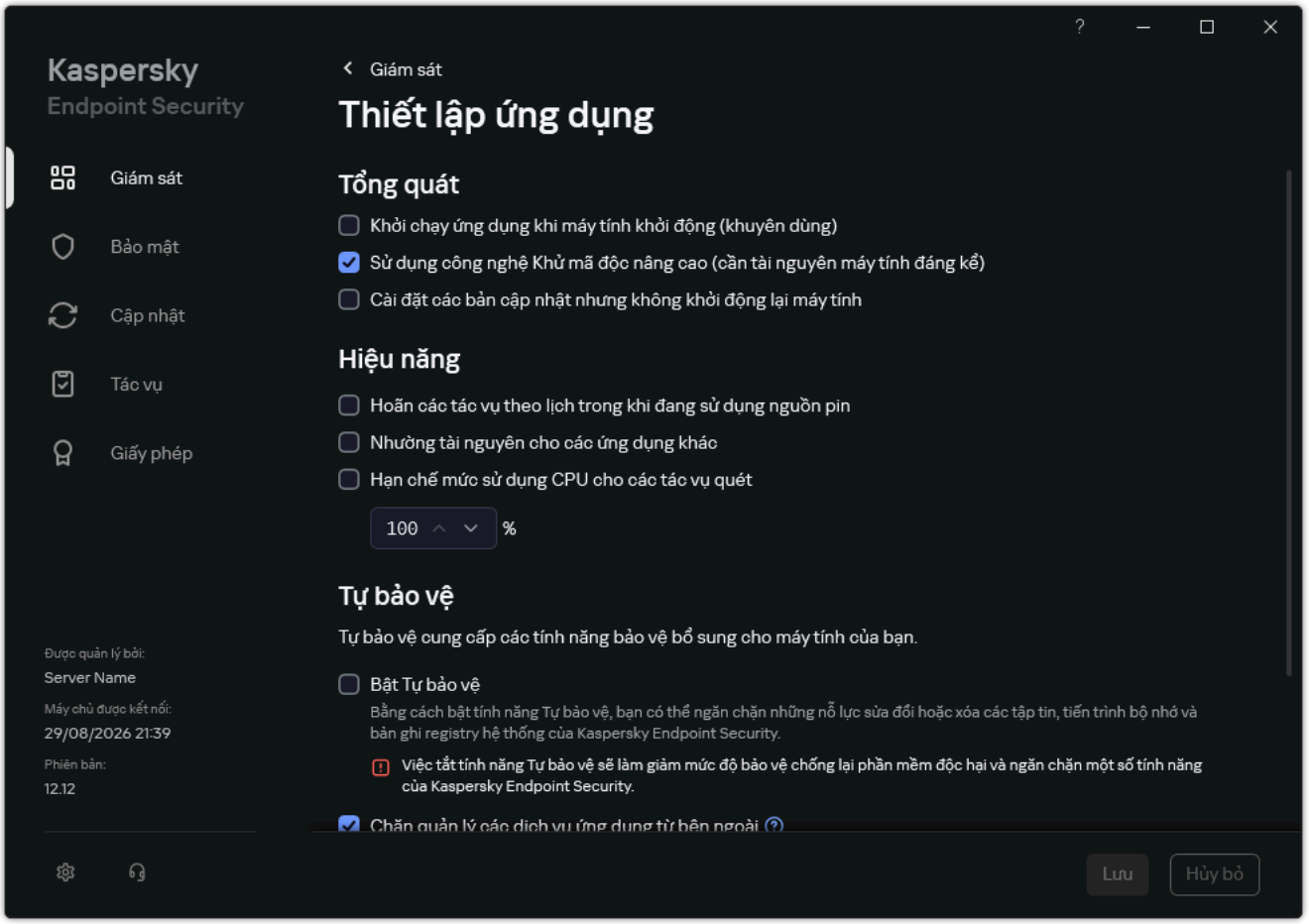
5. Trong mục **Yield resources to other applications**, hãy sử dụng công tắc bật/tắt **Yield resources to other applications** để bật hoặc tắt việc nhường tài nguyên cho các ứng dụng khác.

6. Lưu các thay đổi của bạn.

Cách bật hoặc tắt nhường tài nguyên cho các ứng dụng khác 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**.



Thiết lập Kaspersky Endpoint Security cho Windows

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. Để biết thêm thông tin về cách xử lý các sự cố hiệu năng máy tính, vui lòng tham khảo Cơ sở tri thức hỗ trợ kỹ thuật.

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 phần mềm độc hại trên máy trạm

Bạn nên bật Quét trong nền để đối với tác vụ Quét phần mềm độc hại 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 phần mềm độc hại 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 phần mềm độc hại* phù hợp theo các khuyến nghị sau:

1. Đặt giới hạn mức sử dụng tài nguyên CPU trong khi quét máy tính.

   Bạn có thể giới hạn mức sử dụng CPU khi chạy tác vụ *Quét phần mềm độc hại*. Để thực hiện, trong thiết lập ứng dụng, hãy chỉ định phần trăm mức tải CPU tối đa cho tất cả các lõi có thể được sử dụng trong khi quét máy tính. Làm thậy có thể làm tăng thời gian quét máy tính của bạn.

2. 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 ngoài giờ làm việc, bạn có thể bật chức 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.

   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.

3. Xác định phạm vi quét.

Chọn các đối tượng sau để quét (bộ phạm vi quét tối thiểu):

- Bộ nhớ kernel
- Tiến trình đang chạy và Các đối tượng khởi động
- Sector khởi động
- %systemroot% (không bao gồm các thư mục con)
- %systemroot%\System (không bao gồm các thư mục con)
- %systemroot%\System32 (không bao gồm các thư mục con)
- %systemroot%\System32\drivers (không bao gồm các thư mục con)
- %systemroot%\SysWOW64 (không bao gồm các thư mục con)
- %systemroot%\SysWOW64\drivers (không bao gồm các thư mục con)

4. 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 tác vụ 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 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 tác vụ 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.

5. 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.

6. Vô hiệu hóa khởi chạy đồng thời nhiều tác vụ quét.

   Kaspersky Endpoint Security sẽ xếp hàng các tác vụ quét mới nếu quá trình quét hiện tại tiếp tục. Điều này giúp tối ưu hóa mức tải trên máy tính.

Quét phần mềm độc hại trên máy chủ

Cấu hình tác vụ *Quét phần mềm độc hại* theo các khuyến nghị sau:

1. Đặt giới hạn mức sử dụng tài nguyên CPU trong khi quét máy tính.

   Bạn có thể giới hạn mức sử dụng CPU khi chạy tác vụ *Quét phần mềm độc hại*. Để thực hiện, trong thiết lập ứng dụng, hãy chỉ định phần trăm mức tải CPU tối đa cho tất cả các lõi có thể được sử dụng trong khi quét máy tính. Làm thậy có thể làm tăng thời gian quét máy tính của bạn.

2. 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.

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 tác vụ 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 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 tác vụ 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.

5. Vô hiệu hóa khởi chạy đồng thời nhiều tác vụ quét.

   Kaspersky Endpoint Security sẽ xếp hàng các tác vụ quét mới nếu quá trình quét hiện tại tiếp tục. Điều này giúp tối ưu hóa mức tải trên 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 tiếng của các địa chỉ web được quét, cũng như thông tin về danh mục và danh tiếng của các tập tin 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 Kaspersky Private Security Network.

   Kaspersky Private Security Network (KPSN) 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 và truy cập các dữ liệu thống kê khác mà không cần gửi dữ liệu cho Kaspersky 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.

Quét phần mềm độc hại

Quét phần mềm độc hại là tác vụ 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 thiết lập 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
- 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 của ứng dụng

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 có vai trò 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 thiết lập 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 được định sẵn sau: *Quét toàn bộ*, *Quét khu vực quan trọng*, *Quét tùy chỉnh*. Nếu tổ chức của bạn đã triển khai hệ thống quản trị Kaspersky Security Center, bạn có thể tạo *Quét phần mềm độc hại* và cấu hình tác vụ quét.

Cách chạy tác vụ quét trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Tasks**.

3. Chọn một tác vụ quét và nhấn đúp để mở các thuộc tính tác vụ.

   Nếu cần, hãy tạo một tác vụ *Quét phần mềm độc hại*.

4. Trong cửa sổ thuộc tính tác vụ, hãy chọn mục **Thiết lập**.

5. Cấu hình tác vụ quét (xem bảng bên dưới).

   Nếu cần, hãy cấu hình lịch tác vụ quét.

6. Lưu các thay đổi của bạn.

7. 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 tác vụ quét trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **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 tác vụ quét trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Tác vụ**.

2. Trong danh sách tác vụ, hãy chọn tác vụ quét và nhấn vào ⚙.

> 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.

> Trong giao diện ứng dụng, bạn chỉ có thể cấu hình các tác vụ quét cục bộ: *Quét toàn bộ*, *Quét khu vực quan trọng*, *Quét tùy chỉnh*. Không thể cấu hình các tác vụ nhóm được thêm qua Bảng điều khiển Kaspersky Security Center trong giao diện ứng dụng. Nút ⚙ không hiển thị đối với các tác vụ nhóm.

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**.

Để tối ưu hóa hiệu năng của Kaspersky Endpoint Security trong quá trình quét máy tính, bạn có thể quản lý các thiết lập nâng cao của tác vụ *Quét toàn bộ* và giới hạn việc sử dụng tài nguyên CPU.

Trong Kaspersky Security Center, bạn cũng có thể sử dụng tác vụ *Quét trong nền* thay vì tác vụ *Quét toàn bộ* để tối ưu hóa hiệu năng của ứng dụng. Việc này sẽ không ảnh hưởng đến mức độ bảo mật của máy tính. Không thể cấu hình tác vụ quét trong nền.

Kết quả là Kaspersky Endpoint Security sẽ quét máy tính và nếu phát hiện mối đe dọa, ứng dụng sẽ thực thi hành động được cấu hình trong thiết lập ứng dụng. Thông thường, ứng dụng sẽ cố gắng khử mã độc các tập tin bị nhiễm. Kết quả là các tập tin bị nhiễm có thể nhận được các trạng thái sau:

- **Được hoãn lại**. Không thể khử mã độc tập tin bị nhiễm. Ứng dụng sẽ xóa tập tin bị nhiễm mã độc sau khi khởi động lại máy tính.
- **Đã tạo bản ghi**. Không thể khử mã độc tập tin bị nhiễm. Ứng dụng thêm thông tin về các tập tin bị nhiễm mã độc được phát hiện vào danh sách các mối đe dọa hiện hoạt.
- **Ghi không được hỗ trợ** hoặc **Lỗi ghi**. Không thể khử mã độc tập tin bị nhiễm. Ứng dụng này không có quyền ghi.
- **Đã xử lý**. Ứng dụng đã phát hiện một tập tin bị nhiễm mã độc trước đó. Ứng dụng sẽ khử mã độc hoặc xóa tập tin bị nhiễm mã độc sau khi khởi động lại máy tính.

Cấu hình quét

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 *mức độ bảo mật*: • **Cao**. Kaspersky Endpoint Security sẽ quét tất cả các loại tập tin. Khi quét các tập tin hỗn hợp, ứng dụng sẽ quét các tập tin nén, gói phân phối, tập tin định dạng văn phòng, nhưng không quét các tập tin nén được bảo vệ bằng mật khẩu. Khi thiết lập mức độ bảo mật này, ứng dụng sẽ sử dụng phân tích hành vi với mức độ chi tiết **Quét sâu**. • **Khuyên dùng**. Kaspersky Endpoint Security sẽ quét tất cả các loại tập tin. Khi quét các tập tin hỗn hợp, ứng dụng sẽ quét các tập tin nén, gói phân phối, tập tin định dạng văn phòng, nhưng không quét các tập tin nén được bảo vệ bằng mật khẩu. Khi thiết lập mức độ bảo mật này, ứng dụng sẽ sử dụng phân tích hành vi với mức độ chi tiết **Quét vừa**. • **Thấp**. Kaspersky Endpoint Security chỉ quét các định dạng tập tin được chỉ định. Khi quét các tập tin hỗn hợp, ứng dụng sẽ quét các tập tin nén, gói phân phối, tập tin định dạng văn phòng, nhưng không quét các tập tin nén được bảo vệ bằng mật khẩu. Khi thiết lập mức độ bảo mật này, ứng dụng sẽ sử dụng phân tích hành vi với mức độ chi tiết **Quét nhanh**. 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.

Tham số	Mô tả
Hành động khi phát hiện mối đe dọa	**Khử mã độc, xóa nếu không thể khử mã độc**. Nếu chọn tùy chọn này, ứng dụng sẽ tự động cố gắng khử mã độc tập tin bị nhiễm được phát hiện. Nếu không thể khử mã độc, ứng dụng sẽ xóa 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 khử mã độc thất bại, 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. Trước khi cố gắng khử mã độc hoặc xóa một tập tin bị nhiễm, ứng dụng 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. 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.
Chạy khử mã độc nâng cao ngay lập tức *(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)*	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. 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. 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.
Phạm vi quét	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, ổ đĩa cứng, ổ đĩa di động hoặc ổ đĩa mạng, tập tin hoặc thư mục. Trong Kaspersky Endpoint Security cho Windows 12.12, email không nằm trong phạm vi quét ứng dụng. Tác vụ quét các email đến và đi được thực hiện bởi Thành phần Bảo vệ mối đe dọa thư điện tử. Nếu bạn đang sử dụng phiên bản cũ hơn của tiện ích quản lý, ứng dụng sẽ loại trừ email khỏi phạm vi quét ngay cả khi chính sách bao gồm email.
Lịch quét	**Manually**. Chế độ chạy trong đó bạn có thể tiến hành quét thủ công tại một thời điểm thuận tiện cho bạn. **By schedule**. Trong chế độ chạy tác vụ quét này, ứng dụng 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.
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 bị bỏ qua ngay khi có thể. Có thể bỏ qua tác vụ, ví dụ như nếu máy tính bị tắt vào thời điểm bắt đầu tác vụ được lên lịch. Khi ứng dụng có cơ hội thực thi các tác vụ bị bỏ lỡ, ứng dụng sẽ chạy các tác vụ một cách ngẫu nhiên trong một khoảng thời gian nhất định để phân phối tải trên máy tính. Khi hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ không chạy các tác vụ bị bỏ qua. Thay vào đó, ứng dụng sẽ chạy tác vụ kế tiếp dựa theo lịch hiện tại.
Chỉ chạy khi máy tính đang rảnh	Hoãn bắt đầu tác vụ 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. Tùy chọn lịch này cho phép bạn bảo tiết kiệm nguyên máy tính khi máy tính đang được sử dụng.

Tham số	Mô tả
Chạy quét dưới quyền	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 ứng dụng và chạy tác vụ quét bằng tài khoản của người dùng này.
Loại tập tin	Kaspersky Endpoint Security coi các tập tin không có phần mở rộng là các tập tin có thể được thực thi. Ứng dụng sẽ luôn quét các tập tin thực thi bất kể kiểu tập tin mà bạn đã lựa chọn để quét. **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, ứng dụng 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, ứng dụng 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. 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`).
Chỉ quét các tập tin mới và bị chỉnh sửa	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.
Bỏ qua tập tin quét trong thời gian dài hơn N giây	Giới hạn thời gian thực thi tác vụ. Sau một khoảng thời gian được quy định, Kaspersky Endpoint Security sẽ dừng tác vụ đó. 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.
Không chạy nhiều tác vụ quét cùng lúc	Nếu tác vụ quét theo lịch được khởi chạy từ trước đó vẫn đang chạy thì hãy tạm dừng các tác vụ quét theo lịch. Kaspersky Endpoint Security sẽ xếp hàng các tác vụ quét theo lịch nếu tác vụ quét hiện tại tiếp tục. Điều này giúp tối ưu hóa mức tải trên máy tính. Ví dụ: bạn đã lên lịch các tác vụ quét để chạy lúc 6:00 chiều và 8:00 tối. Kaspersky Endpoint Security sẽ hoãn tác vụ quét lúc 8:00 tối nếu tác vụ quét được lên lịch lúc 6:00 chiều vẫn đang chạy. Ứng dụng sẽ chạy tác vụ quét sau khi tác vụ bắt đầu lúc 6:00 chiều hoàn tất. Tuy nhiên, Kaspersky Endpoint Security sẽ ngay lập tức tiến hành tác vụ quét, ngay cả khi một trong các tác vụ quét sau đang chạy: • Quét các ổ đĩa di động khi kết nối. • Quét từ Menu ngữ cảnh. • Quét khu vực quan trọng đã được khởi chạy khi phát hiện một Dấu hiệu về sự xâm nhập (IoC). Nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ cho phép bạn chạy nhiều tác vụ quét cùng một lúc. Chạy nhiều tác vụ quét đòi hỏi nhiều tài nguyên máy tính hơn.
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. Ứng dụng 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	Quét các gói phân phối của ứng dụng 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. Ứng dụng sẽ quét các tập tin định dạng văn phòng nhỏ hơn 1 MB, bất kể hộp kiểm này có được chọn hay không.

Tham số	Mô tả
Quét các tập tin có định dạng email	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 cũng như các tập tin EML. Kaspersky Endpoint Security không hỗ trợ phiên bản 64 bit của ứng dụng thư Microsoft Outlook. Điều này có nghĩa là Kaspersky Endpoint Security sẽ không quét các tập tin Microsoft Outlook (tập tin PST và OST) nếu phiên bản 64 bit của Microsoft Outlook được cài đặt trên máy tính, ngay cả khi bạn thêm thư vào trong phạm vi quét. 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. Nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ quét tập tin định dạng email như một tập tin duy nhất. Khi phát hiện đối tượng độc hại trong các tập tin PST hoặc OST, Kaspersky Endpoint Security sẽ vô hiệu hóa đối tượng đó theo hành động đã chọn (ví dụ: khử mã độc hoặc xóa tập tin). Nếu phát hiện các đối tượng độc hại trong tập tin của các ứng dụng email khác (ví dụ: Mozilla Thunderbird), Kaspersky Endpoint Security sẽ không khử mã độc hoặc xóa các tập tin đó để tránh xóa nhầm email của bạn. Kaspersky Endpoint Security chỉ thêm thông tin về các đối tượng bị nhiễm mã độc được phát hiện vào danh sách các mối đe dọa hiện hoạt. Bạn cần thực hiện các bước để xóa email có tập tin độc hại trong tệp đính kèm trong giao diện người dùng của ứng dụng email. Nếu lúc này không thể xóa nội dung thư chứa đối tượng độc hại vì bất kỳ lý do gì, bạn có thể xử lý các mối đe dọa đó trong giao diện người dùng Kaspersky Endpoint Security bằng cách thêm các đối tượng được phát hiện vào danh sách loại trừ quét.
Quét tập tin nén có mật khẩu bảo vệ	Nếu hộp kiểm này được chọn, ứng dụng sẽ quét tập tin 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. Nếu hộp kiểm này bị xóa, ứng dụng sẽ bỏ qua việc quét các tập nén có mật khẩu bảo vệ.
Không giải nén các tập tin phức hợp lớn	Nếu hộp kiểm này được chọn, ứng dụng sẽ không quét các tập tin hỗn hợp nếu dung lượng của chúng vượt quá giá trị ấn định. Nếu bỏ chọn hộp kiểm này, ứng dụng sẽ quét các tập tin tổ hợp thuộc mọi kích thước. Ứng dụng sẽ quét các tập tin lớn được trích xuất từ tập tin nén, bất kể hộp kiểm này có được chọn hay không.
Công nghệ máy học và phân tích dấu hiệu	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. Dựa trên khuyến nghị của các chuyên gia Kaspersky, máy học và phân tích dấu hiệu luôn được bật.
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 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.
Công nghệ iSwift *(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)*	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 tác vụ 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 iSwift được cải tiến từ công nghệ iChecker cho hệ thống tập tin NTFS.
Công nghệ iChecker *(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)*	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 tác vụ 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 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 mối 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.

Cách cấu hình chạy Quét ổ đĩa di động trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Tác vụ cục bộ → Quét ổ đĩa di động**.
4. Trong danh sách thả xuống **Hành động khi kết nối ổ đĩa di động**, hãy chọn **Quét chi tiết** hoặc **Quét nhanh**.
5. Cấu hình các tùy chọn nâng cao cho Quét ổ đĩa di động (xem bảng bên dưới).
6. 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 **Asset management → Policies**.
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 **Host Threat Protection → Removable Drives Scan**.
5. Sử dụng nút bật/tắt **Removable Drives Scan ENABLED** để bật hoặc tắt thành phần này.
6. Trong mục **Scan type**, hãy chọn **Detailed Scan** hoặc **Quick Scan**.
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 giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy 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
Scan type	**Detailed Scan**. Nếu chọn tùy chọn này, Kaspersky Endpoint Security sẽ quét tất cả các tập tin trên ổ đĩa di động được kết nối, 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 Office. Kaspersky Endpoint Security không quét các tập tin có định dạng thư hoặc tập tin nén được bảo vệ bằng mật khẩu. **Quick Scan**. 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 dễ bị nhiễm virus nhất, và sẽ không giải nén các tập tin hỗn hợp.
Maximum drive size (MB)	Nếu chọn hộp kiểm này, Kaspersky Endpoint Security sẽ thực hiện hành động đã chọn trên các ổ đĩa di động có dung lượng không lớn hơn dung lượng ổ đĩa tối đa được chỉ định. Nếu dung lượng của ổ đĩa di động vượt quá giá trị đã cấu hình, Kaspersky Endpoint Security sẽ bỏ qua tác vụ quét. Nếu bỏ chọn hộp kiểm, Kaspersky Endpoint Security sẽ thực hiện hành động đã chọn trên ổ đĩa di động có dung lượng bất kỳ.
Hide scan progress bar	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**. Khi hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ thực hiện quét ổ đĩa di động trong nền.
Prevent users from stopping the scan	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.

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.

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. Các tác vụ này có cùng phạm vi quét. Để tối ưu hóa mức tải trên máy tính, ứng dụng không chạy tác vụ Quét toàn bộ và Quét trong nền cùng một lúc. Nếu bạn đã chạy tác vụ Quét toàn bộ thì Kaspersky Endpoint Security sẽ không bắt đầu tác vụ Quét trong nền trong bảy ngày sau khi hoàn thành tác vụ Quét toàn bộ.

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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Tác vụ cục bộ** → **Quét trong nền**.
4. Sử dụng hộp kiểm **Bật Quét trong nền** để bật hoặc tắt quét trong nền.
5. 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 **Asset management** → **Policies**.
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 **Host Threat Protection** → **File Threat Protection**.
5. Trong mục **Background Scan**, hãy sử dụng công tắc bật/tắt **Background Scan ENABLED** để bật hoặc tắt quét trong nền.
6. Lưu các thay đổi của bạn.

Cách bật quét trong nền trong giao diện ứng dụng

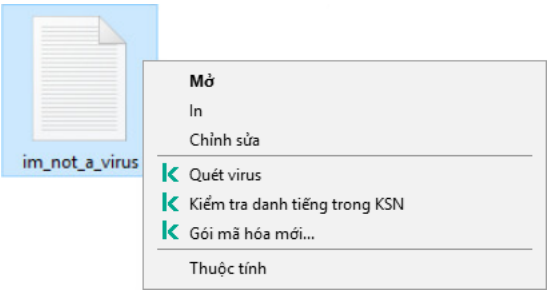
1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Tác vụ**.
2. Trong danh sách tác vụ, hãy chọn tác vụ quét và nhấn vào ⚙.
3. Sử dụng nút bật/tắt **Quét trong nền** để bật hoặc tắt thành phần.
4. Lưu các thay đổi của bạn.

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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Tác vụ cục bộ** → **Quét từ Menu ngữ cảnh**.
4. Cấu hình Quét từ Menu ngữ cảnh (xem bảng bên dưới).
5. 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 **Asset management** → **Policies**.
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 **Host Threat Protection** → **File Threat Protection**.
5. Trong mục **Scan from Context Menu**, hãy 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 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 *mức độ bảo mật*: • **Cao**. Kaspersky Endpoint Security sẽ quét tất cả các loại tập tin. Khi quét các tập tin hỗn hợp, ứng dụng sẽ quét các tập tin nén, gói phân phối, tập tin định dạng văn phòng, nhưng không quét các tập tin nén được bảo vệ bằng mật khẩu. Khi thiết lập mức độ bảo mật này, ứng dụng sẽ sử dụng phân tích hành vi với mức độ chi tiết **Quét sâu**. • **Khuyên dùng**. Kaspersky Endpoint Security sẽ quét tất cả các loại tập tin. Khi quét các tập tin hỗn hợp, ứng dụng sẽ quét các tập tin nén, gói phân phối, tập tin định dạng văn phòng, nhưng không quét các tập tin nén được bảo vệ bằng mật khẩu. Khi thiết lập mức độ bảo mật này, ứng dụng sẽ sử dụng phân tích hành vi với mức độ chi tiết **Quét vừa**. • **Thấp**. Kaspersky Endpoint Security chỉ quét các định dạng tập tin được chỉ định. Khi quét các tập tin hỗn hợp, ứng dụng sẽ quét các tập tin nén, gói phân phối, tập tin định dạng văn phòng, nhưng không quét các tập tin nén được bảo vệ bằng mật khẩu. Khi thiết lập mức độ bảo mật này, ứng dụng sẽ sử dụng phân tích hành vi với mức độ chi tiết **Quét nhanh**.
Hành động khi phát hiện mối đe dọa	**Khử mã độc, xóa nếu không thể khử mã độc**. Nếu chọn tùy chọn này, ứng dụng sẽ tự động cố gắng khử mã độc tập tin bị nhiễm được phát hiện. Nếu không thể khử mã độc, ứng dụng sẽ xóa 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 khử mã độc thất bại, 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.
Loại tập tin	Kaspersky Endpoint Security coi các tập tin không có phần mở rộng là các tập tin có thể được thực thi. Ứng dụng sẽ luôn quét các tập tin thực thi bất kể kiểu tập tin mà bạn đã lựa chọn để quét. **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, ứng dụng 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, ứng dụng 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. 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`).
Chỉ quét các tập tin mới và bị chỉnh sửa	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.
Bỏ qua tập tin quét trong thời gian dài hơn N giây	Giới hạn thời gian thực thi tác vụ. Sau một khoảng thời gian được quy định, Kaspersky Endpoint Security sẽ dừng tác vụ đó. 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.
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. Ứng dụng 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. Ứng dụng sẽ quét các tập tin định dạng văn phòng nhỏ hơn 1 MB, bất kể hộp kiểm này có được chọn hay không.

Tham số	Mô tả
Quét các tập tin có định dạng email	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 cũng như các tập tin EML. Kaspersky Endpoint Security không hỗ trợ phiên bản 64 bit của ứng dụng thư Microsoft Outlook. Điều này có nghĩa là Kaspersky Endpoint Security sẽ không quét các tập tin Microsoft Outlook (tập tin PST và OST) nếu phiên bản 64 bit của Microsoft Outlook được cài đặt trên máy tính, ngay cả khi bạn thêm thư vào trong phạm vi quét. 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. Nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ quét tập tin định dạng email như một tập tin duy nhất. Khi phát hiện đối tượng độc hại trong các tập tin PST hoặc OST, Kaspersky Endpoint Security sẽ vô hiệu hóa đối tượng đó theo hành động đã chọn (ví dụ: khử mã độc hoặc xóa tập tin). Nếu phát hiện các đối tượng độc hại trong tập tin của các ứng dụng email khác (ví dụ: Mozilla Thunderbird), Kaspersky Endpoint Security sẽ không khử mã độc hoặc xóa các tập tin đó để tránh xóa nhầm email của bạn. Kaspersky Endpoint Security chỉ thêm thông tin về các đối tượng bị nhiễm mã độc được phát hiện vào danh sách các mối đe dọa hiện hoạt. Bạn cần thực hiện các bước để xóa email có tập tin độc hại trong tệp đính kèm trong giao diện người dùng của ứng dụng email. Nếu lúc này không thể xóa nội dung thư chứa đối tượng độc hại vì bất kỳ lý do gì, bạn có thể xử lý các mối đe dọa đó trong giao diện người dùng Kaspersky Endpoint Security bằng cách thêm các đối tượng được phát hiện vào danh sách loại trừ quét.
Quét tập tin nén có mật khẩu bảo vệ	Nếu hộp kiểm này được chọn, ứng dụng sẽ quét tập tin 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. Nếu hộp kiểm này bị xóa, ứng dụng sẽ bỏ qua việc quét các tập nén có mật khẩu bảo vệ.
Không giải nén các tập tin phức hợp lớn	Nếu hộp kiểm này được chọn, ứng dụng sẽ không quét các tập tin hỗn hợp nếu dung lượng của chúng vượt quá giá trị ấn định. Nếu bỏ chọn hộp kiểm này, ứng dụng sẽ quét các tập tin tổ hợp thuộc mọi kích thước. Ứng dụng sẽ quét các tập tin lớn được trích xuất từ tập tin nén, bất kể hộp kiểm này có được chọn hay không.
Công nghệ máy học và phân tích dấu hiệu	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. Dựa trên khuyến nghị của các chuyên gia Kaspersky, máy học và phân tích dấu hiệu luôn được bật.
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 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.
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 tác vụ 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 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 tác vụ 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).

Kiểm tra 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 của ứng dụng* được dành để quét các tập tin ứng dụng. Chạy tác vụ *Kiểm tra tính toàn vẹn của ứng dụng* 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 của ứng dụng* 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.

Tín 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 cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Tasks**.
   Danh sách tác vụ sẽ mở.
2. Nhấn vào **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 (14.2)** → **Kiểm tra tính toàn vẹn của ứng dụng**.

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

Hoàn tất 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 **Tasks**.

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **Add**.

   Trình hướng dẫn Tác vụ sẽ được bắt đầu.

3. Cấu hình các thiết lập của tác vụ:

   a. Trong danh sách thả xuống **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.

   b. Trong danh sách thả xuống **Task type**, hãy chọn **Application Integrity Check**.

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 **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. Chọn một tài khoản để chạy tác vụ. Theo mặc định, Kaspersky Endpoint Security khởi chạy tác vụ với quyền của tài khoản người dùng cục bộ.

6. Hoàn tất trình hướng dẫn.

   Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ.

7. 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 vào mục **Tác vụ**.

2. Thao tác này sẽ mở ra danh sách tác vụ; hãy chọn tác vụ *Kiểm tra tính toàn vẹn của ứng dụng* và nhấn vào **Chạy**.

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 tác vụ *Kiểm tra tính toàn vẹn của ứng dụng* 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	**Thủ công**. Chế độ chạy trong đó bạn có thể tiến hành quét thủ công tại một thời điểm thuận tiện cho bạn. **Theo lịch**. Trong chế độ chạy tác vụ quét này, ứng dụng 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.
Chạy các tác vụ bị bỏ qua	Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ bắt đầu lại tác vụ bị bỏ qua ngay khi có thể. Có thể bỏ qua tác vụ, ví dụ như nếu máy tính bị tắt vào thời điểm bắt đầu tác vụ được lên lịch. Khi ứng dụng có cơ hội thực thi các tác vụ bị bỏ lỡ, ứng dụng sẽ chạy các tác vụ một cách ngẫu nhiên trong một khoảng thời gian nhất định để phân phối tải trên máy tính. Khi hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ không chạy các tác vụ bị bỏ qua. Thay vào đó, ứng dụng sẽ chạy tác vụ kế tiếp dựa theo lịch hiện tại.
Chỉ chạy khi máy tính đang rảnh	Hoãn bắt đầu tác vụ 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. Tùy chọn lịch này cho phép bạn bảo tiết kiệm nguyên máy tính khi máy tính đang được sử dụng.

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:

- **Bộ nhớ hệ thống**.
- **Tiến trình đang chạy và 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**.

Trong Kaspersky Endpoint Security cho Windows 12.12, email không nằm trong phạm vi quét ứng dụng. Tác vụ quét các email đến và đi được thực hiện bởi Thành phần Bảo vệ mối đe dọa thư điện tử. Nếu bạn đang sử dụng phiên bản cũ hơn của tiện ích quản lý, ứng dụng sẽ loại trừ email khỏi phạm vi quét ngay cả khi chính sách bao gồm email.

Bạn nên tạo một tác vụ quét riêng để quét ổ đĩa mạng hoặc thư mục dùng chung. Trong thiết lập của tác vụ *Quét phần mềm độc hại*, hãy chỉ định người dùng có quyền ghi vào ổ đĩa này; đây là điều cần thiết để giảm thiểu các mối đe dọa được phát hiện. Nếu máy chủ đặt ổ đĩa mạng có công cụ bảo mật riêng thì không chạy tác vụ quét cho ổ đĩa đó. Nhờ vậy, bạn có thể tránh việc kiểm tra đối tượng hai lần và tăng hiệu năng của máy chủ.

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 cây bảng điều khiển, hãy chọn **Tasks**.
3. Chọn một tác vụ quét và nhấn đúp để mở các thuộc tính tác vụ.
   Nếu cần, hãy tạo một tác vụ *Quét phần mềm độc hại*.
4. Trong cửa sổ thuộc tính tác vụ, hãy chọn mục **Thiết lập**.
5. Trong mục **Phạm vi quét**, hãy nhấn **Thiết lập**.
6. 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.
7. 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 các thư mục con bên trong `Folder`, ngoại trừ chính `Folder`. Một đại diện phải có ít nhất một cấp 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 sử dụng mặt nạ ở bất kỳ đâu trong đường dẫn tập tin hoặc thư mục. Ví dụ: nếu bạn muốn phạm vi quét bao gồm thư mục Downloads cho tất cả tài khoản người dùng trên máy tính, hãy nhập tên đại diện `C:\Users\*\Downloads\`.

      Đối tượng **Máy tính này** trong danh sách tài nguyên tập tin của máy tính bao gồm các đối tượng sau: **Tất cả các ổ đĩa cứng**, **Tất cả ổ đĩa mạng** và **Tất cả các ổ đĩa di động**.

   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. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

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 **Asset management** → **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 *Malware Scan*.

3. Chọn thẻ **Application settings**.

4. Trong mục **Scan scope**, 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 **Add**.

   b. 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 các thư mục con bên trong `Folder`, ngoại trừ chính `Folder`. Một đại diện phải có ít nhất một cấp 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 sử dụng mặt nạ ở bất kỳ đâu trong đường dẫn tập tin hoặc thư mục. Ví dụ: nếu bạn muốn phạm vi quét bao gồm thư mục Downloads cho tất cả tài khoản người dùng trên máy tính, hãy nhập tên đại diện `C:\Users\*\Downloads\`.

   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 vào mục **Tác vụ**.

2. Thao tác này sẽ mở ra 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 tìm phần mềm độc hại bằng tác vụ *Quét phần mềm độc hại* có thể tốn thời gian và làm tăng mức sử dụng tài nguyên máy tính của Kaspersky Endpoint Security. Do đó, nên chọn thời điểm tối ưu để chạy tác vụ này nhằm giảm thiểu ảnh hưởng đến hiệu năng của các ứng dụng khác.

Ví dụ: nếu nhân viên trong tổ chức của bạn làm việc theo lịch cố định, bạn có thể cấu hình để quá trình quét máy tính chạy vào ban đêm hoặc vào cuối tuần. Nếu không thể chạy tác vụ này vì bất cứ lý do gì (ví dụ như 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. Nên sử dụng chức năng này một cách thận trọng, vì có thể làm chậm các ứng dụng trên máy tính của người dùng khi máy tính được bật vào buổi sáng.

Nếu bạn không thể xác định lịch quét tối ưu phù hợp với nhu cầu của mình, bạn có thể cấu hình để tác vụ quét diễn ra khi một trong các điều kiện đặc biệt sau được đáp ứng:

- 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 một khoảng thời gian nhất định, 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.

- Tính năng 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 phần mềm độc hại* 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. Trong trường hợp này, tác vụ Quét toàn bộ có thể mất vài ngày để hoàn tất.

- Khi tác vụ bị bỏ qua.

  Kaspersky Endpoint Security sẽ chạy tác vụ bị bỏ qua ngay khi có thể. Có thể bỏ qua tác vụ, ví dụ như nếu máy tính bị tắt vào thời điểm bắt đầu tác vụ được lên lịch. Khi ứng dụng có cơ hội thực thi các tác vụ bị bỏ lỡ, ứng dụng sẽ chạy các tác vụ một cách ngẫu nhiên trong một khoảng thời gian nhất định để phân phối tải trên máy tính.

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 **Tasks**.

   Danh sách tác vụ sẽ mở.

2. Nhấn vào tác vụ quét.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

3. Trong cửa sổ thuộc tính tác vụ, hãy chọn thẻ **Schedule**.

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 phần mềm độc hại* trong Kaspersky Security Center.

1. Trong cửa sổ chính của ứng dụng, hãy 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	**Thủ công**. Chế độ chạy trong đó bạn có thể tiến hành quét thủ công tại một thời điểm thuận tiện cho bạn. **Theo lịch**. Trong chế độ chạy tác vụ quét này, ứng dụng 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.
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 bị bỏ qua ngay khi có thể. Có thể bỏ qua tác vụ, ví dụ như nếu máy tính bị tắt vào thời điểm bắt đầu tác vụ được lên lịch. Khi ứng dụng có cơ hội thực thi các tác vụ bị bỏ lỡ, ứng dụng sẽ chạy các tác vụ một cách ngẫu nhiên trong một khoảng thời gian nhất định để phân phối tải trên máy tính. Khi hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ không chạy các tác vụ bị bỏ qua. Thay vào đó, ứng dụng sẽ chạy tác vụ kế tiếp dựa theo lịch hiện tại.
Chỉ chạy khi máy tính đang rảnh	Hoãn bắt đầu tác vụ 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. Tùy chọn lịch này cho phép bạn bảo tiết kiệm nguyên máy tính khi máy tính đang được sử dụng.

Tham số	Mô tả
Use automatically randomized delay for task starts *(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)*	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. Dải 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. Nếu hộp kiểm này bị xóa, tác vụ được chạy vào đúng thời gian đã lên lịch.
Use randomized delay for task starts within an interval of (min)	Nếu chọn hộp kiểm này, tác vụ sẽ được chạy trên máy tính vào thời điểm ngẫu nhiên trong một khung thời gian nhất định. 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. Nếu hộp kiểm này bị xóa, tác vụ được chạy vào đúng thời gian đã lên lịch.
Stop the task if it runs longer than (min) *(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)*	Giới hạn thời gian thực thi tác vụ. Sau một khoảng thời gian được quy định, Kaspersky Endpoint Security sẽ dừng tác vụ đó. 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. 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.
Turn on devices by using the Wake-on-LAN function before starting the task (min) *(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)*	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. Chọn hộp kiểm này nếu bạn muốn chạy tác vụ trên tất cả các máy tính kể cả máy tính đã tắt nguồn.
Shut down the devices after completing the task *(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)*	Nếu chọn hộp kiểm này, máy tính sẽ tắt sau khi tác vụ hoàn tất. Ví dụ: bạn có thể bật chức năng này để quét máy tính vào các ngày thứ Sáu, sau giờ làm việc. Khi tác vụ kết thúc, ứng dụng sẽ tắt máy tính vào cuối tuần.
Tạm dừng tác vụ	Bạn có thể chỉ định một khoảng thời gian mà trong đó việc thực thi một tác vụ đã được lên lịch trước đó sẽ bị tạm dừng. Sau khi khoảng thời gian đã chỉ định kết thúc, tác vụ sẽ tiếp tục chạy. Tính năng này có thể cần thiết, ví dụ, để giảm thiểu tác động của Kaspersky Endpoint Security đến hiệu suất máy tính trong các giai đoạn sử dụng cao điểm.
Tắt lịch từ	Nếu chọn hộp kiểm này, Kaspersky Endpoint Security sẽ ngừng chạy tác vụ được lên lịch bắt đầu từ ngày được chỉ định. Tác vụ sẽ được đặt thành chế độ **Thủ công**.

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 ứng dụng 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 **Tasks**.
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 **Account**.
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

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **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 **Settings**.
4. Trong mục **Account**, hãy nhấn nút **Settings**.
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

1. Trong cửa sổ chính của ứng dụng, hãy 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 **Thiết lập nâng cao** → **Chạy quét dưới quyền**.
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

Giới hạn sử dụng CPU trong khi quét máy tính

Bạn có thể giới hạn mức sử dụng CPU khi chạy tác vụ *Quét phần mềm độc hại*. Làm thậy có thể làm tăng thời gian quét máy tính của bạn.

Cách giới hạn mức sử dụng CPU khi quét máy tính trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Thiết lập ứng dụng**.
4. Trong mục **Hiệu năng**, hãy chọn **Hạn chế mức sử dụng CPU cho các tác vụ quét** đánh dấu vào hộp kiểm và nhập giá trị trung bình của mức sử dụng tài nguyên CPU theo phần trăm.
5. Lưu các thay đổi của bạn.

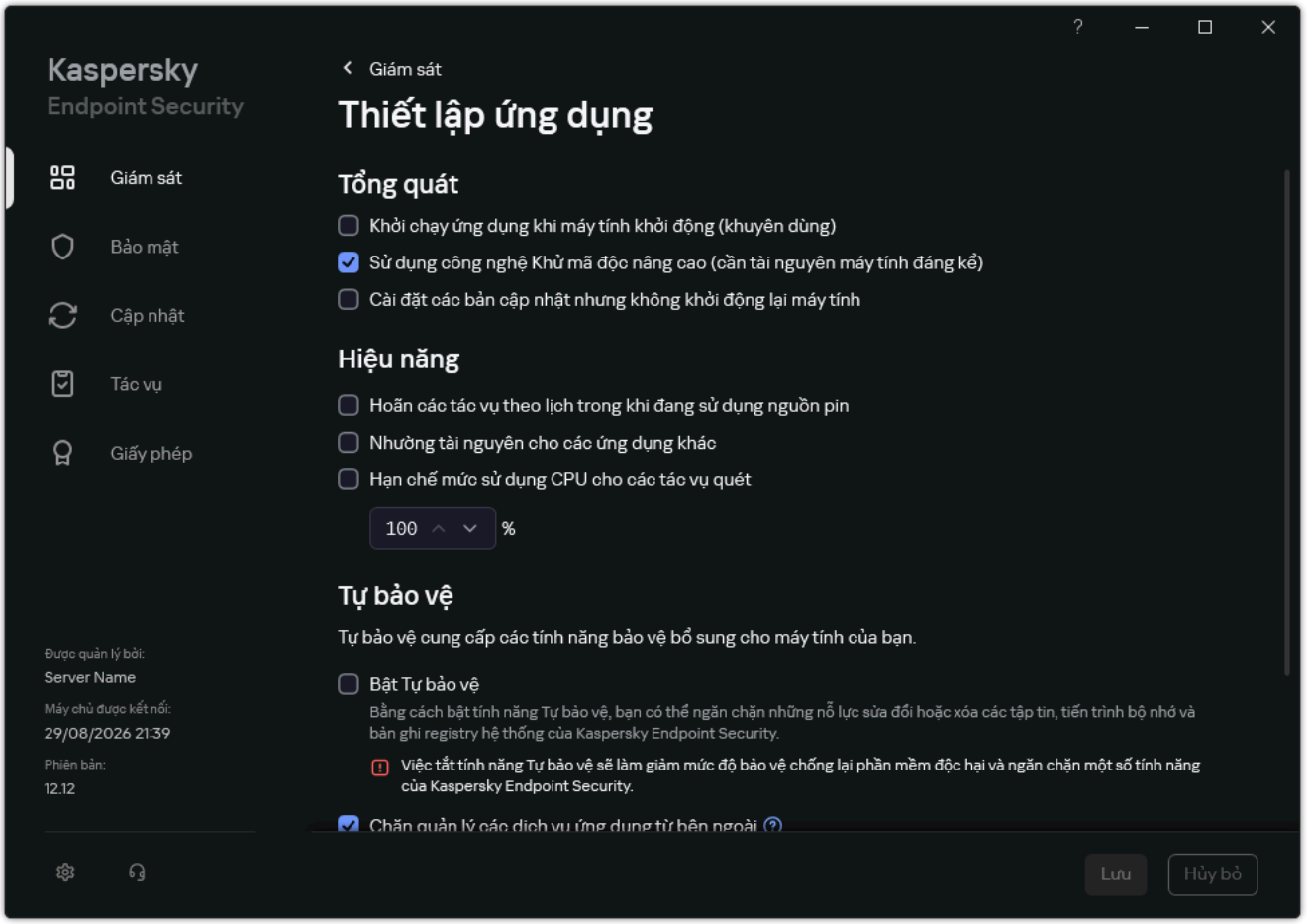
Cách giới hạn mức sử dụng CPU khi quét máy tính trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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** → **Performance**.
5. Trong mục **Limit CPU usage for scan tasks**, hãy đặt công tắc bật/tắt thành **Limit CPU usage for scan tasks** nhập giá trị trung bình của mức sử dụng tài nguyên CPU theo phần trăm.
6. Lưu các thay đổi của bạn.

Cách giới hạn mức sử dụng CPU khi quét máy tính 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**.



Thiết lập Kaspersky Endpoint Security cho Windows

3. Trong mục **Hiệu năng**, hãy chọn **Hạn chế mức sử dụng CPU cho các tác vụ quét** đánh dấu vào hộp kiểm và nhập giá trị trung bình của mức sử dụng tài nguyên CPU theo phần trăm.

4. Lưu các thay đổi của bạn.

Cấu hình thiết lập tác vụ nâng cao cho Quét phần mềm độc hại.

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 cây bảng điều khiển, hãy chọn **Tasks**.
3. Chọn một tác vụ quét và nhấn đúp để mở các thuộc tính tác vụ.

   Nếu cần, hãy tạo một tác vụ *Quét phần mềm độc hại*.
4. Trong cửa sổ thuộc tính tác vụ, hãy chọn mục **Thiết lập**.
5. Trong mục **Mức độ bảo mật**, hãy nhấn nút **Thiết lập**.

   Thao tác này sẽ mở ra cửa sổ thiết lập tác vụ quét.
6. Trong mục **Tối ưu hóa**, hãy cấu hình thiết lập quét:

   - **Chỉ quét các tập tin mới và bị chỉnh sửa**. 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**. Giới hạn thời gian thực thi tác vụ. Sau một khoảng thời gian được quy định, Kaspersky Endpoint Security sẽ dừng tác vụ đó. 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.

   - **Không chạy nhiều tác vụ quét cùng lúc**. Nếu tác vụ quét theo lịch được khởi chạy từ trước đó vẫn đang chạy thì hãy tạm dừng các tác vụ quét theo lịch. Kaspersky Endpoint Security sẽ xếp hàng các tác vụ quét theo lịch nếu tác vụ quét hiện tại tiếp tục. Điều này giúp tối ưu hóa mức tải trên máy tính. Ví dụ: bạn đã lên lịch các tác vụ quét để chạy lúc 6:00 chiều và 8:00 tối. Kaspersky Endpoint Security sẽ hoãn tác vụ quét lúc 8:00 tối nếu tác vụ quét được lên lịch lúc 6:00 chiều vẫn đang chạy. Ứng dụng sẽ chạy tác vụ quét sau khi tác vụ bắt đầu lúc 6:00 chiều hoàn tất.
7. Nhấn vào **Bổ sung**.

   Thao tác này sẽ mở ra cửa sổ thiết lập quét tập tin phức hợp.
8. Trong mục **Giới hạn dung lượng**, hãy chọn hộp kiểm **Không giải nén các tập tin hỗn hợp lớn**. Giới hạn thời gian thực thi tác vụ. Sau một khoảng thời gian được quy định, Kaspersky Endpoint Security sẽ dừng tác vụ đó. 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.

   > 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 hỗn hợp lớn** có được chọn hay không.
9. Nhấn vào **OK**.
10. Vào thẻ **Bổ sung**.

11. 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 tác vụ 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 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 tác vụ 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).

12. Lưu các thay đổi của bạn.

Cách tối ưu hóa quét trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **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 *Malware Scan*.

3. Chọn thẻ **Application settings**.

4. Trong mục **Action on threat detection**, hãy chọn hộp kiểm **Scan only new and modified files**. 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. Trong mục **Scan optimization**, hãy chọn hộp kiểm **Do not unpack large compound files**. Giới hạn thời gian thực thi tác vụ. Sau một khoảng thời gian được quy định, Kaspersky Endpoint Security sẽ dừng tác vụ đó. 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.

   > Kaspersky Endpoint Security sẽ quét các tập tin lớn được giải nén từ tập nén, bất kể là hộp kiểm **Do not unpack large compound files** có được chọn hay không.

6. Chọn hộp kiểm **Do not run multiple scan tasks at the same time**. Nếu tác vụ quét theo lịch được khởi chạy từ trước đó vẫn đang chạy thì hãy tạm dừng các tác vụ quét theo lịch. Kaspersky Endpoint Security sẽ xếp hàng các tác vụ quét theo lịch nếu tác vụ quét hiện tại tiếp tục. Điều này giúp tối ưu hóa mức tải trên máy tính. Ví dụ: bạn đã lên lịch các tác vụ quét để chạy lúc 6:00 chiều và 8:00 tối. Kaspersky Endpoint Security sẽ hoãn tác vụ quét lúc 8:00 tối nếu tác vụ quét được lên lịch lúc 6:00 chiều vẫn đang chạy. Ứng dụng sẽ chạy tác vụ quét sau khi tác vụ bắt đầu lúc 6:00 chiều hoàn tất.

7. Trong mục **Advanced settings**, hãy chọn hộp kiểm **Skip file that is scanned for longer than (sec)**. Giới hạn thời gian thực thi tác vụ. Sau một khoảng thời gian được quy định, Kaspersky Endpoint Security sẽ dừng tác vụ đó. 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.

8. 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 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**, hãy cấu hình thiết lập quét:

   - **Chỉ quét các tập tin mới và bị chỉnh sửa**. 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 tập tin quét trong thời gian dài hơn N giây**. Giới hạn thời gian thực thi tác vụ. Sau một khoảng thời gian được quy định, Kaspersky Endpoint Security sẽ dừng tác vụ đó. 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.

   - **Không chạy nhiều tác vụ quét cùng lúc**. Nếu tác vụ quét theo lịch được khởi chạy từ trước đó vẫn đang chạy thì hãy tạm dừng các tác vụ quét theo lịch. Kaspersky Endpoint Security sẽ xếp hàng các tác vụ quét theo lịch nếu tác vụ quét hiện tại tiếp tục. Điều này giúp tối ưu hóa mức tải trên máy tính. Ví dụ: bạn đã lên lịch các tác vụ quét để chạy lúc 6:00 chiều và 8:00 tối. Kaspersky Endpoint Security sẽ hoãn tác vụ quét lúc 8:00 tối nếu tác vụ quét được lên lịch lúc 6:00 chiều vẫn đang chạy. Ứng dụng sẽ chạy tác vụ quét sau khi tác vụ bắt đầu lúc 6:00 chiều hoàn tất.

5. Trong mục **Giới hạn dung lượng**, hãy chọn hộp kiểm **Không giải nén các tập tin phức hợp lớn**. Giới hạn thời gian thực thi tác vụ. Sau một khoảng thời gian được quy định, Kaspersky Endpoint Security sẽ dừng tác vụ đó. 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.

   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 tác vụ 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 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 tác vụ 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.

Cập nhật chức năng (bao gồm việc cung cấp các bản cập nhật dấu hiệu diệt virus và bản cập nhật bộ mã) có thể không khả dụng trong ứng dụng ở Hoa Kỳ.

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.

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 lỗ hổng bảo mật trong Kaspersky Endpoint Security, bổ sung các chức năng mới, hoặc tăng cường các chức năng sẵn có.

Trong khi cập nhật, các mô-đun ứng dụng và cơ sở dữ liệu trên máy tính của bạn sẽ được so sánh với các phiên bản đã cập nhật tại nguồn cập nhật. Nếu cơ sở dữ liệu và các mô-đun ứng dụng hiện tại của bạn khác với các phiên bản cập nhật tương ứng, phần còn thiếu của bản cập nhật sẽ được cài đặt trên máy tính của bạn.

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.

Nếu ứng dụng đang hoạt động trong Chế độ Light Agent, cần có những cân nhắc đặc biệt đối với việc cập nhật cơ sở dữ liệu và mô-đun ứng dụng.

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:

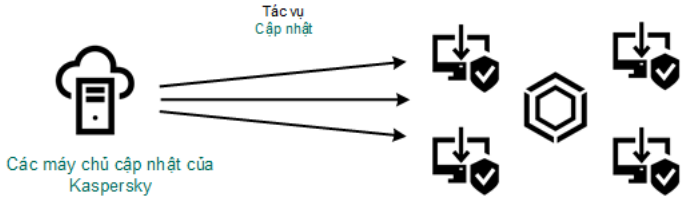
- Cơ sở dữ liệu diệt virus. Cơ sở dữ liệu diệt virus bao gồm các cơ sở dữ liệu dấu hiệu phần mềm độc hại, một mô tả về các cuộc tấn công mạng, cơ sở dữ liệu các địa chỉ web độc hại và lừa đảo, cơ sở dữ liệu bảng quảng cáo, cơ sở dữ liệu thư rác và các dữ liệu khác.

- 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 *Download updates to the Administration Server repository*.

2. Tải gói cập nhật về thư mục chia sẻ (tùy chọn).

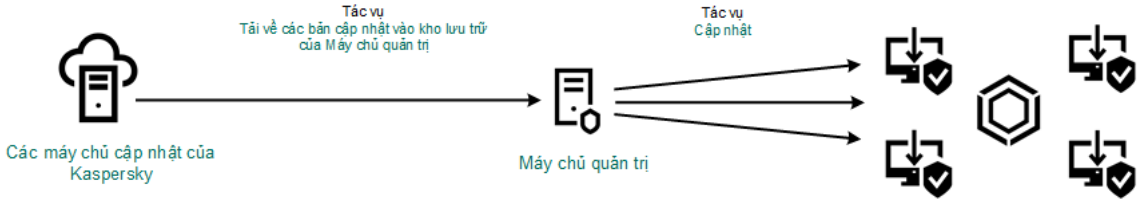
   Bạn có thể tải gói cập nhật về một thư mục chia sẻ bằng các phương thức sau:

   - Sử dụng tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* của Kaspersky Endpoint Security. Tác vụ này dành cho một máy tính trong mạng cục bộ của công ty.

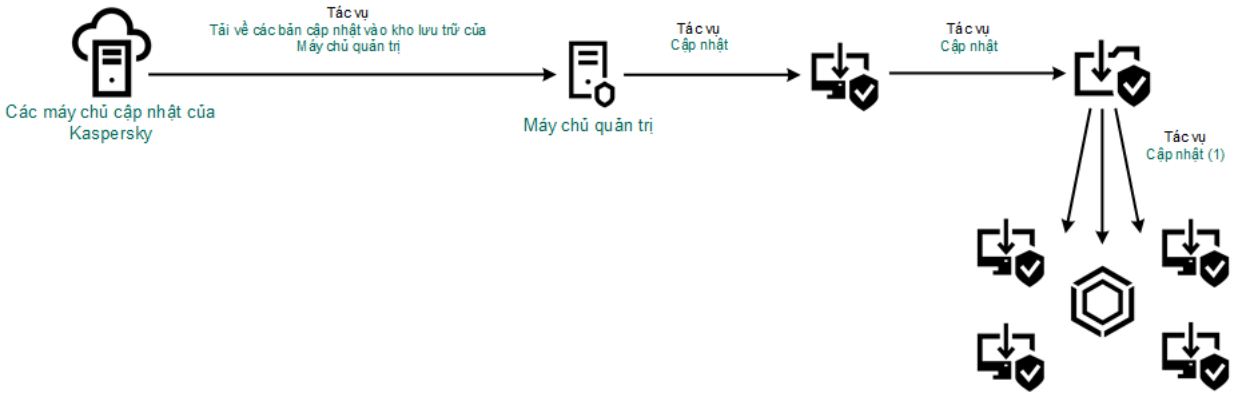
   - Sử dụng Kaspersky Update Utility. Để biết thông tin chi tiết về việc sử dụng Kaspersky Update Utility, hãy tham khảo Cơ sở tri thức của Kaspersky.

3. Phân phối gói cập nhật đến các máy khách.

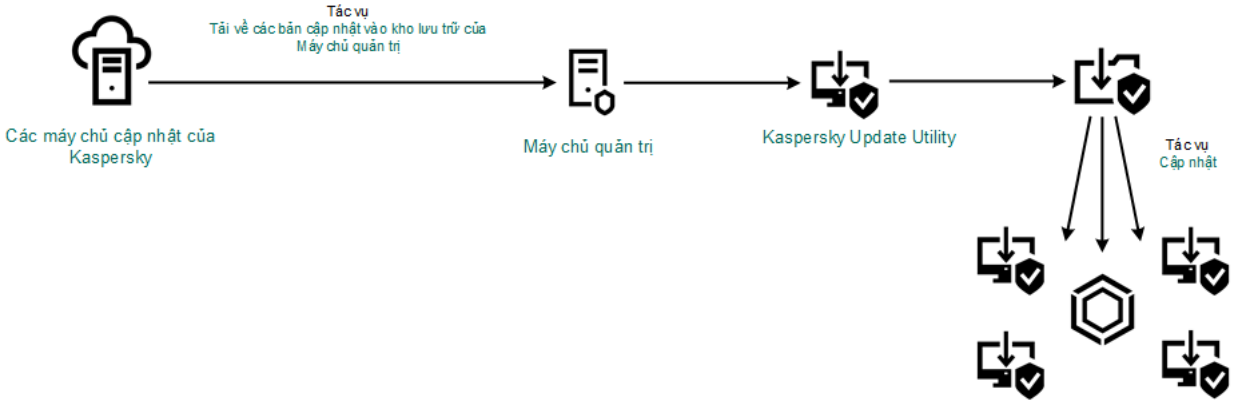
   Gói cập nhật được phân phối đến các máy khách thông qua tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* Kaspersky Endpoint Security. Bạn có thể tạo số lượng không giới hạn tác vụ cập nhật cho mỗi nhóm quản trị.



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 Kaspersky Security Center, 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. 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 tải xuống gói cập nhật vào kho dữ liệu Máy chủ quản trị (tác vụ *Download updates to the Administration Server repository*).

   Tác vụ *Download updates to the Administration Server repository* được tạo tự động bởi trình hướng dẫn sử dụng nhanh Máy chủ quản trị và tác vụ này có thể chỉ có một trường hợp duy nhất. Theo mặc định, Kaspersky Security Center sẽ sao chép gói cập nhật vào thư mục `\\<server name>\KLSHARE\Updates`. Để biết thêm thông tin về việc tải các bản cập nhật về kho lưu trữ Máy chủ quản trị, vui lòng tham khảo Trợ giúp của Kaspersky Security Center.

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 của tổ chức (tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*).

   Cách cấu hình bản cập nhật Kaspersky Endpoint Security từ kho lưu trữ máy chủ được chỉ định trong Bảng điều khiển quản trị (MMC)

   1. Mở Bảng điều khiển quản trị Kaspersky Security Center.

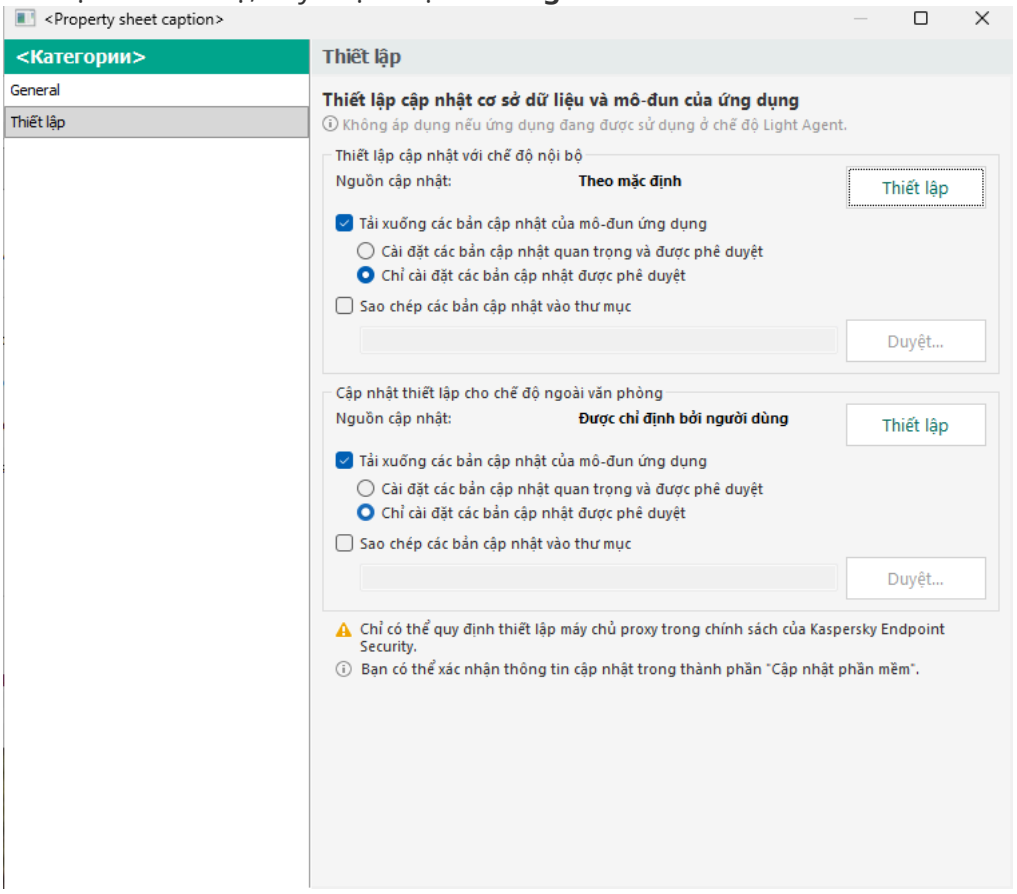
      Trong cây bảng điều khiển, hãy chọn **Tasks**.

   2. Nhấn vào tác vụ **Cập nhật cơ sở dữ liệu và mô-đun ứng dụng** của Kaspersky Endpoint Security.

      Cửa sổ thuộc tính tác vụ sẽ được mở ra.

      Tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* được tạo tự động bởi trình hướng dẫn sử dụng nhanh Máy chủ quản trị. Để tạo tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*, hãy cài đặt Tiện ích quản lý của Kaspersky Endpoint Security cho Windows khi đang chạy Trình hướng dẫn.

3. Trong cửa sổ thuộc tính tác vụ, hãy chọn mục **Settings**.



Thiết lập tác vụ Cập nhật cơ sở dữ liệu và mô-đun ứng dụng

4. Trong mục **Thiết lập cập nhật với chế độ nội bộ**, hãy nhấn nút **Thiết lập**.

5. Trong danh sách các nguồn cập nhật, đảm bảo rằng bản cập nhật từ nguồn **Kaspersky Security Center** được bật. Ngoài ra, nguồn **Kaspersky Security Center** phải có mức ưu tiên cao nhất.

6. Nếu cần, hãy thêm các nguồn cập nhật:

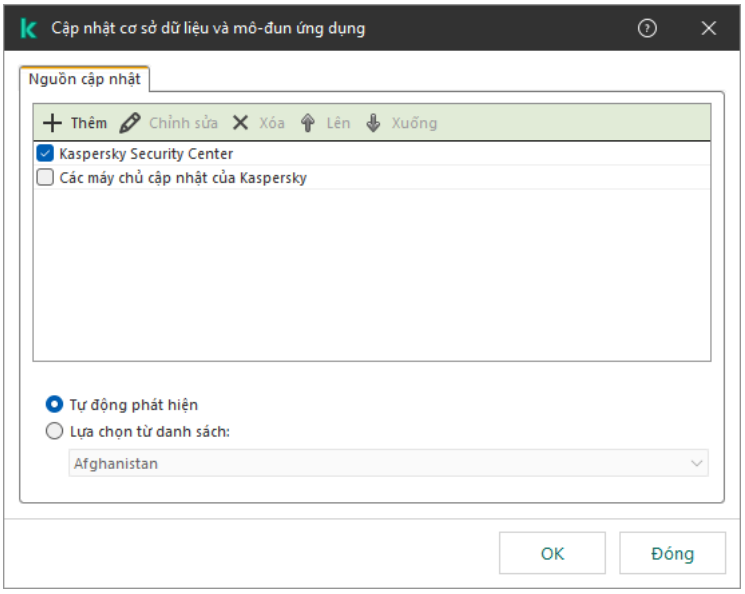
   a. Trong danh sách các nguồn cập nhật, nhấn nút **Thêm**.

   b. Trong trường **Nguồn cập nhật**, 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 (tác vụ *Download updates to the Administration Server repository*).

   c. Nhấn vào **OK**.

Bạn có thể loại trừ nguồn cập nhật mà không cần xóa nó khỏi danh sách nguồn cập nhật. Để thực hiện, hãy bỏ chọn hộp kiểm bên cạnh đối tượng.



Nguồn cập nhật

7. Cấu hình các ưu tiên của nguồn cập nhật bằng cách sử dụng nút **Lên** và **Xuống**.

   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.

8. Trong cửa sổ thuộc tính tác vụ, hãy chọn **Schedule** và cấu hình chế độ chạy tác vụ.

9. Theo mặc định, Kaspersky Endpoint Security sẽ chạy tác vụ ở chế độ thủ công.

10. Lưu các thay đổi của bạn.

Cách cấu hình bản cập nhật Kaspersky Endpoint Security từ kho lưu trữ máy chủ được chỉ định trong Bảng điều khiển web

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

   Danh sách tác vụ sẽ mở.

2. Nhấn vào tác vụ **Update** của Kaspersky Endpoint Security.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

   Tác vụ *Update* được tạo tự động bởi trình hướng dẫn sử dụng nhanh Máy chủ quản trị. Để tạo tác vụ *Update*, hãy cài đặt Tiện ích quản lý 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, đảm bảo rằng bản cập nhật từ nguồn **Kaspersky Security Center** được bật. Ngoài ra, nguồn **Kaspersky Security Center** phải có mức ưu tiên cao nhất.

5. Nếu cần, hãy thêm các nguồn cập nhật:

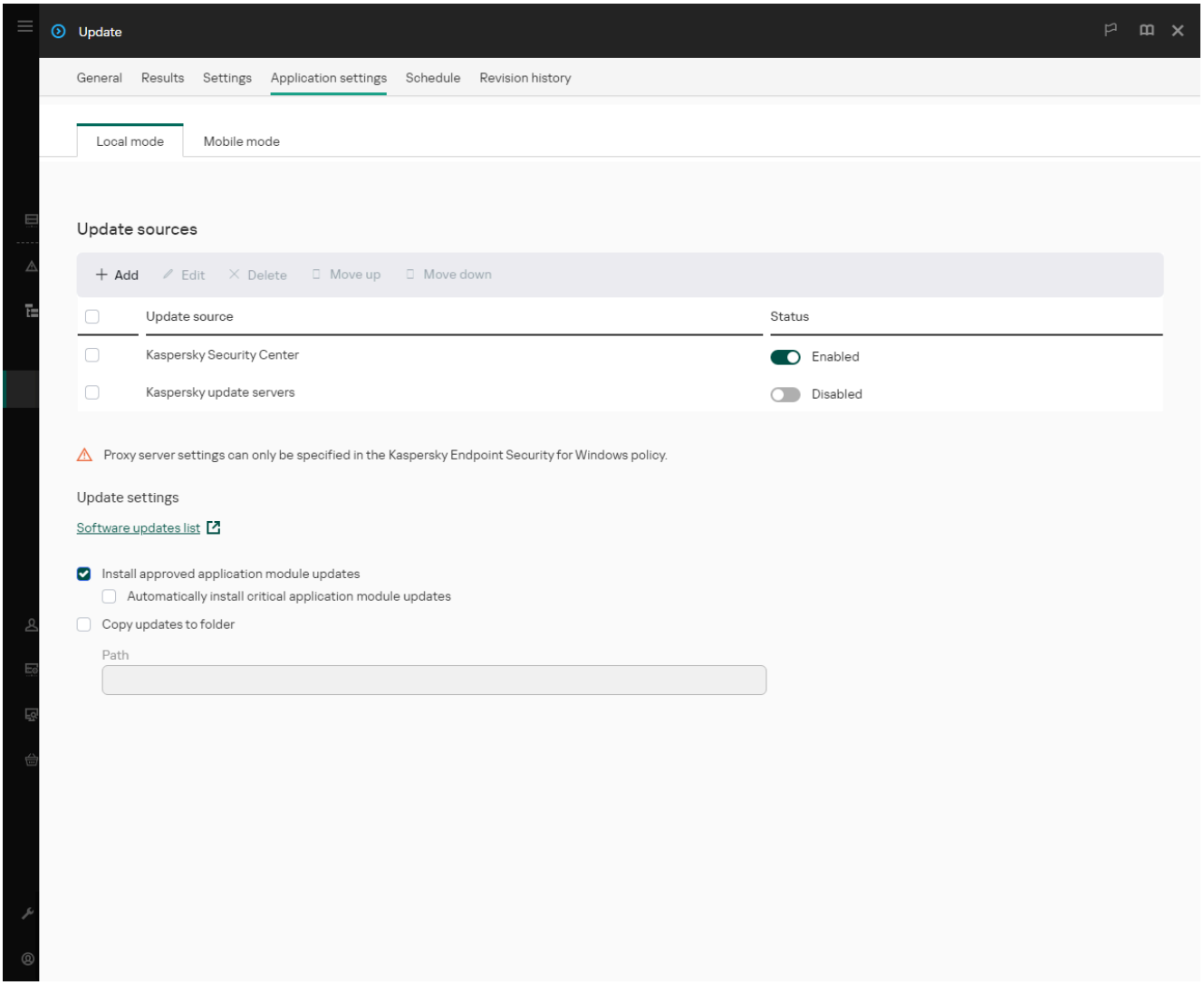
   a. Trong danh sách các nguồn cập nhật, nhấn nút **Add**.

   b. Trong trường **Update sources**, 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 (tác vụ *Download updates to the Administration Server repository*).

   c. Nhấn vào **Save**.

   Bạn có thể loại trừ nguồn cập nhật mà không cần xóa nó khỏi danh sách nguồn cập nhật. Để thực hiện, hãy gạt công tắc bật/tắt bên cạnh sang vị trí tắt.



Nguồn cập nhật

6. Cấu hình các ưu tiên của nguồn cập nhật bằng cách sử dụng nút **Move up** và **Move down**.

   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.

7. Trong cửa sổ thuộc tính tác vụ, hãy chọn **Schedule** và cấu hình chế độ chạy tác vụ.

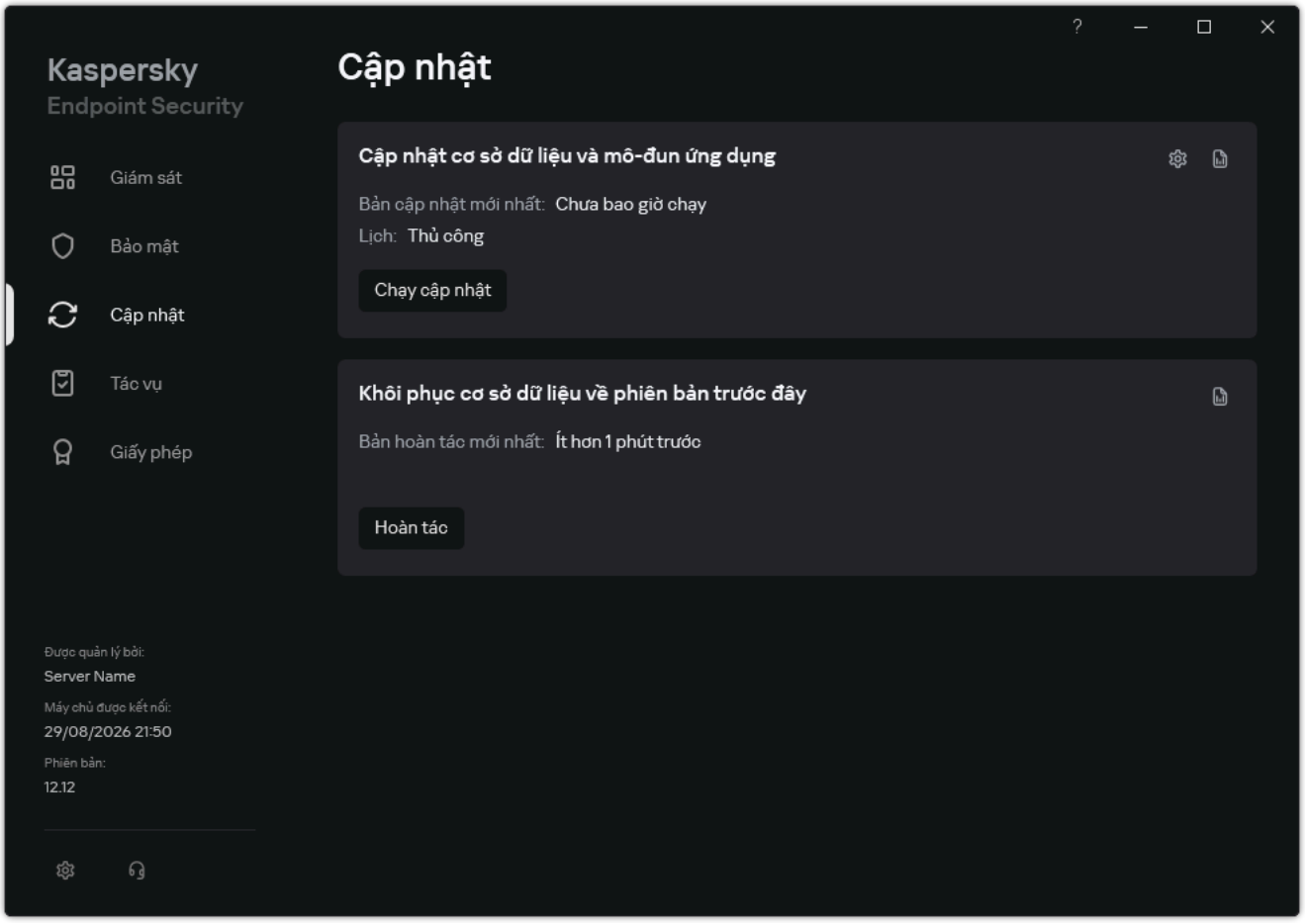
8. Theo mặc định, Kaspersky Endpoint Security sẽ chạy tác vụ ở chế độ thủ công.

9. Lưu các thay đổi của bạn.

Cách cấu hình bản cập nhật Kaspersky Endpoint Security từ kho lưu trữ máy chủ được chỉ định trong giao diện ứng dụng

Bạn không thể cấu hình tác vụ nhóm *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* trong giao diện ứng dụng. Chỉ một tác vụ cập nhật cục bộ là *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* khả dụng với người dùng. Nếu tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* không được hiển thị, điều đó có nghĩa là quản trị viên đã cấm sử dụng các tác vụ cục bộ trong chính sách.

1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Cập nhật**.



Tác vụ cập nhật cục bộ

2. Thao tác này sẽ mở ra danh sách tác vụ; hãy chọn tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* và nhấn vào ⚙.

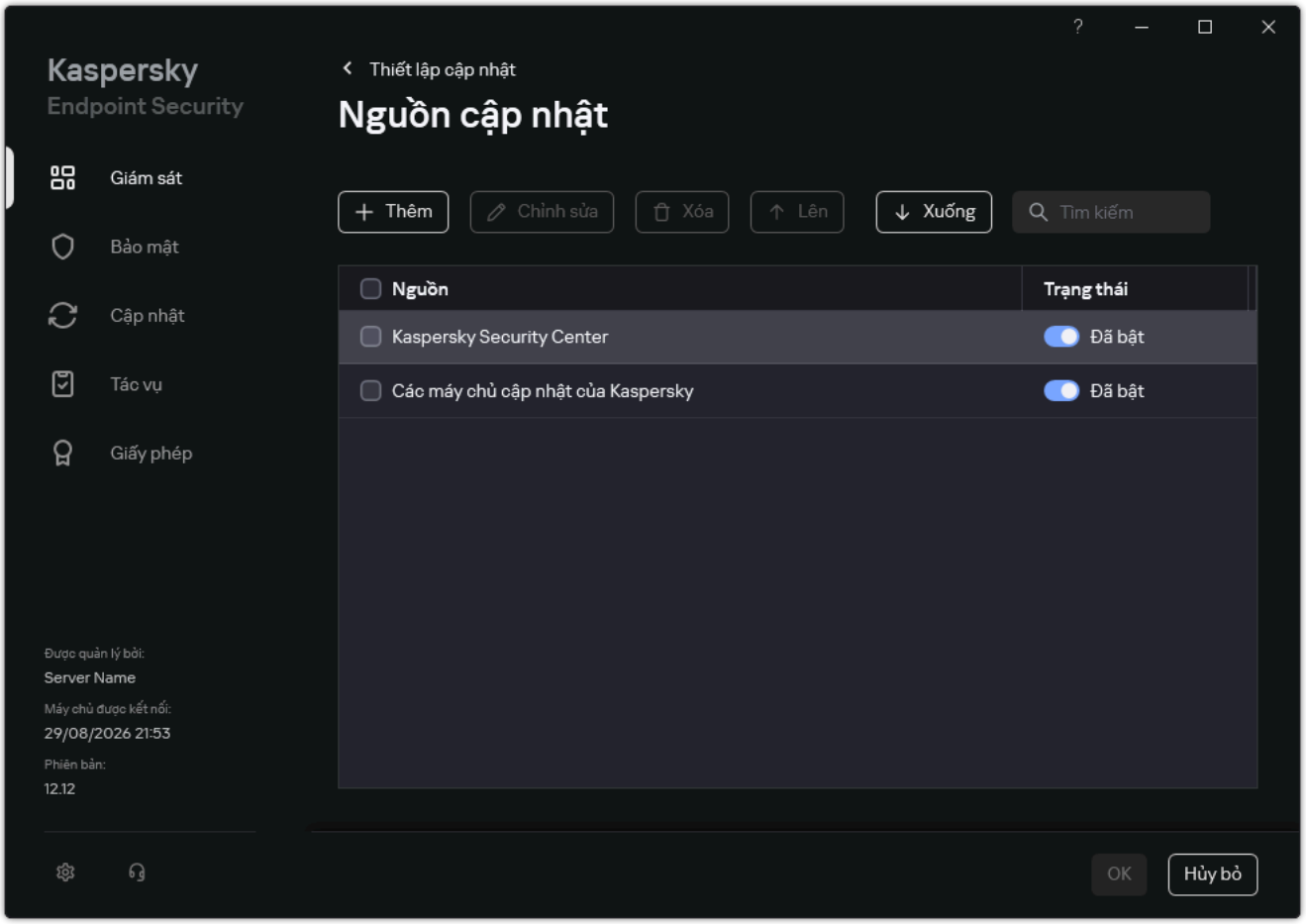
   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

3. Trong cửa sổ thuộc tính tác vụ, hãy nhấn vào **Chọn nguồn cập nhật**.

4. Trong danh sách các nguồn cập nhật, đảm bảo rằng bản cập nhật từ nguồn **Kaspersky Security Center** được bật. Ngoài ra, nguồn **Kaspersky Security Center** phải có mức ưu tiên cao nhất.

5. Nếu cần, hãy thêm các nguồn cập nhật:

   a. Trong danh sách các nguồn cập nhật, nhấn nút **Thêm**.



Nguồn cập nhật

   a. 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 của 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 (tác vụ *Download updates to the Administration Server repository*).

   b. Nhấn vào **Lựa chọn**.

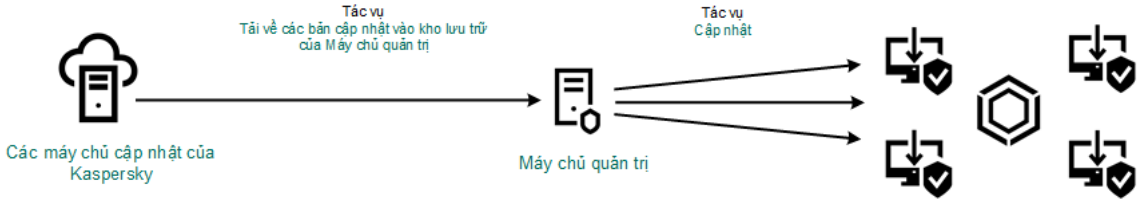
   Bạn có thể loại trừ nguồn cập nhật mà không cần xóa nó khỏi danh sách nguồn cập nhật. Để thực hiện, hãy gạt công tắc bật/tắt bên cạnh sang vị trí tắt.

6. Cấu hình các ưu tiên của nguồn cập nhật bằng cách sử dụng nút **Lên** và **Xuống**.

   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.

Nếu một máy tính được quản lý bởi Kaspersky Security Center thì bạn không thể cấu hình chế độ chạy cho tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*. Bạn chỉ có thể chạy tác vụ đó theo cách thủ công.

7. Lưu các thay đổi của bạn.



Cập nhật từ một máy chủ lưu trữ

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.

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.

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. Bật tính năng sao chép gói cập nhật đến một thư mục được chia sẻ trên một máy tính trên mạng máy tính cục bộ.

   Cách bật sao chép gói cập nhật vào thư mục dùng chung trong Bảng điều khiển quản trị (MMC)

   1. Mở Bảng điều khiển quản trị Kaspersky Security Center.

   2. Trong cây bảng điều khiển, hãy chọn **Tasks**.

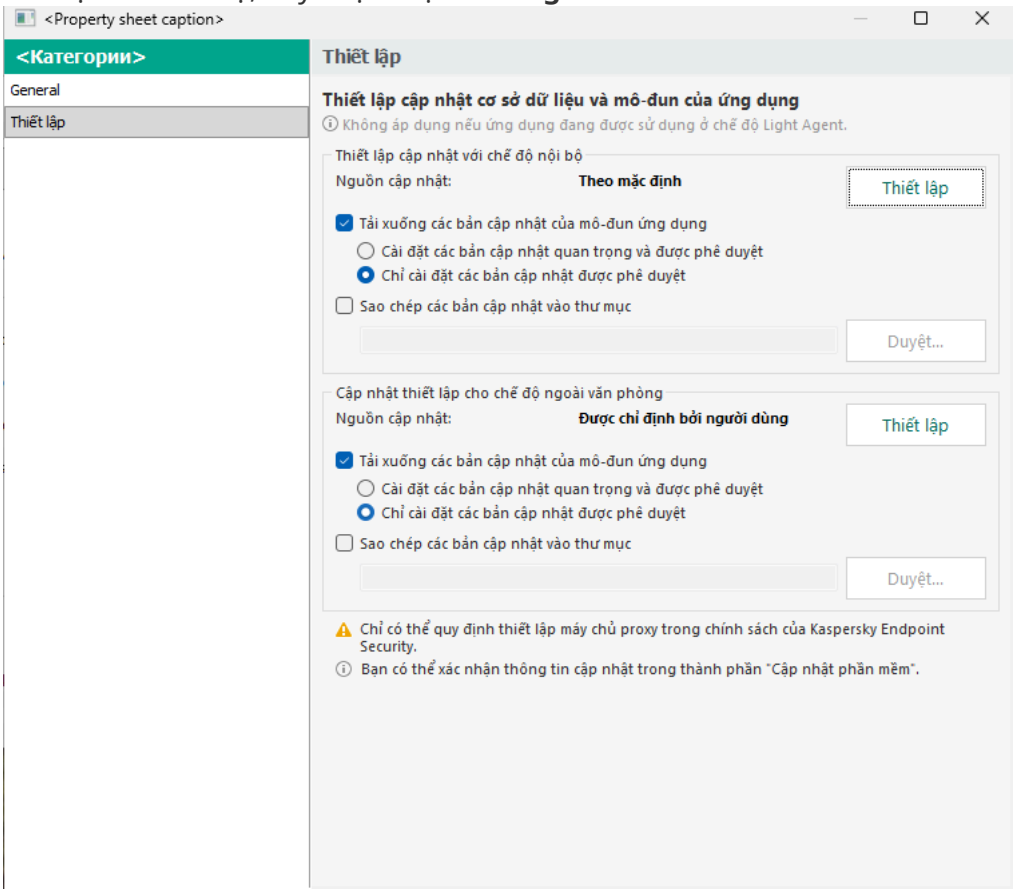
      Tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* phải được gán cho một máy tính làm nguồn cập nhật.

   3. Nhấn vào tác vụ **Cập nhật cơ sở dữ liệu và mô-đun ứng dụng** của Kaspersky Endpoint Security.

      Cửa sổ thuộc tính tác vụ sẽ được mở ra.

      Tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* được tạo tự động bởi trình hướng dẫn sử dụng nhanh Máy chủ quản trị. Để tạo tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*, hãy cài đặt Tiện ích quản lý của Kaspersky Endpoint Security cho Windows khi đang chạy Trình hướng dẫn.

4. Trong cửa sổ thuộc tính tác vụ, hãy chọn mục **Settings**.



Thiết lập tác vụ Cập nhật cơ sở dữ liệu và mô-đun ứng dụng

5. Trong mục **Thiết lập cập nhật với chế độ nội bộ**, hãy nhấn nút **Thiết lập**.

6. 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.

7. Chọn hộp kiểm **Sao chép các bản cập nhật vào thư mục**.

8. Trong trường **Đường dẫn thư mục**, hãy nhập đường dẫn UNC đến thư mục được chia sẻ (ví dụ: `\\<server name>\KLSHARE\Updates`).

   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\AVP12\Update distribution\`.

9. Lưu các thay đổi của bạn.

Cách bật sao chép gói cập nhật vào thư mục dùng chung trong Bảng điều khiển web và Bảng điều khiển đám mây

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

   Danh sách tác vụ sẽ mở.

   > Tác vụ *Update* phải được gán cho một máy tính làm nguồn cập nhật.

2. Nhấn vào tác vụ **Update** của Kaspersky Endpoint Security.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

Tác vụ *Update* được tạo tự động bởi trình hướng dẫn sử dụng nhanh Máy chủ quản trị. Để tạo tác vụ *Update*, hãy cài đặt Tiện ích quản lý 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 name>\KLSHARE\Updates`).

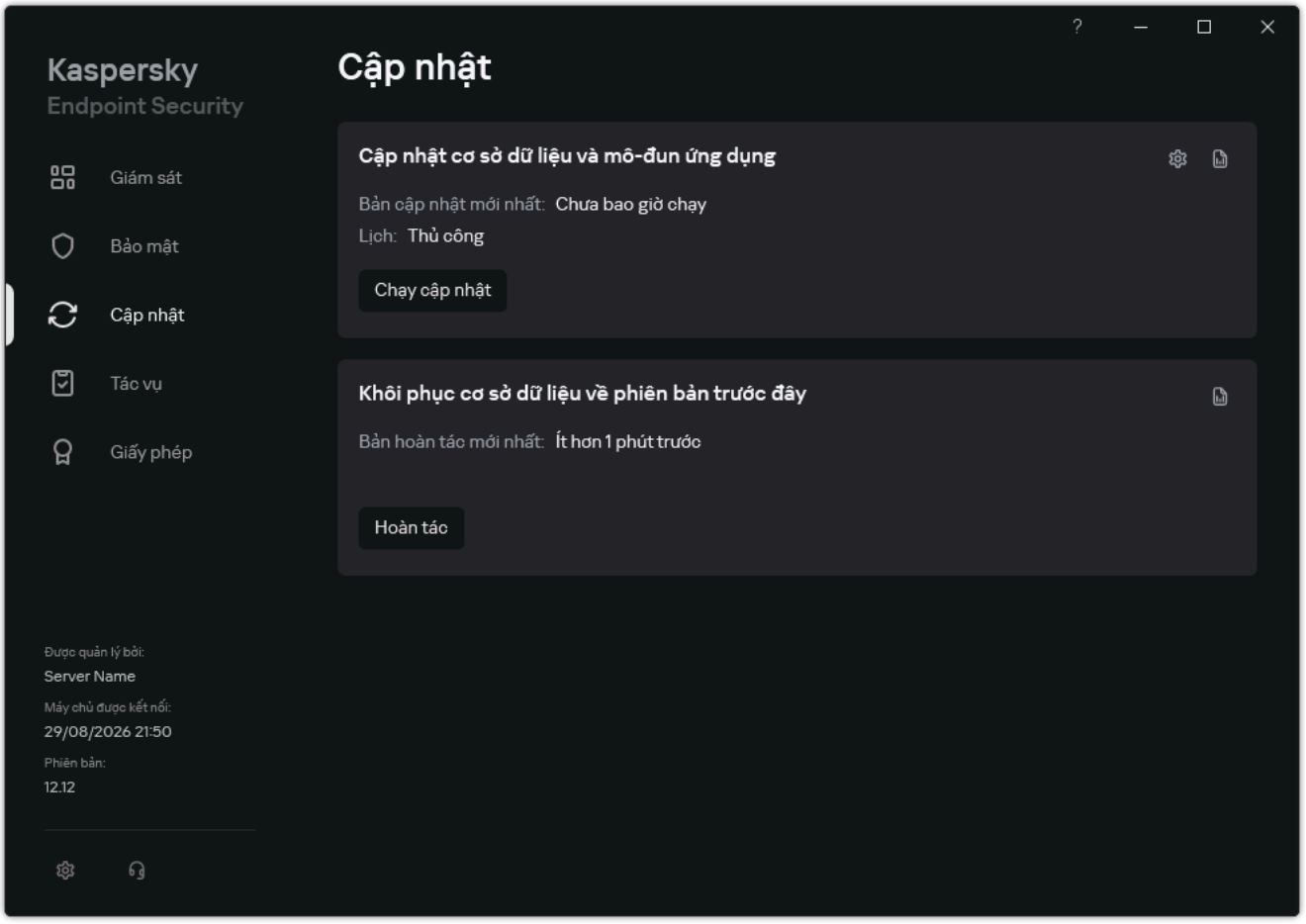
   Nếu trường này được để trống, Kaspersky Endpoint Security sẽ sao chép gói cập nhật vào thư mục `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

7. Lưu các thay đổi của bạn.

Cách bật sao chép gói cập nhật vào thư mục dùng chung trong giao diện ứng dụng

Bạn không thể cấu hình tác vụ nhóm *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* trong giao diện ứng dụng. Chỉ một tác vụ cập nhật cục bộ là *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* khả dụng với người dùng. Nếu tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* không được hiển thị, điều đó có nghĩa là quản trị viên đã cấm sử dụng các tác vụ cục bộ trong chính sách.

1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Cập nhật**.



Tác vụ cập nhật cục bộ

2. Thao tác này sẽ mở ra danh sách tác vụ; hãy chọn tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* và nhấn vào ⚙.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

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 name>\KLSHARE\Updates`).

5. Lưu các thay đổi của bạn.

3. 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.

Cách cấu hình các bản cập nhật từ thư mục được chia sẻ trong Bảng điều khiển quản trị (MMC)

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

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **Add**.

   Trình hướng dẫn Tác vụ sẽ được bắt đầu.

3. Cấu hình các thiết lập của tác vụ:

   a. Trong danh sách thả xuống **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.

   b. Trong danh sách thả xuống **Task type**, hãy chọn **Cập nhật cơ sở dữ liệu và mô-đun ứng dụng**.

4. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Tasks**.

   Danh sách tác vụ sẽ mở.

5. Nhấn vào **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 (14.2) → Cập nhật cơ sở dữ liệu và mô-đun ứng dụng**.

Bước 2. Chọn nguồn cập nhật

Thêm một nguồn cập nhật mới: một thư mục được chia sẻ. Địa chỉ nguồn phải trùng với địa chỉ bạn đặt trước đây trong trường **Đường dẫn thư mục** khi bạn cấu hình sao chép gói cập nhật vào thư mục chia sẻ. Cấu hình các ưu tiên của nguồn cập nhật bằng cách sử dụng nút **Lên** và **Xuống**.

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.

Tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* phải được gán cho các máy tính của mạng LAN của tổ chức, ngoại trừ máy tính làm nguồn cập nhật.

Bước 4. Chọn tài khoản để chạy tác vụ

Chọn một tài khoản để chạy tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*. Theo mặc định, Kaspersky Endpoint Security khởi chạy tác vụ với quyền của tài khoản người dùng cục bộ.

Bước 5. 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 6. Xác định tên tác vụ

Nhập tên của tác vụ, ví dụ: *Cập nhật từ một thư mục được chia sẻ*.

Bước 7. Hoàn tất việc tạo tác vụ

Hoàn tất 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 cập nhật sẽ được thực thi trên máy tính của người dùng theo lịch trình đã chỉ định.

Cách cấu hình cập nhật từ thư mục được chia sẻ trong Bảng điều khiển web và Bảng điều khiển đám mây

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

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **Add**.

   Trình hướng dẫn Tác vụ sẽ được bắt đầu.

3. Cấu hình các thiết lập của tác vụ:

   a. Trong danh sách thả xuống **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.

   b. Trong danh sách thả xuống **Task type**, hãy chọn **Update**.

   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 **Devices to which the task will be assigned**, chọn phạm vi tác vụ.

   > Tác vụ *Update* phải được gán cho các máy tính của mạng LAN của tổ chức, 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. Hoàn tất trình hướng dẫn.
   Một tác vụ mới sẽ được hiển thị trong bảng các tác vụ.
6. Nhấn vào tác vụ *Update* mới được tạo.
   Cửa sổ thuộc tính tác vụ sẽ được mở ra.
7. Chọn thẻ **Application settings → Local mode**.
8. Trong mục **Update sources**, hãy nhấn nút **Add**.
9. Trong cửa sổ mở ra, hãy nhập đường dẫn đến thư mục được chia sẻ.

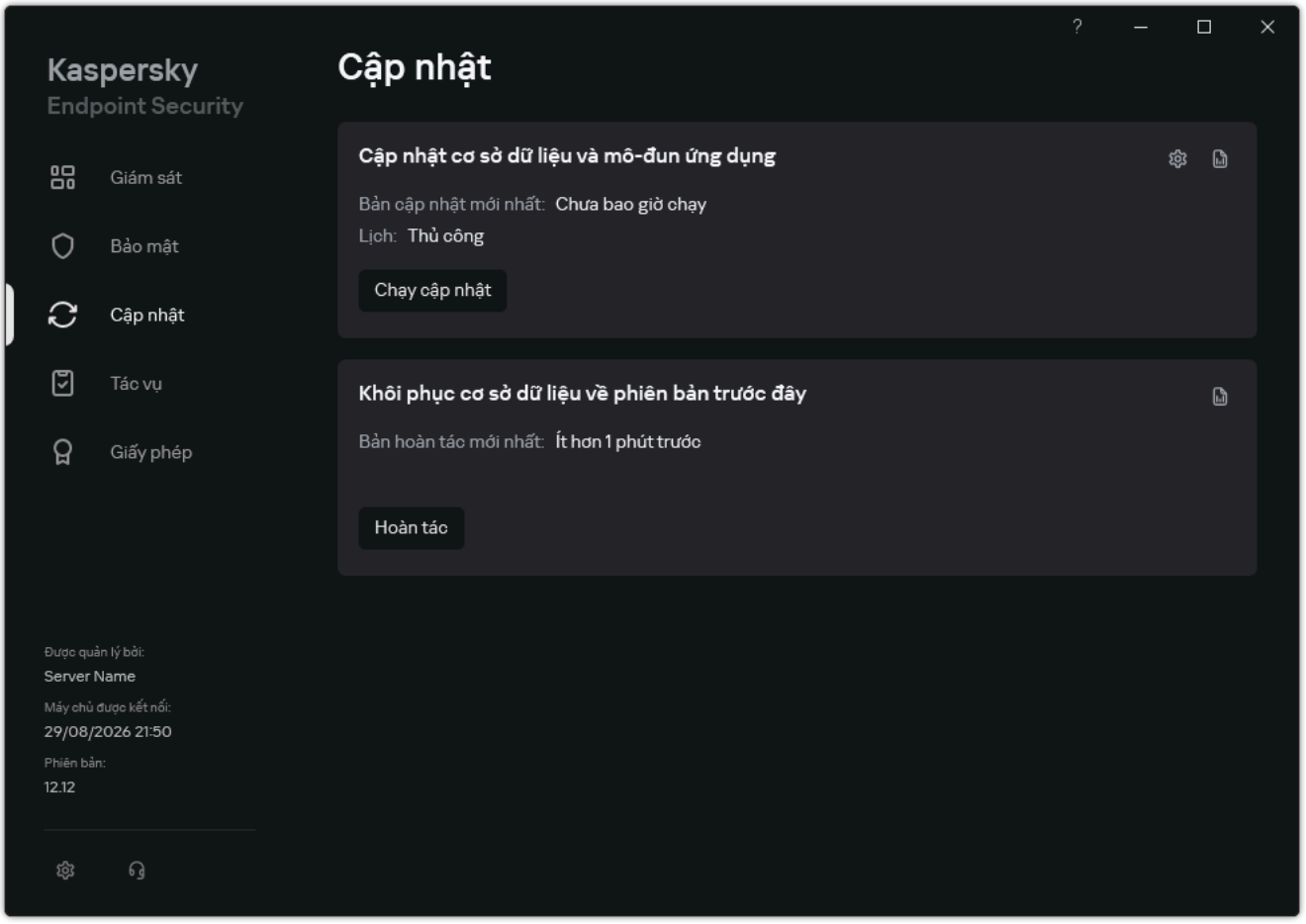
   > Địa chỉ nguồn phải trùng với địa chỉ bạn đặt trước đây trong trường **Path** khi bạn cấu hình sao chép gói cập nhật vào thư mục chia sẻ (xem các hướng dẫn bên trên).

10. Nhấn vào **OK**.
11. Cấu hình các ưu tiên của nguồn cập nhật bằng cách sử dụng nút **Move up** và **Move down**.
12. Lưu các thay đổi của bạn.

Cách cấu hình cập nhật từ thư mục được chia sẻ trong giao diện ứng dụng

Bạn không thể cấu hình tác vụ nhóm *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* trong giao diện ứng dụng. Chỉ một tác vụ cập nhật cục bộ là *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* khả dụng với người dùng. Nếu tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* không được hiển thị, điều đó có nghĩa là quản trị viên đã cấm sử dụng các tác vụ cục bộ trong chính sách.

1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Cập nhật**.



Tác vụ cập nhật cục bộ

2. Thao tác này sẽ mở ra danh sách tác vụ; hãy chọn tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* và nhấn vào ⚙.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

3. Nhấn vào **Chọn nguồn cập nhật**.

4. Trong cửa sổ mở ra, hãy nhấn nút **Thêm**.

5. Trong cửa sổ mở ra, hãy nhập đường dẫn đến thư mục được chia sẻ.

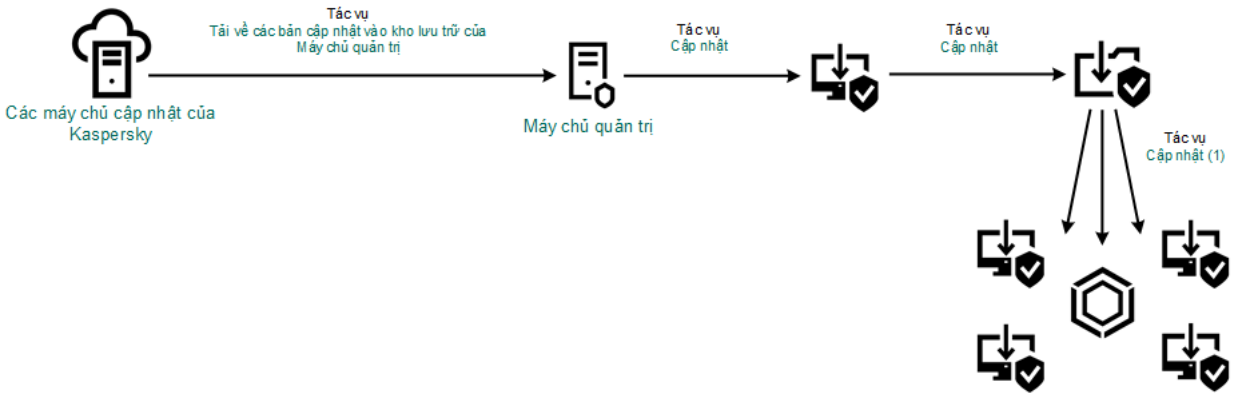
   Địa chỉ nguồn phải trùng với địa chỉ bạn chỉ định từ trước khi bạn cấu hình sao chép gói cập nhật vào thư mục chia sẻ (xem các hướng dẫn bên trên).

6. Nhấn vào **Lựa chọn**.

7. Cấu hình các ưu tiên của nguồn cập nhật bằng cách sử dụng nút **Lên** và **Xuống**.

   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.

8. Lưu các thay đổi của bạn.



Cập nhật từ một thư mục được chia sẻ

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.

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.

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.

   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.

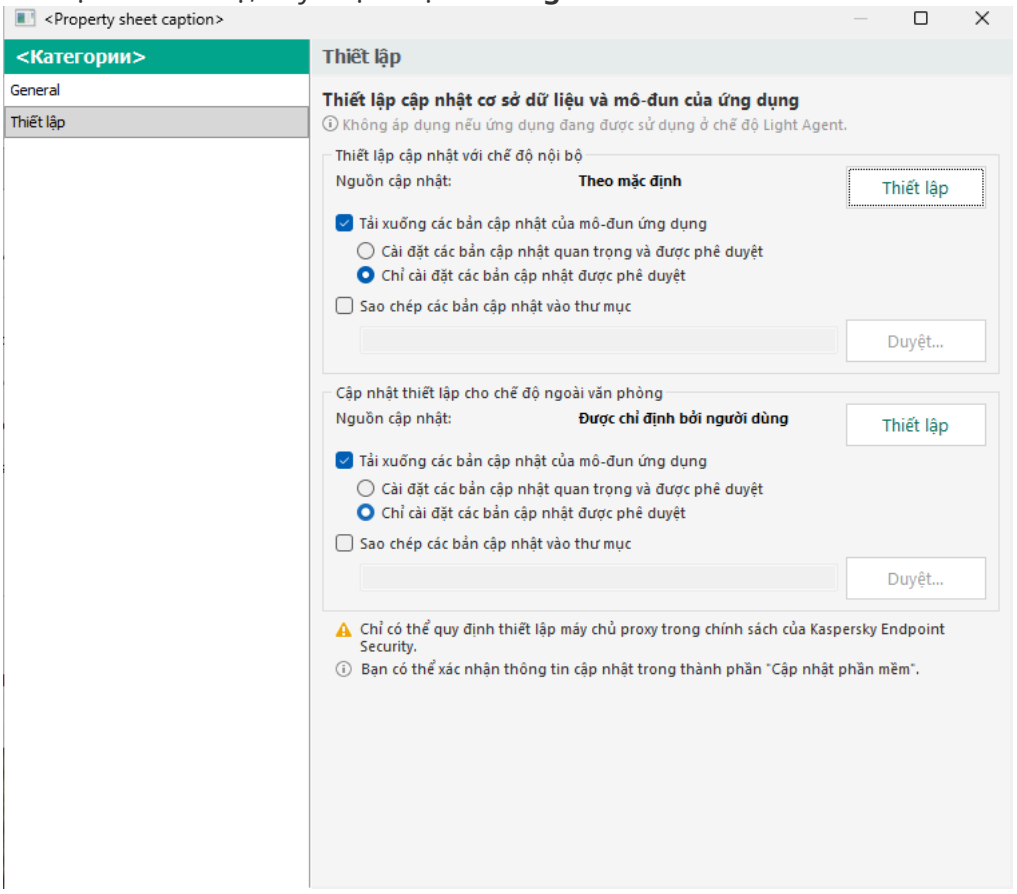
4. Cấu hình việc cập nhật cơ sở dữ liệu và mô-đun ứng dụng từ một thư mục được chia sẻ cụ thể đến các máy tính còn lại trên mạng LAN doanh nghiệp.

Cách cấu hình các bản cập nhật từ thư mục được chia sẻ trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Tasks**.
3. Nhấn vào tác vụ **Cập nhật cơ sở dữ liệu và mô-đun ứng dụng** của Kaspersky Endpoint Security.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

   Tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* được tạo tự động bởi trình hướng dẫn sử dụng nhanh Máy chủ quản trị. Để tạo tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*, hãy cài đặt Tiện ích quản lý của Kaspersky Endpoint Security cho Windows khi đang chạy Trình hướng dẫn.
4. Trong cửa sổ thuộc tính tác vụ, hãy chọn mục **Settings**.



Thiết lập tác vụ Cập nhật cơ sở dữ liệu và mô-đun ứng dụng

5. Trong mục **Thiết lập cập nhật với chế độ nội bộ**, hãy nhấn nút **Thiết lập**.
6. Trong danh sách các nguồn cập nhật, nhấn nút **Thêm**.
7. Trong cửa sổ mở ra, hãy nhập đường dẫn UNC đến thư mục chia sẻ (ví dụ: `\\<server name>\KLSHARE\Updates`).

   Địa chỉ nguồn phải trùng với địa chỉ được ghi trong thiết lập của Kaspersky Update Utility.
8. Nhấn vào **OK**.

9. Cấu hình các ưu tiên của nguồn cập nhật bằng cách sử dụng nút **Lên** và **Xuống**.

   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.

10. Lưu các thay đổi của bạn.

Cách cấu hình cập nhật từ thư mục được chia sẻ trong Bảng điều khiển web và Bảng điều khiển đám mây

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

   Danh sách tác vụ sẽ mở.

2. Nhấn vào tác vụ **Update** của Kaspersky Endpoint Security.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

   Tác vụ *Update* được tạo tự động bởi trình hướng dẫn sử dụng nhanh Máy chủ quản trị. Để tạo tác vụ *Update*, hãy cài đặt Tiện ích quản lý 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 cửa sổ mở ra, hãy nhập đường dẫn UNC đến thư mục chia sẻ (ví dụ: `\\<server name>\KLSHARE\Updates`).

   > Địa chỉ nguồn phải trùng với địa chỉ được ghi trong thiết lập của Kaspersky Update Utility.

6. Nhấn vào **OK**.

7. Cấu hình các ưu tiên của nguồn cập nhật bằng cách sử dụng nút **Lên** và **Xuống**.

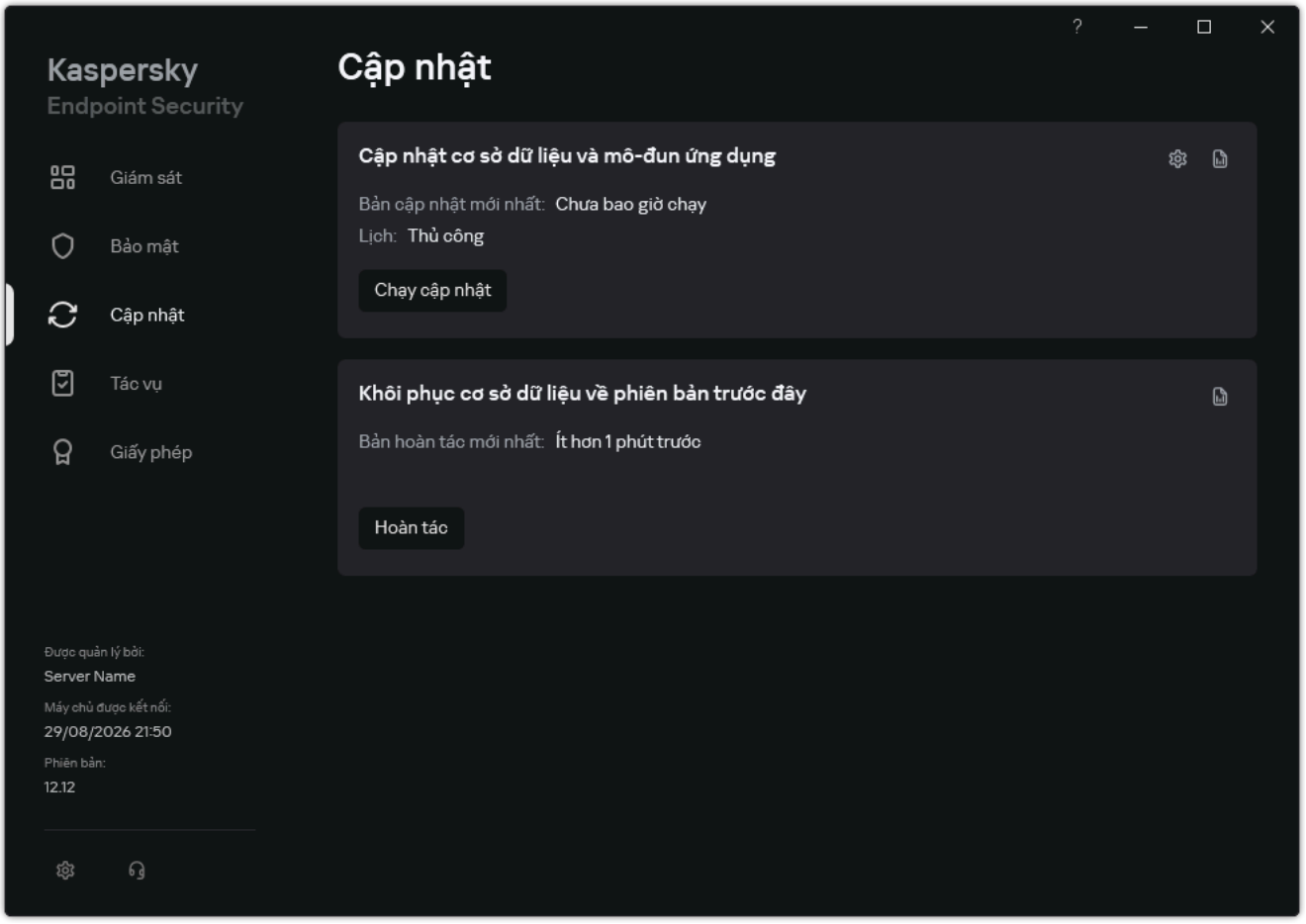
   Nếu không thể thực hiện một bản cập nhật từ nguồn cập nhật đầu tiên, Kaspersky Endpoint Security sẽ tự động chuyển sang nguồn tiếp theo.

8. Lưu các thay đổi của bạn.

Cách cấu hình cập nhật từ thư mục được chia sẻ trong giao diện ứng dụng

Bạn không thể cấu hình tác vụ nhóm *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* trong giao diện ứng dụng. Chỉ một tác vụ cập nhật cục bộ là *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* khả dụng với người dùng. Nếu tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* không được hiển thị, điều đó có nghĩa là quản trị viên đã cấm sử dụng các tác vụ cục bộ trong chính sách.

1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Cập nhật**.



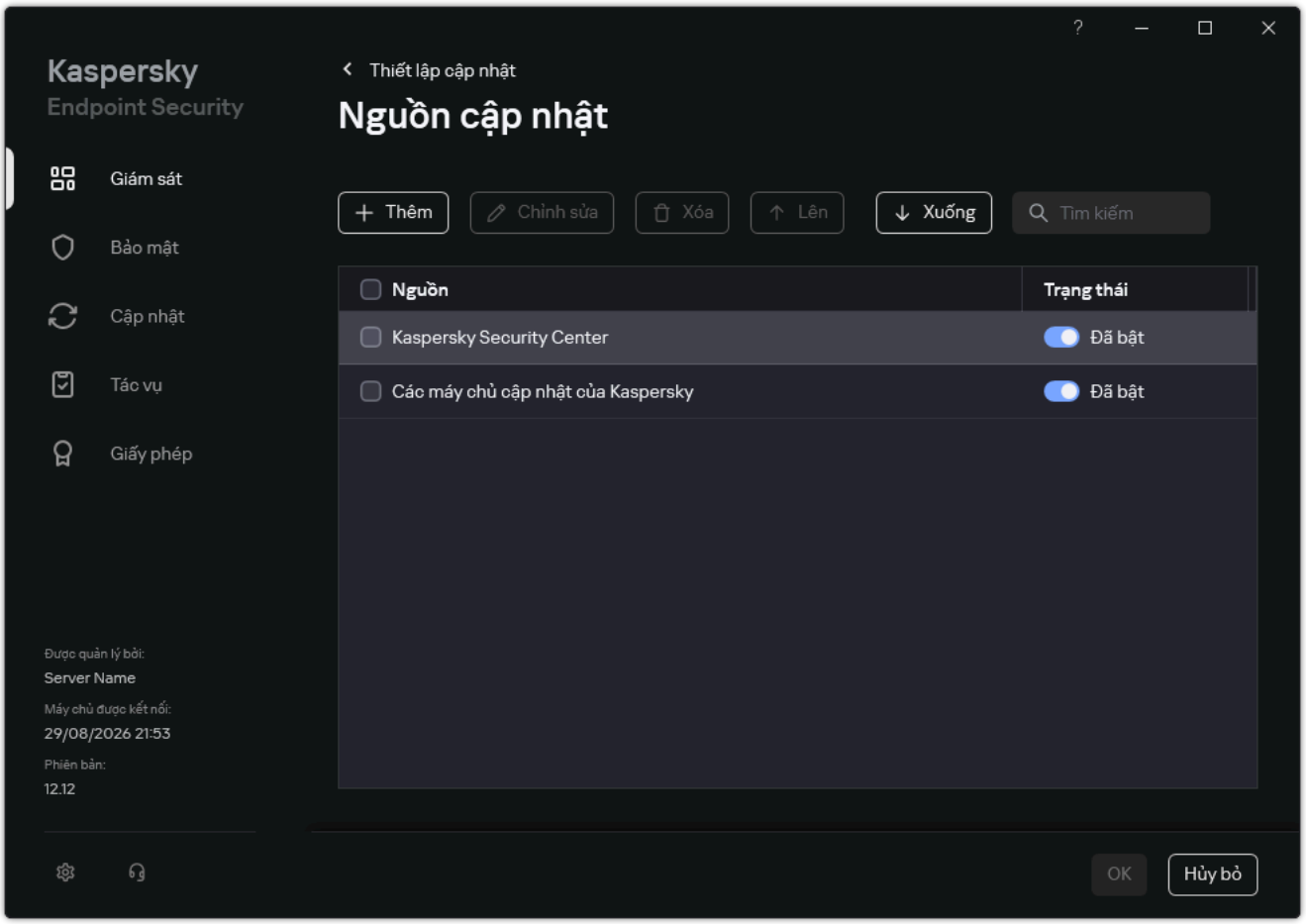
Tác vụ cập nhật cục bộ

2. Thao tác này sẽ mở ra danh sách tác vụ; hãy chọn tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* và nhấn vào ⚙.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

3. Trong cửa sổ thuộc tính tác vụ, hãy nhấn vào **Chọn nguồn cập nhật**.

4. Trong danh sách các nguồn cập nhật, nhấn nút **Thêm**.



Nguồn cập nhật

5. Nhập đường dẫn UNC đến thư mục được chia sẻ (ví dụ: `\\<server name>\KLSHARE\Updates`).

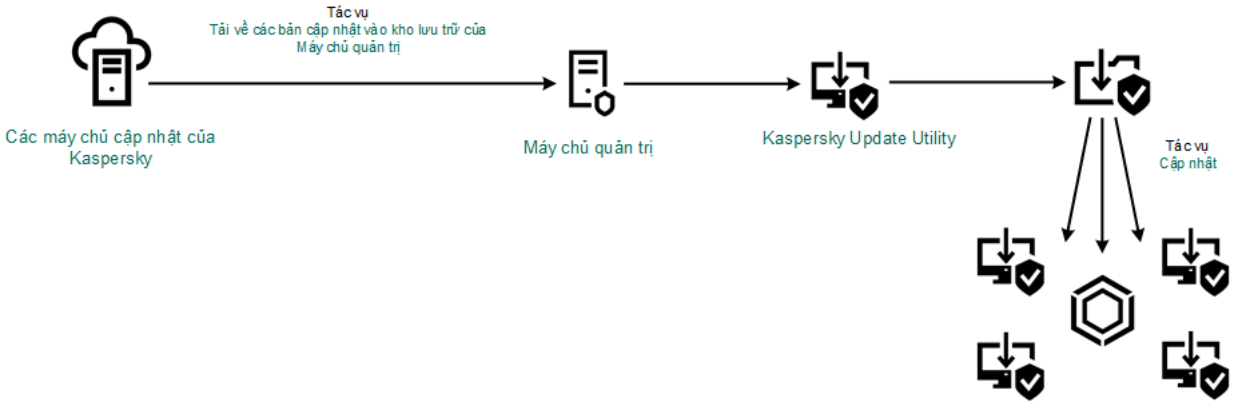
> Địa chỉ nguồn phải trùng với địa chỉ được ghi trong thiết lập của Kaspersky Update Utility.

6. Nhấn vào **Lựa chọn**.

7. Cấu hình các ưu tiên của nguồn cập nhật bằng cách sử dụng nút **Lên** và **Xuống**.

   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.

8. Lưu các thay đổi của bạn.



Cập nhật sử dụng Kaspersky Update Utility

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.

Cách cấu hình thiết lập cập nhật cho chế độ di động trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.

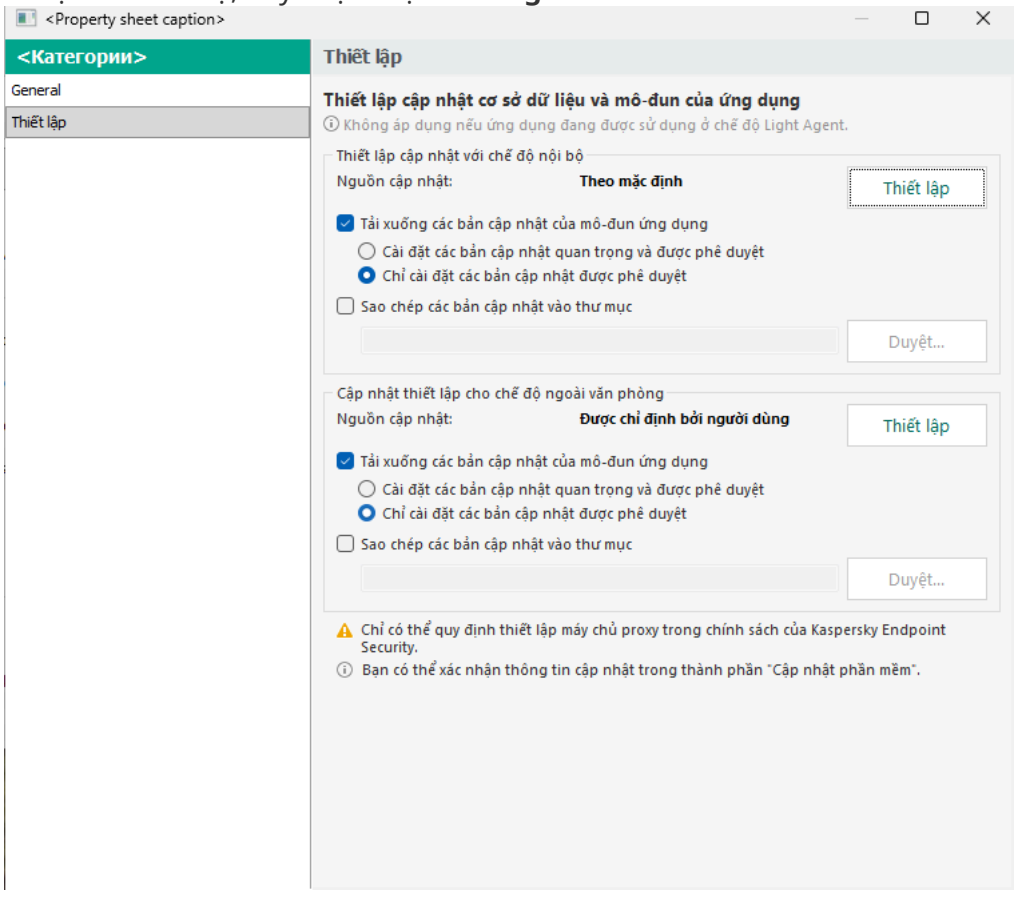
2. Trong cây bảng điều khiển, hãy chọn **Tasks**.

3. Nhấn vào tác vụ **Cập nhật cơ sở dữ liệu và mô-đun ứng dụng** của Kaspersky Endpoint Security.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

   Tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* được tạo tự động bởi trình hướng dẫn sử dụng nhanh Máy chủ quản trị. Để tạo tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*, hãy cài đặt Tiện ích quản lý của Kaspersky Endpoint Security cho Windows khi đang chạy Trình hướng dẫn.

4. Trong cửa sổ thuộc tính tác vụ, hãy chọn mục **Settings**.



Thiết lập tác vụ Cập nhật cơ sở dữ liệu và mô-đun ứng dụng

5. Trong mục **Cập nhật thiết lập cho chế độ ngoài văn phòng**, hãy nhấn nút **Thiết lập**.

6. 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.

7. Lưu các thay đổi của bạn.

Cách cấu hình thiết lập cập nhật cho chế độ 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 **Tasks**.

   Danh sách tác vụ sẽ mở.

2. Nhấn vào tác vụ **Update** của Kaspersky Endpoint Security.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

   Tác vụ *Update* được tạo tự động bởi trình hướng dẫn sử dụng nhanh Máy chủ quản trị. Để tạo tác vụ *Update*, hãy cài đặt Tiện ích quản lý của Kaspersky Endpoint Security cho Windows khi đang chạy Trình hướng dẫn.

3. Chọn thẻ **Application settings** → **Mobile mode**.

4. 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.

5. 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

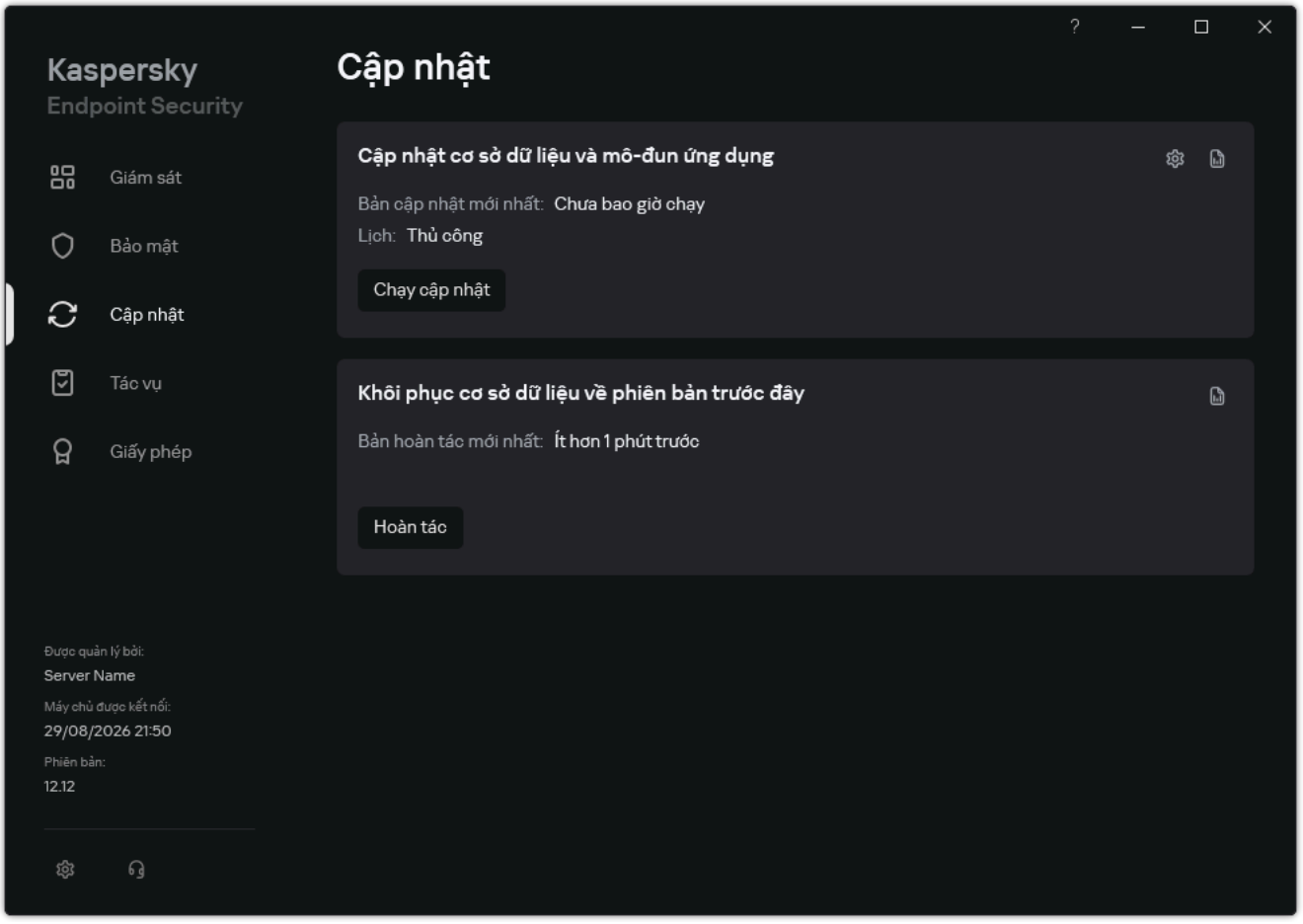
Bắt đầu một tác vụ cập nhật theo quyền của một tài khoản người dùng khác

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 thiết lập ứng dụng, bạn có thể chỉ định một người dùng có các quyền đó và khởi chạy 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:

Bạn không thể cấu hình tác vụ nhóm *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* trong giao diện ứng dụng. Chỉ một tác vụ cập nhật cục bộ là *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* khả dụng với người dùng. Nếu tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* không được hiển thị, điều đó có nghĩa là quản trị viên đã cấm sử dụng các tác vụ cục bộ trong chính sách.

1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Cập nhật**.



Tác vụ cập nhật cục bộ

2. Thao tác này sẽ mở ra danh sách tác vụ; hãy chọn tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* và nhấn vào ⚙.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

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

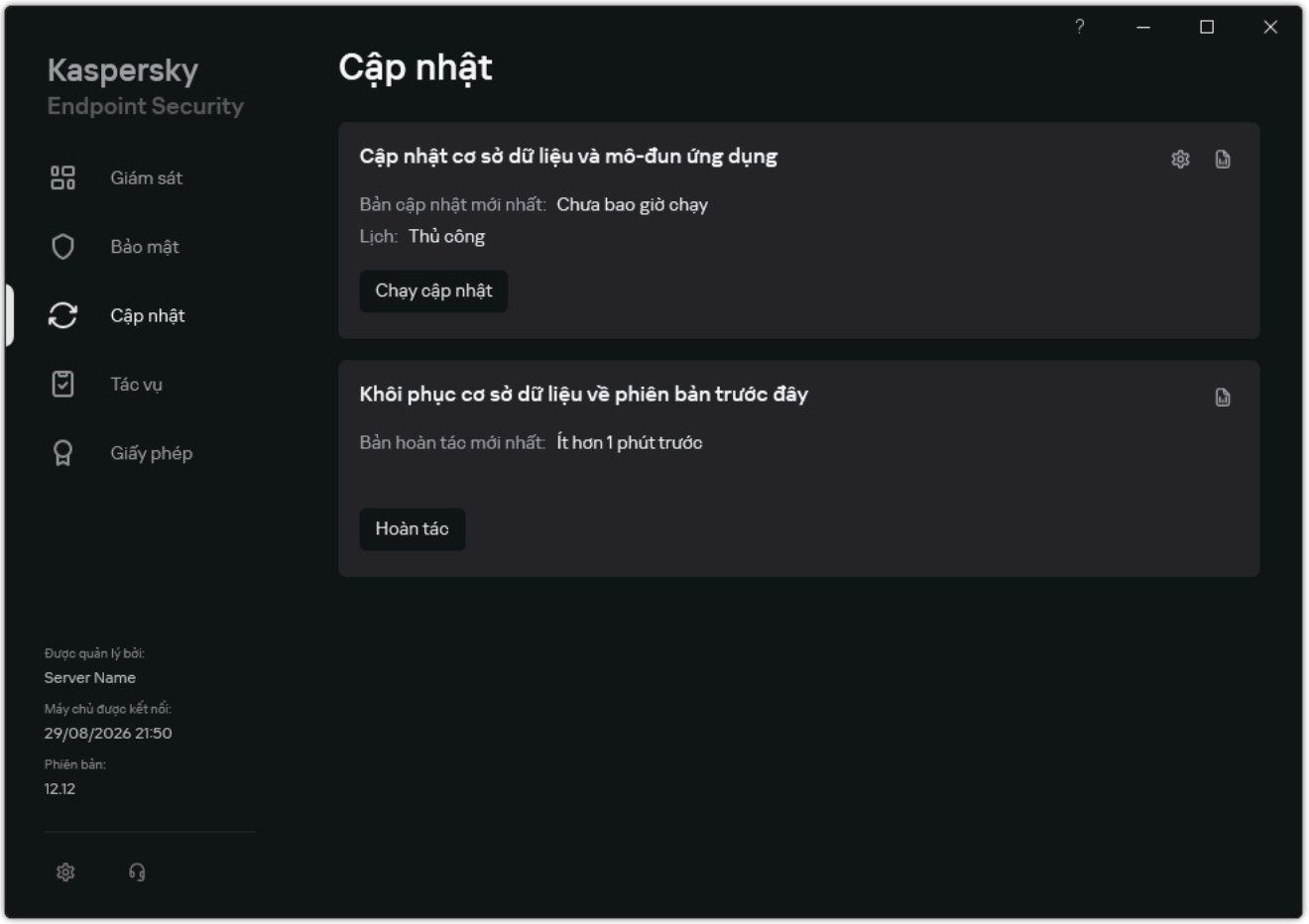
Nếu không thể chạy tác vụ cập nhật vì bất cứ lý do gì (ví dụ, máy tính đang tắt tại thời điểm đó), bạn có thể thiết lập tác vụ bị bỏ qua được tự động chạy lại ngay khi có thể.

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:

Bạn không thể cấu hình tác vụ nhóm *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* trong giao diện ứng dụng. Chỉ một tác vụ cập nhật cục bộ là *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* khả dụng với người dùng. Nếu tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* không được hiển thị, điều đó có nghĩa là quản trị viên đã cấm sử dụng các tác vụ cục bộ trong chính sách.

1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Cập nhật**.



Tác vụ cập nhật cục bộ

2. Thao tác này sẽ mở ra danh sách tác vụ; hãy chọn tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* và nhấn vào ⚙.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

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. Khi ứng dụng có cơ hội thực thi các tác vụ bị bỏ lỡ, ứng dụng sẽ chạy các tác vụ một cách ngẫu nhiên trong một khoảng thời gian nhất định để phân phối tải trên máy tính.

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, máyy chủ cập nhật của Kaspersky và các thư mục cục bộ hoặc thư mục mạng.

> Nếu máy chủ cập nhật của Kaspersky không khả dụng, Kaspersky Endpoint Security có thể sử dụng các tên miền thay thế để cập nhật cơ sở dữ liệu và các mô-đun phần mềm ứng dụng. Để biết thông tin chi tiết, hãy tham khảo Cơ sở tri thức Hỗ trợ kỹ thuật.

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 hồi gói cập nhật từ nguồn khả dụng đầu tiên.

Theo mặc định, Kaspersky Endpoint Security sử dụng máy chủ Kaspersky Security Center làm nguồn cập nhật đầu tiên. Điều này giúp tiết kiệm lưu lượng khi cập nhật. Nếu một chính sách không được áp dụng cho máy tính, các máy chủ của Kaspersky sẽ được chọn làm nguồn cập nhật đầu tiên trong thiết lập của tác vụ cục bộ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* vì ứng dụng có thể không có quyền truy cập vào máy chủ Kaspersky Security Center.

Nếu ứng dụng đang chạy trong Chế độ Light Agent thì một thư mục trên SVM sẽ được chọn làm nguồn cập nhật.

Cách thêm nguồn cập nhật trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.

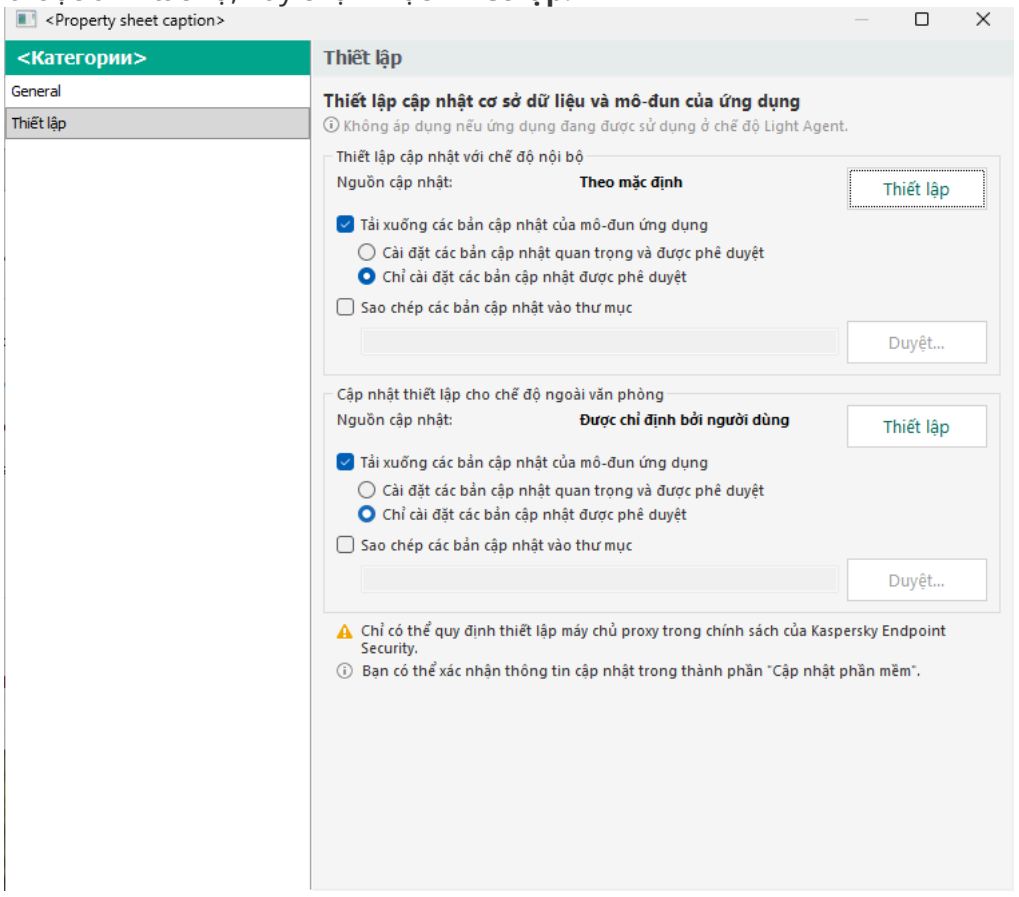
   Trong cây bảng điều khiển, hãy chọn **Tasks**.

2. Nhấn vào tác vụ **Cập nhật cơ sở dữ liệu và mô-đun ứng dụng** của Kaspersky Endpoint Security.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

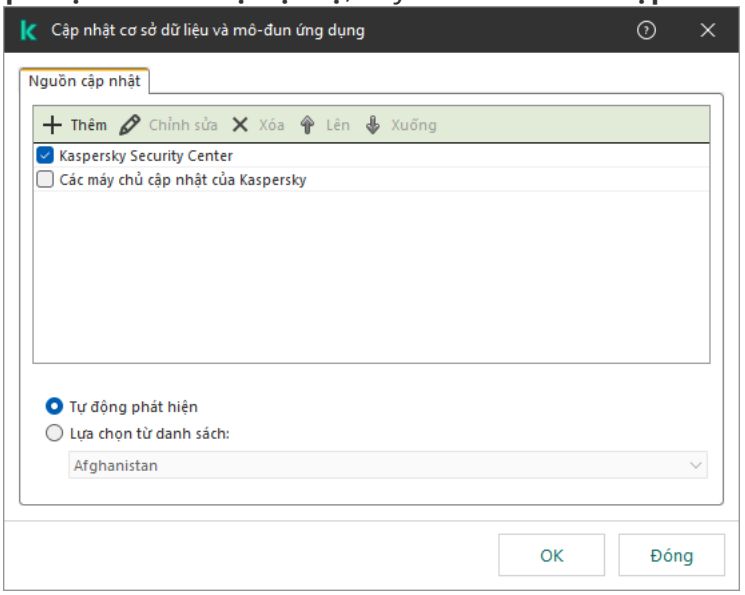
   Tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* được tạo tự động bởi trình hướng dẫn sử dụng nhanh Máy chủ quản trị. Để tạo tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*, hãy cài đặt Tiện ích quản lý của Kaspersky Endpoint Security cho Windows khi đang chạy Trình hướng dẫn.

3. Trong cửa sổ thuộc tính tác vụ, hãy chọn mục **Thiết lập**.



Thiết lập tác vụ Cập nhật cơ sở dữ liệu và mô-đun ứng dụng

4. Trong mục **Thiết lập cập nhật với chế độ nội bộ**, hãy nhấn nút **Thiết lập**.



Nguồn cập nhật

5. Trong danh sách các nguồn cập nhật, nhấn nút **Thêm**.

6. Trong trường **Nguồn cập nhật**, hãy chỉ định địa chỉ của máy chủ FTP hoặc HTTP, thư mục mạng hoặc thư mục trên máy chứa gói cậpp 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://dnl-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://<user name>:<password>@<node>:<port>`.

   - 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\AVP12\Update distribution\`.

   Bạn có thể loại trừ nguồn cập nhật mà không cần xóa nó khỏi danh sách nguồn cập nhật. Để thực hiện, hãy bỏ chọn hộp kiểm bên cạnh đối tượng.

7. Nhấn vào **OK**.

8. Cấu hình các ưu tiên của nguồn cập nhật bằng cách sử dụng nút **Lên** và **Xuống**.

   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.

9. Nếu cần, hãy thêm nguồn cập nhật cho 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*).

10. Lưu các thay đổi của bạn.

Cách thêm nguồn cập nhật trong Bảng điều khiển web

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

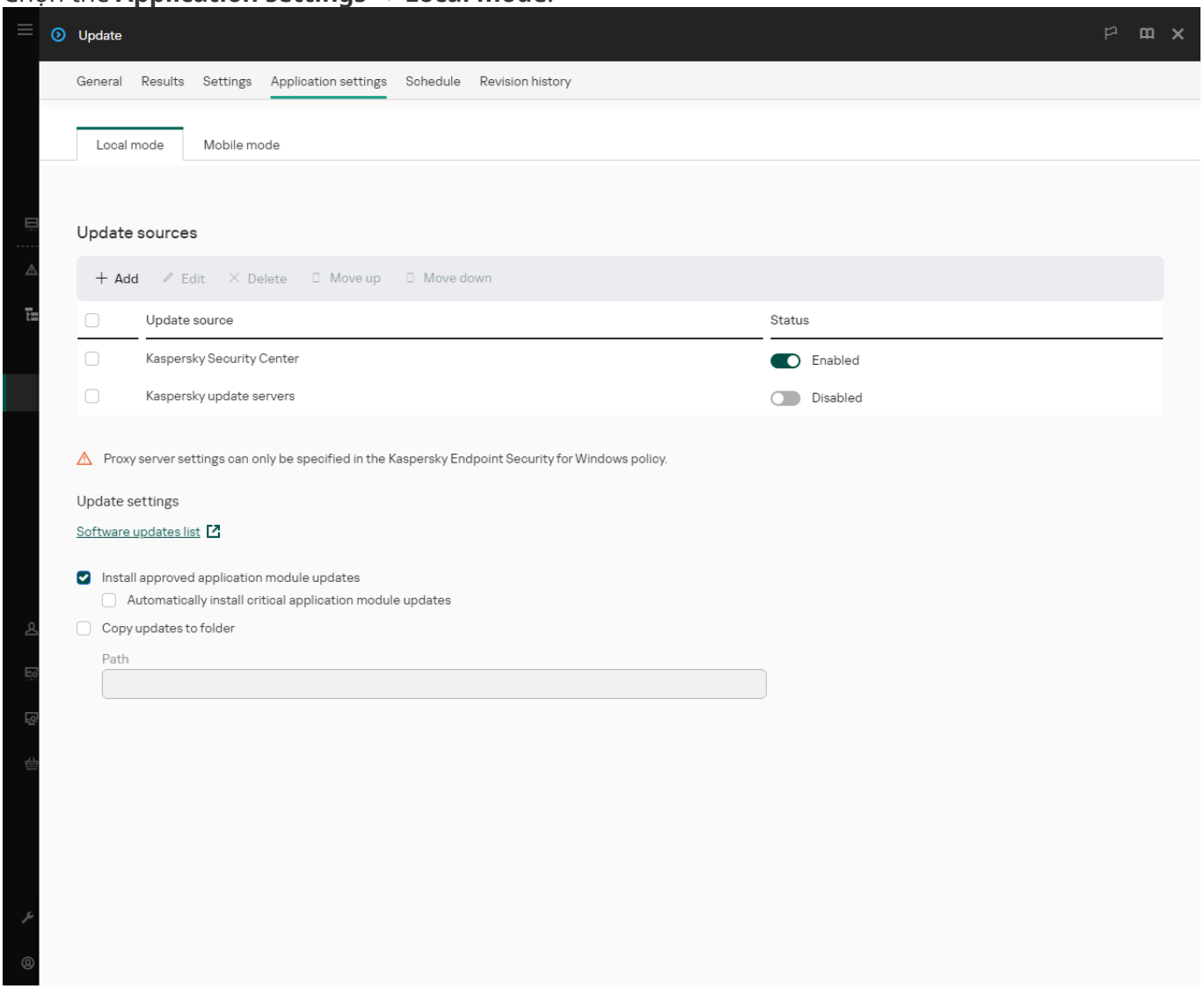
   Danh sách tác vụ sẽ mở.

2. Nhấn vào tác vụ **Update** của Kaspersky Endpoint Security.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

   Tác vụ *Update* được tạo tự động bởi trình hướng dẫn sử dụng nhanh Máy chủ quản trị. Để tạo tác vụ *Update*, hãy cài đặt Tiện ích quản lý của Kaspersky Endpoint Security cho Windows khi đang chạy Trình hướng dẫn.

3. Chọn thẻ **Application settings** → **Local mode**.



Nguồn cập nhật

4. Trong danh sách các nguồn cập nhật, nhấn nút **Add**.

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 cậpp 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://dnl-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://<user name>:<password>@<node>:<port>`.

- 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\AVP12\Update distribution\`.

Bạn có thể loại trừ nguồn cập nhật mà không cần xóa nó khỏi danh sách nguồn cập nhật. Để thực hiện, hãy gạt công tắc bật/tắt bên cạnh sang vị trí tắt.

6. Nhấn vào **OK**.

7. Cấu hình các ưu tiên của nguồn cập nhật bằng cách sử dụng nút **Move up** và **Move down**.

   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.

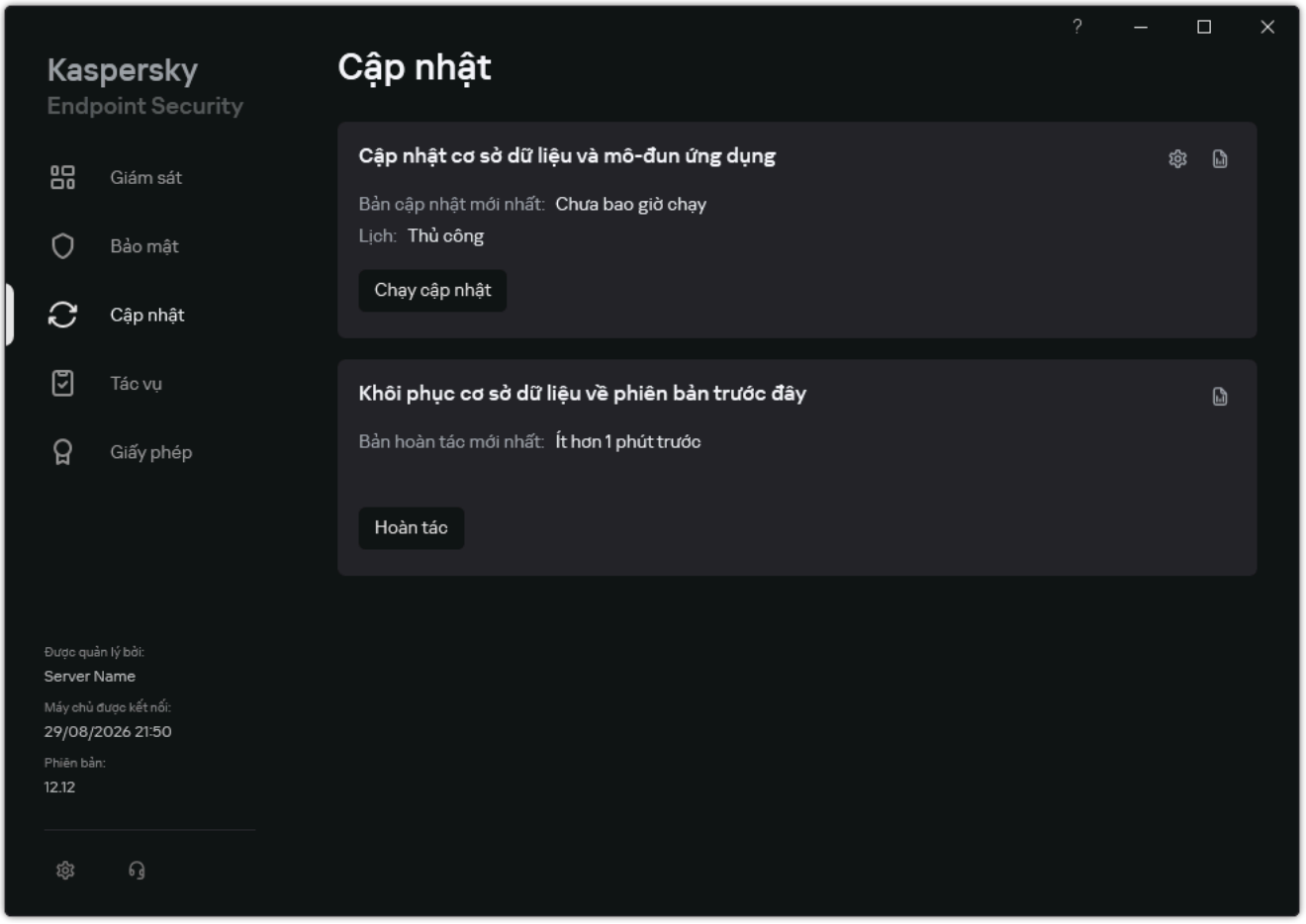
8. Nếu cần, hãy thêm nguồn cập nhật cho chế độ di động. *Chế độ di động* là chế độ hoạt động của Kaspersky Endpoint Security khi một máy tính rời khỏi mạng của tổ chức (*máy tính ngoại tuyến*).

9. Lưu các thay đổi của bạn.

Cách thêm nguồn cập nhật vào giao diện ứng dụng

Bạn không thể cấu hình tác vụ nhóm *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* trong giao diện ứng dụng. Chỉ một tác vụ cập nhật cục bộ là *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* khả dụng với người dùng. Nếu tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* không được hiển thị, điều đó có nghĩa là quản trị viên đã cấm sử dụng các tác vụ cục bộ trong chính sách.

1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Cập nhật**.



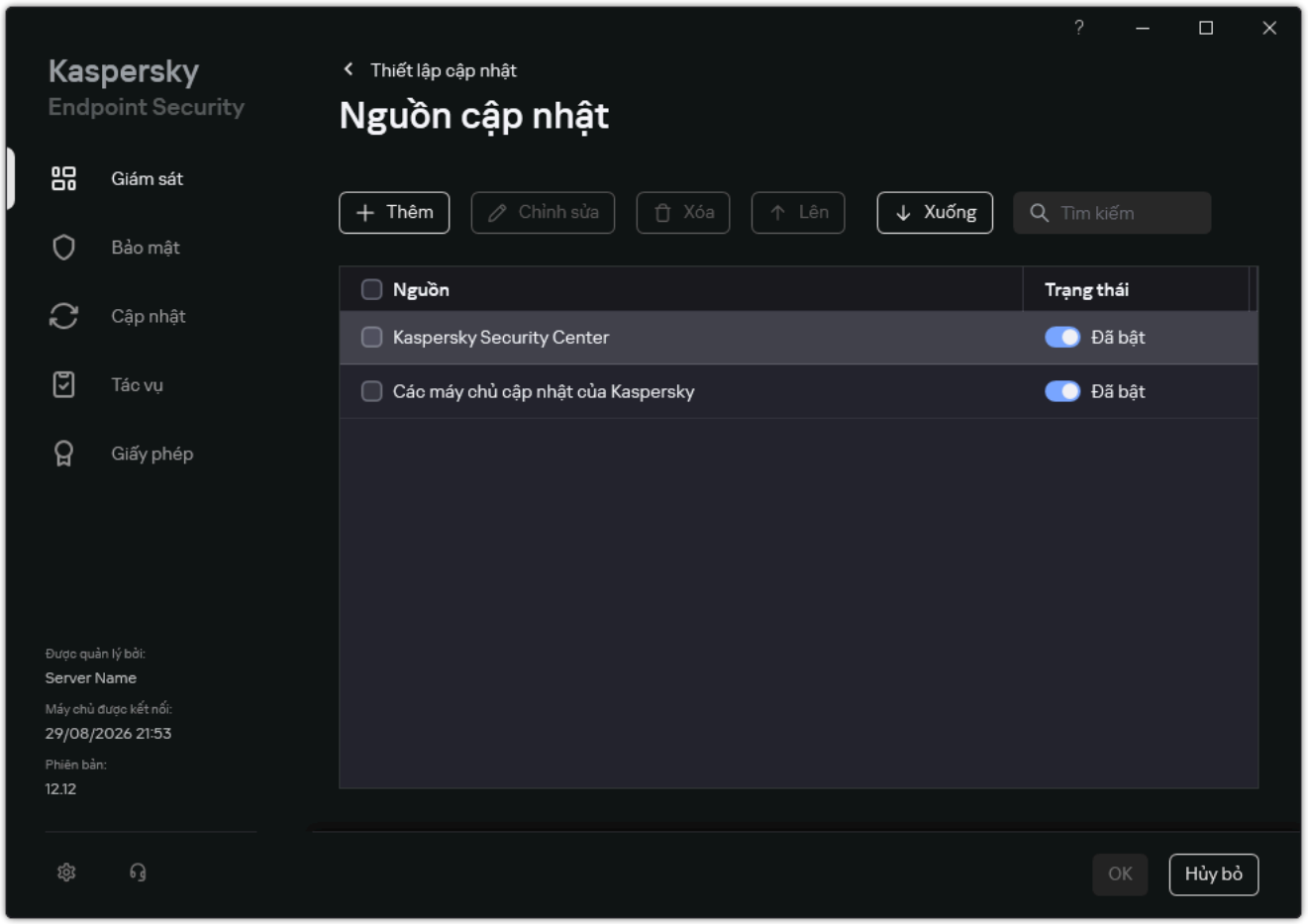
Tác vụ cập nhật cục bộ

2. Thao tác này sẽ mở ra danh sách tác vụ; hãy chọn tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* và nhấn vào ⚙.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

3. Nhấn vào **Chọn nguồn cập nhật**.

4. Trong cửa sổ mở ra, hãy nhấn nút **Thêm**.



Nguồn cập nhật

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 cậpp 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://dnl-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://<user name>:<password>@<node>:<port>`.

   - 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\AVP12\Update distribution\`.

6. Nhấn vào **Lựa chọn**.

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 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.

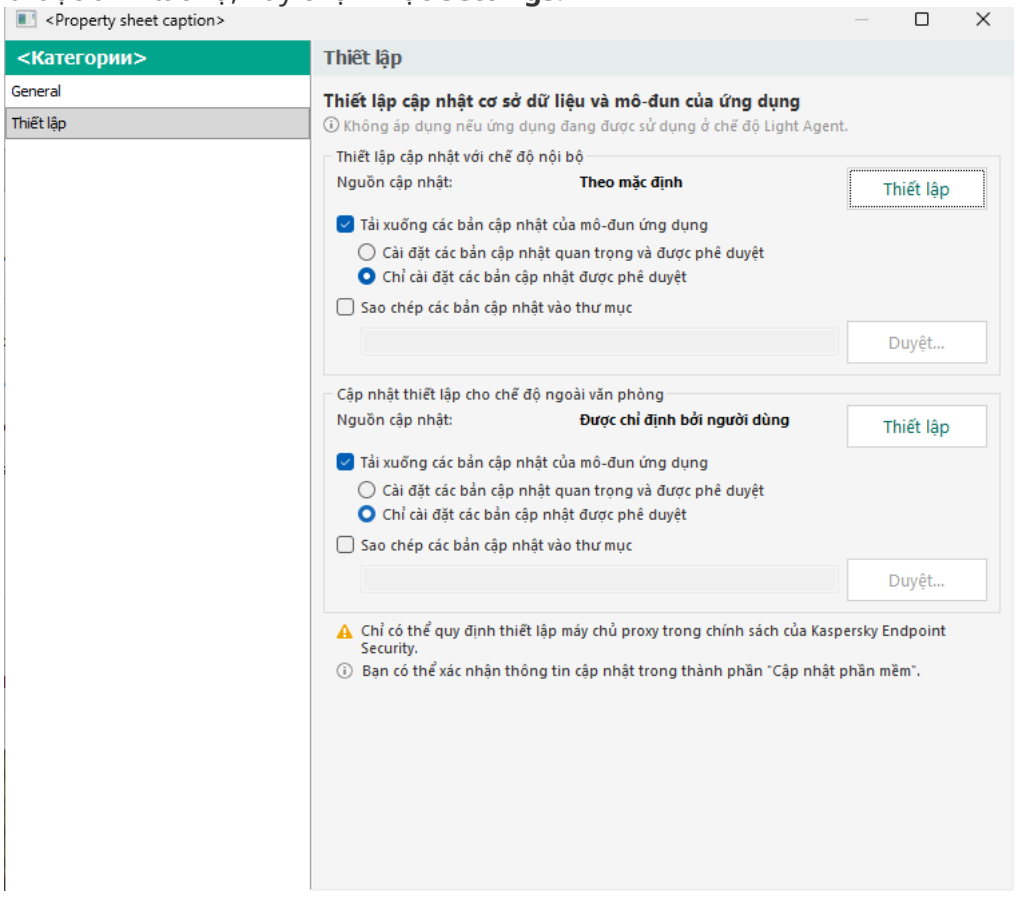
Sau khi cài đặt bản cập nhật ứng dụng, bạn có thể được yêu cầu khởi động lại máy tính.

Cách cấu hình cập nhật mô-đun ứng dụng trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Tasks**.
3. Nhấn vào tác vụ **Cập nhật cơ sở dữ liệu và mô-đun ứng dụng** của Kaspersky Endpoint Security.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

   Tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* được tạo tự động bởi trình hướng dẫn sử dụng nhanh Máy chủ quản trị. Để tạo tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*, hãy cài đặt Tiện ích quản lý của Kaspersky Endpoint Security cho Windows khi đang chạy Trình hướng dẫn.
4. Trong cửa sổ thuộc tính tác vụ, hãy chọn mục **Settings**.



Thiết lập tác vụ Cập nhật cơ sở dữ liệu và mô-đun ứng dụng

5. Trong mục **Thiết lập cập nhật với chế độ nội bộ**, hãy chọn hộp kiểm **Tải xuống các bản cập nhật của mô-đun ứng dụng**.

   Nếu bạn muốn ngăn việc tải xuống các bản cập nhật mô-đun ứng dụng thì hãy xóa hộp kiểm **Tải xuống các bản cập nhật của mô-đun ứng dụng** và cấm người dùng sử dụng các tác vụ cục bộ.

6. 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.

7. Nếu cần, hãy cấu hình cập nhật mô-đun ứng dụng cho 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*).

8. Lưu các thay đổi của bạn.

Cách cấu hình cập nhật mô-đun 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 **Tasks**.

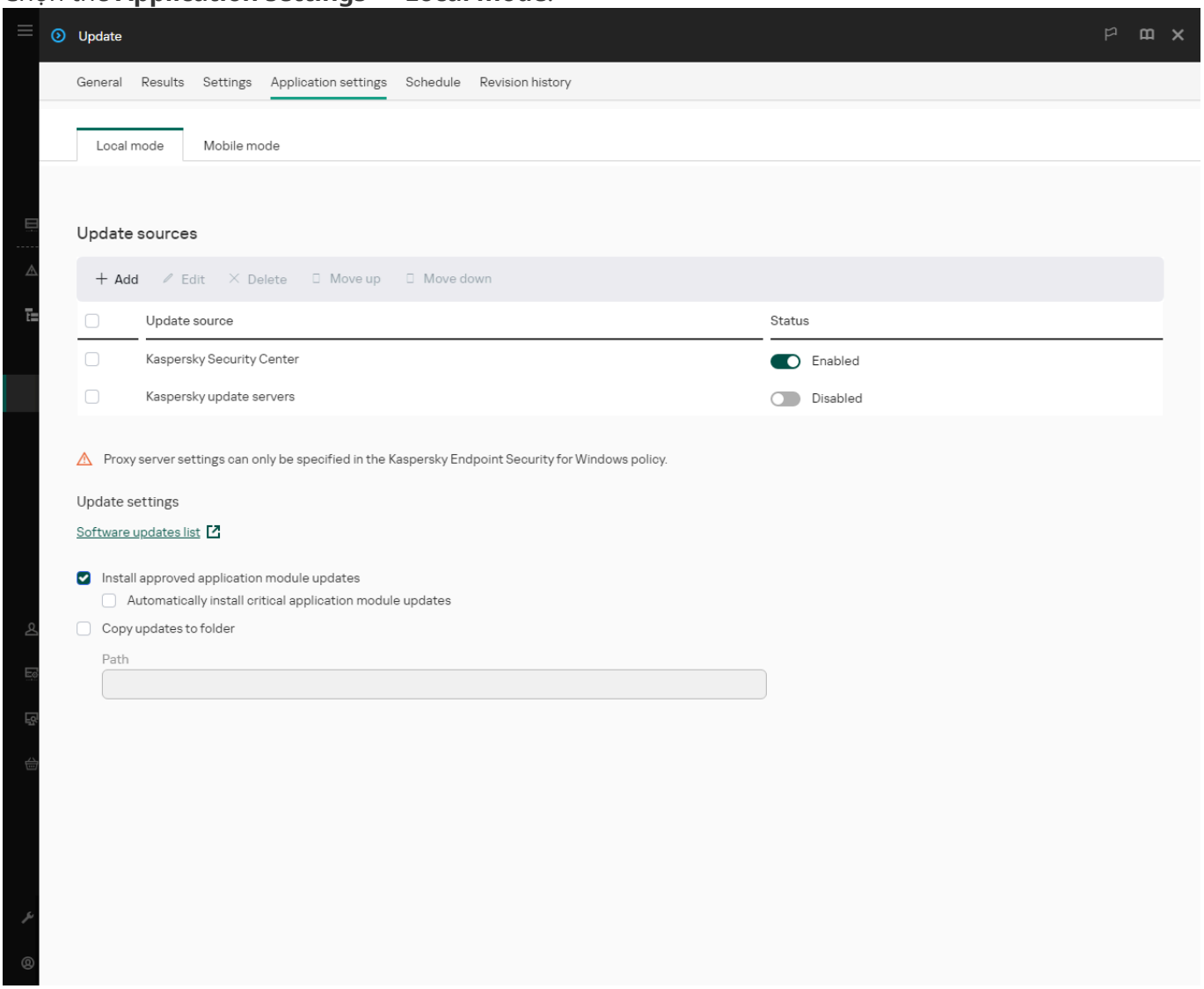
   Danh sách tác vụ sẽ mở.

2. Nhấn vào tác vụ **Cập nhật cơ sở dữ liệu và mô-đun ứng dụng** của Kaspersky Endpoint Security.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

   Tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* được tạo tự động bởi trình hướng dẫn sử dụng nhanh Máy chủ quản trị. Để tạo tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*, hãy cài đặt Tiện ích quản lý của Kaspersky Endpoint Security cho Windows khi đang chạy Trình hướng dẫn.

3. Chọn thẻ **Application settings** → **Local mode**.



Thiết lập tác vụ Update

4. Trong mục **Update settings**, hãy chọn các bản cập nhật mô-đun ứng dụng mà bạn muốn cài đặt:

   - **Install approved application module updates**. 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.

   - **Automatically install critical application module updates**. 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.

   Nếu bạn muốn ngăn việc tải xuống các bản cập nhật mô-đun ứng dụng, hãy xóa hộp kiểm **Install approved application module updates** và **Automatically install critical application module updates** và cấm người dùng sử dụng các tác vụ cục bộ.

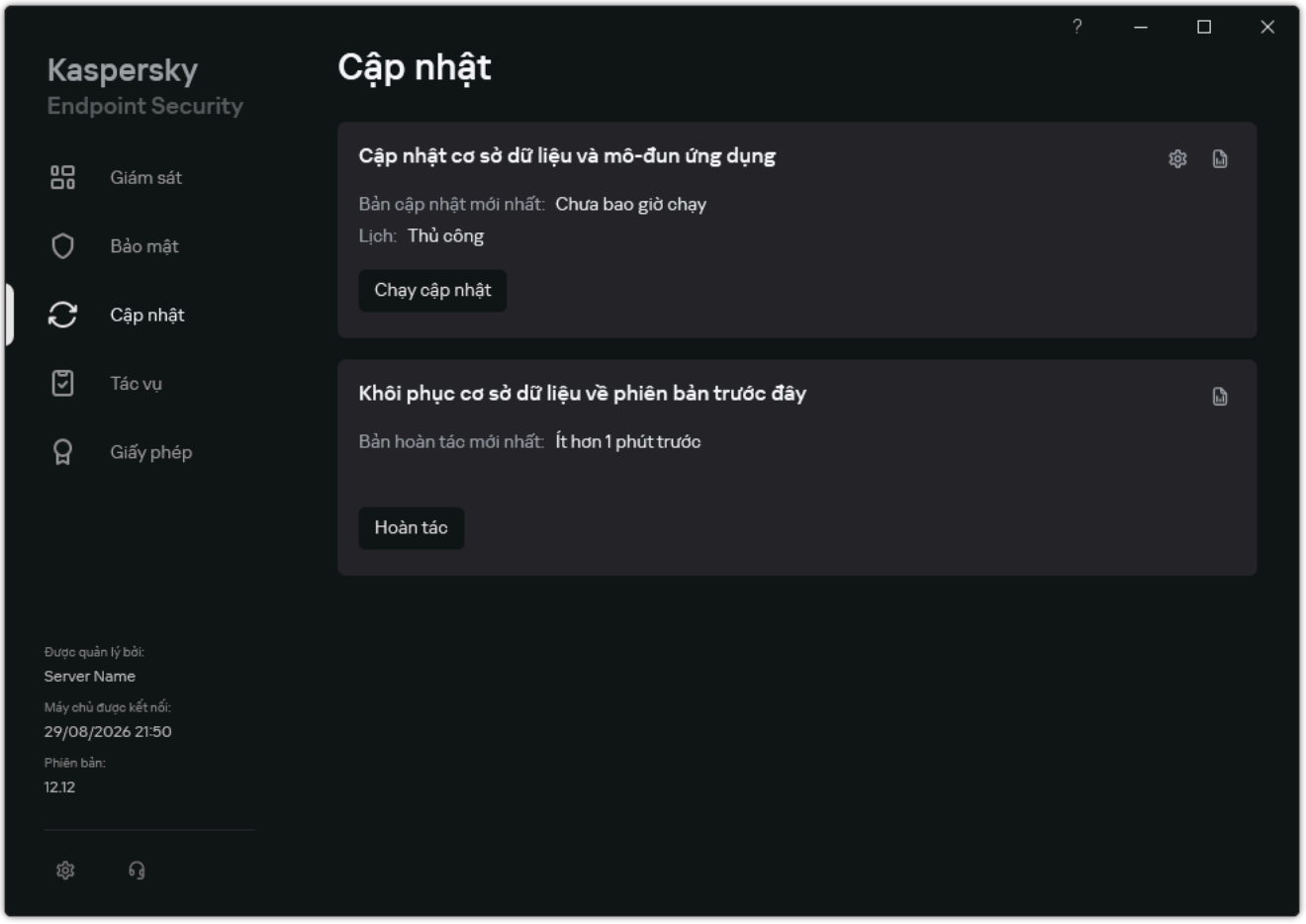
5. Nếu cần, hãy cấu hình cập nhật mô-đun ứng dụng cho chế độ di động. *Chế độ di động* là chế độ hoạt động của Kaspersky Endpoint Security khi một máy tính rời khỏi mạng của tổ chức (*máy tính ngoại tuyến*).

6. Lưu các thay đổi của bạn.

Cách cấu hình cập nhật mô-đun ứng dụng trong giao diện ứng dụng

Bạn không thể cấu hình tác vụ nhóm *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* trong giao diện ứng dụng. Chỉ một tác vụ cập nhật cục bộ là *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* khả dụng với người dùng. Nếu tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* không được hiển thị, điều đó có nghĩa là quản trị viên đã cấm sử dụng các tác vụ cục bộ trong chính sách.

1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Cập nhật**.



Tác vụ cập nhật cục bộ

2. Thao tác này sẽ mở ra danh sách tác vụ; hãy chọn tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* và nhấn vào ⚙.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

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 **Asset management** → **Policies**.

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** → **Network Settings**.

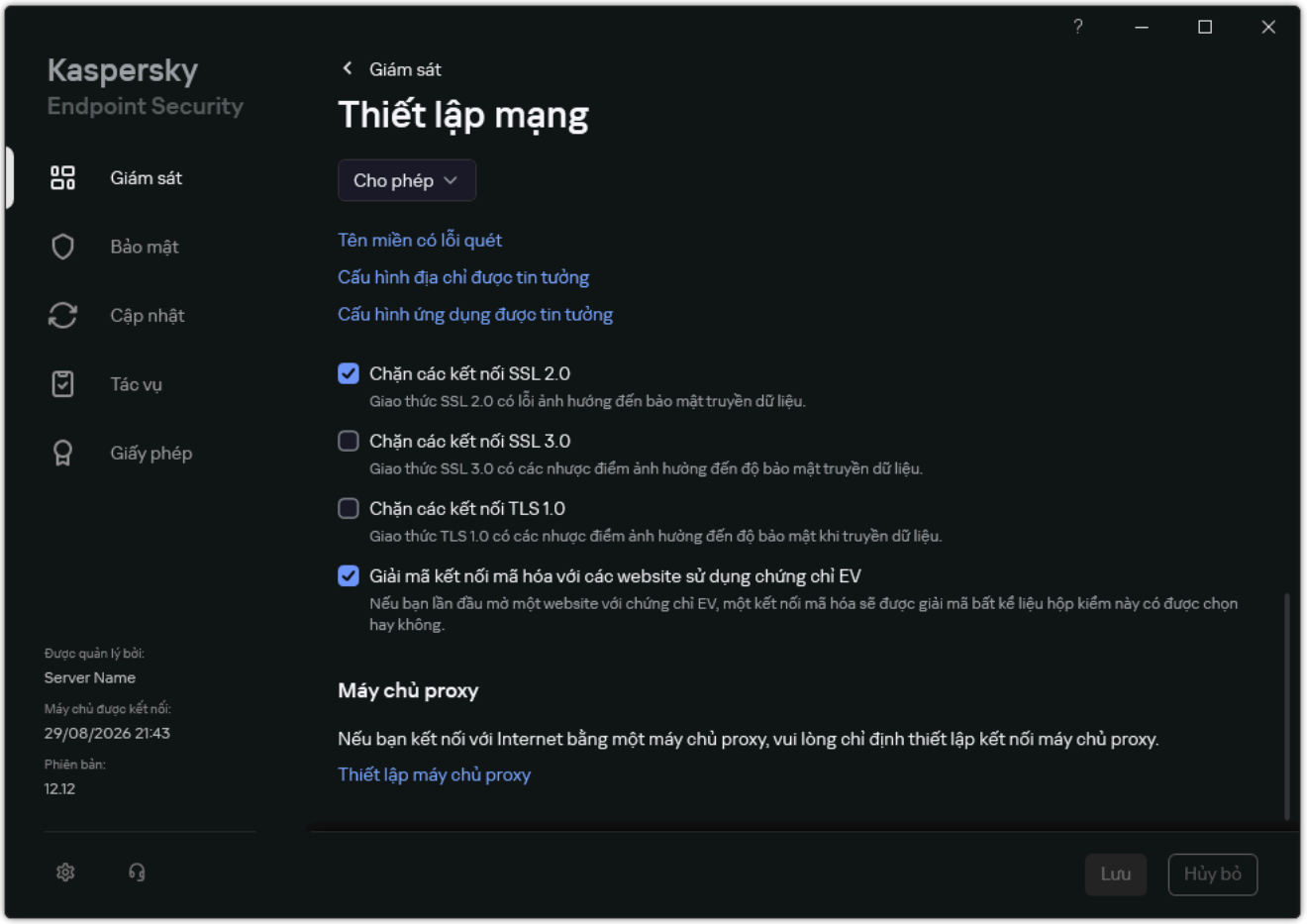
5. Trong mục **Proxy server**, hãy nhấn nút **Settings**.

6. Trong cửa sổ mở ra, hãy chọn hộp kiểm **Bypass a proxy server for local addresses**.

7. Lưu các thay đổi của bạn.

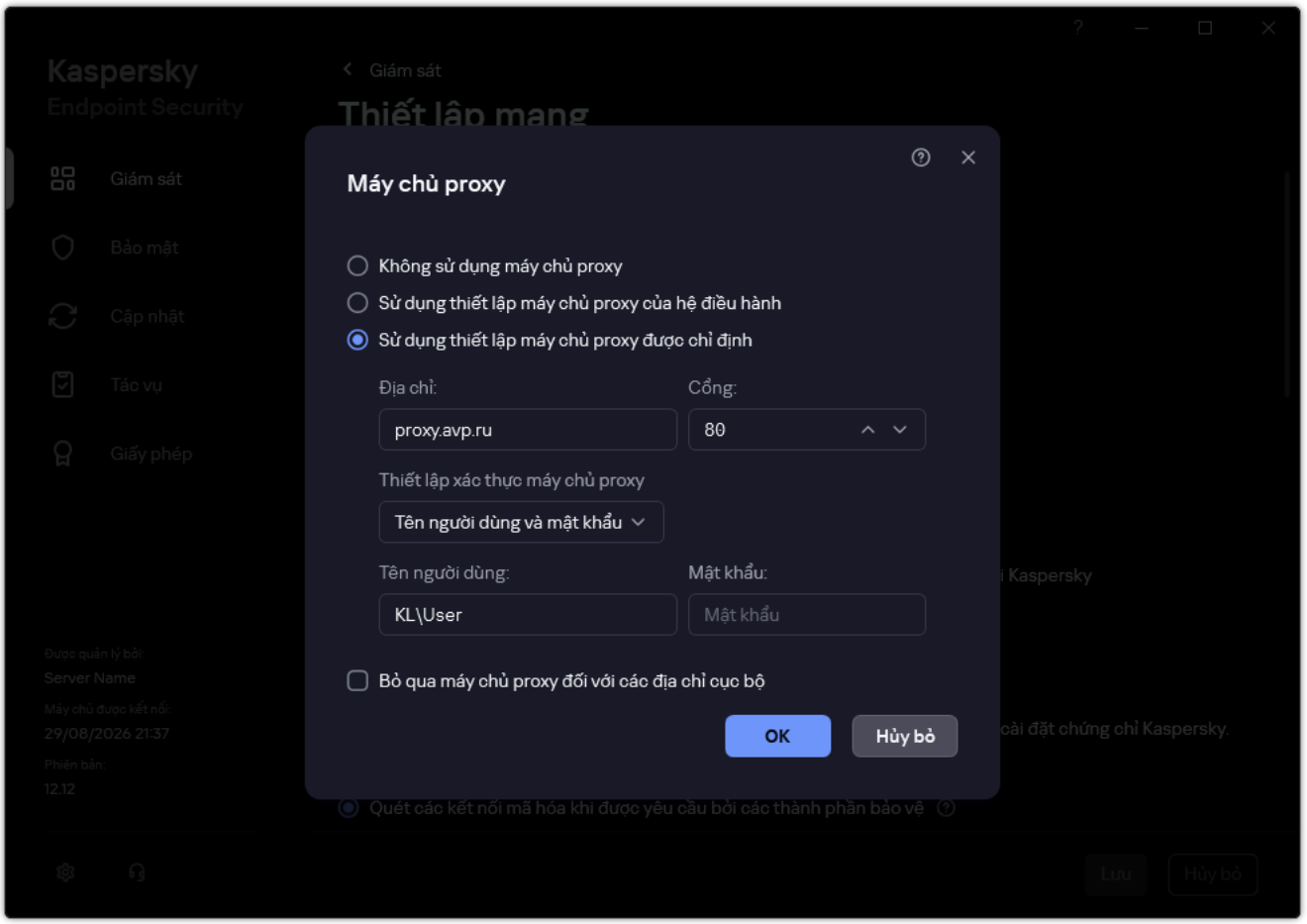
Để cấu hình thiết lập máy chủ proxy trong giao diện ứng dụng:

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**.



Thiết lập mạng của ứng dụng

3. Trong mục **Máy chủ proxy**, hãy nhấn liên kết **Thiết lập máy chủ proxy**.



Thiết lập kết nối 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:

   - **Sử dụng thiết lập máy chủ proxy của hệ điều hành**.

     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. Chọn cách bạn muốn ứng dụng xác thực trên máy chủ proxy. Theo mặc định, ứng dụng sử dụng xác thực NTLM tên miền của người dùng hiện tại.

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 thứ hai, 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. Khôi phục bản cập nhật gần nhất rất hữu ích, ví dụ, khi phiên bản cơ sở dữ liệu mới gây ra cảnh báo sai, dẫn đến việc Kaspersky Endpoint Security chặn một ứng dụng an toàn.

Kaspersky Endpoint Security ở chế độ Light Agent không hỗ trợ tác vụ *Hoàn tác bản cập nhật*.

Cách hoàn tác bản cập nhật gần đây nhất trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Tasks**.
   Danh sách tác vụ sẽ mở.
2. Nhấn vào **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

1. Chọn **Kaspersky Endpoint Security cho Windows (14.2)** → **Hoàn tác bản cập nhật**.

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 tác vụ, ví dụ như theo cách thủ công.

Bước 4. Xác định tên tác vụ

Nhập tên cho tác vụ.

Bước 7. Hoàn tất việc tạo tác vụ

Hoàn tất 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 hoàn tác bản cập nhật gần đây nhất trong Bảng điều khiển web

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

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **Add**.

   Trình hướng dẫn Tác vụ sẽ được bắt đầu.

3. Cấu hình các thiết lập của tác vụ:

   a. Trong danh sách thả xuống **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.

   b. Trong danh sách thả xuống **Task type**, hãy chọn **Rollback**.

   c. Trong trường **Task name**, nhập một mô tả ngắn gọn, ví dụ như *Hoàn tác bản cập nhật*.

   d. Trong phần **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. Chọn một tài khoản để chạy tác vụ. Theo mặc định, Kaspersky Endpoint Security khởi chạy tác vụ với quyền của tài khoản người dùng cục bộ.

6. Hoàn tất trình hướng dẫn.

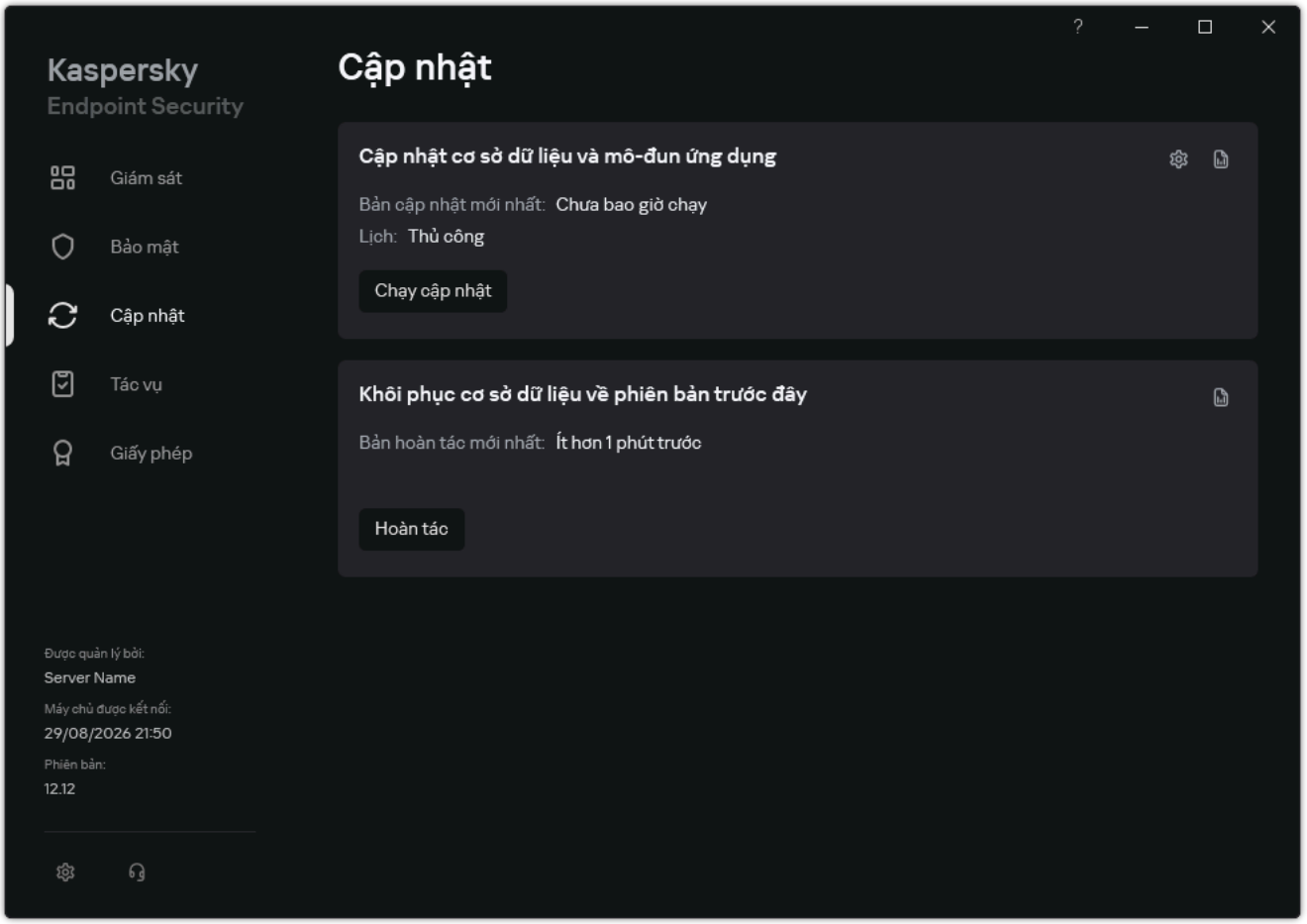
7. Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ.

8. Chọn hộp kiểm cạnh tác vụ.

9. Nhấn vào **Start**.

Cách hoàn tác bản cập nhật gần đây nhất trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy vào mục **Cập nhật**.



Tác vụ cập nhật cục bộ

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 nút **Ngừng cập nhật**.

Công nghệ khử mã độc nâng cao

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 phần mềm độc hại* và trong thiết lập ứng dụng.

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. Đối với các máy tính thuộc chính sách, 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. Đối với các máy tính không thuộc chính sách, tính năng Khử mã độc nâng cao sẽ được bật theo mặc định.

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 phần mềm độc hại*. 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Thiết lập ứng dụng**.
4. Trong mục **Tổng quát**, hãy chọn hộp kiểm **Bật Công nghệ khử mã độc nâng cao** để bật hoặc tắt Công nghệ khử mã độc nâng cao.
5. Lưu các thay đổi của bạn.

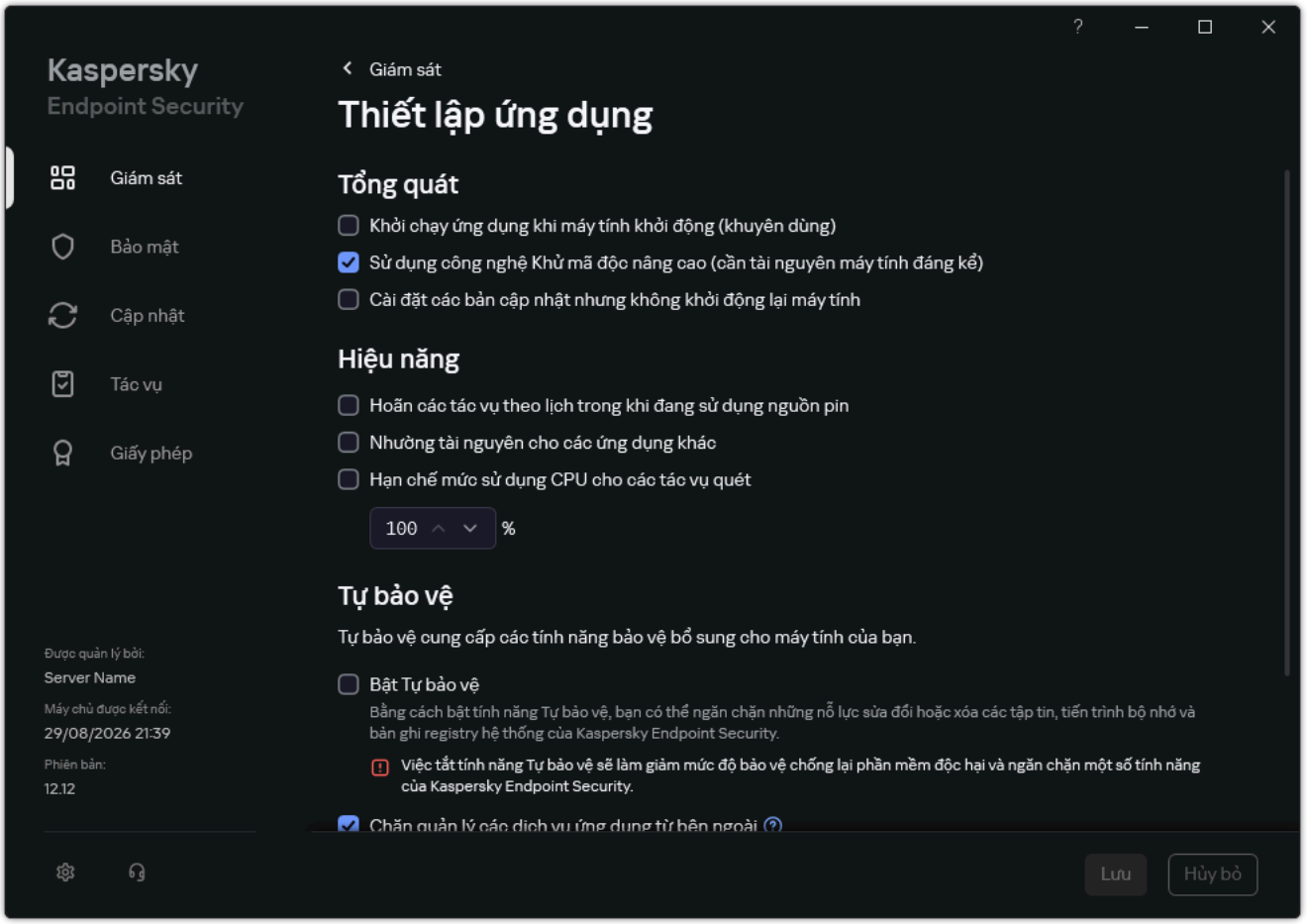
Cách bật hoặc tắt Công nghệ khử mã độc nâng cao trong Bảngg điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **General Settings** → **Detection Settings**.
5. Trong mục **Advanced Disinfection Technology**, hãy bật hoặc tắt công tắc **Advanced Disinfection Technology ENABLED** 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**.



Thiết lập Kaspersky Endpoint Security cho Windows

3. Trong mục **Tổng quát**, 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.

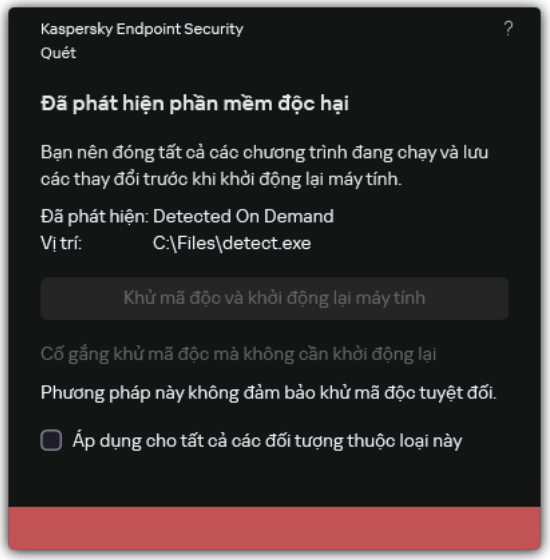
4. Lưu các thay đổi của bạn.

Kết quả là người dùng không thể sử dụng hầu hết các tính năng của hệ điều hành khi Khử mã độc nâng cao đang chạy. Khi quá trình khử mã độc hoàn tất, máy tính sẽ được khởi động lại.

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 phần mềm độc hại*. 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

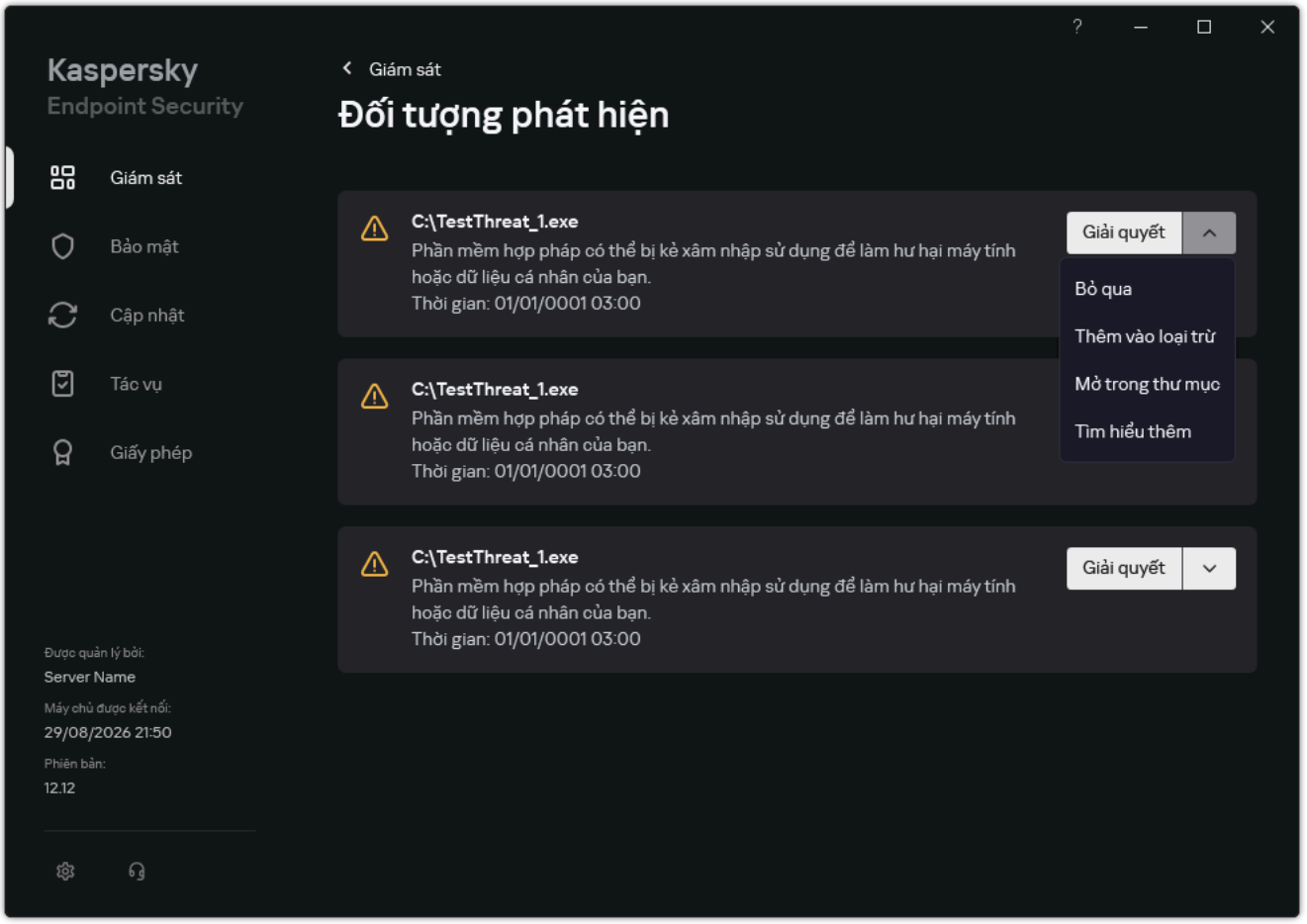
Để xử lý các mối đe dọa đang hoạt động trên máy chủ, bạn cần thao tác như sau:

- 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 phần mềm độc hại*.

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, bạn 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 phần mềm độc hại*. Sau đó bạn cần khởi chạy tác vụ *Quét phần mềm độc hại*.

Loại bỏ các mối đe dọa chưa được xử lý

Kaspersky Endpoint Security sẽ ghi lại thông tin về các tập tin mà nó chưa xử lý vì một lý do nào đó. Thông tin này được ghi lại dưới dạng các sự kiện trong danh sách các mối đe dọa đang hoạt động (xem hình bên dưới).



Danh sách 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 phần mềm độc hại*, 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 *Critical* – .

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 **Administration Server** → **Advanced** → **Repositories** → **Active threats**.

   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:

   - **Disinfect**. Nếu chọn tùy chọn này, ứng dụng sẽ tự động cố gắng khử mã độc tập tin bị nhiễm được phát hiện. Nếu không thể khử mã độc, ứng dụng sẽ xóa tập tin đó.

   - **Delete**. Nếu chọn tùy chọn này, ứng dụng sẽ xóa các tập tin bị nhiễm mã độc được phát hiện từ kho lưu trữ mối đe dọa đang hoạt động. Trong trường hợp này, ứng dụng sẽ lưu giữ tập tin được phát hiện trong bộ nhớ của máy tính. Để loại bỏ mối đe dọa đó khỏi máy tính, hãy chọn **Disinfect**.

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 **Operations** → **Repositories** → **Active threats**.

   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:

   - **Disinfect**. Nếu chọn tùy chọn này, ứng dụng sẽ tự động cố gắng khử mã độc tập tin bị nhiễm được phát hiện. Nếu không thể khử mã độc, ứng dụng sẽ xóa tập tin đó.

   - **Delete**. Nếu chọn tùy chọn này, ứng dụng sẽ xóa các tập tin bị nhiễm mã độc được phát hiện từ kho lưu trữ mối đe dọa đang hoạt động. Trong trường hợp này, ứng dụng sẽ lưu giữ tập tin được phát hiện trong bộ nhớ của máy tính. Để loại bỏ mối đe dọa đó khỏi máy tính, hãy chọn **Disinfect**.

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 chọn tùy chọn này, ứng dụng sẽ tự động cố gắng khử mã độc tập tin bị nhiễm được phát hiện. Nếu không thể khử mã độc, ứng dụng sẽ xóa 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 trang web Cơ sở dữ liệu của Kaspers ky về lỗ hổng bảo mật và mối đe dọa.

Để xử lý các mối đe dọa đang hoạt động trong bảng điều khiển Kaspersky Security Center, bạn phải bật tính năng truyền thông tin về các tập tin chưa được xử lý tới Máy chủ quản trị. Truyền dữ liệu được bật theo mặc định.

Cách bật truyền dữ liệu tập tin chưa được xử lý trong Bảng điều khiển quản trị (MMC)

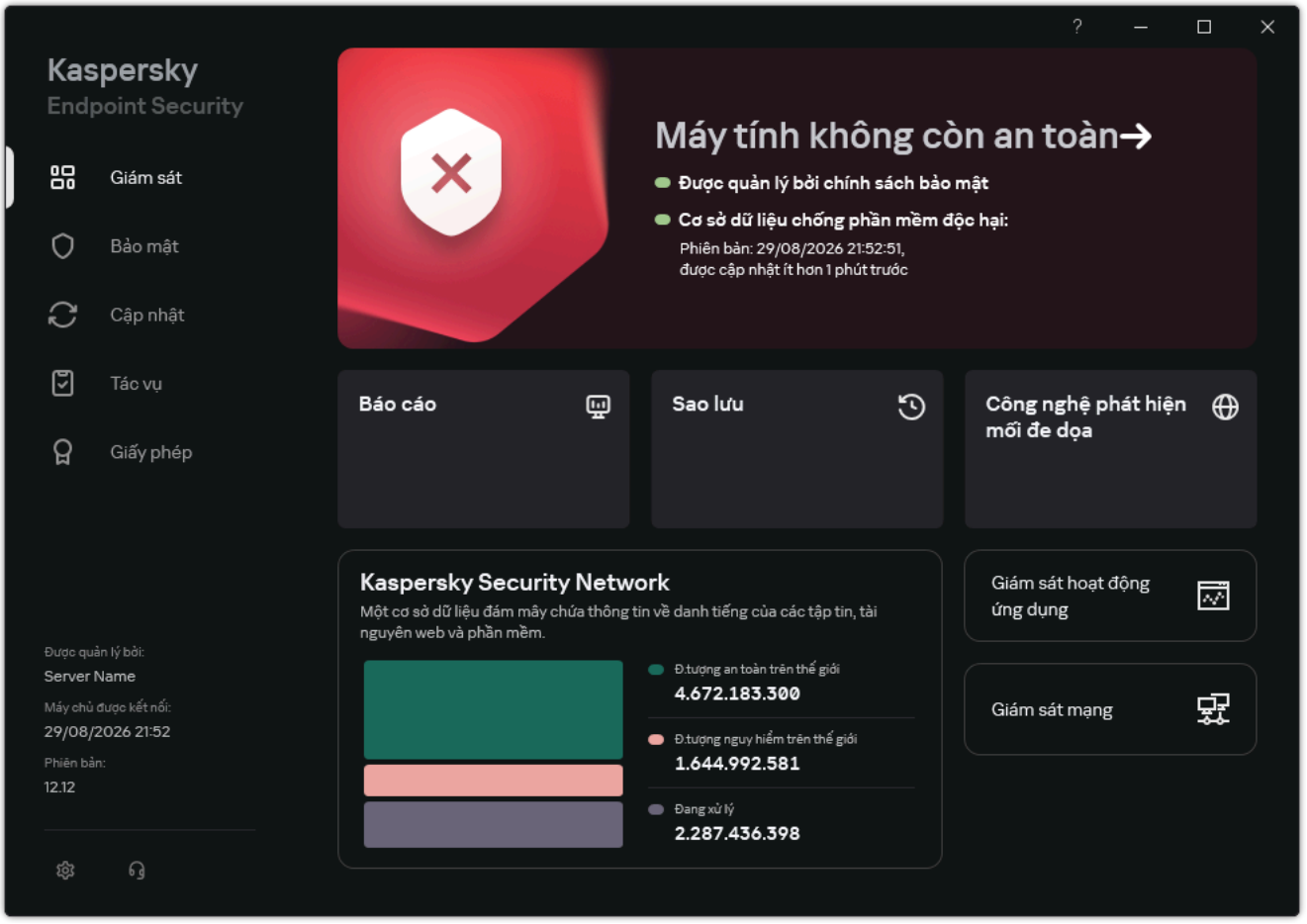
1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Các báo cáo và lưu trữ**.
4. Trong mục **Truyền dữ liệu đến Máy chủ quản trị**, hãy nhấn nút **Thiết lập**.
5. Chọn hộp kiểm **Các tập tin không được xử lý**.
6. Lưu các thay đổi của bạn.

Cách bật truyền dữ liệu tập tin chưa được xử lý trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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** → **KSC Integration**.

5. Trong mục **Data transfer to Administration Server**, hãy chọn hộp kiểm **About unprocessed files**.

6. Lưu các thay đổi của bạn.



Cửa sổ chính của ứng dụng khi phát hiện ra mối đe dọa

Bảo vệ máy tính

Trạng thái bảo vệ theo thời gian thực

Kaspersky Endpoint Security sẽ gửi thiết lập **Real-time protection status** cho Máy chủ quản trị Kaspersky Security Center; giá trị của thiết lập này phụ thuộc vào trạng thái hiện tại của các thành phần bảo vệ ứng dụng trên máy tính được bảo vệ (xem bảng bên dưới).

Kaspersky Endpoint Security xác định trạng thái bảo vệ theo thời gian thực dựa trên trạng thái của các thành phần ứng dụng sau:

- 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 tấn công BadUSB.
- Bảo vệ mối đe dọa mạng.
- Tường lửa.
- Phòng chống khai thác.
- Phát hiện hành vi.
- Công cụ khắc phục.
- Phòng chống xâm nhập máy chủ.

Bạn có thể kiểm tra trạng thái bảo vệ theo thời gian thực của ứng dụng trong bảng điều khiển Kaspersky Security Center.

Cách tìm trạng thái Bảo vệ theo thời gian thực trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Managed devices**.

Trạng thái Bảo vệ Thời gian thực hiện tại được hiển thị trong danh sách thiết bị, trong cột **Real-time protection status**. Nếu cột **Real-time protection status** bị thiếu, hãy quản lý thiết lập cột bằng cách nhấn vào liên kết **Add/Remove Columns**.

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Managed devices**.

Trạng thái Bảo vệ Thời gian thực hiện tại được hiển thị trong danh sách thiết bị, trong cột **Real-time protection status**. Nếu cột **Real-time protection status** bị thiếu, hãy quản lý thiết lập cột bằng cách nhấn vào liên kết **Add/Remove Columns**.

Cách tìm Bảo vệ máy tính theo thời gian thực trong Bảng điều khiển web

Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Assets (Devices)**.

Trạng thái Bảo vệ Thời gian thực hiện tại được hiển thị trong danh sách thiết bị, trong cột **Real-time protection status**. Nếu cột **Real-time protection status** bị thiếu, hãy quản lý thiết lập cột ( ).

Các giá trị khả dĩ của thiết lập Real-time protection status

Giá trị	Mô tả
Unknown	Máy chủ quản trị không có thông tin về trạng thái bảo vệ theo thời gian thực của máy tính này.
Not installed	Chưa có thành phần nào được cài đặt.
Not supported by license	Ứng dụng chưa được kích hoạt hoặc giấy phép không cho phép các thành phần đã cài đặt hoạt động.
Failed	Một hoặc nhiều bộ phận đã bị lỗi.
Stopped	Một hoặc nhiều thành phần bị tắt.
Paused	Một hoặc nhiều thành phần bị tạm dừng.
Starting	Một hoặc nhiều thành phần đang được bật lên.
Running	Các thành phần của ứng dụng đã được khởi chạy và hoạt động.

Nếu giá trị của thiết lập **Real-time protection status** trong Kaspersky Security Center khác với *Running* thì hãy kiểm tra để đảm bảo rằng các thành phần đã cài đặt của Kaspersky Endpoint Security trong danh sách đã được kích hoạt và ứng dụng đã được kích hoạt.

Bảo vệ mối đe dọa tập tin

Thành phần Bảo vệ mối đe dọa tập tin cho phép bạn ngăn chặn sự lây nhiễm vào hệ thống tập tin máy tính. Theo mặc định, thành phần Bảo vệ mối đe dọa tập tin sẽ nằm vĩnh viễn trong RAM của máy tính và quét tất cả các tập tin đã mở, đã lưu và đã chạy theo thời gian thực. Thành phần này sẽ quét các tập tin trên tất cả các ổ đĩa máy tính, bao gồm cả 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 ở trong 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 được gọi là *mức độ bảo mật*: **Cao**, **Khuyên dùng**, **Thấp**. Thiết lập mức độ bảo mật **Khuyên 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.

Thành phần Bảo vệ mối đe dọa tập tin sử dụng dữ liệu nhận được từ các thành phần ứng dụng khác. Không bắt buộc phải bật các thành phần đó. Các thành phần cung cấp dữ liệu bổ sung gồm có:

- Kaspersky Security Network.
- Phòng chống xâm nhập máy chủ.
- Phát hiện hành vi.

Cách bật hoặc tắt thành phần Bảo vệ mối đe dọa tập tin trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Bảo vệ mối đe dọa tập tin**.
4. Sử dụng hộp kiểm **Bảo vệ mối đe dọa tập tin** để bật hoặc tắt thành phần.
5. 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.
     - **Khuyên dùng**. Mức độ bảo mật tập tin này được khuyến nghị bởi các chuyên gia của Kaspersky Lab. Thành phần Bảo vệ mối 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 mối 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 mối 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 mối 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** và định nghĩa thiết lập thành phần của riêng bạn (xem bảng bên dưới).

  Bạn có thể khôi phục các giá trị của các mức bảo mật cài đặt sẵn bằng cách nhấn vào nút **Theo mặc định**.

6. Trong mục **Hành động khi phát hiện mối đe dọa**, chọn hành động được Kaspersky Endpoint Security thực hiện đối với các đối tượng độc hại:

   - **Khử mã độc, xóa nếu không thể khử mã độc**. Nếu chọn tùy chọn này, ứng dụng sẽ tự động cố gắng khử mã độc tập tin bị nhiễm được phát hiện. Nếu không thể khử mã độc, ứng dụng sẽ xóa tập tin đó.

   - **Khử mã độc, chặn nếu không thể khử mã độc**. Nếu chọn tùy chọn này, ứng dụng sẽ tự động cố gắng khử mã độc tập tin bị nhiễm được phát hiện. Nếu việc khử mã độc không thành công, ứng dụng sẽ chặn tập tin này.

   - **Chặn**. Nếu tùy chọn này được chọn, ứng dụng sẽ tự động chặn tập tin bị nhiễm mà không cố gắng khử mã độc hoặc xóa tập tin.

   - **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.

   Trước khi cố gắng khử mã độc hoặc xóa một tập tin bị nhiễm, ứng dụng 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.

7. Lưu các thay đổi của bạn.

Cách bật hoặc tắt thành phần Bảo vệ mối đe dọa tập tin trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.

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 **Host Threat Protection** → **File Threat Protection**.

5. Sử dụng nút bật/tắt **File Threat Protection ENABLED** để bật hoặc tắt thành phần này.

6. Nếu bạn muốn bổ sung một đối tượng mới vào phạm vi bảo vệ:

   a. Trong mục **Advanced settings**, hãy chọn thẻ **Protection scope**.

   b. Nhấn vào **Add**.

   c. Thao tác này sẽ mở một cửa sổ; trong cửa sổ đó, hãy chọn đối tượng mà bạn muốn thêm vào phạm vi bảo vệ.

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 cấp 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 sử dụng mặt nạ ở bất kỳ đâu trong đường dẫn tập tin hoặc thư mục. Ví dụ: nếu bạn muốn phạm vi quét bao gồm thư mục Downloads cho tất cả tài khoản người dùng trên máy tính, hãy nhập tên đại diện `C:\Users\*\Downloads\`.

Bạn có thể loại trừ một đối tượng khỏi phạm vi quét mà không cần xóa nó khỏi danh sách các đối tượng trong phạm vi bảo vệ. Để thực hiện, hãy gạt công tắc bật/tắt bên cạnh sang vị trí tắt.

d. Lưu các thay đổi của bạn.

7. Trong mục **Action on threat detection**, chọn hành động được Kaspersky Endpoint Security thực hiện đối với các đối tượng độc hại:

   - **Disinfect, delete if disinfection fails**. Nếu chọn tùy chọn này, ứng dụng sẽ tự động cố gắng khử mã độc tập tin bị nhiễm được phát hiện. Nếu không thể khử mã độc, ứng dụng sẽ xóa tập tin đó.

   - **Disinfect, block if disinfection fails**. Nếu chọn tùy chọn này, ứng dụng sẽ tự động cố gắng khử mã độc tập tin bị nhiễm được phát hiện. Nếu việc khử mã độc không thành công, ứng dụng sẽ chặn tập tin này.

   - **Block**. Nếu tùy chọn này được chọn, ứng dụng sẽ tự động chặn tập tin bị nhiễm mà không cố gắng khử mã độc hoặc xóa tập tin.

   Trước khi cố gắng khử mã độc hoặc xóa một tập tin bị nhiễm, ứng dụng 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.

8. Nếu cần, hãy chỉnh sửa thiết lập nâng cao của Bảo vệ mối đe dọa tập tin.

9. Lưu các thay đổi của bạn.

Cách bật hoặc tắt thành phần Bảo vệ mối đe dọa tập tin 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 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.

     - **Khuyên dùng**. Mức độ bảo mật tập tin này được khuyến nghị bởi các chuyên gia của Kaspersky Lab. Thành phần Bảo vệ mối 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 mối 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 mối 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 mối 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 (xem bảng bên dưới).

     Bạn có thể khôi phục các giá trị của các mức bảo mật cài đặt sẵn bằng cách nhấn vào nút **Khôi phục cấp bảo mật được khuyến nghị**.

5. Trong mục **Hành động khi phát hiện mối đe dọa**, chọn hành động được Kaspersky Endpoint Security thực hiện đối với các đối tượng độc hại:

   - **Khử mã độc, xóa nếu không thể khử mã độc**. Nếu chọn tùy chọn này, ứng dụng sẽ tự động cố gắng khử mã độc tập tin bị nhiễm được phát hiện. Nếu không thể khử mã độc, ứng dụng sẽ xóa tập tin đó.

   - **Khử mã độc, chặn nếu không thể khử mã độc**. Nếu chọn tùy chọn này, ứng dụng sẽ tự động cố gắng khử mã độc tập tin bị nhiễm được phát hiện. Nếu việc khử mã độc không thành công, ứng dụng sẽ chặn tập tin này.

   - **Chặn**. Nếu tùy chọn này được chọn, ứng dụng sẽ tự động chặn tập tin bị nhiễm mà không cố gắng khử mã độc hoặc xóa tập tin.

   - **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.

   Trước khi cố gắng khử mã độc hoặc xóa một tập tin bị nhiễm, ứng dụng 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.

6. Lưu các thay đổi của bạn.

Thiết lập Bảo vệ mối 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, ứng dụng 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.
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 chỉnh sửa	**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.
Sử dụng 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 tác vụ 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 iSwift được cải tiến từ công nghệ iChecker cho hệ thống tập tin NTFS.
Sử dụng 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 tác vụ 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. Ứng dụng sẽ quét các tập tin định dạng văn phòng nhỏ hơn 1 MB, bất kể hộp kiểm này có được chọn hay không.
Quét các tập tin có định dạng email	**Bật**	Quét các tập tin định dạng email. Ứng dụng sẽ quét các tập tin MSG và EML. Các tập tin định dạng email cũng bao gồm các đối tượng OLE và tập tin MHT. Kaspersky Endpoint Security sẽ quét các tập tin định dạng email nhỏ hơn 1 MB, bất kể hộp kiểm này có được chọn hay không.
Chế độ quét	**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.
Hành động khi phát hiện mối đe dọa	**Khử mã độc, xóa nếu không thể khử mã độc**	Nếu chọn tùy chọn này, ứng dụng sẽ tự động cố gắng khử mã độc tập tin bị nhiễm được phát hiện. Nếu không thể khử mã độc, ứng dụng sẽ xóa tập tin đó.

Tự động tạm ngưng Bảo vệ mối đe dọa tập tin

Bạn có thể cấu hình Bảo vệ mối 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 mối 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 mối 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 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 **Tạm dừng Bảo vệ mối đe dọa tập tin**, hãy nhấn liên kết **Tạm dừng Bảo vệ mối đe dọa tập tin**.
5. Trong cửa sổ mở ra, hãy cấu hình thiết lập để tạm dừng Bảo vệ mối đe dọa tập tin:
   a. Cấu hình lịch tự động tạm dừng Bảo vệ mối đe dọa tập tin.
   b. Tạo một danh sách các ứng dụng có hoạt động khiến thành phần Bảo vệ mối 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 chọn tùy chọn này, ứng dụng sẽ tự động cố gắng khử mã độc tập tin bị nhiễm được phát hiện. Nếu không thể khử mã độc, ứng dụng sẽ xóa tập tin đó.
   - **Khử mã độc, chặn nếu không thể khử mã độc**. Nếu chọn tùy chọn này, ứng dụng sẽ tự động cố gắng khử mã độc tập tin bị nhiễm được phát hiện. Nếu việc khử mã độc không thành công, ứng dụng sẽ chặn tập tin này.
   - **Chặn**. Nếu tùy chọn này được chọn, ứng dụng sẽ tự động chặn tập tin bị nhiễm mà không cố gắng khử mã độc hoặc xóa tập tin.

Trước khi cố gắng khử mã độc hoặc xóa một tập tin bị nhiễm, ứng dụng 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 mối đe dọa thiết yếu → Bảo vệ mối 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 mối 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, ứng dụng 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, ứng dụng 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. 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 các thư mục con bên trong `Folder`, ngoại trừ chính `Folder`. Một đại diện phải có ít nhất một cấp 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 sử dụng mặt nạ ở bất kỳ đâu trong đường dẫn tập tin hoặc thư mục. Ví dụ: nếu bạn muốn phạm vi quét bao gồm thư mục Downloads cho tất cả tài khoản người dùng trên máy tính, hãy nhập tên đại diện `C:\Users\*\Downloads\`.

      Đối tượng **Máy tính này** trong danh sách tài nguyên tập tin của máy tính bao gồm các đối tượng sau: **Tất cả các ổ đĩa cứng**, **Tất cả ổ đĩa mạng** và **Tất cả các ổ đĩa di động**.

   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:
   - **Sử dụng 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 tác vụ 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 iSwift được cải tiến từ công nghệ iChecker cho hệ thống tập tin NTFS.
   - **Sử dụng 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 tác vụ 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 mối 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 mối đe dọa thiết yếu → Bảo vệ mối đe dọa tập tin**.
3. Nhấn vào **Thiết lập nâng cao**.
4. Trong mục **Tối ưu hóa**, hãy chọn hộp kiểm **Chỉ quét các tập tin mới và bị chỉnh sửa**.
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 mối 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 hỗn hợp**, quy định loại tập tin hỗn hợp mà bạn muốn quét: tập tin nén, gói phân phối, tập tin định dạng thư hoặc 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 hỗn 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 hỗn 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.

Quét container

Container là môi trường biệt lập, trong đó ứng dụng có thể chạy mà không cần tương tác trực tiếp với hệ điều hành. Sử dụng container có thể liên quan đến những rủi ro sau:

- Tin tặc có thể khai thác lỗ hổng của container để xâm nhập vào các ứng dụng bên trong container.
- Tin tặc có thể khai thác cấu hình không bảo mật của môi trường container để truy cập trái phép vào dữ liệu trên máy tính hoặc làm tổn hại đến tính toàn vẹn của hệ thống.
- Một cuộc tấn công thành công vào container có thể cho phép tin tặc truy cập vào dữ liệu trên máy tính.
- Tin tặc có thể khai thác lỗ hổng mạng để chặn lưu lượng mạng.

Kaspersky Endpoint Security không chỉ quét các tập tin trên đĩa mà cả bên trong các container. Tức là, Kaspersky Endpoint Security là một công cụ bên ngoài dùng để phát hiện hoạt động độc hại bên trong các container. Điều này cho phép duy trì hiệu năng của container và ngăn ngừa xung đột với các ứng dụng khác bên trong container. Không hỗ trợ cài đặt Kaspersky Endpoint Security bên trong container.

Ngoài việc bảo mật cho container, Kaspersky Endpoint Security còn cho phép quản lý các ứng dụng bên trong container bằng cách sử dụng Kiểm soát ứng dụng. Kiểm soát ứng dụng được cấu hình cho các container theo cùng cách với các ứng dụng được cài đặt trên máy tính. Giám sát tính toàn vẹn của hệ thống cũng hỗ trợ container.

Yêu cầu về container

- Container phải là container Docker. Các công cụ tạo container khác không được hỗ trợ.
- Container phải chạy ở chế độ cô lập tiến trình. Chế độ cô lập Hyper-V không được hỗ trợ.

- Container phải được đặt trên máy chủ Windows Server 2016, 2019 hoặc 2022 (Docker Host).
- Container phải bao gồm một ảnh Windows (Docker Image). Windows 10 và 11 không được hỗ trợ. Không hỗ trợ ảnh Linux.

Hành động khi phát hiện mối đe dọa

Nếu phát hiện mối đe dọa bên trong container, ứng dụng sẽ áp dụng hành động được chọn cho thành phần Bảo vệ mối đe dọa tập tin. Quét container có thêm các cài đặt bổ sung (xem hướng dẫn bên dưới). Nếu phát hiện mối đe dọa, ứng dụng sẽ chặn hoạt động độc hại và thực hiện hành động đã chọn (ví dụ: cố gắng khử mã độc đối tượng). Kaspersky Endpoint Security có thể dừng container nếu đối tượng được phát hiện không thể khử mã độc. Theo mặc định, chức năng dừng container bị vô hiệu hóa.

Cách cấu hình quét container trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa tập tin**.
4. Nhấn vào **Thiết lập**.
5. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy chọn thẻ **Bổ sung**.
6. Trong mục **Quét các thao tác với tập tin được thực thi trong các container Windows**, hãy cấu hình thiết lập quét container:
   - **Dừng container nếu khử mã độc không thành công**. Ứng dụng có thể không có đủ quyền đọc và ghi cho đối tượng được phát hiện. Trong trường hợp đó, khử mã độc hoặc xóa đối tượng được phát hiện là việc không thể. Nếu chọ hộp kiểm này, ứng dụng sẽ chặn đối tượng được phát hiện và dừng container. Nếu bỏ chọn hộp kiểm này, ứng dụng chỉ chặn đối tượng được phát hiện.
   - **Không quét các thao tác tập tin được thực thi trong container Windows**. Nếu chọn hộp kiểm, ứng dụng sẽ chỉ quét container khi container đó được khởi động. Nếu bỏ chọn hộp kiểm, ứng dụng sẽ quét container liên tục theo thời gian thực.
7. Lưu các thay đổi của bạn.

Cách cấu hình quét container trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Host Threat Protection** → **File Threat Protection**.
5. Trong mục **Advanced settings**, hãy chọn thẻ **Performance**.

6. Trong mục **Scan optimization**, hãy cấu hình thiết lập quét container:

   - **Stop container if disinfection fails**. Ứng dụng có thể không có đủ quyền đọc và ghi cho đối tượng được phát hiện. Trong trường hợp đó, khử mã độc hoặc xóa đối tượng được phát hiện là việc không thể. Nếu chọ hộp kiểm này, ứng dụng sẽ chặn đối tượng được phát hiện và dừng container. Nếu bỏ chọn hộp kiểm này, ứng dụng chỉ chặn đối tượng được phát hiện.

   - **Do not scan file operations executed in Windows containers**. Nếu chọn hộp kiểm, ứng dụng sẽ chỉ quét container khi container đó được khởi động. Nếu bỏ chọn hộp kiểm, ứng dụng sẽ quét container liên tục theo thời gian thực.

7. Lưu các thay đổi của bạn.

Cách cấu hình quét container 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 tập tin**.

3. Trong mục **Thao tác quét tập tin được thực thi trong container Windows**, hãy cấu hình thiết lập quét container:

   - **Dừng container nếu khử mã độc không thành công**. Ứng dụng có thể không có đủ quyền đọc và ghi cho đối tượng được phát hiện. Trong trường hợp đó, khử mã độc hoặc xóa đối tượng được phát hiện là việc không thể. Nếu chọ hộp kiểm này, ứng dụng sẽ chặn đối tượng được phát hiện và dừng container. Nếu bỏ chọn hộp kiểm này, ứng dụng chỉ chặn đối tượng được phát hiện.

   - **Không quét các thao tác tập tin được thực thi trong container Windows**. Nếu chọn hộp kiểm, ứng dụng sẽ chỉ quét container khi container đó được khởi động. Nếu bỏ chọn hộp kiểm, ứng dụng sẽ quét container liên tục theo thời gian thực.

4. 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 dữ liệu cá nhân (ví dụ: các tập tin và ứng dụng)

Hoạt động mạng của các ứng dụng được kiểm soát bởi thành phần 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 sử dụng 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. Đặt 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.

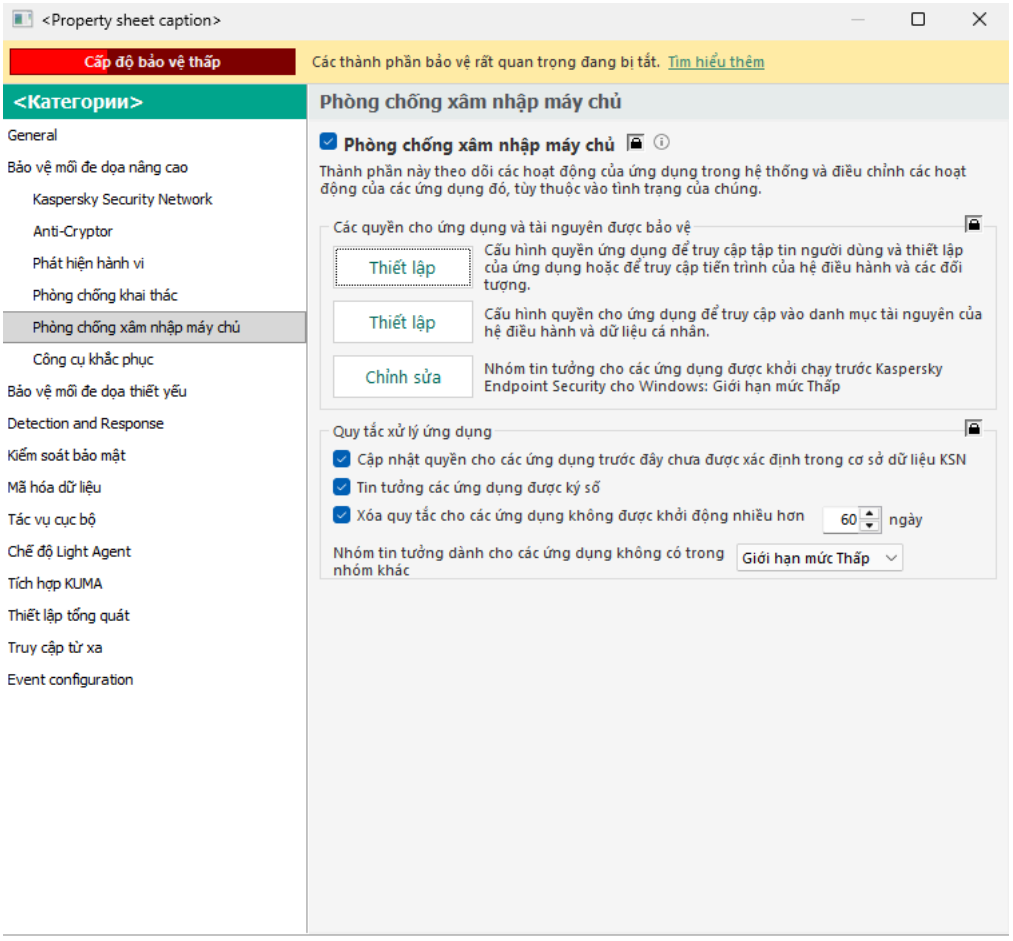
Khi ứng dụng được khởi chạy vào lần tới, Kaspersky Endpoint Security sẽ kiểm tra tính toàn vẹn của ứng dụng. Nếu ứng dụng không thay đổi, thành phần sẽ áp dụng các quyền của ứng dụng hiện tại cho nó. Nếu ứng dụng đã bị sửa đổi, Kaspersky Endpoint Security sẽ phân tích ứng dụng đó như khi ứng dụng đó 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao → Phòng chống xâm nhập máy chủ**.



Thiết lập Phòng chống xâm nhập

4. Sử dụng hộp kiểm **Phòng chống xâm nhập máy chủ** để bật hoặc tắt thành phần.
5. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và 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 **Asset management → Policies**.
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 **Host Threat Protection → Host Intrusion Prevention**.
5. Sử dụng nút bật/tắt **Host Intrusion Prevention ENABLED** để bật hoặc tắt thành phần này.
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 mối 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 này.
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 để tự động đặt mọi ứng dụng chưa xác định vào. Các ứng dụng đã chạy trước khi Kaspersky Endpoint Security được khởi động sẽ tự động được đưa vào nhóm tin tưởng được đặt trong thiết lập 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.

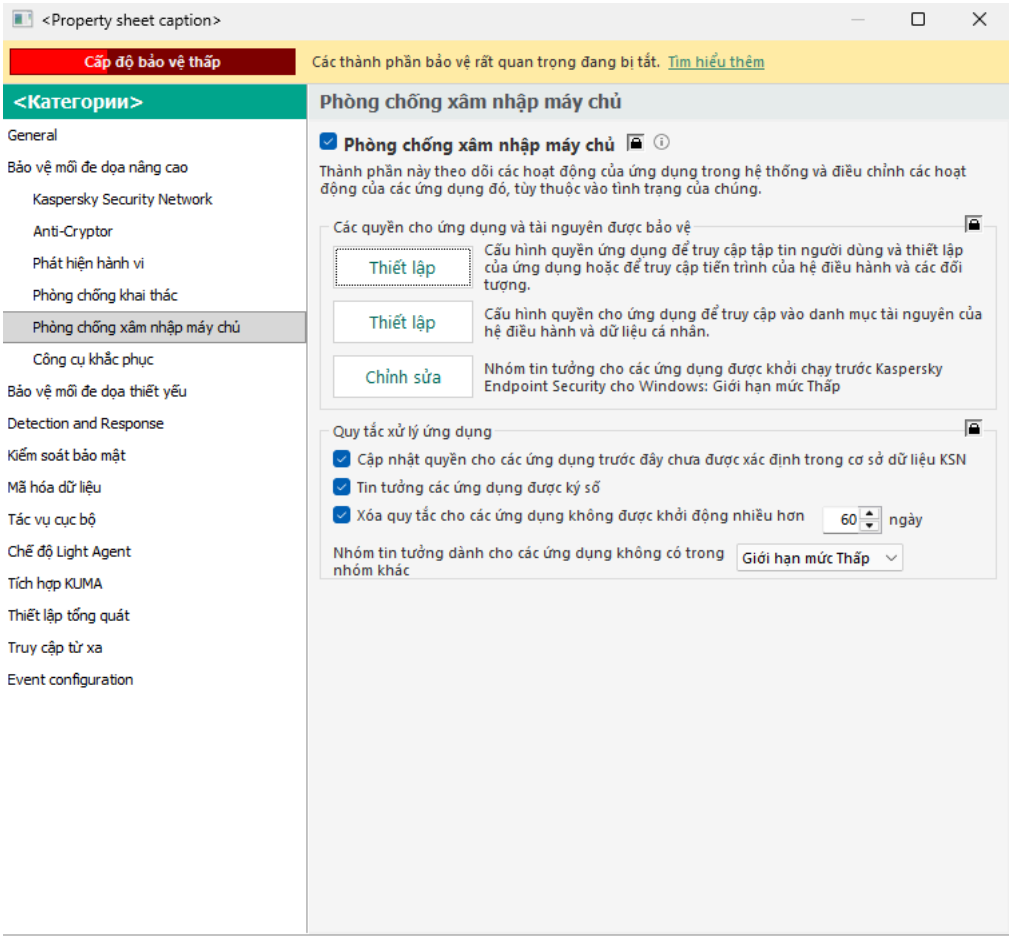
Các chuyên gia Kaspersky không khuyến khích di chuyển ứng dụng từ một nhóm tin tưởng được gán tự động sang một nhóm tin tưởng khác. Thay vào đó, bạn có thể sửa đổi các quyền cho một ứng dụng riêng lẻ nếu cần thiết.

Cách thay đổi nhóm tin tưởng của một ứng dụng trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao → Phòng chống xâm nhập máy chủ**.



Thiết lập Phòng chống xâm nhập

4. 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.

5. Chọn thẻ **Các quyền của ứng dụng**.

6. Nhấn vào **Thêm**.

7. 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.

8. Nhấn vào **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.

9. Chọn ứng dụng cần thiết.

10. Trong danh sách thả xuống **Thêm ứng dụng được chọn vào nhóm tin tưởng**, hãy chọn nhóm tin tưởng cần thiết cho ứng dụng.

11. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách thay đổi nhóm tin tưởng của một ứng dụng trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.

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 **Host Threat Protection** → **Host Intrusion Prevention**.

5. Trong mục **Application rights and protected resources**, hãy nhấn liên kết **Application rights and protected resources**.

   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 **Application rights**.

   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 **Add**.

   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 **Application**. Chuyển sang bước tiếp theo.

   Nếu bạn muốn thay đổi nhóm tin tưởng cho nhiều ứng dụng, hãy chọn loại **Group** 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. Hoàn tất trình hướng dẫn.

    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 vào **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 xác 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

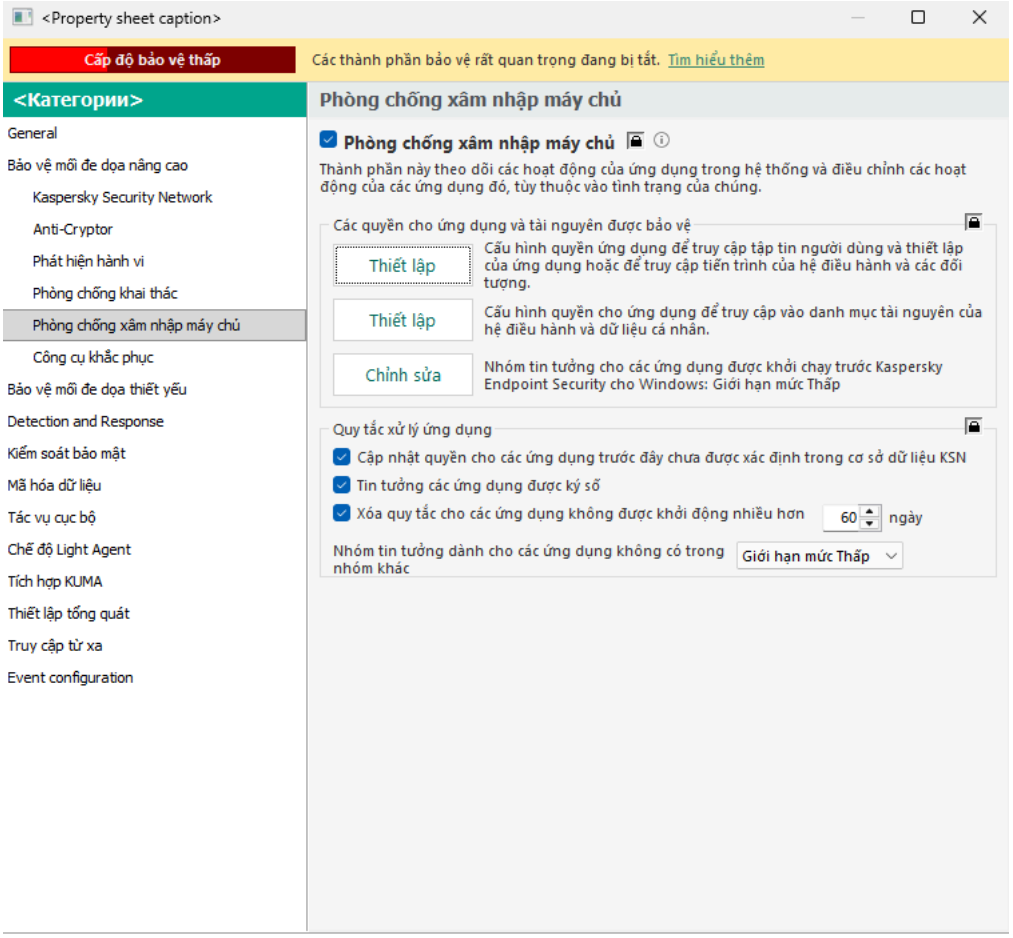
Các quyền ứng dụng tối ưu được tạo cho các nhóm tin tưởng khác nhau theo mặc định. Cấu hình quyền cho nhóm ứng dụng nằm trong một nhóm tin tưởng sẽ kế thừa các giá trị từ thiết lập quyền của các nhóm tin tưởng.

Cách thay đổi quyền của nhóm tin tưởng trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao → Phòng chống xâm nhập máy chủ**.



Thiết lập Phòng chống xâm nhập

4. 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.

5. Vào thẻ **Các quyền của ứng dụng**.

6. Chọn nhóm tin tưởng cần thiết.

7. 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.

8. 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 **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 thành phần Tường lửa bằng cách sử dụng *quy tắc mạng*.

9. 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** (⊘).

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. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và 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 **Asset management** → **Policies**.

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 **Host Threat Protection** → **Host Intrusion Prevention**.

5. Trong mục **Application rights and protected resources**, hãy nhấn liên kết **Application rights and protected resources**.

   Thao tác này sẽ mở ra cửa sổ cấu hình quyền của ứng dụng và danh sách các tài nguyên được bảo vệ.

6. Vào thẻ **Application rights**.

   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 **Files and system registry**.
   - 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 **Rights**.

   Hoạt động mạng của các ứng dụng được kiểm soát bởi thành phần 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: **Inherit**, **Allow** (), **Block** ().

10. Nếu bạn muốn giám sát việc sử dụng tài nguyên máy tính, hãy chọn **Log events** (/).

    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 vào **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 **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 thành phần 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 tùy chỉnh*) sẽ được gán cho nhóm tin tưởng.

Chọn một nhóm tin tưởng cho các ứng dụng được khởi động trước Kaspersky Endpoint Security

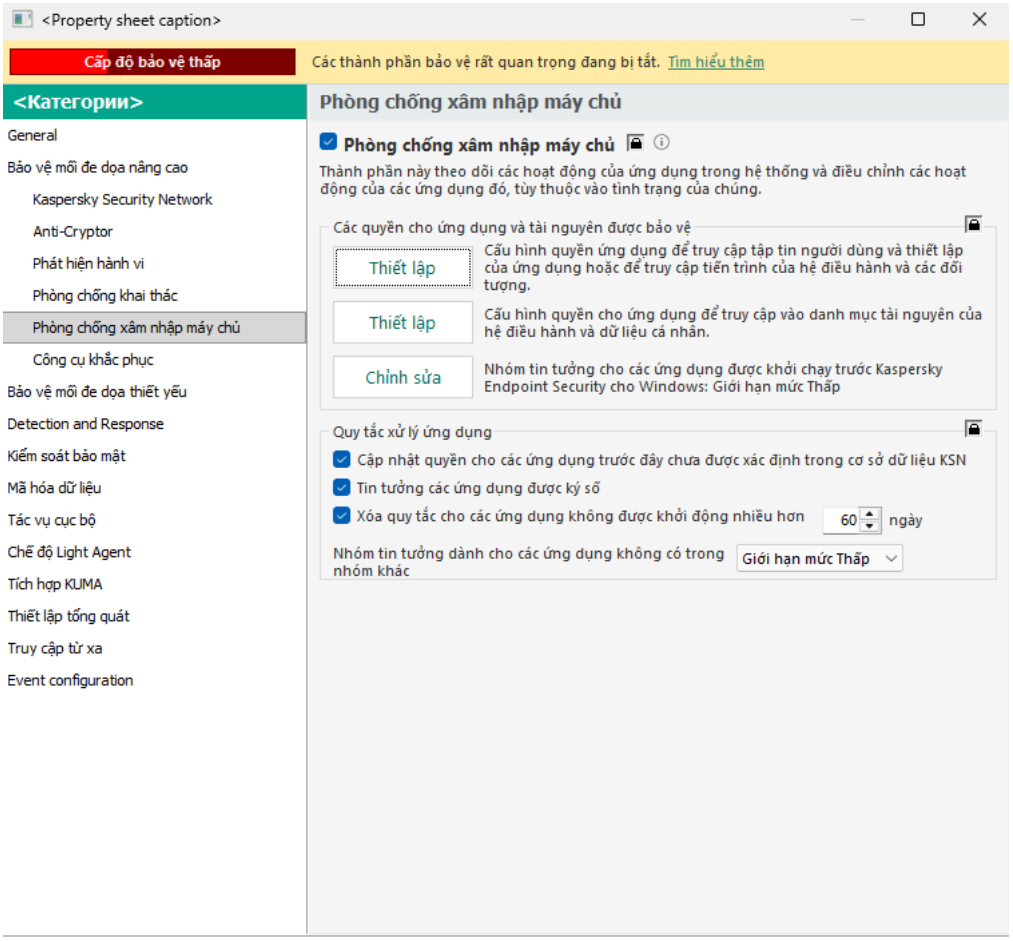
Đối với các ứng dụng đã được khởi động trước Kaspersky Endpoint Security, thành phần này chỉ kiểm soát hoạt động mạng của chúng. Tính năng kiểm soát được thực hiện thông qua các quy tắc mạng được xác định trong thiết lập Tường lửa. Để quy định các quy tắc mạng được áp dụng cho hoạt động mạng của những 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao → Phòng chống xâm nhập máy chủ**.



Thiết lập Phòng chống xâm nhập

4. Trong mục **Các quyền cho ứng dụng và tài nguyên được bảo vệ**, hãy nhấn nút **Chỉnh sửa**.

5. Đối với thiết lập **Trust group for applications started before Kaspersky Endpoint Security**, hãy chọn nhóm tin tưởng thích hợp.

6. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách chọn một nhóm tin tưởng cho các ứng dụng được khởi chạy trước Kaspersky Endpoint Security trong Bảngg điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Policies**.

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 **Host Threat Protection → Host Intrusion Prevention**.

5. Đối với thiết lập **Trust group for applications started before Kaspersky Endpoint Security**, 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 mối đe dọa nâng cao → Phòng chống xâm nhập máy chủ**.
3. Trong mục **Nhóm tin tưởng cho các ứng dụng được khởi chạy trước Kaspersky Endpoint Security** 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.

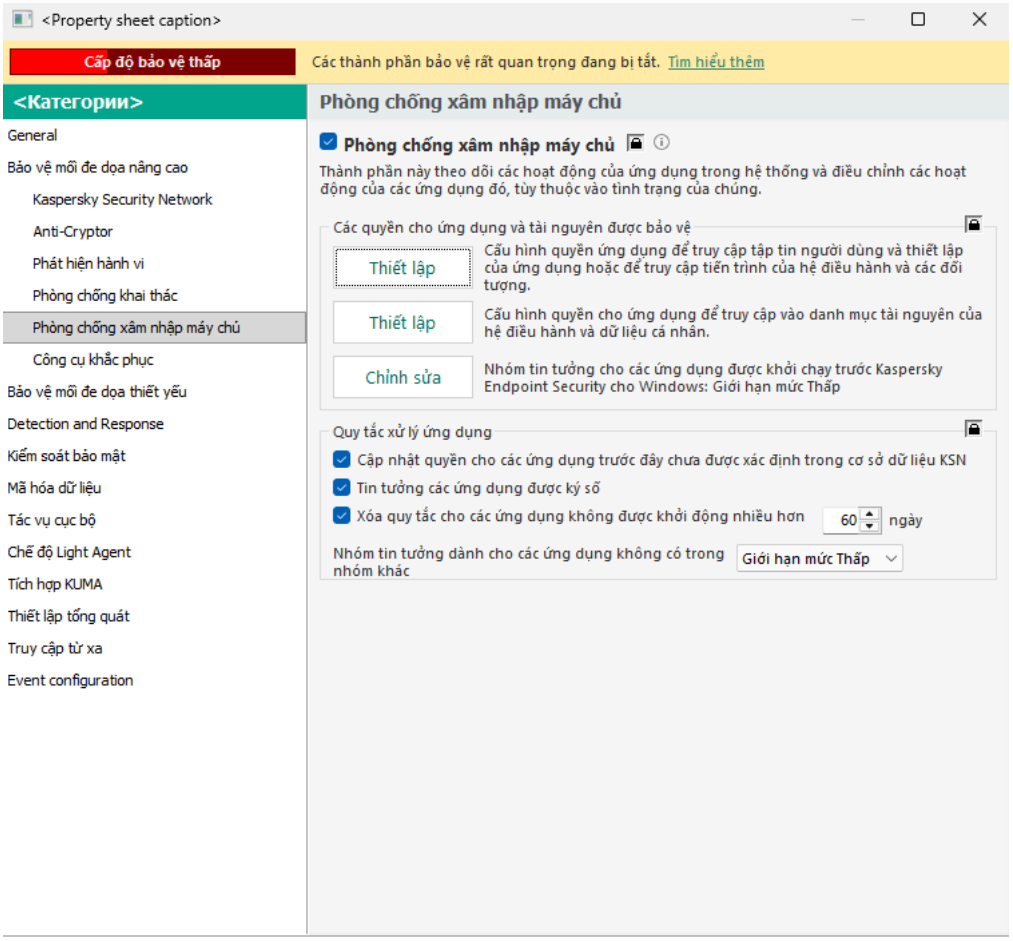
Chọn một nhóm tin tưởng cho các ứng dụng không xác định

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 *Giới hạn mức 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao → Phòng chống xâm nhập máy chủ**.



Thiết lập Phòng chống xâm nhập

4. Trong mục **Application processing rules**, hãy sử dụng danh sách thả xuống **Trust group for applications not included in other groups** 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.

5. Sử dụng hộp kiểm **Update rights for previously unknown applications from KSN database** để cấu hình cập nhật tự động quyền của các ứng dụng chưa biết.

6. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và 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 **Asset management → Policies**.

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 **Host Threat Protection → Host Intrusion Prevention**.

5. Trong mục **Application processing rules**, hãy sử dụng danh sách thả xuống **Trust group for applications not included in other groups** 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 **Update rights for previously unknown applications from KSN database** 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 thích hợp.

   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

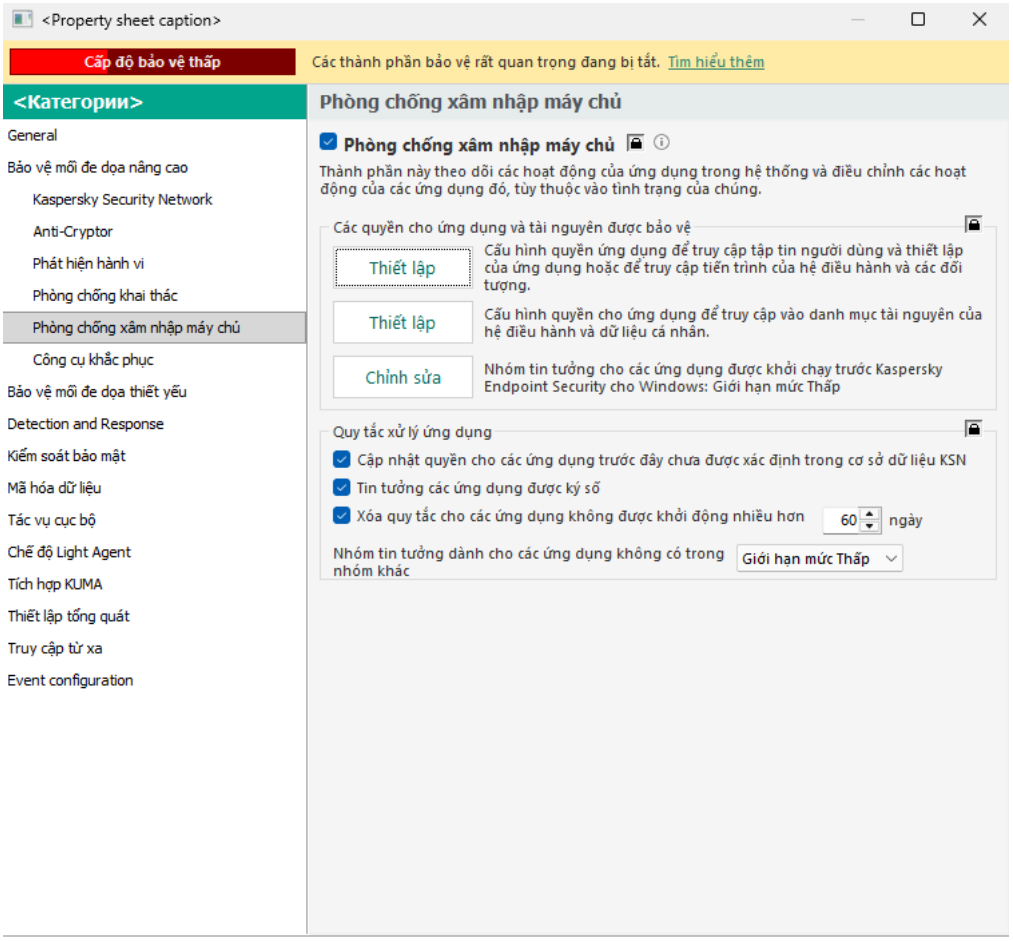
Kaspersky Endpoint Security luôn đặt các ứng dụng được ký bởi chứng chỉ Microsoft hoặc chứng chỉ Kaspersky vào nhóm *Tin tưởng*.

Cách chọn nhóm tin tưởng cho các ứng dụng được ký bằng chữ ký số trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao → Phòng chống xâm nhập máy chủ**.



Thiết lập Phòng chống xâm nhập

4. Trong mục **Application processing rules**, hãy sử dụng hộp kiểm **Trust digitally signed applications** để bật hoặc tắt gán tự động cho nhóm tin tưởng Trusted đối với các ứng dụng chứa chữ ký số của nhà các 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.

5. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và 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 **Asset management → Policies**.

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 **Host Threat Protection → Host Intrusion Prevention**.

5. Trong mục **Application processing rules**, hãy sử dụng hộp kiểm **Trust digitally signed applications** để bật hoặc tắt gán tự động cho nhóm tin tưởng Trusted đối với các ứng dụng chứa chữ ký số của nhà các 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 mối đe dọa nâng cao → Phòng chống xâm nhập máy chủ**.
3. Trong mục **Application processing rules**, hãy sử dụng hộp kiểm **Trust digitally signed applications** để bật hoặc tắt gán tự động cho nhóm tin tưởng Trusted đối với các ứng dụng chứa chữ ký số của nhà các 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.

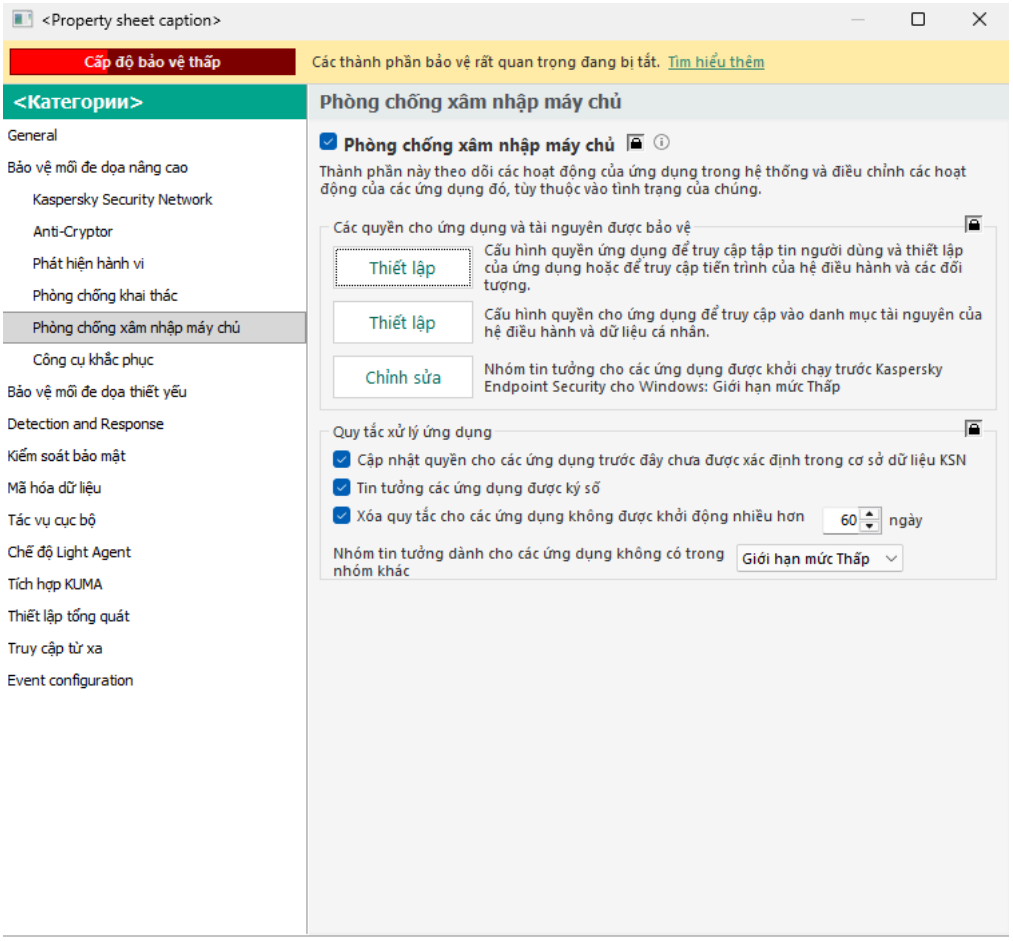
Các quyền của ứng dụng được quy định theo cách thủ công có mức độ ưu tiên cao hơn các quyền của ứng dụng đã được quy định cho một nhóm tin tưởng. Nói cách khác, nếu các quyền ứng dụng được quy định theo cách thủ công khác với các quyền ứng dụng được quy định cho một nhóm tin tưởng, thì thành phần Phòng 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao → Phòng chống xâm nhập máy chủ**.



Thiết lập Phòng chống xâm nhập

4. 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.

5. Vào thẻ **Các quyền của ứng dụng**.

6. Nhấn vào **Thêm**.

7. 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.

8. Nhấn vào **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.

9. Chọn ứng dụng cần thiết.

10. 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.

11. 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.

12. 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 **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 thành phần Tường lửa bằng cách sử dụng *quy tắc mạng*.

13. 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** (⊘).

14. 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.

15. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và 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 **Asset management** → **Policies**.
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 **Host Threat Protection** → **Host Intrusion Prevention**.
5. Trong mục **Application rights and protected resources**, hãy nhấn liên kết **Application rights and protected resources**.

   Thao tác này sẽ mở ra cửa sổ cấu hình quyền của ứng dụng và danh sách các tài nguyên được bảo vệ.
6. Vào thẻ **Application rights**.

   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 **Add**.

   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 **Application**. Chuyển sang bước tiếp theo.

   Nếu bạn muốn thay đổi nhóm tin tưởng cho nhiều ứng dụng, hãy chọn loại **Group** 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. Hoàn tất trình hướng dẫn.

    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 **Files and system registry**.
    - 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 **Rights**.

    > Hoạt động mạng của các ứng dụng được kiểm soát bởi thành phần 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: **Inherit**, **Allow** (), **Block** ().

15. Nếu bạn muốn giám sát việc sử dụng tài nguyên máy tính, hãy chọn **Log events** (/).

    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 vào **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 **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**.

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 tập tin được mở bởi ứng dụng	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. Bạn có thể cấu hình giám sát hoạt động ứng dụng cho các thành phần khác nhau của Kaspersky Endpoint Security: • **Không giám sát các thành phần bảo vệ và kiểm soát**. 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 giám sát Managed Detection and Response và Endpoint Detection and Response**. Hoạt động của ứng dụng được giám sát bởi tác nhân MDR tích hợp và tác nhân EDR (KATA) tích hợp. • **Không chặn nhập liệu tương tác với bảng điều khiển cho Endpoint Detection and Response**. Kaspersky Endpoint Security không gửi dữ liệu đo lường từ xa về việc quản lý ứng dụng trên bảng điều khiển. Dữ liệu đo lường từ xa được sử dụng bởi Kaspersky Anti Targeted Attack Platform (EDR).
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 ứng dụng của trẻ	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. Bạn có thể áp dụng loại trừ theo cách đệ quy. Để ứng dụng không giám sát hoạt động của toàn bộ chuỗi ứng dụng con.
Cho phép tương tác với giao diện của Kaspersky Endpoint Security	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. Kaspersky Endpoint Security phiên bản 14.0 trở về sau không hỗ trợ loại trừ lưu lượng mạng nếu giá trị hash được chỉ định cho một ứng dụng tin tưởng thay vì đường dẫn.

Bảo vệ tài nguyên hệ điều hành và dữ liệu cá nhân

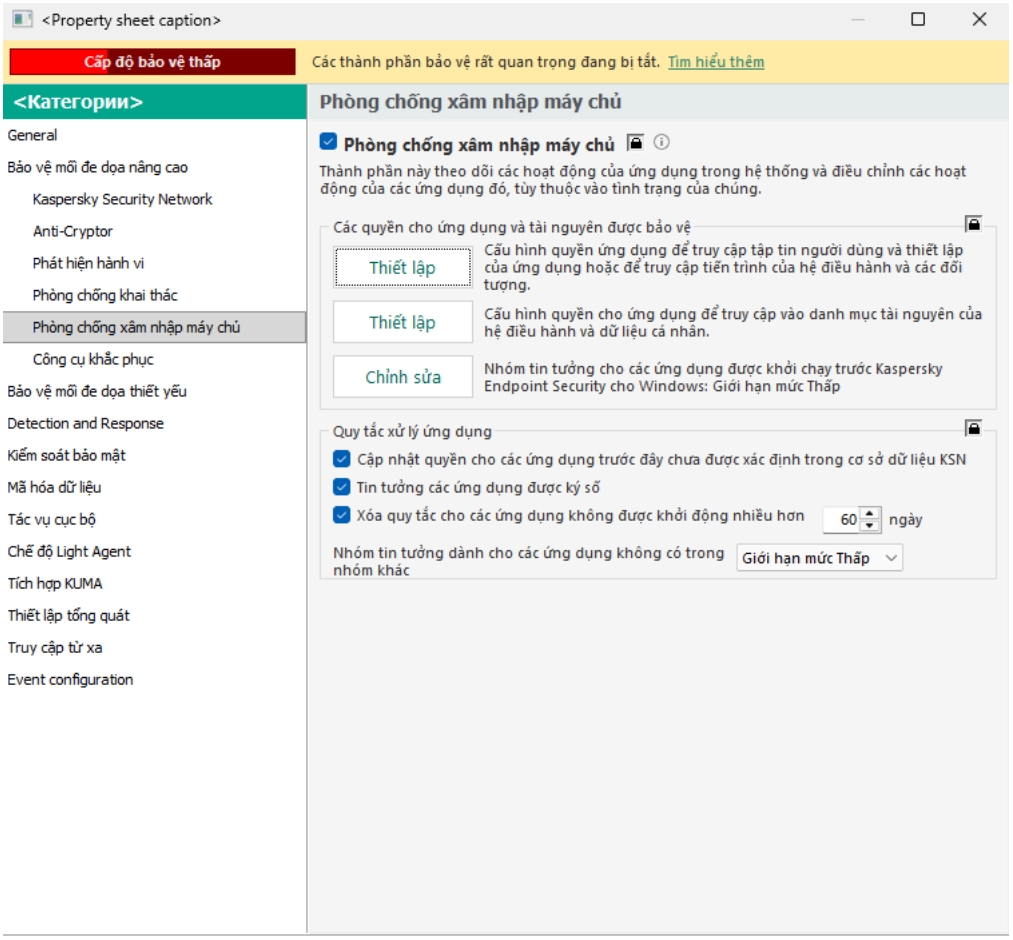
Thành phần Phòng chống xâm nhập máy chủ quản lý các quyền của ứng dụng trong việc thực hiện hành động đối với nhiều danh mục tài nguyên hệ điều hành và dữ liệu cá nhân. Các chuyên gia Kaspersky đã thiết lập sẵn các hạng mục tài nguyên được bảo vệ. Ví dụ: danh mục *Hệ điều hành* có danh mục con *Thiết 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.

Cách thêm tài nguyên được bảo vệ trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao → Phòng chống xâm nhập máy chủ**.



Thiết lập Phòng chống xâm nhập

4. 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.

5. Vào 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.

6. 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**.

7. Nhấn nút **Thêm**. Trong danh sách thả xuống, hãy chọn loại tài nguyên bạn muốn thêm: **Tập tin hoặc thư mục** hoặc **Khóa Registry**.

8. 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.

9. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và 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 **Asset management** → **Policies**.

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 **Host Threat Protection** → **Host Intrusion Prevention**.

5. Trong mục **Application rights and protected resources**, hãy nhấn liên kết **Application rights and protected resources**.

   Thao tác này sẽ mở ra cửa sổ cấu hình quyền của ứng dụng và danh sách các tài nguyên được bảo vệ.

6. Vào thẻ **Protected resources**.

   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 **Add**.

   Trình hướng dẫn Tài nguyên mới sẽ khởi chạy.

8. Trong mục **Group name**, hãy 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 **Category of protected resources**.

9. Hãy chọn loại tài nguyên bạn muốn thêm: **File or folder** hoặc **Registry key**.

10. Chọn một tập tin, thư mục hoặc khóa registry.

11. Hoàn tất trình hướng dẫn.

    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 **Status** 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 vào **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 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 **Bật 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).

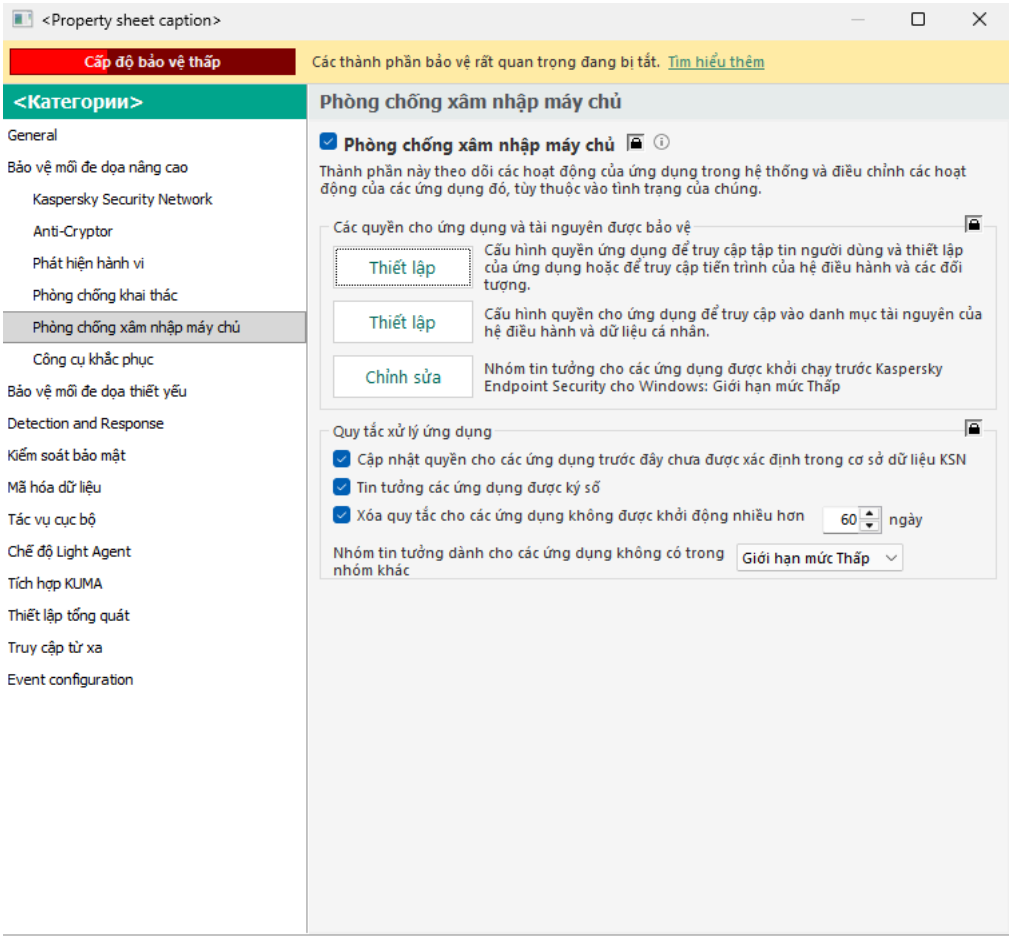
Khi bạn khởi chạy một ứng dụng có thông tin đã bị xóa, Kaspersky Endpoint Security sẽ phân tích ứng dụng đó như thể ứng dụng đó đang khởi chạy lần đầu tiên.

Cách cấu hình xóa tự động thông tin về các ứng dụng không sử dụng trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao → Phòng chống xâm nhập máy chủ**.



Thiết lập Phòng chống xâm nhập

4. Trong mục **Quy tắc xử lý ứng dụng**, hãy thực hiện một trong những hành động sau:

   - Nếu bạn muốn cấu hình xóa tự động, hãy chọn hộp kiểm **Xóa quy tắc cho các ứng dụng không được khởi động nhiều hơn N ngày** 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 thì hãy bỏ chọn 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.

5. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và 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 **Asset management** → **Policies**.
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 **Host Threat Protection** → **Host Intrusion Prevention**.
5. Trong mục **Application processing rules**, hãy thực hiện một trong những hành động sau:

   - Nếu bạn muốn cấu hình xóa tự động, hãy chọn hộp kiểm **Delete rules for applications that have not been started for longer than (days, 1 to 90)** 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 thì hãy bỏ chọn hộp kiểm **Delete rules for applications that have not been started for longer than (days, 1 to 90)**.

     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 xóa tự động, hãy chọn hộp kiểm **Xóa quy tắc cho các ứng dụng không được khởi động nhiều hơn N số ngày (từ 1 đến 90)** 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 thì hãy bỏ chọn hộp kiểm **Xóa quy tắc cho các ứng dụng không được khởi động nhiều hơn N số ngày (từ 1 đến 90)**.

  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 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

Chức năng bảo vệ tín hiệu âm thanh và chức năng bảo vệ truy cập webcam không được hỗ trợ trên các máy tính chạy trên kiến trúc Arm.

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 chỉ cho phép nhận luồng âm thanh và video cho các ứng dụng từ nhóm *Tin tưởng*. Các ứng dụng từ nhóm *Giới hạn mức Thấp*, *Giới hạn mức Cao* và *Không tin tưởng* không được phép nhận luồng âm thanh và luồng video từ 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 nhóm *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.

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.

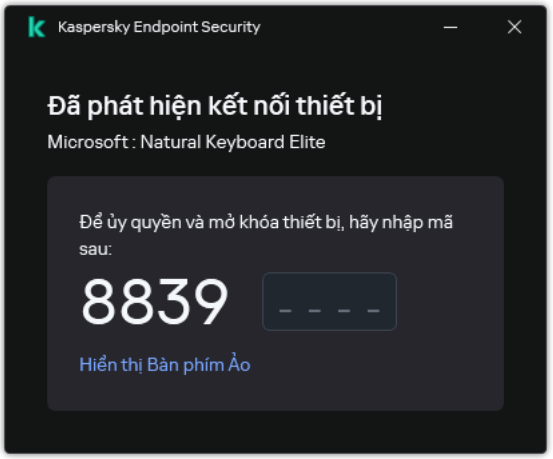
Khi một thiết bị USB được kết nối với máy tính và hệ điều hành xác định đó là một bàn phím thì ứng dụng sẽ nhắc người dùng nhập một mã số do ứng dụng tạo ra từ bàn phím này hoặc sử dụng Bàn phím ảo nếu có (xem hình bên dưới). Thủ tục này được gọi là xác thực bàn phím.

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.



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.

Cách bật hoặc tắt thành phần Phòng chống tấn công BadUSB trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Phòng chống tấn công BadUSB**.
4. Sử dụng hộp kiểm **Phòng chống tấn công BadUSB** để bật hoặc tắt thành phần.
5. 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 lần thử ủy quyền cho 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 năm lần nhập mã cho phép thì ứng dụng sẽ chặn thiết bị USB sau lần thử 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 sẽ lại có năm lần thử nhập mã cho phép.
   - **Kết thúc thời gian chờ khi đạt số lượng lần thử tối đa (số phút)**. Thời gian khóa thiết bị USB sau số lần nhập mã xác thực không thành công được chỉ định. Giá trị hợp lệ là 1 đến 180 (phút).
6. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

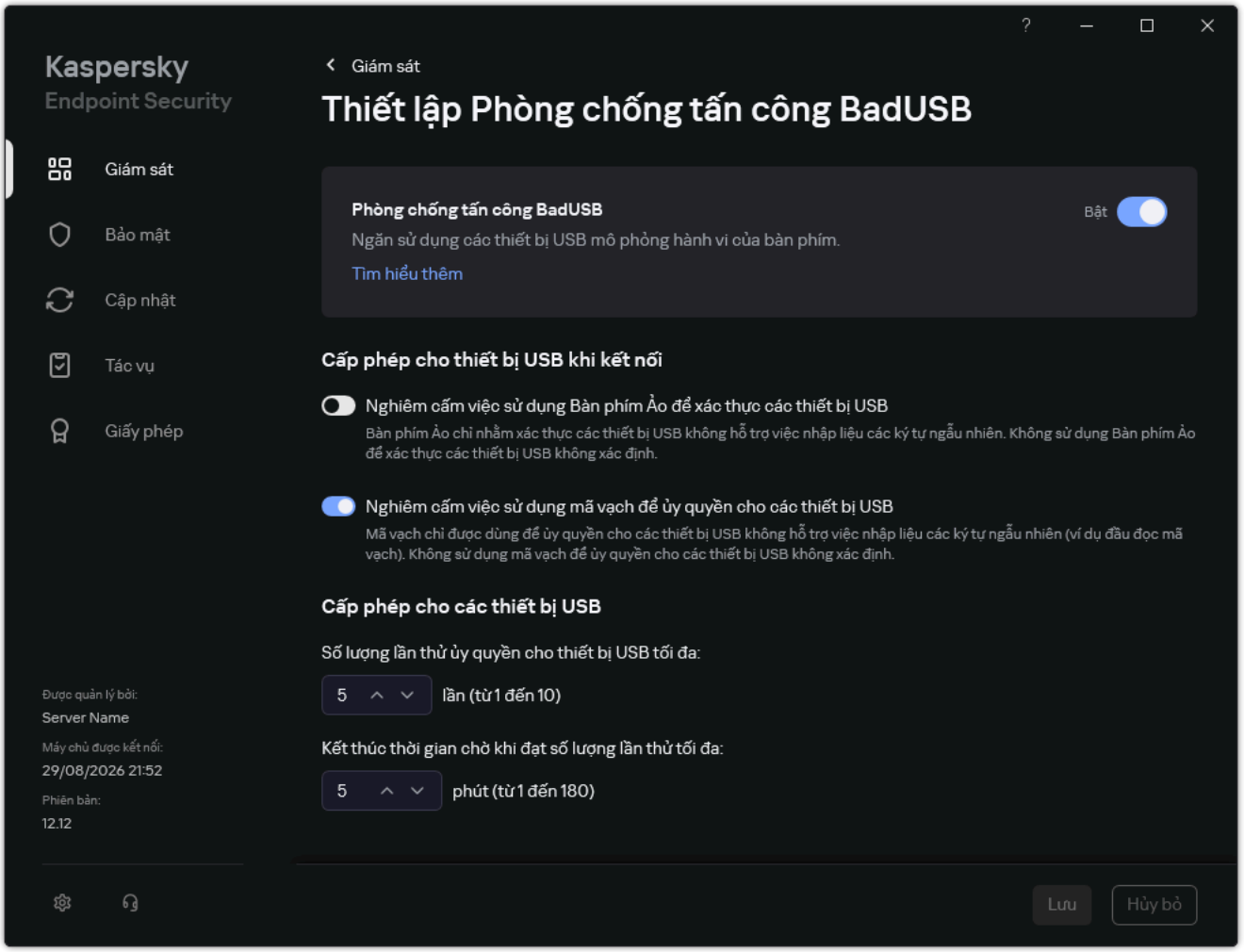
Cách bật hoặc tắt thành phần Phòng chống tấn công BadUSB trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Host Threat Protection** → **BadUSB Attack Prevention**.
5. Sử dụng nút bật/tắt **BadUSB Attack Prevention ENABLED** để bật hoặc tắt thành phần này.
6. Trong mục **Authorization of USB devices**, hãy điều chỉnh thiết lập bảo mật để nhập mã cho phép:
   - **Maximum number of USB device authorization attempts**. 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 năm lần nhập mã cho phép thì ứng dụng sẽ chặn thiết bị USB sau lần thử 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 sẽ lại có năm lần thử nhập mã cho phép.
   - **Timeout when reaching the maximum number of attempts (min)**. Thời gian khóa thiết bị USB sau số lần nhập mã xác thực không thành công được chỉ định. Giá trị hợp lệ là 1 đến 180 (phút).
7. Lưu các thay đổi của bạn.

Cách bật hoặc tắt thành phần Phòng chống tấn công BadUSB 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 → Phòng chống tấn công BadUSB**.



Cấu hình thành phần Phòng chống Tấn công BadUSB

3. Sử dụng nút bật/tắt **Phòng chống tấn công BadUSB** để bật hoặc tắt thành phần này.

4. Trong mục **Cấp phép cho thiết bị USB khi kết nối**, hãy điều chỉnh thiết lập bảo mật để nhập mã cho phép:

   - **Số lượng lần thử ủy quyền cho 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 năm lần nhập mã cho phép thì ứng dụng sẽ chặn thiết bị USB sau lần thử 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 sẽ lại có năm lần thử nhập mã cho phép.

   - **Kết thúc thời gian chờ khi đạt số lượng lần thử tối đa**. Thời gian khóa thiết bị USB sau số lần nhập mã xác thực 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

Chỉ nên sử dụng Bàn phím Ảo để cấp quyền cho các thiết bị USB không hỗ trợ việc nhập liệu ký tự ngẫu nhiên (như đầu quét mã vạch). Bạn không nên sử dụng Bàn phím Ảo để xác thực các thiết bị USB không xác định.

Cách cho phép hoặc cấm sử dụng Bàn phím ảo để xác thực trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Phòng chống tấn công BadUSB**.
4. 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.
5. Lưu các thay đổi của bạn.

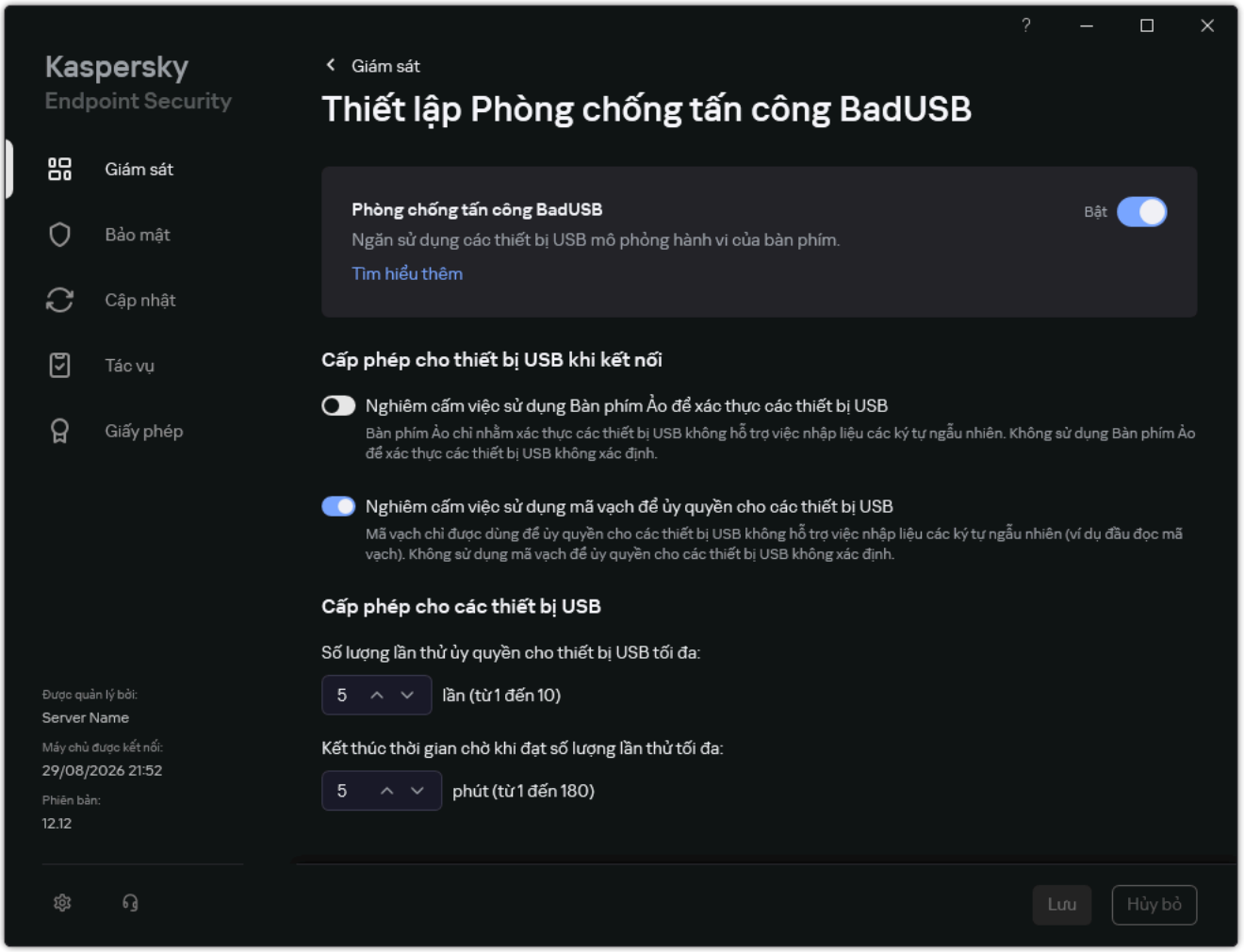
Cách cho phép hoặc cấm sử dụng Bàn phím ảo để xác thực trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Policies**.
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 **Host Threat Protection → BadUSB Attack Prevention**.
5. Sử dụng nút bật/tắt **Prohibit use of On-Screen Keyboard for authorization of USB devices** để chặn hoặc cho phép việc sử dụng Bàn phím ảo để xác thực.
6. Lưu các thay đổi của bạn.

Cách cho phép hoặc cấm sử dụng Bàn phím ảo để xác thực trong giao diện ứng dụng

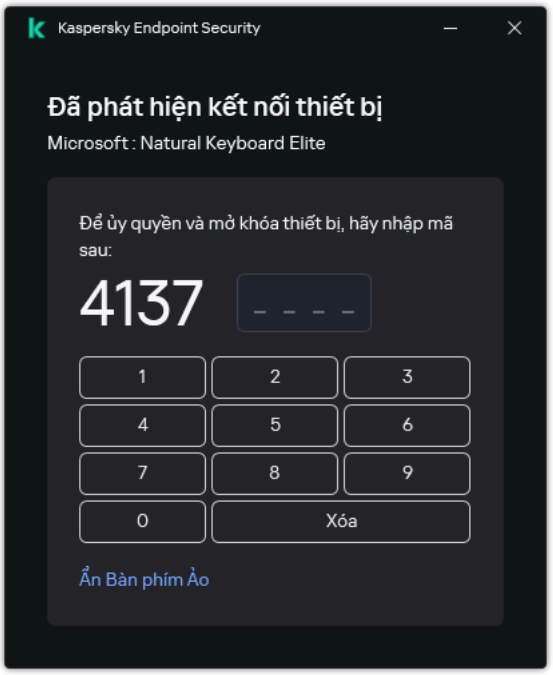
1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút ⚙.
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Phòng chống tấn công BadUSB**.



Cấu hình thành phần Phòng chống Tấn công BadUSB

3. Sử dụng nút bật/tắt **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.



Cấp quyền cho các thiết bị USB

Cấp quyền cho đầu quét mã vạch

Khi kết nối đầu quét mã vạch với máy tính, thành phần Phòng chống tấn công BadUSB sẽ xác định thiết bị này là thiết bị đầu vào và nhắc bạn thực hiện xác thực. Để cấp quyền cho đầu quét mã vạch, bạn phải quét mã vạch hiển thị trên màn hình. Ứng dụng tạo ra một mã vạch ở định dạng Code39 được hầu hết các máy quét mã vạch và mã QR hỗ trợ.

Kaspersky Endpoint Security cũng hỗ trợ một phương thức xác thực đầu quét mã vạch khác. Nếu đang sử dụng thiết bị màn hình cảm ứng, bạn có thể sử dụng bàn phím trên màn hình để nhập mã. Để thực hiện, bạn cần phải cho phép sử dụng bàn phím ảo. Phương thức này rất tiện lợi, ví dụ, trong trường hợp đầu quét mã vạch cố định được tích hợp vào máy tính tiền. Các phương thức xác thực đầu quét mã vạch khác đều bị cấm.

Theo mặc định, ứng dụng không sử dụng mã vạch để xác thực thiết bị USB.

Cách bật cấp quyền cho thiết bị USB bằng mã vạch trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.

2. Trong cây bảng điều khiển, hãy chọn **Policies**.

3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

4. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Phòng chống tấn công BadUSB**.

5. Sử dụng hộp kiểm **Nghiêm cấm việc sử dụng mã vạch để ủy quyền cho các thiết bị USB** để chặn hoặc cho phép sử dụng mã vạch để cấp quyền.

6. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật cấp quyền cho thiết bị USB bằng mã vạch trong bảng điều khiển web và bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.

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**.

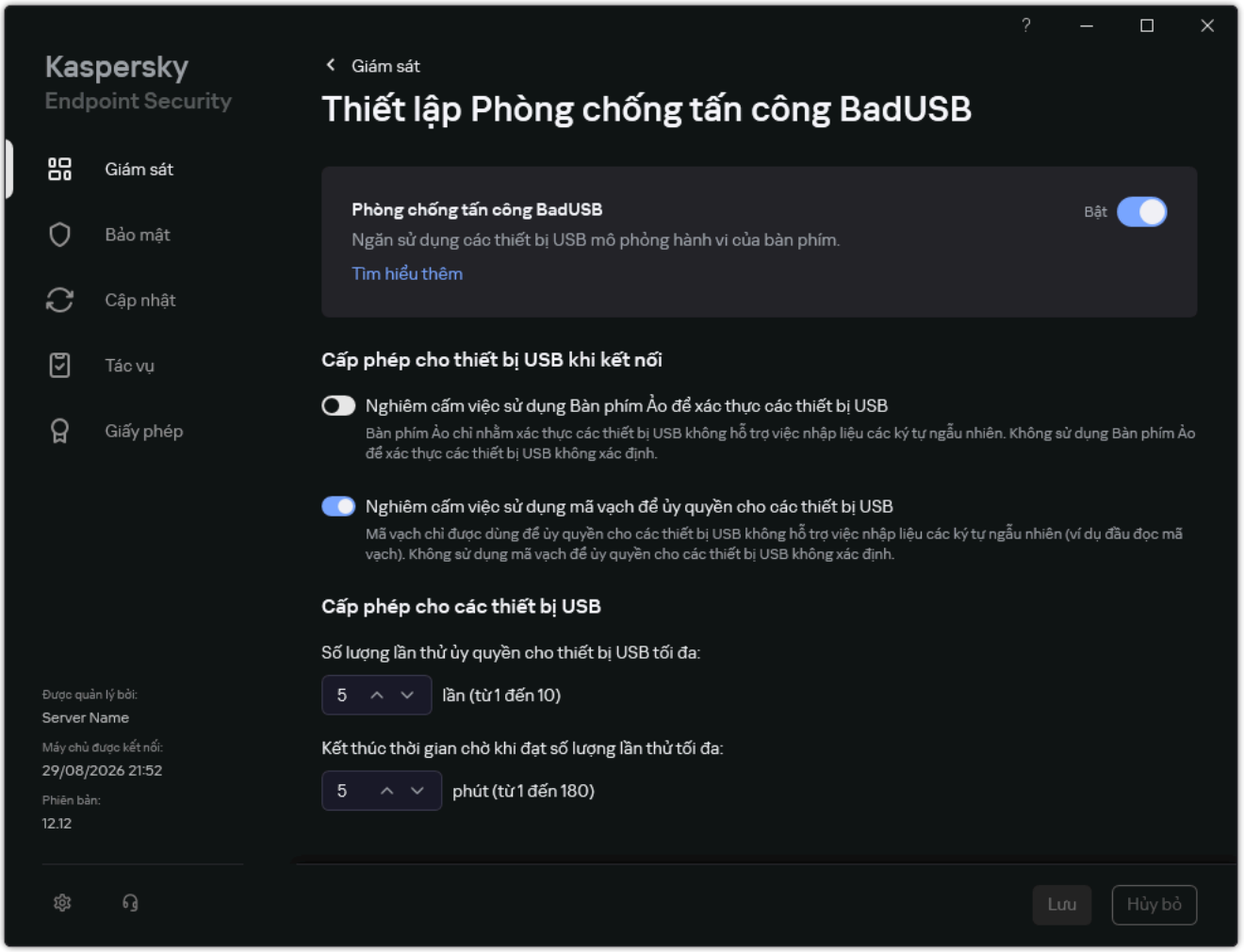
4. Vào **Host Threat Protection** → **BadUSB Attack Prevention**.

5. Sử dụng nút bật/tắt **Prohibit use of a barcode for authorization of USB devices** để chặn hoặc cho phép việc sử dụng mã vạch để cấp quyền.

6. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

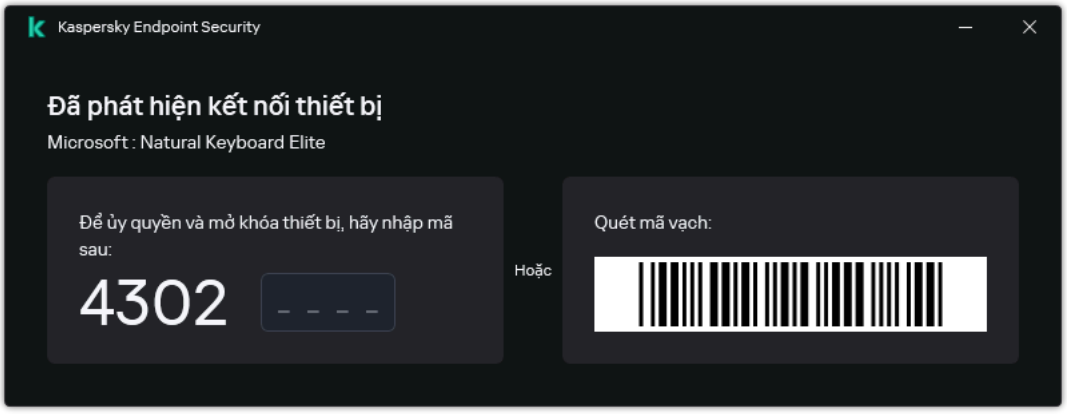
Cách bật cấp quyền cho thiết bị USB bằng mã vạch trong giao diện ứng dụng

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 → Phòng chống tấn công BadUSB**.



Cấu hình thành phần Phòng chống Tấn công BadUSB

3. Sử dụng nút bật/tắt **Nghiêm cấm việc sử dụng mã vạch để ủy quyền cho các thiết bị USB** để chặn hoặc cho phép việc sử dụng mã vạch để cấp quyền.
4. Lưu các thay đổi của bạn.

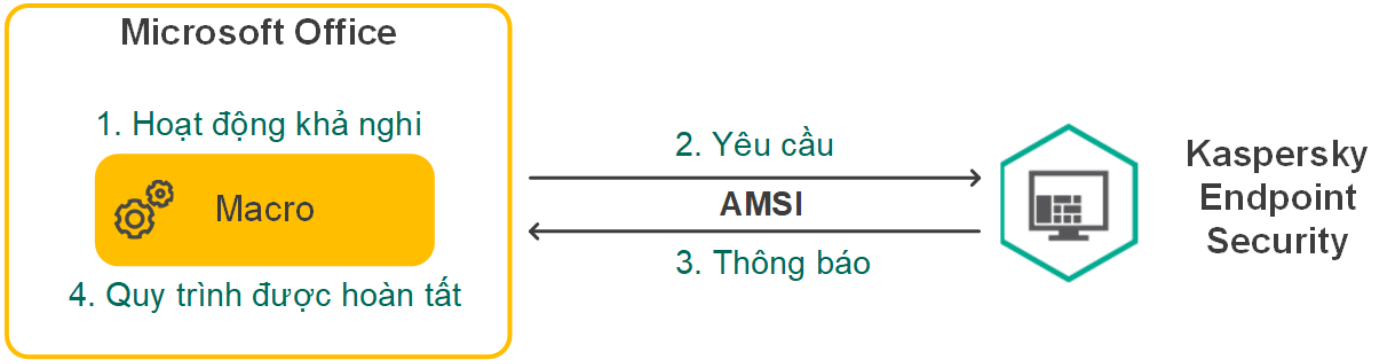


Cấp quyền cho đầu quét mã vạch

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 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 / Enterprise multi-session
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-session
- Windows Server 2016 Essentials / Standard / Datacenter (bao gồm chế độ Server Core);
- Windows Server 2019 Essentials / Standard / Datacenter (bao gồm chế độ Server Core);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (bao gồm chế độ Core Server);
- Windows Server 2025 Standard / Datacenter.

Bật và tắt Bảo vệ AMSI

Theo mặc định, Bảo vệ AMSI được bật và hoạt động ở chế độ được Kaspersky khuyến nghị (xem bảng bên dưới).

Cách bật hoặc tắt Bảo vệ AMSI trong Bảng điều khiển quản trị (MMC)

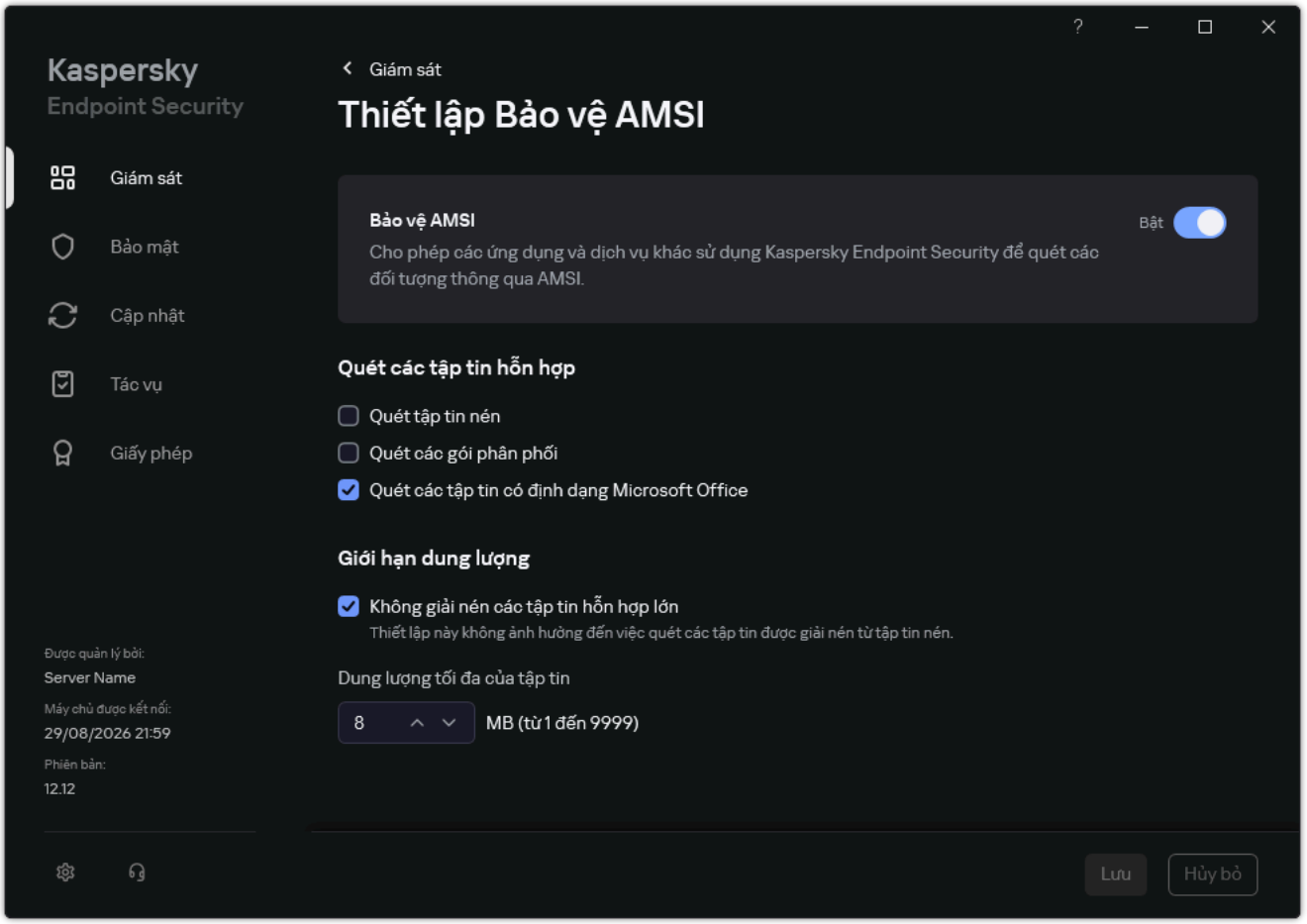
1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Trình quét AMSI**.
4. Sử dụng hộp kiểm **Trình quét AMSI** để bật hoặc tắt thành phần.
5. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật hoặc tắt Bảo vệ AMSI trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Policies**.
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 **Host Threat Protection → AMSI Protection**.
5. Sử dụng nút bật/tắt **AMSI Protection ENABLED** để bật hoặc tắt thành phần này.
6. Lưu các thay đổi của bạn. Để áp dụng chính sách trên máy tính, hãy đóng ổ khóa .

Cách bật hoặc tắt Bảo vệ AMSI 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 AMSI**.



Thiết lập Bảo vệ AMSI

3. Sử dụng nút bật/tắt **Bảo vệ AMSI** để bật hoặc tắt thành phần này.
4. Lưu các thay đổi của bạn.

Thiết lập Bảo vệ AMSI được các chuyên gia Kaspersky khuyến nghị

Tham số	Giá trị	Mô tả
Quét tập tin nén	**Tắt**	Quét định dạng ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE, và các định dạng tập tin nén khác. Ứng dụng 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	**Tắt**	Quét các gói phân phối của ứng dụng bên thứ ba.
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. Ứng dụng sẽ quét các tập tin định dạng văn phòng nhỏ hơn 1 MB, bất kể hộp kiểm này có được chọn hay không.
Không giải nén các tập tin hỗn hợp lớn	**Dung lượng tối đa của tập tin 8 MB**	Nếu hộp kiểm này được chọn, ứng dụng sẽ không quét các tập tin hỗn hợp nếu dung lượng của chúng vượt quá giá trị ấn định. Nếu bỏ chọn hộp kiểm này, ứng dụng sẽ quét các tập tin tổ hợp thuộc mọi kích thước. Ứng dụng sẽ quét các tập tin lớn được trích xuất từ tập tin nén, bất kể hộp kiểm này có được chọn hay không.

Tối ưu hóa quét tập tin bằng Bảo vệ AMSI

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. Bạn có thể chọn các tập tin hỗn hợp cần quét: tập tin nén, gói phân phối hoặc tập tin ở định dạng Office. Bạn cũng có thể giới hạn kích thước của các tập tin hỗn hợp cần được quét. Thành phần Bảo vệ AMSI sẽ không giải nén các tập tin hỗn hợp lớn hơn dung lượng được quy định.

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 loại tập tin hỗn hợp được quét để tăng tốc độ quét.

Cách tối ưu hóa quét bằng Bảo vệ AMSI trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Trình quét AMSI**.
4. Trong mục **Quét các tập tin hỗn 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. Trong mục **Giới hạn dung lượng**, 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 hỗn hợp lớn** và chỉ định giá trị bắt buộc. 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 hỗn 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 hỗn hợp lớn** có được chọn hay không.
6. Lưu các thay đổi của bạn. Để áp dụng chính sách trên máy tính, hãy đóng ổ khóa .

Cách tối ưu hóa quét bằng Bảo vệ AMSI trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Policies**.
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 **Host Threat Protection → AMSI Protection**.
5. Trong mục **Scan of compound files**, quy định loại tập tin hỗn hợp mà bạn muốn quét: tập nén, gói phân phối, hoặc tập tin trong định dạng văn bản.

6. Trong mục **Scan optimization**, hãy thực hiện một trong những hành động sau:

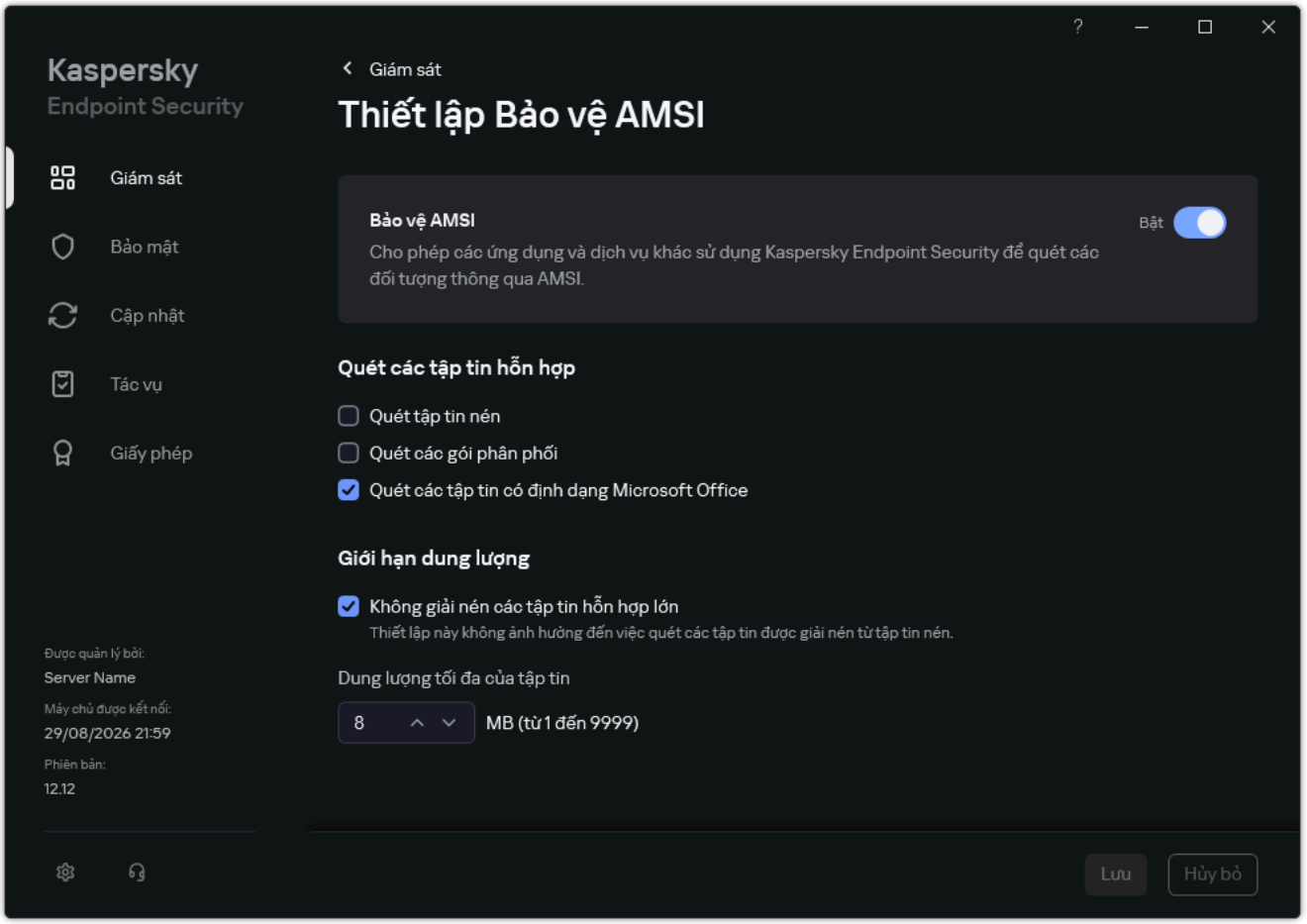
   - Để chặn thành phần Bảo vệ AMSI giải nén các tập tin hỗn hợp quá lớn, hãy chọn hộp kiểm **Size limits enabled** và chỉ định giá trị bắt buộc. Thành phần Bảo vệ AMSI sẽ không giải nén các tập tin hỗn hợp lớn hơn dung lượng được quy định.
   - Để cho phép Bảo vệ AMSI giải nén các tập tin hỗn hợp lớn, hãy xóa hộp kiểm **Size limits enabled**.

   Thành phần Bảo vệ AMSI sẽ quét các tập tin lớn được giải nén từ tập nén, bất kể là hộp kiểm **Size limits enabled** có được chọn hay không.

7. Lưu các thay đổi của bạn. Để áp dụng chính sách trên máy tính, hãy đóng ổ khóa .

Cách tối ưu hóa quét bằng Bảo vệ AMSI 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 AMSI**.



Thiết lập Bảo vệ AMSI

3. Trong mục **Quét các tập tin hỗn 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 **Giới hạn dung lượng**, 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 hỗn hợp lớn** và chỉ định giá trị bắt buộc. 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 hỗn 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 hỗn hợp lớn** có được chọn hay không.

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 kết nối đến 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.

Để sử dụng Bảo vệ mối đe dọa web, bạn phải hoàn thành cấu hình ban đầu của ứng dụng:

- Để giám sát lưu lượng HTTPS, hãy bật kết nối được mã hóa quét (được bật theo mặc định).
- Chọn các cổng mà Kaspersky Endpoint Security phải giám sát (theo mặc định, ứng dụng sẽ giám sát tất cả các cổng).
- Chọn các ứng dụng có lưu lượng mà bạn muốn Kaspersky Endpoint Security giám sát. Hầu hết các trình duyệt đã có trong danh sách ứng dụng đều được Kaspersky khuyên dùng. Hãy thêm theo cách thủ công nếu trình duyệt của bạn không có trong danh sách.
- Bạn nên chèn một tập lệnh tương tác trang web vào lưu lượng truy cập web (chèn tập lệnh bị tắt theo mặc định). Tập lệnh này cho phép đăng ký các sự kiện Bảo vệ mối đe dọa web cho nhật ký sự kiện ứng dụng, nhật ký sự kiện HĐH và báo cáo.

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

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, ứng dụng có thể áp dụng các nhóm thiết lập khác nhau. Các nhóm thiết lập được lưu trữ trong ứng dụng được gọi là *mức độ bảo mật*: **Cao**, **Khuyên dùng**, **Thấp**. Thiết lập mức độ bảo mật lưu lượng web **Khuyên 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 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Bảo vệ mối đe dọa web**.
4. Sử dụng hộp kiểm **Bảo vệ mối đe dọa web** để bật hoặc tắt thành phần.
5. 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 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.
     - **Khuyên dùng**. Mức độ bảo mật email mang đến sự cân bằng tối ưu giữa hiệu năng của ứng dụng 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 nhanh.

   - 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 (xem bảng bên dưới).

     Bạn có thể khôi phục các giá trị của các mức bảo mật cài đặt sẵn bằng cách nhấn vào nút **Theo mặc định**.

6. 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**. 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.

7. Lưu các thay đổi của bạn.

Cách bật hoặc tắt thành phần Bảo vệ mối đe dọa web trong Bảng điều khiển web

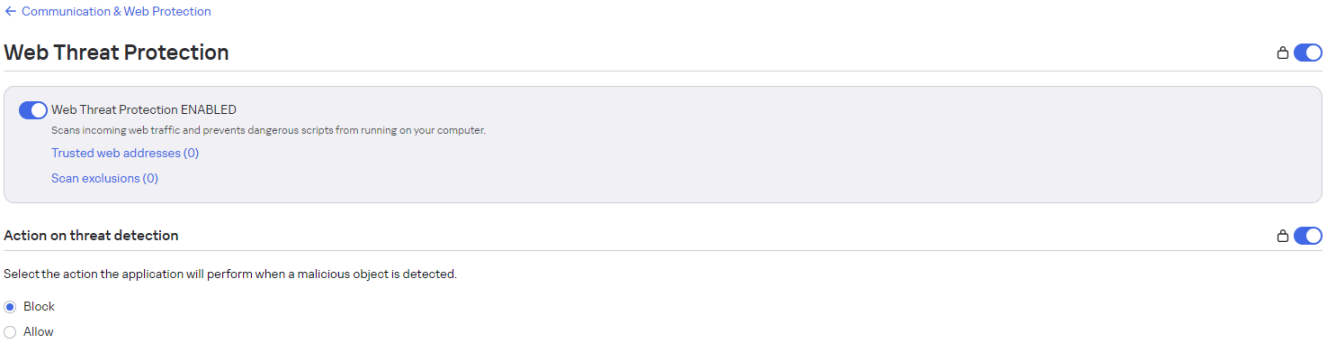
1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.

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 **Communication & Web Protection** → **Web Threat Protection**.



Thiết lập Bảo vệ mối đe dọa web

5. Sử dụng nút bật/tắt **Web Threat Protection ENABLED** để bật hoặc tắt thành phần này.

6. Trong mục **Action on threat detection**, chọn hành động được Kaspersky Endpoint Security thực hiện khi phát hiện các đối tượng lưu lượng web độc hại:

   - **Block**. 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.

   - **Allow, inform, or prompt for action (depends on OS)**. 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. Nếu cần, lập danh sách các địa chỉ web được tin tưởng.

8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật hoặc tắt thành phần Bảo vệ mối 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 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**. 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 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.
     - **Khuyên dùng**. Mức độ bảo mật email mang đến sự cân bằng tối ưu giữa hiệu năng của ứng dụng 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 nhanh.
   - 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 (xem bảng bên dưới).

     Bạn có thể khôi phục các giá trị của các mức bảo mật cài đặt sẵn bằng cách nhấn vào nút **Khôi phục cấp bảo mật được khuyến nghị**.
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**. 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 cơ sở dữ liệu địa chỉ web độc hại	**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 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.

Tham số	Giá trị	Mô tả
Sử dụng phân tích hành vi (Bảo vệ mối 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**	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.

Cấu hình các phương pháp phát hiện địa chỉ web độc hại

Thành phần Bảo vệ mối 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 Security 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Bảo vệ mối đe dọa web**.

4. Trong mục **Mức độ bảo mật**, hãy nhấn nút **Thiết lập**.

5. Trong cửa sổ mở ra, 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.

6. 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 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 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Bảo vệ mối đe dọa web**.

4. Trong mục **Mức độ bảo mật**, hãy nhấn nút **Thiết lập**.

5. Trong cửa sổ mở ra, 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.

6. 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.

7. 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Bảo vệ mối đe dọa web**.
4. Trong mục **Mức độ bảo mật**, hãy nhấn nút **Thiết lập**.
5. Trong cửa sổ mở ra, 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.
6. 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.
7. 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 cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Bảo vệ mối đe dọa web**.
5. Trong mục **Mức độ bảo mật**, hãy nhấn nút **Thiết lập**.
6. Trong cửa sổ mở ra, hãy chọn thẻ **Địa chỉ web được tin tưởng**.
7. Chọn hộp kiểm **Không quét lưu lượng web từ các địa chỉ web được tin tưởng**.

   Nếu chọn tùy chọn này, 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.
8. 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.
9. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách thêm địa chỉ web được tin tưởng trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management → Policies**.
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 **Trusted Zone**.
5. Trong cửa sổ mở ra, hãy nhấn vào liên kết **Web addresses**.

   Thao tác này sẽ mở cửa sổ chứa 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 JSON.

7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và 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 chọn tùy chọn này, 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 mối đe dọa web, Bảo vệ mối đe dọa thư điện tử và 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Bảo vệ mối đe dọa web**.

4. Trong mục **Mức độ bảo mật**, hãy nhấn nút **Thiết lập**.

5. Trong cửa sổ mở ra, hãy chọn thẻ **Địa chỉ web được tin tưởng**.

6. 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 vào 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.

7. Để nhập danh sách địa chỉ được tin tưởng:

   a. Nhấn vào 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.

8. 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 **Asset management** → **Policies**.

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 **Communication & Web Protection** → **Web Threat Protection**.

5. Để xuất danh sách loại trừ trong mục **Rules list**:

   a. Chọn địa chỉ web được tin tưởng mà bạn muốn xuất.

   b. Nhấn nút → **Export**.

   Kaspersky Endpoint Security sẽ xuất danh sách địa chỉ web vào tập tin JSON trong thư mục tải xuống mặc định.

6. Để nhập danh sách loại trừ trong mục **Rules list**:

   a. Nhấn nút → **Import**.

   Trong cửa sổ mở ra, hãy chọn tập tin JSON 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 JSON.

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
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Để quét lưu lượng truy cập trong ứng dụng thư Mozilla Thunderbird, MyOffice Mail và R7-Office Organizer, bạn cần phải thêm chứng chỉ Kaspersky vào kho chứng chỉ và chọn kho chứng chỉ riêng.

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 Mail Threat Protection hỗ trợ các phiên bản 32 bit và 64 bit của Outlook 2010, 2013, 2016, 2019, 2021, 2024 và 365. Trên máy tính có kiến trúc Arm, phần mở rộng Mail Threat Protection hỗ trợ các phiên bản 32 bit và 64 bit của Outlook 2016, Outlook 2021, Outlook 2024 và Outlook 365 dành cho Arm64.

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 phần đính kèm, Kaspersky Endpoint Security sẽ thêm thông tin về hành động đã thực hiện vào chủ đề thư, ví dụ: *[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, ứng dụng có thể áp dụng các nhóm thiết lập khác nhau. Các nhóm thiết lập được lưu trữ trong ứng dụng được gọi là *mức độ bảo mật*: **Cao**, **Khuyên dùng**, **Thấp**. Thiết lập mức độ bảo mật thư điện tử **Khuyên 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.

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.

Cách bật hoặc tắt thành phần Bảo vệ mối đe dọa thư điện tử trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Bảo vệ mối đe dọa thư điện tử**.
4. Sử dụng hộp kiểm **Bảo vệ mối đe dọa thư điện tử** để bật hoặc tắt thành phần.
5. 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.
     - **Khuyên dùng**. Mức độ bảo mật email mang đến sự cân bằng tối ưu giữa hiệu năng của ứng dụng 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** và định nghĩa thiết lập thành phần của riêng bạn (xem bảng bên dưới).

  Bạn có thể khôi phục các giá trị của các mức bảo mật cài đặt sẵn bằng cách nhấn vào nút **Theo mặc định**.

6. Trong mục **Hành động khi phát hiện mối đe dọa**, chọn hành động được Kaspersky Endpoint Security thực hiện đối với các đối tượng độc hại:

   - **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, ứng dụng 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, ứng dụng sẽ xóa đối tượng bị nhiễm. Ứng dụng sẽ thêm thông tin về hành động được thực hiện vào chủ đề thư, ví dụ: *[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, ứng dụng 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, ứng dụng sẽ thêm cảnh báo vào chủ đề thư điện tử. 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, ứng dụng sẽ cố gắng khử mã độc đối tượng được phát hiện. Nếu không thể khử mã độc đối tượng, ứng dụng 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, ứng dụng sẽ thêm cảnh báo vào 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, ứng dụng sẽ chặn gửi thư và ứng dụng thư điện tử sẽ hiển thị lỗi.

7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật hoặc tắt thành phần Bảo vệ mối đe dọa thư điện tử trong Bảng điều khiển web

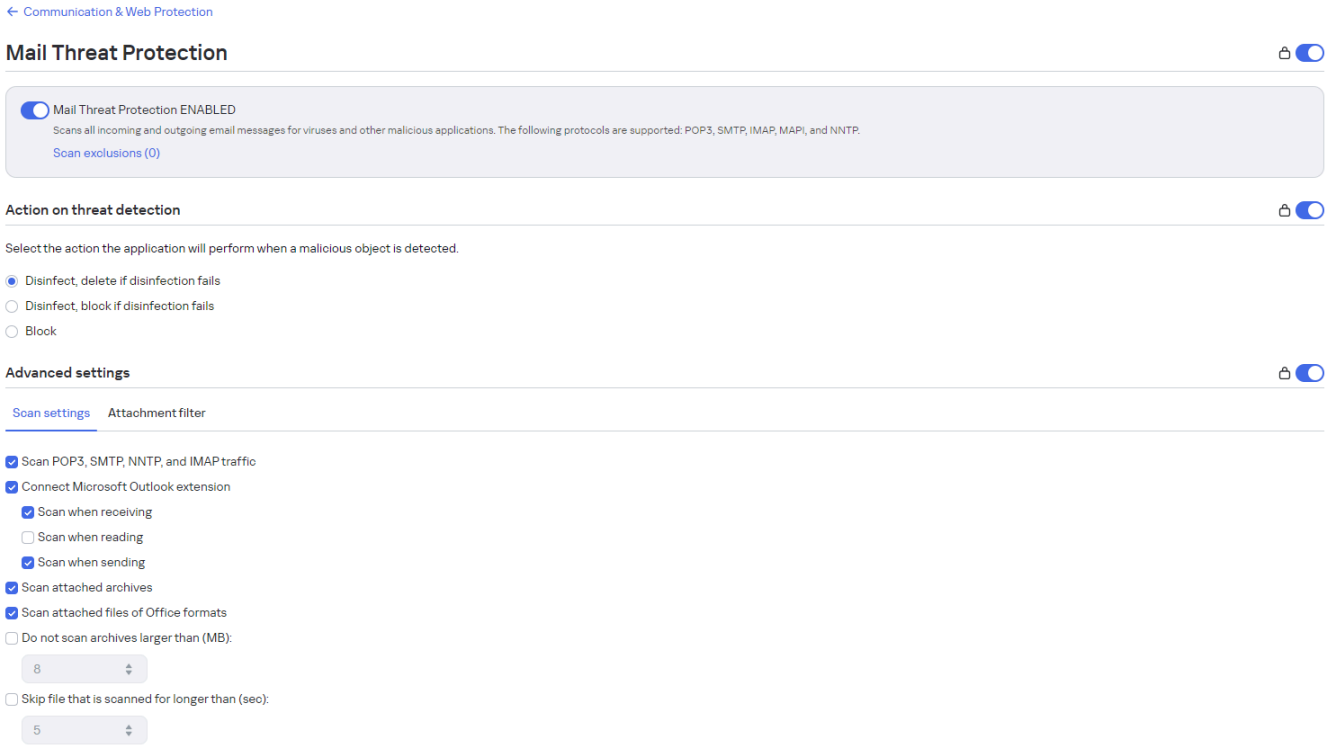
1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Policies**.

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 **Communication & Web Protection** → **Mail Threat Protection**.



Thiết lập Bảo vệ mối đe dọa thư điện tử

5. Sử dụng nút bật/tắt **Mail Threat Protection ENABLED** để bật hoặc tắt thành phần này.

6. Trong mục **Action on threat detection**, chọn hành động được Kaspersky Endpoint Security thực hiện đối với các đối tượng độc hại:

   - **Disinfect, delete if disinfection fails**. Khi phát hiện một đối tượng bị nhiễm mã độc trong một thư được gửi đến hoặc thư được gửi đi, ứng dụng 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, ứng dụng sẽ xóa đối tượng bị nhiễm. Ứng dụng sẽ thêm thông tin về hành động được thực hiện vào chủ đề thư, ví dụ: *[Thư đã được xử lý] <chủ đề thư>*.

   - **Disinfect, block if disinfection fails**. Khi phát hiện một đối tượng bị nhiễm mã độc trong một thư được gửi đến, ứng dụng 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, ứng dụng sẽ thêm cảnh báo vào chủ đề thư điện tử. 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, ứng dụng sẽ cố gắng khử mã độc đối tượng được phát hiện. Nếu không thể khử mã độc đối tượng, ứng dụng sẽ chặn việc gửi thư và ứng dụng thư điện tử sẽ hiển thị lỗi.

   - **Block**. Nếu phát hiện một đối tượng bị nhiễm mã độc trong thư được gửi đến, ứng dụng sẽ thêm cảnh báo vào 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, ứng dụng sẽ chặn gửi thư và ứng dụng thư điện tử sẽ hiển thị lỗi.

7. Nếu cần, hãy chỉnh sửa thiết lập nâng cao của Bảo vệ mối đe dọa thư điện tử.

8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật hoặc tắt thành phần Bảo vệ mối đe dọa thư điện tử 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 thư điện tử**.

3. Sử dụng nút bật/tắt **Bảo vệ mối đe dọa thư điện tử** 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 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.

     - **Khuyên dùng**. Mức độ bảo mật email mang đến sự cân bằng tối ưu giữa hiệu năng của ứng dụng 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 (xem bảng bên dưới).

     Bạn có thể khôi phục các giá trị của các mức bảo mật cài đặt sẵn bằng cách nhấn vào nút **Khôi phục cấp bảo mật được khuyến nghị**.

5. Trong mục **Hành động khi phát hiện mối đe dọa**, chọn hành động được Kaspersky Endpoint Security thực hiện đối với các đối tượng độc hại:

   - **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, ứng dụng 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, ứng dụng sẽ xóa đối tượng bị nhiễm. Ứng dụng sẽ thêm thông tin về hành động được thực hiện vào chủ đề thư, ví dụ: *[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, ứng dụng 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, ứng dụng sẽ thêm cảnh báo vào chủ đề thư điện tử. 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, ứng dụng sẽ cố gắng khử mã độc đối tượng được phát hiện. Nếu không thể khử mã độc đối tượng, ứng dụng 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, ứng dụng sẽ thêm cảnh báo vào 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, ứng dụng sẽ chặn gửi thư và ứng dụng thư điện tử sẽ hiển thị lỗi.

6. 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**	*Phạm vi bảo vệ* 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 thứcPOP3, 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 Cached Exchange Mode. 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. Ứng dụng 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 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. Ứng dụng sẽ quét các tập tin định dạng văn phòng nhỏ hơn 1 MB, bất kể hộp kiểm này có được chọn hay không.
Bộ 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: tattachment.doc_). 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 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.
Hành động khi phát hiện mối đe dọa	**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, ứng dụng 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, ứng dụng sẽ xóa đối tượng bị nhiễm. Ứng dụng sẽ thêm thông tin về hành động được thực hiện vào chủ đề thư, ví dụ: *[Thư đã được xử lý] <chủ đề thư>*.

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, ứng dụng 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, ứng dụng sẽ xóa đối tượng bị nhiễm. Ứng dụng sẽ thêm thông tin về hành động được thực hiện vào chủ đề thư, ví dụ: *[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, ứng dụng 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, ứng dụng sẽ thêm cảnh báo vào chủ đề thư điện tử. 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, ứng dụng sẽ cố gắng khử mã độc đối tượng được phát hiện. Nếu không thể khử mã độc đối tượng, ứng dụng 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, ứng dụng sẽ thêm cảnh báo vào 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, ứng dụng 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 mối 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 mối đe dọa thư điện tử bao gồm các thiết lập để tích hợp thành phần Bảo vệ mối 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 mối 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 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. 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 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 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 hỗn 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. Ứng dụng sẽ quét các tập tin định dạng văn phòng nhỏ hơn 1 MB, bất kể hộp kiểm này có được chọn hay không.

   - **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. Ứng dụng 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).

     Nếu trong quá trình quét, ứng dụng 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. Các tập tin có tiền tố PR.

   - **Không quét tập tin nén lớn hơn N MB (từ 1 đến 9999)**. Nếu hộp kiểm này được chọn, thành phần Bảo vệ mối đe dọa thư điện tử sẽ loại trừ các tập nén 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 nén đính kèm email thuộc mọi kích cỡ.

   - **Giới hạn thời gian kiểm tra các tập tin nén thành N giây (từ 1 đến 9999)**. Nếu hộp kiểm này được chọn, thời gian phân bổ cho việc quét các tập nén 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 bộ 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 **Bộ 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: tattachment.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)

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Communication & Web Protection** → **Mail Threat Protection**.
5. Để xuất danh sách các phần mở rộng trong mục **Attachment filter**:
   a. Chọn các phần mở rộng mà bạn muốn xuất.
   b. Nhấn vào liên kết **Export**.
   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 **Attachment filter**:
   a. Nhấn vào liên kết **Import**.
   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.

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa thư điện tử**.
4. Trong mục **Mức độ bảo mật**, hãy nhấn nút **Thiết lập**.
5. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy chọn thẻ **Bộ lọc tập tin đính kèm**.
6. 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 vào 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.

7. Để nhập danh sách các phần mở rộng:

a. Nhấn vào 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.

8. 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). Phần mở rộng cho phép quét thư ở cấp độ ứng dụng thư điện tử thay vì cấp độ giao thức. Ngoài thư, phần mở rộng cho phép bạn quét các đối tượng nhận được qua giao diện MAPI từ kho lưu trữ Microsoft Exchange (ví dụ: các đối tượng trong Lịch). Quá trình quét này diễn ra trong ứng dụng thư điện tử.

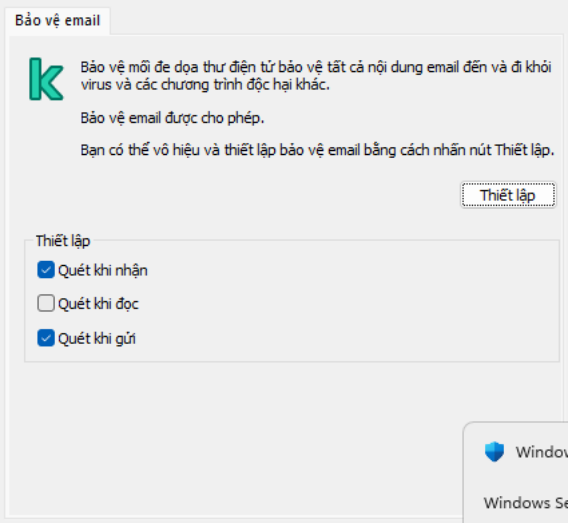
Bạn có thể mở thiết lập thành phần Bảo vệ mối đe dọa thư điện tử từ trong Outlook, và quy định khi nào thì email được quét để phát hiện virus và các mối đe dọa khác.

Phần mở rộng Mail Threat Protection hỗ trợ các phiên bản 32 bit và 64 bit của Outlook 2010, 2013, 2016, 2019, 2021, 2024 và 365.

Trên máy tính có kiến trúc Arm, phần mở rộng Mail Threat Protection hỗ trợ các phiên bản 32 bit và 64 bit của Outlook 2016, Outlook 2021, Outlook 2024 và Outlook 365 dành cho Arm64.

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 (xem hình bên dưới).



Cấu hình thành phần Bảo vệ mối đe dọa thư điện tử trong Outlook

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.

Khi quét email bằng Phần mở rộng Bảo vệ mối đe dọa thư điện tử cho Outlook, bạn nên sử dụng Chế độ bộ nhớ đệm máy chủ Exchange (Use Cached Exchange Mode). 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.

Cách cấu hình chế độ hoạt động của phần mở rộng Bảo vệ mối đe dọa thư điện tử cho Outlook trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Bảo vệ mối đe dọa thư điện tử**.
5. Trong mục **Mức độ bảo mật**, hãy nhấn nút **Thiết lập**.
6. Trong cửa sổ mở ra, trong mục **Khả năng kết nối**, hãy chọn hộp kiểm **Kết nối phần mở rộng Microsoft Outlook**.
7. Nhấn vào **Thiết lập**.

8. Trong cửa sổ **Bảo vệ email**, hãy thực hiện một trong các thao tác sau:

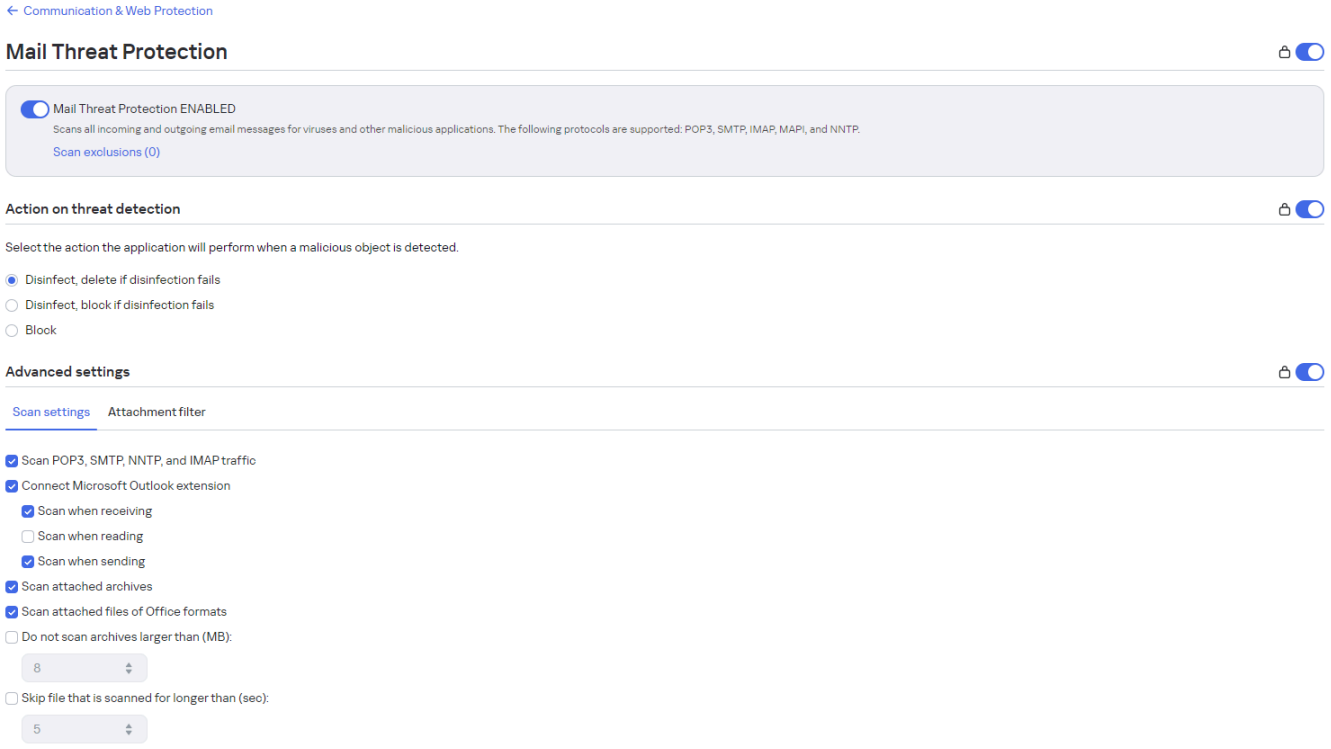
   - Chọn hộp kiểm **Quét khi nhận** nếu bạn muốn tiện ích mở rộng Bảo vệ mối đe dọa thư điện tử cho Outlook quét các email đến khi chúng vào hộp thư.
   - Chọn hộp kiểm **Quét khi đọc** nếu bạn muốn tiện ích mở rộng Bảo vệ mối đe dọa thư điện tử cho Outlook quét các email đến khi người sử dụng đọc chúng.
   - 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. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách cấu hình chế độ hoạt động của phần mở rộng Bảo vệ mối đe dọa thư điện tử cho Outlook trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.
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 **Communication & Web Protection** → **Mail Threat Protection**.



Thiết lập Bảo vệ mối đe dọa thư điện tử

5. Trong mục **Advanced settings**, hãy chọn thẻ **Scan settings**.
6. Chọn hộp kiểm **Connect Microsoft Outlook extension**.

7. Cấu hình chế độ của phần mở rộng:

   - Chọn hộp kiểm **Scan when receiving** 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 **Scan when reading** 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 **Scan when sending** 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.

8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Quét email trong Thunderbird, MyOffice, R7-Office

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. Đối với các trình quản lý thư Mozilla Thunderbird, MyOffice Mail và R7-Office Organizer, ứng dụng chỉ có quyền truy cập thư ở *cấp độ giao thức* (POP3, SMTP, IMAP, NNTP).

Để quét lưu lượng truy cập trong ứng dụng thư Mozilla Thunderbird, MyOffice Mail và R7-Office Organizer, bạn cần phải thêm chứng chỉ Kaspersky vào kho chứng chỉ và chọn kho chứng chỉ riêng.

Thành phần Bảo vệ mối đe dọa thư điện tử không quét thư nếu ứng dụng thư khách được mở trong trình duyệt.

Bảo vệ mối đe dọa qua thư điện tử theo thời gian thực

Bảo vệ mối đe dọa thư điện tử có thể quét cả thư đến và thư đi. 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. Khi phát hiện tập tin độc hại trong phần đính kèm, Kaspersky Endpoint Security sẽ thêm thông tin về hành động đã thực hiện vào chủ đề thư, ví dụ: *[Thư đã được xử lý] <chủ đề thư>*.

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.

Quét phần mềm độc hại trong cơ sở dữ liệu thư điện tử

Chức năng Bảo vệ mối đe dọa qua thư điện tử sẽ ngăn sự lây nhiễm vào máy tính ở cấp độ giao thức, nhưng nếu máy tính đã bị nhiễm trước khi cài đặt Kaspersky Endpoint Security, ứng dụng có thể phát hiện mối đe dọa trong cơ sở dữ liệu thư điện tử bằng tác vụ *Quét phần mềm độc hại*. Ứng dụng này không khử mã độc hoặc xóa các tập tin bị nhiễm virus trong cơ sở dữ liệu thư điện tử, bất kể thiết lập tác vụ nào. Điều này là do Kaspersky Endpoint Security không phân tích thư từ Thunderbird, MyOffice và P7-Office thành các thành phần (tiêu đề, nội dung, tệp đính kèm) giống như thư từ Microsoft Office Outlook. Ứng dụng chỉ thêm thông tin về các đối tượng bị nhiễm mã độc được phát hiện vào danh sách các mối đe dọa hiện hoạt.

Để loại bỏ các mối đe dọa hiện hữu:

1. Tìm và xóa tin nhắn chứa đối tượng đã được phát hiện trong giao diện của ứng dụng email.

   Ứng dụng hiển thị thông tin về các đối tượng được phát hiện vào danh sách các mối đe dọa hiện hoạt.

   Ví dụ về thẻ đối tượng được phát hiện:

   HEUR:Trojan.PDF.Phish.gen
   Đối tượng: `C:\Users\admin\AppData\Roaming\Thunderbird\Profiles\ov56jpz0.default-release\Mail\mail.company.ru\Inbox// [From USER NAME <company@mail.com>][Date 25 Sep 2025 20:05:36] [Subj Mail title X] Object.pdf`

2. Thực hiện thao tác nén cơ sở dữ liệu.

   Khi một tin nhắn bị xóa trong giao diện người dùng, trình soạn thảo thư chỉ thêm dấu hiệu xóa. Ứng dụng email chỉ thực sự xóa tin nhắn sau khi quá trình nén cơ sở dữ liệu hoàn tất. Để biết thêm chi tiết về việc nén cơ sở dữ liệu, hãy xem phần trợ giúp của trình quản lý email của bạn (ví dụ: Mozilla Thunderbird).

3. Chạy lại tác vụ *Quét phần mềm độc hại* và đảm bảo mối đe dọa không còn nữa.

Nếu việc xóa thư chứa tập tin bị nhiễm mã độc hiện không khả dụng vì bất kỳ lý do gì, bạn có thể xử lý các mối đe dọa đó trong giao diện người dùng của Kaspersky Endpoint Security. Đối với các tập tin trong ứng dụng email, bạn có hai lựa chọn để xử lý mối đe dọa: **Bỏ qua** và **Thêm vào loại trừ**. Để ngăn ứng dụng thêm các đối tượng này vào danh sách mối đe dọa hiện hoạt trong quá trình quét lại, hãy thêm chúng vào danh sách loại trừ khỏi quá trình quét.

Bảo vệ mối đe dọa mạng

Thành phần *Bảo vệ mối đe dọa mạng* (còn được gọi là Intrusion Detection System, IDS) sẽ giám sát lưu lượng truy cập mạng đến để biết hoạt động đặc trưng của các cuộc tấn công mạng. Khi ứng dụng 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 ứng dụng. 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.

Bật và tắt Bảo vệ mối đe dọa mạng

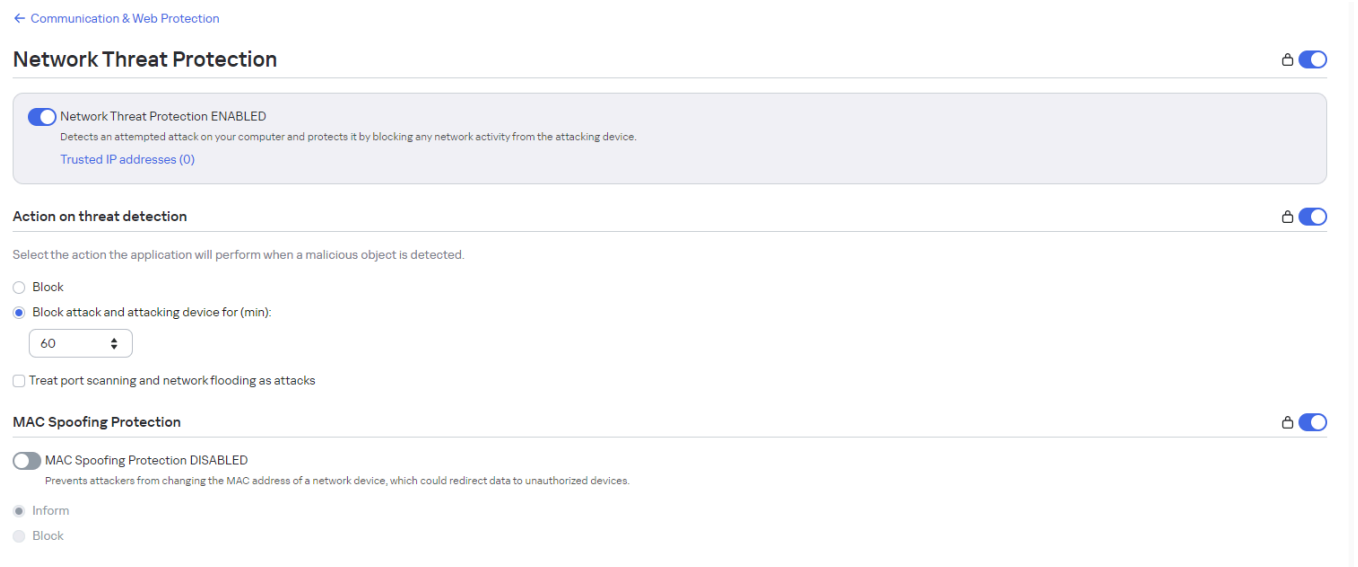
Theo mặc định, Bảo vệ mối đe dọa mạng sẽ được bật và hoạt động trong chế độ tối ưu. Kaspersky Endpoint Security sẽ giám sát lưu lượng truy cập mạng đến để biết hoạt động đặc trưng của các cuộc tấn công mạng và chặn các cuộc tấn công.

Cách bật hoặc tắt Bảo vệ mối đe dọa mạng trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa mạng**.
4. Sử dụng hộp kiểm **Bảo vệ mối đe dọa mạng** để bật hoặc tắt thành phần.
5. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật hoặc tắt Bảo vệ mối đe dọa mạng trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Communication & Web Protection** → **Network Threat Protection**.

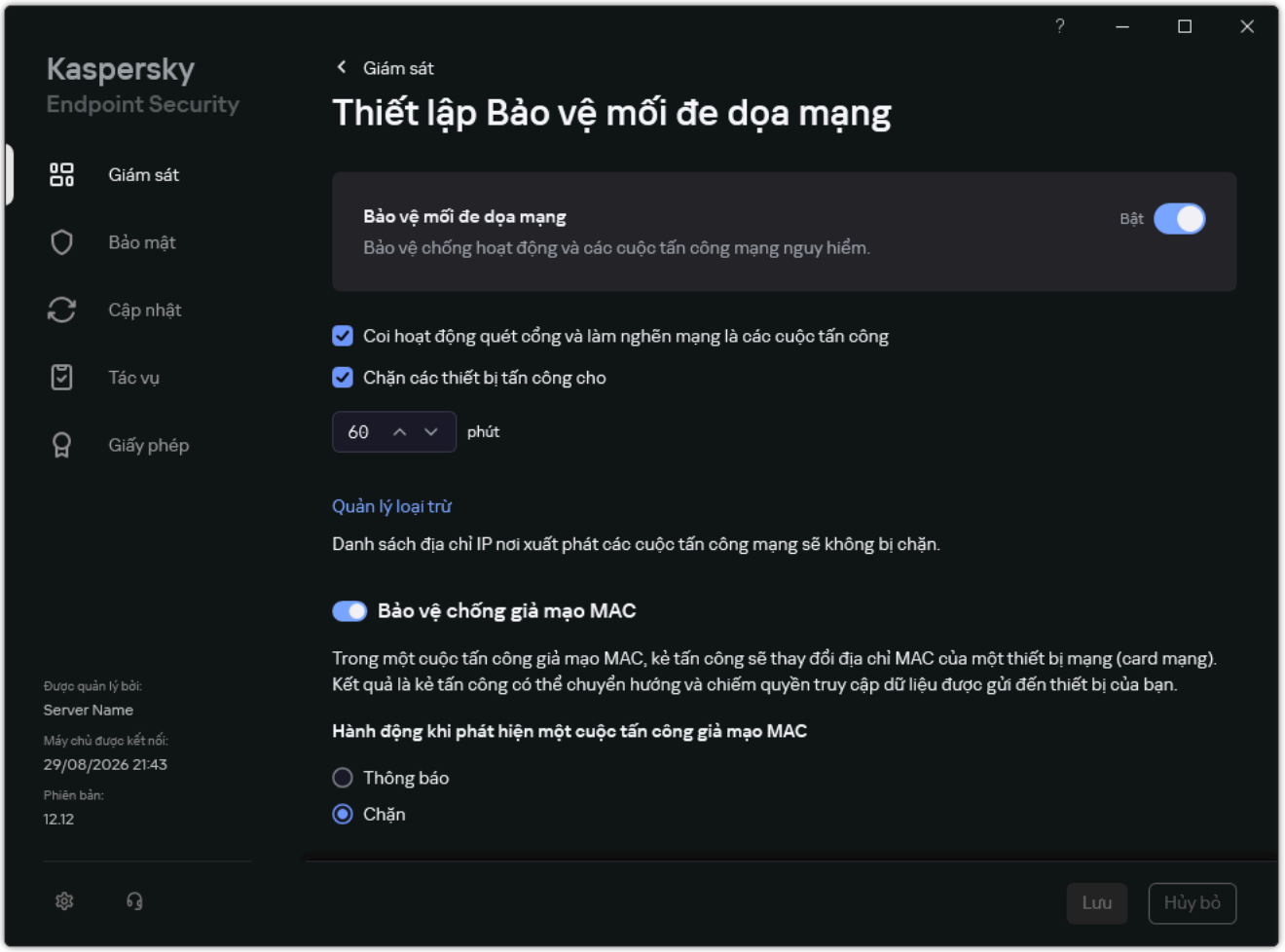


Thiết lập Bảo vệ mối đe dọa mạng

5. Sử dụng nút bật/tắt **Network Threat Protection ENABLED** để bật hoặc tắt thành phần này.
6. Lưu các thay đổi của bạn.

Cách bật hoặc tắt Bảo vệ mối đe dọa mạng 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 mạng**.



Thiết lập Bảo vệ mối đe dọa mạng

3. Sử dụng nút bật/tắt **Bảo vệ mối đe dọa mạng** để bật hoặc tắt thành phần này.
4. Lưu các thay đổi của bạn.

Chặn máy tính tấn công

Nếu thành phần Bảo vệ mối đe dọa mạng được bật, Kaspersky Endpoint Security sẽ tự động chặn các mối đe dọa mạng. Ngoài ra, ứng dụng có thể chặn máy tính tấn công và hạn chế gửi các gói tin mạng trong một khoảng thời gian nhất định. Theo mặc định, Kaspersky Endpoint Security sẽ chặn máy tính trong một giờ.

Cách chặn máy tính tấn công trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Bảo vệ mối đe dọa mạng**.

4. Trong mục **Thiết lập Bảo vệ mối đe dọa mạng**, hãy chọn hộp kiểm **Chặn các thiết bị tấn công cho N phút**.

   Nếu tùy chọn này được bật, thành phần Bảo vệ mối đe dọa mạng sẽ thêm máy tính tấn công vào danh sách chặn. Điều này có nghĩa là thành phần Bảo vệ mối 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 999 phút.

5. Đặt thời lượng chặn khác cho một máy tính tấn công trong trường ở bên phải của hộp kiểm **Chặn các thiết bị tấn công cho N phút**.

6. Lưu các thay đổi của bạn.

Cách chặn máy tính tấn công trong Bảng điều khiển web

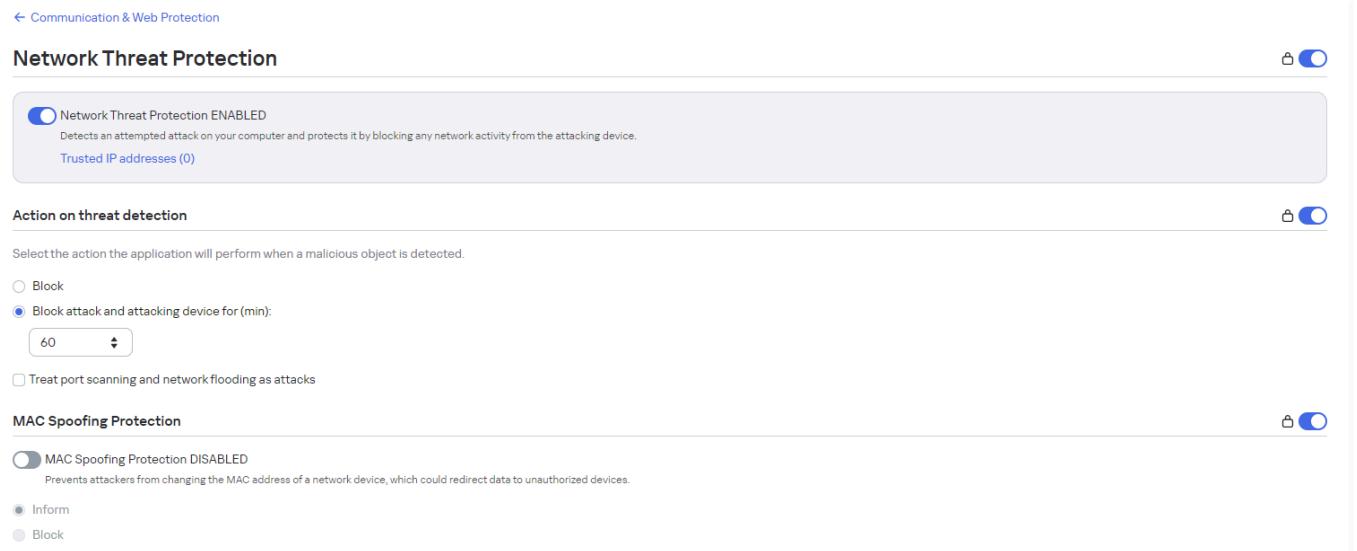
1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.

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 **Communication & Web Protection** → **Network Threat Protection**.



Thiết lập Bảo vệ mối đe dọa mạng

5. Trong mục **Action on threat detection**, hãy chọn hộp kiểm **Block attack and attacking device for (min)**.

   Nếu tùy chọn này được bật, thành phần Bảo vệ mối đe dọa mạng sẽ thêm máy tính tấn công vào danh sách chặn. Điều này có nghĩa là thành phần Bảo vệ mối 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 999 phút.

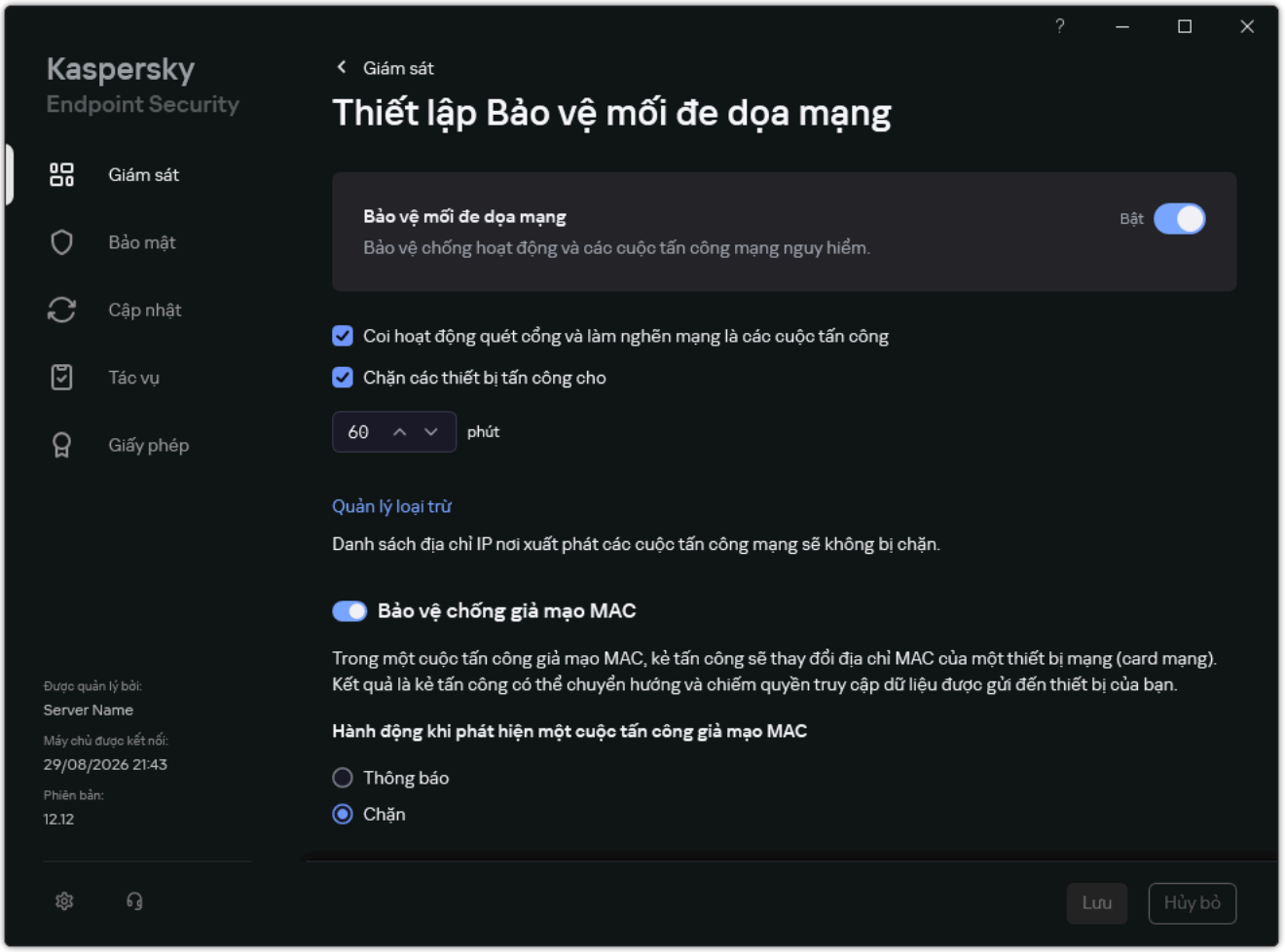
6. Thay đổi thời gian chặn của máy tính tấn công.

7. Lưu các thay đổi của bạn.

Cách chặn máy tính tấn công trong giao diện người dùng của 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 mạng**.



Thiết lập Bảo vệ mối đe dọa mạng

3. Bật nút bật/tắt **Chặn các thiết bị tấn công cho N phút**.

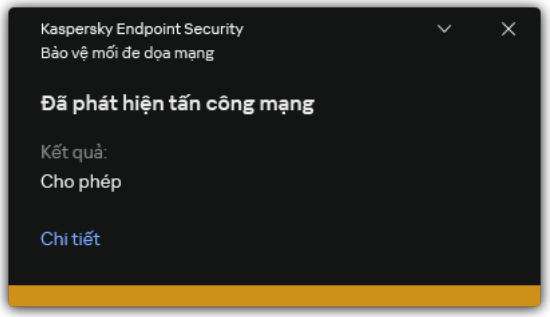
   Nếu tùy chọn này được bật, thành phần Bảo vệ mối đe dọa mạng sẽ thêm máy tính tấn công vào danh sách chặn. Điều này có nghĩa là thành phần Bảo vệ mối đe dọa mạng sẽ chặn kết nối mạng từ máy tính tấn công sau nỗ lực tấn công mạng đầu tiên trong một khoảng thời gian được quy định. Lệnh chặn này sẽ tự động 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 999 phút.

4. Đặt thời lượng chặn khác cho một máy tính tấn công trong trường ở bên dưới nút bật/tắt **Chặn các thiết bị tấn công cho N phút**.

5. 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. Kaspersky Endpoint Security sẽ tạo sự kiện *Network attack detected*. Sự kiện chứa thông tin về máy tính tấn công: địa chỉ IP và MAC.

Bạn có thể xem địa chỉ MAC của máy tính tấn công trong giao diện người dùng của ứng dụng hoặc trong bảng điều khiển Kaspersky Security Center phiên bản 15.1 trở lên.



Thông báo phát hiện tấn công mạng

Kaspersky Endpoint Security sẽ mở khóa máy tính khi hết thời gian quy định. Bảng điều khiển Kaspersky Security Center không cung cấp các công cụ để giám sát máy tính bị chặn ngoài các sự kiện *Network attack detected* trong báo cáo. Bạn chỉ có thể xem danh sách máy tính bị chặn trong giao diện của ứng dụng. Chức năng này được cung cấp bởi công cụ *Giám sát mạng*. Bạn cũng có thể sử dụng công cụ Giám sát mạng để bỏ chặn máy tính.

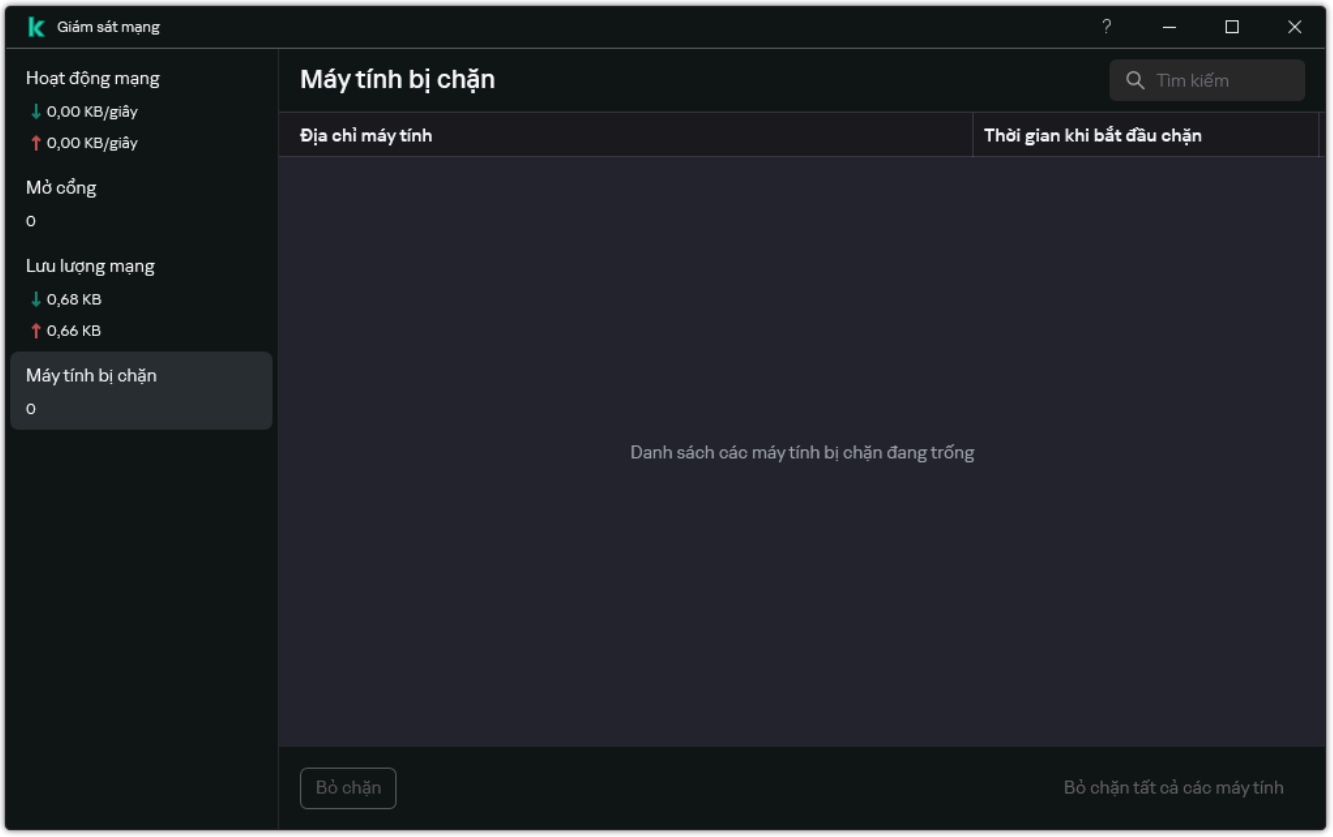
Để bỏ chặn máy tính:

1. Trong cửa sổ chính của ứng dụng, trong mục **Giám sát**, hãy nhấn vào ô **Giám sát mạng**.
2. Vào thẻ **Máy tính bị chặn**.

   Thao tác này sẽ mở danh sách máy tính bị chặn (xem hình bên dưới).

   Kaspersky Endpoint Security sẽ xóa danh sách chặn khi ứng dụng được khởi chạy lại và khi thiết lập Bảo vệ mối đe dọa mạng bị thay đổi.

3. Chọn máy tính mà bạn muốn bỏ chặn và nhấn vào **Bỏ chặn**.



Danh sách các máy tính bị chặn

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. Bạn cũng có thể chọn giao thức và cổng được sử dụng để giao tiếp và cho phép các hoạt động mạng cụ thể.

Cách cấu hình địa chỉ loại trừ khỏi chặn trong Bảng điều khiển quản trị (MMC)

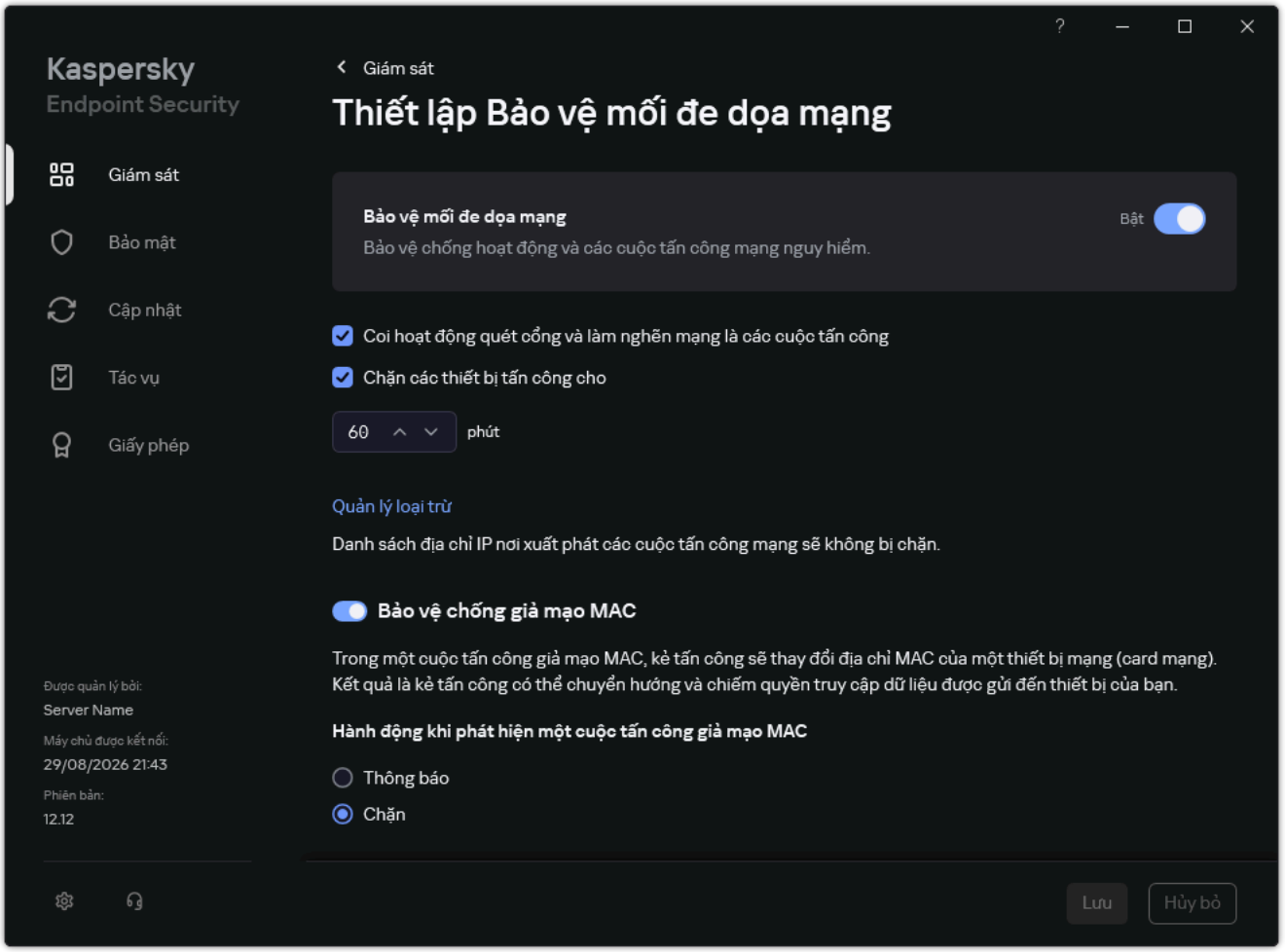
1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Bảo vệ mối đe dọa mạng**.
5. Trong mục **Thiết lập Bảo vệ mối đe dọa mạng**, hãy nhấn nút **Loại trừ**.
6. Trong cửa sổ mở ra, hãy nhấn nút **Thêm**.
7. Nhập vào địa chỉ IP của máy tính mà các cuộc tấn công mạng xuất phát từ đó sẽ không bị chặn. Nếu cần, hãy chọn giao thức và cổng mà dữ liệu được truyền qua.
8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách cấu hình địa chỉ được loại trừ khỏi danh sách chặn trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.
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 **Trusted Zone**.
5. Trong cửa sổ mở ra, hãy nhấn vào liên kết **IP addresses**.
   Thao tác này sẽ mở cửa sổ chứa danh sách các địa chỉ IP được tin tưởng.
6. Trong cửa sổ mở ra, hãy nhấn nút **Add**.
7. Nhập vào địa chỉ IP của máy tính mà các cuộc tấn công mạng xuất phát từ đó sẽ không bị chặn.
   Nếu cần, hãy chỉ định mạng con.
8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách cấu hình địa chỉ loại trừ khỏi chặn trong giao diện người dùng của 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 mạng**.



Thiết lập Bảo vệ mối đe dọa mạng

3. Nhấn vào liên kết **Quản lý loại trừ**.

4. Trong cửa sổ mở ra, hãy nhấn 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.
   Nếu cần, hãy chọn giao thức và cổng mà dữ liệu được truyền qua.

6. Lưu các thay đổi của bạn.

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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Bảo vệ mối đe dọa mạng**.

4. Trong mục **Thiết lập Bảo vệ mối đe dọa mạng**, hãy nhấn nút **Loại trừ**.

5. 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 nút → **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.

6. Để nhập danh sách loại trừ:

   a. Nhấn nút → **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.

Cách xuất và nhập danh sách loại trừ trong Bảng điều khiển web của Kaspersky Security Center

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Communication & Web Protection** → **Network Threat Protection**.
5. Ở phần bên phải của cửa sổ, hãy nhấn vào liên kết **Trusted IP addresses**.
   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 nút → **Export**.
      Kaspersky Endpoint Security sẽ xuất danh sách các loại trừ vào tập tin JSON trong thư mục tải xuống mặc định.
7. Để nhập danh sách loại trừ:
   a. Nhấn nút → **Import**.
      Trong cửa sổ mở ra, hãy chọn tập tin JSON mà bạn muốn nhập danh sách các loại trừ.
   b. 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 JSON.
8. Lưu các thay đổi của bạn.

Cấu hình Bảo vệ mối đe dọa 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.

Bạn không thể cấu hình các ngoại lệ riêng biệt cho các loại tấn công này. Điều này có nghĩa là ngay cả khi địa chỉ IP riêng lẻ được thêm vào khu vực tin tưởng, Kaspersky Endpoint Security sẽ vẫn chặn máy tính tấn công nếu phát hiện thấy cuộc tấn công đó. Bạn có thể bật hoặc tắt tính năng phát hiện các cuộc tấn công đó.

Chúng tôi không khuyến nghị bật tính năng bảo vệ chống giả mạo MAC trên các máy ảo trong cơ sở hạ tầng Microsoft Hyper-V. Do đặc thù của nền tảng Microsoft Hyper-V, Kaspersky Industrial CyberSecurity for Nodes có thể chặn trình quản lý ảo do đưa ra kết quả phát hiện nhầm.

Cách cấu hình Bảo vệ mối đe dọa mạng theo loại trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu** → **Bảo vệ mối đe dọa mạng**.
4. Sử dụng hộp kiểm **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.

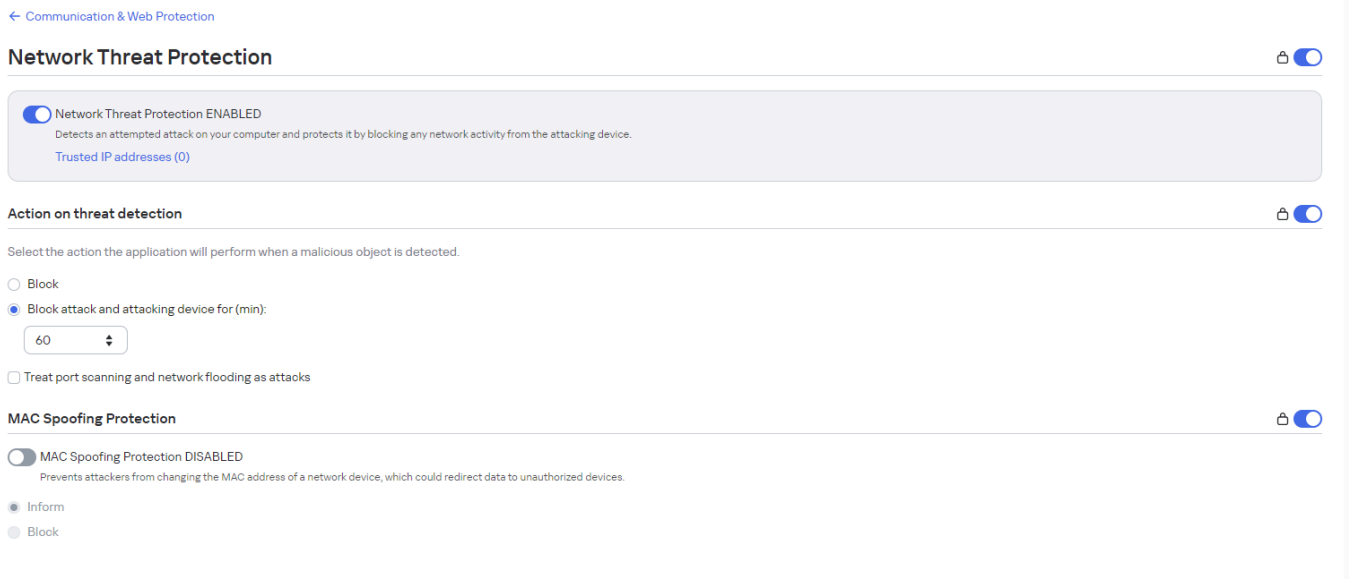
   Nếu chức năng này được bật, Kaspersky Endpoint Security sẽ giám sát lưu lượng mạng để phát hiện hành vi quét cổng và làm tràn mạng. Nếu phát hiện hành vi như vậy, ứng dụng sẽ thông báo cho người dùng và gửi sự kiện tương ứng đến Kaspersky Security Center. Ứng dụng cung cấp thông tin về máy tính đang thực hiện các yêu cầu. Đây là thông tin cần thiết để có phản hồi kịp thời. Tuy nhiên, Kaspersky Endpoint Security không chặn máy tính đang thực hiện yêu cầu vì lưu lượng truy cập như vậy có thể là điều bình thường trên mạng công ty.
5. Trong mục **Chế độ bảo vệ chống mạo danh MAC**, hãy chọn một trong các tùy chọn sau:
   - **Không theo dõi hoạt động mạo danh MAC**.
   - **Thông báo**.
   - **Chặn**.
6. Lưu các thay đổi của bạn.

Cách cấu hình Bảo vệ mối đe dọa mạng theo loại trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Communication & Web Protection** → **Network Threat Protection**.



Thiết lập Bảo vệ mối đe dọa mạng

5. Sử dụng hộp kiểm **Treat port scanning and network flooding as attacks** để bật hoặc tắt tính năng phát hiện các cuộc tấn công này.

   Nếu chức năng này được bật, Kaspersky Endpoint Security sẽ giám sát lưu lượng mạng để phát hiện hành vi quét cổng và làm tràn mạng. Nếu phát hiện hành vi như vậy, ứng dụng sẽ thông báo cho người dùng và gửi sự kiện tương ứng đến Kaspersky Security Center. Ứng dụng cung cấp thông tin về máy tính đang thực hiện các yêu cầu. Đây là thông tin cần thiết để có phản hồi kịp thời. Tuy nhiên, Kaspersky Endpoint Security không chặn máy tính đang thực hiện yêu cầu vì lưu lượng truy cập như vậy có thể là điều bình thường trên mạng công ty.

6. Trong mục **MAC Spoofing Protection**, hãy cấu hình tính năng phát hiện các cuộc tấn công giả mạo địa MAC:

   a. Sử dụng nút bật/tắt **MAC Spoofing Protection ENABLED** để bật hoặc tắt tính năng phát hiện các cuộc tấn công này.

   b. Chọn hành động cần thực hiện khi phát hiện tấn công giả mạo địa MAC:

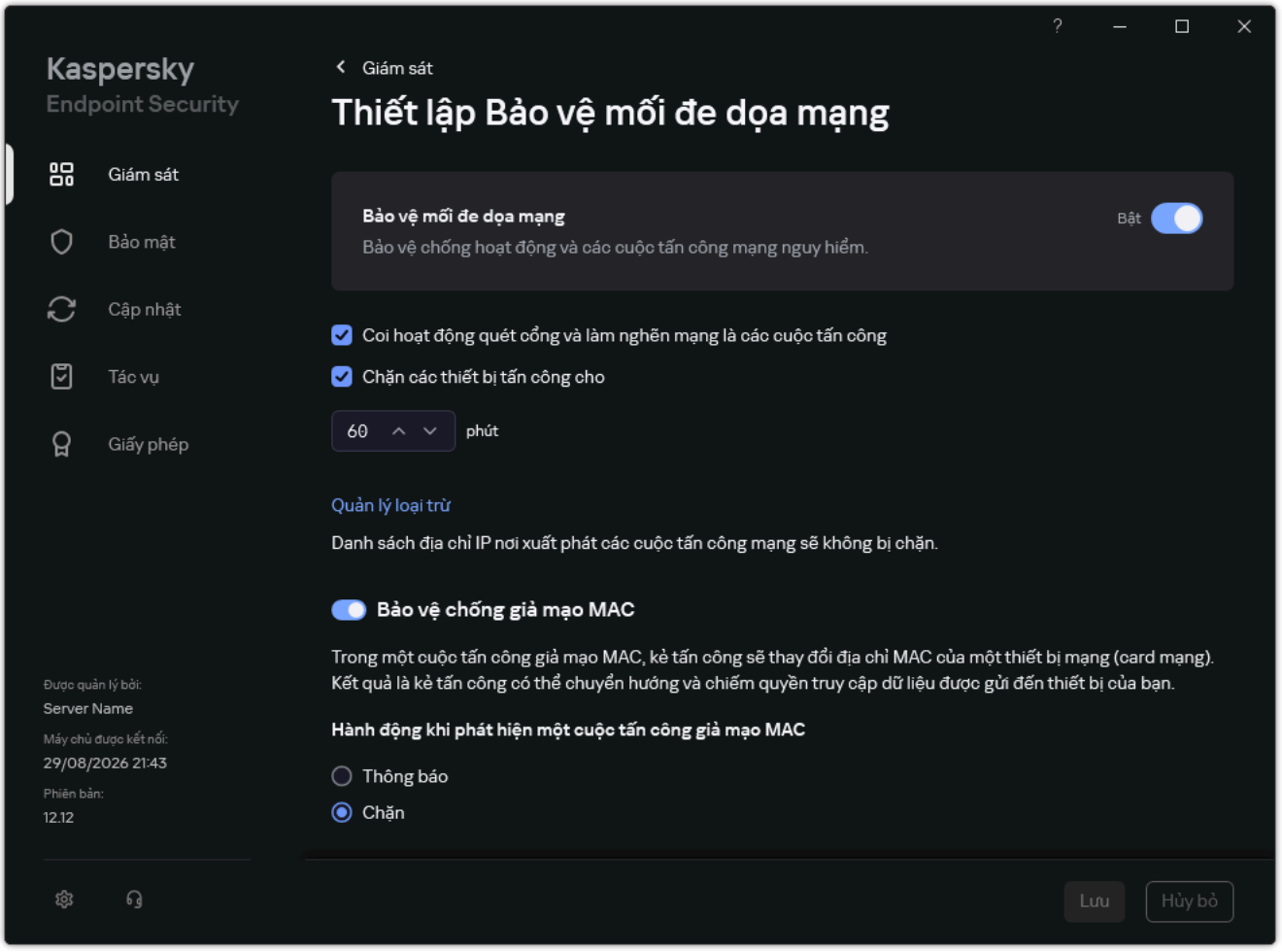
   - **Inform**.
   - **Block**.

7. Lưu các thay đổi của bạn.

Cách cấu hình Bảo vệ mối đe dọa mạng theo loại 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 mạng**.



Thiết lập Bảo vệ mối 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.

   Nếu chức năng này được bật, Kaspersky Endpoint Security sẽ giám sát lưu lượng mạng để phát hiện hành vi quét cổng và làm tràn mạng. Nếu phát hiện hành vi như vậy, ứng dụng sẽ thông báo cho người dùng và gửi sự kiện tương ứng đến Kaspersky Security Center. Ứng dụng cung cấp thông tin về máy tính đang thực hiện các yêu cầu. Đây là thông tin cần thiết để có phản hồi kịp thời. Tuy nhiên, Kaspersky Endpoint Security không chặn máy tính đang thực hiện yêu cầu vì lưu lượng truy cập như vậy có thể là điều bình thường trên mạng công ty.

4. Sử dụng nút bật/tắt **Bảo vệ chống giả mạo MAC** để bật hoặc tắt tính năng phát hiện các cuộc tấn công này.

5. Trong mục **Hành động khi phát hiện một cuộc tấn công giả mạo MAC**, hãy chọn một trong các tùy chọn sau:

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

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

Các kiểu kết nối mạng

Tường lửa cho phép bạn kiểm soát hoạt động mạng tùy thuộc vào kiểu của kết nối mạng. Kaspersky Endpoint Security sẽ nhận kiểu kết nối mạng từ hệ điều hành của máy tính. Kiểu của kết nối mạng trong hệ điều hành được người dùng đặt khi thiết lập kết nối. Bạn có thể thay đổi kiểu của kết nối mạng trong mục thiết lập của Kaspersky Endpoint Security. Tường lửa sẽ giám sát hoạt động mạng tùy thuộc vào kiểu mạng được chỉ định trong mục thiết lập của Kaspersky Endpoint Security chứ không phải trong hệ điều hành.

Có các kiểu kết nối mạng sau đây:

- **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 kiểu *Mạng công cộng* cho Internet theo mặc định. Bạn không thể thay đổi kiểu 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.

Khả năng tương thích với Windows Defender Firewall

Hệ điều hành có tường lửa tích hợp sẵn, đó là *Windows Defender Firewall*. Ứng dụng hoạt động khác nhau tùy thuộc vào loại hệ điều hành:

- **Máy trạm**. Sử dụng Kaspersky Firewall song song với Windows Defender Firewall có thể khiến hệ điều hành hoạt động không ổn định. Do đó, Kaspersky Endpoint Security có một cơ chế ngăn sử dụng đồng thời cả hai tường lửa. Khi bạn bật Kaspersky Firewall, hệ điều hành sẽ tự động tắt Windows Defender Firewall. Khi bạn tắt Kaspersky Firewall, hệ điều hành sẽ tự động bật lại Windows Defender Firewall để tiếp tục bảo vệ máy tính.

- **Máy chủ**. Kaspersky Firewall và Windows Defender Firewall không tương thích với nhau. Bộ cài đặt Kaspersky Endpoint Security sẽ tự động gỡ bỏ Windows Defender Firewall khi cài đặt ứng dụng.

Bật hoặc tắt Tường lửa

Theo mặc định, Tường lửa sẽ được bật và hoạt động trong chế độ tối ưu.

Cách bật hoặc tắt Tường lửa trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Tường lửa**.
4. Sử dụng hộp kiểm **Tường lửa** để bật hoặc tắt thành phần.
5. Lưu các thay đổi của bạn.

Cách bật hoặc tắt Tường lửa trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Policies**.
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 **Communication & Web Protection → Firewall**.
5. Sử dụng nút bật/tắt **Firewall ENABLED** để bật hoặc tắt thành phần này.
6. Lưu các thay đổi của bạn.

Cách bật hoặc tắt Tường lửa 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. Sử dụng nút bật/tắt **Tường lửa** để bật hoặc tắt thành phần này.
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 (còn được gọi là Intrusion Detection System, IDS) sẽ giám sát lưu lượng truy cập mạng đến để biết hoạt động đặc trưng của 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 kiểu kết nối mạng

Tường lửa sẽ gán kiểu *Mạng công cộng* cho Internet theo mặc định. Bạn không thể thay đổi kiểu của Internet.

Để thay đổi kiểu 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 kiểu.

5. Trong cột **Loại mạng**, hãy chọn kiểu 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

Tường lửa lọc mọi hoạt động mạng trên máy tính theo các quy tắc gói tin mạng. Quy tắc gói tin mạng chứa các điều kiện (ví dụ: hướng, giao thức) mà Tường lửa áp dụng để kiểm soát các kết nối mạng của máy tính. Các quy tắc gói tin mạng cũng chỉ định hành động mà Tường lửa thực hiện với kết nối phù hợp với quy tắc (cho phép hoặc chặn kết nối).

Các khuyến nghị để tạo quy tắc gói tin mạng

Bạn có thể chỉ định một địa chỉ IP hoặc một dải địa chỉ IP để lọc hoạt động mạng. Bạn cũng có thể chỉ định tên DNS.

Nếu tên DNS được sử dụng trong một quy tắc, Kaspersky Endpoint Security sẽ phân giải tên DNS này thành địa chỉ IP, sau đó xử lý quy tắc đó như thể địa chỉ IP này đã được chỉ định trong quy tắc.

Kaspersky Endpoint Security có thể phân giải tên DNS trong các trường hợp sau:

- Khởi động ứng dụng
- Thay đổi thiết lập Tường lửa

Khi ứng dụng đang phân giải tên miền DNS từ máy tính đã cài đặt ứng dụng, một lượng lớn truy vấn có thể được thực hiện đến máy chủ DNS. Để tránh tình trạng này, bạn nên sử dụng địa chỉ IP thay vì tên DNS khi tạo quy tắc.

Trong một số trường hợp, sử dụng tên DNS trong tên gói tin mạng có thể không an toàn vì chủ sở hữu máy chủ DNS có thể sửa đổi các tham số của bản ghi DNS. Kẻ tấn công với ý đồ xấu cũng có thể giả mạo tin nhắn DNS và vượt qua các quy tắc của Tường lửa.

Bạn có thể kiểm soát các kết nối mạng bằng tên DNS bằng cách sử dụng quy tắc của Kiểm soát web. Nếu bạn cần chỉ định tên DNS trong quy tắc Tường lửa:

- Đảm bảo tính bảo mật của mạng LAN doanh nghiệp.
- Đảm bảo tính bảo mật của bộ nhớ đệm và máy chủ DNS có thẩm quyền.
- Bật tính năng bảo vệ bản ghi DNS khỏi bị sửa đổi.

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

Phương thức tạo 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.

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 vào ô **Giám sát mạng**.
2. Vào 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 sẵn 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. Sử dụng danh sách thả xuống **Thêm**, chọn vị trí của quy tắc trong danh sách: ở đầu danh sách, ở cuối danh sách hoặc bên cạnh quy tắc đã chọn.

   Vị trí của quy tắc trong danh sách sẽ quyết định mức độ ưu tiên của quy tắc. Quy tắc ở đầu danh sách có mức độ ưu tiên cao nhất.

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 sẵn 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Tường lửa**.

4. 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.

5. Vào 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.

6. Sử dụng danh sách thả xuống **Thêm**, chọn vị trí của quy tắc trong danh sách: ở đầu danh sách, ở cuối danh sách hoặc bên cạnh quy tắc đã chọn.

   Vị trí của quy tắc trong danh sách sẽ quyết định mức độ ưu tiên của quy tắc. Quy tắc ở đầu danh sách có mức độ ưu tiên cao nhất.

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 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.

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 mới.

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. Để thực hiện, hãy bỏ chọn hộp kiểm bên cạnh đối tượng.

Cách tạo quy tắc gói tin mạng trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.

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 **Communication & Web Protection** → **Firewall**.

5. Chọn thẻ **Network packet rules**.

   Thao tác này sẽ mở danh sách các quy tắc mạng mặc định được thiết lập bởi Tường lửa.

6. Nhấn vào **Add**.

   Thao tác này sẽ mở biểu mẫu cho quy tắc mạng mới.

7. Nhập vào thủ công tên của dịch vụ mạng vào trường **Rule name**.

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 **Select rule template**. 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 **Log events**.

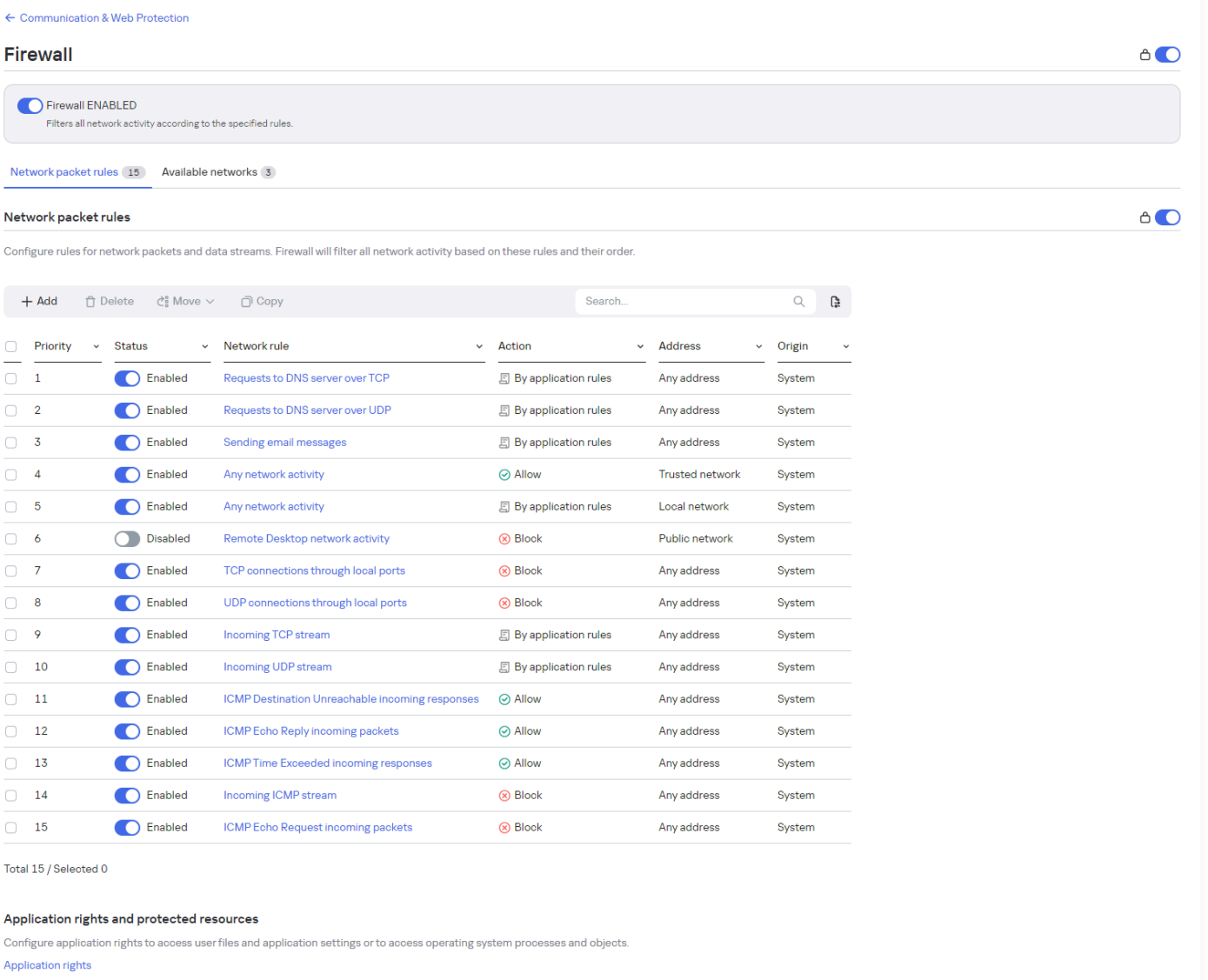
10. Lưu quy tắc mạng.

    Quy tắc mạng mới sẽ được thêm vào danh sách.

11. Sử dụng nút **Move** 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 **Status** để bật hoặc tắt quy tắc gói tin.



Những quy tắc cho gói tin Tường lửa

Thiết lập Quy tắc gói tin mạng

Tham số	Mô tả
Hành động	**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.
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 của các máy tính cục bộ và từ xa mà kết nối giữa chúng được giám sát. Phạm vi giá trị hợp lệ cho số hiệu cổng: 0–65535. Trong mỗi trường, bạn có thể nhập nhiều giá trị được phân tách bằng `,` hoặc chỉ định một khoảng giá trị bằng `-`. Ví dụ: • `100,101` • `100-130` • `100,110-130`

Tham số	Mô tả
Hướng	**Gói tin vào (gói)**. Tường lửa sẽ áp dụng quy tắc mạng cho tất cả các gói mạng gửi đến. **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. **Gói tin vào / Gói tin ra**. Tường lửa sẽ áp dụng quy tắc mạng cho tất cả các gói mạng đến và đi. **Gói tin ra (gói)**. Tường lửa áp dụng quy tắc mạng cho tất cả các gói mạng gửi đi. **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.
Bộ điều hợp mạng	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.
Thời gian sống (TTL)	Giới hạn việc kiểm soát các gói tin mạng theo thời gian tồn tại của chúng (Time to Live, TTL).
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. Nếu trong quy tắc gói tin mạng, bạn đã thêm một tên DNS không thể xác định địa chỉ IP, Kaspersky Endpoint Security sẽ hiển thị một cảnh báo. Trong danh sách các quy tắc gói tin mạng trong Bảng điều khiển web, một cột được thêm vào kèm mô tả về lỗi. Không có mô tả lỗi trong Bảng điều khiển quản trị (MMC). Các quy tắc gói như vậy được đánh dấu màu.
Địa chỉ cục 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. Ứng dụng chỉ lưu trữ địa chỉ cục bộ nếu chỉ định danh sách địa chỉ từ xa. Tức là giá trị **Địa chỉ từ danh sách** đã được chọn cho **Địa chỉ từ xa** và ít nhất một địa chỉ đã được thêm. Đôi khi địa chỉ nội bộ không thể được lấy cho các ứng dụng. Nếu đúng, tham số này sẽ bị bỏ qua.

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 mối 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 mối 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 mối 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Tường lửa**.

4. 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.

5. Vào thẻ **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. 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 vào 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 gói tin mạng:

   a. Nhấn vào 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 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 **Asset management** → **Policies**.
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 **Communication & Web Protection** → **Firewall**.
5. Để xuất danh sách các quy tắc, trong mục **Network packet rules**:

   a. Chọn các quy tắc mà bạn muốn xuất.

   b. Nhấn nút → **Export**.

   Kaspersky Endpoint Security sẽ xuất danh sách các quy tắc vào tập tin JSON trong thư mục tải xuống mặc định.
6. Để nhập danh sách quy tắc, trong mục **Network packet rules**:

   a. Nhấn nút → **Import**.

   Trong cửa sổ mở ra, hãy chọn tập tin JSON 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 JSON.
7. Lưu các thay đổi của bạn.

Định nghĩa quy tắc gói tin mạng trong XML

Tường lửa cho phép xuất các quy tắc gói tin mạng ở định dạng XML. Sau đó, bạn có thể sửa đổi tập tin, ví dụ như thêm một số lượng lớn các quy tắc cùng loại.

Tập tin XML chứa hai nút chính: `Rules` Và `Resources`. Nút `Rules` liệt kê những quy tắc cho gói tin mạng. Nút này chứa những quy tắc được cấu hình theo mặc định (*quy tắc định trước*) cũng như những quy tắc do người dùng thêm vào (*quy tắc tùy chỉnh*).

Đánh dấu quy tắc gói tin mạng

```
<key name="0000">
        <tDWORD name="RuleId">100</tDWORD>
        <tDWORD name="RuleState">1</tDWORD>
        <tDWORD name="RuleTypeId">4</tDWORD>
        <tQWORD name="AppIdEx">0</tQWORD>
        <tDWORD name="ResIdEx">812</tDWORD>
        <tDWORD name="ResIdEx2">0</tDWORD>
        <tDWORD name="AccessFlag">2</tDWORD>
</key>
```

Tham số	Mô tả	Giá trị
`<key name="0000">`	Mức độ ưu tiên của quy tắc. Giá trị này càng thấp thì mức độ ưu tiên càng cao.	Số nguyên Giá trị mức độ ưu tiên phải bao gồm 4 chữ số. Các nút trong tập tin XML phải được sắp xếp theo giá trị ưu tiên, bắt đầu bằng `0000`.
`RuleId`	ID của quy tắc.	**Quy tắc định trước** `100` – **Yêu cầu đến máy chủ DNS qua TCP**. `101` – **Yêu cầu đến máy chủ DNS qua UDP**. `102` – **Gửi nội dung email**. `110` – **Bất kỳ hoạt động mạng** (Mạng tin tưởng). `125` – **Bất kỳ hoạt động mạng** (Mạng cục bộ). `130` – **Hoạt động mạng điều khiển từ xa**. `131` – **Kết nối TCP thông qua cổng nội bộ**. `132` – **Kết nối UDP thông qua cổng nội bộ**. `133` – **Luồng TCP vào**. `134` – **Luồng UDP vào**. `137` – **ICMP không có trả lời từ gói tin vào**. `138` – **Hiển thị trả lời cho gói tin ICMP vào**. `140` – **Thời gian quá hạn để trả lời cho gói tin ICMP vào**. `142` – **Luồng ICMP vào**. `266` – **Hiển thị yêu cầu cho gói tin ICMPv6 vào**.
`RuleState`	Trạng thái của quy tắc.	`0` – quy tắc định trước bị vô hiệu `1` – quy tắc định trước được bật `2` – quy tắc tùy chỉnh bị vô hiệu `3` – quy tắc tùy chỉnh được bật
`RuleTypeId`	ID của loại quy tắc.	`4` – quy tắc gói tin mạng.
`AppIdEx`	ID của ứng dụng chứa quy tắc gói tin mạng.	Nếu quy tắc không thuộc bất kỳ ứng dụng nào thì giá trị này bằng `0`.
`ResIdEx`	ID chính của tài nguyên có thiết lập quy tắc. Bạn có thể sử dụng định danh này để định vị một khối có thiết lập quy tắc trong nút `Resources`.	Số nguyên
`ResIdEx2`	ID của loại mạng.	`0` – **Địa chỉ bất kỳ**. `50` – **Mạng tin tưởng**. `51` – **Mạng cục bộ**. `52` – **Mạng công cộng**. `<Network Identifier>` – **Địa chỉ từ danh sách** (địa chỉ được xác định theo cách thủ công).
`AccessFlag`	Giá trị của tham số **Hành động**.	`0` – **Cho phép**. `2` – **Theo các quy tắc ứng dụng**. `3` – **Chặn**. `4` – **Cho phép** và **Ghi lại sự kiện**. `6` – **Theo các quy tắc ứng dụng** và **Ghi lại sự kiện**. `7` – **Chặn** và **Ghi lại sự kiện**.
`</key>`		

Nút `Resources` chứa thiết lập quy tắc gói tin mạng. Thiết lập quy tắc gói tin mạng tùy chỉnh được liệt kê trong mục `<key name="0004">`.

Đánh dấu quy tắc gói tin mạng tùy chỉnh

```
<key name="0026">
        <key name="Data">
                <key name="RemotePorts"> </key>
                <key name="LocalPorts"> </key>
                <key name="AdapterBindings">
                        <key name="0000">
                                <key name="IpAddresses">
                                        <key name="0000">
                                                <key name="IP">
                                                        <key name="V6">
                                                                <tQWORD name="Hi">0</tQWORD>
                                                                <tQWORD name="Lo">0</tQWORD>
                                                                <tDWORD name="Zone">0</tDWORD>
                                                                <tSTRING name="ZoneStr"/>
                                                        </key>
                                                        <tBYTE name="Version">4</tBYTE>
                                                        <tDWORD name="V4">16909060</tDWORD>
                                                        <tBYTE name="Mask">32</tBYTE>
                                                </key>
                                                <key name="AddressIP"> </key>
                                                <tSTRING name="Address"/>
                                        </key>
                                </key>
                                <key name="MacAddresses">
                                        <key name="0000">
                                                <tDWORD name="Type">0</tDWORD>
                                                <tQWORD name="AddressData0">1108152157446</tQWORD>
                                                <tQWORD name="AddressData1">0</tQWORD>
                                        </key>
                                </key>
                                <tSTRING name="AdapterName">ADAPTER TEST 123</tSTRING>
                                <tDWORD name="InterfaceType">3</tDWORD>
                        </key>
                </key>
                <tTYPE_ID name="unique">3213697024</tTYPE_ID>
                <tBYTE name="Proto">2</tBYTE>
                <tBYTE name="Direction">2</tBYTE>
                <tBYTE name="IcmpType">0</tBYTE>
                <tBYTE name="IcmpCode">0</tBYTE>
                <tDWORD name="Flags">1</tDWORD>
                <tBYTE name="TTL">255</tBYTE>
        </key>
        <key name="Childs"> </key>
        <tDWORD name="Id">1073747214</tDWORD>
        <tDWORD name="ParentID">7</tDWORD>
        <tDWORD name="Flags">38</tDWORD>
        <tSTRING name="Name">TEST1</tSTRING>
</key>
```

Thiết lập quy tắc gói tin mạng tùy chỉnh

Tham số	Mô tả	Giá trị
`<key name="Data">`	ID của mục tham số.	Số nguyên
`RemotePorts`	Giá trị của tham số **Cổng từ xa**.	Danh sách các dải cổng từ xa.
`LocalPorts`	Giá trị của tham số **Cổng nội bộ**.	Danh sách các dải cổng cục bộ.

Tham số	Mô tả	Giá trị
`AdapterBindings`	Giá trị của tham số **Bộ điều hợp mạng**.	`IpAddresses` – giá trị của tham số **Địa chỉ IP**. `MacAddresses` – giá trị của tham số **Địa chỉ MAC**. `AdapterName` – tên của bộ điều hợp mạng. `InterfaceType` – giá trị của tham số **Dạng giao diện**: • `0` – **Khác**. • `1` – **LoopBack**. • `2` – **Mạng có dây (Ethernet)**. • `3` – **Mạng không dây (Wi-Fi)**. • `4` – **Đường hầm**. • `5` – **Kết nối PPP**. • `6` – **Kết nối PPPoE**. • `7` – **Kết nối VPN**. • `8` – **Kết nối modem**.
`unique`	ID bên trong của cấu trúc.	Số nguyên Bạn không nên thay đổi tham số này.
`Proto`	Giá trị của tham số **Giao thức**.	`0` – bị vô hiệu. `1` – **ICMP**. `2` – **IGMP**. `6` – **TCP**. `17` – **UDP**. `47` – **GRE**. `58` – **ICMPv6**.
`Direction`	Giá trị của tham số **Hướng**.	`1` – **Gói tin vào (gói)**. `2` – **Gói tin ra (gói)**. `3` – **Gói tin vào / Gói tin ra**. `4` – **Gói tin vào**. `5` – **Gói tin ra**.

Tham số	Mô tả	Giá trị
`IcmpType`	Giá trị của tham số **Loại ICMP**.	**Giao thức ICMP** `0` – **Trả lời lại** (ICMP) hoặc bị vô hiệu. `3` – **Không tới được đích** (ICMP). `4` – **Nguồn nhúng**. `5` – **Chuyển hướng**. `6` – **Địa chỉ máy chủ thay thế**. `8` – **Yêu cầu lại**. `9` – **Bộ định tuyến quảng cáo**. `10` – **Bộ định tuyến trưng cầu**. `11` – **Vượt quá thời gian**. `12` – **Vấn đề tham biến**. `13` – **Thời gian đóng dấu**. `14` – **Trả lời thời gian đóng dấu**. `15` – **Thông tin yêu cầu**. `16` – **Thông tin trả lời**. `17` – **Địa chỉ đại diện yêu cầu**. `18` – **Địa chỉ đại diện trả lời**. `30` – **Bộ định tuyến theo dõi**. `31` – **Lỗi chuyển đổi dữ liệu**. `32` – **Máy chủ di động chuyển hướng**. `33` – **IPv6 ở đâu**. `34` – **IPv6 là đây**. `35` – **Yêu cầu đăng ký di động**. `36` – **Trả lời đăng ký di động**. `37` – **Tên miền yêu cầu**. `38` – **Tên miền trả lời**. `40` – **Photuris**. **Giao thức ICMPv6** `1` – **Không tới được đích**. `2` – **Gói tin quá lớn**. `3` – **Vượt quá thời gian**. `4` – **Vấn đề tham biến**. `128` – **Yêu cầu lại**. `129` – **Trả lời lại**. `130` – **Truy vấn lắng nghe đa hướng**. `131` – **Báo cáo lắng nghe đa hướng**. `132` – **Thực hiện lắng nghe đa hướng**. `133` – **Bộ định tuyến trưng cầu**. `134` – **Bộ định tuyến quảng cáo**. `135` – **Lời chào**. `136` – **Quảng cáo**. `137` – **Chuyển hướng tin nhắn**. `138` – **Bộ định tuyến Renumbering**. `139` – **Nút truy vấn thông tin ICMP**. `141` – **Thông điệp chào mời làm bạn trên mạng xã hội**. `142` – **Thông điệp chào mời làm bạn trên mạng xã hội**. `143` – **Multicast Listener Report Phiên bản 2**.

Tham số	Mô tả	Giá trị
		`144` – **Thông điệp yêu cầu phát hiện địa chỉ trang chủ**. `145` – **Thông điệp trả lời cho địa chỉ**. `146` – **Tiền tố chào mời trên di động**. `147` – **Quảng cáo tiền tố trên di động**. `148` – **Thông tin bản và chứng chỉ**. `149` – **Thông tin địa chỉ bản vá chứng chỉ**. `151` – **Quảng cáo đa truyền thông**. `152` – **Quảng cáo đa truyền thông**. `153` – **Chấm dứt thông tin truyền thông**.
`IcmpCode`	Giá trị của tham số **Mã ICMP**.	`0` – **Mã 0** hoặc bị vô hiệu. `1` – **Mã 1**. `2` – **Mã 2**.
`Flags`	Con trỏ thuộc tính cấu trúc.	Số nguyên Bạn không nên thay đổi tham số này.
`TTL`	Giá trị của tham số **Thời gian sống (TTL)**.	Giá trị tính bằng giây. Nếu bị vô hiệu, giá trị này bằng `0`.
`</key>`		
`Id`	ID chính của tài nguyên (xem nút `Rules`).	Số nguyên
`ParentID`	ID của nhóm cha.	Số nguyên Bạn không nên thay đổi tham số này.
`Flags`	Trạng thái của quy tắc.	`6` – quy tắc bị vô hiệu. `38` – quy tắc được bật.
`Name`	Tên của quy tắc gói tin mạng.	Chuỗi

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 vào ô **Giám sát mạng**.
2. Vào 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 của 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 sẵn 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 các 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 sẵn 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa thiết yếu → Tường lửa**.

4. 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.

5. Vào thẻ **Quy tắc cho ứng dụng mạng**.

6. Nhấn vào **Thêm**.

7. 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.

8. Nhấn vào **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.

9. Chọn ứng dụng cần thiết.

10. 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.

11. 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.

12. Chọn thẻ **Quy tắc mạng**.

    Thao tác này sẽ mở danh sách các quy tắc mạng mặc định được thiết lập bởi Tường lửa.

13. Nhấn vào **Thêm**.

    Thao tác này sẽ mở các thuộc tính quy tắc mạng.

14. Nhập vào thủ công tên của dịch vụ mạng vào trường **Tên**.

15. 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.

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

17. Lưu quy tắc mạng mới.

18. Sử dụng các nút **Lên** / **Xuống** để đặt mức độ ưu tiên của quy tắc mạng.

19. 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 **Asset management** → **Policies**.

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 **Communication & Web Protection** → **Firewall**.

5. Trong mục **Application rights and protected resources**, hãy nhấn liên kết **Application rights**.

   Thao tác này sẽ mở ra cửa sổ cấu hình quyền của ứng dụng và danh sách các tài nguyên được bảo vệ.

6. Vào thẻ **Application rights**.

   Bạn sẽ thấy danh sách các nhóm tin tưởng ở bên trái cửa sổ và thuộc tính của chúng ở bên phải.

7. Trong mục **Applications**, hãy nhấn nút **Add**.

   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 **Application**. Chuyển sang bước tiếp theo.

   Nếu bạn muốn tạo quy tắc mạng cho nhiều ứng dụng, hãy chọn loại **Group** 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. Hoàn tất trình hướng dẫn.

    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 **Network rules** 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 **Add**.

    Thao tác này sẽ mở các thuộc tính quy tắc ứng dụng.

15. Nhập vào thủ công tên của dịch vụ mạng vào trường **Rule name**.

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 **Select rule template**. 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 **Log events**.

18. Lưu quy tắc mạng.

    Quy tắc mạng mới sẽ được thêm vào danh sách.

19. Sử dụng nút **Move** 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 của các máy tính cục bộ và từ xa mà kết nối giữa chúng được giám sát. Phạm vi giá trị hợp lệ cho số hiệu cổng: 0–65535. Trong mỗi trường, bạn có thể nhập nhiều giá trị được phân tách bằng `,` hoặc chỉ định một khoảng giá trị bằng `-`. Ví dụ: • `100,101` • `100-130` • `100,110-130`
Hướng	**Gói tin vào**. **Gói tin vào / Gói tin ra**. **Gói tin ra**.

Tham số	Mô tả
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. Nếu trong quy tắc gói tin mạng, bạn đã thêm một tên DNS không thể xác định địa chỉ IP, Kaspersky Endpoint Security sẽ hiển thị một cảnh báo. Trong danh sách các quy tắc gói tin mạng trong Bảng điều khiển web, một cột được thêm vào kèm mô tả về lỗi. Không có mô tả lỗi trong Bảng điều khiển quản trị (MMC). Các quy tắc gói như vậy được đánh dấu màu.
Địa chỉ cục 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. Ứng dụng chỉ lưu trữ địa chỉ cục bộ nếu chỉ định danh sách địa chỉ từ xa. Tức là giá trị **Địa chỉ từ danh sách** đã được chọn cho **Địa chỉ từ xa** và ít nhất một địa chỉ đã được thêm. Đôi khi địa chỉ nội bộ không thể được lấy cho các ứng dụng. Nếu đúng, tham số này sẽ bị bỏ qua.

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 mối đe dọa thiết yếu → Tường lửa**.
3. Nhấn vào **Quy tắc cho các 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 mối đe dọa thiết yếu → Tường lửa**.
3. Nhấn vào **Quy tắc cho các 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 các 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 các 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 vào 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 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.

Thành phần Phòng chống khai thác còn giám sát các cổng mạng để tìm các tiến trình của ứng dụng có thể đe dọa đến tính bảo mật của máy tính. Ứng dụng sẽ lấy thông tin về những tiến trình như vậy thông qua cơ sở dữ liệu chống virus.

Bật và tắt Phòng chống khai thác

Theo mặc định, Phòng chống khai thác sẽ được bật và hoạt động trong chế độ tối ưu. Kaspersky Endpoint Security sẽ giám sát các tập tin thực thi đang được chạy bởi các ứng dụng dễ bị tấn công. Nếu Kaspersky Endpoint Security phát hiện một tập tin thực thi từ một ứng dụng có lỗ hổng 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).

Cách bật hoặc tắt thành phần Phòng chống khai thác trong Bảng điều khiển quản trị (MMC)

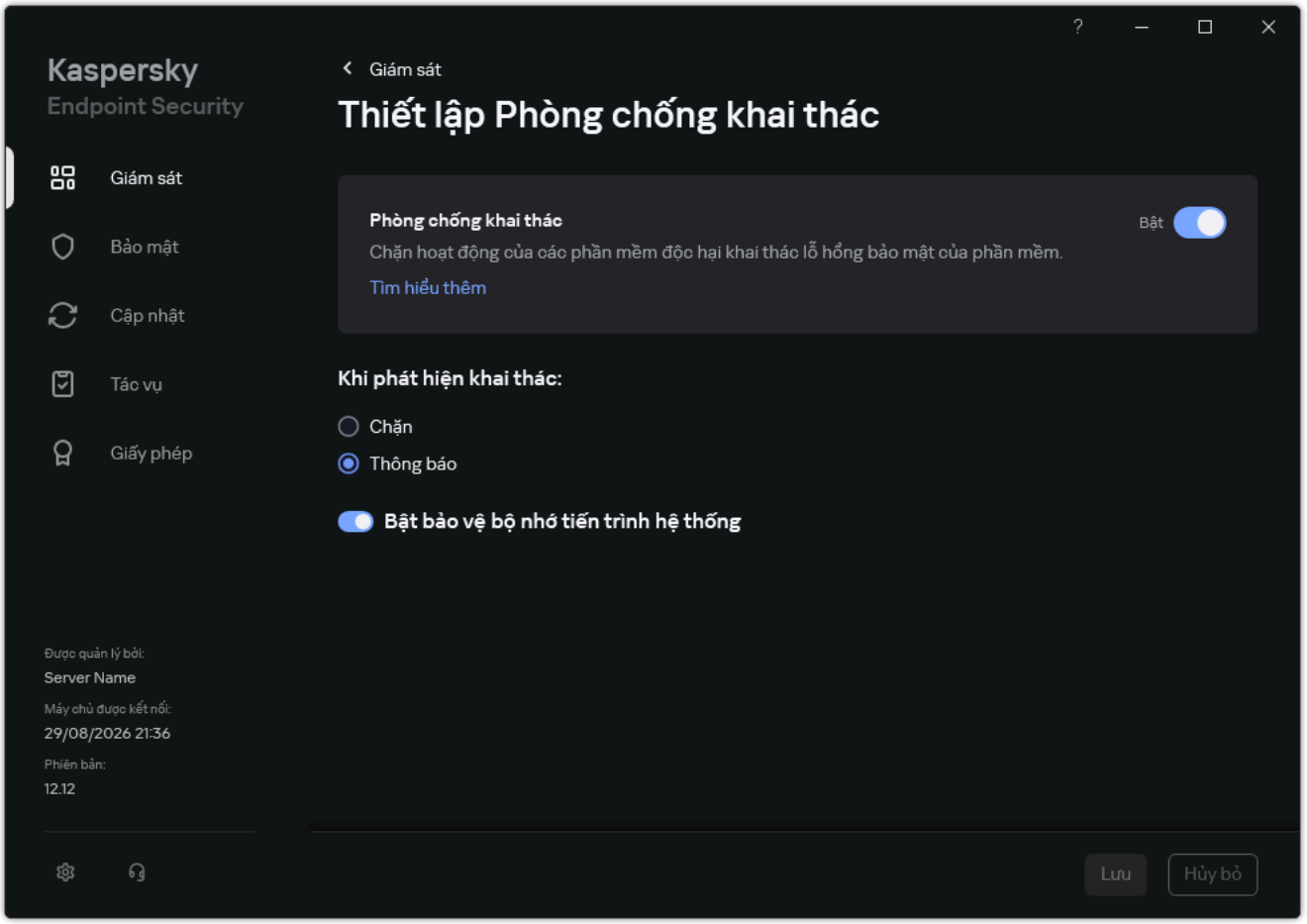
1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao → Phòng chống khai thác**.
4. Sử dụng hộp kiểm **Phòng chống khai thác** để bật hoặc tắt thành phần.
5. Chọn hành động liên quan trong mục **Khi phát hiện khai thác**:
   - **Chặn**. 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.
6. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật hoặc tắt Phòng chống khai thác trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Policies**.
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 **Host Threat Protection → Behavior Analysis → Exploit Prevention**.
5. Sử dụng nút bật/tắt **Exploit Prevention** để bật hoặc tắt thành phần này.
6. Chọn hành động liên quan trong mục **Action on threat detection**:
   - **Block**. 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.
   - **Inform**. 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.
7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật hoặc tắt Phòng chống khai thác 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 khai thác**.



Thiết lập Phòng chống khai thác

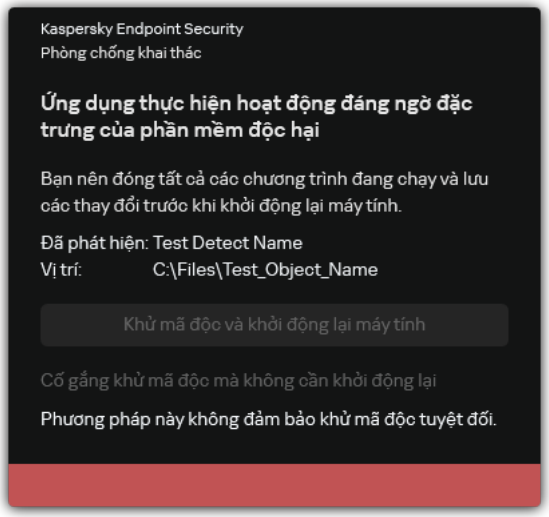
3. Sử dụng nút bật/tắt **Phòng chống khai thác** để bật hoặc tắt thành phần này.

4. Chọn hành động liên quan trong mục **Khi phát hiện khai thác**:

   - **Chặn**. 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.

5. Lưu các thay đổi của bạn.



Thông báo về mối đe dọa đang hoạt động

Bảo vệ bộ nhớ của tiến trình hệ thống

Theo mặc định, tính năng bảo vệ bộ nhớ tiến trình hệ thống được bật. Kaspersky Endpoint Security sẽ chặn các tiến trình bên ngoài cố giành quyền truy cập vào các tiến trình hệ thống.

Cách bật hoặc tắt bảo vệ bộ nhớ tiến trình hệ thống trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao → Phòng chống khai thác**.

4. Sử dụng hộp kiểm **Bật bảo vệ bộ nhớ tiến trình hệ thống** để bật hoặc tắt tùy chọn này.

5. Lưu các thay đổi của bạn.

Cách bật hoặc tắt bảo vệ bộ nhớ tiến trình hệ thống trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Policies**.

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 **Host Threat Protection** → **Behavior Analysis** → **Exploit Prevention**.

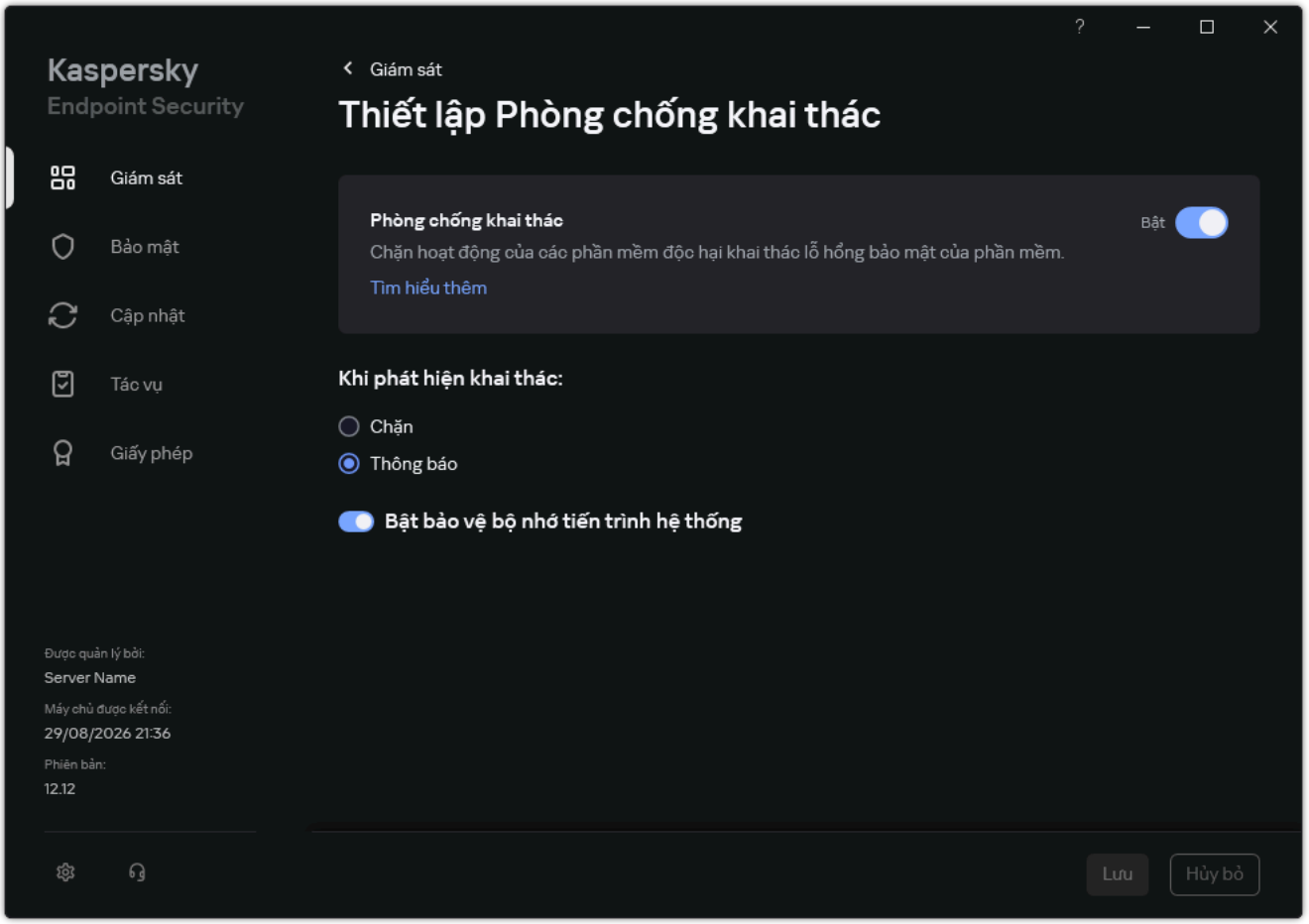
5. Sử dụng nút bật/tắt **System process memory protection ENABLED** để bật hoặc tắt tính năng này.

6. Lưu các thay đổi của bạn.

Cách bật hoặc tắt bảo vệ bộ nhớ tiến trình hệ thống 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 khai thác**.



Thiết lập 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.

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 và cung cấp chức năng bảo vệ chủ động cho máy tính.

Thành phần Phát hiện hành vi còn giám sát các cổng mạng để tìm các tiến trình của ứng dụng có thể đe dọa đến tính bảo mật của máy tính. Ứng dụng sẽ lấy thông tin về những tiến trình như vậy thông qua cơ sở dữ liệu chống virus.

Theo mặc định, Phát hiện hành vi sẽ được bật và chạy trong chế độ được khuyến nghị bởi các chuyên gia của Kaspersky. Khi phát hiện hoạt động độc hại, Kaspersky Endpoint Security sẽ xóa tập tin thực thi của ứng dụng độc hại.

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.

Cách bật hoặc tắt Phát hiện hành vi trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao → Phát hiện hành vi**.
5. Sử dụng hộp kiểm **Phát hiện hành vi** để bật hoặc tắt thành phần.
6. Chọn hành động liên quan trong mục **Hành động khi phát hiện hoạt động của phần mềm độc hại**:
   - **Xóa**. 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.
   - **Chặn**. 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.
7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật hoặc tắt Phát hiện hành vi trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Policies**.
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 **Host Threat Protection → Behavior Analysis → Behavior Detection**
5. Sử dụng nút bật/tắt **Behavior Detection ENABLED** để bật hoặc tắt thành phần này.

6. Chọn hành động liên quan trong mục **Action on threat detection**:

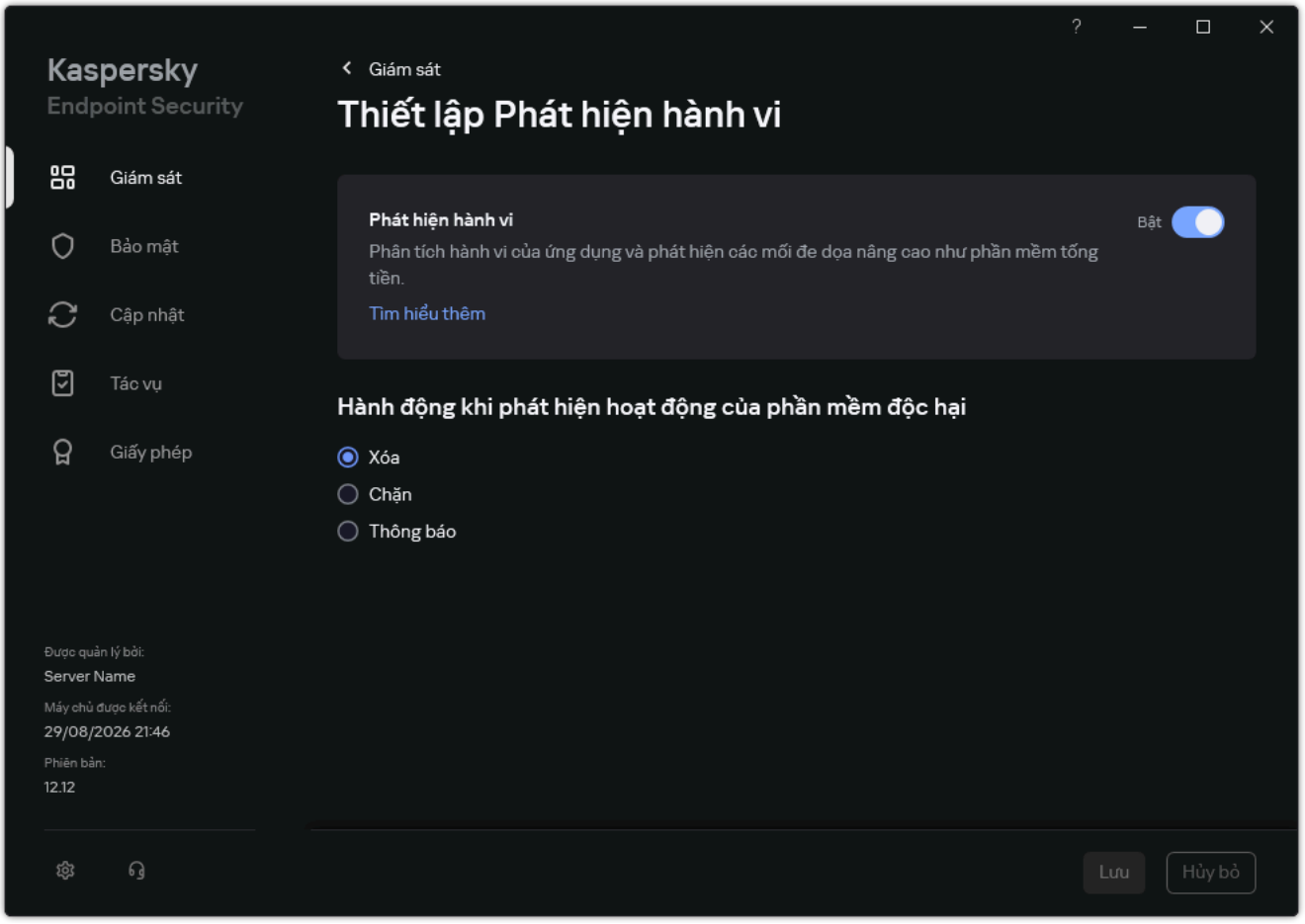
   - **Delete**. Nếu mục này được chọn, khi phát hiện hoạt động độc hại, Kaspersky Endpoint Security sẽ xóa tập tin thực thi của ứng dụng độc hại và tạo một bản sao lưu của tập tin đó trong Sao lưu.
   - **Block**. Nếu đề mục này được chọn, khi phát hiện hoạt động độc hại, Kaspersky Endpoint Security sẽ chấm dứt hoạt động của ứng dụng này.
   - **Inform**. 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.

7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật hoặc tắt Phát hiện 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 nâng cao → Phát hiện hành vi**.



Thiết lập Phát hiện hành vi

3. Sử dụng nút bật/tắt **Phát hiện hành vi** để bật hoặc tắt thành phần này.

4. Chọn hành động liên quan trong mục **Hành động khi phát hiện hoạt động của phần mềm độc hại**:

   - **Xóa**. 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.

   - **Chặn**. 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.

5. 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.

Anti-Cryptor

Kể từ Kaspersky Endpoint Security 12.12 cho Windows, chức năng bảo vệ thư mục chia sẻ trước mã hóa bên ngoài, vốn là một phần của thành phần Phát hiện hành vi, nay đã là một thành phần riêng biệt có tên là Anti-Cryptor.

> 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.

Thành phần Anti-Cryptor sẽ 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.

> Để thành phần Anti-Cryptor hoạt động, bạn phải bật thành phần Phát hiện hành vi.

Nếu 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 trong giao diện ứng dụng cục bộ và 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.

Bật hoặc tắt bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài

Theo mặc định, tính năng bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài được bật và hoạt động theo khuyến nghị của các chuyên gia Kaspersky. Để cấu hình tính năng này, bạn có thể tạo phạm vi bảo vệ và cấu hình loại trừ nếu cần. Theo mặc định, ứng dụng sẽ tự động xác định các thư mục được chia sẻ và theo dõi hoạt động đối với tập tin trong tất cả các thư mục. Khi phát hiện có nỗ lực mã hóa các tập tin từ bên ngoài trong thư mục chia sẻ, Kaspersky Endpoint Security sẽ chặn phiên của người dùng từ xa trong một giờ (theo mặc định).

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.

Cách bật hoặc tắt bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao** → **Anti-Cryptor**.
4. Sử dụng hộp kiểm **Chống công cụ mã hóa** để bật hoặc tắt tính năng phát hiện hoạt động điển hình của mã hóa bên ngoài.
5. Chọn hành động liên quan mà ứng dụng sẽ thực hiện khi phát hiện có nỗ lực sửa đổi tập tin trong thư mục chia sẻ:
   - **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 quyền truy cập sửa đổi tập tin cho phiên đã khởi tạo hoạt động độc hại và sẽ tạo các bản sao lưu của tập tin bị sửa đổi.

     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.

   - **Thông báo**. Nếu tùy chọn 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 này vào danh sách các mối đe dọa đang hoạt động, hãy thêm một mục vào báo cáo giao diện ứng dụng cục bộ và gửi thông tin về hoạt động độc hại được phát hiện tới Kaspersky Security Center.
6. Nếu cần, hãy chỉnh sửa phạm vi bảo vệ và xác định các loại trừ.
7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật hoặc tắt bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.
5. Sử dụng nút bật/tắt **Anti-Cryptor ENABLED** để bật hoặc tắt tính năng phát hiện hoạt động điển hình của mã hóa bên ngoài.
6. Chọn hành động liên quan mà ứng dụng sẽ thực hiện khi phát hiện có nỗ lực sửa đổi tập tin trong thư mục chia sẻ:

   - **Block connection for (min) 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 quyền truy cập sửa đổi tập tin cho phiên đã khởi tạo hoạt động độc hại và sẽ tạo các bản sao lưu của tập tin bị sửa đổi.

     Nếu thành phần Công cụ khắc phục được bật và tùy chọn **Block connection for (min) N phút** được chọn thì các tập tin bị sửa đổi sẽ được khôi phục từ bản sao lưu.

   - **Inform**. Nếu tùy chọn 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 này vào danh sách các mối đe dọa đang hoạt động, hãy thêm một mục vào báo cáo giao diện ứng dụng cục bộ và gửi thông tin về hoạt động độc hại được phát hiện tới Kaspersky Security Center.
7. Nếu cần, hãy chỉnh sửa phạm vi bảo vệ và xác định các loại trừ.
8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật hoặc tắt bảo vệ thư mục được chia sẻ chống lại mã hóa từ bên ngoài 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** → **Chống công cụ mã hóa**.
3. Sử dụng hộp kiểm **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. Sử dụng hộp kiểm **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.

5. Chọn hành động liên quan mà ứng dụng sẽ thực hiện khi phát hiện có nỗ lực sửa đổi tập tin trong thư mục chia sẻ:

   - **Chặn kết nối trong (phút) 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 quyền truy cập sửa đổi tập tin cho phiên đã khởi tạo hoạt động độc hại và sẽ tạo các bản sao lưu của tập tin bị sửa đổi.

     Nếu thành phần Công cụ khắc phục được bật và tùy chọn **Chặn kết nối trong (phút) N phút** được chọn thì các tập tin bị sửa đổi sẽ được khôi phục từ bản sao lưu.

   - **Thông báo**. Nếu tùy chọn 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 này vào danh sách các mối đe dọa đang hoạt động, hãy thêm một mục vào báo cáo giao diện ứng dụng cục bộ và gửi thông tin về hoạt động độc hại được phát hiện tới Kaspersky Security Center.

6. Nếu cần, hãy chỉnh sửa phạm vi bảo vệ và xác định các loại trừ.

7. Lưu các thay đổi của bạn.

Cấu hình thời gian chặn của máy tính không được tin tưởng

Máy tính không được tin tưởng là máy tính từ xa đang thực hiện hoạt động độc hại hoặc mã hóa dữ liệu. Theo mặc định, Kaspersky Endpoint Security sẽ chặn phiên của người dùng từ xa trong một giờ. Khi hết thời gian chặn, Kaspersky Endpoint Security sẽ xóa máy tính khỏi danh sách chặn và khôi phục quyền truy cập thư mục chia sẻ.

Cách cấu hình thời gian chặn máy tính không được tin tưởng trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao → Anti-Cryptor**.

4. Trong mục **Hành động khi phát hiện mối đe dọa**, hãy chọn **Chặn kết nối trong N phút**.

5. Hãy cấu hình thời gian chặn máy tính không được tin tưởng đang tham gia vào hoạt động độc hại hoặc mã hóa dữ liệu.

6. Lưu các thay đổi của bạn.

Cách cấu hình thời gian chặn máy tính 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 **Asset management → Policies**.

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 **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.

5. Trong mục **Action on threat detection**, hãy cấu hình thời gian chặn máy tính không được tin tưởng đang tham gia vào hoạt động độc hại hoặc mã hóa dữ liệu.

6. Lưu các thay đổi của bạn.

Cách cấu hình thời gian chặn máy tính 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 **Bảo vệ mối đe dọa nâng cao** → **Chống công cụ mã hóa**.

3. Trong mục **Hành động khi phát hiện mối đe dọa**, hãy chọn **Chặn kết nối trong (phút)**.

4. Hãy cấu hình thời gian chặn máy tính không được tin tưởng đang tham gia vào hoạt động độc hại hoặc mã hóa dữ liệu.

5. Lưu các thay đổi của bạn.

Kết quả là máy tính từ xa sẽ bị khóa. Để mở khóa máy tính từ xa, bạn có thể khởi động lại Kaspersky Endpoint Security.

Chỉnh sửa phạm vi giám sát

Phạm vi bảo vệ là danh sách các đường dẫn đến các thư mục chia sẻ mà Kaspersky Endpoint Security theo dõi hoạt động đối với tập tin. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện. Theo mặc định, ứng dụng sẽ tự động xác định các thư mục được chia sẻ và theo dõi hoạt động đối với tập tin trong tất cả các thư mục.

Việc loại trừ một thư mục khỏi phạm vi bảo vệ 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.

> Bạn cũng có thể loại trừ các máy tính không cho phép các nỗ lực mã hóa bên ngoài được xử lý.

Cách chỉnh sửa phạm vi bảo vệ trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao** → **Anti-Cryptor**.

4. Trong mục **Phạm vi bảo vệ**, hãy chọn **Chỉ các thư mục chia sẻ được chỉ định**.

5. Trong danh sách thư mục, hãy nhấn vào **Thêm**.

6. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy nhập đường dẫn đến thư mục được chia sẻ mà bạn muốn đưa vào phạm vi bảo vệ (ví dụ: `C:\Share`).

   Hãy sử dụng đường dẫn cục bộ để thêm thư mục chia sẻ vào phạm vi bảo vệ.

7. Nhấn vào **OK**.

8. Nếu cần, hãy xác định các loại trừ phạm vi bảo vệ:

   a. Trong mục **Loại trừ quét**, hãy nhấn nút **Theo tên đại diện**.

   b. Trong cửa sổ mở ra, hãy nhấn nút **Thêm**.

   c. Trong cửa sổ hiển thị, hãy chỉ định phần mở rộng tập tin ở định dạng `*.<file extension>` hoặc đường dẫn thư mục. Kaspersky Endpoint Security hỗ trợ các ký tự `*` và `?` khi nhập tên đại diện.

      Ứng dụng không hỗ trợ một số phần mở rộng tập tin loại trừ. Vì vậy, bạn có thể chỉ định một loại trừ như `*.docx` hoặc `**\Folder\**`.

   Bạn có thể loại trừ một đối tượng khỏi các vụ quét mà không cần xóa đối tượng đó khỏi danh sách các đối tượng trong phạm vi bảo vệ. Để thực hiện, hãy bỏ chọn hộp kiểm bên cạnh đối tượng.

9. Lưu các thay đổi của bạn.

Cách chỉnh sửa phạm vi 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 **Asset management** → **Policies**.

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 **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.

5. Trong mục **Protection scope**, hãy chọn **Only specified shared folders**.

6. Trong danh sách thư mục, hãy nhấn vào **Add**.

7. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy nhập đường dẫn đến thư mục được chia sẻ mà bạn muốn đưa vào phạm vi bảo vệ (ví dụ: `C:\Share`).

   Hãy sử dụng đường dẫn cục bộ để thêm thư mục chia sẻ vào phạm vi bảo vệ.

8. Nhấn vào **OK**.

9. Nếu cần, hãy xác định các loại trừ phạm vi bảo vệ:

   a. Ở phần bên phải của cửa sổ, hãy nhấn vào liên kết **Scan exclusions**.

   b. Trong cửa sổ mở ra, hãy nhấn nút **Add**.

c. Trong cửa sổ hiển thị, hãy chỉ định phần mở rộng tập tin ở định dạng `*.<file extension>` hoặc đường dẫn thư mục. Kaspersky Endpoint Security hỗ trợ các ký tự `*` và `?` khi nhập tên đại diện.

Ứng dụng không hỗ trợ một số phần mở rộng tập tin loại trừ. Vì vậy, bạn có thể chỉ định một loại trừ như `*.docx` hoặc `**\Folder\**`.

Bạn có thể loại trừ một đối tượng khỏi các vụ quét mà không cần xóa đối tượng đó khỏi danh sách các đối tượng trong phạm vi bảo vệ. Để thực hiện, hãy bỏ chọn hộp kiểm bên cạnh đối tượng.

10. Lưu các thay đổi của bạn.

Cách chỉnh sửa phạm vi 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 → Chống công cụ mã hóa**.
3. Trong mục **Phạm vi bảo vệ**, hãy chọn **Chỉ các thư mục chia sẻ được chỉ định**.
4. Trong danh sách thư mục, hãy nhấn vào **Thêm**.
5. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy nhập đường dẫn đến thư mục được chia sẻ mà bạn muốn đưa vào phạm vi bảo vệ (ví dụ: `C:\Share`).

> Hãy sử dụng đường dẫn cục bộ để thêm thư mục chia sẻ vào phạm vi bảo vệ.

6. Nhấn vào **OK**.
7. Nếu cần, hãy xác định các loại trừ phạm vi bảo vệ:

a. Ở phần bên phải của cửa sổ, hãy nhấn vào liên kết **Loại trừ theo tên đại diện**.

b. Trong cửa sổ mở ra, hãy nhấn nút **Thêm**.

c. Trong cửa sổ hiển thị, hãy chỉ định phần mở rộng tập tin ở định dạng `*.<file extension>` hoặc đường dẫn thư mục. Kaspersky Endpoint Security hỗ trợ các ký tự `*` và `?` khi nhập tên đại diện.

Ứng dụng không hỗ trợ một số phần mở rộng tập tin loại trừ. Vì vậy, bạn có thể chỉ định một loại trừ như `*.docx` hoặc `**\Folder\**`.

Bạn có thể loại trừ một đối tượng khỏi các vụ quét mà không cần xóa đối tượng đó khỏi danh sách các đối tượng trong phạm vi bảo vệ. Để thực hiện, hãy bỏ chọn hộp kiểm bên cạnh đối tượng.

8. Lưu các thay đổi của bạn.

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. Nhấn vào **Duyệt** và chọn thư mục chia sẻ.

Bạn cũng có thể nhập đường dẫn này 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 cấp 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 sử dụng tên đại diện ở đầu, ở giữa hoặc ở cuối đường dẫn tập tin. Ví dụ: nếu bạn muốn thêm một thư mục cho tất cả người dùng để loại trừ, hãy nhập tên đại diện `?:\Users\*\Folder\`.

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 một loại trừ bất kỳ lúc nào.

9. Lưu các thay đổi của bạn.

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.

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 **Trusted Zone**.

5. Trong cửa sổ mở ra, hãy nhấn vào liên kết **Malware 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 exclusions** 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. Ngoài ra, nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ ẩn danh sách tổng hợp các loại trừ quét trong giao diện người dùng của ứng dụng.

8. Nhấn vào **Add** và chọn một hành động:

   - **Category**. Bạn có thể nhóm các loại trừ quét thành các danh mục riêng biệt. Để tạo một danh mục mới, hãy nhập tên danh mục và thêm ít nhất một loại trừ quét vào danh mục đó.

   - **New exclusion**. Kaspersky Endpoint Security sẽ thêm một loại trừ quét mới vào gốc của danh sách.

   - **Select exclusion from list**. Để nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager, ứng dụng bao gồm *loại trừ quét được xác định trước*. Ngoài ra, các loại trừ quét được định sẵn cũng đã được thêm vào để hỗ trợ thiết lập ứng dụng trong môi trường ảo Citrix và VMware. Bạn phải chọn loại trừ quét được xác định trước tùy thuộc vào mục đích của máy chủ được bảo vệ.

9. Chọn cách bạn muốn thêm loại trừ **Path to the file or folder**.

10. Nhập đường dẫn đến thư mục chia sẻ.

    Bạn cũng có thể nhập đường dẫn này 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 cấp 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 sử dụng tên đại diện ở đầu, ở giữa hoặc ở cuối đường dẫn tập tin. Ví dụ: nếu bạn muốn thêm một thư mục cho tất cả người dùng để loại trừ, hãy nhập tên đại diện `C:\Users\*\Folder\`.

11. Trong mục **Apply exclusion to**, hãy chọn thành phần **Behavior Detection**.

12. Nếu cần thiết, trong trường **Comment**, nhập một nhận xét ngắn về loại trừ quét mà bạn đang tạo.

13. Chọn trạng thái **Add to exclusions** cho loại trừ.

    Bạn có thể sử dụng nút bật/tắt để dừng một loại trừ bất kỳ lúc nào.

14. Lưu các thay đổi của bạn.

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Loại trừ và loại đối tượng**.

4. Trong mục **Loại trừ quét và ứng dụng được tin tưởng → Loại trừ quét**, hãy nhấn nút **Thiết lập**.

   Thao tác này sẽ mở cửa sổ chứa danh sách các loại trừ.

5. Chọn hộp kiểm **Hợp nhất các giá trị khi kế thừa** 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.

6. Chọn hộp kiểm **Cho phép sử dụng các loại trừ cục bộ** 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. Ngoài ra, nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ ẩn danh sách tổng hợp các loại trừ quét trong giao diện người dùng của ứng dụng.

7. Nhấn vào **Thêm** và chọn một hành động:

   - **Danh mục**. Bạn có thể nhóm các loại trừ quét thành các danh mục riêng biệt. Để tạo một danh mục mới, hãy nhập tên danh mục và thêm ít nhất một loại trừ quét vào danh mục đó.
   - **Loại trừ mới**. Kaspersky Endpoint Security sẽ thêm một loại trừ quét mới vào gốc của danh sách.
   - **Chọn loại trừ trong danh sách**. Để nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager, ứng dụng bao gồm *loại trừ quét được xác định trước*. Ngoài ra, các loại trừ quét được định sẵn cũng đã được thêm vào để hỗ trợ thiết lập ứng dụng trong môi trường ảo Citrix và VMware. Bạn phải chọn loại trừ quét được xác định trước tùy thuộc vào mục đích của máy chủ được bảo vệ.

8. Nhấn vào **Thêm**.

9. Trong mục **Thuộc tính**, hãy chọn hộp kiểm **Tập tin hoặc thư mục**.

10. 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**.

11. Nhấn vào **Duyệt** và chọn thư mục chia sẻ.

Bạn cũng có thể nhập đường dẫn này 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 cấp 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 sử dụng tên đại diện ở đầu, ở giữa hoặc ở cuối đường dẫn tập tin. Ví dụ: nếu bạn muốn thêm một thư mục cho tất cả người dùng để loại trừ, hãy nhập tên đại diện `?:\Users\*\Folder\`.

12. Nếu cần thiết, trong trường **Bình luận**, nhập một nhận xét ngắn về loại trừ quét mà bạn đang tạo.

13. Nhấn vào liên kết trong mục **Mô tả loại trừ quét (bấm vào mục gạch chân để chỉnh sửa)** để mở cửa sổ **Thành phần bảo vệ**.

14. Chọn hộp kiểm cạnh thành phần **Phát hiện hành vi**.

15. Lưu các thay đổi của bạn.

Thêm máy tính được tin tưởng để mã hóa dữ liệu bên ngoài

Nếu tổ chức của bạn sử dụng mã hóa dữ liệu ngoài trong quy trình trao đổi tập tin, bạn phải tạo danh sách các máy tính được tin tưởng. Kaspersky Endpoint Security không giám sát việc mã hóa dữ liệu của các máy tính được tin tưởng.

Dịch vụ Audit Logon phải được bật để có thể loại trừ các địa chỉ khỏi 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 rachỉ khỏi tính năng bảo vệ thư mục được chia sẻ hoạt động trên máy tính từ xa này.

Cách thêm máy tính được tin tưởng để mã hóa dữ liệu bên ngoài trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao → Anti-Cryptor**.
5. Trong mục **Loại trừ quét**, hãy nhấn nút **Theo tên hoặc địa chỉ IP**.
6. Trong cửa sổ mở ra, hãy nhấn nút **Theo tên hoặc địa chỉ IP**.
7. Nhập địa chỉ IP, dải địa chỉ IP hoặc tên của các máy tính không được phép xử lý mã hóa từ bên ngoài.
   Ví dụ:
   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách thêm máy tính được tin tưởng để mã hóa dữ liệu bên ngoài trong Bảng điều khiển web Kaspersky Security Center

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management → Policies**.
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 **Trusted Zone**.
5. Ở phần bên phải của cửa sổ, hãy nhấn vào liên kết **Anti-Cryptor exclusions**.
6. Trong cửa sổ mở ra, hãy nhấn nút **Add**.
7. Nhập địa chỉ IP, dải địa chỉ IP hoặc tên của các máy tính không được phép xử lý mã hóa từ bên ngoài.
   Ví dụ:
   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`

- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách thêm máy tính được tin tưởng để mã hóa dữ liệu bên ngoài 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 → Chống công cụ mã hóa**.
3. Ở phần bên phải của cửa sổ, hãy nhấn vào liên kết **Loại trừ theo tên hoặc địa chỉ IP**.
4. Trong cửa sổ mở ra, hãy nhấn nút **Thêm**.
5. Nhập địa chỉ IP, dải địa chỉ IP hoặc tên của các máy tính không được phép xử lý mã hóa từ bên ngoài. Ví dụ:
   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao → Anti-Cryptor**.
4. Trong mục **Loại trừ quét**, hãy nhấn nút **Theo tên hoặc địa chỉ IP**.
5. 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 nút → **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.

6. Để nhập danh sách loại trừ:

a. Nhấn nút → **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.

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 **Asset management** → **Policies**.

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 **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.

5. Nhấn vào liên kết **Exclusions by name or IP address**.

6. Để xuất danh sách quy tắc:

a. Chọn các loại trừ mà bạn muốn xuất.

b. Nhấn nút → **Export**.

Kaspersky Endpoint Security sẽ xuất danh sách các loại trừ vào tập tin JSON trong thư mục tải xuống mặc định.

7. Để nhập danh sách loại trừ:

a. Nhấn nút → **Import**.

Trong cửa sổ mở ra, hãy chọn tập tin JSON mà bạn muốn nhập danh sách các loại trừ.

b. 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 JSON.

8. Lưu các thay đổi của bạn.

Công cụ khắc phục

Thành phần 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 phần mềm độc hại.

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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao → Công cụ khắc phục**.
4. Sử dụng hộp kiểm **Công cụ khắc phục** để bật hoặc tắt thành phần.
5. 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 **Asset management → Policies**.
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 **Host Threat Protection → Behavior Analysis → Remediation Engine**.
5. Sử dụng nút bật/tắt **Remediation Engine ENABLED** để bật hoặc tắt thành phần này.
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 mối đe dọa nâng cao → Công cụ khắc phục**.
3. Sử dụng nút bật/tắt **Công cụ khắc phục** để bật hoặc tắt thành phần này.
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.

Chức năng KSN có thể không khả dụng trong ứng dụng ở Hoa Kỳ.

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 tiếng của các địa chỉ web được quét, cũng như thông tin về danh mục và danh tiếng của các tập tin được quét. Để biết thêm chi tiết về cách cấu hình quyền truy cập vào KSN, hãy tham khảo Trợ giúp Kaspersky Security Center.

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.

Cơ sở hạ tầng cơ sở dữ liệu danh tiếng của Kaspersky

Kaspersky Endpoint Security hỗ trợ các giải pháp cơ sở hạ tầng sau để làm việc với cơ sở dữ liệu danh tiếng của Kaspersky:

- *Kaspersky Security Network (KSN)* là giải pháp được hầu hết các ứng dụng Kaspersky sử dụng. Người tham gia vào KSN sẽ nhận thông tin từ Kaspersky 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.
- *Kaspersky Private Security Network (KPSN)* 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 và truy cập các dữ liệu thống kê khác mà không cần gửi dữ liệu cho Kaspersky từ máy tính của riêng họ. KPSN được thiết kế dành cho khách hàng doanh nghiệp, là những khách hàng 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.

Bật và tắt sử dụng Kaspersky Security Network

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.

Cách bật hoặc tắt Sử dụng KSN trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao → Kaspersky Security Network**.

4. Sử dụng nút bật/tắt **Kaspersky Security Network** để bật hoặc tắt thành phần này.

   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.

5. Nếu cần, hãy xóa hộp kiểm **Bật chế độ KSN mở rộng**. Theo mặc định, chế độ KSN mở rộng đang được bật.

6. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật hoặc tắt Sử dụng KSN trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Policies**.

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 → Kaspersky Security Network**.

5. Sử dụng nút bật/tắt **Use of Kaspersky Security Network (KSN) ENABLED** để bật hoặc tắt thành phần này.

   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.

6. Nếu cần, hãy tắt **Use extended KSN mode**. Theo mặc định, chế độ KSN mở rộng đang được bật.

7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật hoặc tắt Sử dụng KSN 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 → Kaspersky Security Network**.

3. Sử dụng nút bật/tắt **Kaspersky Security Network** để bật hoặc tắt thành phần này.

   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.

4. Nếu cần, hãy tắt **Bật chế độ KSN mở rộng**. Theo mặc định, chế độ KSN mở rộng đang được bật.

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 Kaspersky Private Security Network

Kaspersky Private Security Network (KPSN) 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 và truy cập các dữ liệu thống kê khác mà không cần gửi dữ liệu cho Kaspersky từ máy tính của riêng họ. Kaspersky Private Security Network 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 tin tưởng* trong cơ sở dữ liệu danh tiếng cục bộ nhưng có danh tiếng *Tin tưởng* trong KSN/KPSN thì Kaspersky Endpoint Security sẽ phát hiện tập tin là *Không 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 mối đe dọa tập tin.

- Kaspersky Endpoint Security ở chế độ Light Agent giao tiếp với Máy chủ KSN thông qua một máy chủ proxy KSN. Không hỗ trợ giao tiếp trực tiếp với KSN.

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.

Nếu ứng dụng đang hoạt động trong Chế độ Light Agent thì Chế độ đám mây sẽ không khả dụng.

Cách bật hoặc tắt chế độ đám mây cho các thành phần bảo vệ trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao → Kaspersky Security Network**.
4. Sử dụng hộp kiểm **Bật chế độ đám mây** để bật hoặc tắt thành phần.
5. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật hoặc tắt chế độ đám mây cho các thành phần 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 **Asset management → Policies**.
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 → Kaspersky Security Network**.
5. Sử dụng nút bật/tắt **Use cloud mode** để bật hoặc tắt thành phần này.
6. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật hoặc tắt chế độ đám mây cho các thành phần 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 → 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 theo cách trực tiếp hoặc thông qua dịch vụ KSN Proxy.

Nếu ứng dụng đang chạy ở Chế độ Light Agent thì giao tiếp trực tiếp với KSN không được hỗ trợ. Kaspersky Endpoint Security giao tiếp với máy chủ KSN thông qua máy chủ proxy KSN.

Dịch vụ KSN Proxy cung cấp các khả 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 KSN Proxy 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 KSN Proxy như sau: bật hoặc tắt KSN Proxy và cấu hình cổng cho kết nối. Để thực hiện, bạn cần mở thuộc tính Máy chủ quản trị. Để biết thêm chi tiết về việc cấu hình KSN Proxy, hãy tham khảo Trợ giúp Kaspersky Security Center. Bạn cũng có thể bật hoặc tắt KSN Proxy 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 cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Bảo vệ mối đe dọa nâng cao → Kaspersky Security Network**.
4. Trong mục **Thiết lập Proxy KSN**, hãy sử dụng hộp kiểm **Sử dụng Máy chủ quản trị làm máy chủ proxy KSN** để bật hoặc tắt KSN Proxy.

5. Nếu cần, hãy chọn hộp kiểm **Sử dụng các máy chủ Kaspersky Security Network nếu máy chủ proxy KSN không khả dụng**.

   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 và trên một bên thứ ba (khi Kaspersky Private Security Network được sử dụng).

6. 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 **Asset management** → **Policies**.

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** → **Kaspersky Security Network**.

5. Sử dụng hộp kiểm **Use Administration Server as a KSN proxy server** để bật hoặc tắt KSN Proxy.

6. Nếu cần, hãy chọn hộp kiểm **Use Kaspersky Security Network servers if the KSN proxy server is unavailable**.

   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 và trên một bên thứ ba (khi Kaspersky Private Security Network được sử dụng). Theo mặc định, hộp kiểm này bị xóa.

7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Địa chỉ KSN Proxy khớp với địa chỉ Máy chủ quản trị. Khi tên miền Máy chủ quản trị được thay đổi, bạn cần cập nhật địa chỉ KSN Proxy theo cách thủ công.

Để cấu hình địa chỉ Proxy KSN:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.

2. Trong cây bảng điều khiển, hãy chọn thư mục **Advanced** → **Remote installation** → **Installation packages**.

3. Trong menu ngữ cảnh của thư mục **Installation packages**, hãy chọn **Properties**.

4. Trên thẻ **General** trong cửa sổ được mở, hãy chỉ định địa chỉ mới của máy chủ Proxy KSN.

5. Lưu các thay đổi của bạn.

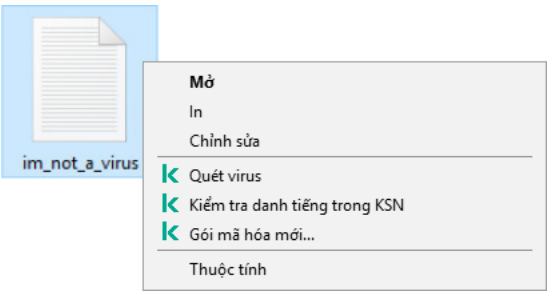
Kiểm tra danh tiếng của một tập tin trong Kaspersky Security Network

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). Ứng dụng sẽ coi một tập tin là được tin tưởng nếu đáp ứng một hoặc nhiều điều kiện sau:

- tập tin được ký kỹ thuật số bởi nhà cung cấp được tin tưởng;
- tập tin có danh tiếng được tin tưởng trong Kaspersky Security Network;
- người dùng đã đưa tập tin vào trong nhóm Được tin tưởng.

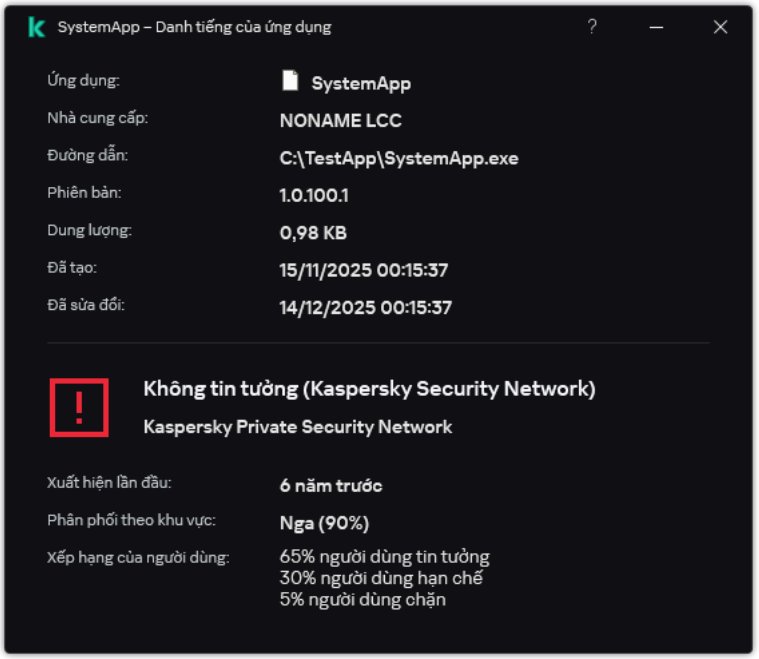
Phần mềm hợp pháp có thể bị kẻ xâm nhập sử dụng làm hư hại máy tính của bạn hoặc dữ liệu cá nhân. Mặc dù chúng không có chức năng độc hại nào, nhưng các ứng dụng đó vẫn có thể bị kẻ xâm nhập khai thác. Để xem chi tiết về các phần mềm hợp pháp có thể bị bọn tội phạm lợi dụng để gây hại cho máy tính hoặc 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: *Kaspersky Security Network* hoặc *Kaspersky Private Security Network*.

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 mối đe dọa thư điện tử, Bảo vệ mối đe dọa web, Phát hiện hành vi và Phòng chống khai thác 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

Theo mặc định, không phải lúc nào Kaspersky Endpoint Security cũng quét các kết nối được mã hóa mà chỉ quét khi được các thành phần bảo vệ yêu cầu.

Cách bật các kết nối 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, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Thiết lập mạng**.
5. Trong mục **Quét kết nối được mã hóa**, hãy chọn chế độ quét kết nối được mã hóa:
   - **Quét các kết nối 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 mối đe dọa web, 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.

   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.
6. Nếu cần, hãy thêm loại trừ quét: địa chỉ và ứng dụng được tin tưởng.
7. Cấu hình thiết lập để quét các kết nối được mã hóa (xem bảng bên dưới).
8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật các kết nối được mã hóa trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.
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** → **Network Settings**.
5. Trong mục **Encrypted Connections Scan**, hãy bật nút gạt **Encrypted Connections Scan ENABLED**.
   Nếu nút bật/tắt bị tắt, Kaspersky Endpoint Security sẽ không có quyền truy cập vào nội dung của các trang web có địa chỉ bắt đầu bằng `https://`.

6. Nhấn vào **Settings** và chọn chế độ quét kết nối được mã hóa:

   - **Scan encrypted connections upon request from protection components**. Kaspersky Endpoint Security sẽ chỉ quét lưu lượng được mã hóa khi được yêu cầu bởi các thành phần Bảo vệ mối đe dọa web, Bảo vệ mối đe dọa thư điện tử và Kiểm soát Web.

   - **Always scan encrypted connections**. 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.

7. Nếu cần, hãy thêm loại trừ quét: địa chỉ và ứng dụng được tin tưởng.

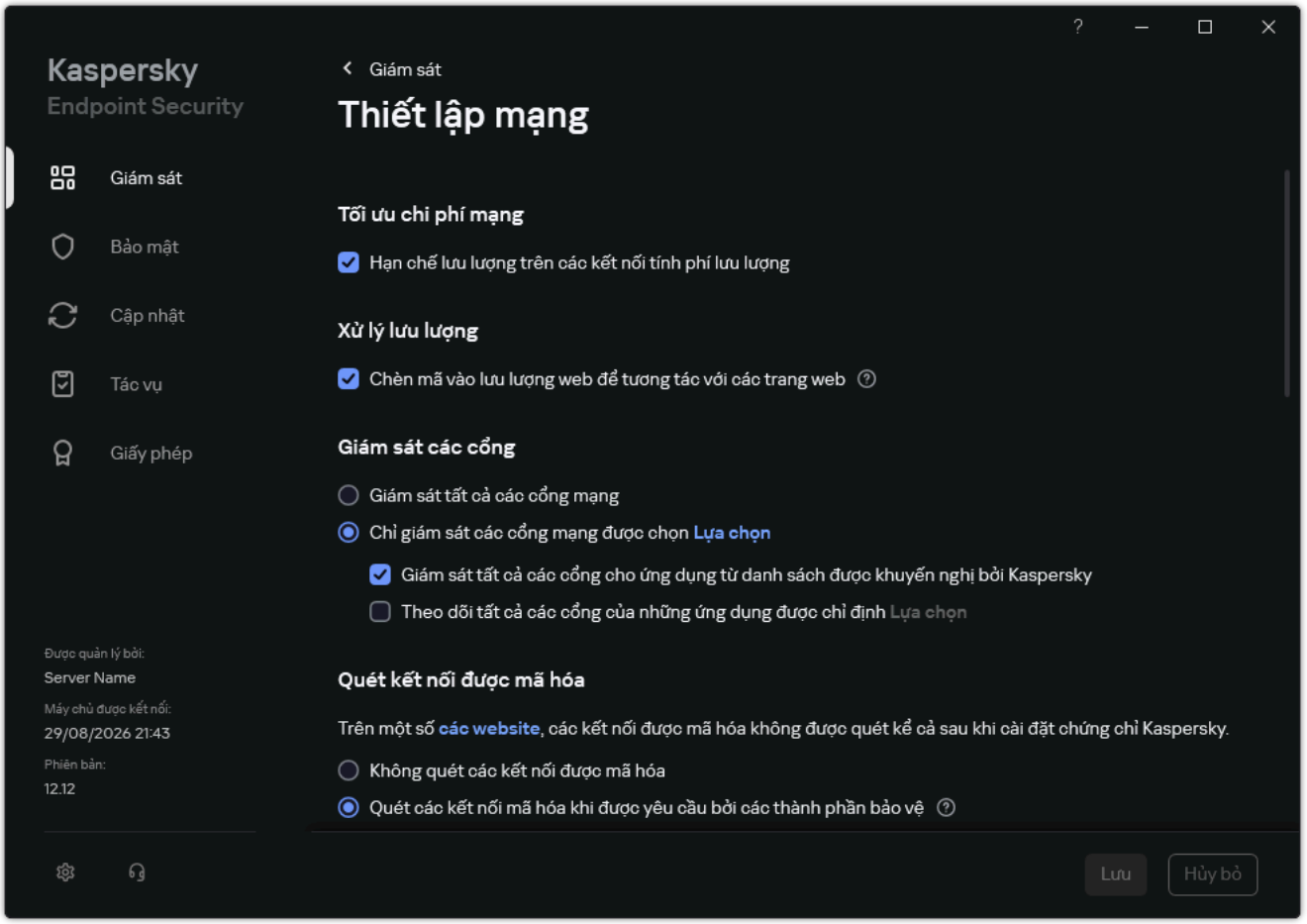
8. Cấu hình thiết lập để quét các kết nối được mã hóa (xem bảng bên dưới).

9. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật các kết nối được mã hóa 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**.



Thiết lập quét các kết nối được mã hóa

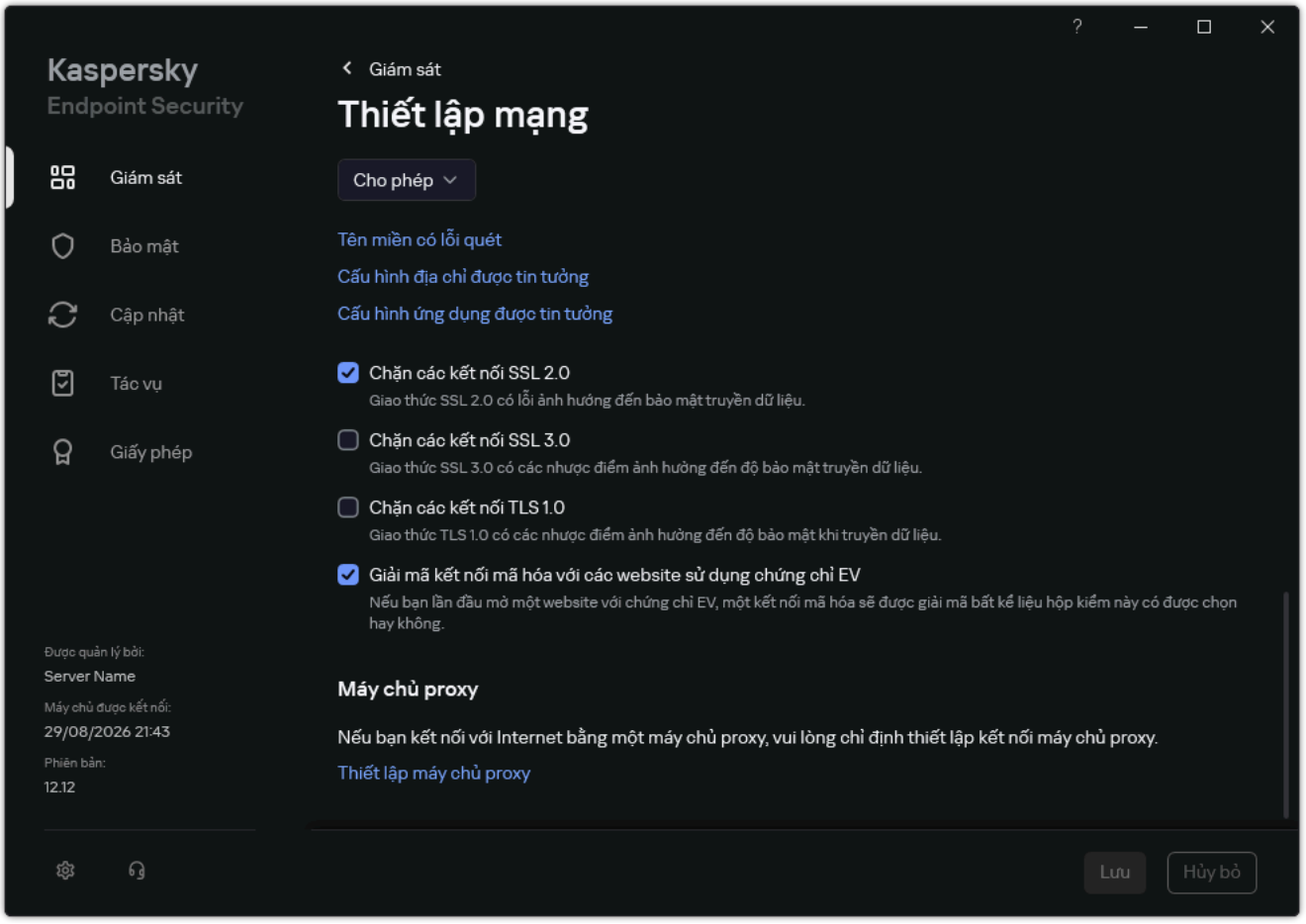
3. Trong mục **Quét kết nối được mã hóa**, hãy chọn chế độ quét kết nối được mã hóa:

- **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 mối đe dọa web, 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.

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).



Thiết lập bổ sung để quét các kết nối được mã hóa

6. Lưu các thay đổi của bạn.

Tham số	Mô tả
Chứng chỉ gốc được tin tưởng	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.
Truy cập một tên miền bằng chứng chỉ không được tin tưởng	• **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 *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. • **Chặn**. 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.
Truy cập một miền có lỗi quét kết nối được mã hóa	• **Chặn**. Nếu một lỗi quét kết nối được mã hóa xảy ra, Kaspersky Endpoint Security sẽ chặn kết nối mạng. • **Cho phép và thêm miền vào loại trừ**. Nếu một lỗi quét kết nối được mã hóa xảy ra, 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**. 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	Nếu hộp kiểm này được chọn, ứng dụng sẽ giám sát và chặn các kết nối mạng được thiết lập qua giao thức SSL 2.0. Nếu hộp kiểm này bị xóa, ứng dụng sẽ không chặn các kết nối mạng được thiết lập qua giao thức SSL 2.0. Tuy nhiên, ứng dụng không giám sát lưu lượng mạng qua giao thức này.
Chặn các kết nối SSL 3.0	Nếu hộp kiểm này được chọn, ứng dụng sẽ chặn các kết nối mạng được thiết lập qua giao thức SSL 3.0. Nếu hộp kiểm này bị xóa, ứng dụng sẽ không chặn các kết nối mạng được thiết lập qua giao thức SSL 3.0. Ứng dụng sẽ giám sát lưu lượng mạng qua giao thức này. Mọi thành phần của ứng dụng đều hoạt động mà không có hạn chế.
Chặn các kết nối TLS 1.0	Nếu hộp kiểm này được chọn, ứng dụng sẽ chặn các kết nối mạng được thiết lập qua giao thức TLS 1.0. Nếu hộp kiểm này bị xóa, ứng dụng sẽ không chặn các kết nối mạng được thiết lập qua giao thức TLS 1.0. Ứng dụng sẽ giám sát lưu lượng mạng qua giao thức này. Mọi thành phần của ứng dụng đều hoạt động mà không có hạn chế.
Giải mã kết nối mã hóa với các website sử dụng chứng chỉ EV	Các chứng chỉ EV (Extended Validation Certificate) sẽ xác nhận tính xác thực của các trang web 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. Nếu hộp kiểm được chọn, ứng dụng sẽ giải mã và giám sát các kết nối được mã hóa với các website sử dụng chứng chỉ EV. Nếu hộp kiểm này không được chọn, ứng dụng 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Thiết lập mạng**.
4. Trong mục **Chứng chỉ gốc được tin tưởng**, hãy nhấn nút **Thêm**.
5. 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.
6. Lưu các thay đổi của bạn.

Cách cài đặt chứng chỉ gốc được tin tưởng trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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** → **Network Settings**.
5. Nhấn vào liên kết **Trusted root certificates**.
6. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy nhấn vào **Add** 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 nút **Hiện 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.

  > Về mặt kỹ thuật, trong một số trường hợp, Kaspersky Endpoint Security không thể hiển thị trang HTML có cảnh báo trong trình duyệt (xem hình bên dưới). Ví dụ: nếu tài nguyên web sử dụng phiên bản lỗi thời của giao thức mạng và cổng không chuẩn. Trong những trường hợp này, Kaspersky Endpoint Security sẽ chặn quyền truy cập miền này và trình duyệt sẽ hiển thị cửa sổ `ERR_CONNECTION_RESET` tiêu chuẩn. Để truy cập một tài nguyên web, bạn có thể thêm tên miền vào danh sách loại trừ hoặc sử dụng chứng chỉ 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Thiết lập mạng**.
4. Trong mục **Quét kết nối được mã hóa**, hãy nhấn nút **Thiết lập nâng cao**.
5. Trong cửa sổ mở ra, hãy chọn chế độ vận hành ứng dụng khi truy cập miền có chứng chỉ không được tin tưởng: **Cho phép** or **Chặn**.
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 Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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** → **Network Settings**.
5. Trong mục **Encrypted Connections Scan**, hãy nhấn liên kết **Settings**.
6. Trong cửa sổ mở ra, hãy chọn chế độ vận hành ứng dụng khi truy cập miền có chứng chỉ không được tin tưởng: **Allow connection** or **Block connection**.
7. 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 miền có chứng chỉ không được tin tưởng: **Cho phép** hoặc **Chặn**.

4. Lưu các thay đổi của bạn.



Cảnh báo về việc truy cập một tên miền có chứng chỉ không được tin tưởng

Thêm chứng chỉ Kaspersky vào kho chứng chỉ riêng

Trình duyệt và ứng dụng thư sử dụng chứng chỉ để xác minh tính bảo mật và tính xác thực của tài nguyên web. Chứng chỉ cũng cung cấp mã hóa dữ liệu giữa tài nguyên web và người dùng. Hầu hết các trình duyệt và ứng dụng thư đều sử dụng kho chứng chỉ được tin tưởng (kho chứng chỉ Windows). Ví dụ: Google Chrome. Theo mặc định, một số trình duyệt và ứng dụng thư sử dụng kho chứng chỉ riêng thay vì kho chứng chỉ Windows. Ví dụ: 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). 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 các trình duyệt và ứng dụng thư 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 trình duyệt và ứng dụng thư sử dụng. Nếu bạn đã chọn kho chứng chỉ của riêng mình, hãy thêm chứng chỉ Kaspersky vào kho chứng chỉ 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, ứng dụng sẽ không quét lưu lượng được mã hóa trong trình duyệt Mozilla Firefox và ứng dụng thư điện tử Thunderbird. Cũng phải bật quét kết nối được mã hóa để quét lưu lượng truy cập trong ứng dụng thư MyOffice Mail và R7-Office Organizer.

Trước khi thêm chứng chỉ vào kho chứng chỉ riêng của trình duyệt hoặc tác nhân thư điện tử, hãy xuất chứng chỉ Kaspersky từ Bảng điều khiển Windows (thuộc tính Internet). Bạn có thể tìm hiểu thêm về cách thêm chứng chỉ vào kho, ví dụ: trên 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 kho chứng chỉ để quét các kết nối được mã hóa trong trình duyệt và ứng dụng thư:

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 hộp kiểm **Để quét kết nối được mã hóa trong các ứng dụng có kho chứng chỉ riêng, hãy sử dụng**.
4. Chọn kho chứng chỉ:
   - **Kho chứng chỉ Windows (khuyên dùng)**. Chứng chỉ gốc của Kaspersky được thêm vào kho này trong quá trình cài đặt Kaspersky Endpoint Security.
   - **Kho chứng chỉ riêng**. 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.

     Ứng dụng thư MyOffice Mail và R7-Office Organizer cũng sử dụng kho chứng chỉ riêng.
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*. 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 mối đe dọa web, Bảo vệ mối đe dọa thư điện tử và Kiểm soát web đang hoạt động.

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.

Cách loại trừ địa chỉ web khỏi các tác vụ quét kết nối 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, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Thiết lập mạng**.
5. Trong mục **Quét kết nối được mã hóa**, hãy nhấn nút **Cấu hình địa chỉ được tin tưởng**.
6. Nhấn vào **Thêm**.
7. 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 biểu tượng `*` cho các địa chỉ IP. Bạn có thể chọn một dải địa chỉ IP bằng cách sử dụng mặt nạ mạng con (ví dụ: 198.51.100.0/24).

Ví dụ:

- `domain.com` – 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`).
- `subdomain.domain.com` –bản ghi này bao gồm các địa chỉ sau: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Bản ghi không bao gồm tên miền `domain.com`.
- `*.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`.

8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách loại trừ địa chỉ web khỏi các tác vụ quét kết nối được mã hóa trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.
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** → **Network Settings**.
5. Trong mục **Encrypted Connections Scan**, hãy nhấn nút **Trusted domains**.
6. Nhấn vào **Add**.
7. 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 biểu tượng `*` cho các địa chỉ IP. Bạn có thể chọn một dải địa chỉ IP bằng cách sử dụng mặt nạ mạng con (ví dụ: 198.51.100.0/24).

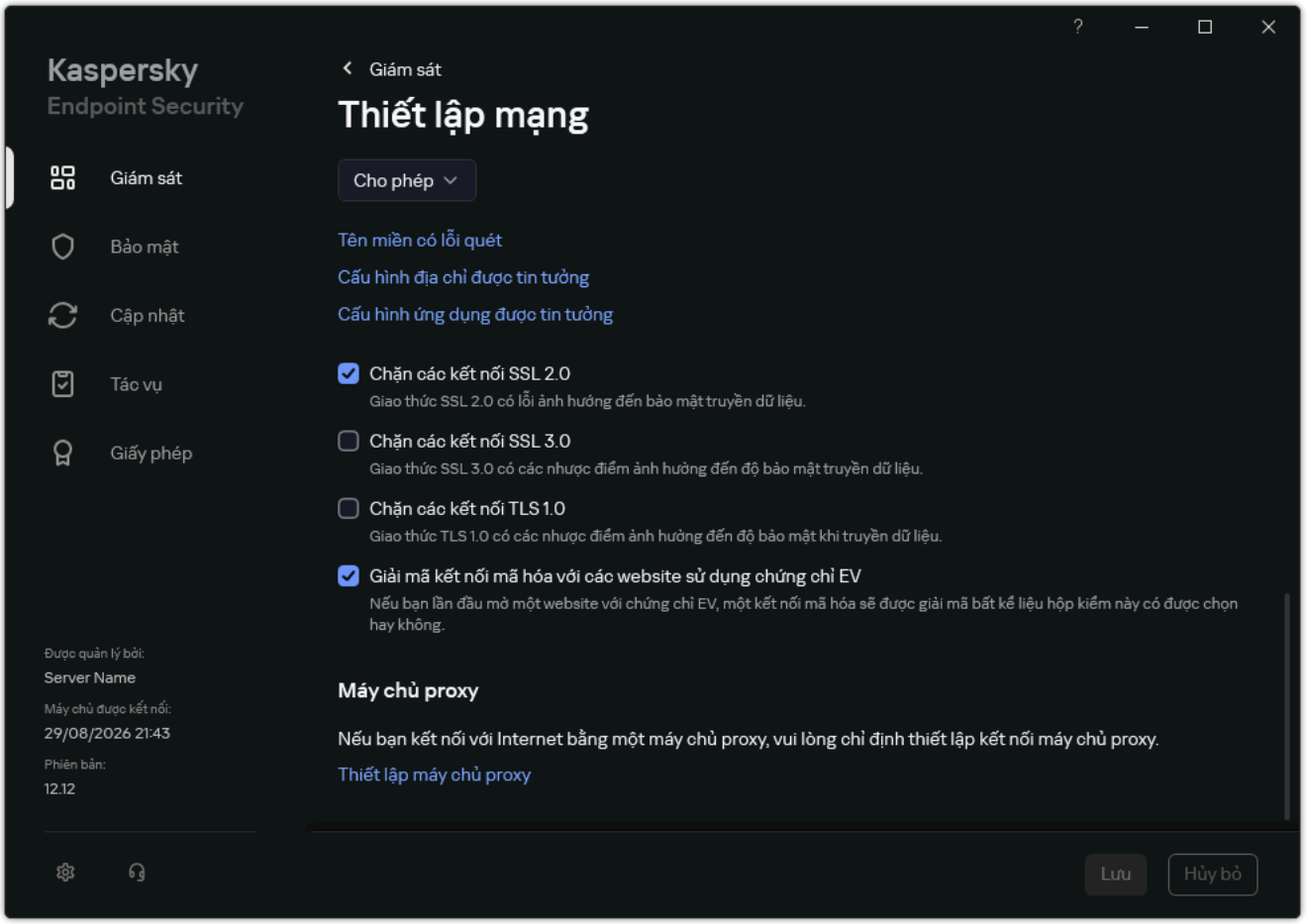
Ví dụ:

- `domain.com` – 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`).
- `subdomain.domain.com` –bản ghi này bao gồm các địa chỉ sau: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Bản ghi không bao gồm tên miền `domain.com`.
- `*.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`.

8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách loại trừ địa chỉ web khỏi các tác vụ quét kết nối được mã hóa 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**.



Thiết lập mạng của ứng dụng

3. Trong mục **Quét kết nối được mã hóa**, hãy nhấn nút **Cấu hình 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 biểu tượng `*` cho các địa chỉ IP. Bạn có thể chọn một dải địa chỉ IP bằng cách sử dụng mặt nạ mạng con (ví dụ: 198.51.100.0/24).

Ví dụ:

- `domain.com` – 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`).
- `subdomain.domain.com` –bản ghi này bao gồm các địa chỉ sau: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Bản ghi không bao gồm tên miền `domain.com`.
- `*.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.

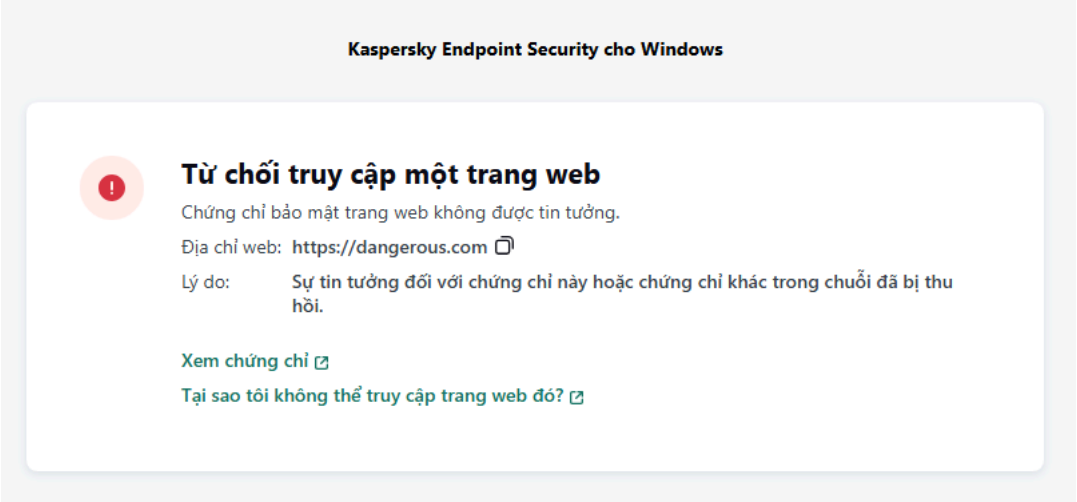
Chặn truy cập vào các tên miền có chứng chỉ không được tin tưởng

Trong một số trường hợp, khi chặn truy cập vào một tên miền có chứng chỉ không được tin tưởng, Kaspersky Endpoint Security sẽ hiển thị một trang cảnh báo HTML trong trình duyệt, nhưng trang này lại thiếu liên kết đến tài nguyên web được yêu cầu.

Sự cố này có thể xảy ra vì những lý do sau:

- Quản trị viên đã chặn truy cập vào một tên miền có chứng chỉ không được tin tưởng.
- Tên miền có chứng chỉ không được tin tưởng hoặc không hợp lệ và máy chủ web sử dụng cơ chế HTTP Strict Transport Security (HSTS). *HSTS* là một cơ chế bảo mật nhằm đảm bảo việc sử dụng giao thức HTTPS bảo mật để liên lạc giữa máy khách và máy chủ web. Trong trường hợp này, bạn không thể truy cập vào tên miền ngay cả khi đã thêm vào danh sách địa chỉ được tin tưởng. Cơ chế HSTS được mô tả trong RFC 6797.

  Trong một số trường hợp, trang web có thể được mở trực tiếp trong trình duyệt mà không cần sử dụng Kaspersky Endpoint Security. Trình duyệt không phải lúc nào cũng phát hiện được chứng chỉ bị thu hồi, trong khi Kaspersky Endpoint Security thực hiện kiểm tra trực tuyến việc thu hồi chứng chỉ khi thiết lập kết nối. Điều này cho phép ứng dụng phát hiện vấn đề về chứng chỉ trước khi trình duyệt phát hiện và hiển thị thông báo lỗi tương ứng.



Cảnh báo về việc truy cập một tên miền có chứng chỉ không được tin tưởng

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 mắt 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 vũ 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 **Tasks**.

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **Add**.

   Trình hướng dẫn Tác vụ sẽ được bắt đầu.

3. Cấu hình các thiết lập của tác vụ:

   a. Trong danh sách thả xuống **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.

   b. Trong danh sách thả xuống **Task type**, hãy chọn **Wipe data**.

   c. Trong trường **Task name**, nhập một mô tả ngắn, ví dụ như *Xóa sạch dữ liệu (Chống mất cắp)*.

   d. Trong phần **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. Hoàn tất trình hướng dẫn.

   Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ.

6. Nhấn vào tác vụ **Wipe data** của 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:

   - **Delete by means of the operating system**. Kaspersky Endpoint Security sẽ sử dụng các tài nguyên của hệ điều hành để xóa tập tin mà không gửi chúng vào thùng rác.
   - **Delete completely, no recovery possible**. 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 **Automatically wipe data when there is no connection to Kaspersky Security Center for more than N days**. 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 trì hoãn, hãy lưu ý rằng nhân viên có thể có lịch làm việc khác nhau. 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 máy tính tắt nguồn và mất kết nối trong thời gian dài hơn thời gian đã cấu hình, sau khi bật máy tính, Kaspersky Endpoint Security sẽ không xóa dữ liệu ngay lập tức. Ứng dụng sẽ chờ đồng bộ hóa với Kaspersky Security Center trong một giờ. Đây là điều cần thiết để ngăn xóa dữ liệu trái phép trên máy tính của người dùng đã tắt máy tính, ví dụ như trước khi đi nghỉ.

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.
  - **Temporary Internet Explorer files**. 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.
  - **Temporary files**. 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.
  - **Outlook files**. 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).
  - **User profile**. 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 **Start**.

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).

Để sử dụng Kiểm soát web, bạn phải hoàn tất cấu hình ban đầu của ứng dụng:

- Để giám sát lưu lượng HTTPS, hãy bật kết nối được mã hóa quét (được bật theo mặc định).
- Chọn các cổng mà Kaspersky Endpoint Security phải giám sát (theo mặc định, ứng dụng sẽ giám sát tất cả các cổng).
- Chọn các ứng dụng có lưu lượng mà bạn muốn Kaspersky Endpoint Security giám sát. Hầu hết các trình duyệt đã có trong danh sách ứng dụng đều được Kaspersky khuyên dùng. Hãy thêm theo cách thủ công nếu trình duyệt của bạn không có trong danh sách.
- Bạn nên chèn một tập lệnh tương tác trang web vào lưu lượng truy cập web (chèn tập lệnh bị tắt theo mặc định). 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.

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 ẩn các ảnh. 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 *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 *Các tập tin ứng dụng văn phòng* chỉ với danh mục website *Email 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.

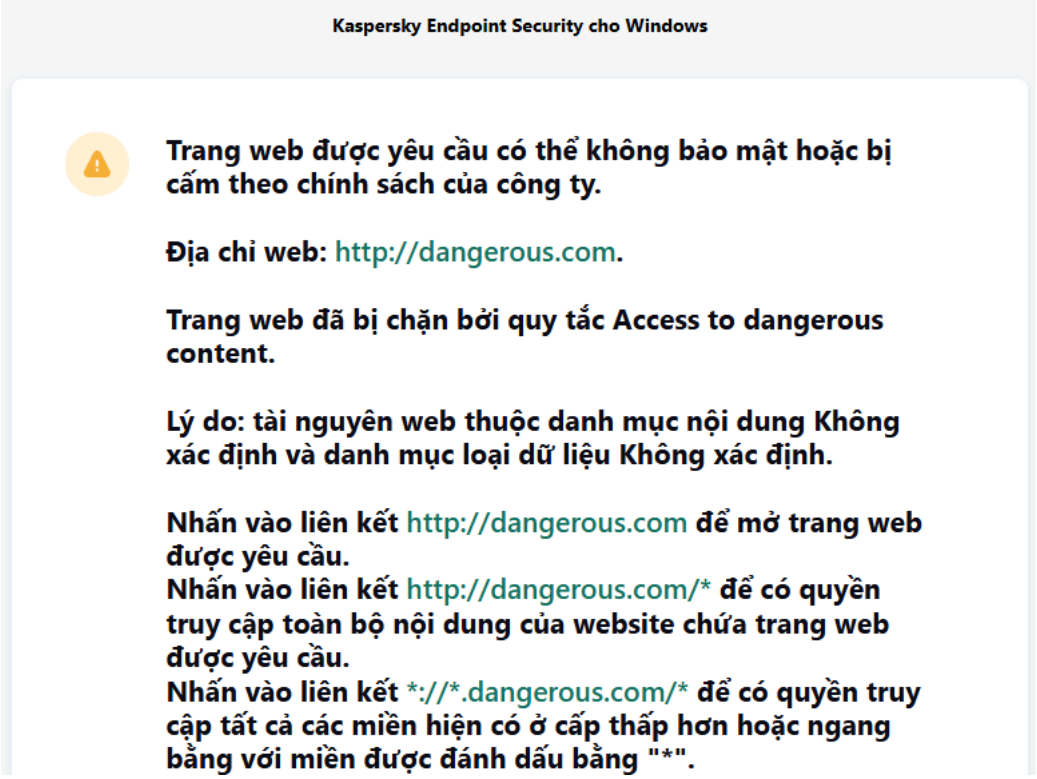
- Lịch quy tắc.

  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.





Thông báo của Kiểm soát Web

Bổ sung một quy tắc truy cập tài nguyên web

Một *quy tắc truy cập tài nguyên web* là một tập hợp các bộ lọc và hành động Kaspersky Endpoint Security được áp dụng khi người dùng truy cập tài nguyên web. Quy tắc truy cập có thể bao gồm một lịch quy tắc.

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 trống. *Quy tắc mặc định* được cài sẵn. Quy tắc này được áp dụng cho mọi tài nguyên web không được bao gồm bởi các quy tắc khắc, và cho phép hoặc chặn truy cập của tất cả người dùng đến các tài nguyên web này.

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.

Cách thêm một quy tắc truy cập tài nguyên web trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật → Kiểm soát Web**.

4. Chọn hộp kiểm **Kiểm soát Web**.

5. Trong mục **Thiết lập Kiểm soát Web**, hãy nhấn nút **Thêm**.

   Cửa sổ **Quy tắc truy cập tài nguyên web** sẽ mở ra.

6. Cấu hình quy tắc truy cập tài nguyên web (xem bảng bên dưới).

7. Nếu bạn muốn Kiểm soát web chấm dứt kết nối với tài nguyên web bị cấm ngay sau khi áp dụng chính sách, hãy chọn hộp kiểm **Chấm dứt các phiên trình duyệt của người dùng đang hoạt động sau khi áp dụng quy tắc**.

   > Kiểm soát web chỉ cho phép ngắt kết nối ngay lập tức các tài nguyên web trong trình duyệt web. Đối với các ứng dụng khác, Kiểm soát web chỉ hạn chế các kết nối mới.

   Nếu bỏ chọn hộp kiểm này, Kiểm soát web sẽ chỉ hạn chế các kết nối mới tới các tài nguyên web bị cấm. Kiểm soát web không chấm dứt các kết nối đang hoạt động.

8. Lưu các thay đổi của bạn.

Cách thêm quy tắc truy cập tài nguyên web trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Security Controls** → **Web Control**.
5. Bật nút bật/tắt **Web Control ENABLED**.
6. Trong mục **Rules list**, hãy nhấn nút **Add**.
7. Cấu hình quy tắc truy cập tài nguyên web (xem bảng bên dưới).
8. Nếu bạn muốn Kiểm soát web chấm dứt kết nối với tài nguyên web bị cấm ngay sau khi áp dụng chính sách, hãy chọn hộp kiểm **Terminate active user browser sessions after the rule is applied**.

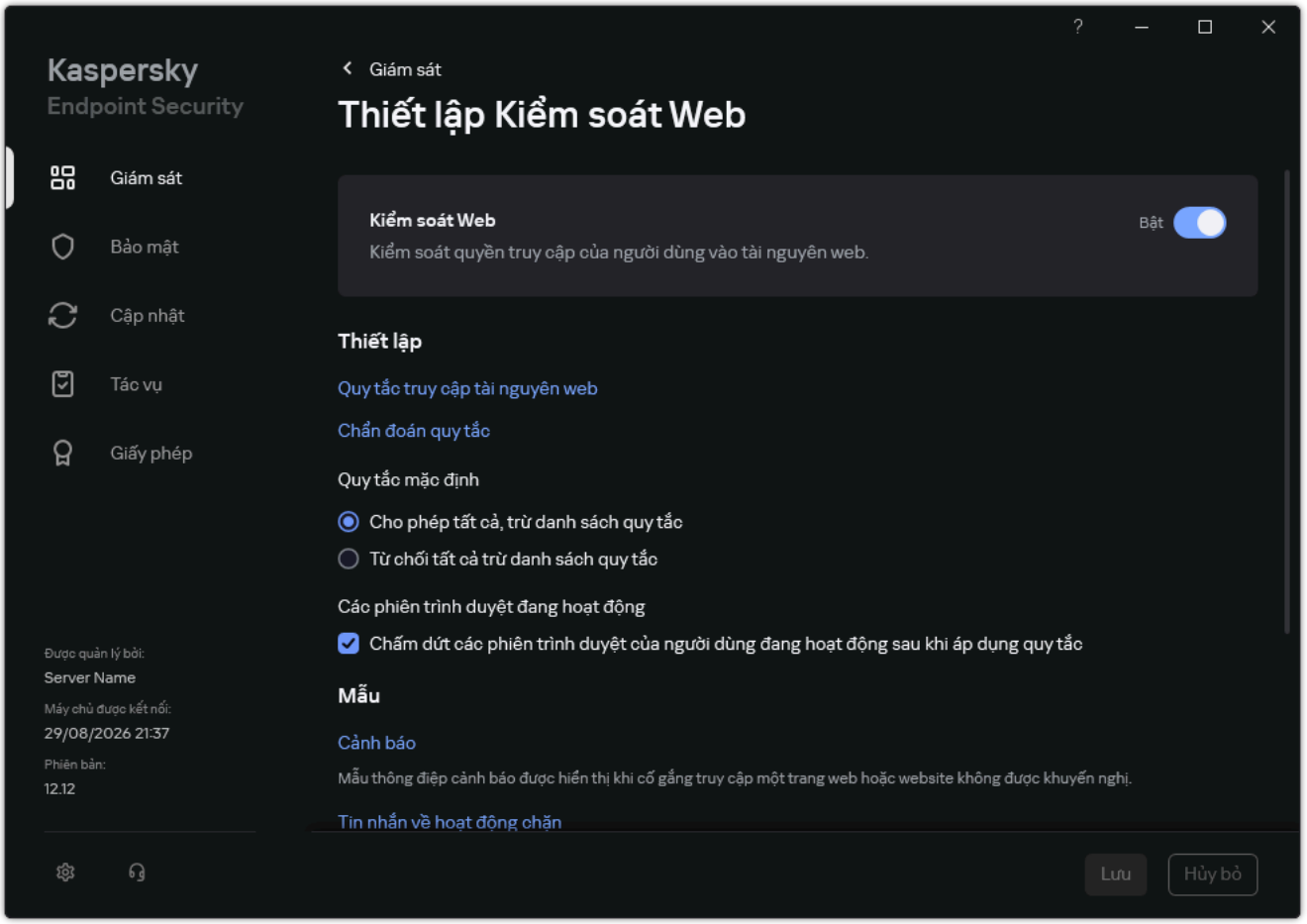
   > Kiểm soát web chỉ cho phép ngắt kết nối ngay lập tức các tài nguyên web trong trình duyệt web. Đối với các ứng dụng khác, Kiểm soát web chỉ hạn chế các kết nối mới.

   Nếu bỏ chọn hộp kiểm này, Kiểm soát web sẽ chỉ hạn chế các kết nối mới tới các tài nguyên web bị cấm. Kiểm soát web không chấm dứt các kết nối đang hoạt động.

9. Lưu các thay đổi của bạn.

Cách thêm quy tắc truy cập tài nguyên web 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 **Kiểm soát bảo mật → Kiểm soát Web**.



Thiết lập Kiểm soát web

3. Bật nút bật/tắt **Kiểm soát Web**.
4. Trong mục **Thiết lập**, hãy nhấn nút **Quy tắc truy cập tài nguyên web**.
5. Trong cửa sổ mở ra, hãy nhấn nút **Thêm**.
   Cửa sổ **Quy tắc truy cập tài nguyên web** sẽ mở ra.
6. Cấu hình quy tắc truy cập tài nguyên web (xem bảng bên dưới).
7. Nếu bạn muốn Kiểm soát web chấm dứt kết nối với tài nguyên web bị cấm ngay sau khi áp dụng chính sách, hãy chọn hộp kiểm **Chấm dứt các phiên trình duyệt của người dùng đang hoạt động sau khi áp dụng quy tắc**.

   > Kiểm soát web chỉ cho phép ngắt kết nối ngay lập tức các tài nguyên web trong trình duyệt web. Đối với các ứng dụng khác, Kiểm soát web chỉ hạn chế các kết nối mới.

   Nếu bỏ chọn hộp kiểm này, Kiểm soát web sẽ chỉ hạn chế các kết nối mới tới các tài nguyên web bị cấm. Kiểm soát web không chấm dứt các kết nối đang hoạt động.
8. Lưu các thay đổi của bạn.

Kết quả là quy tắc Kiểm soát web mới sẽ được thêm vào danh sách. Nếu cần, hãy thay đổi mức độ ưu tiên của quy tắc Kiểm soát web. Bạn cũng có thể sử dụng nút bật/tắt để tắt quy tắc truy cập tài nguyên web bất kỳ lúc nào mà không cần xóa quy tắc đó khỏi danh sách.

Tham số của quy tắc Kiểm soát web

Tham số	Mô tả
Tên quy tắc	Tên của quy tắc Kiểm soát web.
Trạng thái	• **Bật**. • **Tắt**. Bạn có thể sử dụng nút bật/tắt để tắt quy tắc truy cập tài nguyên web bất kỳ lúc nào.
Hành động	• **Cho phép**. Kiểm soát web cho phép truy cập tài nguyên web phù hợp với các tham số của quy tắc. • **Chặn**. Kiểm soát web chặn truy cập các tài nguyên web phù hợp với các tham số của quy tắc và hiển thị thông báo từ chối truy cập trang web. • **Cảnh báo**. Khi người dùng cố lấy quyền truy cập tài nguyên web phù hợp với quy tắc, Kiểm soát web sẽ hiển thị cảnh báo rằng không nên truy cập tài nguyên web. Qua việc sử dụng các liên kết trong cảnh báo, người dùng có thể yêu cầu quyền truy cập đến tài nguyên web này.
Nội dung của bộ lọc	• **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: *Đồ họa*).
Địa chỉ	• **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. 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. Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền. Nếu Quét các kết nối đã được mã hóa bị tắt, bạn chỉ có thể lọc theo tên máy chủ cho giao thức HTTPS.
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. Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.
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. Ví dụ như bạn có thể chỉ hạn chế truy cập Internet thông qua một trình duyệt trong giờ làm việc.

Lọc theo địa chỉ tài nguyên web

Để kiểm soát quyền truy cập các tài nguyên web riêng lẻ, bạn phải tạo quy tắc Kiểm soát web, tạo danh sách địa chỉ web và chọn hành động Kiểm soát web. Khi tạo danh sách địa chỉ web, bạn có thể nhập địa chỉ URL hoặc sử dụng địa chỉ đại diện.

Quy tắc có thể bao gồm lịch quy tắc và danh sách người dùng áp dụng quy tắc. Ví dụ: bạn có thể chỉ cho phép truy cập các trang web trong giờ làm việc hoặc cho phép truy cập trang web đối với người dùng trong một số nhóm nhất định.

Cách bật bộ lọc địa chỉ tài nguyên web trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật → Kiểm soát Web**.

4. Chọn hộp kiểm **Kiểm soát Web**.

5. Trong mục **Thiết lập Kiểm soát Web**, hãy nhấn nút **Thêm**.
   Cửa sổ **Quy tắc truy cập tài nguyên web** sẽ mở ra.

6. Cấu hình quy tắc truy cập tài nguyên web:

   a. Trong trường **Tên**, hãy nhập tên của quy tắc.

   b. Trong danh sách thả xuống **Áp dụng cho địa chỉ**, hãy chọn **Đến các địa chỉ được chỉ định**.

   c. Tạo một danh sách các 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.

      Nếu Quét các kết nối đã được mã hóa bị tắt, bạn chỉ có thể lọc theo tên máy chủ cho giao thức HTTPS.

   d. Trong danh sách thả xuống **Áp dụng cho người dùng**, hãy chọn bộ lọc phù hợp cho người dùng:

      - **Cho tất cả người dùng**. Kiểm soát Web sẽ không lọc tài nguyên web theo địa chỉ.
      - **Cho người dùng cá nhân hoặc nhóm**. Kiểm soát Web sẽ chỉ lọc các địa chỉ tài nguyên web trong danh sách. 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. Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.

   e. Trong danh sách thả xuống **Hành động** hãy chọn một tùy chọn:

      - **Cho phép**. Kiểm soát web cho phép truy cập tài nguyên web phù hợp với các tham số của quy tắc.
      - **Chặn**. Kiểm soát web chặn truy cập các tài nguyên web phù hợp với các tham số của quy tắc và hiển thị thông báo từ chối truy cập trang web.
      - **Cảnh báo**. Khi người dùng cố lấy quyền truy cập tài nguyên web phù hợp với quy tắc, Kiểm soát web sẽ hiển thị cảnh báo rằng không nên truy cập tài nguyên web. Qua việc sử dụng các liên kết trong cảnh báo, người dùng có thể yêu cầu quyền truy cập đến tài nguyên web này.

   f. Trong danh sách thả xuống **Lịch quy tắc**, hãy chọn một lịch hoặc tạo một lịch mới.

7. Nếu bạn muốn Kiểm soát web chấm dứt kết nối với tài nguyên web bị cấm ngay sau khi áp dụng chính sách, hãy chọn hộp kiểm **Chấm dứt các phiên trình duyệt của người dùng đang hoạt động sau khi áp dụng quy tắc**.

   Kiểm soát web chỉ cho phép ngắt kết nối ngay lập tức các tài nguyên web trong trình duyệt web. Đối với các ứng dụng khác, Kiểm soát web chỉ hạn chế các kết nối mới.

Nếu bỏ chọn hộp kiểm này, Kiểm soát web sẽ chỉ hạn chế các kết nối mới tới các tài nguyên web bị cấm. Kiểm soát web không chấm dứt các kết nối đang hoạt động.

8. Lưu các thay đổi của bạn.

Cách bật bộ lọc địa chỉ tài nguyên web trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Security Controls** → **Web Control**.
5. Bật nút bật/tắt **Web Control ENABLED**.
6. Trong mục **Rules list**, hãy nhấn nút **Add**.
7. Cấu hình quy tắc truy cập tài nguyên web:

   a. Trong trường **Rule name**, hãy nhập tên của quy tắc.

   b. Chọn trạng thái **Enabled** 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 mà không cần xóa quy tắc đó khỏi danh sách.

   c. Trong mục **Action**, hãy chọn tùy chọn liên quan:

   - **Allow**. Kiểm soát web cho phép truy cập tài nguyên web phù hợp với các tham số của quy tắc.
   - **Block**. Kiểm soát web chặn truy cập các tài nguyên web phù hợp với các tham số của quy tắc và hiển thị thông báo từ chối truy cập trang web.
   - **Inform**. Khi người dùng cố lấy quyền truy cập tài nguyên web phù hợp với quy tắc, Kiểm soát web sẽ hiển thị cảnh báo rằng không nên truy cập tài nguyên web. Qua việc sử dụng các liên kết trong cảnh báo, người dùng có thể yêu cầu quyền truy cập đến tài nguyên web này.

   d. Trong mục **Scope**, hãy chọn **Individual websites**.

   e. Cấu hình bộ lọc nội dung:

   - **Individual address**. Tạo một danh sách các 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.

     Nếu Quét các kết nối đã được mã hóa bị tắt, bạn chỉ có thể lọc theo tên máy chủ cho giao thức HTTPS.

   - **Data type**. 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: *Đồ họa*).

f. Trong mục **User or group**, hãy chọn những người dùng mà bạn muốn Kiểm soát web áp dụng quy tắc.

Kiểm soát Web sẽ chỉ lọc các địa chỉ tài nguyên web trong danh sách. 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. Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.

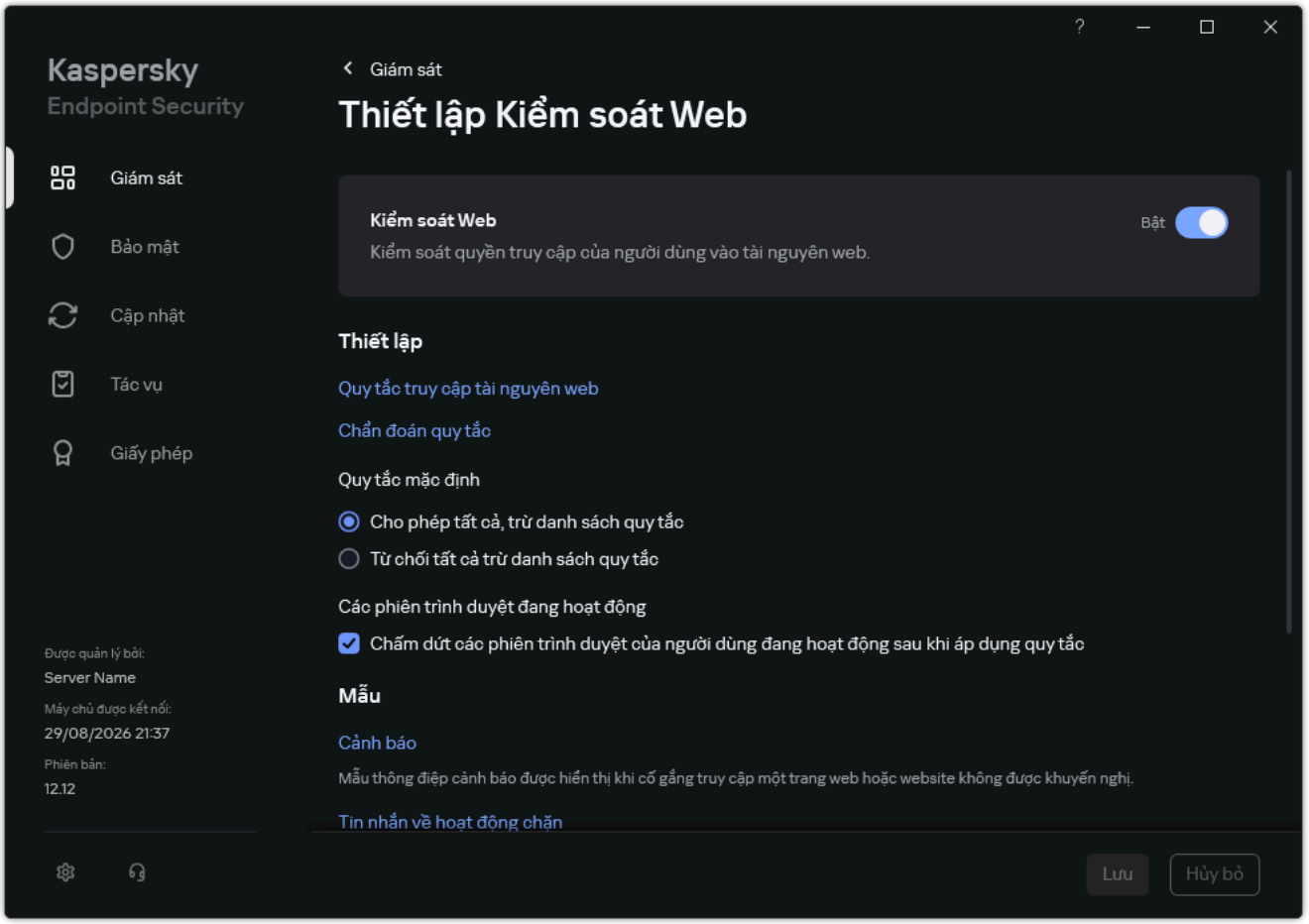
g. Trong mục **Access schedule**, hãy chọn một lịch hoặc tạo một lịch mới.

8. Lưu các thay đổi của bạn.

Cách bật bộ lọc địa chỉ tài nguyên web 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 **Kiểm soát bảo mật → Kiểm soát Web**.



Thiết lập Kiểm soát web

3. Trong mục **Thiết lập**, hãy nhấn nút **Quy tắc truy cập tài nguyên web**.

4. Trong cửa sổ mở ra, hãy nhấn nút **Thêm**.

Cửa sổ **Quy tắc truy cập tài nguyên web** sẽ 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**. Kiểm soát web cho phép truy cập tài nguyên web phù hợp với các tham số của quy tắc.
   - **Chặn**. Kiểm soát web chặn truy cập các tài nguyên web phù hợp với các tham số của quy tắc và hiển thị thông báo từ chối truy cập trang web.
   - **Cảnh báo**. Khi người dùng cố lấy quyền truy cập tài nguyên web phù hợp với quy tắc, Kiểm soát web sẽ hiển thị cảnh báo rằng không nên truy cập tài nguyên web. 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 **Địa chỉ**, hãy chọn **Đến các địa chỉ được chỉ định**.

   Tạo một danh sách các 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.

   > Nếu Quét các kết nối đã được mã hóa bị tắt, bạn chỉ có thể lọc theo tên máy chủ cho giao thức HTTPS.

9. 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 địa chỉ tài nguyên web trong danh sách. 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. Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.

10. Trong danh sách thả xuống **Lịch quy tắc**, hãy chọn một lịch hoặc tạo một lịch mới.

11. Nếu bạn muốn Kiểm soát web chấm dứt kết nối với tài nguyên web bị cấm ngay sau khi áp dụng chính sách, hãy chọn hộp kiểm **Chấm dứt các phiên trình duyệt của người dùng đang hoạt động sau khi áp dụng quy tắc**.

    > Kiểm soát web chỉ cho phép ngắt kết nối ngay lập tức các tài nguyên web trong trình duyệt web. Đối với các ứng dụng khác, Kiểm soát web chỉ hạn chế các kết nối mới.

    Nếu bỏ chọn hộp kiểm này, Kiểm soát web sẽ chỉ hạn chế các kết nối mới tới các tài nguyên web bị cấm. Kiểm soát web không chấm dứt các kết nối đang hoạt động.

12. Lưu các thay đổi của bạn.

Kết quả là quy tắc Kiểm soát web mới sẽ được thêm vào danh sách. Nếu cần, hãy thay đổi mức độ ưu tiên của quy tắc Kiểm soát web. Bạn cũng có thể sử dụng nút bật/tắt để tắt quy tắc truy cập tài nguyên web bất kỳ lúc nào mà không cần xóa quy tắc đó khỏi danh sách.

Lọc theo nội dung tài nguyên web

Để kiểm soát quyền truy cập theo nội dung tài nguyên web, thành phần Kiểm soát web cung cấp bộ lọc danh mục và bộ lọc loại dữ liệu.

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.

Bạn có thể hạn chế quyền truy cập của người dùng vào trang web theo loại dữ liệu, chẳng hạn như để ẩn hình ảnh. Kaspersky Endpoint Security xác định loại dữ liệu dựa theo định dạng tập tin, không dựa theo phần mở rộng của tập tin. Kiểm soát web phân biệt các loại dữ liệu sau:

- Video
- Âm thanh
- Các tập tin ứng dụng văn phòng
- Tập tin thực thi
- Tập tin nén
- Đồ họa
- Kịch bản

> 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 *Đồ họa*.

Quy tắc có thể bao gồm lịch quy tắc và danh sách người dùng áp dụng quy tắc. Ví dụ: bạn có thể chỉ cho phép truy cập các trang web trong giờ làm việc hoặc cho phép truy cập trang web đối với người dùng trong một số nhóm nhất định.

Cách bật bộ lọc nội dung tài nguyên web trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát Web**.
4. Chọn hộp kiểm **Kiểm soát Web**.
5. Trong mục **Thiết lập Kiểm soát Web**, hãy nhấn nút **Thêm**.
   Cửa sổ **Quy tắc truy cập tài nguyên web** sẽ mở ra.

6. Cấu hình quy tắc truy cập tài nguyên web:

   a. Trong trường **Tên**, hãy nhập tên của quy tắc.

   b. Trong danh sách thả xuống **Lọc nội dung** 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: *Đồ họa*).
   - **Theo danh mục nội dung và loại dữ liệu**. Bộ lọc theo danh mục nội dung và loại dữ liệu được bật.

   Sau khi chọn bộ lọc, hãy cấu hình các thông số bộ lọc.

   c. Trong danh sách thả xuống **Áp dụng cho người dùng**, hãy chọn bộ lọc phù hợp cho người dùng:

   - **Cho tất cả người dùng**. Kiểm soát Web sẽ không lọc tài nguyên web theo địa chỉ.
   - **Cho người dùng cá nhân hoặc nhóm**. Kiểm soát Web sẽ chỉ lọc các địa chỉ tài nguyên web trong danh sách. 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. Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.

   d. Trong danh sách thả xuống **Hành động** hãy chọn một tùy chọn:

   - **Cho phép**. Kiểm soát web cho phép truy cập tài nguyên web phù hợp với các tham số của quy tắc.
   - **Chặn**. Kiểm soát web chặn truy cập các tài nguyên web phù hợp với các tham số của quy tắc và hiển thị thông báo từ chối truy cập trang web.
   - **Cảnh báo**. Khi người dùng cố lấy quyền truy cập tài nguyên web phù hợp với quy tắc, Kiểm soát web sẽ hiển thị cảnh báo rằng không nên truy cập tài nguyên web. Qua việc sử dụng các liên kết trong cảnh báo, người dùng có thể yêu cầu quyền truy cập đến tài nguyên web này.

   e. Trong danh sách thả xuống **Lịch quy tắc**, hãy chọn một lịch hoặc tạo một lịch mới.

7. Nếu bạn muốn Kiểm soát web chấm dứt kết nối với tài nguyên web bị cấm ngay sau khi áp dụng chính sách, hãy chọn hộp kiểm **Chấm dứt các phiên trình duyệt của người dùng đang hoạt động sau khi áp dụng quy tắc**.

   > Kiểm soát web chỉ cho phép ngắt kết nối ngay lập tức các tài nguyên web trong trình duyệt web. Đối với các ứng dụng khác, Kiểm soát web chỉ hạn chế các kết nối mới.

   Nếu bỏ chọn hộp kiểm này, Kiểm soát web sẽ chỉ hạn chế các kết nối mới tới các tài nguyên web bị cấm. Kiểm soát web không chấm dứt các kết nối đang hoạt động.

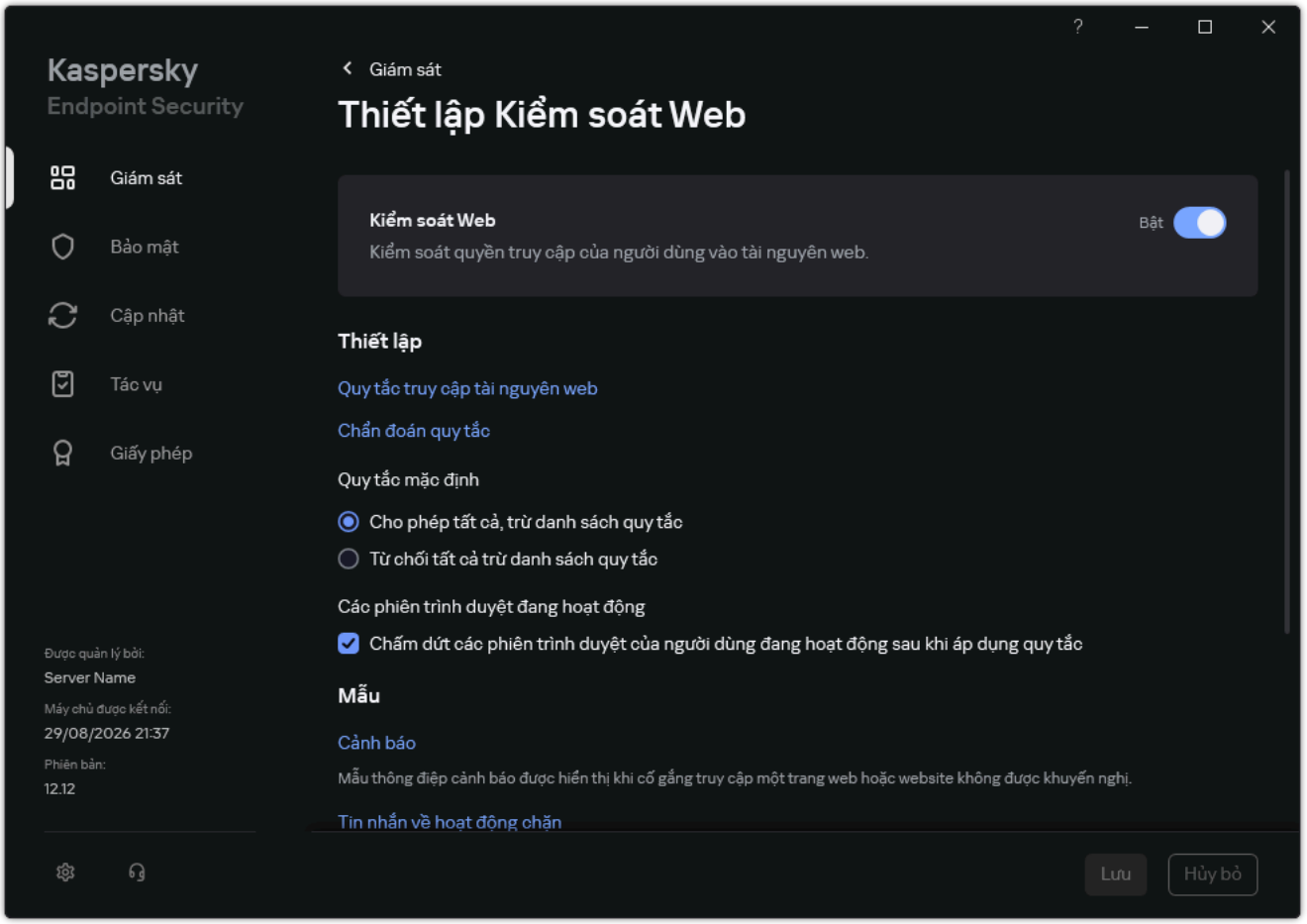
8. Lưu các thay đổi của bạn.

Cách bật bộ lọc nội dung tài nguyên web trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Security Controls** → **Web Control**.
5. Bật nút bật/tắt **Web Control ENABLED**.
6. Trong mục **Rules list**, hãy nhấn nút **Add**.
7. Cấu hình quy tắc truy cập tài nguyên web:
   a. Trong trường **Rule name**, hãy nhập tên của quy tắc.
   b. Chọn trạng thái **Enabled** 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.
   c. Trong mục **Action**, hãy chọn tùy chọn liên quan:
      - **Allow**. Kiểm soát web cho phép truy cập tài nguyên web phù hợp với các tham số của quy tắc.
      - **Block**. Kiểm soát web chặn truy cập các tài nguyên web phù hợp với các tham số của quy tắc và hiển thị thông báo từ chối truy cập trang web.
      - **Inform**. Khi người dùng cố lấy quyền truy cập tài nguyên web phù hợp với quy tắc, Kiểm soát web sẽ hiển thị cảnh báo rằng không nên truy cập tài nguyên web. Qua việc sử dụng các liên kết trong cảnh báo, người dùng có thể yêu cầu quyền truy cập đến tài nguyên web này.
   d. Trong mục **Scope**, hãy chọn **Content category**.
   e. Cấu hình bộ lọc nội dung:
      - **Content category**. 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*).
      - **Data type**. 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: *Đồ họa*).
   f. Trong mục **User or group**, hãy chọn những người dùng mà bạn muốn Kiểm soát web áp dụng quy tắc.
      Kiểm soát Web sẽ chỉ lọc các địa chỉ tài nguyên web trong danh sách. 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. Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.
   g. Trong mục **Access schedule**, hãy chọn một lịch hoặc tạo một lịch mới.
8. Lưu các thay đổi của bạn.

Cách bật bộ lọc nội dung tài nguyên web 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 **Kiểm soát bảo mật → Kiểm soát Web**.



Thiết lập Kiểm soát web

3. Trong mục **Thiết lập**, hãy nhấn nút **Quy tắc truy cập tài nguyên web**.
4. Trong cửa sổ mở ra, hãy nhấn nút **Thêm**.
   Cửa sổ **Quy tắc truy cập tài nguyên web** sẽ 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**. Kiểm soát web cho phép truy cập tài nguyên web phù hợp với các tham số của quy tắc.
   - **Chặn**. Kiểm soát web chặn truy cập các tài nguyên web phù hợp với các tham số của quy tắc và hiển thị thông báo từ chối truy cập trang web.
   - **Cảnh báo**. Khi người dùng cố lấy quyền truy cập tài nguyên web phù hợp với quy tắc, Kiểm soát web sẽ hiển thị cảnh báo rằng không nên truy cập tài nguyên web. 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: *Đồ họa*).

   Để cấu hình bộ lọc nội dung:

   a. Nhấn vào 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 **Người dùng**, hãy chọn bộ lọc phù hợp cho người dùng:

   - **Cho tất cả người dùng**. Kiểm soát Web sẽ không lọc tài nguyên web theo địa chỉ.
   - **Cho người dùng cá nhân và / hoặc nhóm**. Kiểm soát Web sẽ chỉ lọc các địa chỉ tài nguyên web trong danh sách. 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. Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền. 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.

10. 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 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.

11. Nếu bạn muốn Kiểm soát web chấm dứt kết nối với tài nguyên web bị cấm ngay sau khi áp dụng chính sách, hãy chọn hộp kiểm **Chấm dứt các phiên trình duyệt của người dùng đang hoạt động sau khi áp dụng quy tắc**.

Kiểm soát web chỉ cho phép ngắt kết nối ngay lập tức các tài nguyên web trong trình duyệt web. Đối với các ứng dụng khác, Kiểm soát web chỉ hạn chế các kết nối mới.

Nếu bỏ chọn hộp kiểm này, Kiểm soát web sẽ chỉ hạn chế các kết nối mới tới các tài nguyên web bị cấm. Kiểm soát web không chấm dứt các kết nối đang hoạt động.

12. Lưu các thay đổi của bạn.

Kết quả là quy tắc Kiểm soát web mới sẽ được thêm vào danh sách. Nếu cần, hãy thay đổi mức độ ưu tiên của quy tắc Kiểm soát web. Bạn cũng có thể sử dụng nút bật/tắt để tắt quy tắc truy cập tài nguyên web bất kỳ lúc nào mà không cần xóa quy tắc đó khỏi danh sách.

Kiểm tra các quy tắc truy cập tài nguyên web

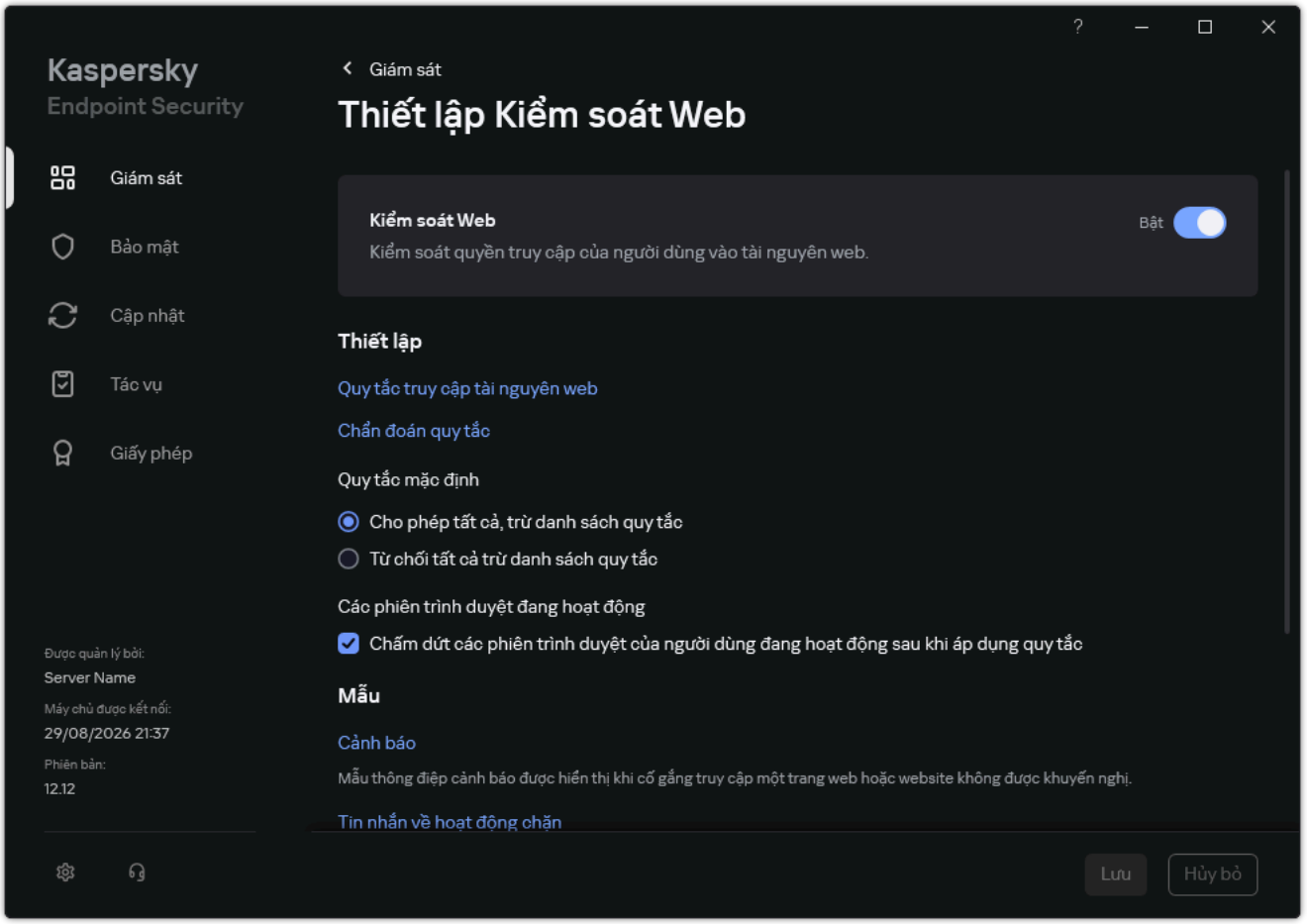
Khi cấu hình Kiểm soát web, bạn có thể vô tình chặn quyền truy cập tài nguyên web mà người dùng cần cho công việc của họ. Để biết được quy tắc Kiểm soát web nào đang chặn quyền truy cập tài nguyên web, bạn có thể sử dụng công cụ *chẩn đoán quy tắc Kiểm soát web*. Công cụ chẩn đoán quy tắc Kiểm soát web chỉ khả dụng trong giao diện của Kaspersky Endpoint Security. Trong bảng điều khiển Kaspersky Security Center, bạn không tìm thấy quy tắc Kiểm soát web nào có một tài nguyên nhất định.

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.

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**.



Thiết lập Kiểm soát web

3. Trong mục **Thiết lập**, hãy nhấn liên kết **Chẩn đoán quy tắc**.

   Cửa sổ **Chẩn đoán quy tắc** sẽ 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.

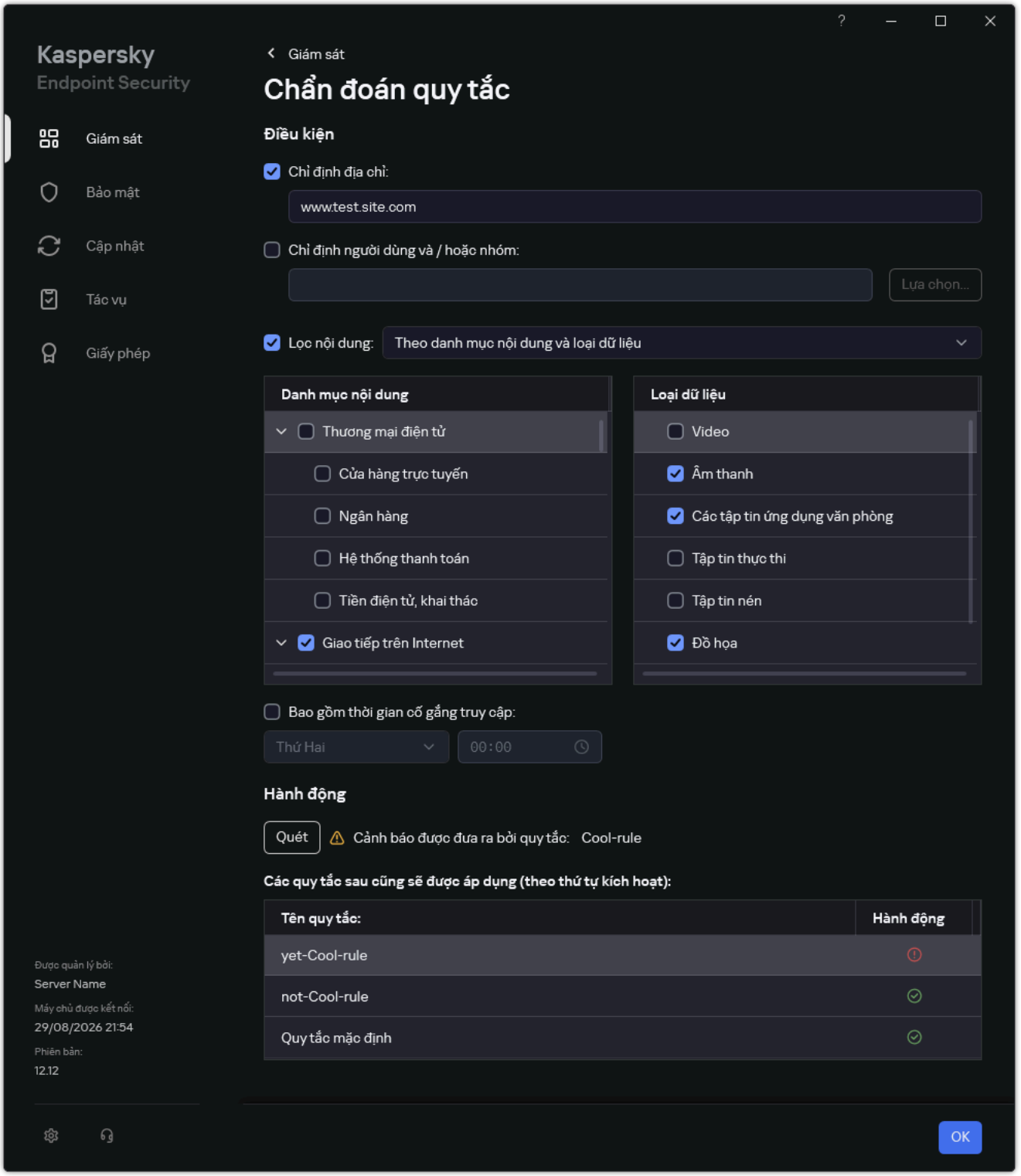
5. Nếu bạn muốn kiểm tra các quy tắc mà Kaspersky Endpoint Security sử dụng để kiểm soát truy cập đến các tài nguyên web cho những người dùng và / hoặc nhóm người dùng được quy định, nhập một danh sách người dùng và / hoặc nhóm người dùng.

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 các Quy tắc kiểm soát web

Bạn có thể xuất danh sách Quy tắc kiểm soát web ra một tập tin XML hoặc JSON. 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát Web**.
4. 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 vào 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.
5. Để nhập danh sách Quy tắc kiểm soát web:
   a. Nhấn vào 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.
6. 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 **Asset management** → **Policies**.
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 **Security Controls** → **Web Control**.

5. Để xuất danh sách các quy tắc, trong mục **Rules list**:

   a. Chọn các quy tắc mà bạn muốn xuất.

   b. Nhấn nút → **Export**.

      Kaspersky Endpoint Security sẽ xuất danh sách các quy tắc vào tập tin JSON trong thư mục tải xuống mặc định.

6. Để nhập danh sách quy tắc, trong mục **Rules list**:

   a. Nhấn nút → **Import**.

      Trong cửa sổ mở ra, hãy chọn tập tin JSON 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 JSON.

7. Lưu các thay đổi của bạn.

Xuất và nhập địa chỉ tài nguyên web của quy tắc Kiểm soát 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:

- Ở định dạng TXT trong Bảng điều khiển quản trị (MMC)
- Ở định dạng JSON trong Bảng điều khiển web
- Ở định dạng CSV trong giao diện ứng dụng

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.

Bạn cũng có thể xuất/nhập tất cả các quy tắc Kiểm soát web và không chỉ các địa chỉ tài nguyên web của một quy tắc riêng lẻ.

Cách xuất/nhập địa chỉ tài nguyên web của quy tắc Kiểm soát web trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát Web**.

5. Trong mục **Thiết lập Kiểm soát Web**, hãy chọn quy tắc có danh sách địa chỉ tài nguyên web mà bạn muốn xuất hoặc nhập.

   Thuộc tính quy tắc Kiểm soát web sẽ được hiển thị.

6. Để xuất danh sách tài nguyên web, hãy thực hiện thao tác sau trong danh sách 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 nút .

   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.

7. Để nhập danh sách tài nguyên web, hãy thực hiện thao tác sau trong danh sách địa chỉ:

   a. Nhấn nút .

      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.

8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách xuất/nhập địa chỉ tài nguyên web của quy tắc Kiểm soát web trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.

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 **Security Controls** → **Web Control**.

5. Trong mục **Rules list**, hãy chọn quy tắc có danh sách địa chỉ tài nguyên web mà bạn muốn xuất hoặc nhập.

   Thuộc tính quy tắc Kiểm soát web sẽ được hiển thị.

6. Trong mục **Scope** → **Individual websites**, hãy nhấn nút **Edit**.

7. Để xuất danh sách tài nguyên web, hãy thực hiện thao tác sau trong danh sách địa chỉ:

   a. Chọn các địa chỉ mà bạn muốn xuất.

   b. Nhấn nút → **Export**.

      Kaspersky Endpoint Security sẽ xuất danh sách địa chỉ tài nguyên web vào tập tin JSON trong thư mục tải xuống mặc định.

8. Để nhập danh sách tài nguyên web, hãy thực hiện thao tác sau trong danh sách địa chỉ:

   a. Nhấn nút → **Import**.

      Trong cửa sổ mở ra, hãy chọn tập tin JSON mà bạn muốn nhập danh sách địa chỉ 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 JSON.

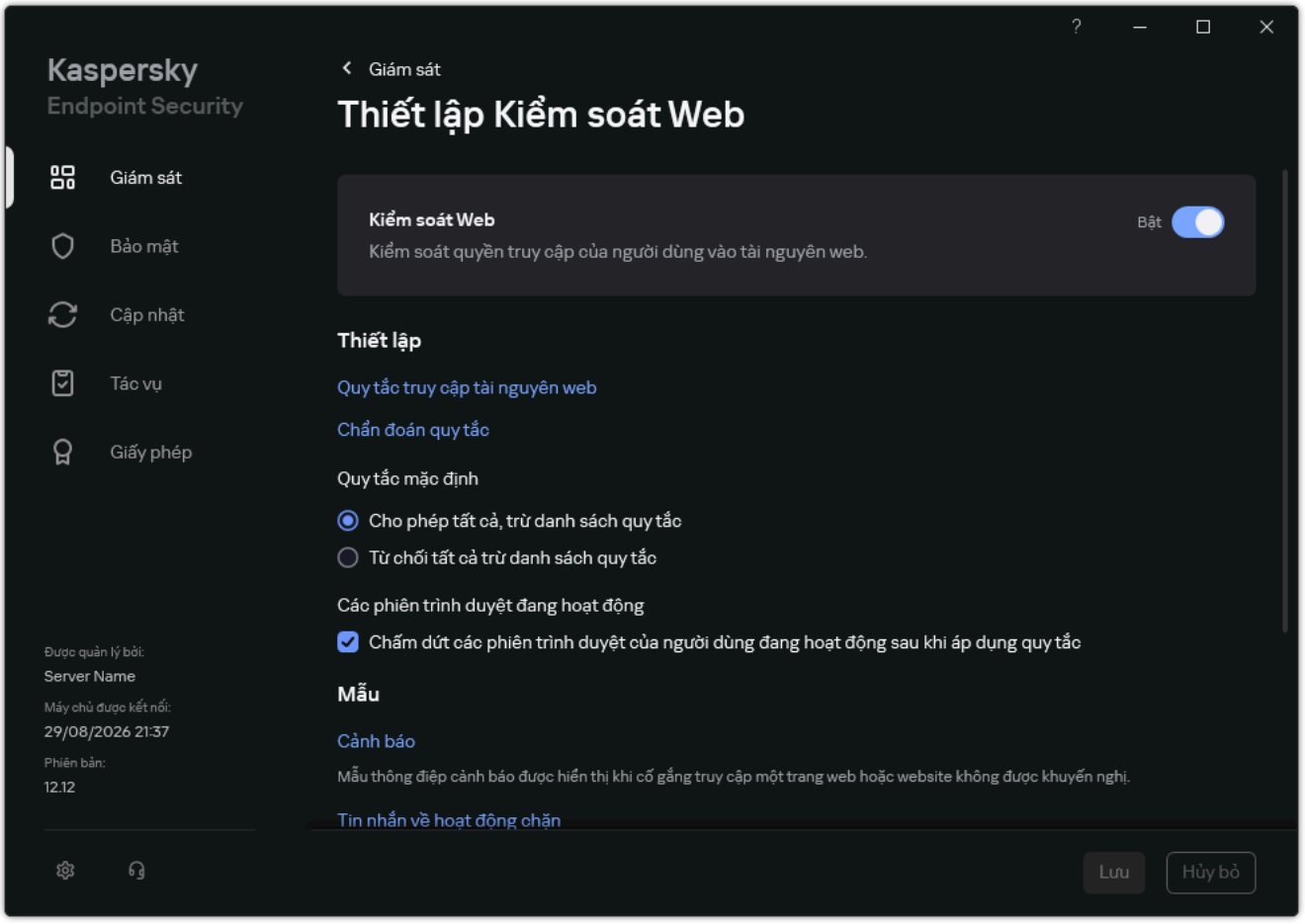
   Bạn có thể xuất và nhập các nhóm trang web theo cùng một cách.

9. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách xuất/nhập địa chỉ tài nguyên web của quy tắc Kiểm soát web 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 **Kiểm soát bảo mật** → **Kiểm soát Web**.



Thiết lập Kiểm soát web

3. Trong mục **Thiết lập**, hãy nhấn 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 CSV 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 CSV.

6. Để nhập danh sách tài nguyên web, hãy thực hiện như sau trong mục **Địa chỉ**:

a. Nhấn vào **Nhập**.

Trong cửa sổ mở ra, hãy chọn tập tin CSV 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 CSV.

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 trang website (trạng thái *Critical*).
- Truy cập vào một website không được khuyến nghị (trạng thái *Warning*).
- Truy cập vào một website được cho phép (trạng thái *Info*).

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.

Chèn một tập lệnh tương tác trang web

Cách chèn một tập lệnh tương tác trang web vào lưu lượng truy cập web trong Bảng điều khiển quản trị (MMC)

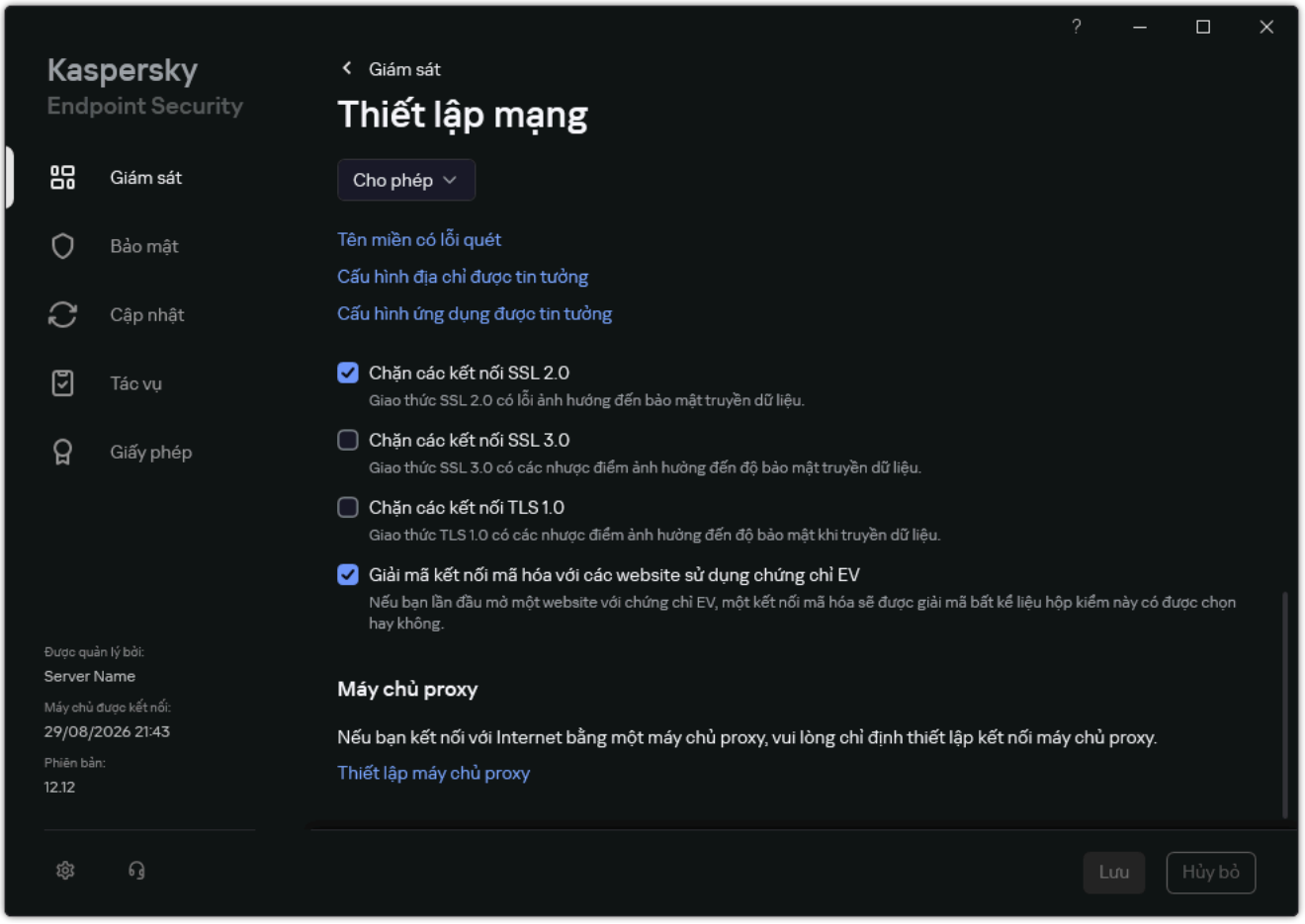
1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Thiết lập mạng**.
4. Trong mục **Quét kết nối được mã hóa**, hãy chọn hộp kiểm **Chèn mã vào lưu lượng web để tương tác với các trang web**.
5. Lưu các thay đổi của bạn.

Cách chèn một tập lệnh tương tác trang web vào lưu lượng truy cập web trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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. Trong cửa sổ chính sách, hãy chọn **General Settings** → **Network Settings**.
5. Trong mục **Monitoring of internet connections**, hãy bật nút gạt **Monitoring of internet connections ENABLED**.
6. Lưu các thay đổi của bạn.

Cách chèn một tập lệnh tương tác trang web vào lưu lượng truy cập web 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**.



Thiết lập mạng của ứng dụng

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.

Cấu hình ghi nhật ký các sự kiện Kiểm soát web

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 **Cấu hình 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:

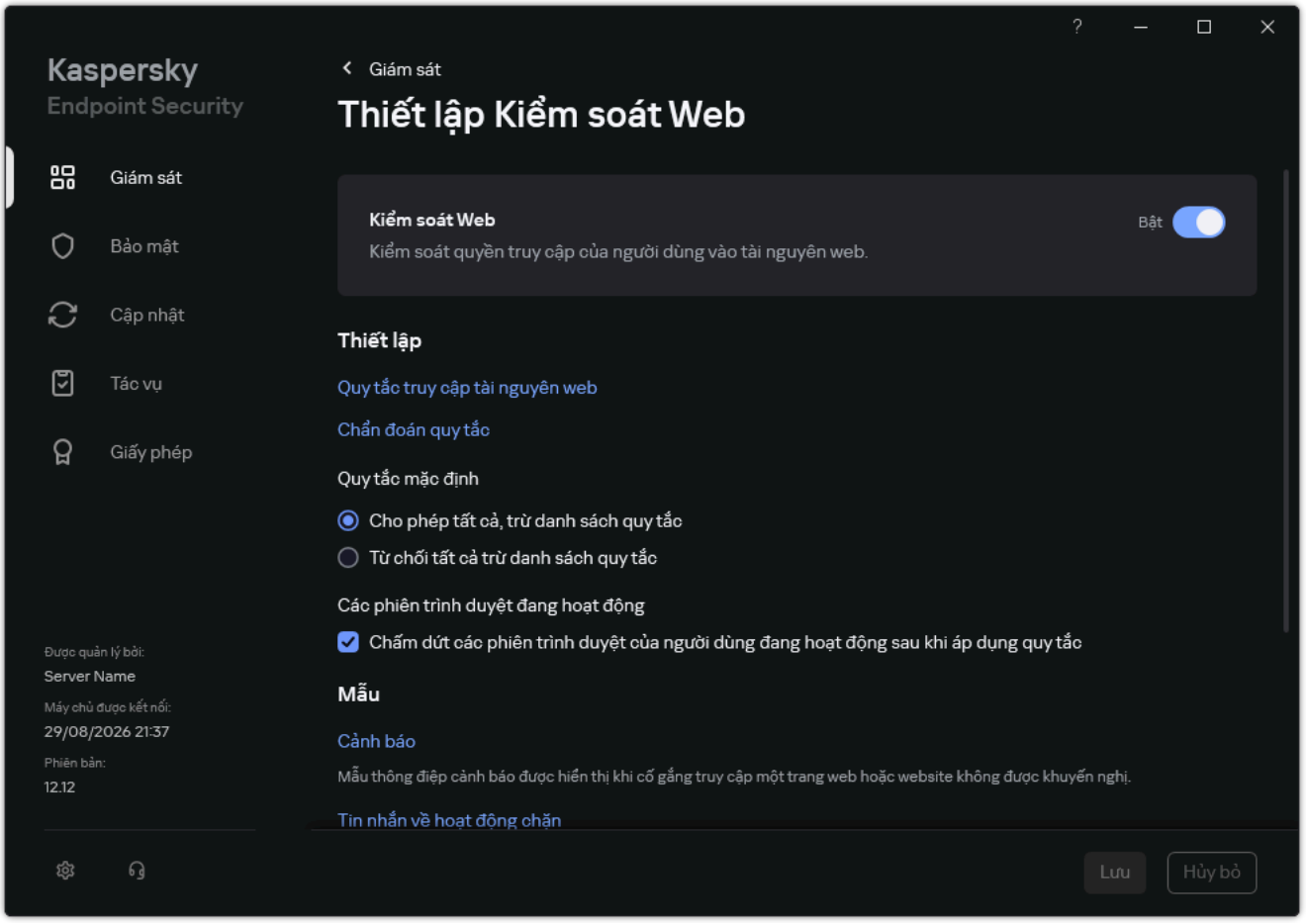
- Nếu bạn đang sử dụng Kaspersky Security Center, thành phần Kiểm soát Web sẽ gửi các sự kiện cho tất cả các đối tượng tạo nên trang web. Vì lý do này, nhiều sự kiện có thể được tạo khi một trang web bị chặn. Ví dụ: khi chặn trang web http://www.example.com, Kaspersky Endpoint Security có thể chuyển 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, http://www.example.com/gallery, Kaspersky Endpoint Security sẽ chỉ gửi một sự kiện với đối tượng http://www.example.com.

Ghi nhật ký sự kiện khi truy cập các trang web được phép

Để bật lưu ký các sự kiện khi truy cập các website được cho phép:

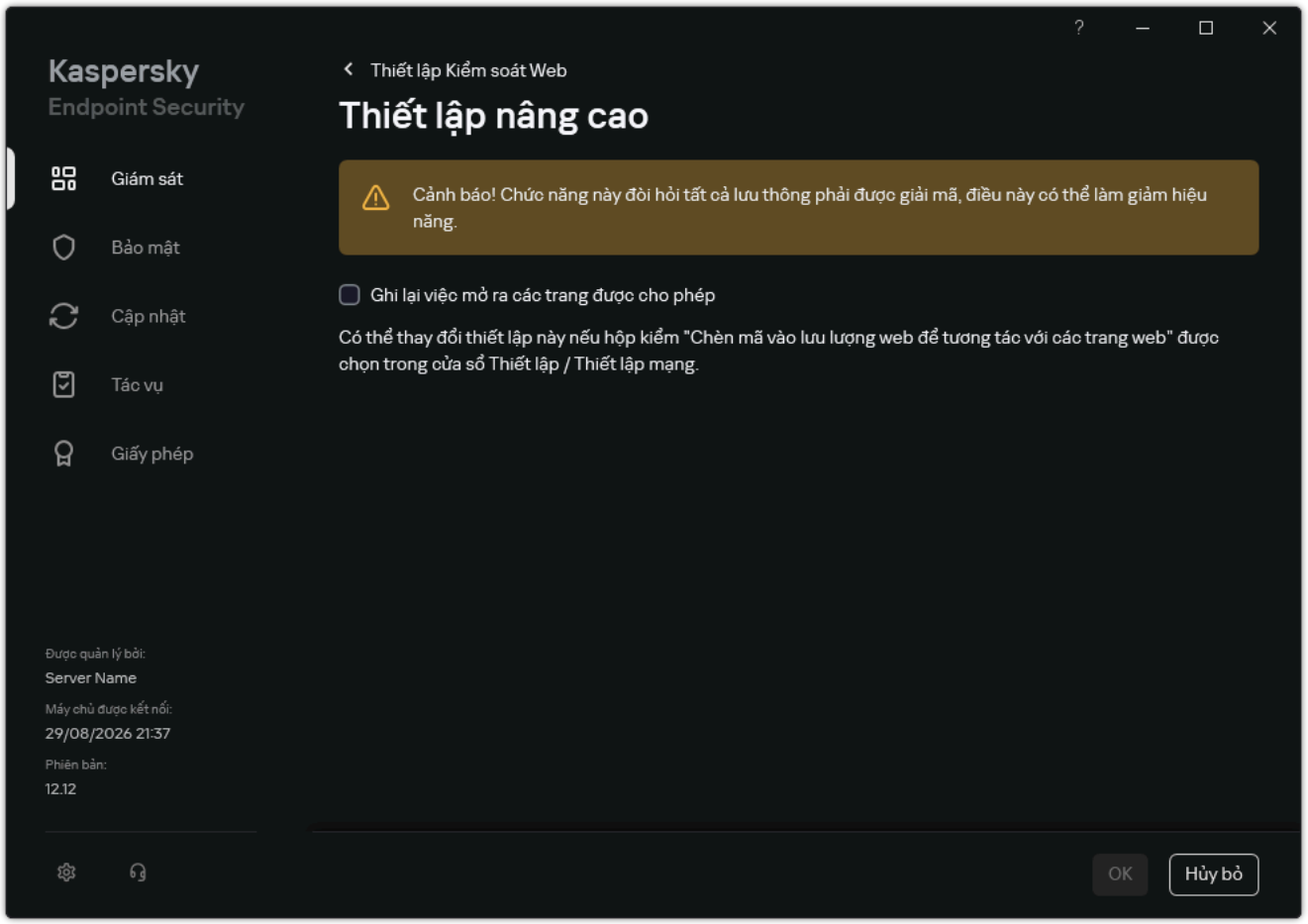
1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút ⚙.
2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Kiểm soát bảo mật → Kiểm soát Web**.



Thiết lập 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**.



Thiết lập nâng cao của Kiểm soát web

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 (xem hình bên dưới) 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.



Thông báo về việc chặn tài nguyên web

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. Các biến đặc biệt được cung cấp để quản lý mẫu tin nhắn (ví dụ: `%USER_NAME%`). Biến cho phép sử dụng một mẫu tin nhắn duy nhất cho nhiều máy tính khác nhau. Khi tạo tin nhắn, Kaspersky Endpoint Security sẽ lấy giá trị của biến từ thiết lập của hệ điều hành và chèn vào tin nhắn phù hợp với máy tính, người dùng và sự kiện cụ thể.

Cách thay đổi mẫu thông báo của Kiểm soát web trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát Web**.
4. Trong mục **Thiết lập mẫu tin nhắn**, hãy nhấn nút **Mẫu**.

5. Cấu hình mẫu thông báo của 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.

   Để thêm biến vào văn bản mẫu, hãy đặt con trỏ vào vị trí mong muốn, nhấn vào **Biến số** và chọn biến cần dùng trong danh sách các tùy chọn có sẵn.

   Bạn cũng có thể khôi phục văn bản mẫu mặc định bằng cách sử dụng nút **Theo mặc định**.

6. Lưu các thay đổi của bạn.

Cách thay đổi mẫu thông báo của 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 **Asset management** → **Policies**.

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 **Security Controls** → **Web Control**.

5. Trong mục **Message templates**, hãy nhấn vào liên kết **Message about website blocking** và cấu hình mẫu cho thông báo của Kiểm soát web:

   - **Warning**. 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.

   - **Message about blocking**. 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.

   - **Message to administrator**. 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.

   Để thêm biến vào văn bản mẫu, hãy đặt con trỏ vào vị trí mong muốn, nhấn vào **Add variable** và chọn biến cần dùng trong danh sách các tùy chọn có sẵn.

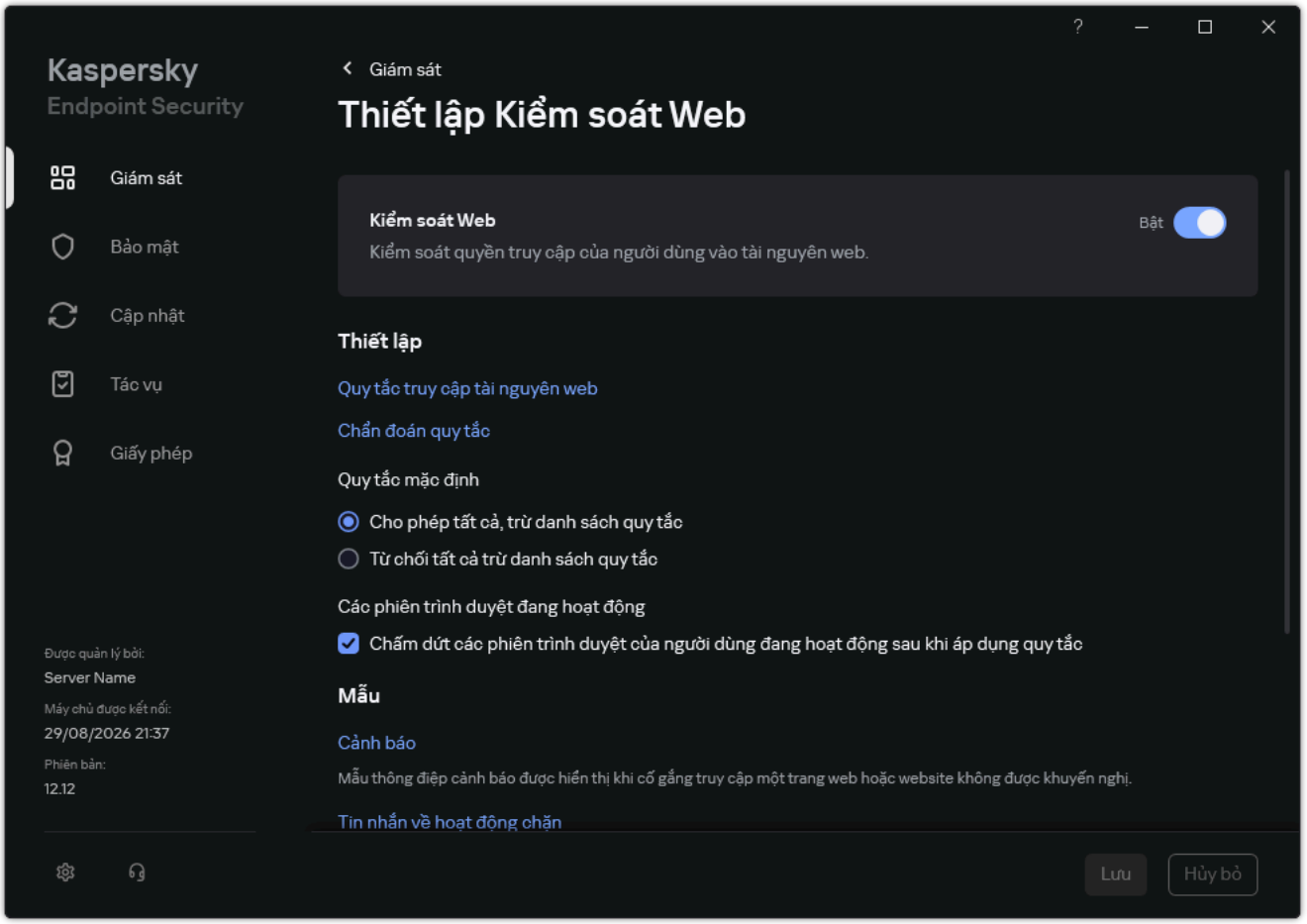
Bạn cũng có thể khôi phục văn bản mẫu mặc định bằng cách sử dụng nút **Reset to default**.

6. Lưu các thay đổi của bạn.

Cách thay đổi mẫu thông báo của Kiểm soát web 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 **Kiểm soát bảo mật → Kiểm soát Web**.



Thiết lập 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.

Để thêm biến vào văn bản mẫu, hãy đặt con trỏ vào vị trí mong muốn, nhấn vào **Thêm biến số** và chọn biến cần dùng trong danh sách các tùy chọn có sẵn.

Bạn cũng có thể khôi phục văn bản mẫu mặc định bằng cách sử dụng nút **Đặt lại**.

4. Lưu các thay đổi của bạn.

Sửa mặt nạ cho các địa chỉ tài nguyên web

Việc sử dụng một *mặt nạ địa chỉ tài nguyên web* (còn được gọi là một "mặt nạ địa chỉ") có thể là hữu ích nếu bạn cần nhập nhiều địa chỉ tài nguyên web giống nhau khi tạo một quy tắc truy cập tài nguyên web. Nếu được viết tốt, một mặt nạ địa chỉ có thể thay thế một lượng lớn các địa chỉ tài nguyên web.

Khi tạo một mặt nạ địa chỉ, cần tuân theo các quy tắc sau đây:

1. Ký tự `*` thay thế bất kỳ chuỗi ký tự nào chứa từ 0 ký tự hoặc hơn.

   Ví dụ: nếu bạn nhập 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 `pictures.`.
   - `http://user.pictures.example.com`. .Tên miền đại diện `*.` sẽ đại diện cho `pictures.` và `user.`.
   - `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.

Kiểm soát web cho máy ảo

Kiểm soát web sẽ kiểm soát lưu lượng truy cập trên máy tính cũng như trên máy ảo được triển khai cục bộ trên máy tính. Tính năng này hoạt động mà không cần phải cài đặt ứng dụng Kaspersky Endpoint Security trên máy ảo cục bộ. Điều này có nghĩa là nếu người dùng cố mở một trang web bị chặn bởi quy tắc Kiểm soát web trong trình duyệt trên *máy ảo*, ứng dụng được cài đặt trên hệ điều hành chủ của *máy tính* sẽ từ chối truy cập vào trang web đó.

Kiểm soát web hoạt động theo cách khác nhau trên các máy ảo khác nhau.

Oracle VM VirtualBox

Kaspersky Endpoint Security hỗ trợ các quy tắc Kiểm soát web trên máy ảo Oracle VM VirtualBox mà không có hạn chế nào. Ứng dụng có thể kiểm soát tất cả lưu lượng truy cập của máy ảo. Nếu bộ lọc theo người dùng được cấu hình trong quy tắc Kiểm soát web, ứng dụng sẽ hoạt động bình thường vì tất cả các tiến trình của máy ảo đều do người dùng cục bộ khởi động.

VMware Workstation

Kaspersky Endpoint Security hỗ trợ các quy tắc Kiểm soát web trên máy ảo VMware Workstation với một số hạn chế. Ứng dụng không hỗ trợ các quy tắc có bộ lọc do người dùng cấu hình. Các tiến trình máy ảo đang chạy dưới quyền người dùng hệ thống (SYSTEM). Điều này khiến không thể xác định được người dùng đang cố mở trang web trên máy ảo.

Microsoft Hyper-V

Kaspersky Endpoint Security không hỗ trợ các quy tắc Kiểm soát web trên máy ảo Microsoft Hyper-V.

Các biến trong mẫu thông báo của Kiểm soát web

Bạn có thể sử dụng các biến sau trong mẫu tin nhắn người dùng hoặc mẫu tin nhắn quản trị viên:

- **Tên người dùng** – `%USER_NAME%`.

  Tên tài khoản người dùng hiện tại trên máy tính, là nơi tạo tin nhắn, theo định dạng `<device name>\<user alias>` (ví dụ: `DESKTOP-123\John.Smith`).

- **Địa chỉ tài nguyên web** – `%CANONIC_REQUEST_URL%`.

  Địa chỉ của tài nguyên web bị chặn.

- **Tên quy tắc** – `%RULE%`.

  Tên của quy tắc đã chặn tài nguyên web.

- **Email để gửi thư** – `%COMPLAIN_EMAIL%`.

  Địa chỉ email để gửi phản hồi về các hoạt động chặn tài nguyên web. Nhấn vào địa chỉ email sẽ mở một cửa sổ cho phép người dùng viết tin nhắn cho quản trị viên.

- **Tên danh mục nội dung** – `%CONTENT_CATEGORY_LIST%`.

  Danh mục trang web chứa tài nguyên bị chặn (ví dụ: *Hệ thống thanh toán*).

- **Tên danh mục loại dữ liệu** – `%TYPE_CATEGORY_LIST%`.

  Loại dữ liệu trên tài nguyên web bị chặn (ví dụ: *Đồ họa*).

- **Liên kết đến tài nguyên web yêu cầu** – `%CONTINUE_PAGE%`.

  Liên kết đến trang web được yêu cầu (ví dụ: `http://www.example.com/pagename.html`).

- **Liên kết đến website** – `%CONTINUE_SITE%`.

  Liên kết đến trang web chứa trang được yêu cầu (ví dụ: `http://www.example.com/`).

- **Liên kết để truy cập vào tên miền** – `%CONTINUE_DOMAIN%`.

  Liên kết có thể nhấn vào để truy cập tất cả các trang web hiện có của tên miền đó. Ví dụ:: nếu địa chỉ của trang web bị chặn là `http://www.example.com` thì biến `%CONTINUE_DOMAIN%` sẽ được thay thế bằng liên kết `http://*.example.com`. Nhấn vào liên kết này sẽ cho phép truy cập vào tất cả các địa chỉ web của tên miền gốc. `http://www.example.com/` bao gồm cả các tên miền phụ, ví dụ: `http://start.example.com/*` hoặc `http://domain.domain.example.com/*`, trong đó ký tự `*` có thể đại diện cho bất kỳ chuỗi ký tự nào (bao gồm cả chuỗi rỗng).

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 mất hoặc rò rỉ dữ liệu.

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 **Advanced** → **Repositories** → **Hardware**.

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 – .
  - Bởi quy tắc (chỉ dành cho máy in và thiết bị di động) – .

- Tùy thuộc vào bus kết nối (ngoại trừ Wi-Fi) – .
- Chặn với ngoại lệ (Chỉ 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). Nếu như chế độ **Tùy thuộc vào bus kết nối** được chọn cho loại thiết bị, ứng dụng sẽ cho phép hoặc từ chối truy cập thiết bị, tùy thuộc vào giao diện kết nối (ví dụ: 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 (Hardware ID hay HWID). Bạn có thể xem ID trong thuộc tính thiết bị bằng cách sử dụng công cụ hệ điều hành. Ví dụ về ID thiết bị: `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 Vendor ID (VID) và một Product ID (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.

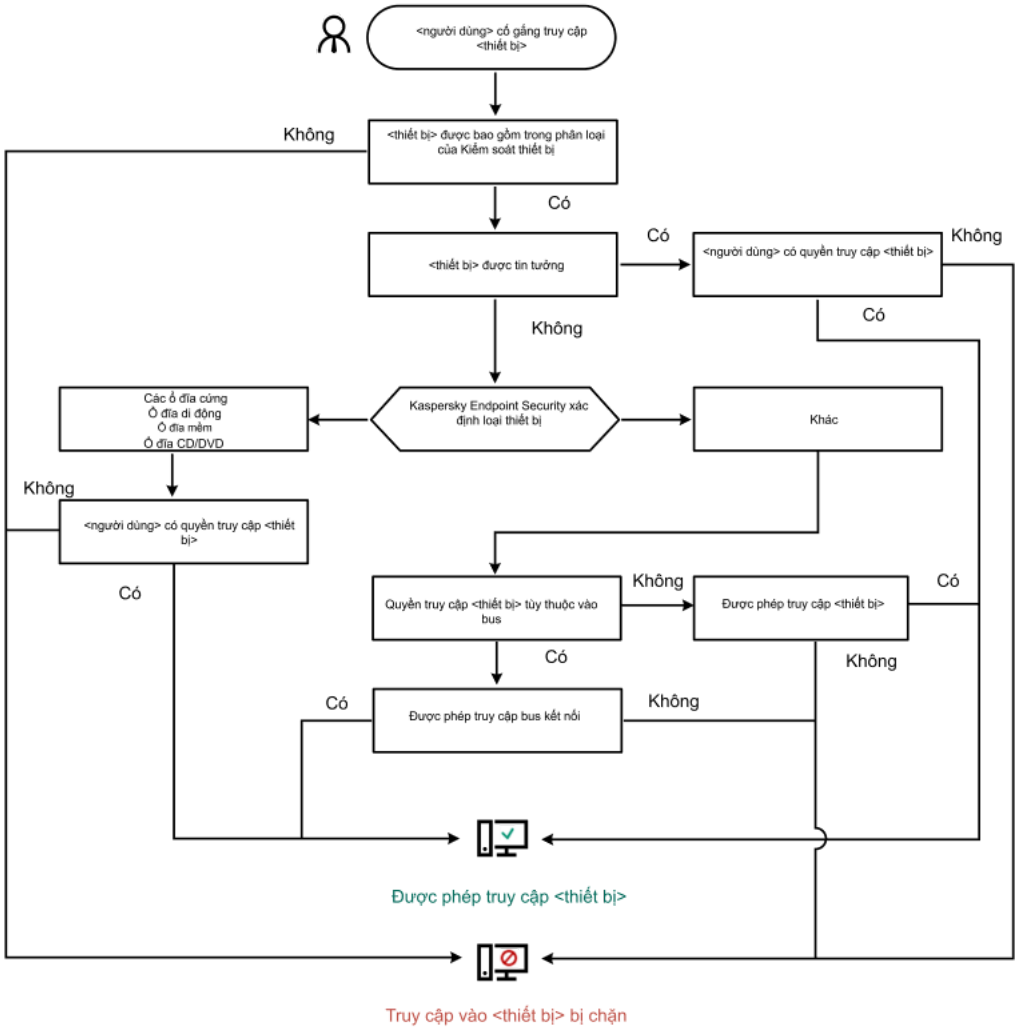
Khi một thiết bị bị chặn bởi Kiểm soát thiết bị được kết nối đến máy tính, Kaspersky Endpoint Security sẽ chặn quyền truy cập và hiển thị một thông báo (xem hình dưới đây).



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).



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.

Thông tin về quy tắc truy cập

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. 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 (bao gồm các ổ đĩa flash USB)	✓	✓	✓	✓	✓
Ổ đĩa mềm	✓	✓	✓	✓	✓
Ổ đĩa CD/DVD	✓	✓	✓	✓	✓
Thiết bị di động (MTP)	✓	✓	✓	✓	✓
Máy in cục bộ	✓	–	✓	✓	–
Máy in qua mạng	✓	–	✓	✓	–
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	✓	–	–	–	–
Bluetooth	✓	–	–	–	–
Máy ảnh và máy quét	✓	–	–	–	–

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

Nếu giá trị **Tùy thuộc vào bus kết nối** được chọn cho quy tắc truy cập theo loại thiết bị, ứng dụng sẽ cho phép hoặc từ chối truy cập vào thiết bị tùy thuộc vào giao diện kết nối. Các quy tắc cho phép truy cập đến bus theo mặc định sẽ được tạo cho tất cả các bus kết nối có trong phân loại của thành phần Kiểm soát Thiết bị.

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 ⊘). Mức độ ưu tiên của quy tắc truy cập loại thiết bị cao hơn mức độ ưu tiên của quy tắc truy cập bus kết nối.

Không thể khóa bàn phím và chuột bằng Kiểm soát thiết bị. Nếu bạn cấm truy cập vào bus kết nối USB thì người dùng sẽ tiếp tục làm việc với bàn phím và chuột được kết nối qua USB. Thành phần Phòng chống Tấn công BadUSB được thiết kế để ngăn không cho các thiết bị USB bị nhiễm giả mạo bàn phím kết nối với máy tính.

Lấy thông tin về các thiết bị được lắp đặt

Kaspersky Security Center nhận thông tin về các thiết bị được lắp đặt từ các nhà cung cấp sau: Network Agent và Kaspersky Endpoint Security. Thông tin về các thiết bị được lắp đặt là thông tin cần thiết cho việc quản lý quyền truy cập và tạo danh sách các thiết bị được tin tưởng.

Thông tin về phần cứng máy tính

Nếu Network Agent được cài đặt trên thiết bị Windows, thành phần đó sẽ gửi các thông tin sau về phần cứng của thiết bị đến Máy chủ quản trị:

- RAM
- các thiết bị lưu trữ (bao gồm ổ cứng)
- bo mạch chủ
- CPU
- bộ điều hợp mạng
- màn hình

- GPU
- card âm thanh

Network Agent sẽ cung cấp các thông tin này mỗi lần đồng bộ với Kaspersky Security Center. Bạn có thể xem thông tin phần cứng của máy tính trong phần thuộc tính của máy tính (**Registry phần cứng**).

Thông tin về phần cứng

Kaspersky Endpoint Security cung cấp các thông tin về phần cứng được lắp đặt: máy in, ổ đĩa di động, thiết bị di động (MTP), v.v. Để nhận thông tin về phần cứng, bạn cần áp dụng một chính sách chủ động cho phép truyền thông tin về các thiết bị được lắp đặt (truyền thông tin được bật theo mặc định).

Cách bật truyền dữ liệu về các thiết bị được lắp đặt trong Bảng điều khiển quản lý (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Các báo cáo và lưu trữ**.
5. Trong mục **Truyền dữ liệu đến Máy chủ quản trị**, hãy nhấn nút **Thiết lập**.
6. Chọn hộp kiểm **Các thiết bị được cài đặt**.
7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật truyền dữ liệu về các thiết bị được lắp đặt trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management → Policies**.
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 → KSC Integration**.
5. Trong mục **Data transfer to Administration Server**, hãy nhấn nút **Advanced settings**.
6. Chọn hộp kiểm **About installed devices**.
7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Kết quả là bạn có thể xem danh sách các thiết bị được lắp đặt trong bảng điều khiển Kaspersky Security Center (**Repositories → Hardware**).

Quản lý quyền truy cập thiết bị theo loại

Kiểm soát thiết bị cho phép quản lý quyền truy cập thiết bị theo từng loại. Loại thiết bị được xác định bởi hệ điều hành khi thiết bị được kết nối. Bạn có thể tra cứu loại thiết bị bằng công cụ Trình quản lý thiết bị được tích hợp trong hệ điều hành. Bạn phải cấu hình các quy tắc để quản lý quyền 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. 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.

Theo mặc định, Kiểm soát thiết bị cho phép mọi người dùng truy cập tất cả các thiết bị.

Bạn có thể cấu hình quyền truy cập thiết bị như sau:

- **Cho phép**.

  Kaspersky Endpoint Security sẽ cấp cho mọi người dùng toàn quyền truy cập thiết bị.

- **Chặn**.

  Kaspersky Endpoint Security sẽ chặn kết nối thiết bị. Ứng dụng cho phép chỉ những thiết bị được tin tưởng mới được kết nối.

- **Tùy thuộc vào bus kết nối**.

  Kaspersky Endpoint Security xác định giao diện kết nối của thiết bị và hạn chế quyền truy cập thiết bị theo trạng thái kết nối bus của chúng. Ứng dụng cũng cho phép kết nối các thiết bị được tin tưởng.

- **Bởi quy tắc**.

  Đối với một số loại thiết bị, bạn có thể chỉ định người dùng riêng lẻ hoặc nhóm người dùng được phép sử dụng thiết bị, thiết lập lịch truy cập thiết bị và cấu hình quyền đọc và ghi. Ứng dụng cũng cho phép kết nối các thiết bị được tin tưởng.

Hãy cẩn thận khi cấu hình quyền truy cập các thiết bị thuộc loại **Các ổ đĩa cứng**. Nếu bạn chặn quyền truy cập ổ đĩa hệ thống, ứng dụng có thể gây ra sự cố (BSOD) khi khởi động hệ điều hành.

Nếu một thiết bị không phù hợp với sơ đồ phân loại của Kiểm soát thiết bị thì không thể hạn chế quyền truy cập thiết bị đó.

Cách quản lý quyền truy cập thiết bị theo loại trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật → Kiểm soát thiết bị**.
5. Trong mục **Thiết lập Kiểm soát thiết bị**, hãy chọn thẻ **Các loại thiết bị**.

   Thẻ **Các loại thiết bị** 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.

6. Cấu hình quy tắc truy cập cho thiết bị:

   a. Chọn chế độ truy cập: **Cho phép**, **Chặn**, **Tùy thuộc vào bus kết nối**, **Bởi quy tắc**.

      Để chọn chế độ **Bởi quy tắc**, bạn phải nhấp đúp để mở thuộc tính quy tắc truy cập.

   b. Nếu chọn chế độ truy cập **Tùy thuộc vào bus kết nối**, bạn phải cấu hình quy tắc truy cập cho các giao diện kết nối trên thẻ **Các Bus kết nối**.

   c. Đối với thiết bị lưu trữ (ví dụ: phương tiện di động), bạn có thể cấu hình quyền truy cập cho từng người dùng. Bạn cũng có thể thiết lập lịch truy cập thiết bị và cấu hình quyền đọc và ghi.

      Bạn có thể thêm các thiết bị vào danh sách 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.

   d. Nếu cần thiết, hãy cấu hình các quy tắc in.

   e. Nếu cần thiết, hãy cấu hình các quy tắc truy cập thiết bị Bluetooth.

   f. Nếu cần thiết, hãy cấu hình quy tắc kết nối Wi-Fi của máy tính.

7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách quản lý quyền truy cập thiết bị trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.

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 **Security Controls** → **Device Control**.

5. Trong mục **Device access rules**, hãy chọn thẻ **Devices and Wi-Fi networks**.

   Bảng này liệt kê các quy tắc truy cập cho tất cả các thiết bị có trong phân loại của thành phần Kiểm soát thiết bị.

6. Cấu hình quy tắc truy cập cho thiết bị:

   a. Chọn chế độ truy cập: **Allow**, **Block**, **Depends on bus**, **Custom**.

      Nếu chế độ truy cập không có trong menu thả xuống, hãy mở thuộc tính quy tắc truy cập bằng cách nhấn đúp vào loại thiết bị.

   b. Nếu chọn chế độ truy cập **Depends on bus**, bạn phải cấu hình quy tắc truy cập cho các giao diện kết nối trên thẻ **Connection buses**.

   c. Đối với thiết bị lưu trữ (ví dụ: phương tiện di động), bạn có thể cấu hình quyền truy cập cho từng người dùng. Bạn cũng có thể thiết lập lịch truy cập thiết bị và cấu hình quyền đọc và ghi.

      Bạn có thể thêm các thiết bị vào danh sách 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.

   d. Nếu cần thiết, hãy cấu hình các quy tắc in.

e. Nếu cần thiết, hãy cấu hình các quy tắc truy cập thiết bị Bluetooth.

f. Nếu cần thiết, hãy cấu hình quy tắc kết nối Wi-Fi của máy tính.

7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách quản lý quyền truy cập thiết bị 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 **Kiểm soát bảo mật → Kiểm soát thiết bị**.

3. Trong mục **Thiết lập truy cập**, hãy nhấn liên kết **Các thiết bị và mạng Wi-Fi**.

   Bảng này liệt kê các quy tắc truy cập cho tất cả các thiết bị có trong phân loại của thành phần Kiểm soát thiết bị.

4. Cấu hình quy tắc truy cập cho thiết bị:

   a. Chọn chế độ truy cập: **Cho phép**, **Chặn**, **Tùy thuộc vào bus kết nối**, **Bởi quy tắc**.

   Nếu chế độ truy cập không có trong menu thả xuống, hãy mở thuộc tính quy tắc truy cập bằng cách nhấn đúp vào loại thiết bị.

   b. Nếu chọn chế độ truy cập **Tùy thuộc vào bus kết nối**, bạn phải cấu hình quy tắc truy cập cho các giao diện kết nối trên thẻ **Các Bus kết nối**.

   c. Đối với thiết bị lưu trữ (ví dụ: phương tiện di động), bạn có thể cấu hình quyền truy cập cho từng người dùng. Bạn cũng có thể thiết lập lịch truy cập thiết bị và cấu hình quyền đọc và ghi.

   Bạn có thể thêm các thiết bị vào danh sách 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.

   d. Nếu cần thiết, hãy cấu hình các quy tắc in.

   e. Nếu cần thiết, hãy cấu hình các quy tắc truy cập thiết bị Bluetooth.

   f. Nếu cần thiết, hãy cấu hình quy tắc kết nối Wi-Fi của máy tính.

5. Lưu các thay đổi của bạn.

Do đó, khi người dùng cố gắng truy cập thiết bị, ứng dụng sẽ chặn quyền truy cập theo các quy tắc. Kaspersky Endpoint Security cũng sẽ ghi lại sự kiện tương ứng. Nếu muốn cấp quyền truy cập cho từng thiết bị, bạn có thể thêm các thiết bị này vào danh sách các thiết bị được tin tưởng.

Quản lý quyền truy cập thiết bị bằng 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**.

   Nếu bạn đã thay đổi quyền truy cập vào bus kết nối **Cổng nối tiếp** (COM) hoặc **Cổng song song** (LPT) thì bạn phải khởi động lại máy tính để kích hoạt quy tắc truy cập.

6. Lưu các thay đổi của bạn.

Phân biệt quyền truy cập của người dùng vào thiết bị

Bạn có thể cấu hình quyền truy cập của người dùng theo loại thiết bị hoặc theo thiết bị được tin tưởng.

Phân biệt quyền truy cập của người dùng theo loại thiết bị

Kiểm soát thiết bị cho phép cấu hình quyền truy cập của người dùng vào dữ liệu trên *thiết bị lưu trữ*. Đối với những thiết bị như vậy, bạn có thể cấu hình quyền ghi và quyền đọc. Kiểm soát thiết bị hỗ trợ các loại *thiết bị lưu trữ* sau đây:

- Các ổ đĩa cứng
- Ổ đĩa di động (bao gồm các ổ đĩa flash USB)
- Ổ đĩa mềm
- Ổ đĩa CD/DVD
- Thiết bị di động (MTP) Thiết bị di động (MTP) bao gồm các thiết bị di động, máy ảnh, máy nghe nhạc, v.v.

Theo cách này, bạn có thể cho phép nhóm quản trị viên chỉ được sử dụng phương tiện di động. Đối với các loại thiết bị khác, bạn có thể từ chối hoặc cho phép truy cập đối với mọi người dùng. Bạn cũng có thể cấu hình quyền truy cập sử dụng của người dùng đối với máy in.

Cách cấu hình quyền truy cập của người dùng vào dữ liệu trên thiết bị lưu trữ trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.

2. Trong cây bảng điều khiển, hãy chọn **Policies**.

3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

4. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thiết bị**.

5. Trong mục **Thiết lập Kiểm soát thiết bị**, hãy chọn thẻ **Các loại thiết bị**.

   Thẻ **Các loại thiết bị** 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.

6. Để cấu hình quy tắc truy cập thiết bị lưu trữ, hãy nhấn đúp để mở danh sách quy tắc.

7. Cấu hình quy tắc truy cập thiết bị lưu trữ:

   a. Trong mục **Quy tắc truy cập**, hãy nhấn nút **Thêm**.

      Thao tác này sẽ mở ra một cửa sổ để thêm quy tắc truy cập thiết bị lưu trữ mới.

   b. Trong trường **Mức ưu tiên quy tắc**, hãy đặt mức độ ưu tiên *ghi 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 bạn 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.

   c. Trong mục **Quy tắc dành cho người dùng và nhóm**, hãy chọn người dùng hoặc nhóm người dùng. Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.

   d. Nhấn vào **OK**.

8. Trong mục **Lịch dành cho quy tắc truy cập được chọn**, hãy cấu hình một lịch truy cập thiết bị lưu trữ dành cho người dùng.

   Ví dụ: bạn có thể cho phép người dùng chỉ sử dụng thiết bị lưu trữ trong giờ làm việc.

9. Cấu hình quyền truy cập của người dùng đối với thiết bị lưu trữ trong trình quản lý tập tin (**Đọc** / **Ghi**).

10. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách cấu hình quyền truy cập của người dùng vào dữ liệu trên thiết bị lưu trữ trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.

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 **Security Controls** → **Device Control**.

5. Trong mục **Device access rules**, trong bảng quy tắc truy cập, hãy mở thuộc tính của quy tắc truy cập cho thiết bị lưu trữ.

6. Trong mục **Device access rules**, hãy chọn **Custom**.

7. Cấu hình quy tắc truy cập thiết bị lưu trữ:

   a. Trong mục **Users and their rights**, hãy nhấn nút **Add**.

      Thao tác này sẽ mở ra một cửa sổ để thêm quy tắc truy cập thiết bị lưu trữ mới.

   b. Trong trường **Priority**, hãy đặt mức độ ưu tiên *ghi 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 bạn 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.

   c. Trong mục **User or group**, hãy chọn người dùng hoặc nhóm người dùng. Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.

   d. Trong mục **Access schedule**, hãy cấu hình một lịch truy cập thiết bị lưu trữ dành cho người dùng.

      Ví dụ: bạn có thể cho phép người dùng chỉ sử dụng thiết bị lưu trữ trong giờ làm việc.

   e. Cấu hình quyền truy cập của người dùng đối với thiết bị lưu trữ trong trình quản lý tập tin (**Read** / **Write**).

   f. Nhấn vào **Save**.

8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách cấu hình quyền truy cập của người dùng vào dữ liệu trên thiết bị lưu trữ 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 **Kiểm soát bảo mật → Kiểm soát thiết bị**.

3. Trong mục **Thiết lập truy cập**, hãy nhấn liên kết **Các thiết bị và mạng Wi-Fi**.

   Bảng này liệt kê các quy tắc truy cập cho tất cả các thiết bị có trong phân loại của thành phần Kiểm soát thiết bị.

4. Để cấu hình quy tắc truy cập thiết bị di động, hãy nhấn chuột phải để mở danh sách quy tắc.

5. Cấu hình quy tắc truy cập thiết bị lưu trữ:

   a. 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 lưu trữ mới.

   b. Trong trường **Ưu tiên**, hãy đặt mức độ ưu tiên *ghi 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 bạn 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.

   c. Trong mục **Người dùng**, hãy chọn người dùng hoặc nhóm người dùng. Bạn có thể chọn người dùng trong Active Directory hoặc nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.

   d. Nhấn vào **OK**.

6. Trong mục **Lịch để truy cập thiết bị**, hãy cấu hình một lịch truy cập thiết bị lưu trữ dành cho người dùng.

   Ví dụ: bạn có thể cho phép người dùng chỉ sử dụng thiết bị lưu trữ trong giờ làm việc.

7. Cấu hình quyền truy cập của người dùng đối với thiết bị lưu trữ trong trình quản lý tập tin (**Đọc** / **Ghi**).

8. Lưu các thay đổi của bạn.

Phân biệt quyền truy cập của người dùng vào 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. Bạn có thể cấu hình quyền truy cập của người dùng trong thuộc tính của thiết bị được tin tưởng.

Quản lý quyền truy cập thiết bị di động

Kaspersky Endpoint Security cho phép bạn kiểm soát quyền truy cập dữ liệu trên thiết bị di động chạy Android và iOS. Các thiết bị di động thuộc danh mục thiết bị di động (MTP). Do đó, để cấu hình quyền truy cập dữ liệu vào thiết bị di động, bạn cần chỉnh sửa thiết lập truy cập cho 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 hoặt một thiết bị khác. Loại thiết bị sẽ phụ thuộc vào kiểu máy của thiết bị di động và chế độ kết nối USB đã chọn. Kaspersky Endpoint Security cho phép bạn cấu hình các quyền truy cập riêng lẻ cho dữ liệu trên thiết bị di động trong ứng dụng ADB, iTunes hoặc trình quản lý tập tin. Trong tất cả các trường hợp khác, thành phần Kiểm soát thiết bị sẽ cho phép truy cập thiết bị di động theo quy tắc truy cập thiết bị di động (MTP).

Truy cập thiết bị di động

Các thiết bị di động thuộc danh mục thiết bị di động (MTP), do đó, chúng có cùng thiết lập. Bạn có thể chọn một trong các chế độ truy cập thiết bị di động sau đây:

- **Cho phép** . Kaspersky Endpoint Security cho phép truy cập đầy đủ thiết bị di động. Bạn có thể mở, tạo, sửa đổi, sao chép hoặc xóa tập tin trên thiết bị di động bằng trình quản lý tập tin hoặc ứng dụng ADB và iTunes. Bạn cũng có thể sạc pin của thiết bị bằng cách kết nối thiết bị di động với cổng USB của máy tính.

- **Chặn** . Kaspersky Endpoint Security hạn chế quyền truy cập thiết bị di động trong trình quản lý tập tin cũng như các ứng dụng ADB và iTunes. Ứng dụng này chỉ cho phép truy cập thiết bị di động được tin tưởng. Bạn cũng có thể sạc pin của thiết bị bằng cách kết nối thiết bị di động với cổng USB của máy tính.

- **Tùy thuộc vào bus kết nối** . Kaspersky Endpoint Security sẽ cho phép kết nối với thiết bị di động theo Trạng thái kết nối USB (**Cho phép** hoặc **Chặn**).

- **Bởi quy tắc** . Kaspersky Endpoint Security hạn chế quyền truy cập thiết bị di động theo các quy tắc. Trong quy tắc, bạn có thể cấu hình quyền truy cập (đọc/ghi), chọn người dùng hoặc nhóm người dùng có thể có quyền truy cập thiết bị di động và cấu hình lịch truy cập cho thiết bị di động. Bạn cũng có thể hạn chế quyền truy cập các thiết bị bằng ứng dụng ADB và iTunes.

Cấu hình quy tắc truy cập thiết bị di động

Quy tắc truy cập cho thiết bị di động (MTP), thiết bị ADB và thiết bị iTunes được cấu hình khác nhau. Đối với thiết bị di động (MTP) và thiết bị ADB, bạn có thể cấu hình quy tắc cho từng người dùng hoặc nhóm người dùng và tạo lịch áp dụng quy tắc. Đối với các thiết bị iTunes thì bạn không thể làm điều đó. Bạn chỉ có thể cho phép hoặc từ chối quyền truy cập dữ liệu thông qua ứng dụng iTunes cho tất cả người dùng.

Cách cấu hình quy tắc truy cập thiết bị di động trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát thiết bị**.

4. Trong mục **Thiết lập Kiểm soát thiết bị**, hãy chọn thẻ **Các loại thiết bị**.

   Bảng này liệt kê các quy tắc truy cập cho tất cả các thiết bị có trong phân loại của thành phần Kiểm soát thiết bị.

5. Trong menu ngữ cảnh cho loại thiết bị **Thiết bị di động (MTP)**, hãy cấu hình chế độ truy cập thiết bị di động: **Cho phép**, **Chặn** hoặc **Tùy thuộc vào bus kết nối**.

6. Để cấu hình quy tắc truy cập thiết bị di động, hãy nhấn đúp để mở danh sách quy tắc.

7. Cấu hình quy tắc truy cập thiết bị di động:

   a. Trong mục **Quy tắc truy cập**, hãy nhấn nút **Thêm**.

      Thao tác này sẽ mở ra một cửa sổ để thêm quy tắc truy cập thiết bị di động mới.

   b. Trong trường **Ưu tiên**, hãy đặt mức độ ưu tiên ghi quy tắc. Một quy tắc bao gồm các thuộc tính sau: tài khoản người dùng, lịch, quyền (đọc/ghi/ADB) 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 bạn 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.

   c. Trong mục **Quy tắc dành cho người dùng và nhóm**, hãy chọn người dùng hoặc nhóm người dùng. Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.

   d. Nhấn vào **OK**.

8. Trong mục **Lịch dành cho quy tắc truy cập được chọn**, hãy cấu hình một lịch truy cập thiết bị di động dành cho người dùng.

   > Không thể cấu hình lịch truy cập riêng cho các thiết bị ADB. Bạn có thể cấu hình lịch truy cập chung cho thiết bị ADB và thiết bị di động (MTP).

9. Cấu hình quyền truy cập của người dùng đối với thiết bị di động trong trình quản lý tập tin (**Đọc** / **Ghi**).

10. Cấu hình quyền truy cập dữ liệu trên thiết bị di động thông qua ứng dụng ADB bằng cách sử dụng hộp kiểm **Truy cập qua ADB**.

    Nếu hộp kiểm này bị xóa, khi thiết bị di động được kết nối, ứng dụng ADB sẽ không thể phát hiện thiết bị.

11. Trong **Truy cập qua iTunes**, cấu hình quyền truy cập dữ liệu trên thiết bị di động thông qua ứng dụng iTunes.

    Kaspersky Endpoint Security sẽ áp dụng thiết lập truy cập thiết bị di động thông qua ứng dụng iTunes cho tất cả người dùng. Không thể cấu hình lịch truy cập riêng cho các thiết bị iTunes.

12. Lưu các thay đổi của bạn.

Cách cấu hình quy tắc truy cập thiết bị trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Security Controls** → **Device Control**.
5. Trong mục **Device access rules**, hãy nhấn liên kết **Devices and Wi-Fi networks**.

   Bảng này liệt kê các quy tắc truy cập cho tất cả các thiết bị có trong phân loại của thành phần Kiểm soát thiết bị.
6. Chọn loại thiết bị **Portable devices (MTP)**.

   Thao tác này sẽ mở quyền truy cập thiết bị di động (MTP).
7. Cấu hình chế độ truy cập thiết bị di động: **Allow**, **Block**, **Depends on bus** hoặc **Custom**.
8. Sử dụng công tắc bật/tắt **Access via iTunes for all users ENABLED**, cấu hình quyền truy cập dữ liệu trên thiết bị di động thông qua ứng dụng iTunes.

   Kaspersky Endpoint Security sẽ áp dụng thiết lập truy cập thiết bị di động thông qua ứng dụng iTunes cho tất cả người dùng. Không thể cấu hình lịch truy cập riêng cho các thiết bị iTunes.

9. Nếu chọn chế độ **Custom**, bạn phải thêm quy tắc truy cập cho thiết bị. Để thực hiện, trong mục **Users and their rights**, hãy nhấn vào **Add** và cấu hình quy tắc truy cập thiết bị di động:

   a. Trong trường **Priority**, hãy đặt mức độ ưu tiên ghi quy tắc. Một quy tắc bao gồm các thuộc tính sau: tài khoản người dùng, lịch, quyền (đọc/ghi/ADB) 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 bạn 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.

b. Trong mục **User or group**, hãy chọn người dùng hoặc nhóm người dùng để truy cập thiết bị di động. Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.

c. Trong mục **Access schedule**, hãy cấu hình một lịch truy cập thiết bị di động dành cho người dùng.

> Không thể cấu hình lịch truy cập riêng cho các thiết bị ADB. Bạn có thể cấu hình lịch truy cập chung cho thiết bị ADB và thiết bị di động (MTP).

d. Cấu hình quyền truy cập của người dùng đối với thiết bị di động trong trình quản lý tập tin (**Read** / **Write**).

e. Cấu hình quyền truy cập dữ liệu trên thiết bị di động thông qua ứng dụng ADB bằng cách sử dụng hộp kiểm **Access via ADB**.

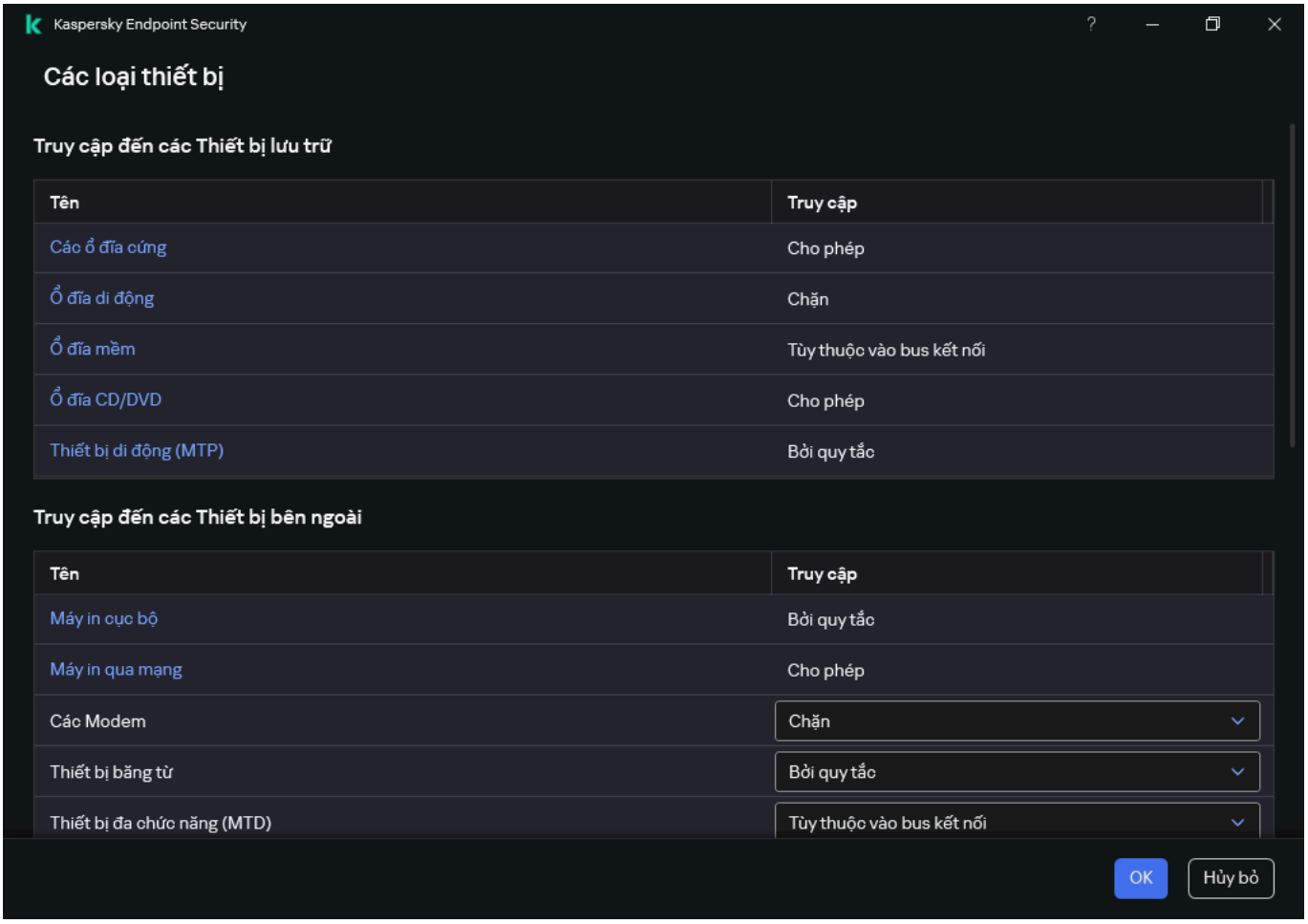
Nếu hộp kiểm này bị xóa, khi thiết bị di động được kết nối, ứng dụng ADB sẽ không thể phát hiện thiết bị.

10. Lưu các thay đổi của bạn.

Cách cấu hình quy tắc truy cập thiết bị di động 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 **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.



Các loại thiết bị trong thành phần Kiểm soát thiết bị

4. Trong mục **Truy cập đến các Thiết bị lưu trữ**, hãy nhấn liên kết **Thiết bị di động (MTP)**.

   Thao tác này sẽ mở ra một cửa sổ chứa các quy tắc truy cập thiết bị di động (MTP).

5. Trong mục **Truy cập**, hãy cấu hình chế độ truy cập thiết bị di động: **Cho phép**, **Chặn**, **Tùy thuộc vào bus kết nối** hoặc **Bởi quy tắc**.

6. Nếu chọn chế độ **Bởi quy tắc**, bạn phải thêm quy tắc truy cập cho thiết bị:

   a. 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 di động mới.

   b. Trong trường **Ưu tiên**, hãy đặt mức độ ưu tiên ghi quy tắc. Một quy tắc bao gồm các thuộc tính sau: tài khoản người dùng, lịch, quyền (đọc/ghi/ADB) 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 bạn 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.

c. Trong mục **Trạng thái**, hãy bật quy tắc truy cập thiết bị di động.

d. Trong mục **Quy tắc truy cập**, hãy cấu hình quyền truy cập thiết bị di động cho người dùng.

- Cấu hình quyền truy cập của người dùng đối với thiết bị di động trong trình quản lý tập tin (**Đọc** / **Ghi**).
- Cấu hình quyền truy cập dữ liệu trên thiết bị di động thông qua ứng dụng ADB bằng cách sử dụng hộp kiểm **Truy cập qua ADB**.

  Nếu hộp kiểm này bị xóa, khi thiết bị di động được kết nối, ứng dụng ADB sẽ không thể phát hiện thiết bị.

e. Trong mục **Người dùng**, hãy chọn người dùng hoặc nhóm người dùng để truy cập thiết bị di động. Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.

f. Trong mục **Lịch để truy cập thiết bị**, hãy cấu hình một lịch truy cập thiết bị cho người dùng.

> Không thể cấu hình lịch truy cập riêng cho các thiết bị ADB. Bạn có thể cấu hình lịch truy cập chung cho thiết bị ADB và thiết bị di động (MTP).

g. Trong **Truy cập qua iTunes**, cấu hình quyền truy cập dữ liệu trên thiết bị di động thông qua ứng dụng iTunes.

> Kaspersky Endpoint Security sẽ áp dụng thiết lập truy cập thiết bị di động thông qua ứng dụng iTunes cho tất cả người dùng. Không thể cấu hình lịch truy cập riêng cho các thiết bị iTunes.

7. Lưu các thay đổi của bạn.

Kết quả là quyền truy cập của người dùng vào thiết bị di động bị hạn chế theo các quy tắc. Nếu bạn đã cấm truy cập thiết bị di động trong ứng dụng ADB và iTunes thì khi bạn kết nối thiết bị di động, ứng dụng ADB và iTunes sẽ bị ngăn phát hiện thiết bị di động.

Thiết bị di động được tin tưởng

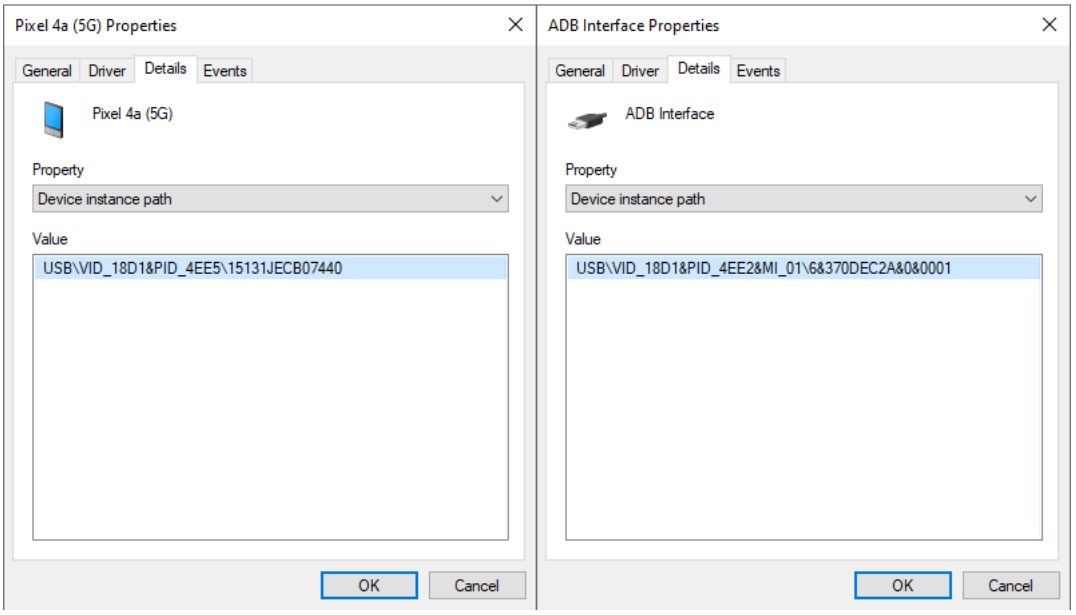
Thiết bị được tin tưởng là các thiết bị mà những người dùng được quy định trong thiết lập thiết bị được tin tưởng có thể truy cập vào bất cứ lúc nào.

Các bước để thêm thiết bị di động được tin tưởng hoàn toàn giống như các bước thêm các loại thiết bị được tin tưởng khác. Bạn có thể thêm thiết bị di động theo ID hoặc mẫu máy của thiết bị.

Để thêm một thiết bị di động được tin tưởng theo ID, bạn cần một ID duy nhất (Hardware ID – HWID). Bạn có thể tìm ID trong thuộc tính thiết bị bằng cách sử dụng các công cụ của hệ điều hành (xem hình bên dưới). Công cụ Trình quản lý thiết bị cho phép bạn thực hiện việc này. ID của thiết bị di động (MTP) và thiết bị ADB, iTunes sẽ khác nhau ngay cả đối với cùng một thiết bị di động. ID của thiết bị di động (MTP) có thể trông giống như sau: `15131JECB07440`. ID của thiết bị ADB có thể trông giống như sau: `6&370DEC2A&0&0001`. Thêm thiết bị theo ID là một cách thuận tiện nếu bạn muốn thêm một số thiết bị cụ thể. Bạn cũng có thể sử dụng ký tự đại diện.

Nếu bạn đã cài đặt ứng dụng ADB và 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.

Để thêm một thiết bị di động được tin tưởng theo mẫu máy của thiết bị, bạn sẽ cần Vendor ID (VID) và Product ID (PID) của thiết bị đó. Bạn có thể tìm cá ID trong thuộc tính thiết bị bằng cách sử dụng các công cụ của hệ điều hành (xem hình bên dưới). Mẫu để nhập VID và PID: `VID_18D1&PID_4EE5`. 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.



ID thiết bị trong Trình quản lý thiết bị

Quản lý quyền truy cập thiết bị Bluetooth

Kaspersky Endpoint Security cho phép quản lý quyền truy cập các thiết bị Bluetooth. Các thiết bị Bluetooth bao gồm bàn phím không dây, chuột, tai nghe, máy in, v.v. Bạn cũng có thể sử dụng Bluetooth để liên lạc, ví dụ như với một thiết bị di động.

Khi thiết bị Bluetooth được kết nối hoặc ngắt kết nối, ứng dụng có thể tạo nhiều sự kiện về thiết bị. Lý do là hệ điều hành có thể phát hiện một thiết bị Bluetooth là nhiều thiết bị thuộc các loại khác nhau. Kaspersky Endpoint Security cũng quản lý bộ điều hợp Bluetooth qua đó thiết bị được kết nối như một thiết bị riêng biệt. Đó là lý do tại sao ứng dụng tạo sự kiện cho từng thiết bị được phát hiện.

Bạn có thể chọn một trong các chế độ truy cập thiết bị Bluetooth sau đây:

- **Cho phép và không ghi** . Kaspersky Endpoint Security cho phép kết nối bất kỳ thiết bị Bluetooth nào và không lưu thông tin về kết nối vào nhật ký sự kiện. Bạn có thể kết nối các thiết bị đầu vào Bluetooth (bàn phím, chuột, v.v.), gửi dữ liệu qua Bluetooth, quản lý các thiết bị Bluetooth khác (tai nghe, tai nghe, v.v.).
- **Cho phép** . Kaspersky Endpoint Security cho phép kết nối mọi thiết bị Bluetooth. Bạn có thể kết nối các thiết bị đầu vào Bluetooth (bàn phím, chuột, v.v.), gửi dữ liệu qua Bluetooth, quản lý các thiết bị Bluetooth khác (tai nghe, tai nghe, v.v.).
- **Chặn** . Kaspersky Endpoint Security hạn chế quyền truy cập vào các thiết bị Bluetooth. Bạn có thể cho phép chỉ kết nối các thiết bị đầu vào Bluetooth (lớp Human Interface Devices). Những thiết bị này bao gồm bàn phím, thiết bị chuột, cần điều khiển, v.v.

Không thể tạo danh sách các thiết bị Bluetooth được tin tưởng. Nếu bạn bị hạn chế quyền truy cập các thiết bị Bluetooth, bạn chỉ có thể kết nối các thiết bị đầu vào Bluetooth.

Cách cấu hình quy tắc truy cập thiết bị Bluetooth trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật → Kiểm soát thiết bị**.
5. Trong mục **Thiết lập Kiểm soát thiết bị**, hãy chọn thẻ **Các loại thiết bị**.

   Bảng này liệt kê các quy tắc truy cập cho tất cả các thiết bị có trong phân loại của thành phần Kiểm soát thiết bị.
6. Trong menu ngữ cảnh cho loại thiết bị **Bluetooth**, hãy cấu hình chế độ truy cập thiết bị Bluetooth: **Cho phép** , **Chặn** hoặc **Cho phép và không ghi** .
7. Nếu chọn chế độ **Chặn**, bạn chỉ có thể cho phép kết nối các thiết bị đầu vào Bluetooth (bàn phím, chuột, v.v.). Để thực hiện, trong mục **Loại trừ**, hãy chọn hộp kiểm **Thiết bị đầu vào (chuột và bàn phím)**.
8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách cấu hình quy tắc truy cập thiết bị Bluetooth trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management → Policies**.
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 **Security Controls → Device Control**.

5. Trong mục **Device access rules**, hãy nhấn liên kết **Devices and Wi-Fi networks**.

   Bảng này liệt kê các quy tắc truy cập cho tất cả các thiết bị có trong phân loại của thành phần Kiểm soát thiết bị.

6. Chọn loại thiết bị **Bluetooth devices**.

   Thao tác này sẽ mở thiết lập truy cập thiết bị Bluetooth.

7. Cấu hình chế độ truy cập thiết bị Bluetooth: **Allow**, **Block**, **Allow and do not log**.

8. Nếu chọn chế độ **Block**, bạn chỉ có thể cho phép kết nối các thiết bị đầu vào Bluetooth (bàn phím, chuột, v.v.). Để thực hiện, trong mục **Exclusions**, hãy chọn hộp kiểm **Input devices (mice and keyboards)**.

9. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

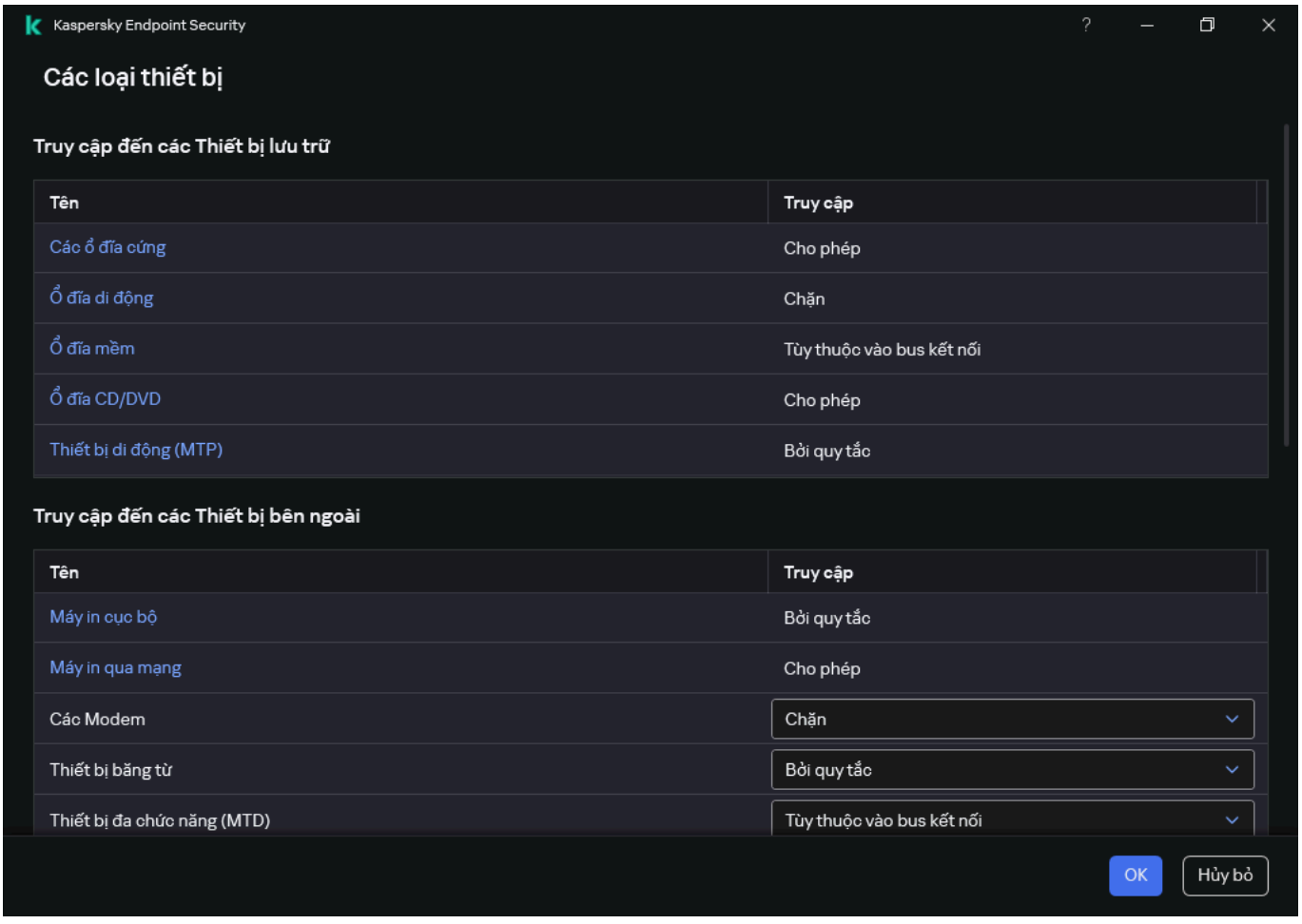
Cách cấu hình quy tắc truy cập thiết bị Bluetooth trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .

2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **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.



Các loại thiết bị trong thành phần Kiểm soát thiết bị

4. Trong mục **Truy cập đến các Thiết bị bên ngoài**, hãy nhấn liên kết **Bluetooth**.

   Thao tác này sẽ mở thiết lập truy cập thiết bị Bluetooth.

5. Trong mục **Truy cập**, hãy cấu hình chế độ truy cập thiết bị Bluetooth: **Cho phép**, **Chặn**, **Cho phép và không ghi**.

6. Nếu chọn chế độ **Chặn**, bạn chỉ có thể cho phép kết nối các thiết bị đầu vào Bluetooth (bàn phím, chuột, v.v.). Để thực hiện, trong mục **Loại trừ**, hãy chọn hộp kiểm **Thiết bị đầu vào (chuột và bàn phím)**.

7. Lưu các thay đổi của bạn.

Kiểm soát in

Kiểm soát in không được hỗ trợ trên các máy tính chạy trên kiến trúc Arm.

Bạn có thể sử dụng Kiểm soát in để cấu hình quyền truy cập của người dùng vào máy in qua mạng và máy in cục bộ.

Kiểm soát máy in cục bộ

Kaspersky Endpoint Security cho phép cấu hình quyền truy cập vào máy in cục bộ ở hai cấp độ: *kết nối* và *in*.

Kaspersky Endpoint Security kiểm soát kết nối máy in cục bộ qua các bus sau: USB, Cổng nối tiếp (COM), Cổng song song (LPT).

Kaspersky Endpoint Security sẽ kiểm soát kết nối của máy in cục bộ với cổng COM và LPT chỉ ở cấp độ bus. Do đó, để chặn kết nối máy in qua cổng COM và LPT, bạn cần chọn chế độ truy cập Tùy thuộc vào bus kết nối cho máy in cục bộ và cấm kết nối với bus COM và LPT.

Đối với máy in được kết nối với cổng USB, ứng dụng thực hiện kiểm soát ở hai cấp độ: loại thiết bị (máy in cục bộ) và bus kết nối (USB).

Bạn có thể chọn một trong các chế độ truy cập sau vào máy in cục bộ qua cổng USB:

- **Cho phép** ✓. Kaspersky Endpoint Security cấp quyền truy cập đầy đủ vào máy in cục bộ cho tất cả người dùng. Người dùng có thể kết nối máy in và in tài liệu bằng các phương thức mà hệ điều hành cung cấp.

- **Chặn** ⊘. Kaspersky Endpoint Security sẽ chặn kết nối của máy in cục bộ. Ứng dụng chỉ cho phép kết nối máy in được tin tưởng.

- **Tùy thuộc vào bus kết nối**. Kaspersky Endpoint Security sẽ cho phép kết nối với máy in cục bộ theo trạng thái kết nối bus USB (**Cho phép** hoặc **Chặn**).

- **Bởi quy tắc**. Để kiểm soát in, bạn phải thêm *quy tắc in*. Trong các quy tắc, bạn có thể chọn người dùng hoặc nhóm người dùng mà bạn muốn cho phép hoặc chặn quyền truy cập tài liệu in trên máy in cục bộ.

Kiểm soát máy in qua mạng

Kaspersky Endpoint Security cho phép cấu hình quyền truy cập để in trên máy in qua mạng. Bạn có thể chọn một trong các chế độ truy cập máy in qua a mạng sau đây:

- **Cho phép và không ghi**. Kaspersky Endpoint Security không kiểm soát việc in trên máy in quan mạng. Ứng dụng cấp quyền truy cập in cho tất cả người dùng và không lưu thông tin về việc in vào nhật ký sự kiện.

- **Cho phép**. Kaspersky Endpoint Security sẽ cấp quyền truy cập in trên máy in qua mạng cho tất cả người dùng.

- **Chặn**. Kaspersky Endpoint Security sẽ hạn chế quyền truy cập máy in qua mạng đối với tất cả người dùng. Ứng dụng này chỉ cho phép truy cập máy in được tin tưởng.

- **Bởi quy tắc**. Kaspersky Endpoint Security sẽ cấp quyền truy cập in theo các quy tắc in. Trong các quy tắc, bạn có thể chọn người dùng hoặc nhóm người dùng sẽ được phép hoặc ngăn không cho in tài liệu trên máy in qua mạng.

Thêm quy tắc in cho máy in

Cách thêm quy tắc in trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật → Kiểm soát thiết bị**.

4. Trong mục **Thiết lập Kiểm soát thiết bị**, hãy chọn thẻ **Các loại thiết bị**.

   Bảng này liệt kê các quy tắc truy cập cho tất cả các thiết bị có trong phân loại của thành phần Kiểm soát thiết bị.

5. Trong menu ngữ cảnh cho loại thiết bị **Máy in cục bộ** và **Máy in qua mạng**, hãy cấu hình chế độ truy cập cho các máy in liên quan: **Cho phép**, **Chặn**, **Cho phép và không ghi** (chỉ dành cho máy in qua mạng) hoặc **Tùy thuộc vào bus kết nối** (chỉ dành cho máy in cục bộ).

6. Để cấu hình quy tắc in trên máy in qua mạng và máy in cục bộ, hãy nhấn đúp vào danh sách quy tắc để mở chúng.

7. Chọn **Bởi quy tắc** làm chế độ truy cập máy in.

8. Chọn người dùng hoặc nhóm người dùng mà bạn muốn áp dụng quy tắc in.

   a. Nhấn vào **Thêm**.

      Thao tác này sẽ mở ra một cửa sổ để thêm quy tắc in mới.

   b. Gán một mức ưu tiên cho mục quy tắc. Mục quy tắc bao gồm các thuộc tính sau: tài khoản người dùng, hành động (cho phép/chặn) 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 bạn 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.

   c. Trong mục **Hành động**, hãy cấu hình quyền truy cập của người dùng để in trên máy in.

   d. Nhấn vào **Người dùng và nhóm** và chọn người dùng hoặc nhóm người dùng để truy cập in. Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.

   e. Nhấn vào **OK**.

9. Lưu các thay đổi của bạn.

Cách thêm quy tắc in trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.

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 **Security Controls** → **Device Control**.

5. Trong mục **Device access rules**, hãy nhấn liên kết **Devices and Wi-Fi networks**.

   Bảng này liệt kê các quy tắc truy cập cho tất cả các thiết bị có trong phân loại của thành phần Kiểm soát thiết bị.

6. Chọn loại thiết bị **Local printers** hoặc **Network printers**.

   Thao tác này sẽ mở các quy tắc truy cập máy in.

7. Cấu hình chế độ truy cập cho các máy in liên quan: **Allow**, **Block**, **Allow and do not log** (chỉ dành cho máy in qua mạng), **Depends on bus** (chỉ dành cho máy in cục bộ) hoặc **Custom**.

8. Nếu chọn chế độ **Custom**, bạn phải thêm quy tắc in cho máy in cục bộ hoặc máy in qua mạng. Để thực hiện, hãy nhấn nút **Add** trong bảng quy tắc in.

   Thao tác này sẽ mở thiết lập của quy tắc in mới.

9. Gán một mức ưu tiên cho mục quy tắc. Mục quy tắc bao gồm các thuộc tính sau: tài khoản người dùng, hành động (cho phép/chặn) 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 bạn 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.

10. Trong mục **Action**, hãy cấu hình quyền truy cập của người dùng để in trên máy in.

11. Trong mục **User or group**, hãy chọn người dùng hoặc nhóm người dùng để truy cập in. Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.

12. Lưu các thay đổi của bạn.

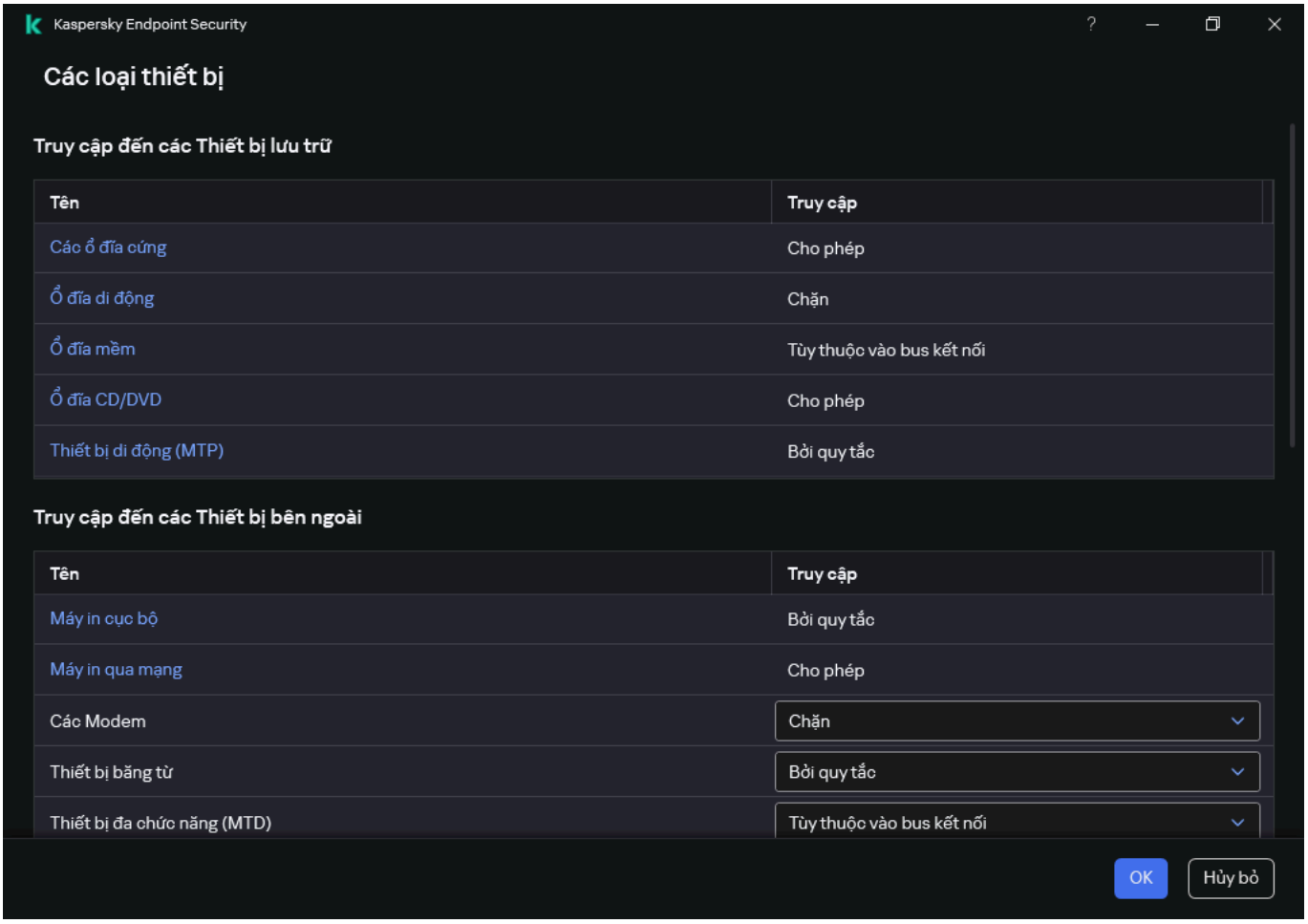
Cách thêm quy tắc in trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút ⚙.

2. Trong cửa sổ thiết lập ứng dụng, hãy chọn **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.



Các loại thiết bị trong thành phần Kiểm soát thiết bị

4. Trong mục **Truy cập đến các Thiết bị bên ngoài**, hãy nhấn vào **Máy in cục bộ** hoặc **Máy in qua mạng**.

   Thao tác này sẽ mở ra một cửa sổ chứa các quy tắc truy cập máy in.

5. Trong mục **Truy cập vào máy in cục bộ** hoặc **Truy cập vào máy in mạng** hãy cấu hình chế độ truy cập cho máy in: **Cho phép**, **Chặn**, **Cho phép và không ghi** (chỉ dành cho máy in qua mạng), **Tùy thuộc vào bus kết nối** (chỉ dành cho máy in cục bộ) hoặc **Bởi quy tắc**.

6. Nếu chọn chế độ **Bởi quy tắc**, bạn phải thêm quy tắc in cho máy in. Chọn người dùng hoặc nhóm người dùng mà bạn muốn áp dụng quy tắc in.

   a. Nhấn vào **Thêm**.

      Thao tác này sẽ mở ra một cửa sổ để thêm quy tắc in mới.

   b. Gán một mức ưu tiên cho mục quy tắc. Mục quy tắc bao gồm các thuộc tính sau: tài khoản người dùng, các quyền (cho phép/chặn) 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 bạn 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.

c. Trong mục **Hành động**, hãy cấu hình quyền truy cập của người dùng để in.

d. Trong mục **Người dùng và nhóm**, hãy chọn người dùng hoặc nhóm người dùng để truy cập in. Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.

7. Lưu các thay đổi của bạn.

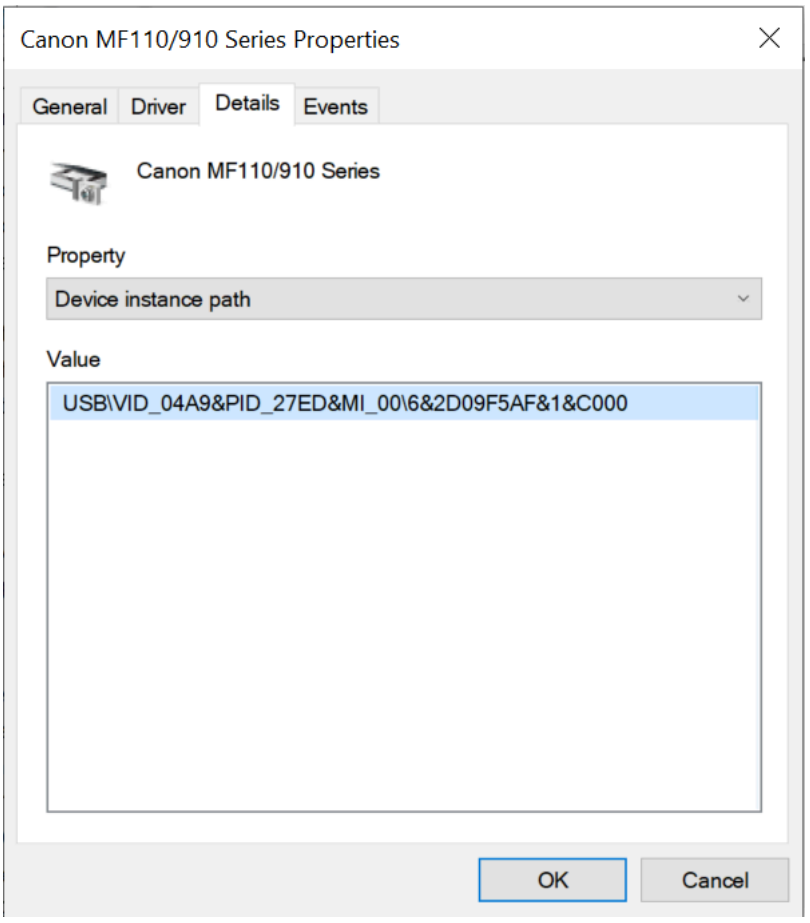
Máy in được tin tưởng

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.

Các bước để thêm máy in được tin tưởng hoàn toàn giống như các bước thêm các loại thiết bị được tin tưởng khác. Bạn có thể thêm máy in cục bộ theo ID hoặc mẫu máy của thiết bị. Bạn chỉ có thể thêm máy in qua mạng theo ID thiết bị.

Để thêm một máy in cục bộ được tin tưởng theo ID, bạn cần một ID duy nhất (Hardware ID – HWID). Bạn có thể tìm ID trong thuộc tính thiết bị bằng cách sử dụng các công cụ của hệ điều hành (xem hình bên dưới). Công cụ Device Manager cho phép bạn thực hiện việc này. ID của máy in cục bộ có thể trông như sau: `6&2D09F5AF&1&C000`. Thêm thiết bị theo ID là một cách thuận tiện nếu bạn muốn thêm một số thiết bị cụ thể. Bạn cũng có thể sử dụng ký tự đại diện.

Để thêm máy in cục bộ được tin tưởng theo mẫu máy của thiết bị, bạn sẽ cần Vendor ID (VID) và Product ID (PID) của thiết bị đó. Bạn có thể tìm cá ID trong thuộc tính thiết bị bằng cách sử dụng các công cụ của hệ điều hành (xem hình bên dưới). Mẫu để nhập VID và PID: `VID_04A9&PID_27FD`. 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.



ID thiết bị trong Trình quản lý thiết bị

Để thêm một máy in qua mạng được tin tưởng, bạn sẽ cần ID thiết bị của thiết bị đó. Đối với máy in qua mạng, ID thiết bị có thể là tên mạng của máy in (tên của máy in được chia sẻ), địa chỉ IP của máy in hoặc URL của máy in.

Kiểm soát các kết nối Wi-Fi

Kiểm soát thiết bị cho phép quản lý các kết nối Wi-Fi của máy tính (laptop). Các mạng Wi-Fi công cộng có thể không bảo mật và việc sử dụng các mạng như vậy có thể làm mất dữ liệu. Kiểm soát thiết bị cho phép bạn chặn người dùng kết nối với mạng Wi-Fi hoặc chỉ cho phép kết nối với các mạng được tin tưởng. Ví dụ: bạn có thể chỉ cho phép kết nối với mạng Wi-Fi công ty đủ bảo mật. 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.

Trên máy tính chạy Windows 11, bạn cần bật Dịch vụ định vị để kiểm soát các kết nối Wi-Fi. Để thực hiện việc này, bạn cần bật nút gạt **Dịch vụ định vị** chuyển đổi trong cài đặt hệ điều hành (**Cài đặt** → **Quyền riêng tư và bảo mật** → **Vị trí**). Nếu Dịch vụ định vị bị tắt, Kaspersky Endpoint Security sẽ không kiểm soát các kết nối với mạng Wi-Fi.

Cách hạn chế các kết nối Wi-Fi trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật → Kiểm soát thiết bị**.
4. Trong mục **Thiết lập Kiểm soát thiết bị**, hãy chọn thẻ **Các loại thiết bị**.

   Bảng này liệt kê các quy tắc truy cập cho tất cả các thiết bị có trong phân loại của thành phần Kiểm soát thiết bị.
5. Trong menu ngữ cảnh cho loại thiết bị **Wi-Fi**, hãy chọn hành động Kiểm soát thiết bị được thực hiện khi kết nối với mạng Wi-Fi: **Cho phép** (), **Chặn** () hoặc **Chặn với ngoại lệ** ().
6. Nếu bạn đã chọn tùy chọn **Chặn với ngoại lệ**, hãy tạo danh sách các mạng Wi-Fi được tin tưởng:

   a. Nhấn đúp để mở danh sách các mạng Wi-Fi được tin tưởng.

   b. Trong mục **Mạng Wi-Fi tin tưởng**, hãy nhấn nút **Thêm**.

   c. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy cấu hình mạng Wi-Fi được tin tưởng (xem hình bên dưới):

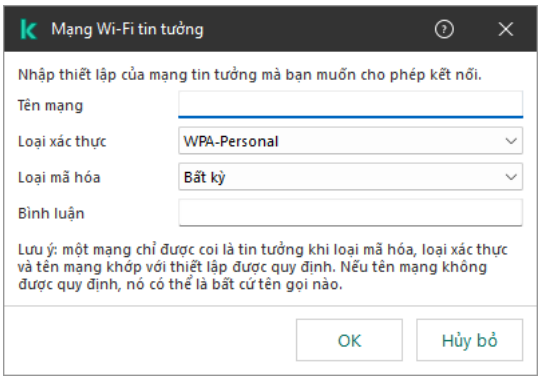
   - **Tên mạng**. Tên hoặc SSID (Service Set Identifier) của mạng Wi-Fi.
   - **Loại xác thực**. Loại xác thực được sử dụng khi kết nối với mạng Wi-Fi.

     Đã thêm hỗ trợ giao thức WPA3 vào ứng dụng kể từ Kaspersky Endpoint Security cho Windows phiên bản 12.0. Nếu một chính sách của Kaspersky Endpoint Security phiên bản 12.2 được áp dụng trên một máy tính thì giao thức WPA2 sẽ được chọn trên các máy tính có Kaspersky Endpoint Security phiên bản 11.11.0 trở về trước; WPA2/WPA3 được chọn cho các phiên bản 12.0 đến 12.1; WPA3 được chọn cho các phiên bản 12.2 trở lên.
   - **Loại mã hóa**. Loại mã hóa được sử dụng để bảo vệ lưu lượng truy cập Wi-Fi.
   - **Bình luận**. Thông tin thêm về mạng Wi-Fi đã thêm.

   Bạn có thể xem thiết lập của mạng Wi-Fi được tin tưởng trong thiết lập của bộ định tuyến.

   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.

7. Lưu các thay đổi của bạn.



Thiết lập của mạng Wi-Fi được tin tưởng

Cách hạn chế các kết nối Wi-Fi trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Security Controls** → **Device Control**.
5. Trong mục **Device access rules**, hãy chọn thẻ **Devices and Wi-Fi networks**.
   Bảng này liệt kê các quy tắc truy cập cho tất cả các thiết bị có trong phân loại của thành phần Kiểm soát thiết bị.
6. Trong mục **Wi-Fi networks**, hãy nhấn liên kết **Wi-Fi**.
7. Trong cửa sổ mở ra, hãy chọn hành động Kiểm soát thiết bị được thực hiện khi kết nối với mạng Wi-Fi: **Allow**, **Block** hoặc **Block with exclusions**.
8. Nếu bạn đã chọn tùy chọn **Block with exclusions**, hãy tạo danh sách các mạng Wi-Fi được tin tưởng:
   a. Nhấn đúp để mở danh sách các mạng Wi-Fi được tin tưởng.
   b. Trong mục **Trusted Wi-Fi networks**, hãy nhấn nút **Add**.
   c. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy cấu hình mạng Wi-Fi được tin tưởng (xem hình bên dưới):
      - **Name**. Tên hoặc SSID (Service Set Identifier) của mạng Wi-Fi.
      - **Authentication type**. Loại xác thực được sử dụng khi kết nối với mạng Wi-Fi.

> Đã thêm hỗ trợ giao thức WPA3 vào ứng dụng kể từ Kaspersky Endpoint Security cho Windows phiên bản 12.0. Nếu một chính sách của Kaspersky Endpoint Security phiên bản 12.2 được áp dụng trên một máy tính thì giao thức WPA2 sẽ được chọn trên các máy tính có Kaspersky Endpoint Security phiên bản 11.11.0 trở về trước; WPA2/WPA3 được chọn cho các phiên bản 12.0 đến 12.1; WPA3 được chọn cho các phiên bản 12.2 trở lên.

- **Encryption type**. Loại mã hóa được sử dụng để bảo vệ lưu lượng truy cập Wi-Fi.
- **Comment**. Thông tin thêm về mạng Wi-Fi đã thêm.

Bạn có thể xem thiết lập của mạng Wi-Fi được tin tưởng trong thiết lập của bộ định tuyến.

> Một mạng Wi-Fi được coi là tin tưởng nếu cấu hình của nó khớp với tất cả các cấu hình được quy định trong quy tắc.

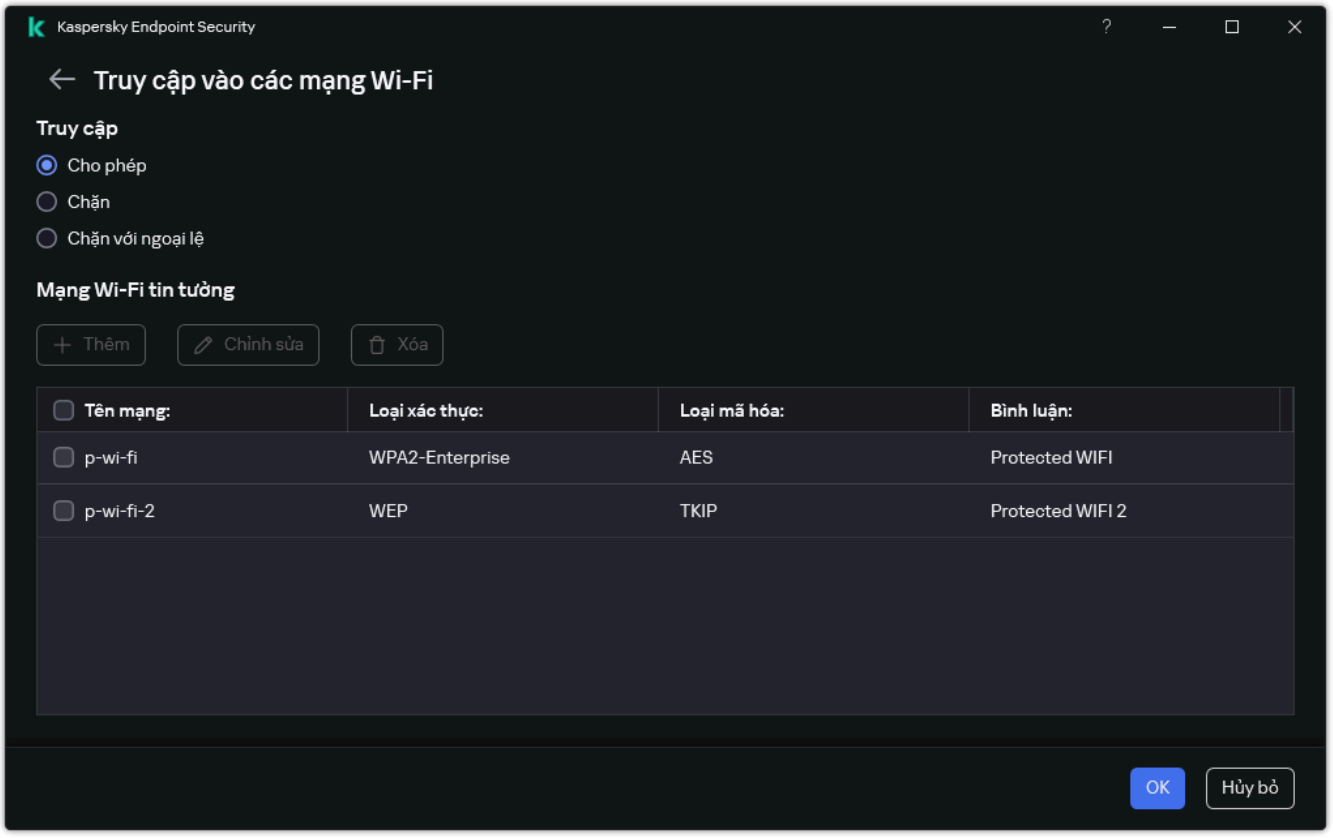
9. Lưu các thay đổi của bạn.

Cách hạn chế các kết nối Wi-Fi 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 **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.



Thiết lập truy cập Wi-Fi

5. Trong mục **Truy cập**, hãy chọn hành động Kiểm soát thiết bị được thực hiện khi kết nối với mạng Wi-Fi: **Cho phép**, **Chặn** hoặc **Chặn với ngoại lệ**.

6. Nếu bạn đã chọn tùy chọn **Chặn với ngoại lệ**, hãy tạo danh sách các mạng Wi-Fi được tin tưởng:

   a. Trong mục **Mạng Wi-Fi tin tưởng**, hãy nhấn nút **Thêm**.

   b. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy cấu hình mạng Wi-Fi được tin tưởng (xem hình bên dưới):

   - **Tên mạng**. Tên hoặc SSID (Service Set Identifier) của mạng Wi-Fi.
   - **Loại xác thực**. Loại xác thực được sử dụng khi kết nối với mạng Wi-Fi.

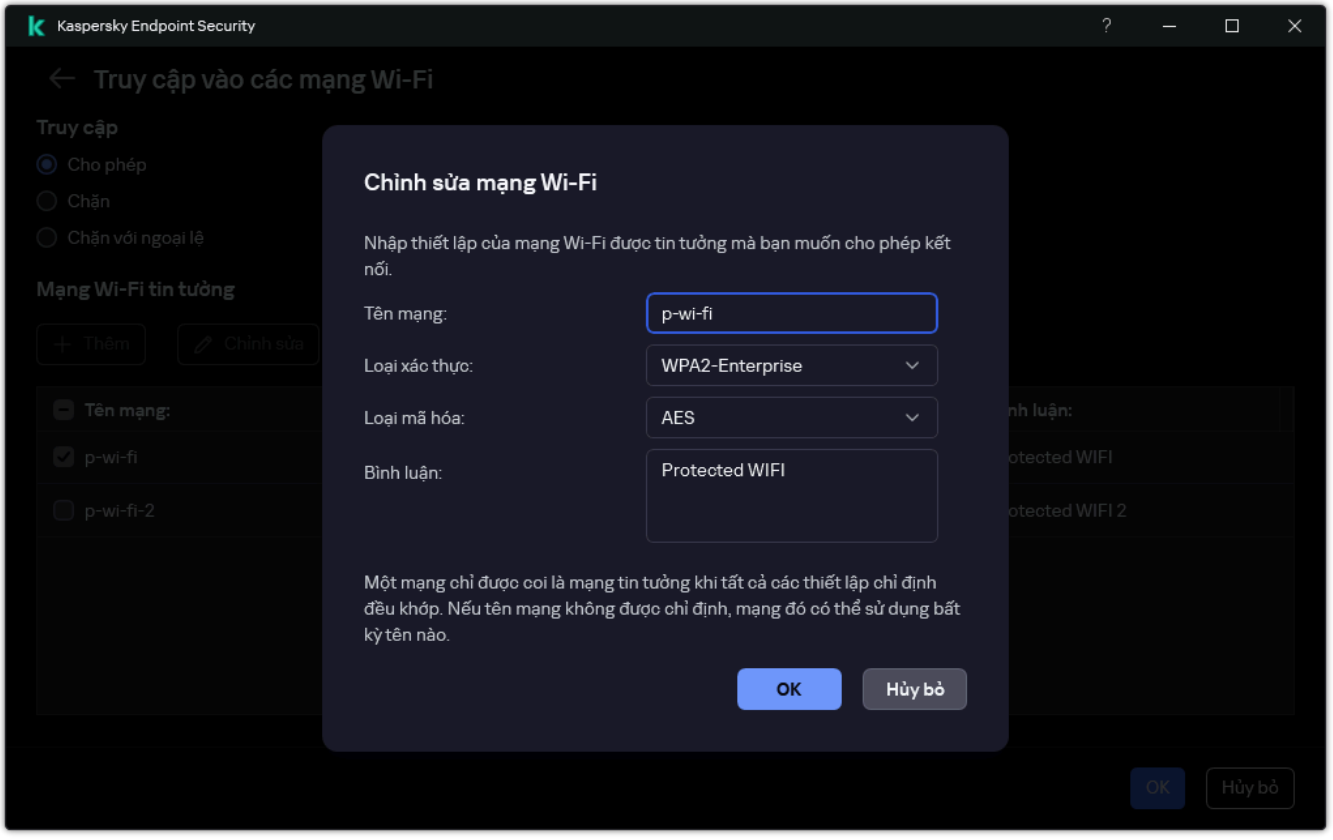
     Đã thêm hỗ trợ giao thức WPA3 vào ứng dụng kể từ Kaspersky Endpoint Security cho Windows phiên bản 12.0. Nếu một chính sách của Kaspersky Endpoint Security phiên bản 12.2 được áp dụng trên một máy tính thì giao thức WPA2 sẽ được chọn trên các máy tính có Kaspersky Endpoint Security phiên bản 11.11.0 trở về trước; WPA2/WPA3 được chọn cho các phiên bản 12.0 đến 12.1; WPA3 được chọn cho các phiên bản 12.2 trở lên.

   - **Loại mã hóa**. Loại mã hóa được sử dụng để bảo vệ lưu lượng truy cập Wi-Fi.
   - **Bình luận**. Thông tin thêm về mạng Wi-Fi đã thêm.

   Bạn có thể xem thiết lập của mạng Wi-Fi được tin tưởng trong thiết lập của bộ định tuyến.

   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.

7. Lưu các thay đổi của bạn.



Thiết lập của mạng Wi-Fi được tin tưởng

Kết quả là khi người dùng cố gắng kết nối với mạng Wi-Fi không có trong danh sách được tin tưởng thì ứng dụng sẽ chặn kết nối và hiển thị thông báo (xem hình bên dưới).



Thông báo Kiểm soát thiết bị

Giám sát việc sử dụng ổ đĩa di động

Giám sát việc sử dụng ổ đĩa di động bao gồm:

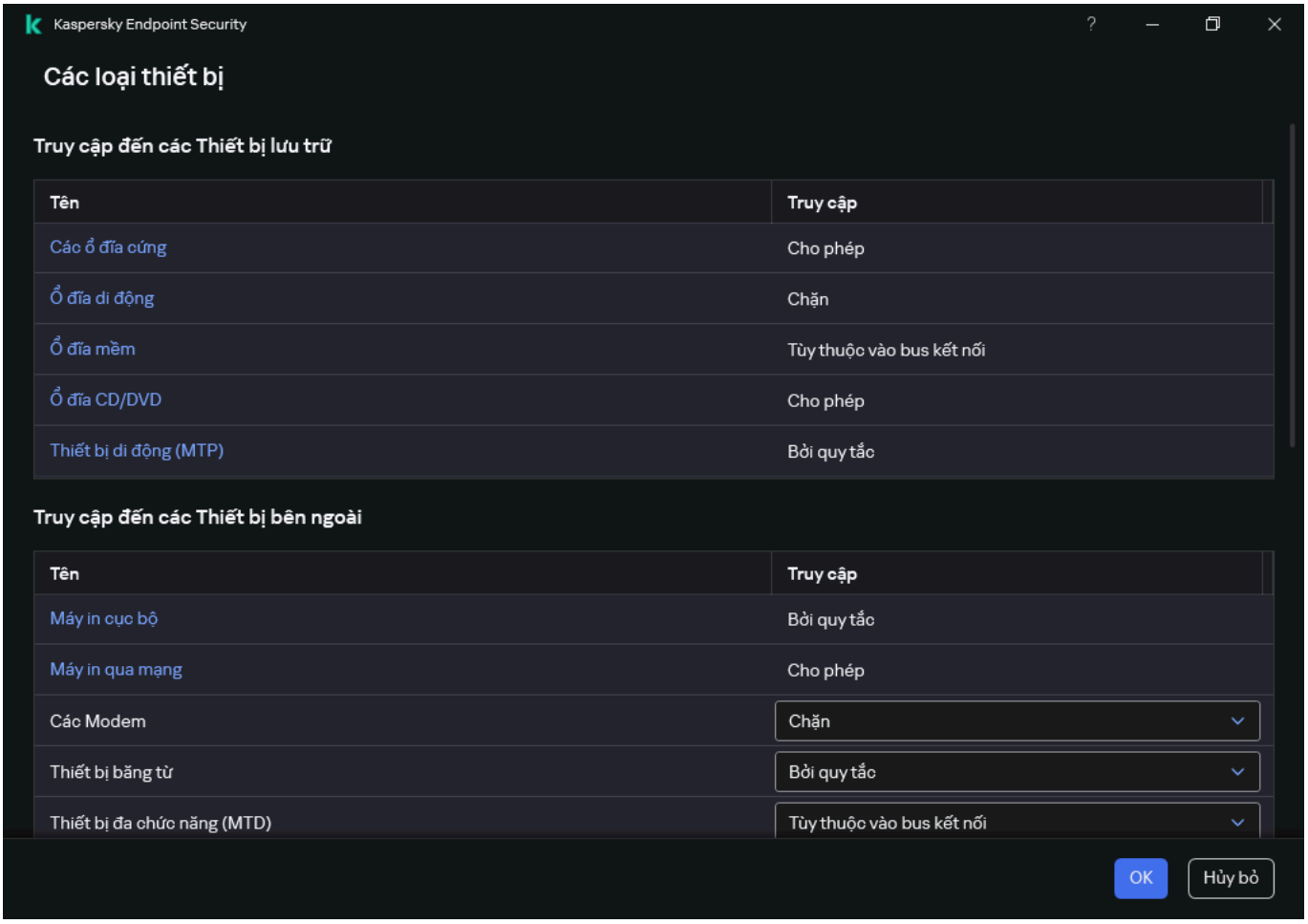
- Giám sát hoạt động trên các tập tin trên ổ đĩa di động.
- Giám sát kết nối và ngắt kết nối của các ổ đĩa di động được tin tưởng.

  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**.

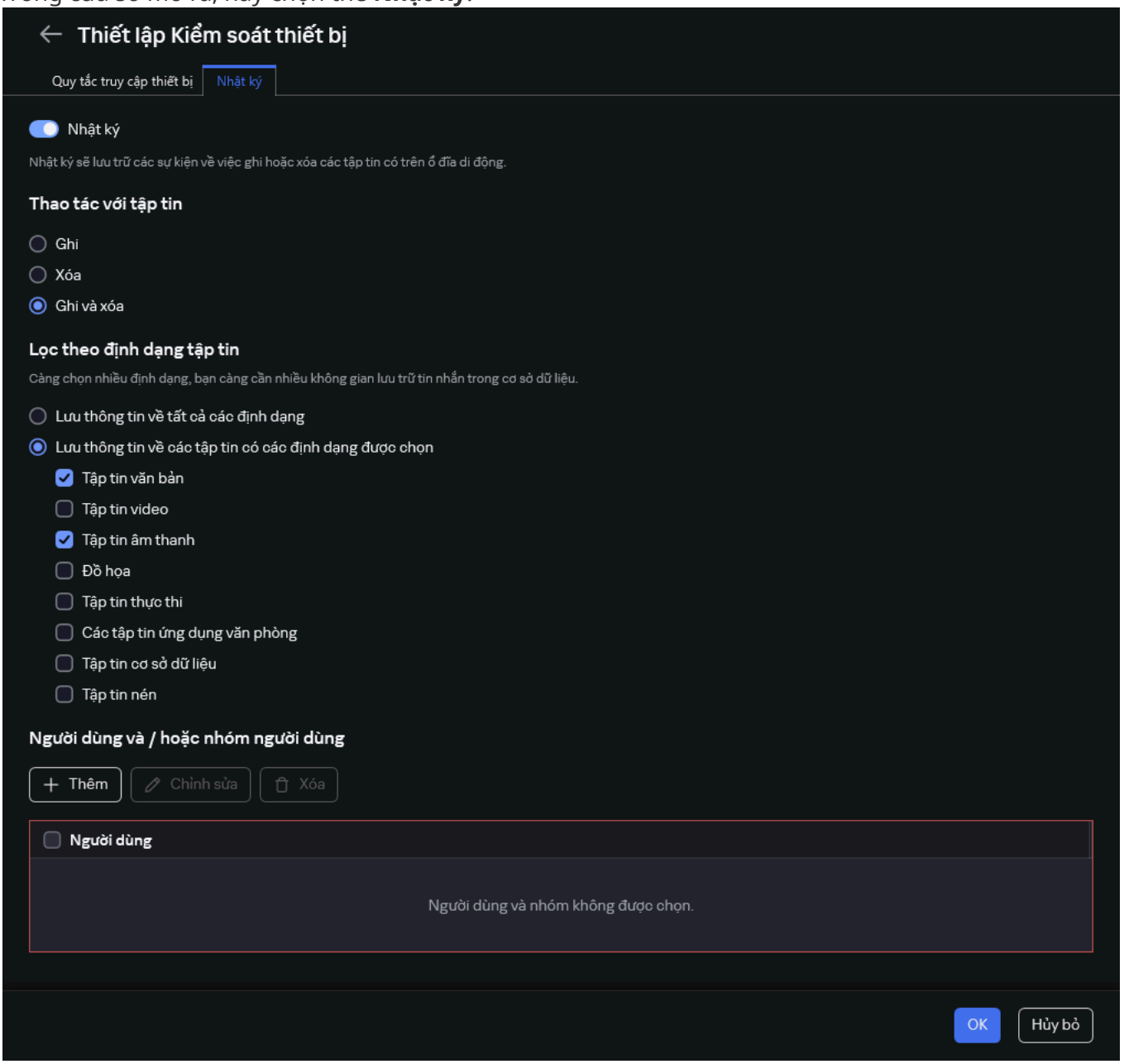
Cửa sổ được mở sẽ hiển thị các quy tắc truy cập cho tất cả các thiết bị được thêm vào danh mục thành phần Kiểm soát thiết bị.



Các loại thiết bị trong 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**.



Thiết lập giám sát sử dụng ổ đĩa di động

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 **Events**. 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
- Cho phép ứng dụng thực hiện 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.14.2\environment]`
   - Đối với hệ điều hành 32-bit:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES.14.2\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 được tin tưởng và cấu hình quyền truy cập của người dùng.

Bạn không nên thêm quá 5000 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 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 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 *Informational messages*.

Thêm thiết bị vào danh sách được tin tưởng

Kaspersky Security Center sẽ nhận thông tin về các thiết bị nếu Kaspersky Endpoint Security được cài đặt trên máy tính, Kiểm soát thiết bị được bật và truyền dữ liệu 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.

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).

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 (Hardware ID hay HWID). Bạn có thể xem ID trong thuộc tính thiết bị bằng cách sử dụng công cụ hệ điều hành. Ví dụ về ID thiết bị: `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 Vendor ID (VID) và một Product ID (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_*`.

Cách thêm thiết bị 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 cây bảng điều khiển, hãy chọn **Policies**.

3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

4. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật → Kiểm soát thiết bị**.

5. Ở phần bên phải của cửa sổ, chọn thẻ **Thiết bị 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 thiết 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.

7. Nhấn vào nút **Thêm** và chọn phương thức để thêm thiết bị vào danh sách được tin tưởng.

8. Để lọc thiết bị, hãy chọn loại thiết bị trong danh sách thả xuống **Loại thiết bị** (ví dụ: **Ổ đĩa di động**).

> Kaspersky Endpoint Security không hỗ trợ việc thêm thiết bị thuộc loại **Ổ đĩa mềm** vào danh sách được tin tưởng.

9. 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 **Upgrade**. Để hiển thị đúng danh sách các thiết bị, bạn có thể thêm thiết bị theo tên đại diện ID thiết bị.

10. Để lọc các thiết bị, trong trường **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.

11. Nhấn vào **Upgrade**.

    Bảng này hiển thị danh sách các thiết bị đáp ứng các tiêu chí lọc được xác định.

12. Chọn các hộp kiểm cạnh tên của thiết bị mà bạn muốn thêm vào danh sách các thiết bị được tin tưởng.

13. Trong trường **Bình luận**, hãy nhập mô tả lý do thêm thiết bị vào danh sách được tin tưởng.

14. Nhấn vào nút **Select** ở bên phải trường **Cho phép người dùng và / hoặc nhóm người dùng**.

    Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.

    Theo mặc định, nhóm mọi người được phép truy cập vào các thiết bị được tin tưởng.

15. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách thêm thiết bị vào danh sách được tin tưởng trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.
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 **Trusted Zone**.
5. Trong cửa sổ mở ra, hãy nhấn vào liên kết **Devices**.

   Thao tác này sẽ mở cửa sổ chứa danh sách các thiết bị được tin tưởng.
6. Ở phần bên phải của cửa sổ, chọn thẻ **Thiết bị được tin tưởng**.

7. Chọn hộp kiểm **Merge values when inheriting** nếu bạn muốn tạo một danh sách tổng hợp các thiết 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 **Add**.

   Thao tác này sẽ mở ra biểu mẫu để thêm thiết bị được tin tưởng.

9. Trong mục **User or group**, hãy chọn những người dùng mà bạn muốn cho phép truy cập vào các thiết bị được tin tưởng.

   Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.

   Theo mặc định, nhóm mọi người được phép truy cập vào các thiết bị được tin tưởng.

10. Để lọc thiết bị, hãy chọn loại thiết bị trong danh sách thả xuống **Device type** (ví dụ: **Removable drives**).

    Kaspersky Endpoint Security không hỗ trợ việc thêm thiết bị thuộc loại **Floppy disks** vào danh sách được tin tưởng.

11. Nếu bạn không biết chính xác ID thiết bị hoặc kiểu máy, hãy chọn hộp kiểm **Use mask**.

12. Chọn cách bạn muốn thêm thiết bị: bằng ID thiết bị hoặc kiểu máy (VID và PID).

    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 thiết bị trống sẽ được hiển thị trong Kaspersky Security Center. Để hiển thị đúng danh sách các thiết bị, bạn có thể thêm thiết bị theo tên đại diện ID thiết bị.

13. Để lọc các thiết bị, trong trường **Search for trusted devices**, 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.

    Bảng này hiển thị danh sách các thiết bị đáp ứng các tiêu chí lọc được xác định.

14. Chọn các hộp kiểm cạnh tên của thiết bị mà bạn muốn thêm vào danh sách các thiết bị được tin tưởng.

15. Trong trường **Comment**, hãy nhập mô tả lý do thêm thiết bị vào danh sách được tin tưởng.

16. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách thêm thiết bị 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 **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.

   > Kaspersky Endpoint Security không hỗ trợ việc thêm thiết bị thuộc loại **Ổ đĩa mềm** 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.

   Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.
8. 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.

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

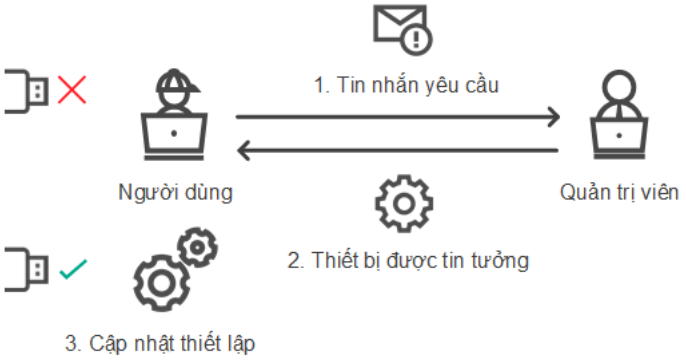
Bạn chỉ có thể cấp quyền truy cập tới một thiết bị bị chặn ở chế độ trực tuyến nếu Kaspersky Security Center được triển khai trong tổ chức và máy tính đó đã được áp dụng chính sách. Máy tính đó phải có khả năng thiết lập một kết nối với Máy chủ quản trị.

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 nhận được một tin nhắn kèm yêu cầu trong bảng điều khiển Kaspersky Security Center.

   Bảng điều khiển Kaspersky Security Center có lựa chọn sự kiện được định trước *User requests* để tiện theo dõi tin nhắn từ người dùng.
3. 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.
4. 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

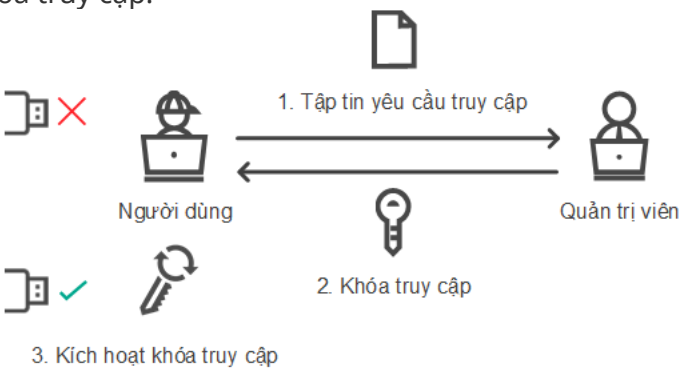
Chế độ ngoại tuyến để cấp quyền truy cập

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 các 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**.



Thông báo Kiểm soát thiết bị

Tiếp theo, quản trị viên trong bảng điều khiển Kaspersky Security Center sẽ nhận được sự kiện *Thông báo chặn truy cập thiết bị gửi đến quản trị viên*. Sự kiện này bao gồm tên người dùng, tên máy tính, thông tin chi tiết về thiết bị mà người dùng đang cố gắng truy cập và các thông tin khác. Bạn có thể cấu hình cách quản trị viên được thông báo về các sự kiện như vậy, chẳng hạn như chọn thông báo qua email. Bảng điều khiển Kaspersky Security Center có lựa chọn sự kiện được định trước *User requests* để tiện theo dõi tin nhắn từ người dùng.

Để cho phép truy cập, bạn phải thêm thiết bị vào danh sách được tin tưởng. Sau khi bạn cập nhật thiết lập Kaspersky Endpoint Security trên máy tính, người dùng có thể có quyền truy cập vào 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 các 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 mạn 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. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, 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 **Asset management → Assets (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 **Overview** 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 dụng 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 viến 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. Các chuyên gia của Kaspersky cung cấp cho người dùng mẫu tin nhắn mô tả lý do tại sao thiết bị lại bị chặn truy cập (xem hình bên dưới).

Các biến đặc biệt được cung cấp để quản lý mẫu tin nhắn (ví dụ: `%USER_NAME%`). Biến cho phép sử dụng một mẫu tin nhắn duy nhất cho nhiều máy tính khác nhau. Khi tạo tin nhắn, Kaspersky Endpoint Security sẽ lấy giá trị của biến từ thiết lập của hệ điều hành và chèn vào tin nhắn phù hợp với máy tính, người dùng và sự kiện cụ thể.



Thông báo Kiểm soát thiết bị

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. Để thực hiện, người dùng phải nhấn vào **Yêu cầu truy cập** hoặc **Yêu cầu quyền truy cập tạm thời** và gửi tin nhắn cho quản trị viên để mô tả tình huống. Bạn cũng có thể chuẩn bị mẫu tin nhắn gửi cho quản trị viên, thêm vào đó dữ liệu có thể giúp bạn đưa ra quyết định cho phép hay chặn quyền truy cập thiết bị. 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.

Cách thay đổi mẫu tin nhắn của Kiểm soát thiết bị trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật → Kiểm soát thiết bị**.
4. Trong mục **Thiết lập mẫu tin nhắn**, hãy nhấn nút **Mẫu**.
5. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy cấu hình mẫu Kiểm soát ứng dụng:

   - **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.

   Để thêm biến vào văn bản mẫu, hãy đặt con trỏ vào vị trí mong muốn, nhấn vào **Biến số** và chọn biến cần dùng trong danh sách các tùy chọn có sẵn.

Bạn cũng có thể khôi phục mẫu văn bản mặc định.

6. Lưu các thay đổi của bạn.

Cách thay đổi mẫu tin nhắn của Kiểm soát thiết bị trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Security Controls** → **Device Control**.
5. Trong mục **Message templates**, hãy cấu hình các mẫu cho tin nhắn Kiểm soát ứng dụng:

   - **Message to user**. 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.
   - **Message to administrator**. 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.

   Để thêm biến vào văn bản mẫu, hãy đặt con trỏ vào vị trí mong muốn, nhấn vào **Add variable** và chọn biến cần dùng trong danh sách các tùy chọn có sẵn.

   Bạn cũng có thể khôi phục mẫu văn bản mặc định.
6. Lưu các thay đổi của bạn.

Cách thay đổi mẫu tin nhắn của Kiểm soát thiết bị 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 **Kiểm soát bảo mật** → **Kiểm soát ứng dụng**.
3. Trong mục **Tin nhắn mẫu**, hãy cấu hình các mẫu cho tin nhắn Kiểm soát ứng dụng:

   - **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.

   Để thêm biến vào văn bản mẫu, hãy đặt con trỏ vào vị trí mong muốn, nhấn vào **Thêm biến số** và chọn biến cần dùng trong danh sách các tùy chọn có sẵn.

   Bạn cũng có thể khôi phục mẫu văn bản mặc 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 không điển hình (ví dụ, quy tắc *Khởi chạy Microsoft PowerShell từ ứng dụng office*). 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

Việc 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 huấn luyện, Kaspersky Endpoint Security sẽ ghi lại sự kiện này trong báo cáo kích hoạt quy tắc và kho lưu trữ **Rule triggers in Smart Training state**.

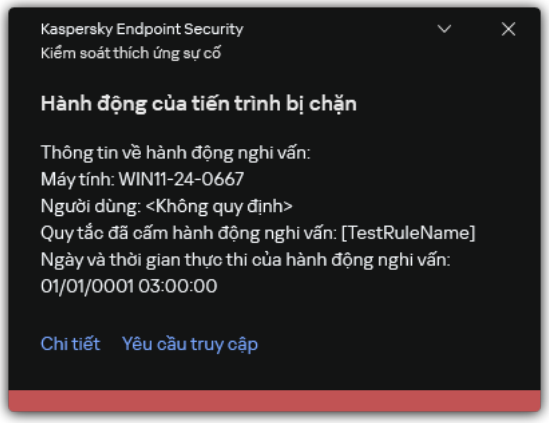
2. Phân tích báo cáo kích hoạt quy tắc.

   Quản trị viên sẽ phân tích báo cáo kích hoạt quy tắc hoặc nội dung của kho lưu trữ **Rule triggers 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 theo thời gian thực 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 **Rule triggers in Smart Training state**. Bạn nên kiểm tra báo cáo về việc kích hoạt các quy tắc và nội dung của kho lưu trữ **Rule triggers in Smart Training state**.

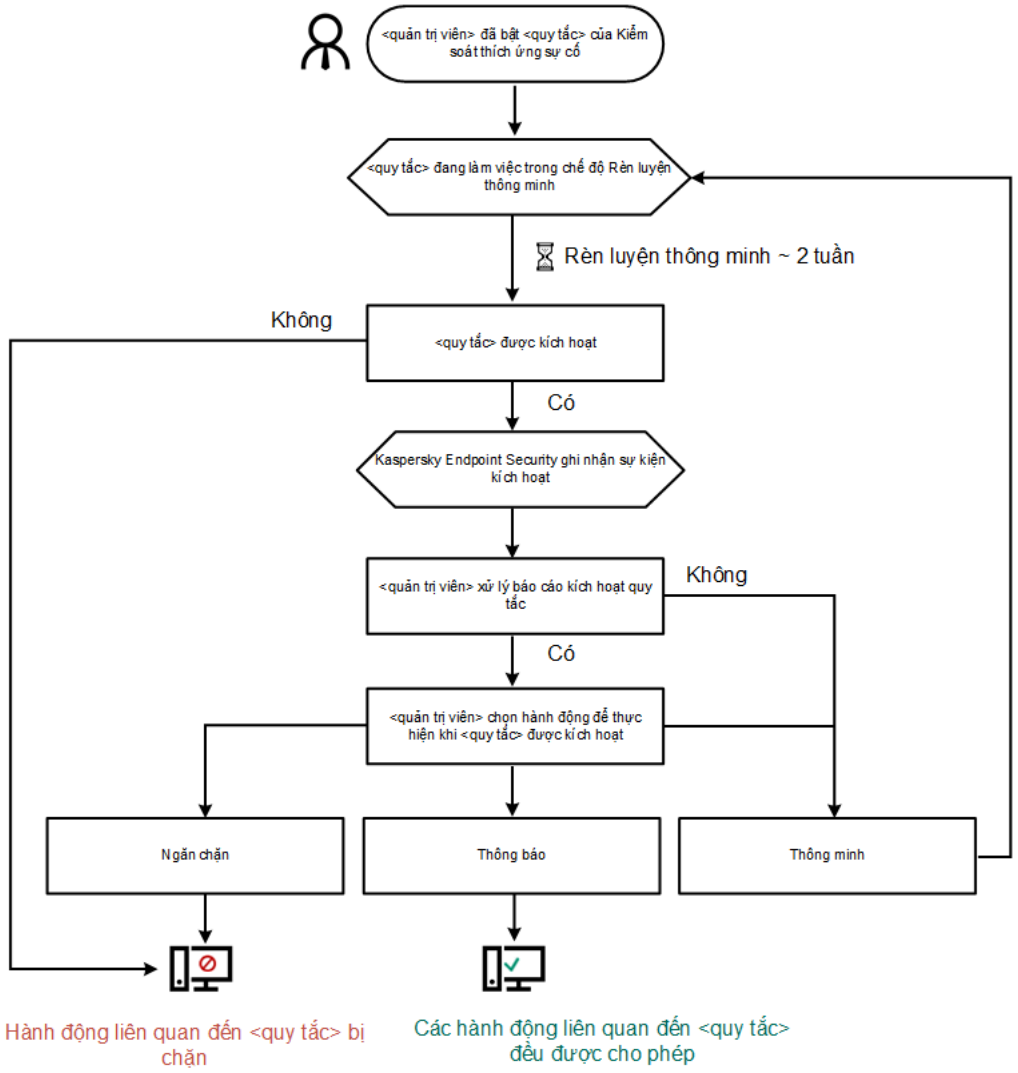
Khi một ứng dụng độc hại cố gắng thực hiện một hành động, Kaspersky Endpoint Security sẽ chặn hành động đó và hiển thị một thông báo (xem hình dưới đây).



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

Rèn luyện Kiểm soát thích ứng sự cố

Kiểm soát thích ứng sự cố bao gồm một tập hợp các quy tắc (mẫu hành vi). 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. Kiểm soát thích ứng sự cố không chặn hoạt động của ứng dụng trên máy tính mà chỉ thông báo cho quản trị viên. Bạn cũng có thể chọn hành động được thực hiện theo cách thủ công khi quy tắc Kiểm soát thích ứng sự cố được kích hoạt.

Cách xem danh sách quy tắc Kiểm soát thích ứng sự cố trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.

2. Trong cây bảng điều khiển, hãy chọn **Policies**.

3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Security Controls → Adaptive Anomaly Control**.
5. Chọn hộp kiểm **Kiểm soát thích ứng sự cố**.
6. Trong mục **Thiết lập quy tắc Kiểm soát thích ứng sự cố**, hãy xem danh sách các quy tắc.
   Theo mặc định, tất cả các quy tắc đều hoạt động ở chế độ **Thông minh**.
7. Nếu cần, hãy xác nhận việc cập nhật quy tắc Kiểm soát thích ứng sự cố.
8. Nếu cần, hãy chọn một hành động khi quy tắc Kiểm soát thích ứng sự cố được kích hoạt:
   - **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.
9. Nếu cần, hãy vô hiệu những quy tắc mà bạn không muốn sử dụng.
10. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách xem quy tắc Kiểm soát thích ứng sự cố trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management → Policies**.
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 **Security Controls → Adaptive Anomaly Control**.
5. Bật nút bật/tắt **Adaptive Anomaly Control ENABLED**.
6. Trong mục **Rules**, hãy xem danh sách các quy tắc.
   Theo mặc định, tất cả các quy tắc đều hoạt động ở chế độ **Smart**.
7. Nếu cần, hãy xác nhận việc cập nhật quy tắc Kiểm soát thích ứng sự cố.
8. Nếu cần, hãy chọn một hành động khi quy tắc Kiểm soát thích ứng sự cố được kích hoạt:
   - **Block**. 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.
   - **Inform**. 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.

9. Nếu cần, hãy vô hiệu những quy tắc mà bạn không muốn sử dụng.
10. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách xem danh sách quy tắc Kiểm soát thích ứng sự cố 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 **Security Controls → Adaptive Anomaly Control**.
3. Bật nút bật/tắt **Kiểm soát thích ứng sự cố**.
4. Trong mục **Quy tắc**, hãy nhấn liên kết **Chỉnh sửa quy tắc**.

   Danh sách quy tắc Kiểm soát thích ứng sự cố sẽ mở ra. Theo mặc định, tất cả các quy tắc đều hoạt động ở chế độ **Thông minh**.
5. Nếu cần, hãy xác nhận việc cập nhật quy tắc Kiểm soát thích ứng sự cố.
6. Nếu cần, hãy chọn một hành động khi quy tắc Kiểm soát thích ứng sự cố được kích hoạt:

   - **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. Nếu cần, hãy vô hiệu những quy tắc mà bạn không muốn sử dụng.
8. Lưu các thay đổi của bạn.

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 trong quá trình đào tạo có một quy tắc không bao giờ được kích hoạt, Kiểm soát thích ứng sự cố sẽ coi hành vi đó là không điển hình và thay đổi trạng thái của quy tắc thành **Chặn thông minh**. Sau đó, ứng dụng sẽ chặn mọi hoạt động phù hợp với quy tắc này.

Nếu một quy tắc được kích hoạt trong quá trình đào tạo, bạn cần phải cấu hình thủ công hành động mà ứng dụng áp dụng cho hoạt động được phát hiện phù hợp với quy tắc này. Nếu bạn không chọn hành động khi quy tắc được kích hoạt, Kiểm soát thích ứng sự cố sẽ tiếp tục ở chế độ đào tạo.

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 chạy Microsoft PowerShell từ ứng dụng office*).

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**, hãy 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 **Rule triggers 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 nút **Thêm**.

   Cửa sổ thuộc tính loại trừ sẽ mở ra.
7. Chọn người dùng mà bạn muốn cấu hình một mục loại trừ.

   Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.

   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**. Giá trị hash SHA256 của 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... Chỉ định đối tượng theo mẫu sau: `object://<object>`, trong đó `<object>` chỉ 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**. Giá trị hash SHA256 của 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**. Giá trị hash SHA256 của tập tin.

    - **Đối tượng đích**. Lệnh để khởi chạy tiến trình đích. Quy định lệnh theo dạng sau `object://<command>`, 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**. Giá trị hash SHA256 của 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 loại trừ:

a. Nhấn vào **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 *Đã 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.

Có sẵn các mẫu đặc biệt để gửi tin nhắn cho người quản trị về việc chặn hành động có khả năng gây hại. Các biến đặc biệt được cung cấp để quản lý mẫu tin nhắn (ví dụ: `%USER_NAME%`). Biến cho phép sử dụng một mẫu tin nhắn duy nhất cho nhiều máy tính khác nhau. Khi tạo tin nhắn, Kaspersky Endpoint Security sẽ lấy giá trị của biến từ thiết lập của hệ điều hành và chèn vào tin nhắn phù hợp với máy tính, người dùng và sự kiện cụ thể.

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.

   Để thêm biến vào văn bản mẫu, hãy đặt con trỏ vào vị trí mong muốn, nhấn vào **Thêm biến số** và chọn biến cần dùng trong danh sách các tùy chọn có sẵn.

   Bạn cũng có thể khôi phục văn bản mẫu mặc định bằng cách sử dụng nút **Đặt lại**.
4. Lưu các thay đổi của bạn.

Giám sát hoạt động của Kiểm soát thích ứng sự cố

Kiểm soát thích ứng sự cố bao gồm một số công cụ giám sát. Mục đích chính của việc giám sát Kiểm soát thích ứng sự cố là để cấu hình thành phần trong quá trình đào tạo.

Báo cáo Kiểm soát thích ứng sự cố

Kiểm soát thích ứng sự cố sử dụng các báo cáo sau:

- **Báo cáo về trạng thái các quy tắc Kiểm soát thích ứng sự cố**. Báo cáo chứa thông tin về trạng thái của các quy tắc Kiểm soát thích ứng sự cố (*Off*, *Smart Training*, *Smart Block*, *Notify*, *Block*). Báo cáo này cho phép phân tích mức độ đào tạo của Kiểm soát thích ứng sự cố và đánh giá số lượng quy tắc đã chuyển từ chế độ *Smart Training* sang chế độ hoạt động bình thường (ví dụ: *Smart Block*).

- **Báo cáo về các quy tắc Kiểm soát thích ứng sự cố được kích hoạt**. Báo cáo chứa thông tin về các quy tắc kích hoạt. Báo cáo cũng hiển thị chế độ kích hoạt quy tắc: *Block* (bao gồm *Smart Block*) hoặc *Notify*. Báo cáo này cho phép đánh giá hoạt động của Kiểm soát thích ứng sự cố trên máy tính của người dùng.

Cách xem báo cáo Kiểm soát thích ứng sự cố trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật → Kiểm soát thích ứng sự cố**.

4. Thực hiện một trong các thao tác sau:

   - Nếu bạn muốn xem báo cáo về trạng thái quy tắc Kiểm soát thích ứng sự cố, hãy nhấn vào liên kết **Báo cáo về trạng thái các quy tắc Kiểm soát thích ứng sự cố**.

   - Nếu bạn muốn xem báo cáo về quy tắc Kiểm soát thích ứng sự cố đã kích hoạt, hãy nhấn vào liên kết **Báo cáo về các quy tắc Kiểm soát thích ứng sự cố được kích hoạt**.

5. Tiến trình tạo báo cáo sẽ được bắt đầu.

   Báo cáo sẽ được hiển thị trong một cửa sổ mới.

Cách xem báo cáo Kiểm soát thích ứng sự cố trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management → Policies**.

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 **Security Controls → Adaptive Anomaly Control**.

5. Trong mục **Rules**, hãy thực hiện một trong những hành động sau:

   - Nếu bạn muốn xem báo cáo về trạng thái quy tắc Kiểm soát thích ứng sự cố, hãy chọn **View report → Rules state**.

   - Nếu bạn muốn xem báo cáo về quy tắc Kiểm soát thích ứng sự cố đã kích hoạt, hãy nhấn vào **View report → Detections**.

6. Tiến trình tạo báo cáo sẽ được bắt đầu.

Báo cáo sẽ được hiển thị trong một cửa sổ mới.

Để tạo báo cáo trong bảng điều khiển Kaspersky Security Center, bạn phải bật tính năng truyền dữ liệu tới Máy chủ quản trị. Truyền dữ liệu được bật theo mặc định.

Cách bật truyền dữ liệu cho Kiểm soát thích ứng sự cố trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Các báo cáo và lưu trữ**.
4. Trong mục **Truyền dữ liệu đến Máy chủ quản trị**, hãy nhấn nút **Thiết lập**.
5. Đánh dấu vào các ô sau:
   - **Báo cáo về trạng thái các quy tắc Kiểm soát thích ứng sự cố**.
   - **Báo cáo về các quy tắc Kiểm soát thích ứng sự cố được kích hoạt**.
6. Lưu các thay đổi của bạn.

Cách bật truyền dữ liệu cho Kiểm soát thích ứng sự cố trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Policies**.
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 → KSC Integration**.
5. Trong mục **Data transfer to Administration Server**, hãy chọn các hộp kiểm sau:
   - **Report on Adaptive Anomaly Control rules state**.
   - **Report on triggered Adaptive Anomaly Control rules**.
6. Lưu các thay đổi của bạn.

Lưu trữ Rule triggers in Smart Training state

Ở chế độ đào tạo, Kiểm soát thích ứng sự cố sẽ gửi thông tin về các quy tắc được kích hoạt đến một kho lưu trữ riêng biệt, **Rule triggers in Smart Training state**. Thông tin về các quy tắc được kích hoạt được thể hiện trong kho lưu trữ dưới dạng danh sách các sự kiện. Để tinh chỉnh Kiểm soát thích ứng sự cố, bạn có thể xác nhận hành vi bất thường trên máy tính hoặc thêm một loại trừ khỏi quy tắc.

Sự kiện Kiểm soát thích ứng sự cố

Kiểm soát thích ứng sự cố sẽ ghi lại các sự kiện quy tắc trong các chế độ *Block* (bao gồm *Smart Block*) và *Notify*. Các sự kiện sau đây được cung cấp cho mục đích này:

Process action blocked

Process action skipped

Sự kiện chứa thông tin về hoạt động đáng ngờ bao gồm mã tổng kiểm của tập tin, người dùng liên quan, thời gian kích hoạt quy tắc và tên máy tính. Sau khi phân tích sự kiện, bạn có thể ngay lập tức thêm các loại trừ khỏi quy tắc nếu thấy hoạt động đó hợp lệ.

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* hoặc danh mục khác), 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. Quản trị viên có thể tạo nhiều quy tắc. Một ứng dụng có thể khớp tiêu chí của nhiều quy tắc. Một quy tắc chặn được ưu tiên hơn một quy tắc cho phép. Kaspersky Endpoint Security sẽ kiểm tra xem ứng dụng có khớp với quy tắc nào không mỗi khi khởi động. Kaspersky Endpoint Security sẽ so sánh tuần tự ứng dụng với tất cả các quy tắc Kiểm soát ứng dụng.

3. Chọn chế độ Kiểm soát ứng dụng.

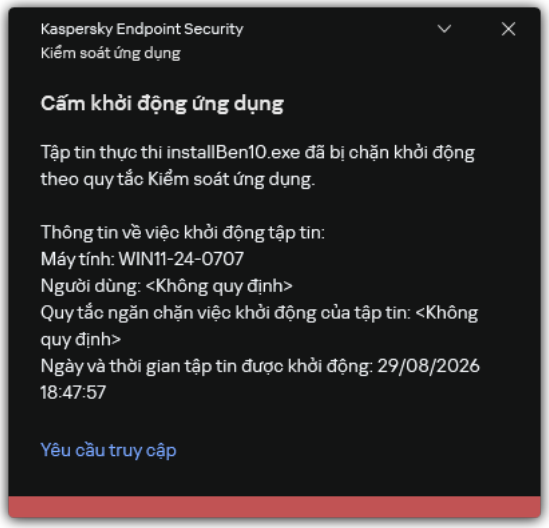
   Quản trị viên sẽ chọn chế độ làm việc với các ứng dụng không có trong bất kỳ quy tắc nào (danh sách ứng dụng không được phép và được phép).

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.

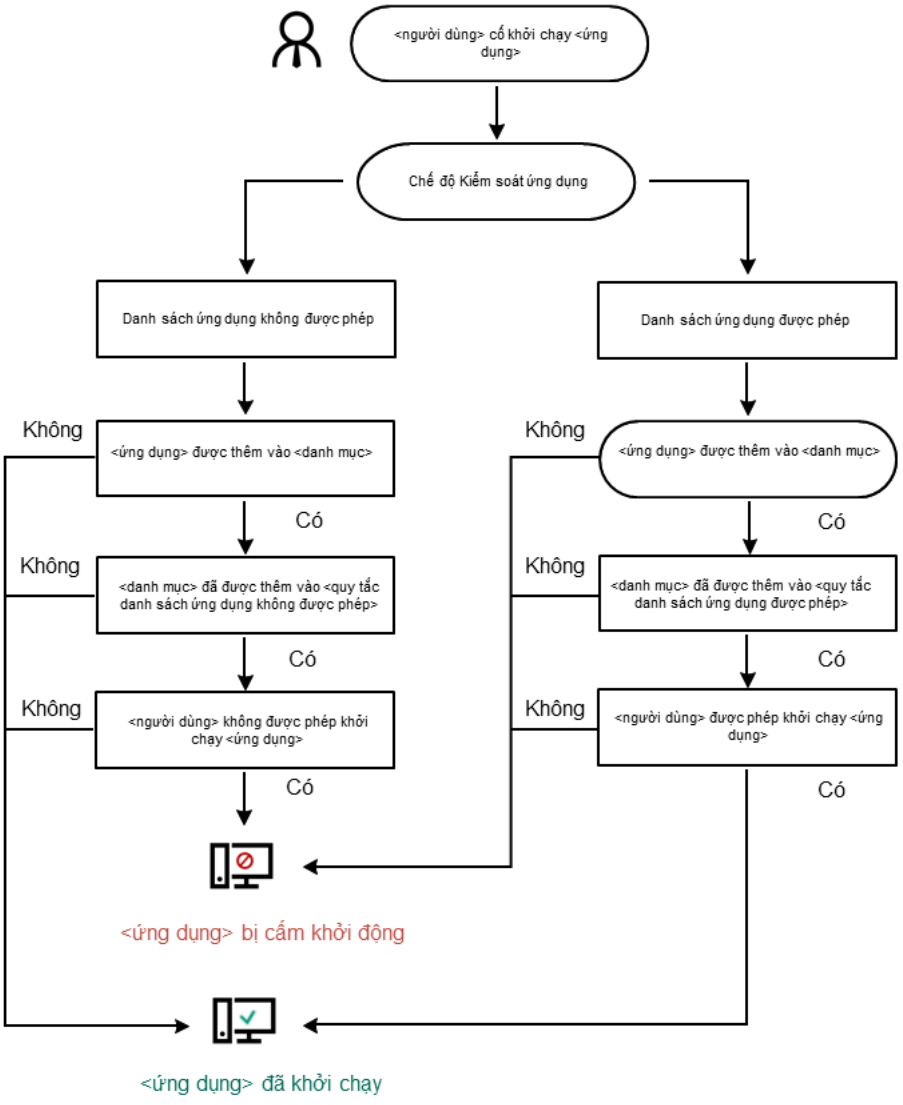
  Quy tắc kiểm soát ứng dụng được tạo trong Bảng điều khiển quản trị Kaspersky Security Center dựa trên các danh mục ứng dụng tùy chỉnh của bạn chứ không dựa trên các điều kiện bao gồm và loại trừ như trong trường hợp trong giao diện cục bộ của Kaspersky Endpoint Security.

- 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.
- 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 **Phần mềm khác\Các ứng dụng được tin tưởng theo danh tiếng trong KSN** có thể sẽ khác tùy thuộc vào việc có kết nối khả dụng đến các 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

Lấy thông tin về các ứng dụng được cài đặt

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.

Xem thông tin ứng dụng

Thông tin về các ứng dụng đã cài đặt được cung cấp bởi Kaspersky Security Center Network Agent. Thông tin về các ứng dụng đã cài đặt có sẵn trong bảng điều khiển Kaspersky Security Center trong thư mục **Applications registry**. Network Agent sẽ cập nhật thông tin sau mỗi lần đồng bộ hóa với Kaspersky Security Center. Để biết thêm chi tiết về thông tin được gửi bởi Network Agent, vui lòng tham khảo Trợ giúp của Kaspersky Security Center.

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 **Advanced → Application management → Applications registry**.
3. Chọn một ứng dụng.
4. Trong menu ngữ cảnh của ứng dụng, hãy chọn **Properties**.

Xem thông tin về các tập tin thực thi

Bạn có thể giảm tải cho cơ sở dữ liệu khi truy vấn thông tin về các tập tin thực thi. Để đạt được điều này, bạn nên chạy tác vụ *Kho* trên một số máy tính tham chiếu có bộ phần mềm tiêu chuẩn được cài đặt của bạn.

Thông tin về các tập tin thực thi được cung cấp bởi Kaspersky Endpoint Security. Để nhận thông tin phần cứng, bạn cần áp dụng một chính sách chủ động cho phép truyền thông tin của các ứng dụng được cài đặt (truyền thông tin được bật theo mặc định).

Cách kích hoạt tính năng gửi thông tin ứng dụng trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Các báo cáo và lưu trữ**.
4. Trong mục **Truyền dữ liệu đến Máy chủ quản trị**, hãy nhấn nút **Thiết lập**.
5. Chọn hộp kiểm **Các ứng dụng khởi động**.
6. Lưu các thay đổi của bạn.

Cách bật gửi thông tin 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 **Asset management → Policies**.
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 → KSC Integration**.
5. Trong mục **Data transfer to Administration Server**, hãy nhấn nút **Advanced settings**.
6. Trong cửa sổ mở ra, hãy chọn hộp kiểm **About started applications**.
7. Lưu các thay đổi của bạn.

Bạn có thể lấy danh sách các tập tin thực thi bằng cách sử dụng tác vụ *Kho* của Kaspersky Endpoint Security. Bạn có thể xem danh sách các tập tin thực thi trong bảng điều khiển Kaspersky Security Center, trong thư mục **Executable files**.

Trước khi chạy tác vụ *Kho*, hãy đảm bảo rằng cơ sở dữ liệu đáp ứng các khuyến nghị của Kaspersky Security Center. Để biết chi tiết về các hạn chế của cơ sở dữ liệu, vui lòng tham khảo Trợ giúp của Kaspersky Security Center.

Cách chạy tác vụ Kho trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Tasks**.
   Danh sách tác vụ sẽ mở.
2. Nhấn vào **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 (14.2)** → **Kho**.

Bước 2. Phạm vi kiểm kê

Tạo danh sách các thư mục mà bạn muốn Kaspersky Endpoint Security tìm kiếm các tập tin thực thi. Cấu hình thiết lập kiểm kê (xem bảng bên dưới).

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. Chọn tài khoản để chạy tác vụ

Chọn một tài khoản để chạy tác vụ *Kho*. Theo mặc định, Kaspersky Endpoint Security khởi chạy tác vụ với quyền của tài khoản người dùng cục bộ. Nếu phạm vi kiểm kê 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 5. Cấu hình lịch khởi chạy tác vụ

Cấu hình lịch tác vụ, ví dụ như theo cách thủ công.

Bước 6. Xác định tên tác vụ

Nhập tên cho tác vụ, ví dụ: *Kiểm kê cơ sở*.

Bước 7. Hoàn tất việc tạo tác vụ

Hoàn tất 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, việc tìm kiếm các tập tin thực thi sẽ được thực hiện trên máy tính của người dùng theo lịch đã cấu hình.

Cách chạy một tác vụ Kho trong Bảng điều khiển web và Bảng điều khiển đám mây

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

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **Add**.

   Trình hướng dẫn Tác vụ sẽ được bắt đầu.

3. Cấu hình các thiết lập của tác vụ:

   a. Trong danh sách thả xuống **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.

   b. Trong danh sách thả xuống **Task type**, hãy chọn **Inventory**.

   c. Trong trường **Task name**, nhập một mô tả ngắn gọn, ví dụ như *Kiểm kê cơ sở*.

   d. Trong phần **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. Chọn một tài khoản để chạy tác vụ. Theo mặc định, Kaspersky Endpoint Security khởi chạy tác vụ với quyền của tài khoản người dùng cục bộ.

6. Hoàn tất trình hướng dẫn.

   Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ.

7. Để cấu hình tác vụ, hãy vào thuộc tính tác vụ (xem bảng bên dưới).

8. Chọn hộp kiểm cạnh tác vụ.

9. Nhấn vào **Start**.

   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, các tập tin thực thi sẽ được tìm kiếm trên máy tính của người dùng theo lịch được quy định.

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, hãy chọn **Advanced** → **Application management** → **Executable files**.

3. Chọn một tập tin thực thi.

4. Trong menu ngữ cảnh của tập tin thực thi, chọn **Properties**.

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**.

Cập nhật thông tin về các ứng dụng được cài đặt và các tập tin thực thi

Đã tối ưu hóa hoạt động của thành phần Kiểm soát ứng dụng với cơ sở dữ liệu các tập tin thực thi trong Kaspersky Endpoint Security. Kaspersky Endpoint Security tự động cập nhật cơ sở dữ liệu sau khi tập tin bị xóa khỏi máy tính. Điều này cho phép cập nhật cơ sở dữ liệu và tiết kiệm tài nguyên của Kaspersky Security Center. Để cơ sở dữ liệu các ứng dụng được cài đặt được cập nhật, bạn phải bật gửi thông tin ứng dụng đến Máy chủ quản trị (tính năng đó được bật theo mặc định).

Thiết lập kiểm kê

Tham số	Mô tả
Inventory scopes	Danh sách các đối tượng sẽ tạo thành phạm vi kiểm kê.
DLL modules inventory	Kaspersky Endpoint Security tìm kiếm các mô-đun DLL trong phạm vi kiểm kê và gửi thông tin đến Kaspersky Security Center. Việc bật tính năng kiểm kê mô-đun DLL sẽ làm tăng đáng kể thời gian hoàn thành tác vụ Kiểm kê và kích thước của cơ sở dữ liệu.
Script files inventory	Kaspersky Endpoint Security tìm kiếm các tập lệnh trong phạm vi kiểm kê và gửi thông tin đến Kaspersky Security Center. Việc bật tính năng kiểm kê tập tin tập lệnh sẽ làm tăng đáng kể thời gian hoàn thành tác vụ Kiểm kê và kích thước của cơ sở dữ liệu.

Tham số	Mô tả
Run only when the computer is idle	Hoãn bắt đầu tác vụ 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. Tùy chọn lịch này cho phép bạn bảo tiết kiệm nguyên máy tính khi máy tính đang được sử dụng.
Scan only new and modified files	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.
Skip file that is scanned for longer than (sec) N giây	Giới hạn thời gian thực thi tác vụ. Sau một khoảng thời gian được quy định, Kaspersky Endpoint Security sẽ dừng tác vụ đó. 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.
Scan archives	Quét định dạng ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE, và các định dạng tập tin nén khác. Ứng dụng 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).
Scan distribution packages	Quét các gói phân phối của ứng dụng bên thứ ba.
Do not unpack large compound files	Nếu hộp kiểm này được chọn, ứng dụng sẽ không quét các tập tin hỗn hợp nếu dung lượng của chúng vượt quá giá trị ấn định. Nếu bỏ chọn hộp kiểm này, ứng dụng sẽ quét các tập tin tổ hợp thuộc mọi kích thước. Ứng dụng sẽ quét các tập tin lớn được trích xuất từ tập tin nén, bất kể hộp kiểm này có được chọn hay không.

Cách bật chế độ Ứng dụng bị chặn

Chế độ này sẽ là *Ứng dụng bị chặn* khi 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. Tức là, nếu không có quy tắc từ chối nào tồn tại, Kiểm soát ứng dụng sẽ cho phép khởi chạy ứng dụng. Chế độ này của thành phần Kiểm soát ứng dụng được bật theo mặc định.

Trước khi kích hoạt chế độ *Ứng dụng bị chặn*, bạn nên thử nghiệm các quy tắc Kiểm soát ứng dụng của mình. Vì mục đích này, bạn có thể bật chế độ thử nghiệm.

Cách bật chế độ Ứng dụng bị chặn trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật → Kiểm soát ứng dụng**.
5. Chọn hộp kiểm **Kiểm soát ứng dụng**.
6. Trong mục **Thiết lập Kiểm soát ứng dụng**, hãy sử dụng danh sách thả xuống **Chế độ kiểm soát** để chọn **Danh sách không được phép**.
7. Trong danh sách thả xuống **Hành động**, hãy chọn hành động cho Kiểm soát ứng dụng:
   - **Kiểm tra quy tắc**. Kiểm soát ứng dụng không chặn các ứng dụng bị ngăn chạy theo quy tắc, mà tạo ra các sự kiện về hoạt động chạy các ứng dụng vốn sẽ bị chặn.
   - **Áp dụng quy tắc**. Kiểm soát ứng dụng chặn các ứng dụng bị chặn và tạo ra các sự kiện tương ứng.

8. Chọn trạng thái cho quy tắc Kiểm soát ứng dụng:

- **Bật**. Trạng thái này có nghĩa rằng quy tắc được sử dụng khi thành phần Kiểm soát ứng dụng đang chạy.
- **Tắt**. Trạng thái này có nghĩa rằng quy tắc bị bỏ qua khi thành phần Kiểm soát ứng dụng đang chạy.
- **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.

Nếu cần, hãy thêm quy tắc Kiểm soát ứng dụng mới.

9. Cấu hình các thiết lập nâng cao của Kiểm soát ứng dụng:

- **Giám sát việc tải các mô-đun DLL (tăng mức tải đáng kể lên hệ thống)**. 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.

  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 "**Tập tin ảnh hoàn hảo\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.

  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.

- **Sử dụng xác minh chữ ký số nghiêm ngặt**. Bạn có thể chọn chứng chỉ làm điều kiện kích hoạt cho một quy tắc Kiểm soát ứng dụng. Nếu chọn hộp kiểm này, Kaspersky Endpoint Security sẽ chỉ áp dụng các quy tắc cho các ứng dụng được ký bằng chứng chỉ từ kho chứng chỉ hệ thống được tin tưởng. Các ứng dụng được ký bằng chứng chỉ như vậy cũng được coi là được tin tưởng bởi các thành phần bảo vệ, ví dụ như tác vụ *Quét phần mềm độc hại*. Tuy nhiên, nếu bạn chỉ định chứng chỉ từ một kho khác trong quy tắc Kiểm soát ứng dụng thì Kaspersky Endpoint Security sẽ không áp dụng quy tắc đó.

  Nếu bỏ chọn hộp kiểm này, Kaspersky Endpoint Security sẽ áp dụng các quy tắc cho các ứng dụng được ký bằng chứng chỉ từ Windows Trusted Root Certificate Store (Kho chứng chỉ gốc được tin tưởng của Windows). Những ứng dụng như vậy không thuộc vùng tin tưởng. Các thành phần bảo vệ sẽ giám sát hoạt động của các ứng dụng đó.

- **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 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.

10. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật chế độ Ứng dụng 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 thẻ **Asset management** → **Policies**.
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 **Security Controls** → **App Control**.
5. Bật nút bật/tắt **Application Control ENABLED**.
6. Trong mục **Operating mode**, hãy chọn **Block all except the rules list**.
7. Trong mục **Action**, hãy chọn hành động cho Kiểm soát ứng dụng:
   - **Inform**. Kiểm soát ứng dụng không chặn các ứng dụng bị ngăn chạy theo quy tắc, mà tạo ra các sự kiện về hoạt động chạy các ứng dụng vốn sẽ bị chặn.
   - **Apply rules**. Kiểm soát ứng dụng chặn các ứng dụng bị chặn và tạo ra các sự kiện tương ứng.
8. Chọn trạng thái cho quy tắc Kiểm soát ứng dụng:
   - **Enabled**. Trạng thái này có nghĩa rằng quy tắc được sử dụng khi thành phần Kiểm soát ứng dụng đang chạy.
   - **Disabled**. Trạng thái này có nghĩa rằng quy tắc bị bỏ qua khi thành phần Kiểm soát ứng dụng đang chạy.
   - **Test mode**. 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.

   Nếu cần, hãy thêm quy tắc Kiểm soát ứng dụng mới.
9. Cấu hình các thiết lập nâng cao của Kiểm soát ứng dụng:
   - **Monitor loading of DLL modules**. 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.

     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 "**Tập tin ảnh hoàn hảo\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.

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.

- **Use strict digital signature verification**. Bạn có thể chọn chứng chỉ làm điều kiện kích hoạt cho một quy tắc Kiểm soát ứng dụng. Nếu chọn hộp kiểm này, Kaspersky Endpoint Security sẽ chỉ áp dụng các quy tắc cho các ứng dụng được ký bằng chứng chỉ từ kho chứng chỉ hệ thống được tin tưởng. Các ứng dụng được ký bằng chứng chỉ như vậy cũng được coi là được tin tưởng bởi các thành phần bảo vệ, ví dụ như tác vụ *Quét phần mềm độc hại*. Tuy nhiên, nếu bạn chỉ định chứng chỉ từ một kho khác trong quy tắc Kiểm soát ứng dụng thì Kaspersky Endpoint Security sẽ không áp dụng quy tắc đó.

  Nếu bỏ chọn hộp kiểm này, Kaspersky Endpoint Security sẽ áp dụng các quy tắc cho các ứng dụng được ký bằng chứng chỉ từ Windows Trusted Root Certificate Store (Kho chứng chỉ gốc được tin tưởng của Windows). Những ứng dụng như vậy không thuộc vùng tin tưởng. Các thành phần bảo vệ sẽ giám sát hoạt động của các ứng dụng đó.

- **Message to user**. Mẫu thông báo được hiển thị khi kích hoạt một quy tắc Kiểm soát ứng dụng chặn ứng dụng khởi chạy.

- **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.

10. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật chế độ Ứng dụng bị chặn 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 **Kiểm soát bảo mật → Kiểm soát ứng dụng**.
3. Bật nút bật/tắt **Kiểm soát ứng dụng**.
4. Trong mục **Chế độ Kiểm soát khởi động ứng dụng**, hãy chọn **Danh sách không được phép. Tất cả các ứng dụng, trừ các ứng dụng trong danh sách quy tắc mới được cho phép**.
5. Trong mục **Hành động khi khởi động các ứng dụng bị chặn theo quy tắc**, hãy chọn hành động cho Kiểm soát ứng dụng:

   - **Thông báo (Chế độ thử nghiệm) và ghi lại sự kiện trong báo cáo**. Kiểm soát ứng dụng không chặn các ứng dụng bị ngăn chạy theo quy tắc, mà tạo ra các sự kiện về việc chạy các ứng dụng vốn sẽ bị chặn.

   - **Chặn**. Kiểm soát ứng dụng chặn các ứng dụng bị chặn và tạo ra các sự kiện tương ứng.

6. Chọn trạng thái cho quy tắc Kiểm soát ứng dụng:

- **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.
- **Chế độ thử nghiệm**. 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.

Nếu cần, hãy thêm quy tắc Kiểm soát ứng dụng mới.

7. Cấu hình các thiết lập nâng cao của Kiểm soát ứng dụng:

- **Giám sát việc tải các mô-đun DLL**. 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.

  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 "**Tập tin ảnh hoàn hảo\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.

  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.

- **Sử dụng xác minh chữ ký số nghiêm ngặt**. Bạn có thể chọn chứng chỉ làm điều kiện kích hoạt cho một quy tắc Kiểm soát ứng dụng. Nếu chọn hộp kiểm này, Kaspersky Endpoint Security sẽ chỉ áp dụng các quy tắc cho các ứng dụng được ký bằng chứng chỉ từ kho chứng chỉ hệ thống được tin tưởng. Các ứng dụng được ký bằng chứng chỉ như vậy cũng được coi là được tin tưởng bởi các thành phần bảo vệ, ví dụ như tác vụ *Quét phần mềm độc hại*. Tuy nhiên, nếu bạn chỉ định chứng chỉ từ một kho khác trong quy tắc Kiểm soát ứng dụng thì Kaspersky Endpoint Security sẽ không áp dụng quy tắc đó.

  Nếu bỏ chọn hộp kiểm này, Kaspersky Endpoint Security sẽ áp dụng các quy tắc cho các ứng dụng được ký bằng chứng chỉ từ Windows Trusted Root Certificate Store (Kho chứng chỉ gốc được tin tưởng của Windows). Những ứng dụng như vậy không thuộc vùng tin tưởng. Các thành phần bảo vệ sẽ giám sát hoạt động của các ứng dụng đó.

- **Mẫu tin nhắn về việc chặn ứng dụng**. Mẫu thông báo được hiển thị khi kích hoạt một quy tắc Kiểm soát ứng dụng chặn ứng dụng khởi chạy.
- **Mẫu tin nhắn văn bản được hiển thị khi một ứng dụng bị chặn từ khi khởi động**. 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.

8. Lưu các thay đổi của bạn.

Kết quả là, Kiểm soát ứng dụng sẽ chặn các ứng dụng bị chặn. Kaspersky Endpoint Security cũng tạo sự kiện *Cấm khởi động ứng dụng*. Bạn có thể sử dụng các sự kiện này để tạo báo cáo *Report on prohibited applications* trong bảng điều khiển Kaspersky Security Center. Trong phần tóm tắt của báo cáo, bạn có thể xem danh sách các ứng dụng và máy tính mà quy tắc Kiểm soát ứng dụng đã kích hoạt.

Kiểm soát ứng dụng dựa trên máy tính cơ sở

Bạn có thể sử dụng máy tính cơ sở để tạo ảnh chứa một bộ ứng dụng mà bạn cần. Sau đó, bạn có thể sử dụng ảnh này để triển khai hệ điều hành và ứng dụng trên các máy tính khác. Không phải lúc nào cũng có thể cập nhật ảnh. Kiểm soát ứng dụng cho phép bạn duy trì danh sách các ứng dụng được cho phép dựa trên máy tính cơ sở. Kiểm soát ứng dụng sẽ tự động xác định ứng dụng nào được cài đặt trên máy tính cơ sở và sẽ cập nhật danh mục. Bằng cách này, máy tính sẽ nhận được danh sách cập nhật về các ứng dụng được cho phép.

Việc cấu hình Kiểm soát ứng dụng dựa trên máy tính cơ sở bao gồm các bước sau:

1. Tạo danh mục tự động cập nhật. Khi tạo danh mục mới, hãy chọn danh mục **Category that includes executable files from a specific folder** và chọn máy tính cơ sở của bạn.

   Cách tạo danh mục tự động cập nhật 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, hãy chọn **Advanced → Application management → Application categories**.
   3. Nhấn nút **New category** trong không gian làm việc.

      Thao tác này sẽ khởi chạy trình hướng dẫn tạo danh mục ứng dụng.
   4. Làm theo chỉ dẫn của trình hướng dẫn tạo danh mục ứng dụng.

Bước 1. Chọn loại danh mục

Chọn **Category that includes executable files from selected devices** làm loại danh mục.

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

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 **Add** 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 SHA256 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.

Bước 4. Lọc

Ở bước này, hãy cấu hình bộ lọc cho các tập tin.

Bạn có thể chỉ định loại tập tin muốn sử dụng để tạo danh mục ứng dụng.

- **All files**. Danh mục này sẽ khớp với tất cả các tập tin. Tùy chọn này được chọn mặc định.
- **Only files outside the application categories**. Danh mục này chỉ khớp với các tập tin nằm ngoài danh mục ứng dụng.

Bạn có thể chỉ định các thư mục của máy tính đã chọn, nơi chứa các tập tin mà bạn muốn sử dụng để tạo danh mục ứng dụng.

- **All folders**. Danh mục này sẽ khớp với tất cả các thư mục. Tùy chọn này được chọn mặc định.
- **Specified folder**. Danh mục này chỉ khớp với thư mục được chỉ định. Nếu chọn tùy chọn này, bạn cần chỉ định đường dẫn thư mục.

Bước 5. Tạo một danh mục tùy chỉnh

Hoàn tất trình hướng dẫn.

Cách tạo danh mục chứa nội dung được thêm tự động trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Operations** → **Third-party applications** → **Application categories**.

   Thao tác này sẽ mở danh sách danh mục ứng dụng.

2. Nhấn vào **Add**.

   Thao tác này sẽ khởi chạy trình hướng dẫn tạo danh mục ứng dụng.

3. Cấu hình thiết lập tổng quát của danh mục ứng dụng:

   - Tên danh mục.
   - Phương thức tạo danh mục. Chọn **Category that includes executable files from selected devices** làm loại danh mục.

   Chuyển sang bước tiếp theo.

4. Cấu hình thiết lập nâng cao của danh mục ứng dụng:

   - Chỉ định máy tính được Kaspersky Security Center thêm tập tin thực thi vào danh mục ứng dụng. 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.
   - Chọn một thuật toán tính toán hàm tạo hash.
   - Cấu hình khoảng thời gian để đồng bộ dữ liệu với kho lưu trữ của Máy chủ quản trị.
   - Cấu hình bộ lọc cho các tập tin.

5. Hoàn tất trình hướng dẫn.

Khi tạo danh mục tự động cập nhật, có thể sẽ thuận tiện hơn khi chia các tập tin thành nhiều danh mục. Ví dụ: tập tin hệ điều hành và tập tin từ thư mục Program Files. Để thực hiện, bạn có thể sử dụng bộ lọc trong thiết lập danh mục và chọn từng thư mục riêng lẻ.

2. Chọn chế độ Kiểm soát ứng dụng. Bạn cần ngăn thực thi tất cả các ứng dụng không được cho phép rõ ràng. Để thực hiện, hãy chọn chế độ *Ứng dụng bị chặn*.

3. Tạo một Quy tắc kiểm soát ứng dụng. Trong thiết lập quy tắc, hãy chọn danh mục chứa các tập tin thực thi từ máy tính cơ sở.

   Cách cấu hình Kiểm soát ứng dụng dựa trên máy tính cơ sở trong Bảng điều khiển quản trị (MMC)

   1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
   2. Trong cây bảng điều khiển, hãy chọn **Policies**.
   3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
   4. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật** → **Kiểm soát ứng dụng**.
   5. Chọn hộp kiểm **Kiểm soát ứng dụng**.

6. Trong mục **Thiết lập Kiểm soát ứng dụng**, hãy sử dụng danh sách thả xuống **Chế độ kiểm soát** để chọn **Danh sách không được phép**.

7. Trong danh sách thả xuống **Hành động**, hãy chọn hành động cho Kiểm soát ứng dụng:

   - **Kiểm tra quy tắc**. Kiểm soát ứng dụng không chặn các ứng dụng bị ngăn chạy theo quy tắc, mà tạo ra các sự kiện về hoạt động chạy các ứng dụng vốn sẽ bị chặn.

   - **Áp dụng quy tắc**. Kiểm soát ứng dụng chặn các ứng dụng bị chặn và tạo ra các sự kiện tương ứng.

8. Trong danh sách quy tắc Kiểm soát ứng dụng, hãy nhấn nút **Thêm**.

   Thao tác này sẽ khởi chạy trình hướng dẫn để thêm quy tắc Kiểm soát ứng dụng.

9. Trong danh sách thả xuống **Danh mục**, hãy chọn danh mục được cập nhật tự động dựa trên máy tính cơ sở.

10. Chọn người dùng hoặc nhóm người dùng mà bạn muốn áp dụng quy tắc Kiểm soát ứng dụng.

11. Cấu hình thiết lập nâng cao của quy tắc Kiểm soát ứng dụng:

    - **Từ chối người sử dụng khác**. Ứng dụng ngăn khởi chạy các ứng dụng thuộc danh mục đã chọn đối với tất cả người dùng không có trong danh sách.

    - **Trình cập nhật được tin tưởng**. Kaspersky Endpoint Security coi các ứng dụng được bao gồm trong danh mục được chọn là các trình cập nhật được tin tưởng, được phép tạo các tập tin thực thi khác có thể chạy sau đó.

12. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách cấu hình Kiểm soát ứng dụng dựa trên máy tính cơ sở trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management → Policies**.

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 **Security Controls → App Control**.

5. Bật nút bật/tắt **Application Control ENABLED**.

6. Trong mục **Operating mode**, hãy chọn **Block all except the rules list**.

7. Trong mục **Action**, hãy chọn hành động cho Kiểm soát ứng dụng:

   - **Inform**. Kiểm soát ứng dụng không chặn các ứng dụng bị ngăn chạy theo quy tắc, mà tạo ra các sự kiện về hoạt động chạy các ứng dụng vốn sẽ bị chặn.

   - **Apply rules**. Kiểm soát ứng dụng chặn các ứng dụng bị chặn và tạo ra các sự kiện tương ứng.

8. Trong danh sách quy tắc Kiểm soát ứng dụng, hãy nhấn nút **Add**.

   Thao tác này sẽ khởi chạy trình hướng dẫn để thêm quy tắc Kiểm soát ứng dụng.

9. Trong phần **Categories/Applications**, hãy chọn danh mục được cập nhật tự động dựa trên máy tính cơ sở.

10. Chọn người dùng hoặc nhóm người dùng mà bạn muốn áp dụng quy tắc Kiểm soát ứng dụng.

11. Cấu hình thiết lập nâng cao của quy tắc Kiểm soát ứng dụng:

    - **Users**. Ứng dụng ngăn khởi chạy các ứng dụng thuộc danh mục đã chọn đối với tất cả người dùng không có trong danh sách.

    - **Trusted Updaters**. Kaspersky Endpoint Security coi các ứng dụng được bao gồm trong danh mục được chọn là các trình cập nhật được tin tưởng, được phép tạo các tập tin thực thi khác có thể chạy sau đó.

12. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách cấu hình Kiểm soát ứng dụng dựa trên máy tính cơ sở 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 **Kiểm soát bảo mật** → **Kiểm soát ứng dụng**.

3. Bật nút bật/tắt **Kiểm soát ứng dụng**.

4. Trong mục **Chế độ Kiểm soát khởi động ứng dụng**, hãy chọn **Danh sách không được phép. Tất cả các ứng dụng, trừ các ứng dụng trong danh sách quy tắc mới được cho phép**.

5. Trong mục **Hành động khi khởi động các ứng dụng bị chặn theo quy tắc**, hãy chọn hành động cho Kiểm soát ứng dụng:

    - **Thông báo (Chế độ thử nghiệm) và ghi lại sự kiện trong báo cáo**. Kiểm soát ứng dụng không chặn các ứng dụng bị ngăn chạy theo quy tắc, mà tạo ra các sự kiện về việc chạy các ứng dụng vốn sẽ bị chặn.

    - **Chặn**. Kiểm soát ứng dụng chặn các ứng dụng bị chặn và tạo ra các sự kiện tương ứng.

6. Trong danh sách quy tắc Kiểm soát ứng dụng, hãy nhấn nút **Thêm**.

   Thao tác này sẽ khởi chạy trình hướng dẫn để thêm quy tắc Kiểm soát ứng dụng.

7. Trong phần **Danh mục**, hãy chọn danh mục được cập nhật tự động dựa trên máy tính cơ sở.

8. Chọn người dùng hoặc nhóm người dùng mà bạn muốn áp dụng quy tắc Kiểm soát ứng dụng.

9. Cấu hình thiết lập nâng cao của quy tắc Kiểm soát ứng dụng:

    - **Từ chối người sử dụng khác**. Ứng dụng ngăn khởi chạy các ứng dụng thuộc danh mục đã chọn đối với tất cả người dùng không có trong danh sách.

    - **Trình cập nhật được tin tưởng**. Kaspersky Endpoint Security coi các ứng dụng được bao gồm trong danh mục được chọn là các trình cập nhật được tin tưởng, được phép tạo các tập tin thực thi khác có thể chạy sau đó.

10. Lưu các thay đổi của bạn.

Quản lý các Quy tắc Kiểm soát 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 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.
- **Chế độ thử nghiệm**. 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.

Bổ sung một điều kiện kích hoạt cho quy tắc Kiểm soát 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 trong Bảng điều khiển quản trị:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây Bảng điều khiển quản trị, hãy chọn **Advanced** → **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 danh mục mới.

Bước 1. Chọn loại danh mục

Ở bước này, chọn một trong các loại danh mục ứng dụng sau:

- Category with content added manually. Data of executable files is manually added to the category Nếu bạn đã chọn loại danh mục này, tại bước *Configuring conditions for inclusion of applications in categories* và bước *Configuring conditions for exclusion of applications from categories* thì bạn có thể xác định tiêu chí mà theo đó các tập tin thực thi sẽ được đưa vào danh mục.
- Category that includes executable files from selected devices. These executable files are processed automatically and their metrics are added to the category Nếu bạn đã chọn loại danh mục này, ở bước *Settings* 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. Executable files of applications copied to the specified folder are automatically processed and their metrics are added to the category Nếu bạn đã chọn loại danh mục này, ở bước *Repository folder* 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

Khi thêm một số lượng lớn điều kiện vào các Quy tắc kiểm soát ứng dụng (ví dụ: hash của tập tin), mức tiêu thụ tài nguyên máy tính sẽ tăng lên. Khi tổng số điều kiện đạt 50.000, các vấn đề về hiệu năng có thể xảy ra. Để tối ưu hóa hiệu năng, nên xem lại và giảm số lượng điều kiện.

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 fingerprint**.

- **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 thuộc tính chủ đề. Danh sách này được duy trì bởi các chuyên gia Kaspersky. Ví dụ: danh mục KL mang tên *Office Applications* 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 (masks supported)**. 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 fingerprint**.

  Bạn có thể chọn kho chứng chỉ. Theo mặc định, thành phần Kiểm soát ứng dụng chỉ áp dụng các quy tắc cho các ứng dụng được ký bằng chứng chỉ từ kho chứng chỉ hệ thống tin tưởng. Thiết lập này được bật thông qua hộp kiểm **Sử dụng xác minh chữ ký số nghiêm ngặt**.

- **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 thuộc tính chủ đề. Danh sách này được duy trì bởi các chuyên gia Kaspersky. Ví dụ: danh mục KL mang tên *Office Applications* 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 (masks supported)**. 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 **Add** 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 SHA256 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.

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 SHA256 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 interval (1–168 hours)**. 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

Hoàn tất trình hướng dẫn.

Để thêm một điều kiện kích hoạt cho một quy tắc Kiểm soát 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 **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: N** hoặc thẻ **Loại trừ: N** và nhấn vào 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 thuộc tính 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 hỗ trợ các ký tự `*` và `?` để nhập tên đại diện vào siêu dữ liệu: **File name**, **Application name**, **Vendor**.
- 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 chứng chỉ** 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**.

Bổ sung các tập tin thực thi từ thư mục Tập tin thực thi đến danh mục ứng dụng

Thư mục **Executable files** 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 **Advanced → 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 SHA256 hashes for files without a certificate)**.

     - **Certificate details (files without a certificate will be skipped)**.

     - **Only SHA256 (files without a hash will be skipped)**.

     - **Only MD5 (discontinued mode, only for Kaspersky Endpoint Security 10 Service Pack 1 version)**.

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)**.
     - **Only MD5 (discontinued mode, only for Kaspersky Endpoint Security 10 Service Pack 1 version)**.
8. Lưu các thay đổi của bạn.

Thêm một Quy tắc kiểm soát ứng dụng

Để thêm một quy tắc Kiểm soát ứng dụng sử dụng Kaspersky Security Center:

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. 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.
4. Nhấn vào **Thêm**.
   Cửa sổ **Quy tắc Kiểm soát ứng dụng** sẽ mở ra.
5. 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 danh mục mới.
     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.
6. Trong bảng **Người dùng và quyền của họ**, hãy nhấn nút **Thêm**.
   Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.
7. Trong bảng **Người dùng 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 **Chặn** trong hàng tương ứng.

8. Chọn hộp kiểm **Từ chối người sử dụng khác** nếu bạn muốn tất cả người dùng không có tên trong cột **Người dùng hoặc nhóm** và không thuộc nhóm người dùng được quy định trong cột **Người dùng hoặc nhóm** bị chặn khỏi việc khởi động các ứng dụng thuộc danh mục được chọn.

9. 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.

10. Lưu các thay đổi của bạn.

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 sẻ 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. Trong bảng **Người dùng và quyền của họ**, hãy nhấn nút **Thêm**.
      Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.
      Quy tắc này được áp dụng cho tất cả người dùng theo mặc định.

      Nếu không có người dùng nào được quy định trong bảng, quy tắc không thể được lưu lại.

   d. Trong bảng **Người dùng 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 **Người dùng và quyền của họ** và không phải là thành viên của các nhóm người dùng được liệt kê trong bảng **Người dùng 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 **Người dùng và quyền của họ** và không thuộc nhóm người dùng được quy định trong bảng **Người dùng 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: N**, hãy tạo hoặc chỉnh sửa danh sách các điều kiện loại trừ để kích hoạt quy tắc.
7. Trên thẻ **Loại trừ: N**, 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.

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 trong Bảng điều khiển quản trị:

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. 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.

4. 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 được sử dụng khi thành phần Kiểm soát ứng dụng đang chạy.
   - **Tắt**. Trạng thái này có nghĩa rằng quy tắc bị bỏ qua khi thành phần Kiểm soát ứng dụng đang chạy.
   - **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.

Để thay đổi trạng thái của một quy tắc Kiểm soát 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 **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.
   - **Chế độ thử nghiệm**. 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.

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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật → Kiểm soát ứng dụng**.
4. 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 vào 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.
5. Để nhập danh sách Quy tắc kiểm soát ứng dụng:
   a. Nhấn vào 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.
6. 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 **Asset management → Policies**.
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 **Security Controls → App Control**.
5. Trong mục **Operating mode**, hãy chọn danh sách các quy tắc: danh sách ứng dụng được phép và danh sách ứng dụng không được phép.
6. Để xuất danh sách quy tắc:
   a. Chọn các quy tắc mà bạn muốn xuất.
   b. Nhấn nút → **Export**.
      Kaspersky Endpoint Security sẽ xuất danh sách các quy tắc vào tập tin JSON trong thư mục tải xuống mặc định.

7. Để nhập danh sách quy tắc:

   a. Nhấn nút → **Import**.

      Trong cửa sổ mở ra, hãy chọn tập tin JSON 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 JSON.

8. Lưu các thay đổi của bạn.

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 **Cấm khởi động ứng dụng**.
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 vào **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 **Other → 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. 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.

Bật và tắt kiểm tra quy tắc Kiểm soát ứng dụng

Để bật hoặc tắt kiểm tra các Quy tắc kiểm soát ứng dụng trong Kaspersky Security Center:

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. 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.

4. Trong danh sách thả xuống **Chế độ kiểm soát**, hãy 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.

5. Thực hiện một trong các thao tác sau:

   - Nếu bạn muốn bật kiểm tra các Quy tắc kiểm soát ứng dụng, hãy chọn **Kiểm tra quy tắc** 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**.

6. Lưu các thay đổi của bạn.

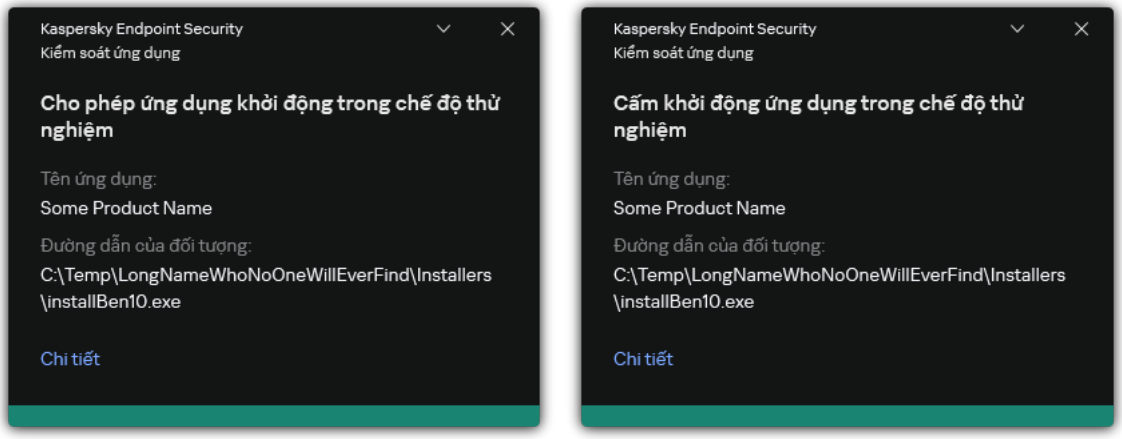
Để bật chế độ thử nghiệm các Quy tắc Kiểm soát ứng dụng hoặc chọn một hành động chặn cho Kiểm soát ứng dụng:

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 **Chế độ thử nghiệm**.

   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

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 vào **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 **Other → 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 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 **Events**, 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**.

Quản lý hoạt động ứng dụng

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.

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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Giao diện**.
4. Sử dụng hộp kiểm **Ẩn mục Giám sát hoạt động ứng dụng** để cấp hoặc thu hồi quyền truy cập vào công cụ.
5. 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 **Asset management → Policies**.
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 → User Interaction**.

5. Sử dụng hộp kiểm **Hide Application Activity Monitor section** 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.

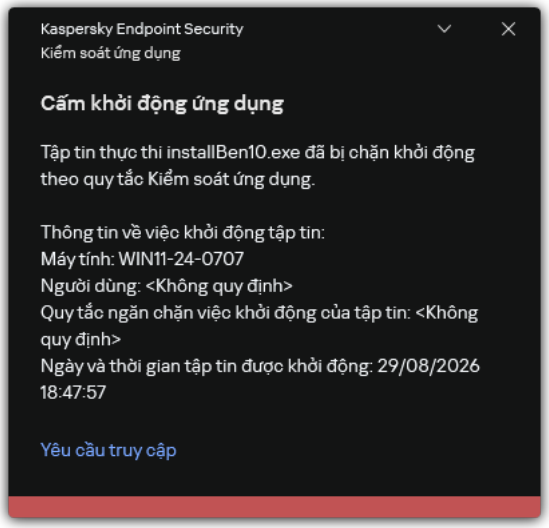
Bạn có thể sử dụng các ký tự sau đây để tạo một tên đại diện tập tin hoặc thư mục:

- 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. Các chuyên gia của Kaspersky cung cấp cho người dùng mẫu tin nhắn mô tả lý do tại sao ứng dụng bị chặn (xem hình bên dưới). Các biến đặc biệt được cung cấp để quản lý mẫu tin nhắn (ví dụ: `%USER_NAME%`). Biến cho phép sử dụng một mẫu tin nhắn duy nhất cho nhiều máy tính khác nhau. Khi tạo tin nhắn, Kaspersky Endpoint Security sẽ lấy giá trị của biến từ thiết lập của hệ điều hành và chèn vào tin nhắn phù hợp với máy tính, người dùng và sự kiện cụ thể.



Thông báo của Kiểm soát ứng dụng

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. Để thực hiện, người dùng phải nhấn vào **Yêu cầu truy cập** và gửi tin nhắn cho quản trị viên để mô tả tình huống. Bạn cũng có thể chuẩn bị mẫu tin nhắn gửi cho quản trị viên, thêm vào đó dữ liệu có thể giúp bạn đưa ra quyết định cho phép hay chặn quyền truy cập ứng dụng. 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.

Cách chỉnh sửa mẫu tin nhắn của Kiểm soát ứng dụng trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật → Kiểm soát ứng dụng**.
4. Trong mục **Thiết lập mẫu tin nhắn**, hãy nhấn nút **Mẫu**.
5. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy cấu hình mẫu 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.

     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.

   Để thêm biến vào văn bản mẫu, hãy đặt con trỏ vào vị trí mong muốn, nhấn vào **Biến số** và chọn biến cần dùng trong danh sách các tùy chọn có sẵn.

   Bạn cũng có thể khôi phục văn bản mẫu mặc định bằng cách sử dụng nút **Theo mặc định**.
6. Lưu các thay đổi của bạn.

Cách chỉnh sửa mẫu thông báo của 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 **Asset management → Policies**.
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 **Security Controls → App Control**.

5. Trong mục **Message templates**, hãy nhấn vào liên kết **Messages about application startup block** và cấu hình các mẫu cho thông báo của Kiểm soát ứng dụng:

   - **Message to user**. Mẫu thông báo được hiển thị khi kích hoạt một quy tắc Kiểm soát ứng dụng chặn ứng dụng khởi chạy.

     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.

   - **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.

   Để thêm biến vào văn bản mẫu, hãy đặt con trỏ vào vị trí mong muốn, nhấn vào **Add variable** và chọn biến cần dùng trong danh sách các tùy chọn có sẵn.

   Bạn cũng có thể khôi phục văn bản mẫu mặc định bằng cách sử dụng nút **Reset to default**.

6. Lưu các thay đổi của bạn.

Cách chỉnh sửa mẫu tin nhắn của Kiểm soát 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 **Kiểm soát bảo mật → Kiểm soát ứng dụng**.

3. Trong mục **Mẫu tin nhắn về việc chặn ứng dụng**, hãy cấu hình các mẫu cho 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.

     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.

   Để thêm biến vào văn bản mẫu, hãy đặt con trỏ vào vị trí mong muốn, nhấn vào **Thêm biến số** và chọn biến cần dùng trong danh sách các tùy chọn có sẵn.

   Bạn cũng có thể khôi phục văn bản mẫu mặc định bằng cách sử dụng nút **Đặt lại**.

4. Lưu các thay đổi của bạn.

Các biến trong mẫu thông báo của Kiểm soát ứng dụng

Bạn có thể sử dụng các biến sau trong mẫu tin nhắn người dùng hoặc mẫu tin nhắn quản trị viên:

- **Tên của quy tắc được kích hoạt** – `%RULE%`.

  Tên của quy tắc đã chặn thực thi một tập tin.

- **Ngày hiện tại** – `%DATE%`.

  Ngày tháng chặn thực thi tập tin, được ghi theo định dạng DD.MM.YYYY.

- **Thời gian hiện tại** – `%TIME%`.

  Thời điểm chặn thực thi tập tin theo định dạng HH:MM.

- **Tên người dùng** – `%USER_NAME%`.

  Tên tài khoản người dùng hiện tại trên máy tính nơi chặn thực thi tập tin, theo định dạng `<device name>\<user alias>` (ví dụ: `DESKTOP-123\John.Smith`).

- **Tên máy tính** – `%COMPUTER_NAME%`.

  Tên máy tính nơi việc thực thi tập tin bị chặn.

- **Tên tập tin thực thi** – `%FILE_NAME%`.

  Tên của tập tin thực thi của ứng dụng bị chặn.

- **Danh mục KL của tập tin thực thi** – `%KL_CAT%`.

  Danh mục KL chứa ứng dụng bị chặn (ví dụ: *Trình duyệt* hoặc danh mục khác).

- **Đường dẫn đến tập tin thực thi** – `%FILE_PATH%`.

  Đường dẫn đầy đủ đến tập tin thực thi của ứng dụng bị chặn.

- **Phiên bản tập tin thực thi** – `%FILE_VERSION%`.

  Phiên bản của tập tin thực thi của ứng dụng bị chặn.

- **Tên ban đầu của tập tin thực thi** – `%ORIGINAL_FILE_NAME%`.

  Tên gốc của tập tin thực thi của ứng dụng bị chặn. Tên tập tin được chỉ định trong thuộc tính của tập tin thực thi của ứng dụng.

- **Nhà cung cấp** – `%FILE_PUBLISHER%`.

  Nhà cung cấp ứng dụng bị chặn.

- **Tên ứng dụng** – `%FILE_PRODUCT_NAME%`.

  Tên của ứng dụng bị chặn.

- **Phiên bản ứng dụng** – `%PRODUCT_VERSION%`.

  Phiên bản của ứng dụng bị chặn.

- **Hash tập tin thực thi** – `%FILE_HASH%`.

  Hash của tập tin thực thi của ứng dụng bị chặn.

- **Đơn vị cấp chứng chỉ** – `%CERT_ISSUER%`.

  Đơn vị phát hành chứng chỉ dùng để ký tập tin thực thi.

- **Tiêu đề chứng chỉ** – `%CERT_SUBJECT%`.

  Chủ đề của chứng chỉ dùng để ký tập tin thực thi.

- **Dấu vân tay chứng chỉ** – `%CERT_THUMBPRINT%`.

  Dấu vân tay của chứng chỉ dùng để ký tập tin thực thi.

Các phương pháp tốt nhất để kiểm kê tập tin thực thi

Tác vụ *Inventory* thu thập thông tin về các tập tin thực thi (ví dụ: EXE, BAT, CMD), mô-đun DLL và tập lệnh (PowerShell, JS, và các loại khác). Thông tin này cần thiết cho việc cấu hình các danh mục Kiểm soát ứng dụng và quyền ứng dụng cho thành phần Phòng chống xâm nhập máy chủ. Tác vụ *Inventory* nên được chạy định kỳ để cập nhật thông tin. Tác vụ *Inventory*, cũng giống như tác vụ *Malware Scan* tốn nhiều tài nguyên. Do đó, bạn nên cấu hình tác vụ để chạy vào ban đêm hoặc cuối tuần.

Các bước kiểm kê tập tin thực thi

1. Chọn nhóm máy tính tham chiếu có bộ phần mềm điển hình của bạn được cài đặt. Bạn nên giữ số lượng máy tính ở mức tối thiểu cho quy trình kiểm kê tập tin thực thi. Càng ít tác vụ *Inventory*, mức tải lên Máy chủ quản trị Kaspersky Security Center càng thấp.

2. Chuyển các máy tính tham chiếu sang một nhóm quản trị riêng biệt trong bảng điều khiển Kaspersky Security Center. Bạn có thể đặt tên cho nhóm, ví dụ như: *Máy tính tham chiếu*.

3. Tạo một tác vụ *Inventory* cho nhóm quản trị *Máy tính tham chiếu*. Bạn nên giữ nguyên thiết lập mặc định của tác vụ.

Ví dụ về kiểm kê tập tin thực thi trong một tổ chức

Ví dụ: tổ chức của bạn có 100 máy tính đang chạy Windows 11 25H2. Tất cả các máy tính đều có cùng phiên bản và ngôn ngữ bản địa hóa hệ điều hành. Nhóm các bản cập nhật được cài đặt trên các máy tính cũng giống nhau.

Trong một tổ chức như vậy, bạn không cần chạy tác vụ *Inventory* trên tất cả các máy tính. Hầu hết các tập tin thực thi trên các máy tính này đều giống hệt nhau. Chỉ cần tạo một tác vụ cho một máy tính tham chiếu là đủ. Bạn có thể tạo các tác vụ *Inventory* bổ sung dành cho máy tính có cấu hình khác với máy tính tham chiếu.

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 "**Application folder**" 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 **Application folder** 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 **Subject** 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 **Application folder** và chỉ 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 "**Application folder**" 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 **Application folder** 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 tập 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 cổng mạng

Trong quá trình hoạt động của Kaspersky Endpoint Security, các thành phần Kiểm soát Web, Bảo vệ mối đe dọa thư điện tử Bảo vệ mối đe dọa web, Phát hiện hành vi và Phòng chống khai thác 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 mối đe dọa thư điện tử sẽ phân tích thông tin được truyền tải qua SMTP, trong khi thành phần Bảo vệ mối đe dọa web phân tích thông tin được truyền tải qua HTTP và FTP.

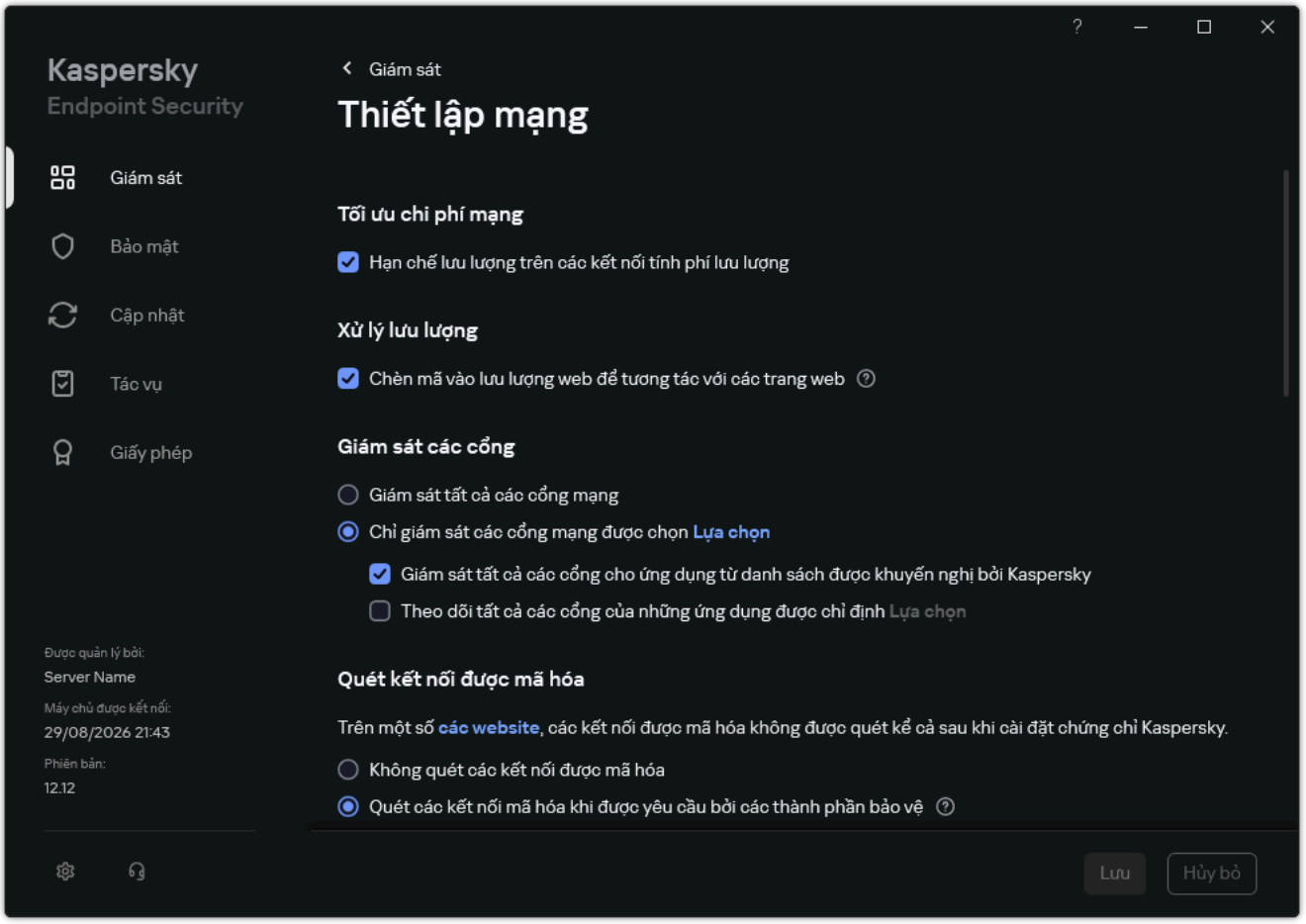
Kaspersky Endpoint Security sẽ chia các cổng TCP và UDP của máy tính người dùng thành vài nhóm, tùy thuộc vào khả năng chúng bị xâm nhập. Một số cổng mạng được dành riêng cho các dịch vụ có lỗ hổng bảo mật. Bạn được khuyến cáo giám sát các cổng này kỹ lưỡng hơn bởi vì chúng có khả năng lớn hơn được chọn 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 mối đe dọa thư điện tử và Bảo vệ mối đe dọa web trong hoạt động giám sát lưu lượng mạng.

Để giúp đảm bảo khả năng bảo mật cho máy tính, thành phần Phát hiện hành vi và Phòng chống khai thác cũng giám sát các luồng dữ liệu đi qua các cổng mạng. Các thành phần này sẽ liên tục giám sát lưu lượng mạng để phát hiện các tiến trình riêng lẻ có thể gây nguy hiểm.

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**.



Thiết lập giám sát cổng 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 Acrobat 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. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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** → **Network Settings**.
5. Để xuất danh sách cổng mạng:
   a. Trong mục **Monitored ports**, hãy chọn **Monitor selected network ports only**.
   b. Nhấn vào liên kết **selected N ports**.

      Cửa sổ **Network ports** sẽ mở ra. Cửa sổ **Network ports** 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 **Export**.
   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 **Monitored ports**, hãy chọn hộp kiểm **Monitor all ports for specified applications**.
   b. Nhấn vào liên kết **selected N applications**.
   c. Trong danh sách ứng dụng, hãy chọn ứng dụng bạn muốn xuất.
   d. Nhấn vào **Export**.
   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 **Import**.

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 **Import**.

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.

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Thiết lập mạng**.

4. Trong mục **Giám sát các cổng**, hãy chọn **Chỉ giám sát các cổng mạng được chọn**.

5. Nhấn vào **Thiết lập**.

Cửa sổ **Cổng mạng** sẽ 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. Lưu các thay đổi của bạn.

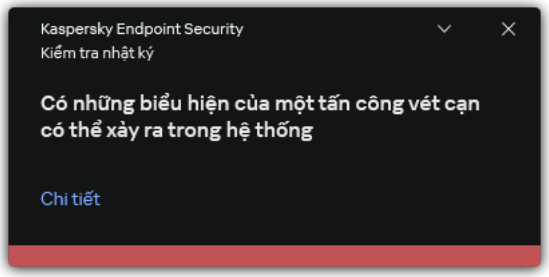
Kiểm tra nhật ký

Thành phần này khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows cho máy chủ. Thành phần này không khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows dành cho máy trạm.

Kiểm tra nhật ký sẽ giám sát tính toàn vẹn của môi trường được bảo vệ dựa trên phân tích nhật ký sự kiện của Windows. Khi ứng dụng phát hiện các dấu hiệu của hành vi bất thường trong hệ thống, ứng dụng sẽ thông báo cho quản trị viên, vì hành vi này có thể chỉ báo một nỗ lực tấn công mạng.

Kaspersky Endpoint Security sẽ phân tích nhật ký sự kiện của Windows và phát hiện vi phạm theo các quy tắc. Thành phần này bao gồm quy tắc định trước. Các quy tắc định trước được cung cấp bởi phân tích hành vi. Bạn cũng có thể thêm các quy tắc của riêng của mình (quy tắc tùy chỉnh). Khi một quy tắc kích hoạt, ứng dụng sẽ tạo một sự kiện có trạng thái *Critical* (xem hình bên dưới).

Nếu bạn muốn sử dụng Kiểm tra nhật ký, hãy đảm bảo rằng thiết lập bảo mật chính sách kiểm tra được cấu hình và hệ thống đang ghi nhật ký các sự kiện liên quan (để biết chi tiết, hãy xem Website hỗ trợ kỹ thuật của Microsoft.).



Thông báo Kiểm tra nhật ký

Cấu hình quy tắc định trước

Các quy tắc định trước bao gồm các mẫu hoạt động bất thường trên máy tính được bảo vệ. Hoạt động bất thường có thể báo hiệu một cuộc tấn công có chủ đích. Các quy tắc định trước được cung cấp bởi phân tích hành vi. Bảy quy tắc định trước có sẵn để Kiểm tra nhật ký. Bạn có thể bật hoặc tắt các quy tắc này. Không thể xóa các quy tắc định trước.

Bạn có thể cấu hình tiêu chí kích hoạt cho các quy tắc giám sát sự kiện cho các hoạt động sau:

- Phát hiện tấn công vét cạn mật khẩu
- Phát hiện đăng nhập mạng

Cách cấu hình quy tắc xác định trước trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật → Kiểm tra nhật ký**.
4. Đảm bảo rằng hộp kiểm **Kiểm tra nhật ký** được chọn.
5. Trong mục **Các quy tắc định trước**, hãy nhấn nút **Thiết lập**.
6. Chọn hoặc bỏ chọn các hộp kiểm để cấu hình quy tắc định trước:
   - **Có những biểu hiện của một tấn công vét cạn có thể xảy ra trong hệ thống**.
   - **Đã phát hiện một hoạt động không điển hình trong một phiên đăng nhập mạng**.
   - **Có những biểu hiện về khả năng xảy ra việc lạm dụng Nhật ký sự kiện của Windows**.

- **Đã phát hiện các hành động không điển hình thay cho một dịch vụ được cài đặt**.
- **Đã phát hiện hoạt động đăng nhập không điển hình, sử dụng thông tin đăng nhập hiện rõ**.
- **Có những biểu hiện của một cuộc tấn công Kerberos forged PAC (MS14-068) có thể xảy ra trong hệ thống**.
- **Đã phát hiện các thay đổi đáng ngờ trong nhóm Quản trị viên đặc quyền tích hợp**.

7. Nếu cần, hãy cấu hình quy tắc **Có những biểu hiện của một tấn công vét cạn có thể xảy ra trong hệ thống**:
   a. Nhấn nút **Thiết lập** bên dưới quy tắc.
   b. Trong cửa sổ mở ra, hãy chỉ định số lần thử và khoảng thời gian phải thực hiện thao tác nhập mật khẩu để quy tắc được kích hoạt.
   c. Nhấn vào **OK**.
8. Nếu đã chọn **Đã phát hiện một hoạt động không điển hình trong một phiên đăng nhập mạng**, bạn cần cấu hình thiết lập của nó:
   a. Nhấn nút **Thiết lập** bên dưới quy tắc.
   b. Trong mục **Phát hiện đăng nhập mạng**, hãy chỉ định thời điểm bắt đầu và kết thúc khoảng thời gian.

      Kaspersky Endpoint Security sẽ coi các nỗ lực đăng nhập được thực hiện trong khoảng thời gian được xác định là hoạt động bất thường.

      Theo mặc định, khoảng thời gian không được đặt và ứng dụng không giám sát các lượt thử đăng nhập. Để ứng dụng liên tục theo dõi các nỗ lực đăng nhập, hãy đặt khoảng thời gian từ 00 giờ 00 giờ đến 23 giờ 59. Thời điểm bắt đầu và kết thúc khoảng thời gian không được trùng nhau. Nếu trùng nhau, ứng dụng sẽ không giám sát các lần đăng nhập.
   c. Tạo danh sách người dùng được tin tưởng và địa chỉ IP được tin tưởng (IPv4 và IPv6).

      Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền. Kaspersky Endpoint Security không giám sát các nỗ lực đăng nhập của những người dùng và máy tính này.
   d. Nhấn vào **OK**.
9. Lưu các thay đổi của bạn.

Cách cấu hình quy tắc định trước trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Security Controls** → **Log Inspection**.

5. Đảm bảo rằng công tắc bật/tắt **Log Inspection ENABLED** được bật.

6. Trong mục **Predefined rules**, hãy bật hoặc tắt các quy tắc định trước bằng cách sử dụng các nút bật/tắt:

   - **There are patterns of a possible brute-force attack in the system**.
   - **There is an atypical activity detected during a network logon session**.
   - **There are patterns of a possible Windows Event Log abuse**.
   - **Atypical actions detected on behalf of a new service installed**.
   - **Atypical logon that uses explicit credentials detected**.
   - **There are patterns of a possible Kerberos forged PAC (MS14-068) attack in the system**.

   a. **Suspicious changes detected in the privileged built-in Administrators group**.

7. Nếu cần, hãy cấu hình quy tắc **There are patterns of a possible brute-force attack in the system**:

   a. Nhấn vào **Settings** bên dưới quy tắc.

   b. Trong cửa sổ mở ra, hãy chỉ định số lần thử và khoảng thời gian phải thực hiện thao tác nhập mật khẩu để quy tắc được kích hoạt.

   c. Nhấn vào **OK**.

8. Nếu đã chọn **There is an atypical activity detected during a network logon session**, bạn cần cấu hình thiết lập của nó:

   a. Nhấn vào **Settings** bên dưới quy tắc.

   b. Trong mục **Network logon detection**, hãy chỉ định thời điểm bắt đầu và kết thúc khoảng thời gian.

   Kaspersky Endpoint Security sẽ coi các nỗ lực đăng nhập được thực hiện trong khoảng thời gian được xác định là hoạt động bất thường.

   Theo mặc định, khoảng thời gian không được đặt và ứng dụng không giám sát các lượt thử đăng nhập. Để ứng dụng liên tục theo dõi các nỗ lực đăng nhập, hãy đặt khoảng thời gian từ 00 giờ 00 giờ đến 23 giờ 59. Thời điểm bắt đầu và kết thúc khoảng thời gian không được trùng nhau. Nếu trùng nhau, ứng dụng sẽ không giám sát các lần đăng nhập.

   c. Trong mục **Exclusions**, hãy thêm người dùng được tin tưởng và địa chỉ IP được tin tưởng (IPv4 và IPv6).

   Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền. Kaspersky Endpoint Security không giám sát các nỗ lực đăng nhập của những người dùng và máy tính này.

   d. Nhấn vào **OK**.

9. Lưu các thay đổi của bạn.

Cách cấu hình quy tắc định sẵn 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 **Kiểm soát bảo mật → Kiểm tra nhật ký**.
3. Đảm bảo rằng công tắc bật/tắt **Kiểm tra nhật ký** được bật.
4. Trong mục **Các quy tắc định trước**, hãy nhấn nút **Cấu hình**.
5. Chọn hoặc bỏ chọn các hộp kiểm để cấu hình quy tắc định trước:
   - **Có những biểu hiện của một tấn công vét cạn có thể xảy ra trong hệ thống**.
   - **Đã phát hiện một hoạt động không điển hình trong một phiên đăng nhập mạng**.
   - **Có những biểu hiện về khả năng xảy ra việc lạm dụng Nhật ký sự kiện của Windows**.
   - **Đã phát hiện các hành động không điển hình thay cho một dịch vụ được cài đặt**.
   - **Đã phát hiện hoạt động đăng nhập không điển hình, sử dụng thông tin đăng nhập hiện rõ**.
   - **Có những biểu hiện của một cuộc tấn công Kerberos forged PAC (MS14-068) có thể xảy ra trong hệ thống**.

   a. **Đã phát hiện các thay đổi đáng ngờ trong nhóm Quản trị viên đặc quyền tích hợp**.
6. Nếu cần, hãy cấu hình quy tắc **Có những biểu hiện của một tấn công vét cạn có thể xảy ra trong hệ thống**:

   a. Nhấn vào **Thiết lập** bên dưới quy tắc.

   b. Trong cửa sổ mở ra, hãy chỉ định số lần thử và khoảng thời gian phải thực hiện thao tác nhập mật khẩu để quy tắc được kích hoạt.
7. Nếu đã chọn **Đã phát hiện một hoạt động không điển hình trong một phiên đăng nhập mạng**, bạn cần cấu hình thiết lập của nó:

   a. Nhấn vào **Thiết lập** bên dưới quy tắc.

   b. Trong mục **Phát hiện đăng nhập mạng**, hãy chỉ định thời điểm bắt đầu và kết thúc khoảng thời gian.

   Kaspersky Endpoint Security sẽ coi các nỗ lực đăng nhập được thực hiện trong khoảng thời gian được xác định là hoạt động bất thường.

   Theo mặc định, khoảng thời gian không được đặt và ứng dụng không giám sát các lượt thử đăng nhập. Để ứng dụng liên tục theo dõi các nỗ lực đăng nhập, hãy đặt khoảng thời gian từ 00 giờ 00 giờ đến 23 giờ 59. Thời điểm bắt đầu và kết thúc khoảng thời gian không được trùng nhau. Nếu trùng nhau, ứng dụng sẽ không giám sát các lần đăng nhập.

c. Trong mục **Loại trừ**, hãy thêm người dùng được tin tưởng và địa chỉ IP được tin tưởng (IPv4 và IPv6).

   Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền. Kaspersky Endpoint Security không giám sát các nỗ lực đăng nhập của những người dùng và máy tính này.

8. Lưu các thay đổi của bạn.

Kết quả là khi quy tắc kích hoạt, Kaspersky Endpoint Security sẽ tạo *Sự kiện nghiêm trọng*.

Thêm quy tắc tùy chỉnh

Bạn có thể đặt tiêu chí kích hoạt quy tắc Kiểm tra nhật ký của riêng mình. Để thực hiện, bạn phải nhập ID sự kiện và chọn nguồn sự kiện. Bạn có thể tra cứu ID sự kiện trên Website hỗ trợ kỹ thuật của Microsoft. Bạn có thể chọn một nguồn sự kiện trong số các nhật ký tiêu chuẩn: *Application*, *Security* hoặc *System*. Bạn cũng có thể chỉ định nhật ký của ứng dụng bên thứ ba. Bạn có thể tìm tên của nhật ký ứng dụng của bên thứ ba bằng cách sử dụng công cụ Trình xem sự kiện. Nhật ký ứng dụng của bên thứ ba được lưu trong thư mục Nhật ký ứng dụng và dịch vụ (ví dụ: nhật ký *Windows PowerShell*).

> Ứng dụng không kiểm tra xem nhật ký được chỉ định có thực sự hiện diện trong nhật ký sự kiện Windows hay không. Nếu có sai sót trong tên của nhật ký, ứng dụng sẽ không giám sát các sự kiện từ nhật ký đó.

Danh sách các quy tắc tùy chỉnh đã bao gồm ba quy tắc do các chuyên gia của Kaspersky tạo ra.

Cách thêm quy tắc tùy chỉnh trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật → Kiểm tra nhật ký**.
4. Đảm bảo rằng hộp kiểm **Kiểm tra nhật ký** được chọn.
5. Trong mục **Quy tắc tùy chỉnh**, hãy nhấn nút **Thiết lập**.
6. Trong cửa sổ mở ra, hãy chọn hộp kiểm bên cạnh các quy tắc tùy chỉnh mà bạn muốn bật.
7. Nếu cần, hãy nhấn vào **Thêm** để tạo các quy tắc tùy chỉnh của riêng bạn.
8. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy cấu hình quy tắc tùy chỉnh:
   - **Tên quy tắc**.
   - **Tên nhật ký**. Nhật ký sự kiện Windows. Có sẵn các nhật ký sau đây: *Application*, *Security*, *System*.

- **Nguồn**. Nhật ký ứng dụng của bên thứ ba. Bạn có thể tìm tên của nhật ký ứng dụng của bên thứ ba bằng cách sử dụng công cụ Trình xem sự kiện. Nhật ký ứng dụng của bên thứ ba được lưu trong thư mục Nhật ký ứng dụng và dịch vụ (ví dụ: nhật ký *Windows PowerShell*).

- **Định danh sự kiện**. ID sự kiện trong Nhật ký sự kiện của Windows. Bạn có thể tra cứu ID sự kiện trong tài liệu kỹ thuật của Microsoft.

9. Lưu các thay đổi của bạn.

Cách thêm một quy tắc tùy chỉnh trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.

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 **Security Controls** → **Log Inspection**.

5. Đảm bảo rằng công tắc bật/tắt **Log Inspection ENABLED** được bật.

6. Trong mục **Custom rules**, hãy chọn các quy tắc tùy chỉnh mà bạn muốn bật.

7. Nếu cần, hãy nhấn vào **Add** để tạo các quy tắc tùy chỉnh của riêng bạn.

8. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy cấu hình quy tắc tùy chỉnh:

   - **Rule name**.

   - **Custom log name**. Nhật ký sự kiện Windows. Có sẵn các nhật ký sau đây: *Application*, *Security*, *System*.

   - **Origin**. Nhật ký ứng dụng của bên thứ ba. Bạn có thể tìm tên của nhật ký ứng dụng của bên thứ ba bằng cách sử dụng công cụ Trình xem sự kiện. Nhật ký ứng dụng của bên thứ ba được lưu trong thư mục Nhật ký ứng dụng và dịch vụ (ví dụ: nhật ký *Windows PowerShell*).

   - **Event Identifiers**. ID sự kiện trong Nhật ký sự kiện của Windows. Bạn có thể tra cứu ID sự kiện trong tài liệu kỹ thuật của Microsoft.

9. Lưu các thay đổi của bạn.

Cách thêm quy tắc tùy chỉnh 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 **Kiểm soát bảo mật** → **Kiểm tra nhật ký**.

3. Đảm bảo rằng công tắc bật/tắt **Kiểm tra nhật ký** được bật.

4. Trong mục **Quy tắc tùy chỉnh**, hãy nhấn nút **Cấu hình**.

5. Trong cửa sổ mở ra, hãy chọn hộp kiểm bên cạnh các quy tắc tùy chỉnh mà bạn muốn bật.

6. Nếu cần, hãy nhấn vào **Thêm** để tạo các quy tắc tùy chỉnh của riêng bạn.

7. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy cấu hình quy tắc tùy chỉnh:

   - **Tên quy tắc**.
   - **Tên nhật ký**. Nhật ký sự kiện Windows. Có sẵn các nhật ký sau đây: *Application*, *Security*, *System*.
   - **Nguồn**. Nhật ký ứng dụng của bên thứ ba. Bạn có thể tìm tên của nhật ký ứng dụng của bên thứ ba bằng cách sử dụng công cụ Trình xem sự kiện. Nhật ký ứng dụng của bên thứ ba được lưu trong thư mục Nhật ký ứng dụng và dịch vụ (ví dụ: nhật ký *Windows PowerShell*).
   - **Định danh sự kiện**. ID sự kiện trong Nhật ký sự kiện của Windows. Bạn có thể tra cứu ID sự kiện trong tài liệu kỹ thuật của Microsoft.

8. Lưu các thay đổi của bạn.

Kết quả là khi quy tắc kích hoạt, Kaspersky Endpoint Security sẽ tạo *Critical*.

Giám sát tính toàn vẹn của hệ thống

> Thành phần này khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows cho máy chủ. Thành phần này không khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows dành cho máy trạm.

Kể từ phiên bản 12.6, Kaspersky Endpoint Security cho Windows đã bao gồm thành phần Giám sát toàn vẹn của hệ thống thay vì thành phần Giám sát tính toàn vẹn của tập tin. Thành phần Giám sát tính toàn vẹn của hệ thống bao gồm tất cả chức năng của Giám sát tính toàn vẹn của tập tin và ngoài ra còn cho phép giám sát các thay đổi của registry và kết nối của các thiết bị bên ngoài.

Thành phần Giám sát tính toàn vẹn của hệ thống sẽ giám sát những thay đổi trong hệ điều hành, có thể cho biết các hành vi xâm nhập bảo mật máy tính. Khi phát hiện những thay đổi như vậy, Kaspersky Endpoint Security sẽ tạo ra các sự kiện tương ứng và cảnh báo cho quản trị viên. Giám sát tính toàn vẹn hệ thống có thể hoạt động ở chế độ thời gian thực và cũng có thể thực hiện kiểm tra tính toàn vẹn hệ thống theo yêu cầu.

Giám sát tính toàn vẹn của hệ thống theo thời gian thực

Ở chế độ thời gian thực, Giám sát tính toàn vẹn của hệ thống theo dõi các thay đổi trong các đối tượng mà bạn đã đưa vào phạm vi của thành phần (*phạm vi giám sát*). Giám sát tính toàn vẹn hệ thống cũng cho phép chặn truy cập trái phép vào các đối tượng đó trong thời gian thực.

Kiểm tra tính toàn vẹn của hệ thống theo yêu cầu

Kiểm tra tính toàn vẹn của hệ thống theo yêu cầu là một tác vụ mà bạn có thể chạy thủ công hoặc theo lịch. Để chạy tác vụ *Kiểm tra tính toàn vẹn của hệ thống*, bạn phải cấu hình phạm vi của thành phần (*phạm vi giám sát*) và tạo đường cơ sở. *Đường cơ sở* là trạng thái được ghi lại của các đối tượng trong hệ thống, được ứng dụng sử dụng làm tham chiếu khi so sánh với trạng thái hiện tại.

Chuyển thiết lập Giám sát tính toàn vẹn của tập tin

Khi bạn cập nhật Kaspersky Endpoint Security lên phiên bản 12.6, thiết lập Giám sát tính toàn vẹn tập tin sẽ được di chuyển tự động. Là một phần của quá trình chuyển đổi, ứng dụng sẽ chuyển các quy tắc giám sát sang Giám sát tính toàn vẹn của hệ thống. Các quy tắc Giám sát tính toàn vẹn của tập tin cũng được chuyển sang Giám sát tính toàn vẹn của hệ thống khi chuyển từ KSWS sang KES.

Để đảm bảo tính năng Giám sát tính toàn vẹn của hệ thống hoạt động đúng, ứng dụng Kaspersky Endpoint Security và tiện ích quản lý đều phải được cập nhật lên phiên bản 12.6. Nếu bạn đã cài đặt phiên bản cũ hơn của tiện ích quản lý, bạn không thể cấu hình Giám sát tính toàn vẹn của hệ thống vì tiện ích quản lý thiếu phần **Giám sát tính toàn vẹn của hệ thống**.

Giới thiệu về quy tắc Giám sát tính toàn vẹn của hệ thống

Để tính năng Giám sát tính toàn vẹn hệ thống hoạt động, bạn phải thêm ít nhất một quy tắc. *Quy tắc Giám sát tính toàn vẹn của hệ thống* là một bộ tiêu chí xác định quyền truy cập của người dùng vào các tập tin và registry. Giám sát tính toàn vẹn hệ thống phát hiện các thay đổi trong tập tin và registry trong *phạm vi giám sát* được chỉ định. Phạm vi giám sát là một trong những tiêu chí của quy tắc Giám sát tính toàn vẹn hệ thống.

Giám sát tính toàn vẹn hệ thống cho phép giám sát các đối tượng sau:

- Tập tin
- Registry
- Thiết bị bên ngoài

Những cân nhắc đặc biệt liên quan đến việc giám sát tập tin

Giám sát tính toàn vẹn hệ thống sẽ giám sát các thay đổi trong tập tin và thư mục cũng như các tập tin được thêm vào phạm vi giám sát hoặc bị xóa khỏi phạm vi giám sát. Những thay đổi này có thể chỉ báo một vi phạm bảo mật máy tính. Bạn nên thêm các đối tượng hiếm khi được sửa đổi hoặc các đối tượng chỉ quản trị viên mới có quyền truy cập. Điều này giúp giảm số lượng sự kiện của Giám sát tính toàn vẹn hệ thống.

Tính năng Giám sát tính toàn vẹn hệ thống không theo dõi những thay đổi đối với các tập tin trong thư mục được chia sẻ trên máy chủ. Chỉ có thể sử dụng tính năng Giám sát tính toàn vẹn của hệ thống ở dạng cục bộ.

Kaspersky Endpoint Security chỉ giám sát những thay đổi của tập tin và thư mục trên những ổ đĩa được kết nối khi Giám sát tính toàn vẹn hệ thống theo thời gian thực bắt đầu hoạt động. Nếu ổ đĩa không được kết nối khi Giám sát tính toàn vẹn của hệ thống theo thời gian thực bắt đầu hoạt động, ứng dụng sẽ không giám sát những thay đổi của tập tin và thư mục trên ổ đĩa đó ngay cả khi các tập tin và thư mục đó được thêm vào phạm vi giám sát.

Những cân nhắc đặc biệt liên quan đến giám sát registry

Giám sát tính toàn vẹn hệ thống giám sát registry. Những thay đổi này có thể chỉ báo một vi phạm bảo mật máy tính.

Giám sát tính toàn vẹn hệ thống giám sát các khóa gốc sau của registry:

- `HKCR`
- `HKLM`
- `HKU`
- `HKCC`
- `HKEY_CLASSES_ROOT`
- `HKEY_LOCAL_MACHINE`
- `HKEY_USERS`
- `HKEY_CURRENT_CONFIG` (chỉ khả dụng trong Giám sát tính toàn vẹn của hệ thống theo thời gian thực)
- `HKEY_CURRENT_USER` (chỉ khả dụng trong Giám sát tính toàn vẹn của hệ thống theo thời gian thực)

> Tác vụ *Kiểm tra tính toàn vẹn của hệ thống* không hỗ trợ khóa `HKEY_CURRENT_USER`. Bạn có thể chỉ định một khóa trong `HKEY_USERS` dưới dạng `HKEY_USERS\<user profile ID>\<key>`.

Những cân nhắc đặc biệt liên quan đến giám sát thiết bị bên ngoài

Giám sát tính toàn vẹn hệ thống sẽ giám sát kết nối và ngắt kết nối của các thiết bị bên ngoài. Đây là điều cần thiết để bảo vệ máy tính trước các mối đe dọa bảo mật có thể xảy ra do trao đổi tập tin với các thiết bị đó. Giám sát tính toàn vẹn hệ thống không giám sát quyền truy cập vào các thiết bị bên ngoài và không chặn việc trao đổi tập tin. Bạn có thể cấu hình quyền truy cập thiết bị bằng thành phần ứng dụng khác, Kiểm soát thiết bị.

> Khi chạy tác vụ *Giám sát tính toàn vẹn của hệ thống cơ sở* ứng dụng sẽ bỏ qua việc kết nối lại các thiết bị bên ngoài nếu các thiết bị có cùng ký tự ổ đĩa trong hệ điều hành. Để được ghi nhật ký, các thiết bị được kết nối lại phải có ký tự ổ đĩa khác nhau.

Giám sát tính toàn vẹn hệ thống giám sát kết nối của các loại thiết bị bên ngoài sau:

- Ổ đĩa di động (bao gồm các ổ đĩa flash USB)
- Ổ đĩa cứng
- Bộ điều hợp mạng gắn ngoài

- Ổ đĩa CD/DVD/Blu-ray
- Máy quét / camera

Giám sát tính toàn vẹn của hệ thống theo thời gian thực

Giám sát tính toàn vẹn hệ thống cho phép theo dõi các thay đổi trong hệ điều hành theo thời gian thực. Bạn có thể theo dõi những thay đổi có thể chỉ báo các vi phạm bảo mật trên máy tính. Thành phần này cho phép chặn những thay đổi này hoặc chỉ ghi lại các sự kiện thay đổi.

Để tính năng Giám sát tính toàn vẹn hệ thống hoạt động, bạn phải thêm ít nhất một quy tắc. *Quy tắc Giám sát tính toàn vẹn của hệ thống* là một bộ tiêu chí xác định quyền truy cập của người dùng vào các tập tin và registry. Giám sát tính toàn vẹn hệ thống phát hiện các thay đổi trong tập tin và registry trong *phạm vi giám sát* được chỉ định. Phạm vi giám sát là một trong những tiêu chí của quy tắc Giám sát tính toàn vẹn hệ thống.

Chế độ giám sát tính toàn vẹn của hệ thống theo thời gian thực

Để đảm bảo rằng các quy tắc Giám sát tính toàn vẹn của hệ thống không chặn bất kỳ hành động nào có tài nguyên quan trọng đối với hoạt động của hệ điều hành hoặc các dịch vụ khác, bạn nên bật chế độ Kiểm tra và phân tích cách thành phần này ảnh hưởng đến hệ thống. Khi chế độ Kiểm tra được bật, Kaspersky Endpoint Security sẽ không chặn hoạt động của người dùng bị cấm theo quy tắc, thay vào đó sẽ tạo ra các sự kiện *Cảnh báo* ⚠.

Thành phần Giám sát tính toàn vẹn của hệ thống theo thời gian thực có hai chế độ:

- Chặn

  Ở chế độ này, Giám sát tính toàn vẹn hệ thống sẽ theo dõi các thay đổi trong hệ thống và thực hiện hành động theo các quy tắc: **Cho phép** hoặc **Chặn**. Giám sát tính toàn vẹn hệ thống cũng tạo ra một sự kiện tương ứng và thay đổi trạng thái của thiết bị trong bảng điều khiển Kaspersky Security Center.

- Thông báo

  Ở chế độ này, Giám sát tính toàn vẹn hệ thống cho phép thực hiện các hành động với tập tin và khóa registry từ phạm vi giám sát. Nếu hành động với tập tin hoặc registry bị cấm, ứng dụng sẽ tạo ra một sự kiện: *Đã cho phép thao tác bị cấm trong chế độ thử nghiệm*. Để phân tích các quy tắc ảnh hưởng đến hệ thống như thế nào, bạn có thể xem báo cáo.

Bật tính năng Giám sát tính toàn vẹn của hệ thống theo thời gian thực

Cách bật tính năng Giám sát tính toàn vẹn của hệ thống theo thời gian thực trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật → Giám sát tính toàn vẹn của hệ thống**.

4. Chọn hộp kiểm **Giám sát tính toàn vẹn của hệ thống**.

5. Trong mục **Chế độ hoạt động để chặn quy tắc**, hãy chọn chế độ Giám sát tính toàn vẹn của hệ thống theo thời gian thực:

   - **Chặn**. Ở chế độ này, Giám sát tính toàn vẹn hệ thống sẽ chặn các hành động với tập tin và khóa registry khỏi phạm vi giám sát và tạo ra một sự kiện tương ứng.

   - **Thông báo**. Ở chế độ này, Giám sát tính toàn vẹn hệ thống cho phép thực hiện các hành động với tập tin và khóa registry từ phạm vi giám sát và tạo ra một sự kiện tương ứng.

6. Trong mục **Giám sát tính toàn vẹn của hệ thống theo thời gian thực**, hãy chọn hộp kiểm **Giám sát tính toàn vẹn của hệ thống theo thời gian thực**.

7. Cấu hình giám sát thiết bị bên ngoài:

   a. Chọn hộp kiểm **Giám sát thiết bị**.

   b. Trong danh sách thả xuống **Mức nghiêm trọng của sự kiện**, hãy chọn mức độ quan trọng của các sự kiện giám sát thiết bị bên ngoài: *Thông tin*, *Cảnh báo*, *Nghiêm trọng*.

   Giám sát tính toàn vẹn hệ thống sẽ ghi lại kết nối hiện tại của các thiết bị bên ngoài. Ứng dụng sẽ tiến hành giám sát kết nối và ngắt kết nối của các thiết bị bên ngoài sau khi thành phần này được bật trong cài đặt ứng dụng. Sau đó, khi một thiết bị bên ngoài được kết nối hoặc ngắt kết nối, ứng dụng sẽ tạo ra một sự kiện tương ứng.

8. Cấu hình giám sát tập tin và registry:

   a. Chọn hộp kiểm **Giám sát tập tin và registry**.

   b. Nhấn vào **Thiết lập**.

   Thao tác này sẽ mở ra danh sách các quy tắc Giám sát tính toàn vẹn của hệ thống.

   c. Nhấn vào **Thêm**.

   Bạn cũng có thể nhập quy tắc từ nguồn khác.

   d. Cấu hình quy tắc Giám sát tính toàn vẹn của hệ thống (xem bảng bên dưới).

9. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật Giám sát tính toàn vẹn của hệ thống theo thời gian thực trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.

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 **Security Controls** → **System Integrity Monitoring**.

5. Bật nút bật/tắt **System Integrity Monitoring ENABLED**.

6. Chọn thẻ **Windows**.

7. Trong mục **Real-Time System Integrity Monitoring**, hãy chọn chế độ Giám sát tính toàn vẹn của hệ thống theo thời gian thực:

   - **Apply rules**. Ở chế độ này, Giám sát tính toàn vẹn hệ thống sẽ chặn các hành động với tập tin và khóa registry khỏi phạm vi giám sát và tạo ra một sự kiện tương ứng.
   - **Test rules (Inform)**. Ở chế độ này, Giám sát tính toàn vẹn hệ thống cho phép thực hiện các hành động với tập tin và khóa registry từ phạm vi giám sát và tạo ra một sự kiện tương ứng.

8. Cấu hình giám sát tập tin và registry:

   a. Chọn hộp kiểm **Monitor files and the registry**.

   b. Nhấn vào **Rules**.

   Thao tác này sẽ mở ra danh sách các quy tắc Giám sát tính toàn vẹn của hệ thống.

   c. Nhấn vào **Add**.

   Bạn cũng có thể nhập quy tắc từ nguồn khác.

   d. Cấu hình quy tắc Giám sát tính toàn vẹn của hệ thống (xem bảng bên dưới).

9. Cấu hình giám sát thiết bị bên ngoài:

   a. Chọn hộp kiểm **Monitor devices**.

   b. Trong danh sách thả xuống **Event severity level**, hãy chọn mức độ quan trọng của các sự kiện giám sát thiết bị bên ngoài: *Informational*, *Warning*, *Critical*.

   Giám sát tính toàn vẹn hệ thống sẽ ghi lại kết nối hiện tại của các thiết bị bên ngoài. Ứng dụng sẽ tiến hành giám sát kết nối và ngắt kết nối của các thiết bị bên ngoài sau khi thành phần này được bật trong cài đặt ứng dụng. Sau đó, khi một thiết bị bên ngoài được kết nối hoặc ngắt kết nối, ứng dụng sẽ tạo ra một sự kiện tương ứng.

10. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bật Giám sát tính toàn vẹn của hệ thống theo thời gian thực trong giao diện của 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 → Giám sát tính toàn vẹn của hệ thống**.
3. Bật nút gạt **Giám sát tính toàn vẹn của hệ thống**.
4. Trong mục **Chế độ hoạt động để chặn quy tắc**, hãy chọn chế độ Giám sát tính toàn vẹn của hệ thống theo thời gian thực:

   - **Chặn**. Ở chế độ này, Giám sát tính toàn vẹn hệ thống sẽ chặn các hành động với tập tin và khóa registry khỏi phạm vi giám sát và tạo ra một sự kiện tương ứng.
   - **Thông báo**. Ở chế độ này, Giám sát tính toàn vẹn hệ thống cho phép thực hiện các hành động với tập tin và khóa registry từ phạm vi giám sát và tạo ra một sự kiện tương ứng.

5. Trong mục **Giám sát tính toàn vẹn của hệ thống theo thời gian thực**, hãy chọn hộp kiểm **Giám sát tính toàn vẹn của hệ thống theo thời gian thực**.

6. Cấu hình giám sát thiết bị bên ngoài:

   a. Chọn hộp kiểm **Giám sát thiết bị**.

   b. Trong danh sách thả xuống **Mức nghiêm trọng của sự kiện**, hãy chọn mức độ quan trọng của các sự kiện giám sát thiết bị bên ngoài: *Thông tin*, *Cảnh báo*, *Nghiêm trọng*.

   Giám sát tính toàn vẹn hệ thống sẽ ghi lại kết nối hiện tại của các thiết bị bên ngoài. Ứng dụng sẽ tiến hành giám sát kết nối và ngắt kết nối của các thiết bị bên ngoài sau khi thành phần này được bật trong cài đặt ứng dụng. Sau đó, khi một thiết bị bên ngoài được kết nối hoặc ngắt kết nối, ứng dụng sẽ tạo ra một sự kiện tương ứng.

7. Cấu hình giám sát tập tin và registry:

   a. Chọn hộp kiểm **Giám sát tập tin và registry**.

   b. Nhấn vào **Thiết lập**.

   Thao tác này sẽ mở ra danh sách các quy tắc Giám sát tính toàn vẹn của hệ thống.

   c. Nhấn vào **Thêm**.

   Bạn cũng có thể nhập quy tắc từ nguồn khác.

8. Cấu hình quy tắc Giám sát tính toàn vẹn của hệ thống (xem bảng bên dưới).

9. Lưu các thay đổi của bạn.

Thiết lập quy tắc Giám sát tính toàn vẹn của hệ thống theo thời gian thực

Tham số	Mô tả
Tên quy tắc	Tên của quy tắc Giám sát tính toàn vẹn của hệ thống theo thời gian thực
Các thao tác với tập tin và registry	• **Cho phép**. Giám sát tính toàn vẹn hệ thống cho phép thực hiện các hành động với tập tin và khóa registry từ phạm vi giám sát. • **Chặn**. Hành vi của Giám sát tính toàn vẹn của hệ thống phụ thuộc vào chế độ đã chọn. Nếu bạn đã chọn *Chế độ bảo vệ hệ thống*, Giám sát tính toàn vẹn hệ thống sẽ chặn các hành động với tập tin và khóa registry từ phạm vi giám sát, tạo ra sự kiện tương ứng và thay đổi trạng thái của thiết bị trong bảng điều khiển Kaspersky Security Center. Nếu bạn đã chọn *Chế độ thử nghiệm*, Giám sát tính toàn vẹn hệ thống cho phép thực hiện các hành động với tập tin và khóa registry từ phạm vi giám sát.

Tham số	Mô tả
Mức nghiêm trọng của sự kiện	Kaspersky Endpoint Security ghi lại các sự kiện sửa đổi tập tin bất cứ khi nào tập tin hoặc khóa registry trong phạm vi giám sát được sửa đổi. Có sẵn các mức độ nghiêm trọng của sự kiện sau: *Thông tin*, *Cảnh báo*, *Nghiêm trọng*.

Phạm vi giám sát	• **Tập tin**. Danh sách các tập tin và thư mục được theo dõi bởi thành phần. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện.
	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 cấp 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.
	• **Registry**. Danh sách các khóa và giá trị registry được thành phần này giám sát. Kaspersky Endpoint Security hỗ trợ các ký tự `*` và `?` khi nhập tên đại diện.

Loại trừ	• **Tập tin**. Danh sách loại trừ khỏi phạm vi giám sát. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện. Ví dụ: `C:\Folder\Application\*.log`. Các mục loại trừ có mức độ ưu tiên cao hơn các mục phạm vi giám sát.
	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 cấp 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.
	• **Registry**. Danh sách loại trừ khỏi phạm vi giám sát. Kaspersky Endpoint Security hỗ trợ các ký tự `*` và `?` khi nhập tên đại diện. Các mục loại trừ có mức độ ưu tiên cao hơn các mục phạm vi giám sát.

Người dùng và / hoặc nhóm người dùng được tin tưởng	*Người dùng được tin tưởng* là người dùng được phép thực hiện các hành động với tập tin và khóa registry trong phạm vi giám sát. Nếu Kaspersky Endpoint Security phát hiện một hành động được thực hiện bởi một người dùng được tin tưởng, Giám sát tính toàn vẹn hệ thống sẽ tạo một sự kiện *Thông tin*. Bạn có thể chọn người dùng trong Active Directory, trong danh sách tài khoản trong Kaspersky Security Center hoặc bằng cách nhập tên người dùng cục bộ theo cách thủ công. Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền.
Bộ đánh dấu thao tác với tập tin / Các thao tác được giám sát	Các điểm đánh dấu đặc trưng cho hành động có các tập tin hoặc khóa registry mà ứng dụng sẽ giám sát.
Tạo giá trị băm	Tính toán giá trị hash của tập tin khi sửa đổi. Kaspersky Endpoint Security bổ sung thông tin về giá trị hash của tập tin khi một sự kiện được tạo ra.

Kiểm tra tính toàn vẹn của hệ thống theo yêu cầu

Kiểm tra tính toàn vẹn của hệ thống theo yêu cầu là một tác vụ mà bạn có thể chạy thủ công hoặc theo lịch. Khi chạy tác vụ *Kiểm tra tính toàn vẹn của hệ thống*, ứng dụng sẽ so sánh trạng thái hiện tại của các đối tượng trong phạm vi giám sát với trạng thái *đường cơ sở*. Ngược lại với Giám sát tính toàn vẹn của hệ thống theo thời gian thực, tác vụ *Kiểm tra tính toàn vẹn của hệ thống* sẽ giúp giới hạn số lượng sự kiện và cho phép bạn tạo báo cáo tổng thể về những thay đổi trong hệ điều hành.

Để tính năng Giám sát tính toàn vẹn hệ thống hoạt động, bạn phải thêm ít nhất một quy tắc. *Quy tắc Giám sát tính toàn vẹn của hệ thống* là một bộ tiêu chí xác định quyền truy cập của người dùng vào các tập tin và registry. Giám sát tính toàn vẹn hệ thống phát hiện các thay đổi trong tập tin và registry trong *phạm vi giám sát* được chỉ định. Phạm vi giám sát là một trong những tiêu chí của quy tắc Giám sát tính toàn vẹn hệ thống. Bạn có thể cấu hình các quy tắc được chia sẻ bởi Giám sát tính toàn vẹn của hệ thống theo thời gian thực và tác vụ *Kiểm tra tính toàn vẹn của hệ thống* hoặc tạo các quy tắc riêng cho tác vụ. Để tạo đường cơ sở, Kaspersky Endpoint Security sẽ áp dụng phạm vi giám sát từ tác vụ *Kiểm tra tính toàn vẹn của hệ thống* đến tác vụ *Cập nhật cơ sở*.

Tạo và cập nhật đường cơ sở

Các tác vụ *Kiểm tra tính toàn vẹn của hệ thống* cần một đường cơ sở để làm việc. *Đường cơ sở* là trạng thái được ghi lại của các đối tượng trong hệ thống, được ứng dụng sử dụng làm tham chiếu khi so sánh với trạng thái hiện tại. Nếu trạng thái hiện tại của hệ thống khác với trạng thái của hệ thống được ghi trong đường cơ sở, Kaspersky Endpoint Security sẽ tạo ra sự kiện tương ứng. Bạn có thể tạo hoặc cập nhật đường cơ sở bằng cách sử dụng tác vụ *Cập nhật cơ sở*.

Bạn có thể cập nhật đường cơ sở ở các chế độ sau:

- Cập nhật đầy đủ.
  Ứng dụng sẽ cập nhật tất cả các đối tượng trong phạm vi giám sát.
- Cập nhật tăng dần.
  Ứng dụng chỉ phát hiện và cập nhật các đối tượng được sửa đổi hoặc mới.

Cách tạo hoặc cập nhật đường cơ sở trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Tasks**.
   Danh sách tác vụ sẽ mở.
2. Nhấn vào **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 (14.2)** → **Cập nhật cơ sở**.

Bước 2. Chọn chế độ cập nhật cơ sở

Chọn chế độ cập nhật cơ sở:

- **Cập nhật đầy đủ**. Ứng dụng sẽ cập nhật tất cả các đối tượng trong phạm vi giám sát.
- **Cập nhật tăng dần**. Ứng dụng chỉ phát hiện và cập nhật các đối tượng được sửa đổi hoặc mới.

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 nhiệm vụ, ví dụ *Đường cơ sở 2024*.

Bước 5. Hoàn tất việc tạo tác vụ

Hoàn tất 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 tạo hoặc cập nhật đường cơ sở trong Bảng điều khiển web

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

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **Add**.

   Trình hướng dẫn Tác vụ sẽ được bắt đầu.

3. Cấu hình các thiết lập của tác vụ:

   a. Trong danh sách thả xuống **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.

   b. Trong danh sách thả xuống **Task type**, hãy chọn **Baseline update**.

c. Trong trường **Task name**, nhập một mô tả ngắn gọn, ví dụ như *Đường cơ sở 2024*.

d. Trong phần **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. Chọn một tài khoản để chạy tác vụ. Theo mặc định, Kaspersky Endpoint Security khởi chạy tác vụ với quyền của tài khoản người dùng cục bộ.
6. Hoàn tất 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. Chọn chế độ cập nhật cơ sở:
   - **Full update**. Ứng dụng sẽ cập nhật tất cả các đối tượng trong phạm vi giám sát.
   - **Incremental update**. Ứng dụng chỉ phát hiện và cập nhật các đối tượng được sửa đổi hoặc mới.
10. Lưu các thay đổi của bạn.
11. Chọn hộp kiểm cạnh tác vụ.
12. Nhấn vào **Start**.

Cấu hình phạm vi giám sát cho tác vụ Kiểm tra tính toàn vẹn của hệ thống

Theo mặc định, phạm vi giám sát của tác vụ *Kiểm tra tính toàn vẹn của hệ thống* giống như phạm vi giám sát của Giám sát tính toàn vẹn của hệ thống theo thời gian thực. Bạn có thể cấu hình phạm vi giám sát khác cho tác vụ.

> Giám sát tính toàn vẹn của hệ thống không hỗ trợ nhập các khóa `HKEY_CURRENT_USER` và `HKEY_CURRENT_CONFIG` cho tác vụ *Kiểm tra tính toàn vẹn của hệ thống*. Nếu phạm vi giám sát của tác vụ chứa các khóa này, ứng dụng sẽ tạo sự kiện *Phạm vi giám sát bao gồm các đối tượng không đúng*.

Cách cấu hình phạm vi giám sát khác cho tác vụ Kiểm tra tính toàn vẹn của hệ thống trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật → Giám sát tính toàn vẹn của hệ thống**.
4. Chọn hộp kiểm **Giám sát tính toàn vẹn của hệ thống**.

5. Trong mục **Kiểm tra tính toàn vẹn của hệ thống**, hãy chọn chế độ cấu hình tác vụ: **Thiết lập tùy chỉnh**.

6. Cấu hình giám sát thiết bị bên ngoài:

   a. Chọn hộp kiểm **Giám sát thiết bị**.

   b. Trong danh sách thả xuống **Mức nghiêm trọng của sự kiện**, hãy chọn mức độ quan trọng của các sự kiện giám sát thiết bị bên ngoài: *Thông tin*, *Cảnh báo*, *Nghiêm trọng*.

   Giám sát tính toàn vẹn hệ thống sẽ ghi lại thông tin về các thiết bị bên ngoài được kết nối tại thời điểm đường cơ sở được tạo. Sau đó, khi một thiết bị bên ngoài được kết nối, ứng dụng sẽ tạo ra một sự kiện tương ứng. Khi chạy tác vụ *Kiểm tra tính toàn vẹn của hệ thống*, ứng dụng không giám sát việc ngắt kết nối của các thiết bị bên ngoài.

7. Cấu hình giám sát tập tin và registry:

   a. Chọn hộp kiểm **Giám sát tập tin và registry**.

   b. Nhấn vào **Thiết lập**.

   Thao tác này sẽ mở ra danh sách các quy tắc Giám sát tính toàn vẹn của hệ thống.

   c. Nhấn vào **Thêm**.

   Bạn cũng có thể nhập quy tắc từ nguồn khác.

   d. Cấu hình quy tắc Giám sát tính toàn vẹn của hệ thống (xem bảng bên dưới).

8. Lưu các thay đổi của bạn.

Cách cấu hình phạm vi giám sát khác cho tác vụ System Integrity Check trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.

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 **Security Controls** → **System Integrity Monitoring**.

5. Chọn thẻ **Windows**.

6. Bật nút bật/tắt **System Integrity Monitoring ENABLED**.

7. Trong mục **System Integrity Check**, hãy chọn chế độ cấu hình tác vụ: **Custom settings**.

8. Cấu hình giám sát thiết bị bên ngoài:

   a. Chọn hộp kiểm **Monitor devices**.

   b. Trong danh sách thả xuống **Event severity level**, hãy chọn mức độ quan trọng của các sự kiện giám sát thiết bị bên ngoài: *Informational*, *Warning*, *Critical*.

Giám sát tính toàn vẹn hệ thống sẽ ghi lại thông tin về các thiết bị bên ngoài được kết nối tại thời điểm đường cơ sở được tạo. Sau đó, khi một thiết bị bên ngoài được kết nối, ứng dụng sẽ tạo ra một sự kiện tương ứng. Khi chạy tác vụ *Kiểm tra tính toàn vẹn của hệ thống*, ứng dụng không giám sát việc ngắt kết nối của các thiết bị bên ngoài.

9. Cấu hình giám sát tập tin và registry:

   a. Chọn hộp kiểm **Monitor files and the registry**.

   b. Nhấn vào **Rules**.

   Thao tác này sẽ mở ra danh sách các quy tắc Giám sát tính toàn vẹn của hệ thống.

   c. Nhấn vào **Add**.

   Bạn cũng có thể nhập quy tắc từ nguồn khác.

   d. Cấu hình quy tắc Giám sát tính toàn vẹn của hệ thống (xem bảng bên dưới).

10. Lưu các thay đổi của bạn.

Cách cấu hình phạm vi giám sát khác cho tác vụ Kiểm tra tính toàn vẹn của hệ thống 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 **Kiểm soát bảo mật → Giám sát tính toàn vẹn của hệ thống**.

3. Bật nút gạt **Giám sát tính toàn vẹn của hệ thống**.

4. Trong mục **Kiểm tra tính toàn vẹn của hệ thống**, hãy chọn chế độ cấu hình tác vụ: **Thiết lập tùy chỉnh**.

5. Cấu hình giám sát thiết bị bên ngoài:

   a. Chọn hộp kiểm **Giám sát thiết bị**.

   b. Trong danh sách thả xuống **Mức nghiêm trọng của sự kiện**, hãy chọn mức độ quan trọng của các sự kiện giám sát thiết bị bên ngoài: *Thông tin* ⓘ, *Cảnh báo* ⚠, *Nghiêm trọng* ⓘ.

   Giám sát tính toàn vẹn hệ thống sẽ ghi lại thông tin về các thiết bị bên ngoài được kết nối tại thời điểm đường cơ sở được tạo. Sau đó, khi một thiết bị bên ngoài được kết nối, ứng dụng sẽ tạo ra một sự kiện tương ứng. Khi chạy tác vụ *Kiểm tra tính toàn vẹn của hệ thống*, ứng dụng không giám sát việc ngắt kết nối của các thiết bị bên ngoài.

6. Cấu hình giám sát tập tin và registry:

   a. Chọn hộp kiểm **Giám sát tập tin và registry**.

   b. Nhấn vào **Thiết lập**.

   Thao tác này sẽ mở ra danh sách các quy tắc Giám sát tính toàn vẹn của hệ thống.

c. Nhấn vào **Thêm**.

Bạn cũng có thể nhập quy tắc từ nguồn khác.

d. Cấu hình quy tắc Giám sát tính toàn vẹn của hệ thống (xem bảng bên dưới).

7. Lưu các thay đổi của bạn.

Thiết lập của một quy tắc tác vụ Kiểm tra tính toàn vẹn của hệ thống

Tham số	Mô tả
Tên quy tắc	Tên của quy tắc tác vụ *Kiểm tra tính toàn vẹn của hệ thống*.
Mức nghiêm trọng của sự kiện	Kaspersky Endpoint Security ghi lại các sự kiện sửa đổi tập tin bất cứ khi nào tập tin hoặc khóa registry trong phạm vi giám sát được sửa đổi. Có sẵn các mức độ nghiêm trọng của sự kiện sau: *Thông tin*, *Cảnh báo*, *Nghiêm trọng*.

Phạm vi giám sát	• **Tập tin**. Danh sách các tập tin và thư mục được theo dõi bởi thành phần. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện.
	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 cấp 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.
	• **Registry**. Danh sách các khóa và giá trị registry được thành phần này giám sát. Kaspersky Endpoint Security hỗ trợ các ký tự `*` và `?` khi nhập tên đại diện.

Loại trừ	• **Tập tin**. Danh sách loại trừ khỏi phạm vi giám sát. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện. Ví dụ: `C:\Folder\Application\*.log`. Các mục loại trừ có mức độ ưu tiên cao hơn các mục phạm vi giám sát.
	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 cấp 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.
	• **Registry**. Danh sách loại trừ khỏi phạm vi giám sát. Kaspersky Endpoint Security hỗ trợ các ký tự `*` và `?` khi nhập tên đại diện. Các mục loại trừ có mức độ ưu tiên cao hơn các mục phạm vi giám sát.

Chạy tác vụ Kiểm tra tính toàn vẹn của hệ thống

Tác vụ *Kiểm tra tính toàn vẹn của hệ thống* cho phép kiểm tra các tập tin hoặc khóa registry để tìm các thay đổi và cũng kiểm tra kết nối của các thiết bị bên ngoài. Để kiểm tra các thay đổi của tập tin, bạn có thể chạy tác vụ *Kiểm tra tính toàn vẹn của hệ thống* ở các chế độ sau:

- Quét nhanh.

  Khi kiểm tra các thay đổi của tập tin, ứng dụng chỉ kiểm tra các thuộc tính của tập tin. Ứng dụng không kiểm tra nội dung của tập tin.

- Quét toàn bộ.

  Khi kiểm tra các thay đổi của tập tin, ứng dụng sẽ kiểm tra tất cả các thuộc tính tập tin và nội dung của tập tin.

Chế độ mà tác vụ chạy trong đó không ảnh hưởng đến việc kiểm tra registry hoặc các thiết bị bên ngoài.

Cách chạy tác vụ Kiểm tra tính toàn vẹn của hệ thống trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Tasks**.

   Danh sách tác vụ sẽ mở.
3. Nhấn vào **New task**.

   Trình hướng dẫn Tác vụ sẽ được bắt đầu. Làm theo chỉ dẫn của Trình hướng dẫn.
4. Chọn **Kaspersky Endpoint Security → Giám sát tính toàn vẹn của hệ thống cơ sở**. Chọn chế độ Giám sát tính toàn vẹn của hệ thống:

   - **Quét toàn bộ**. Ở chế độ này, ứng dụng sẽ kiểm tra tất cả các thuộc tính và giá trị hash của các tập tin.
   - **Quét nhanh**. Ở chế độ này, ứng dụng chỉ kiểm tra các thuộc tính của tập tin.
5. Chọn các máy tính sẽ được thực hiện tác vụ trên đó. Các tùy chọn sau có thể được sử dụng:

   - 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.
   - Chỉ định danh sách thiết bị mà bạn muốn chạy tác vụ.
   - 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.
6. Chọn một tài khoản để chạy tác vụ. Theo mặc định, Kaspersky Endpoint Security khởi chạy tác vụ với quyền của tài khoản người dùng cục bộ.
7. Cấu hình lịch để khởi chạy một tác vụ, ví dụ như chạy thủ công hoặc vào một ngày cụ thể trong tuần.

8. Nhập tên cho tác vụ.

9. Hoàn tất 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 chạy tác vụ System Integrity Check trong Bảng điều khiển web

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

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **Add**.

   Trình hướng dẫn Tác vụ sẽ được bắt đầu.

3. Cấu hình các thiết lập của tác vụ:

   a. Trong danh sách thả xuống **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.

   b. Trong danh sách thả xuống **Task type**, hãy chọn **System Integrity Check**.

   c. Trong trường **Task name**, nhập một mô tả ngắn, ví dụ như *Kiểm tra tính toàn vẹn hệ thống hàng tuần*.

   d. Trong phần **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. Chọn một tài khoản để chạy tác vụ. Theo mặc định, Kaspersky Endpoint Security khởi chạy tác vụ với quyền của tài khoản người dùng cục bộ.

6. Hoàn tất 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. Chọn chế độ Kiểm tra tính toàn vẹn của hệ thống:

   - **Quick Scan**. Ứng dụng chỉ kiểm tra các thuộc tính của tập tin. Ứng dụng không kiểm tra nội dung của tập tin.

   - **Full Scan**. Ứng dụng kiểm tra tất cả các thuộc tính cũng như nội dung của tập tin.

10. Lưu các thay đổi của bạn.

11. Chọn hộp kiểm cạnh tác vụ.

12. Nhấn vào **Start**.

Để tác vụ *Kiểm tra tính toàn vẹn của hệ thống* hoàn tất thành công, phạm vi giám sát của tác vụ *Kiểm tra tính toàn vẹn của hệ thống* phải hoàn toàn phù hợp với đường cơ sở. Nếu phạm vi giám sát khác, tác vụ sẽ kết thúc kèm một lỗi. Để đồng bộ hóa phạm vi giám sát, hãy chạy tác vụ *Cập nhật cơ sở* với phạm vi giám sát mới.

Xuất và nhập quy tắc Giám sát tính toàn vẹn hệ thống

Bạn có thể xuất danh sách các quy Giám sát tính toàn vẹn của hệ thống vào tập tin XML. Sau đó, bạn có thể sửa đổi tập tin, ví dụ như thêm một số lượng lớn các bản ghi cùng loại. Bạn có thể sử dụng chức năng xuất/nhập để sao lưu danh sách quy tắc Giám sát tính toàn vẹn của hệ thống hoặc để chuyển danh sách sang máy chủ khác.

Giám sát tính toàn vẹn của hệ thống không hỗ trợ nhập các khóa `HKEY_CURRENT_USER` và `HKEY_CURRENT_CONFIG` cho tác vụ *Kiểm tra tính toàn vẹn của hệ thống*. Nếu phạm vi giám sát của tác vụ chứa các khóa này, ứng dụng sẽ tạo sự kiện *Phạm vi giám sát bao gồm các đối tượng không đúng*.

Cách xuất và nhập danh sách quy tắc Giám sát tính toàn vẹn của hệ thống trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Kiểm soát bảo mật → Giám sát tính toàn vẹn của hệ thống**.
4. Để xuất hoặc nhập các quy tắc *Giám sát tính toàn vẹn của hệ thống theo thời gian thực*:
   a. Trong mục **Giám sát tính toàn vẹn của hệ thống theo thời gian thực**, hãy nhấn nút **Thiết lập**.
   b. Để xuất danh sách các quy tắc Giám sát tính toàn vẹn của hệ thống theo thời gian thực:
      1. 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.
      2. Nhấn vào liên kết **Xuất**.
      3. 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.
      4. Lưu tập tin.
         Kaspersky Endpoint Security sẽ xuất danh sách các quy tắc vào tập tin XML.
   c. Để nhập danh sách các quy tắc Giám sát tính toàn vẹn của hệ thống theo thời gian thực:
      1. Nhấn vào liên kết **Nhập**.
         Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách các quy tắc.
      2. 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.

5. Để xuất hoặc nhập các quy tắc *Kiểm tra tính toàn vẹn của hệ thống*:

   a. Trong mục **Kiểm tra tính toàn vẹn của hệ thống**, hãy chọn **Thiết lập tùy chỉnh**.

   b. Nhấn vào **Thiết lập**.

   c. Để xuất danh sách quy tắc Kiểm tra tính toàn vẹn của hệ thống:

      1. 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.
      2. Nhấn vào liên kết **Xuất**.
      3. 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.
      4. Lưu tập tin.

      Kaspersky Endpoint Security sẽ xuất danh sách các quy tắc vào tập tin XML.

   d. Để nhập danh sách quy tắc Kiểm tra tính toàn vẹn của hệ thống:

      1. Nhấn vào liên kết **Nhập**.
         Trong cửa sổ mở ra, hãy chọn tập tin XML mà bạn muốn nhập danh sách các quy tắc.
      2. 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.

6. Lưu các thay đổi của bạn.

Cách xuất và nhập danh sách quy tắc Giám sát tính toàn vẹn hệ thống trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Policies**.
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 **Security Controls → System Integrity Monitoring**.
5. Chọn thẻ **Windows**.

6. Để xuất hoặc nhập các quy tắc *Giám sát tính toàn vẹn của hệ thống theo thời gian thực*:

   a. Trong mục **Real-Time System Integrity Monitoring**, hãy nhấn liên kết **Rules**.

   b. Để xuất danh sách các quy tắc Giám sát tính toàn vẹn của hệ thống theo thời gian thực:

      1. Chọn các quy tắc mà bạn muốn xuất.

      2. Nhấn nút → **Export**.

         Kaspersky Endpoint Security sẽ xuất danh sách các quy tắc vào tập tin JSON trong thư mục tải xuống mặc định.

   c. Để nhập danh sách các quy tắc Giám sát tính toàn vẹn của hệ thống theo thời gian thực:

      1. Nhấn nút → **Import**.

         Trong cửa sổ mở ra, hãy chọn tập tin JSON mà bạn muốn nhập danh sách địa chỉ được tin tưởng.

      2. 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 JSON.

7. Để xuất hoặc nhập các quy tắc *Kiểm tra tính toàn vẹn của hệ thống*:

   a. Trong mục **On-Demand System Integrity Check**, hãy chọn **Custom settings**.

   b. Nhấn vào liên kết **Rules**.

   c. Để xuất danh sách quy tắc Kiểm tra tính toàn vẹn của hệ thống:

      1. Chọn các quy tắc mà bạn muốn xuất.

      2. Nhấn nút → **Export**.

         Kaspersky Endpoint Security sẽ xuất danh sách các quy tắc vào tập tin JSON trong thư mục tải xuống mặc định.

   d. Để nhập danh sách quy tắc Kiểm tra tính toàn vẹn của hệ thống:

      1. Nhấn nút → **Import**.

         Trong cửa sổ mở ra, hãy chọn tập tin JSON mà bạn muốn nhập danh sách địa chỉ được tin tưởng.

      2. 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 JSON.

8. Lưu các thay đổi của bạn.

Xem báo cáo Giám sát tính toàn vẹn của hệ thống

Để phân tích hiệu năng của các quy tắc Giám sát tính toàn vẹn của hệ thống, bạn có thể xem các báo cáo và sự kiện do ứng dụng tạo ra. Kaspersky Endpoint Security tạo các báo cáo sau về thành phần này:

- Trong giao diện ứng dụng:
  - Báo cáo Giám sát tính toàn vẹn của hệ thống
  - Báo cáo Kiểm tra tính toàn vẹn của hệ thống
  - Báo cáo cập nhật đường cơ sở

  Các báo cáo chứa sự kiện của Giám sát tính toàn vẹn của hệ thống.
- Trong Bảng điều khiển Kaspersky Security Center:
  - Báo cáo về các máy tính có quy tắc giám sát được kích hoạt nhiều lần nhất
  - Báo cáo về các quy tắc giám sát được kích hoạt thường xuyên nhất

  Theo mặc định, một báo cáo được tạo trong 30 ngày trước đó, bao gồm cả ngày tạo báo cáo.

  Cách xem báo cáo Giám sát tính toàn vẹn hệ thống trong Bảng điều khiển quản trị (MMC)

  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 vào **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**, hãy chọn báo cáo Giám sát tính toàn vẹn hệ thống (phần **Other**):
     - **Top 10 devices with File Integrity Monitor / System Integrity Monitoring rules most frequently triggered**.
     - **Top 10 rules of File Integrity Monitor / System Integrity Monitoring that were triggered on devices most frequently**.

     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.

Cách xem báo cáo Giám sát tính toàn vẹn của hệ thống trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Monitoring → Reports**.
2. Nhấn vào **Add**.

   Trình hướng dẫn tạo mẫu báo cáo mới sẽ khởi chạy.
3. Trong **Template type**, trong phần **Other**, hãy chọn báo cáo Giám sát tính toàn vẹn hệ thống:

   - **Top 10 devices with File Integrity Monitor / System Integrity monitoring rules most frequently triggered**.
   - **Top 10 rules of File Integrity Monitor / System Integrity Monitoring that were triggered on devices most frequently**.

   Sau khi bạn đã hoàn tất với Trình hướng dẫn Mẫu Báo cáo Mới, một mẫu báo cáo mới sẽ xuất hiện trong bảng.
4. Chọn và chạy báo cáo.

Tiến trình tạo báo cáo sẽ được bắt đầu. Báo cáo sẽ được hiển thị trong một cửa sổ mới.

Để xem các sự kiện do ứng dụng tạo ra, bạn cũng có thể sử dụng các lựa chọn sự kiện trong bảng điều khiển Kaspersky Security Center.

Đặt lại trạng thái toàn vẹn của hệ thống

Các máy tính trong bảng điều khiển Kaspersky Security Center có một trong các trạng thái sau: *OK*, *Warning*, hoặc *Critical*. Nếu Giám sát tính toàn vẹn hệ thống phát hiện việc sửa đổi tập tin hoặc khóa registry trong phạm vi giám sát thì trạng thái của máy tính sẽ thay đổi thành *Warning* hoặc *Critical*. Trạng thái được chỉ định bởi Giám sát tính toàn vẹn hệ thống được gọi là *trạng thái toàn vẹn của hệ thống*. Bạn có thể đặt lại trạng thái toàn vẹn của hệ thống, chẳng hạn như nếu quá trình phân tích thuyết phục bạn rằng việc sửa đổi đối tượng được phát hiện không ảnh hưởng đến tính bảo mật của máy tính.

Cách đặt lại trạng thái toàn vẹn của hệ thống trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Tasks**.

   Danh sách tác vụ sẽ mở.
2. Nhấn vào **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 (14.2) → Đặt lại trạng thái tính toàn vẹn của hệ thống**.

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 tác vụ, ví dụ như theo cách thủ công.

Bước 4. Xác định tên tác vụ

Nhập tên của tác vụ, ví dụ: *Đặt lại trạng thái sau khi sửa đổi phạm vi giám sát*.

Bước 5. Hoàn tất việc tạo tác vụ

Hoàn tất 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 đặt lại trạng thái toàn vẹn của hệ thống trong Bảng điều khiển web

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

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **Add**.

   Trình hướng dẫn Tác vụ sẽ được bắt đầu.

3. Cấu hình các thiết lập của tác vụ:

   a. Trong danh sách thả xuống **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.

   b. Trong danh sách thả xuống **Task type**, hãy chọn **System integrity status reset**.

c. Trong trường **Task name**, hãy nhập mô tả ngắn gọn, ví dụ: *Đặt lại trạng thái sau khi sửa đổi phạm vi giám sát*.

d. Trong phần **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. Chọn một tài khoản để chạy tác vụ. Theo mặc định, Kaspersky Endpoint Security khởi chạy tác vụ với quyền của tài khoản người dùng cục bộ.

6. Hoàn tất trình hướng dẫn.

   Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ.

7. Chọn hộp kiểm cạnh tác vụ.

8. Nhấn vào **Start**.

Kết quả là, nếu trạng thái của máy tính được thay đổi thành *Warning* hoặc *Critical* do sự kiện Giám sát tính toàn vẹn hệ thống, trạng thái của máy tính được đặt lại về *OK*. Nếu trạng thái của máy tính cũng bị thay đổi do các sự kiện khác thì trạng thái của máy tính vẫn không thay đổi.

Cloud Discovery

Cloud Discovery quản lý quyền truy cập của người dùng vào các dịch vụ đám mây. Các ví dụ về dịch vụ đám mây bao gồm Microsoft Teams, Salesforce và Microsoft Office 365. Các dịch vụ đám mây được phân loại thành nhiều nhóm, ví dụ như: *File sharing*, *Messengers*, *Email*. Chuyên gia của Kaspersky thường xuyên cập nhật các danh mục Cloud Discovery và các dịch vụ đám mây được phân loại trong các danh mục đó. Kaspersky Endpoint Security cập nhật bộ danh mục và dịch vụ đám mây cùng với cơ sở dữ liệu ứng dụng. Điều này có nghĩa là Cloud Discovery không sử dụng Kaspersky Security Network để phân loại các dịch vụ đám mây.

Cloud Discovery cung cấp các chức năng sau:

- Giám sát việc sử dụng dịch vụ đám mây
- Chặn người dùng truy cập dịch vụ đám mây

Yêu cầu hệ thống

Cloud Discovery khả dụng nếu đáp ứng các điều kiện sau:

- Ứng dụng được cài đặt trên máy tính chạy Windows dành cho máy trạm.

  Thành phần này không khả dụng trên máy chủ.

- Kaspersky Security Center phiên bản 15.1 trở lên.

  Thành phần này không khả dụng trong Bảng điều khiển quản trị (MMC). Bạn có thể cấu hình Cloud Discovery trong Bảng điều khiển web Kaspersky Security Center hoặc Bảng điều khiển đám mây Kaspersky Security Center.

- Giấy phép Kaspersky Next.

Bật chức năng ứng dụng mà thành phần Cloud Discovery yêu cầu:

1. **Quét các kết nối mã hóa**. Đây là điều cần thiết để theo dõi lưu lượng HTTPS. Bạn có thể quản lý chức năng này trong phần **Thiết lập mạng**.

2. **Chèn mã vào lưu lượng web để tương tác với các trang web**. Tập lệnh này cho phép đăng ký các sự kiện Cloud Discovery. Tập lệnh này cũng cung cấp đầy đủ tính năng chặn truy cập vào các dịch vụ đám mây. Nếu không có tập lệnh này, ứng dụng sẽ chỉ chặn truy cập của các miền dịch vụ đám mây. Bạn có thể quản lý chức năng này trong phần **Thiết lập mạng**.

Bạn cũng có thể kích hoạt chức năng **Ghi lại việc mở ra các trang được cho phép**. Chức năng này bao gồm nhóm các sự kiện khi người dùng truy cập các trang web thuộc cùng một tên miền. Bằng cách này, khi người dùng sử dụng dịch vụ đám mây, Cloud Discovery sẽ chỉ ghi lại một sự kiện thay vì nhiều sự kiện cho mỗi trang web. Bạn có thể quản lý chức năng này trong phần **Kiểm soát Web**.

Giám sát dịch vụ đám mây

Khi người dùng bắt đầu sử dụng dịch vụ đám mây, Kaspersky Endpoint Security sẽ đăng ký sự kiện đó và tạo một mục trong báo cáo. Cloud Discovery kiểm soát việc sử dụng dịch vụ đám mây trong trình duyệt cũng như trong các ứng dụng tương ứng. Cloud Discovery kiểm soát việc sử dụng dịch vụ đám mây qua HTTP và HTTPS.

Cách bật giám sát dịch vụ đám mây trong Cloud Console

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.

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 **Communication & Web Protection** → **Cloud Discovery**.

5. Bật nút bật/tắt **Cloud Discovery ENABLED**.

6. Lưu các thay đổi của bạn.

   Kết quả là ứng dụng sẽ chuyển tiếp thông tin về các dịch vụ đám mây đang được sử dụng tới Kaspersky Security Center. Bạn có thể xem thông tin sử dụng dịch vụ đám mây trong các báo cáo. Nếu cần, bạn có thể chặn quyền truy cập vào các dịch vụ đám mây.

Chặn quyền truy cập dịch vụ đám mây

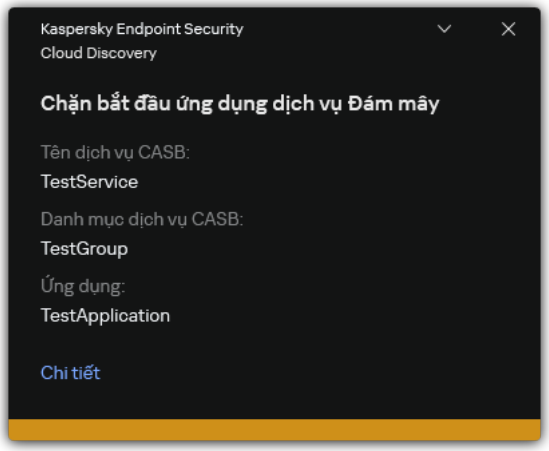
Việc chặn truy cập các dịch vụ đám mây chỉ khả dụng đối với giấy phép Kaspersky Next EDR Optimum và XDR Expert. Tính năng này không khả dụng với giấy phép Kaspersky Next EDR Foundations. So sánh chức năng của ứng dụng tùy thuộc vào loại giấy phép Kaspersky Next, hãy xem trong Trợ giúp của Kaspersky Next.

Quản trị viên có thể hạn chế quyền truy cập của người dùng vào các danh mục Cloud Discovery hoặc các dịch vụ đám mây riêng lẻ. Bằng cách này, quản trị viên có thể chỉ cho phép sử dụng các dịch vụ đám mây bảo mật và tránh rò rỉ dữ liệu. *Thông tin mức độ rủi ro* được hiển thị cho từng dịch vụ đám mây trong Cloud Discovery. Mức độ rủi ro giúp phát hiện các dịch vụ không đáp ứng các yêu cầu về bảo mật của tổ chức.

Mức độ rủi ro chỉ là sự ước lượng và không ngụ ý bất kỳ tuyên bố nào về chất lượng của dịch vụ đám mây hoặc nhà cung cấp dịch vụ đó. Mức độ rủi ro chỉ đơn giản là khuyến nghị của các chuyên gia Kaspersky.

Mức độ rủi ro của dịch vụ đám mây được hiển thị trong mục **Cloud Discovery** của chính sách trong danh sách tất cả các dịch vụ đám mây được kiểm soát.

Các thành phần khác của Kaspersky Endpoint Security cung cấp khả năng bảo vệ trước các mối đe dọa và theo dõi hoạt động đáng ngờ của người dùng khi sử dụng dịch vụ đám mây.



Thông báo của Cloud Discovery

Cloud Discovery không chặn các ứng dụng đám mây đã được khởi chạy trước Kaspersky Endpoint Security.

Cách chặn truy cập các dịch vụ đám mây trong Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Communication & Web Protection** → **Cloud Discovery**.
5. Bật nút bật/tắt **Cloud Discovery ENABLED**.

   Một danh sách tất cả các dịch vụ đám mây được hiển thị. Các dịch vụ đám mây được phân loại thành nhiều nhóm, ví dụ như: *File sharing*, *Messengers*, *Email*. Chuyên gia của Kaspersky thường xuyên cập nhật các danh mục Cloud Discovery và các dịch vụ đám mây được phân loại trong các danh mục đó. Kaspersky Endpoint Security cập nhật bộ danh mục và dịch vụ đám mây cùng với cơ sở dữ liệu ứng dụng.

6. Sử dụng nút bật/tắt trong cột **Access** để cấu hình quyền truy cập dịch vụ đám mây.

7. Lưu các thay đổi của bạn.

Kết quả là ứng dụng sẽ kiểm soát việc sử dụng dịch vụ đám mây trên trình duyệt cũng như trong các ứng dụng tương ứng.

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.

Kể từ Kaspersky Endpoint Security 12.5 cho Windows, bạn có thể thêm đo lường từ xa EDR vào vùng tin tưởng. Điều này cho phép tối ưu hóa dữ liệu mà ứng dụng gửi đến máy chủ Đo lường từ xa cho giải pháp Kaspersky Anti Targeted Attack Platform (EDR).

Kể từ Kaspersky Endpoint Security 12.6 cho Windows, loại trừ quét và ứng dụng được tin tưởng được thêm vào khu vực tin tưởng. Các ứng dụng được tin tưởng và loại trừ quét được xác định trước giúp nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager. Điều này có nghĩa là bạn không cần thiết lập khu vực tin tưởng theo cách thủ công cho ứng dụng trên máy chủ.

Kể từ Kaspersky Endpoint Security 12.8 cho Windows, bạn có thể cài đặt ứng dụng ở chế độ Light Agent để bảo vệ môi trường ảo. Các loại trừ quét được định sẵn và các ứng dụng được tin tưởng có thể giúp bạn nhanh chóng cấu hình Kaspersky Endpoint Security trong các môi trường máy ảo Citrix và VMware.

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 pháp. Đây là các phần mềm có thể bị khai thác bởi bọn tội phạm để làm hỏng máy tính hoặc dữ liệu người dùng. Những ứng dụng như vậy không nhất thiết có mục đích xấu, nhưng có thể bị tin tặc lợi dụng. Để biết thông tin chi tiết về các ứng dụng hợp pháp mà kẻ xâm nhập có thể lợi dụng để xâm nhập máy tính hoặc dữ liệu người dùng, vui lòng truy cập trang web Bách khoa toàn thư của Kaspersky.

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 phần mềm độc hại*

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 cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Loại trừ và loại đối tượng**.
5. Trong mục **Loại trừ quét và ứng dụng được tin tưởng → Loại trừ quét**, hãy nhấn nút **Thiết lập**.

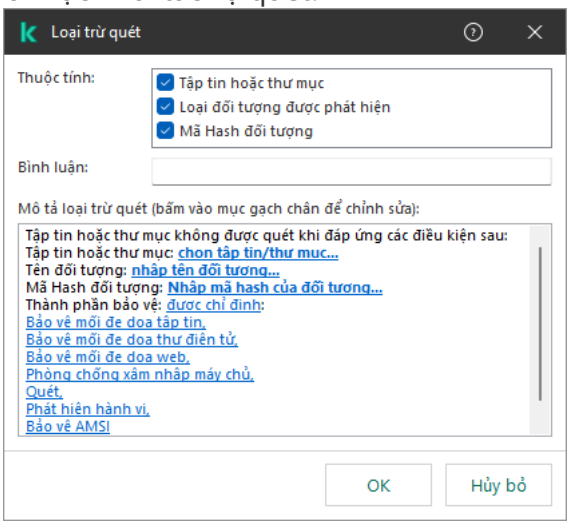
   Thao tác này sẽ mở cửa sổ chứa danh sách các loại trừ.
6. Chọn hộp kiểm **Hợp nhất các giá trị khi kế thừa** nếu bạn muốn tạo một danh sách tổng hợp các loại trừ cho tất cả các máy tính trong công ty. Danh sách các loại trừ trong chính sách cha và chính sách con sẽ được hợp nhất. Các danh sách sẽ được 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 **Cho phép sử dụng các loại trừ cục bộ** 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. Ngoài ra, nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ ẩn danh sách tổng hợp các loại trừ quét trong giao diện người dùng của ứng dụng.
8. Nhấn vào **Thêm** và chọn một hành động:
   - **Danh mục**. Bạn có thể nhóm các loại trừ quét thành các danh mục riêng biệt. Để tạo một danh mục mới, hãy nhập tên danh mục và thêm ít nhất một loại trừ quét vào danh mục đó.
   - **Loại trừ mới**. Kaspersky Endpoint Security sẽ thêm một loại trừ quét mới vào gốc của danh sách.

- **Chọn loại trừ trong danh sách**. Để nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager, ứng dụng bao gồm *loại trừ quét được xác định trước*. Ngoài ra, các loại trừ quét được định sẵn cũng đã được thêm vào để hỗ trợ thiết lập ứng dụng trong môi trường ảo Citrix và VMware. Bạn phải chọn loại trừ quét được xác định trước tùy thuộc vào mục đích của máy chủ được bảo vệ.

- **Mục loại trừ mới cho danh mục đã chọn**. Hãy chọn một danh mục để thêm một loại trừ quét mới vào một danh mục cụ thể.

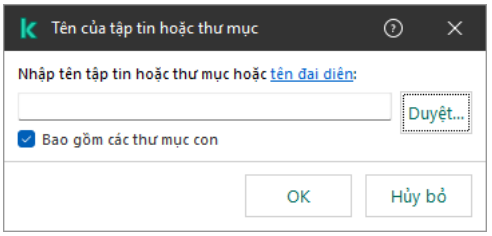
9. Để loại trừ một tập tin hoặc thư mục khỏi tác vụ quét:



Thiết lập loại trừ

a. Trong mục **Thuộc tính**, hãy chọn hộp kiểm **Tập tin hoặc thư mục**.

b. Nhấn vào liên kết trong mục bên dưới để mở cửa sổ **Tên của tập tin hoặc thư mục**.



Chọn tập tin hoặc thư mục

a. 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 cấp 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 sử dụng tên đại diện ở đầu, ở giữa hoặc ở cuối đường dẫn tập tin. Ví dụ: nếu bạn muốn thêm một thư mục cho tất cả người dùng để loại trừ, hãy nhập tên đại diện `?:\Users\*\Folder\`.

Kaspersky Endpoint Security hỗ trợ các biến môi trường

Bạn có thể loại trừ các thư mục mạng. Để thực hiện, hãy nhập đường dẫn đến thư mục mạng theo cách thủ công (ví dụ: `\\Network Share\*`).

> Kaspersky Endpoint Security không hỗ trợ biến môi trường `%userprofile%` khi tạo một danh sách các loại trừ bằng 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.

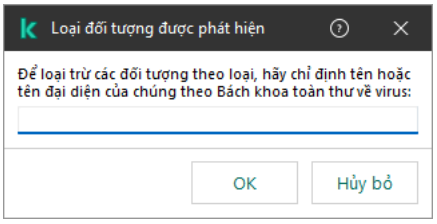
b. Nếu cần, hãy tắt chức năng **Bao gồm các thư mục con**. Nếu chức năng này được bật, ứng dụng sẽ không quét các tập tin trong tất cả các thư mục con. Nếu chức năng này bị tắt, ứng dụng chỉ loại trừ thư mục đã chọn khỏi phạm vi quét. Tùy chọn này được bật theo mặc định.

c. Lưu các thay đổi của bạn.

10. Để loại trừ các đối tượng có tên cụ thể khỏi tác vụ quét:

    a. Trong mục **Thuộc tính**, hãy chọn hộp kiểm **Loại đối tượng được phát hiện**.

    b. Nhấn vào liên kết trong mục bên dưới để mở cửa sổ **Loại đối tượng được phát hiện**.



Chọn đối tượng

    a. 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.

    b. Lưu các thay đổi của bạn.

11. 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 trong mục bên dưới để mở cửa sổ **Mã Hash đối tượng**.



Chọn tập tin

    a. Nhập giá trị băm của tập tin hoặc chọn tập tin bằng cách nhấn vào nút **Duyệt**.

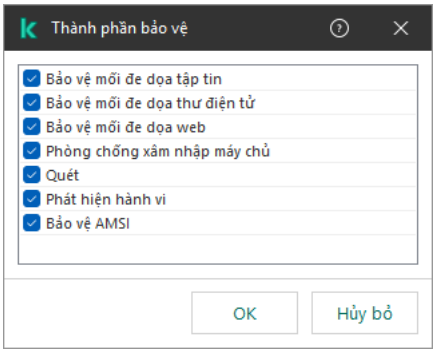
    Nếu tập tin bị sửa đổi, giá trị băm của tập tin cũng sẽ được sửa đổi. Nếu điều này xảy ra, tập tin bị sửa đổi sẽ không được thêm vào loại trừ.

    b. Lưu các thay đổi của bạn.

12. Nếu cần thiết, trong trường **Bình luận**, nhập một nhận xét ngắn về loại trừ quét mà bạn đang tạo.

13. Quy định thành phần Kaspersky Endpoint Security nên sử dụng loại trừ quét:

    a. Nhấn vào liên kết trong mục bên dưới để mở cửa sổ **Thành phần bảo vệ**.



Chọn các thành phần bảo vệ

    a. Chọn hộp kiểm đối diện các thành phần mà quy tắc loại trừ quét nên được áp dụng.

    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.

14. Nhấn vào **OK**.

    Loại trừ mới sẽ được thêm vào danh sách. Bạn có thể tắt loại trừ bất kỳ lúc nào bằng cách sử dụng hộp kiểm bên cạnh đối tượng.

15. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách tạo loại trừ quét trong Bảng điều khiển web Kaspersky Security Center

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.

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 **Trusted Zone**.

5. Trong cửa sổ mở ra, hãy nhấn vào liên kết **Malware 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 exclusions** 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. Ngoài ra, nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ ẩn danh sách tổng hợp các loại trừ quét trong giao diện người dùng của ứng dụng.

8. Nhấn vào **Add** và chọn một hành động:

   - **Category**. Bạn có thể nhóm các loại trừ quét thành các danh mục riêng biệt. Để tạo một danh mục mới, hãy nhập tên danh mục và thêm ít nhất một loại trừ quét vào danh mục đó.

   - **New exclusion**. Kaspersky Endpoint Security sẽ thêm một loại trừ quét mới vào gốc của danh sách.

   - **Select exclusion from list**. Để nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager, ứng dụng bao gồm *loại trừ quét được xác định trước*. Ngoài ra, các loại trừ quét được định sẵn cũng đã được thêm vào để hỗ trợ thiết lập ứng dụng trong môi trường ảo Citrix và VMware. Bạn phải chọn loại trừ quét được xác định trước tùy thuộc vào mục đích của máy chủ được bảo vệ.

   Để thêm một loại trừ quét mới vào một danh mục cụ thể, hãy chọn hộp kiểm bên cạnh danh mục đó và chọn tùy chọn **New exclusion**.

9. Chọn cách bạn muốn thêm loại trừ: **Path to the file or folder**, **Object type** hoặc **Object hash**.

10. Để loại trừ một tập tin hoặc thư mục khỏi tác vụ quét, hãy 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:

    - 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 cấp 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 sử dụng tên đại diện ở đầu, ở giữa hoặc ở cuối đường dẫn tập tin. Ví dụ: nếu bạn muốn thêm một thư mục cho tất cả người dùng để loại trừ, hãy nhập tên đại diện `?:\Users\*\Folder\`.

      Bạn có thể loại trừ các thư mục mạng. Để thực hiện, hãy nhập đường dẫn đến thư mục mạng theo cách thủ công (ví dụ: `\\Network Share\*`).

11. Nếu bạn muốn loại trừ một loại đối tượng cụ thể khỏi tác vụ quét, trong trường **Object type**, 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 **Apply exclusion to**, 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. Nhấn vào **OK**.

    Loại trừ mới sẽ được thêm vào danh sách. Bạn có thể sử dụng nút bật/tắt để dừng một loại trừ bất kỳ lúc nào.

16. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

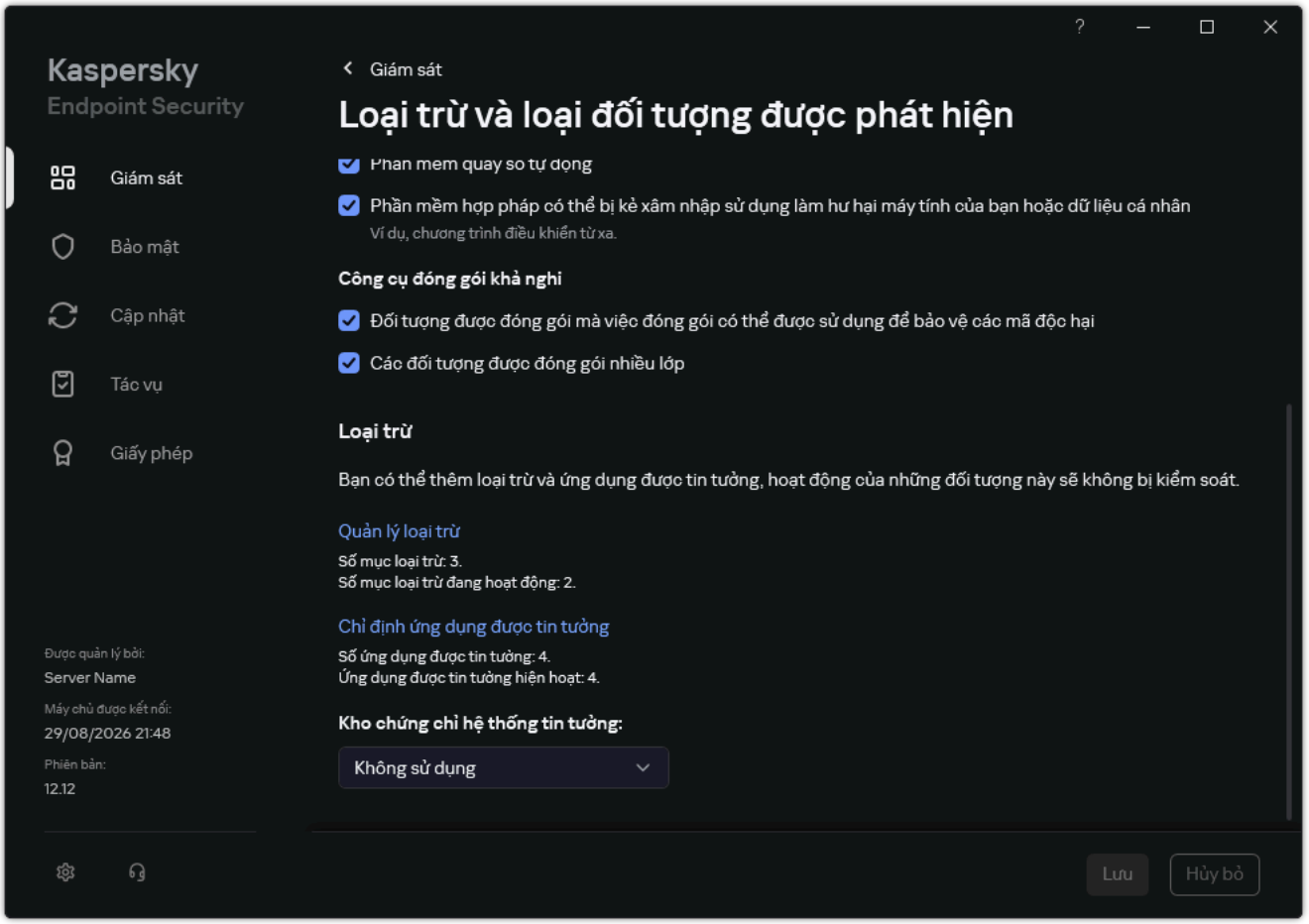
Cách tạo loại trừ quét trong giao diện ứng dụng

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**.

> Kaspersky Endpoint Security ẩn danh sách loại trừ quét trong giao diện người dùng của ứng dụng nếu cấu hình loại trừ quét bị quản trị viên chặn trong bảng điều khiển (biểu tượng "ổ khóa đóng") và loại trừ quét cục bộ bị cấm (hộp kiểm **Cho phép sử dụng các loại trừ cục bộ** bị xóa).



Cấu hình loại trừ

4. Nhấn vào **Thêm** và chọn một hành động:

   - **Danh mục**. Bạn có thể nhóm các loại trừ quét thành các danh mục riêng biệt. Để tạo một danh mục mới, hãy nhập tên danh mục và thêm ít nhất một loại trừ quét vào danh mục đó.
   - **Loại trừ mới**. Kaspersky Endpoint Security sẽ thêm một loại trừ quét mới vào gốc của danh sách.
   - **Chọn loại trừ trong danh sách**. Để nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager, ứng dụng bao gồm *loại trừ quét được xác định trước*. Ngoài ra, các loại trừ quét được định sẵn cũng đã được thêm vào để hỗ trợ thiết lập ứng dụng trong môi trường ảo Citrix và VMware. Bạn phải chọn loại trừ quét được xác định trước tùy thuộc vào mục đích của máy chủ được bảo vệ.

   Để thêm một loại trừ quét mới vào một danh mục cụ thể, hãy chọn hộp kiểm bên cạnh danh mục đó và chọn tùy chọn **Loại trừ mới**.

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 này theo cách thủ công. Kaspersky Endpoint Security hỗ trợ các biến môi trường và 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 cấp 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 sử dụng tên đại diện ở đầu, ở giữa hoặc ở cuối đường dẫn tập tin. Ví dụ: nếu bạn muốn thêm một thư mục cho tất cả người dùng để loại trừ, hãy nhập tên đại diện `?:\Users\*\Folder\`.

     Bạn có thể loại trừ các thư mục mạng. Để thực hiện, hãy nhập đường dẫn đến thư mục mạng theo cách thủ công (ví dụ: `\\Network Share\*`).

6. Nếu bạn muốn loại trừ một loại đối tượng cụ thể khỏi tác vụ quét, trong trường **Loại đối tượng được phát hiện**, 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 **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 **Thành phần bảo vệ**, hãy chọn các thành phần mà bạn muốn áp dụng loại trừ quét.

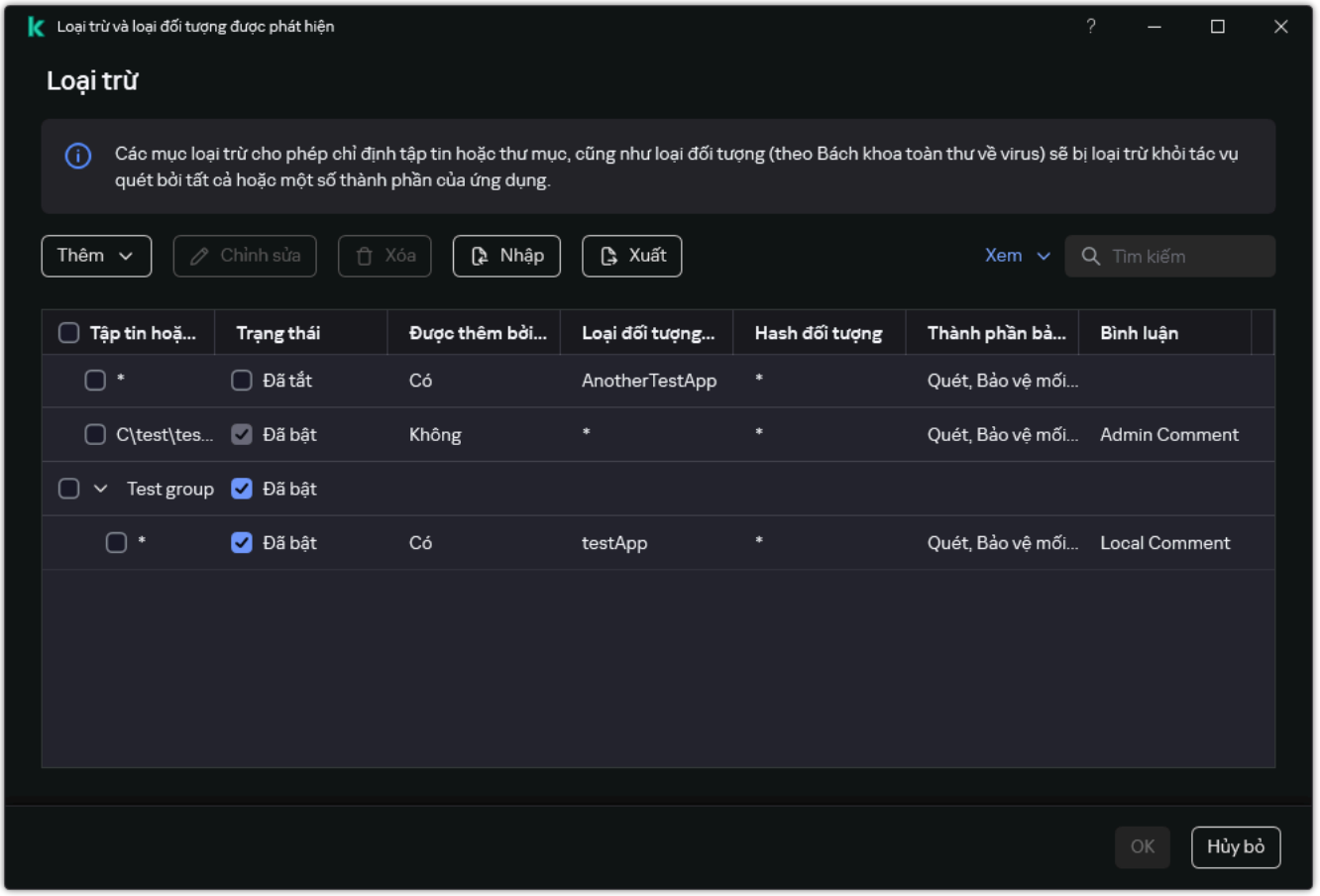
9. Nếu cần thiết, trong trường **Bình luận**, nhập một nhận xét ngắn về loại trừ quét mà bạn đang tạo.

10. Chọn trạng thái **Hoạt động** cho loại trừ.

11. Nhấn vào **Thêm**.

    Loại trừ mới sẽ được thêm vào danh sách. Bạn có thể tắt loại trừ bất kỳ lúc nào bằng cách sử dụng hộp kiểm trong cột **Trạng thái**.

12. Lưu các thay đổi của bạn.



Danh sách loại trừ

Ví dụ về tên đại diện đường dẫn:

Bạn nên chỉ định đường dẫn tương đối thay vì đường dẫn tuyệt đối. Làm vậy cho phép loại trừ không chỉ các đối tượng hệ thống tập tin mà còn cả các đối tượng không có tập tin. Ví dụ: `*\Program Files (x86)\Folder\Subfolder`.

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 trong `C:\dir\`, nhưng không có 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\`.
- Tên đại diện `C:\dir1\*\dir3\` sẽ bao gồm tất cả các đường dẫn đến tập tin trong thư mục con dir3 một cấp vào thư mục `C:\dir1\`.
- Tên đại diện `C:\dir1\**\dirN\` sẽ bao gồm tất cả các đường dẫn đến tập tin trong thư mục con dirN trong thư mục `C:\dir1\` ở bất kỳ cấp nào.

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.

Tạo ngoại lệ dựa trên loại đối tượng được phát hiện

Kaspersky Endpoint Security phân loại các đối tượng được phát hiện như sau:

- **Virus và sâu**

  Danh mục con: Virus và sâu (Viruses_and_Worms)

  Cấp độ nguy hiểm: 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 kịch bản* và *virus macro*.

Virus có thể lây nhiễm cho các tập tin sử dụng nhiều kỹ thuật khác nhau. *Overwriting* 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. *Parasitic* virus sẽ sửa nội dung tập tin, để chúng vận hành toàn bộ hoặc một phần chức năng. *Companion* 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 Link*, *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	Name	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 tin nhanh	Chúng được phát tán qua các ứng dụng nhắn 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 Internet Relay Chats, 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 gẫu 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.

Loại	Name	Mô tả
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: • 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

  Cấp độ nguy hiểm: 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	Name	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: • **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.

Loại	Name	Mô tả
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 bảng 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: • 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	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. 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).
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 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). 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. 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.
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.

Loại	Name	Mô tả
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	Name	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	*Mã khai thác* 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". 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. 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.
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 Tán gẫu 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.

Loại	Name	Mô tả
Spoofer	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 Spoofer 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

  Cấp độ nguy hiểm: 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: Phần mềm quay số tự động (Dialer).

  Cấp độ nguy hiểm: Trung bình

  Phần mềm quay số tự động có thể bí mật thiết lập kết nối điện thoại bằng modem.

- **Phần mềm hợp pháp có thể bị kẻ xâm nhập sử dụng làm hư hại máy tính của bạn hoặc dữ liệu cá nhân**

  Danh mục con: Các phần mềm hợp pháp có thể được sử dụng bởi kẻ xâm nhập để gây tổn hại cho 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	Name	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 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 ngầm 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 ngầm 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 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**

  Danh mục con: Các tập tin được đóng gói có thể gây hại.

  Cấp độ nguy hiểm: Trung bình.

  Tập tin được đóng gói bằng một trình đóng gói đặc biệt, dùng để đóng gói phần mềm độc hại: virus, sâu, Trojan. Kaspersky Endpoint Security sẽ quét mô-đun giải nén trong các tập nén SFX (tự động giải nén).

  Để ẩn phần mềm độc hại khỏi sự phát hiện của phần mềm diệt virus, tin tặc đóng gói phần mềm đó bằng các trình đóng gói đặc biệt. Chuyên gia của Kaspersky đã xác định các trình nén phổ biến nhất trong giới tin tặc.

- **Các đối tượng được đóng gói nhiều lớp**

  Danh mục con: Tập tin được đóng gói nhiều lớp.

  Cấp độ nguy hiểm: Trung bình.

  Tập tin được đóng gói bằng một hoặc nhiều trình đóng gói từ ba lần trở lên.

  Để ẩn phần mềm độc hại trước sự phát hiện của phần mềm diệt virus, tin tặc có thể đóng gói một tập tin nhiều lớp. Kaspersky Endpoint Security sẽ quét các tập tin được đóng gói.

Theo mặc định, Kaspersky Endpoint Security sẽ phát hiện tất cả các loại đối tượng. Bạn nên bật tính năng phát hiện tất cả các loại đối tượng để tăng cường bảo mật cho máy tính. Nếu đang sử dụng các tiện ích nội bộ mà ứng dụng phát hiện là độc hại, hãy thêm các tiện ích này vào danh sách loại trừ, nhưng không được vô hiệu hóa việc phát hiện toàn bộ loại đối tượng.

Cách chọn các loại đối tượng có thể được phát hiện trong Bảng điều khiển quản trị (MMC)

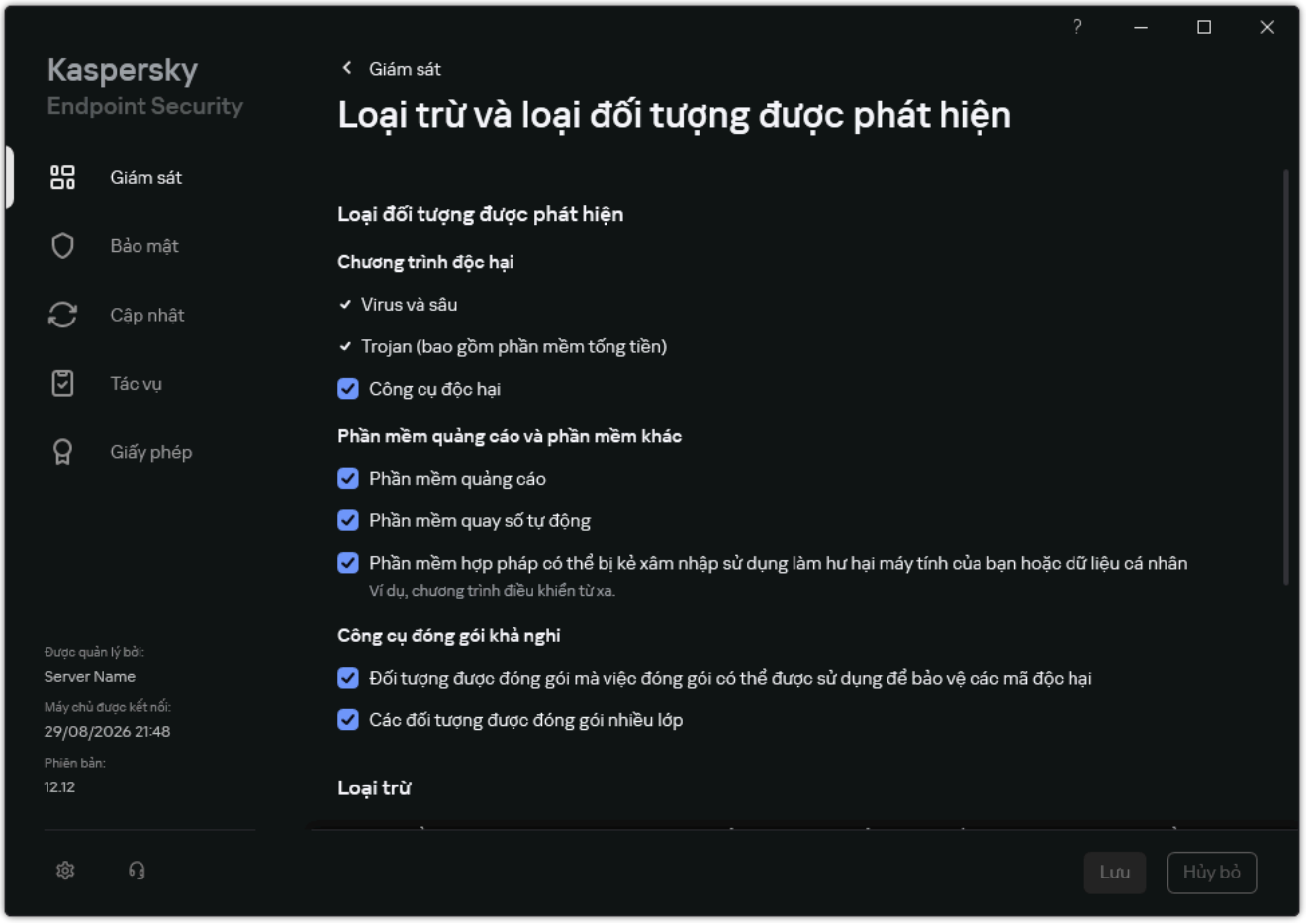
1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Loại trừ và loại đối tượng**.
5. Trong mục **Loại đối tượng được phát hiện**, hãy nhấn nút **Thiết lập**.
6. Trong cửa sổ mở ra, hãy chọn hộp kiểm đối diện các loại đối tượng mà bạn muốn Kaspersky Endpoint Security phát hiện.
7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách chọn các loại đối tượng có thể phát hiện được trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management → Policies**.
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 → Detection Settings**.
5. Trong mục **Detection of other types of objects**, hãy chọn hộp kiểm đối diện các loại đối tượng mà bạn muốn Kaspersky Endpoint Security phát hiện.
6. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách chọn các loại đối tượng có thể phát hiện được 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 đối tượng được phát hiện**, hãy chọn hộp kiểm đối diện các loại đối tượng mà bạn muốn Kaspersky Endpoint Security phát hiện.
4. Lưu các thay đổi của bạn.



Các loại đối tượng có thể phát hiện

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 giám sát 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. Sau khi một ứng dụng được thêm vào danh sách các ứng dụng được tin tưởng, Kaspersky Endpoint Security sẽ ngừng giám sát hoạt động của ứng dụng đó.

Sự khác nhau giữa loại trừ quét và ứng dụng được tin tưởng là đối với loại trừ, Kaspersky Endpoint Security sẽ không quét các tập tin, trong khi đối với ứng dụng được tin tưởng thì ứng dụng không kiểm soát các tiến trình được khởi chạy. Nếu một ứng dụng được tin tưởng tạo một tập tin độc hại trong thư mục không có trong loại trừ quét thì Kaspersky Endpoint Security sẽ phát hiện tập tin đó và loại bỏ mối đe dọa. Nếu thư mục đó được thêm vào loại trừ thì Kaspersky Endpoint Security sẽ bỏ qua tập tin này.

Ví dụ: nếu bạn coi các đối tượng được sử dụng bởi ứng dụng Microsoft Windows Notepad là các đối tượng an toàn, có nghĩa là bạn tin tưởng ứng dụng này thì bạn có thể thêm Microsoft Windows Notepad vào danh sách các ứng dụng được tin tưởng để các đối tượng được sử dụng bởi ứng dụng này sẽ không bị giám sát. Làm vậy sẽ tăng hiệu năng máy tính, điều này đặc biệt quan trọng khi sử dụng các ứng dụng máy chủ.

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.

Các ứng dụng được tin tưởng sẽ giúp tránh các sự cố tương thích giữa Kaspersky Endpoint Security và các ứng dụng khác (ví dụ: sự cố quét hai lần lưu lượng mạng của một máy tính bên thứ ba bởi Kaspersky Endpoint Security và bởi một ứng dụng chống virus khác).

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 cây bảng điều khiển, hãy chọn **Policies**.

3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

4. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Loại trừ và loại đối tượng**.

5. Trong mục **Loại trừ quét và ứng dụng được tin tưởng → Ứng dụng được tin tưởng**, hãy nhấn nút **Thiết lập**.

   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. Ngoài ra, nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ ẩn danh sách tổng hợp các ứng dụng được tin tưởng trong giao diện người dùng của ứng dụng.

8. Nhấn vào **Thêm** và chọn một hành động:

- **Danh mục**. Bạn có thể nhóm các ứng dụng được tin tưởng thành các danh mục riêng biệt. Để tạo một danh mục mới, hãy nhập tên danh mục và thêm ít nhất một ứng dụng được tin tưởng vào danh mục đó.
- **Loại trừ mới**. Kaspersky Endpoint Security sẽ thêm một ứng dụng được tin tưởng mới vào gốc của danh sách.
- **Chọn loại trừ trong danh sách**. Để nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager, ứng dụng bao gồm *các ứng dụng được tin tưởng được xác định trước*. Ngoài ra, các ứng dụng được tin tưởng được định sẵn cũng đã được thêm vào để hỗ trợ thiết lập ứng dụng trong môi trường ảo Citrix và VMware. Bạn phải chọn các ứng dụng được tin tưởng được xác định trước tùy thuộc vào mục đích của máy chủ được bảo vệ.
- **Mục loại trừ mới cho danh mục đã chọn**. Hãy chọn một danh mục để thêm một ứng dụng được tin tưởng mới vào một danh mục cụ thể.

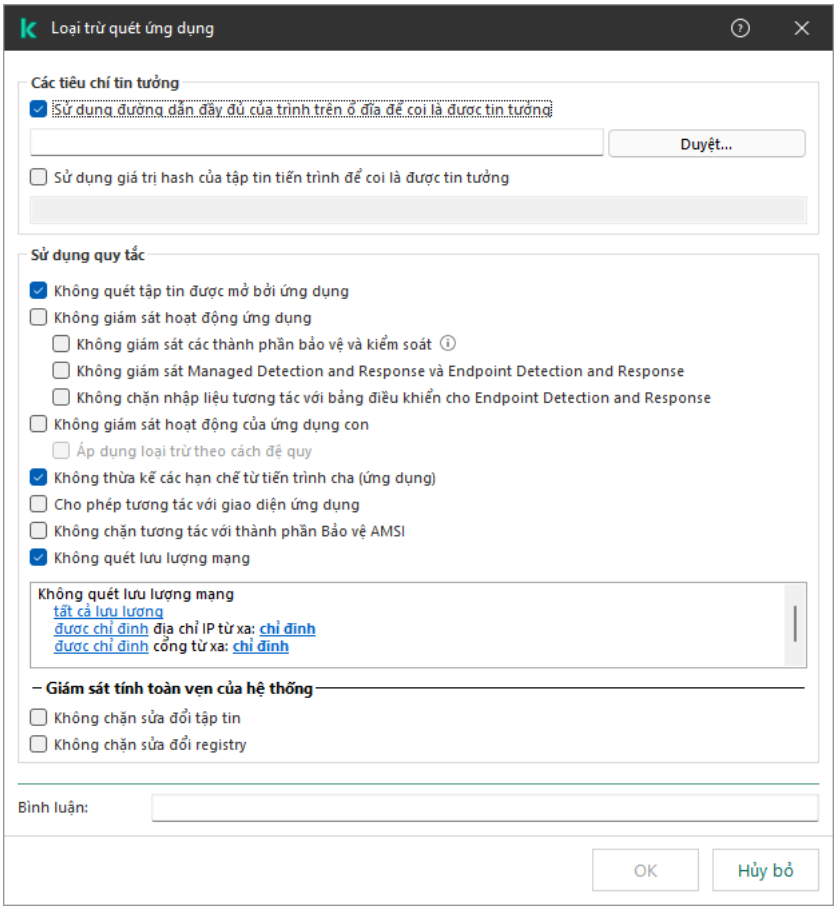
9. Chọn các tiêu chí tin cậy:

- **Sử dụng đường dẫn đầy đủ của trình trên ổ đĩa để coi là được tin tưởng**. Nhập đường dẫn đến tập tin thực thi của ứng dụng tin tưởng.

  Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện.

  Kaspersky Endpoint Security phân biệt chữ hoa và chữ thường trong tên tập tin của ứng dụng được tin tưởng. Nếu tên tập tin bạn nhập không đúng chữ hoa và chữ thường, Kaspersky Endpoint Security sẽ không nhận dạng được ứng dụng được tin tưởng.
- **Sử dụng giá trị hash của tập tin tiến trình để coi là được tin tưởng**.

Kaspersky Endpoint Security không hỗ trợ biến môi trường `%userprofile%` khi tạo một danh sách các ứng dụng được tin tưởng trong 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.



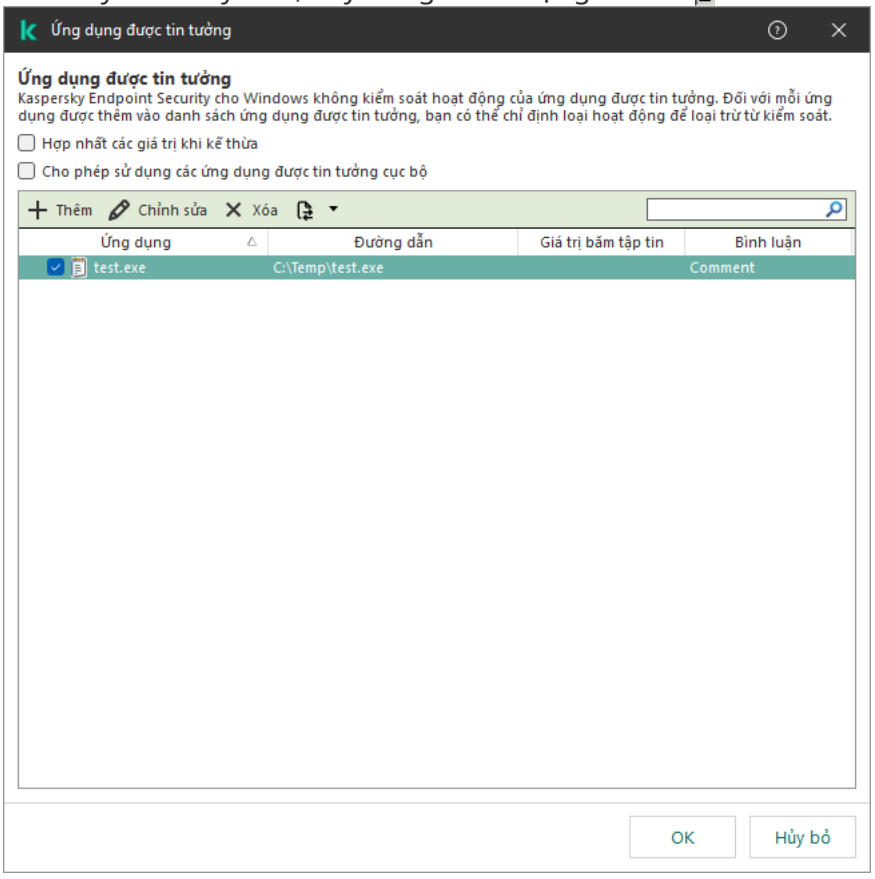
Thiết lập ứng dụng được tin tưởng

10. Cấu hình thiết lập nâng cao cho ứng dụng được tin tưởng (xem bảng bên dưới).

11. Nhấn vào **OK**.

    Ứng dụng được tin tưởng mới sẽ được thêm vào danh sách. Bạn có thể loại trừ một ứng dụng khỏi vùng được tin tưởng bất kỳ lúc nào bằng cách sử dụng hộp kiểm bên cạnh đối tượng.

12. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.



Danh sách các ứng dụng được tin tưởng

Cách thêm một ứng dụng vào danh sách được tin tưởng trong Bảng điều khiển web Kaspersky Security Center

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.
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 **Trusted Zone**.
5. Trong cửa sổ mở ra, hãy nhấn vào liên kết **Applications**.

   Thao tác này sẽ mở cửa sổ chứa danh sách các ứng dụng được tin tưởng.
6. Chọn hộp kiểm **Merge values when inheriting** 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 **Allow use of local exclusions** 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. Ngoài ra, nếu hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ ẩn danh sách tổng hợp các ứng dụng được tin tưởng trong giao diện người dùng của ứng dụng.

8. Nhấn vào **Add** và chọn một hành động:

   - **Category**. Bạn có thể nhóm các ứng dụng được tin tưởng thành các danh mục riêng biệt. Để tạo một danh mục mới, hãy nhập tên danh mục và thêm ít nhất một ứng dụng được tin tưởng vào danh mục đó.
   - **New exclusion**. Kaspersky Endpoint Security sẽ thêm một ứng dụng được tin tưởng mới vào gốc của danh sách.
   - **Select exclusion from list**. Để nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager, ứng dụng bao gồm *các ứng dụng được tin tưởng được xác định trước*. Ngoài ra, các ứng dụng được tin tưởng được định sẵn cũng đã được thêm vào để hỗ trợ thiết lập ứng dụng trong môi trường ảo Citrix và VMware. Bạn phải chọn các ứng dụng được tin tưởng được xác định trước tùy thuộc vào mục đích của máy chủ được bảo vệ.

   Để thêm một ứng dụng được tin tưởng mới vào một danh mục cụ thể, hãy chọn hộp kiểm bên cạnh danh mục đó và chọn tùy chọn **New exclusion**.

9. Chọn các tiêu chí tin cậy:

   - **Path to the file or folder**. Nhập đường dẫn đến tập tin thực thi của ứng dụng tin tưởng.

     Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện.

     Kaspersky Endpoint Security phân biệt chữ hoa và chữ thường trong tên tập tin của ứng dụng được tin tưởng. Nếu tên tập tin bạn nhập không đúng chữ hoa và chữ thường, Kaspersky Endpoint Security sẽ không nhận dạng được ứng dụng được tin tưởng.

   - **Application hash**.

   > Kaspersky Endpoint Security không hỗ trợ biến môi trường %userprofile% khi tạo một danh sách các ứng dụng được tin tưởng trong 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. Nhấn vào **OK**.

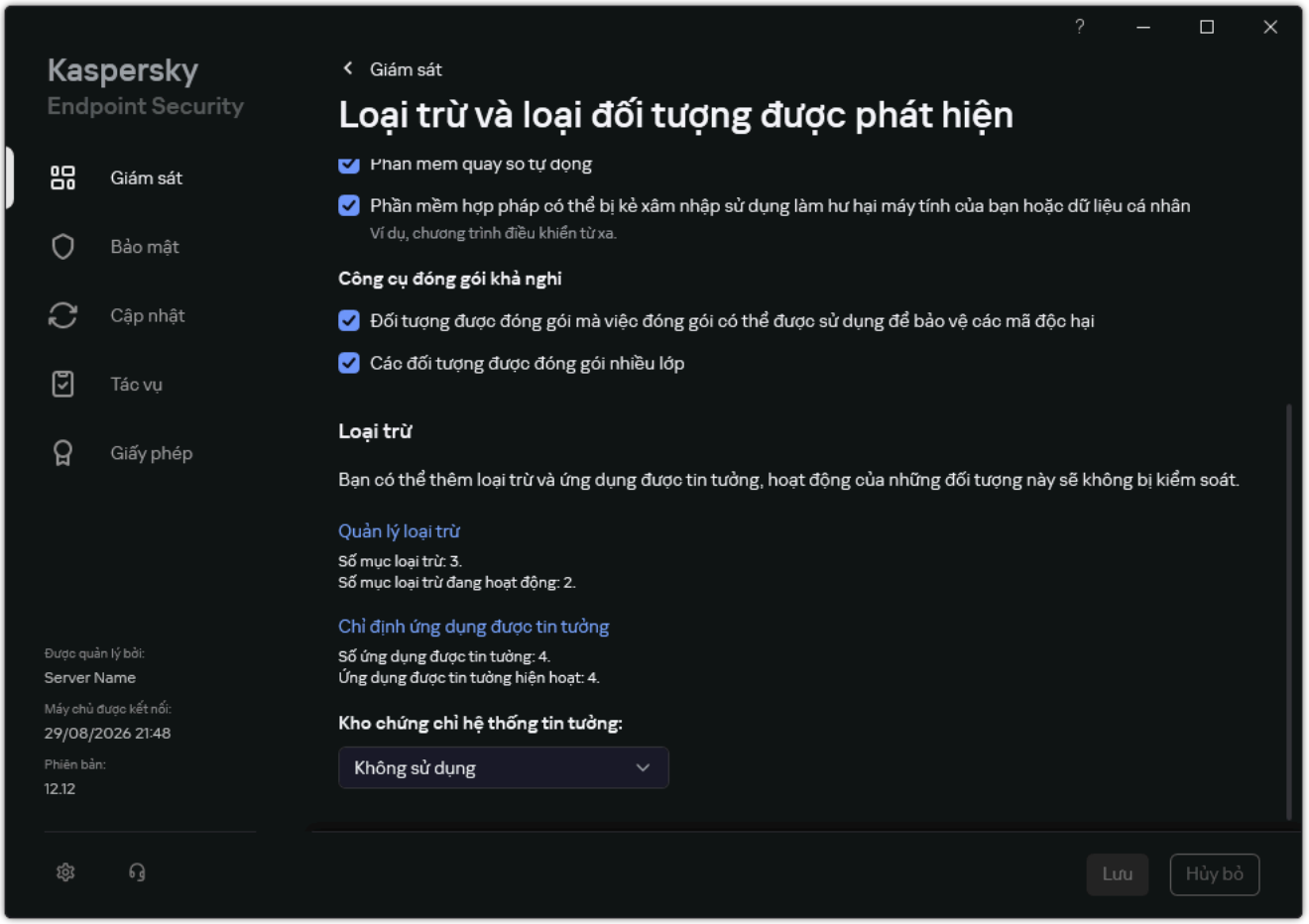
    Ứng dụng được tin tưởng mới sẽ được thêm vào danh sách. Bạn có thể loại trừ một ứng dụng khỏi vùng được tin tưởng bất cứ lúc nào bằng cách sử dụng hộp kiểm trong cột **Status**.

12. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và 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 → Loại trừ và loại đối tượng được phát hiện**.
3. Trong mục **Loại trừ**, hãy nhấn liên kết **Chỉ định ứng dụng được tin tưởng**.

Kaspersky Endpoint Security ẩn danh sách tổng hợp các ứng dụng được tin tưởng trong giao diện người dùng của ứng dụng nếu cấu hình của các ứng dụng được tin tưởng bị quản trị viên chặn trong bảng điều khiển (biểu tượng "ổ khóa đóng") và các ứng dụng được tin tưởng cục bộ bị cấm (hộp kiểm **Cho phép sử dụng các ứng dụng được tin tưởng cục bộ** bị xóa).



Cấu hình loại trừ

4. Nhấn vào **Thêm** và chọn một hành động:

   - **Danh mục**. Bạn có thể nhóm các ứng dụng được tin tưởng thành các danh mục riêng biệt. Để tạo một danh mục mới, hãy nhập tên danh mục và thêm ít nhất một ứng dụng được tin tưởng vào danh mục đó.
   - **Loại trừ mới**. Kaspersky Endpoint Security sẽ thêm một ứng dụng được tin tưởng mới vào gốc của danh sách.
   - **Chọn loại trừ trong danh sách**. Để nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager, ứng dụng bao gồm *các ứng dụng được tin tưởng được xác định trước*. Ngoài ra, các ứng dụng được tin tưởng được định sẵn cũng đã được thêm vào để hỗ trợ thiết lập ứng dụng trong môi trường ảo Citrix và VMware. Bạn phải chọn các ứng dụng được tin tưởng được xác định trước tùy thuộc vào mục đích của máy chủ được bảo vệ.

   Để thêm một ứng dụng được tin tưởng mới vào một danh mục cụ thể, hãy chọn hộp kiểm bên cạnh danh mục đó và chọn tùy chọn **Loại trừ mới**.

5. Chọn các tiêu chí tin cậy:

   - **Sử dụng đường dẫn đầy đủ của tiến trình trên ổ đĩa để coi là được tin tưởng**. Nhập đường dẫn đến tập tin thực thi của ứng dụng tin tưởng.

     Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện.

     Kaspersky Endpoint Security phân biệt chữ hoa và chữ thường trong tên tập tin của ứng dụng được tin tưởng. Nếu tên tập tin bạn nhập không đúng chữ hoa và chữ thường, Kaspersky Endpoint Security sẽ không nhận dạng được ứng dụng được tin tưởng.

   - **Sử dụng giá trị hash của tập tin tiến trình để coi là được tin tưởng**.

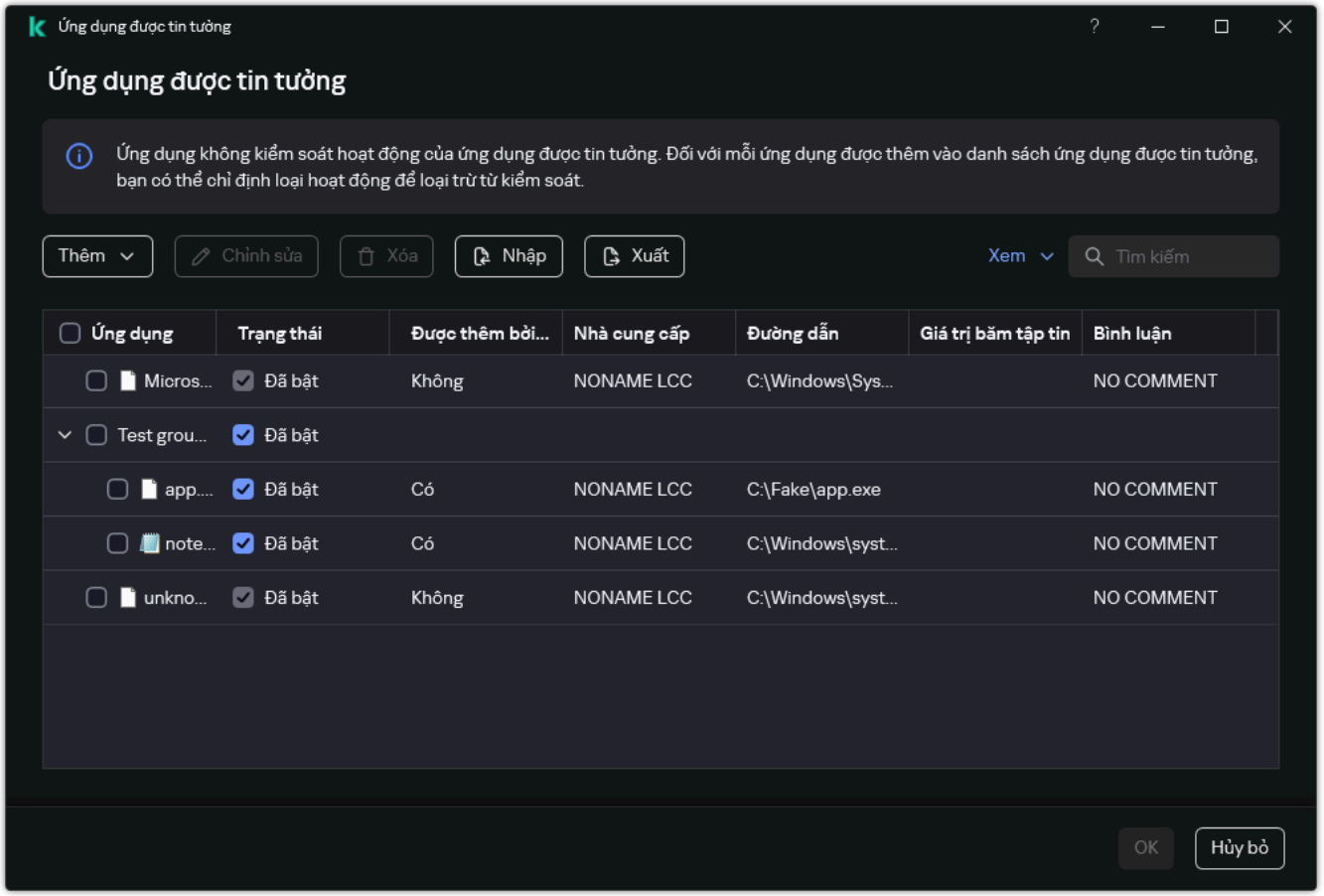
   Kaspersky Endpoint Security hỗ trợ các biến môi trường và chuyển đổi đường dẫn trong giao diện cục bộ của ứng dụng. Nói cách khác, nếu bạn nhập đường dẫn tập tin `%userprofile%\Documents\File.exe` thì một bản ghi `C:\Users\Fred123\Documents\File.exe` sẽ được thêm vào giao diện cục bộ của ứng dụng cho 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.

7. Nhấn vào **OK**.

   Ứng dụng được tin tưởng mới sẽ được thêm vào danh sách. Bạn có thể loại trừ một ứng dụng khỏi vùng được tin tưởng bất cứ lúc nào bằng cách sử dụng hộp kiểm trong cột **Trạng thái**.

8. Lưu các thay đổi của bạn.



Danh sách các ứng dụng được tin tưởng

Thiết lập ứng dụng được tin tưởng

Tham số	Mô tả
Không quét tập tin được mở bởi ứng dụng	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. Bạn có thể cấu hình giám sát hoạt động ứng dụng cho các thành phần khác nhau của Kaspersky Endpoint Security: • **Không giám sát các thành phần bảo vệ và kiểm soát**. 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 giám sát Managed Detection and Response và Endpoint Detection and Response**. Hoạt động của ứng dụng được giám sát bởi tác nhân MDR tích hợp và tác nhân EDR (KATA) tích hợp. • **Không chặn nhập liệu tương tác với bảng điều khiển cho Endpoint Detection and Response**. Kaspersky Endpoint Security không gửi dữ liệu đo lường từ xa về việc quản lý ứng dụng trên bảng điều khiển. Dữ liệu đo lường từ xa được sử dụng bởi Kaspersky Anti Targeted Attack Platform (EDR).
Không giám sát hoạt động ứng dụng của trẻ	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. Bạn có thể áp dụng loại trừ theo cách đệ quy. Để ứng dụng không giám sát hoạt động của toàn bộ chuỗi ứng dụng con.
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 ứng dụng của trẻ	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. Bạn có thể áp dụng loại trừ theo cách đệ quy. Để ứng dụng không giám sát hoạt động của toàn bộ chuỗi 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 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.

Tham số	Mô tả
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. Kaspersky Endpoint Security phiên bản 14.0 trở về sau không hỗ trợ loại trừ lưu lượng mạng nếu giá trị hash được chỉ định cho một ứng dụng tin tưởng thay vì đường dẫn.
Không chặn sửa đổi tập tin *(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)*	Kaspersky Endpoint Security không giám sát các thay đổi trong các tập tin từ phạm vi giám sát Giám sát tính toàn vẹn của hệ thống. Ứng dụng này áp dụng loại trừ cho tất cả các chế độ Giám sát tính toàn vẹn của hệ thống: Giám sát tính toàn vẹn của hệ thống theo thời gian thực và Kiểm tra tính toàn vẹn của hệ thống theo yêu cầu.
Không chặn sửa đổi registry *(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)*	Kaspersky Endpoint Security không giám sát các thay đổi trong khóa registry từ phạm vi giám sát Giám sát tính toàn vẹn của hệ thống. Ứng dụng này áp dụng loại trừ cho tất cả các chế độ Giám sát tính toàn vẹn của hệ thống: Giám sát tính toàn vẹn của hệ thống theo thời gian thực và Kiểm tra tính toàn vẹn của hệ thống theo yêu cầu.
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: • 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.

Tạo vùng cục bộ được tin tưởng

Bây giờ người dùng có thể tạo vùng cục bộ được tin tưởng của riêng mình cho một máy tính cụ thể. Nhờ vậy, người dùng đó 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 trong thiết lập chính sách. Để thực hiện, hãy sử dụng các hộp kiểm **Cho phép sử dụng các loại trừ cục bộ** và **Cho phép sử dụng các ứng dụng được tin tưởng cục bộ** trong phần chính sách **Loại trừ**.

Nếu quản trị viên cho phép tạo vùng cục bộ được tin tưởng thì người dùng có thể thêm loại trừ quét của riêng họ và ứng dụng được tin tưởng trong giao diện người dùng của ứng dụng. Đồng thời, người dùng không có quyền sửa đổi hoặc xóa các đối tượng khỏi vùng được tin tưởng được cấu hình trong chính sách. Quản trị viên cũng có thể xem, thêm, sửa đổi hoặc xóa các mục danh sách trong bảng điều khiển Kaspersky Security Center nếu cần thêm các tùy chọn loại trừ cho một máy tính riêng rẽ.

Kaspersky Endpoint Security sẽ ẩn danh sách các loại trừ quét và ứng dụng được tin tưởng trong giao diện người dùng của ứng dụng nếu cấu hình của vùng tin tưởng bị quản trị viên chặn trong bảng điều khiển (biểu tượng "ổ khóa đóng") và các loại trừ quét cục bộ và các ứng dụng được tin tưởng bị cấm.

Cách thêm đối tượng vào vùng cục bộ 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, hãy chọn thẻ **Devices**.

4. Nhấn đúp để mở cửa sổ thuộc tính máy tính.

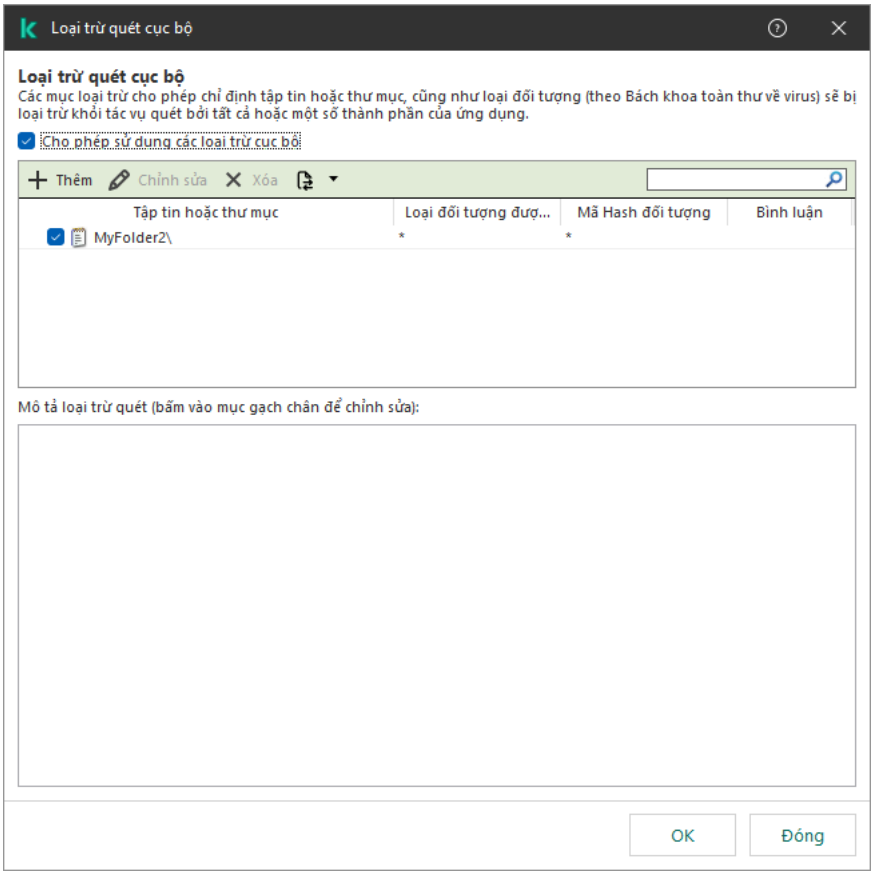
5. Trong cửa sổ thuộc tính máy tính, chọn phần **Applications**.

6. Trong danh sách các ứng dụng Kaspersky được cài đặt trên máy tính, hãy chọn **Kaspersky Endpoint Security cho Windows (14.2)** và nhấn đúp để mở thuộc tính ứng dụng.

7. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát → Loại trừ và loại đối tượng**.

8. Trong mục **Loại trừ quét và ứng dụng được tin tưởng → Loại trừ quét cục bộ**, hãy nhấn nút **Thiết lập**.

   Thao tác này sẽ mở cửa sổ chứa danh sách các loại trừ cục bộ.



Thiết lập khu vực tin tưởng

9. Lập danh sách loại trừ quét cục bộ.

   Các quy tắc tạo loại trừ quét cục bộ cũng giống như đối với loại trừ thông thường. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện.

10. Trong mục **Loại trừ quét và ứng dụng được tin tưởng → Ứng dụng cục bộ được tin tưởng**, hãy nhấn nút **Thiết lập**.

    Thao tác này sẽ mở cửa sổ chứa danh sách các ứng dụng cục bộ được tin tưởng.

11. Lập danh sách các ứng dụng cục bộ được tin tưởng.

    Quy tắc thêm ứng dụng vào danh sách ứng dụng cục bộ được tin tưởng cũng giống như quy tắc quy tắc để thêm chúng vào danh sách chung. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự * cùng ? khi nhập tên đại diện.

12. Lưu các thay đổi của bạn.

Cách thêm đối tượng vào vùng cục bộ được tin tưởng trong Bảng điều khiển web Kaspersky Security Center

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Assets (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 **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. Trong cửa sổ thiết lập ứng dụng, hãy chọn **General settings** → **Exclusions and types of detected objects**.
7. Trong mục **Scan exclusions and trusted applications**, hãy nhấn liên kết **Local scan exclusions**.
8. Lập danh sách loại trừ quét cục bộ.

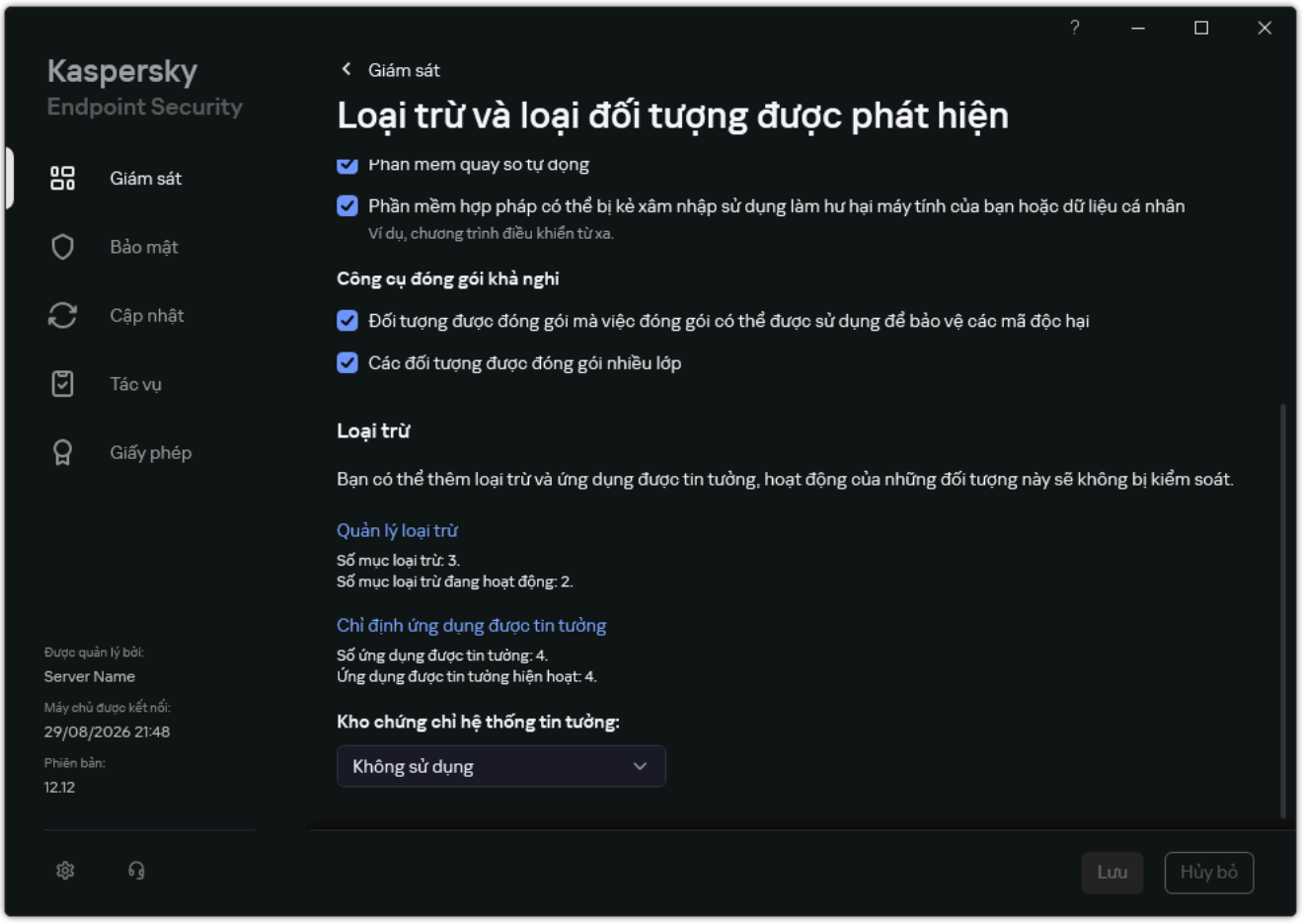
   Quy tắc để tạo loại trừ cục bộ cũng giống như quy tắc quy tắc tạo loại trừ thông thường. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự * cùng ? khi nhập tên đại diện.
9. Trong mục **Scan exclusions and trusted applications**, hãy nhấn liên kết **Local trusted applications**.
10. Lập danh sách các ứng dụng cục bộ được tin tưởng.

    Quy tắc thêm ứng dụng vào danh sách ứng dụng cục bộ được tin tưởng cũng giống như quy tắc quy tắc để thêm chúng vào danh sách chung. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện.
11. Lưu các thay đổi của bạn.

Cách tạo loại trừ quét cục bộ 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**.

Kaspersky Endpoint Security ẩn danh sách loại trừ quét trong giao diện người dùng của ứng dụng nếu cấu hình loại trừ quét bị quản trị viên chặn trong bảng điều khiển (biểu tượng "ổ khóa đóng") và loại trừ quét cục bộ bị cấm (hộp kiểm **Cho phép sử dụng các loại trừ cục bộ** bị xóa).



Cấu hình loại trừ

4. Nhấn vào **Thêm** và chọn một hành động:

   - **Danh mục**. Bạn có thể nhóm các loại trừ quét thành các danh mục riêng biệt. Để tạo một danh mục mới, hãy nhập tên danh mục và thêm ít nhất một loại trừ quét vào danh mục đó.
   - **Loại trừ mới**. Kaspersky Endpoint Security sẽ thêm một loại trừ quét mới vào gốc của danh sách.
   - **Chọn loại trừ trong danh sách**. Để nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager, ứng dụng bao gồm *loại trừ quét được xác định trước*. Ngoài ra, các loại trừ quét được định sẵn cũng đã được thêm vào để hỗ trợ thiết lập ứng dụng trong môi trường ảo Citrix và VMware. Bạn phải chọn loại trừ quét được xác định trước tùy thuộc vào mục đích của máy chủ được bảo vệ.

   Để thêm một loại trừ quét mới vào một danh mục cụ thể, hãy chọn hộp kiểm bên cạnh danh mục đó và chọn tùy chọn **Loại trừ mới**.

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 này theo cách thủ công. Kaspersky Endpoint Security hỗ trợ các biến môi trường và 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 cấp 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 sử dụng tên đại diện ở đầu, ở giữa hoặc ở cuối đường dẫn tập tin. Ví dụ: nếu bạn muốn thêm một thư mục cho tất cả người dùng để loại trừ, hãy nhập tên đại diện `?:\Users\*\Folder\`.

  Bạn có thể loại trừ các thư mục mạng. Để thực hiện, hãy nhập đường dẫn đến thư mục mạng theo cách thủ công (ví dụ: `\\Network Share\*`).

6. Nếu bạn muốn loại trừ một loại đối tượng cụ thể khỏi tác vụ quét, trong trường **Loại đối tượng được phát hiện**, 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 **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 **Thành phần bảo vệ**, hãy chọn các thành phần mà bạn muốn áp dụng loại trừ quét.

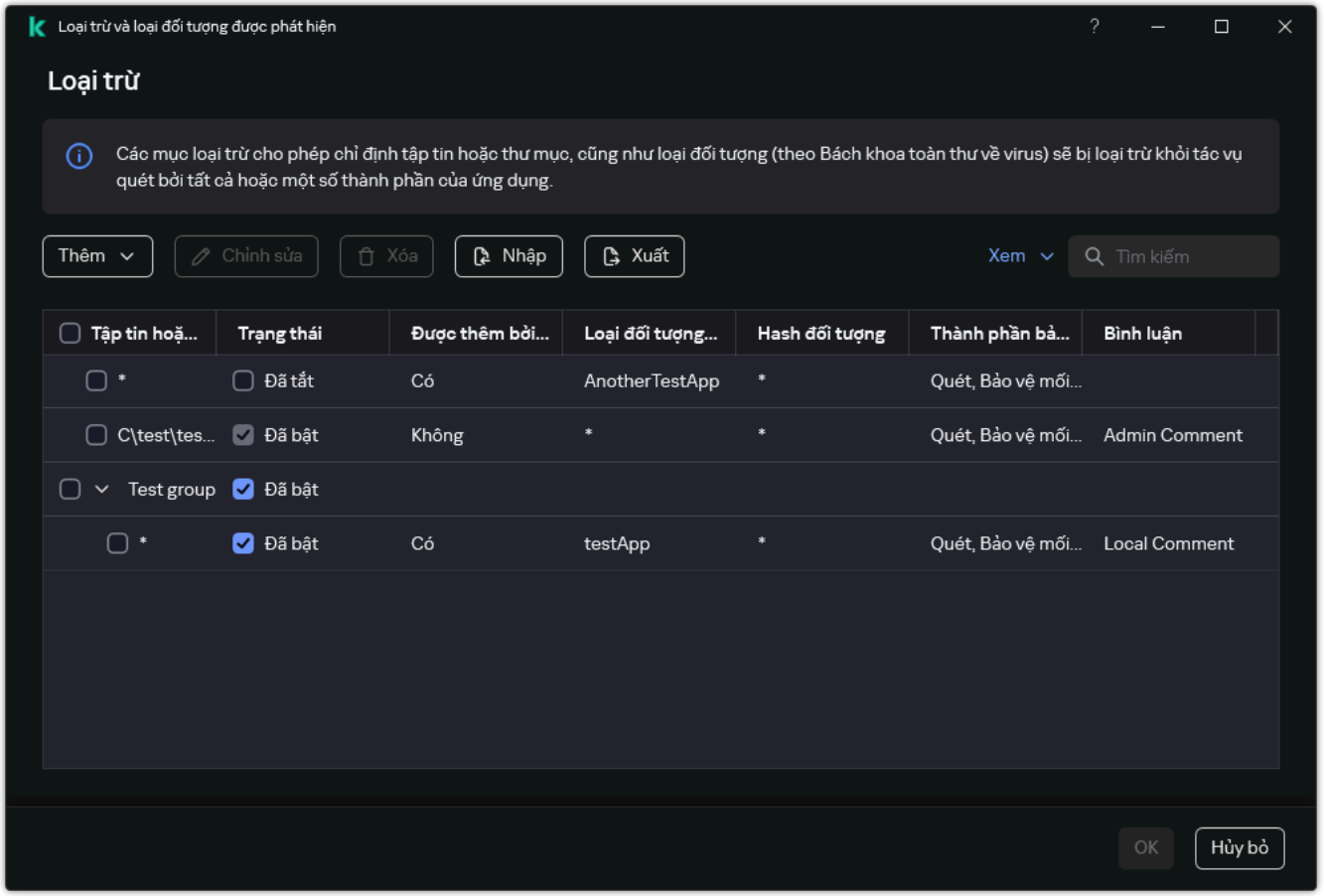
9. Nếu cần thiết, trong trường **Bình luận**, nhập một nhận xét ngắn về loại trừ quét mà bạn đang tạo.

10. Chọn trạng thái **Hoạt động** cho loại trừ.

11. Nhấn vào **Thêm**.

    Loại trừ mới sẽ được thêm vào danh sách. Bạn có thể tắt loại trừ bất kỳ lúc nào bằng cách sử dụng hộp kiểm trong cột **Trạng thái**.

12. Lưu các thay đổi của bạn.

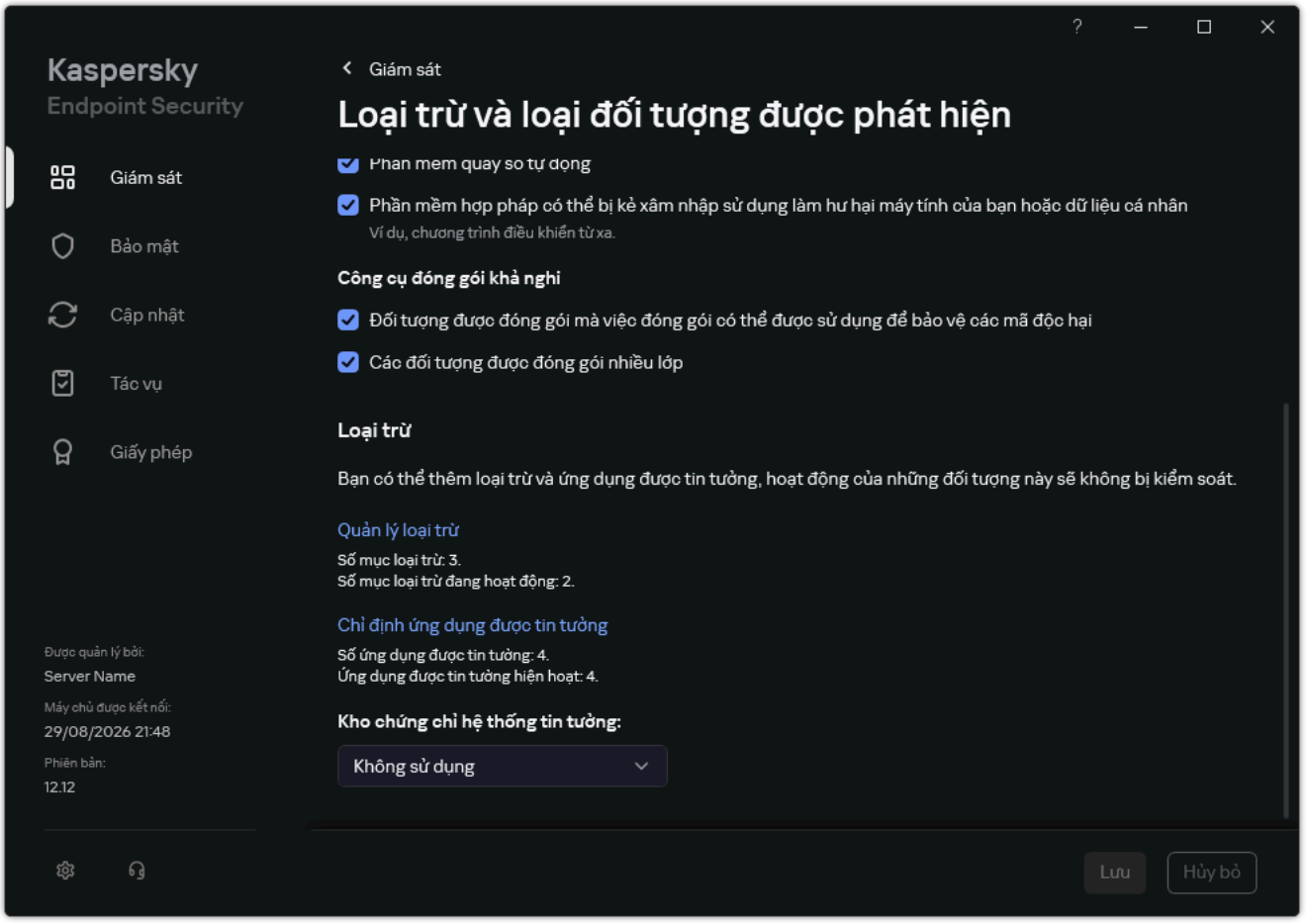


Danh sách loại trừ

Cách thêm một ứng dụng vào danh sách ứng dụng cục bộ 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 → Loại trừ và loại đối tượng được phát hiện**.
3. Trong mục **Loại trừ**, hãy nhấn liên kết **Chỉ định ứng dụng được tin tưởng**.

Kaspersky Endpoint Security ẩn danh sách tổng hợp các ứng dụng được tin tưởng trong giao diện người dùng của ứng dụng nếu cấu hình của các ứng dụng được tin tưởng bị quản trị viên chặn trong bảng điều khiển (biểu tượng "ổ khóa đóng") và các ứng dụng được tin tưởng cục bộ bị cấm (hộp kiểm **Cho phép sử dụng các ứng dụng được tin tưởng cục bộ** bị xóa).



Cấu hình loại trừ

4. Nhấn vào **Thêm** và chọn một hành động:

- **Danh mục**. Bạn có thể nhóm các ứng dụng được tin tưởng thành các danh mục riêng biệt. Để tạo một danh mục mới, hãy nhập tên danh mục và thêm ít nhất một ứng dụng được tin tưởng vào danh mục đó.
- **Loại trừ mới**. Kaspersky Endpoint Security sẽ thêm một ứng dụng được tin tưởng mới vào gốc của danh sách.
- **Chọn loại trừ trong danh sách**. Để nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager, ứng dụng bao gồm *các ứng dụng được tin tưởng được xác định trước*. Ngoài ra, các ứng dụng được tin tưởng được định sẵn cũng đã được thêm vào để hỗ trợ thiết lập ứng dụng trong môi trường ảo Citrix và VMware. Bạn phải chọn các ứng dụng được tin tưởng được xác định trước tùy thuộc vào mục đích của máy chủ được bảo vệ.

Để thêm một ứng dụng được tin tưởng mới vào một danh mục cụ thể, hãy chọn hộp kiểm bên cạnh danh mục đó và chọn tùy chọn **Loại trừ mới**.

5. Chọn các tiêu chí tin cậy:

- **Sử dụng đường dẫn đầy đủ của tiến trình trên ổ đĩa để coi là được tin tưởng**. Nhập đường dẫn đến tập tin thực thi của ứng dụng tin tưởng.

  Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện.

  Kaspersky Endpoint Security phân biệt chữ hoa và chữ thường trong tên tập tin của ứng dụng được tin tưởng. Nếu tên tập tin bạn nhập không đúng chữ hoa và chữ thường, Kaspersky Endpoint Security sẽ không nhận dạng được ứng dụng được tin tưởng.

- **Sử dụng giá trị hash của tập tin tiến trình để coi là được tin tưởng**.

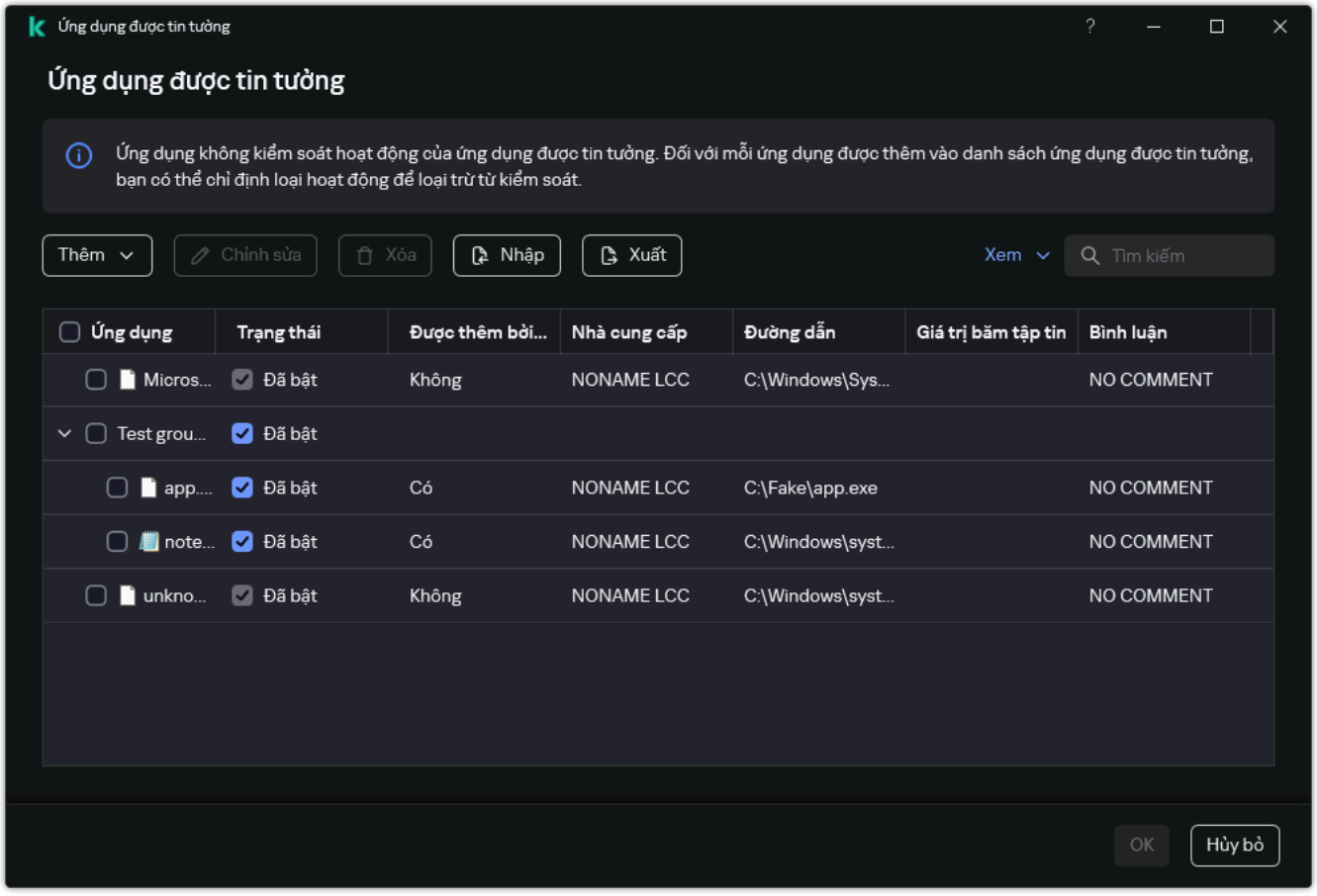
> Kaspersky Endpoint Security hỗ trợ các biến môi trường và chuyển đổi đường dẫn trong giao diện cục bộ của ứng dụng. Nói cách khác, nếu bạn nhập đường dẫn tập tin `%userprofile%\Documents\File.exe` thì một bản ghi `C:\Users\Fred123\Documents\File.exe` sẽ được thêm vào giao diện cục bộ của ứng dụng cho 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.

7. Nhấn vào **OK**.

   Ứng dụng được tin tưởng mới sẽ được thêm vào danh sách. Bạn có thể loại trừ một ứng dụng khỏi vùng được tin tưởng bất cứ lúc nào bằng cách sử dụng hộp kiểm trong cột **Trạng thái**.

8. Lưu các thay đổi của bạn.



Danh sách các ứng dụng được tin tưởng

Xuất và nhập vùng được 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. Vùng tin tưởng bao gồm các danh sách sau: *loại trừ quét* và *ứng dụng được tin tưởng*. Bạn có thể xuất các danh sách này sang tập tin XML và các định dạng khác. 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 và danh sách ứng dụng được tin tưởng, hoặc để chuyển danh sách sang máy chủ khác.

Ứng dụng sử dụng các định dạng sau để xuất và nhập *danh sách loại trừ*:

- XML khả dụng trong Bảng điều khiển quản trị (MMC), Bảng điều khiển web và Bảng điều khiển đám mây.
- DAT chỉ khả dụng để nhập trong Bảng điều khiển quản trị (MMC). Mục đích của định dạng này là để duy trì khả năng tương thích với các phiên bản cũ hơn của ứng dụng. Bạn có thể chuyển đổi tập tin DAT thành XML trong Bảng điều khiển quản trị (MMC) để di chuyển danh sách loại trừ sang Bảng điều khiển web.
- CSV chỉ khả dụng trong giao diện cục bộ của ứng dụng.

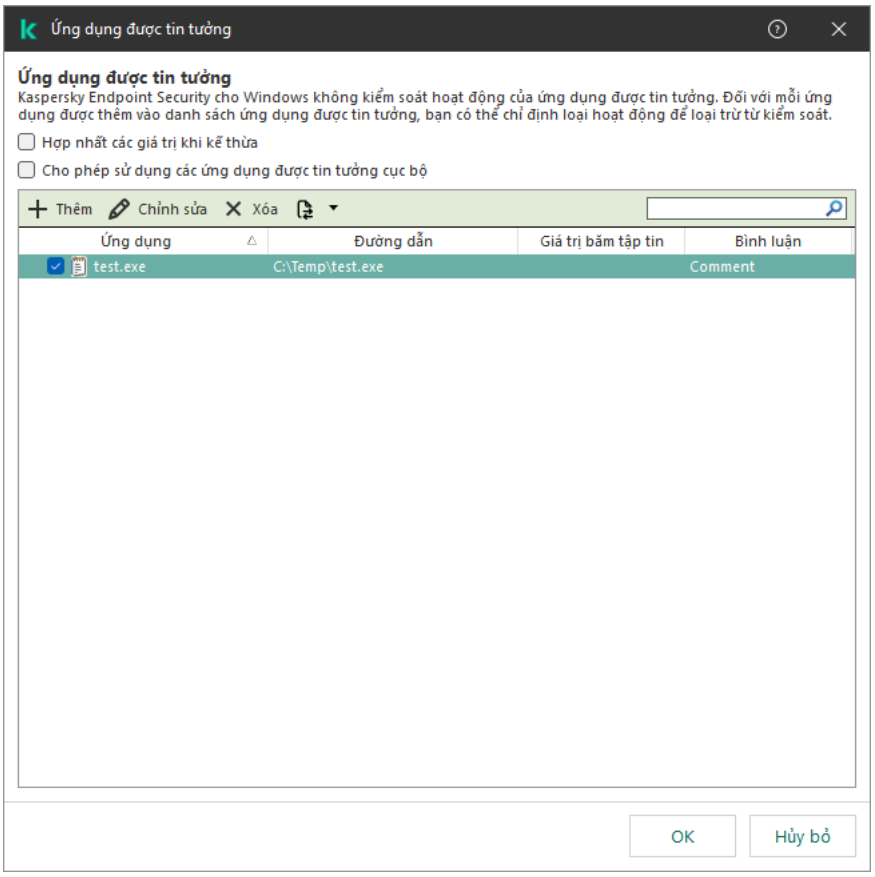
Kaspersky Endpoint Security sử dụng định dạng XML để xuất và nhập *danh sách ứng dụng được tin tưởng*.

Cách xuất và nhập vùng tin tưởng trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Loại trừ và loại đối tượng**.
4. Trong mục **Loại trừ quét và ứng dụng được tin tưởng**, hãy chọn thành phần của vùng tin tưởng mà bạn muốn xuất hoặc nhập: **Loại trừ quét** hoặc **Ứng dụng được tin tưởng**.
5. Nhấn vào **Thiết lập**.
6. 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 nút → **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. Kaspersky Endpoint Security cũng hỗ trợ xuất danh sách loại trừ ra tập tin DAT.



Danh sách các ứng dụng được tin tưởng

7. Để nhập danh sách loại trừ:

a. Nhấn nút → **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. Kaspersky Endpoint Security cũng hỗ trợ nhập danh sách loại trừ từ tập tin DAT.

8. Lưu các thay đổi của bạn.

Cách xuất hoặc nhập vùng 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 **Asset management** → **Policies**.

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 **Trusted Zone**.

5. Để xuất danh sách quy tắc:

   a. Nhấn vào liên kết **Malware Scan exclusions**.

   b. Chọn các loại trừ mà bạn muốn xuất.

   c. Nhấn nút → **Export**.

      Kaspersky Endpoint Security sẽ xuất danh sách các loại trừ vào tập tin JSON trong thư mục tải xuống mặc định.

6. Để xuất danh sách các ứng dụng được tin tưởng:

   a. Chọn các ứng dụng được tin tưởng mà bạn muốn xuất.

   b. Nhấn nút → **Export**.

      Kaspersky Endpoint Security sẽ xuất danh sách ứng dụngg được tin tưởng vào tập tin JSON trong thư mục tải xuống mặc định.

7. Để nhập danh sách loại trừ:

   a. Nhấn vào liên kết **Malware Scan exclusions**.

   b. Nhấn nút → **Import**.

      Trong cửa sổ mở ra, hãy chọn tập tin JSON 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 JSON.

8. Để nhập danh sách các ứng dụng được tin tưởng:

   a. Nhấn vào liên kết **Applications**.

   b. Nhấn nút → **Import**.

      Thao tác này sẽ mở một cửa sổ; trong cửa sổ đó, hãy chọn tập tin JSON mà bạn muốn nhập danh sách ứng dụng được tin tưởng.

   c. Mở tập tin.

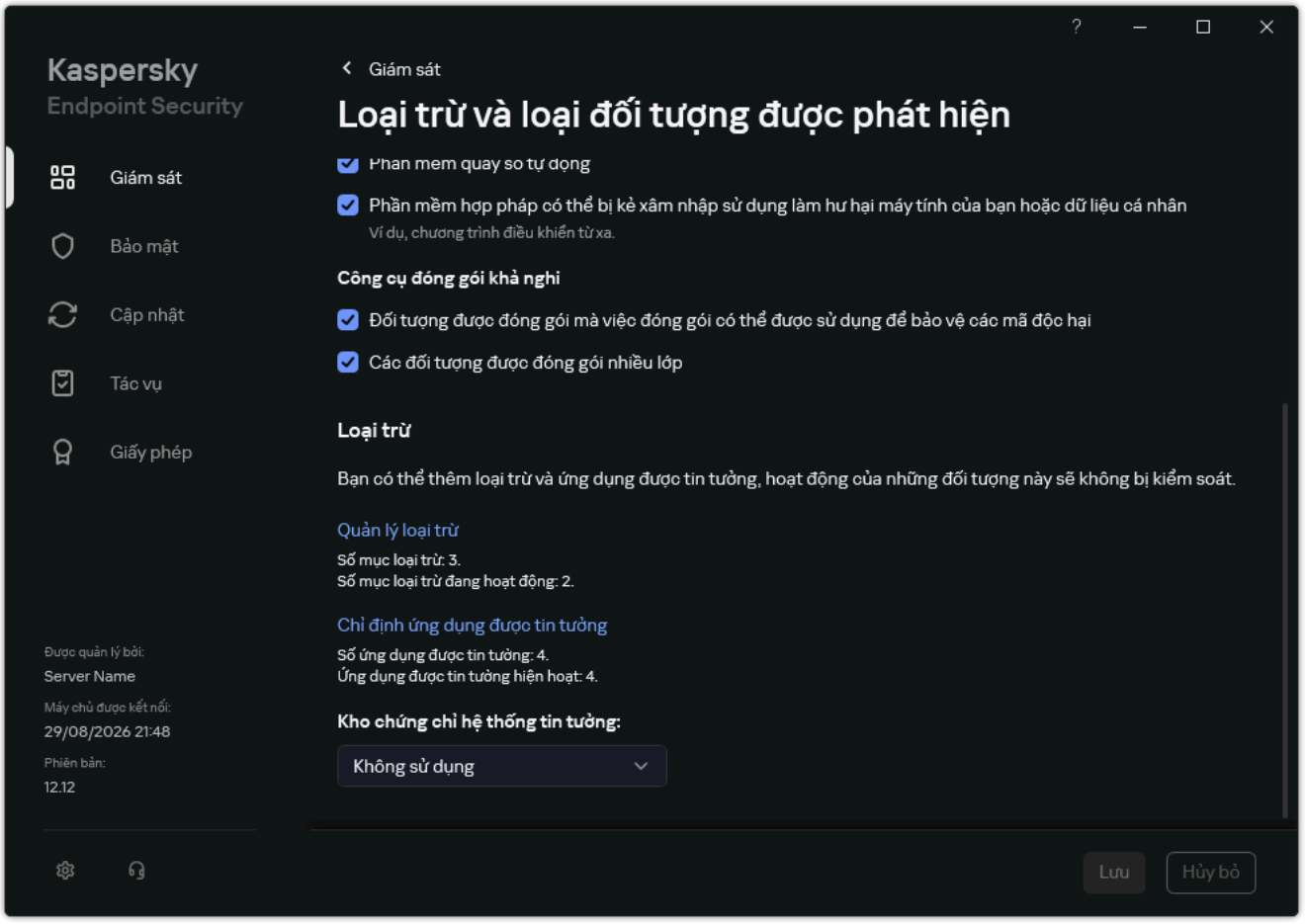
      Nếu máy tính đã có danh sách ứng dụng được tin tưởng, Kaspersky Endpoint Security sẽ nhắc bạn xóa danh sách hiện có hoặc thêm các mục mới vào từ tập tin JSON.

9. Lưu các thay đổi của bạn.

Cách xuất hoặc nhập vùng 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 → Loại trừ và loại đối tượng được phát hiện**.



Cấu hình loại trừ

3. Để xuất danh sách quy tắc:

   a. Trong mục **Loại trừ**, hãy nhấn liên kết **Quản lý loại trừ**.

   b. Chọn các loại trừ mà bạn muốn xuất.

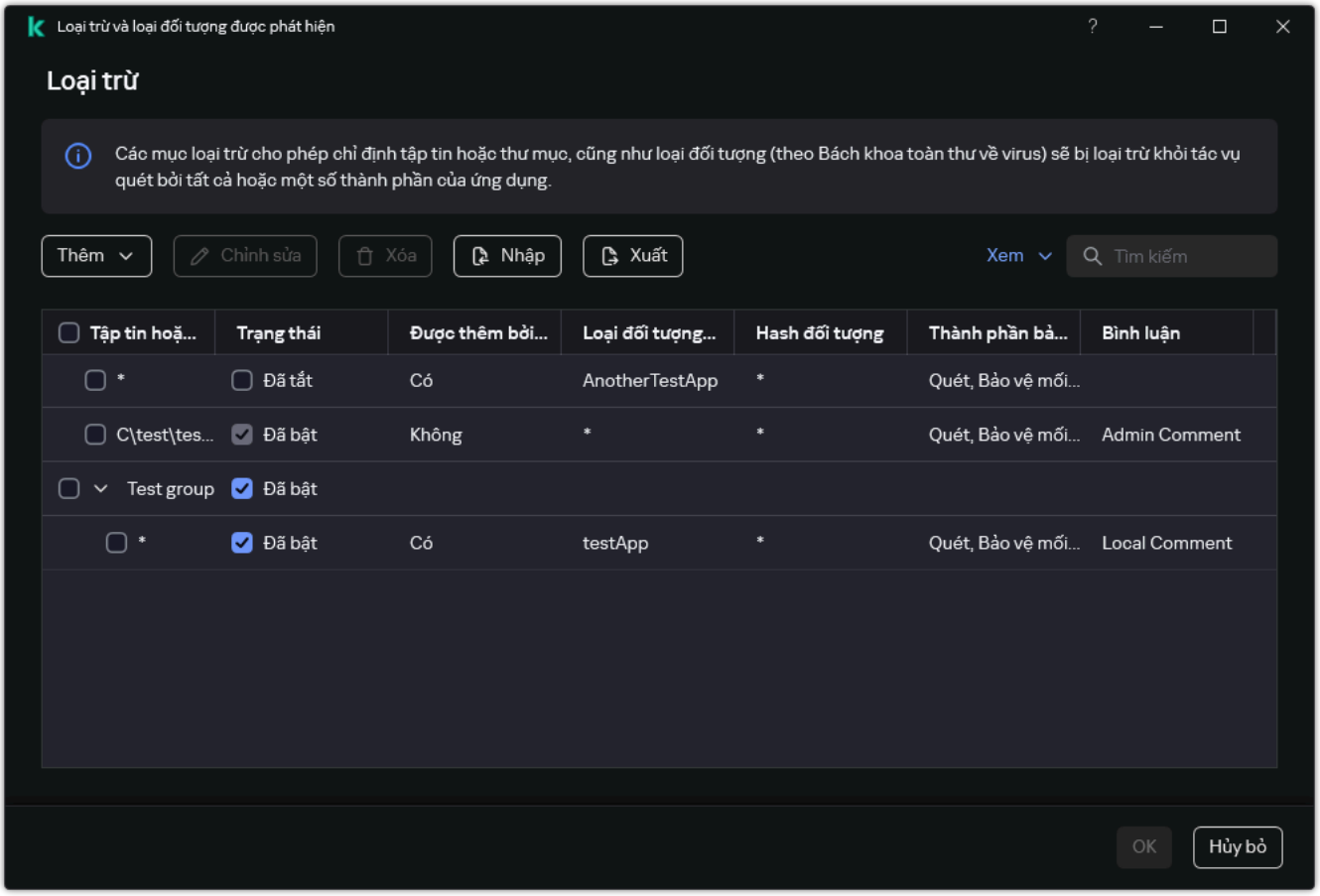
   c. Nhấn vào **Xuất**.

   d. Xác nhận rằng bạn chỉ muốn xuất các loại trừ đã chọn hoặc xuất toàn bộ danh sách loại trừ.

   e. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin CSV mà bạn muốn xuất danh sách các loại trừ 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 loại trừ vào tập tin CSV.



Danh sách loại trừ

4. Để xuất danh sách các ứng dụng được tin tưởng:

   a. Trong mục **Loại trừ**, hãy nhấn liên kết **Chỉ định ứng dụng được tin tưởng**.

   b. Chọn các ứng dụng được tin tưởng mà bạn muốn xuất.

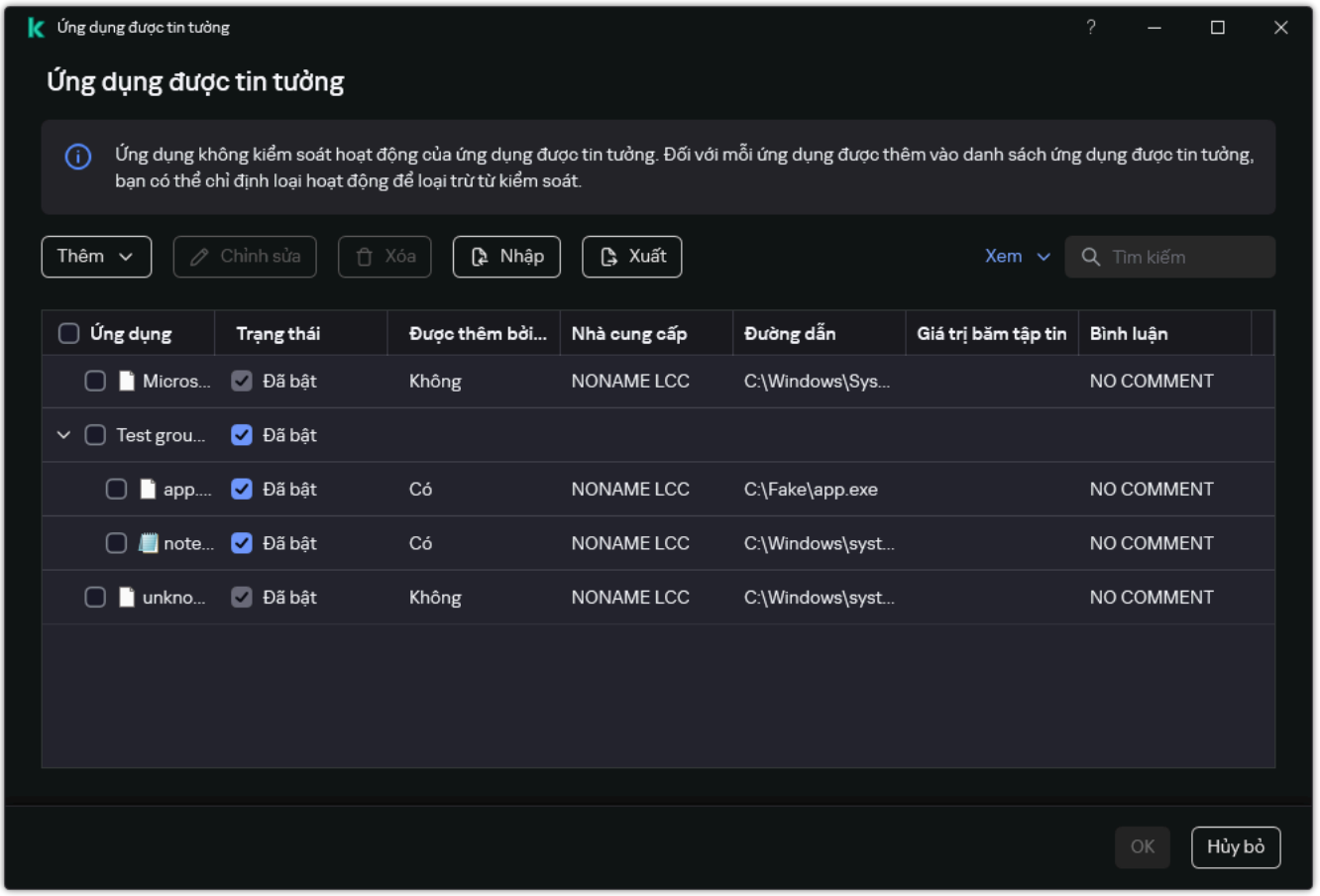
   c. Nhấn vào **Xuất**.

   d. Xác nhận rằng bạn chỉ muốn xuất các ứng dụng được tin tưởng đã chọn hoặc xuất toàn bộ danh sách.

   e. Thao tác này sẽ mở một cửa sổ; trong cửa sổ đó, hãy nhập tên của tập tin XML mà bạn muốn xuất danh sách các ứng dụng được tin tưởng 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 được tin tưởng vào tập tin XML.



Danh sách các ứng dụng được tin tưởng

5. Để nhập danh sách loại trừ:

a. Trong mục **Loại trừ**, hãy nhấn liên kết **Quản lý loại trừ**.

b. Nhấn vào **Nhập**.

c. Trong cửa sổ mở ra, hãy chọn tập tin CSV mà bạn muốn nhập danh sách các loại trừ.

d. 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 CSV.

6. Để nhập danh sách các ứng dụng được tin tưởng:

a. Trong mục **Loại trừ**, hãy nhấn liên kết **Chỉ định ứng dụng được tin tưởng**.

b. Nhấn vào **Nhập**.

c. Thao tác này sẽ mở một cửa sổ; trong cửa sổ đó, hãy chọn tập tin XML mà bạn muốn nhập danh sách ứng dụng được tin tưởng.

d. Mở tập tin.

Nếu máy tính đã có danh sách ứng dụng 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.

Xử lý các ứng dụng có chữ ký số 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*.

Cách bắt đầu sử dụng kho chứng chỉ hệ thống tin tưởng trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Loại trừ và loại đối tượng**.
4. Trong mục **Kho chứng chỉ hệ thống tin tưởng**, hãy chọn hộp kiểm **Sử dụng kho chứng chỉ hệ thống tin tưởng**.
5. Trong danh sách thả xuống, hãy chọn kho hệ thống sẽ được Kaspersky Endpoint Security coi là tin tưởng.
6. Lưu các thay đổi của bạn.

Cách bắt đầu sử dụng kho chứng chỉ hệ thống 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 thẻ **Asset management → Policies**.
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 **Trusted Zone**.
5. Trong cửa sổ mở ra, hãy nhấn vào liên kết **Root certificates**.
6. Trong cửa sổ mở ra, hãy chọn hộp kiểm **Use trusted system certificate store**.
7. Hãy chọn kho hệ thống sẽ được Kaspersky Endpoint Security coi là tin tưởng.
8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách bắt đầu sử dụng kho chứng chỉ hệ thống 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 → Loại trừ và loại đối tượng được phát hiện**.
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.

Phụ lục. Các loại trừ quét được định sẵn và các ứng dụng được tin tưởng

Kể từ Kaspersky Endpoint Security 12.6 cho Windows, loại trừ quét và ứng dụng được tin tưởng được thêm vào khu vực tin tưởng. Các ứng dụng được tin tưởng và loại trừ quét được xác định trước giúp nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager. Điều này có nghĩa là bạn không cần thiết lập khu vực tin tưởng theo cách thủ công cho ứng dụng trên máy chủ. Kể từ Kaspersky Endpoint Security 12.8 cho Windows, bạn có thể cài đặt ứng dụng ở chế độ Light Agent để bảo vệ môi trường ảo. Các loại trừ quét được định sẵn và các ứng dụng được tin tưởng có thể giúp bạn nhanh chóng cấu hình Kaspersky Endpoint Security trong các môi trường máy ảo Citrix và VMware.

Bạn có thể chọn các loại trừ định sẵn và các ứng dụng được tin tưởng theo những cách sau:

- Cài đặt ứng dụng.
  - Cài đặt ứng dụng một cách cục bộ bằng Trình hướng dẫn
  - Thuộc tính gói cài đặt
- Thiết lập chính sách.
  - Trình hướng dẫn chính sách mới
  - Thuộc tính chính sách: các loại trừ quét và các ứng dụng được tin tưởng

Microsoft SQL Server

Khi cài đặt Kaspersky Endpoint Security trên máy chủ SQL, bạn phải tạo một khu vực tin tưởng từ các loại trừ và các ứng dụng được tin tưởng để đảm bảo hoạt động của máy chủ không bị can thiệp.

Loại trừ quét định sẵn

Đường dẫn	Phiên bản SQL
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??.*\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles%\Microsoft SQL Server\MSSQL??.**\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022

Microsoft Exchange Server

Khi cài đặt Kaspersky Endpoint Security trên máy chủ Microsoft Exchange, bạn phải tạo một khu vực tin tưởng từ các loại trừ và các ứng dụng được tin tưởng để đảm bảo hoạt động của máy chủ không bị can thiệp.

Loại trừ quét định sẵn

Đường dẫn	Phiên bản Microsoft Exchange
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.jsl	2013 2016 2019

Đường dẫn	Phiên bản Microsoft Exchange
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.jsl	2013 2016 2019

Các ứng dụng được tin tưởng định sẵn

Đường dẫn	Phiên bản Microsoft Exchange
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\EdgeTransport.exe	2013 2016 2019
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe	2013 2016 2019

Microsoft System Center Configuration Manager

Nếu Microsoft System Center Configuration Manager được cài đặt trên hệ điều hành của máy tính được bảo vệ thì bạn cần thêm một ngoại lệ được định sẵn vào danh sách ngoại lệ quét để giải pháp hoạt động ổn định.

Loại trừ quét định sẵn

Đường dẫn	Phiên bản System Center Configuration Manager
%ProgramFiles%\Microsoft Configuration Manager\Inboxes	2012 2012 R2

Citrix

Khi cài đặt Kaspersky Endpoint Security trong môi trường ảo Citrix, bạn phải tạo một khu vực tin tưởng từ các loại trừ và các ứng dụng được tin tưởng để đảm bảo hoạt động của máy chủ không bị can thiệp.

Loại trừ quét định sẵn

Đường dẫn
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName_log.ldf
%ProgramData%\Citrix\Broker\Cache
%SystemRoot%\System32\drivers\CtxUvi.sys
%ProgramFiles%\Citrix\HDX\bin\CitrixLogonCsp.dll
mcsdif.vhdx
%Temp%\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%Temp%\Citrix\HDXRTConnector**.txt
%SystemDrive%\Users*\AppData\Local\Temp\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%ProgramFiles(x86)%\Citrix\ICA Client\epclient32.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epclient64.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epinject.sys
%ProgramFiles(x86)%\Citrix\ICA Client\EntryProtect.dll
*.vhd
*.avhd
*.vhdx
*.avhdx
*.pvp
*.lok
%SystemRoot%\System32\drivers\CVhdMp.sys (Windows Server 2012 R2)
%SystemRoot%\System32\drivers\CfsDep2.sys
%ProgramData%\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN
.vdiskcache

Đường dẫn
vdiskdif.vhdx
%SystemRoot%\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore**\PersistentDictionary.edb

Các ứng dụng được tin tưởng định sẵn

Đường dẫn	Citrix Solution
%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe	Virtual App and Desktops
%ProgramFiles%\Microsoft SQL Server\150\LocalDB\Binn\sqlservr.exe	Virtual App and Desktops
%ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe	Virtual App and Desktops
%ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe	Virtual App and Desktops
%ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe	Virtual App and Desktops
%ProgramFiles%\Citrix\Virtual Desktop Agent\BrokerAgent.exe	Virtual App and Desktops
%SystemRoot%\System32\drivers\CVhdFilter.sys	Virtual App and Desktops
%ProgramFiles(x86)%\Citrix\ICAService\CtxSvcHost.exe	Virtual App and Desktops
%ProgramFiles%\Citrix\System32\ctxgfx.exe	Virtual App and Desktops
%ProgramFiles%\Citrix\ICAService\picaSvc2.exe	Virtual App and Desktops
%ProgramFiles%\Citrix\ICAService\CpSvc.exe	Virtual App and Desktops
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Virtual App and Desktops
%ProgramFiles%\Citrix\HDX\bin\CtxSvcHost.exe	Virtual App and Desktops
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Virtual App and Desktops
%ProgramFiles%\Citrix\HDX\bin\picaSvc2.exe	Virtual App and Desktops
%ProgramFiles%\Citrix\HDX\bin\CpSvc.exe	Virtual App and Desktops
%ProgramFiles(x86)%\Citrix\System32\WebSocketService.exe	Virtual App and Desktops

Đường dẫn	Citrix Solution
%ProgramFiles%\Citrix\ICAService\WebSocketService.exe	Virtual App and Desktops
%ProgramFiles(x86)%\Citrix\HDX\bin\WebSocketService.exe	Virtual App and Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\AudioTranscoder.exe	Virtual App and Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngine.Net.Service.exe	Virtual App and Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngineService.exe	Virtual App and Desktops
%ProgramFiles(x86)%\Citrix\ICA Client\MediaEngineService.exe	Ứng dụng Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\CDViewer.exe	Ứng dụng Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\concentr.exe	Ứng dụng Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\wfica32.exe	Ứng dụng Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\bgblursvc.exe	Ứng dụng Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\AuthManager\AuthManSvr.exe	Ứng dụng Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfService.exe	Ứng dụng Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe	Ứng dụng Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\HdxRtcEngine.exe	Ứng dụng Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\HdxTeams.exe	Ứng dụng Workspace
%ProgramFiles%\Citrix\Provisioning Services\BNTFTP.EXE	Provisionin
%ProgramFiles%\Citrix\Provisioning Services\PVSTSB.EXE	Provisionin
%ProgramFiles%\Citrix\Provisioning Services\StreamService.exe	Provisionin
%ProgramFiles%\Citrix\Provisioning Services\StreamProcess.exe	Provisionin
%ProgramFiles%\Citrix\Provisioning Services\soapserver.exe	Provisionin
%ProgramFiles%\Citrix\Provisioning Services\Inventory.exe	Provisionin
%ProgramFiles%\Citrix\Provisioning Services\Notifier.exe	Provisionin
%ProgramFiles%\Citrix\Provisioning Services\MgmtDaemon.exe	Provisionin
%ProgramFiles%\Citrix\Provisioning Services\BNPXE.exe	Provisionin
%ProgramFiles%\Citrix\Provisioning Services\CdfSvc.exe	Provisionin
%ProgramFiles%\Citrix\Provisioning Services\BNAbsService.exe	Provisionin
%SystemRoot%\System32\drivers\bnistack6.sys	Provisionin
%SystemRoot%\System32\drivers\CfsDep2.sys	Provisionin
%SystemRoot%\System32\drivers\cnicteam.sys	Provisionin

Đường dẫn	Citrix Solution
%ProgramFiles%\Citrix\Provisioning Services\BNDevice.exe	Provisionin
%ProgramFiles%\Citrix\Provisioning Services\drivers\BNIstack6.sys	Provisionin
%ProgramFiles%\Citrix\Provisioning Services\drivers\CNicTeam.sys	Provisionin
%ProgramFiles%\Citrix\Provisioning Services\drivers\CFsDep2.sys	Provisionin
%ProgramFiles%\Citrix\Provisioning Services\drivers\CVhdMp.sys	Provisionin
%ProgramFiles%\Citrix\Receiver StoreFront\Services\SubscriptionsStoreService\Citrix.DeliveryServices.SubscriptionsStore.ServiceHost.exe	StoreFron
%ProgramFiles%\Citrix\Receiver StoreFront\Services\CredentialWallet\Citrix.DeliveryServices.CredentialWallet.ServiceHost.exe	StoreFron

VMware

Khi cài đặt Kaspersky Endpoint Security trong môi trường ảo VMware, bạn phải tạo một khu vực tin tưởng từ các ứng dụng được tin tưởng để đảm bảo hoạt động của máy chủ không bị can thiệp.

Các ứng dụng được tin tưởng định sẵn

Đường dẫn	VMware Solution
C:\Program Files\VMware\VMware View\Agent\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\wsnm_jms.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\ws_scripthost.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastS.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastW.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\SecurityGateway.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\x64\pcoip_server_win32.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\pcoip_server_win32.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\Scanner.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\tsdrvdisvc.dll	Horizon
C:\Program Files\VMware\VMware View\Server\appblastgateway\nssm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\SecurityGateway.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_TunnelService.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_SecurityServer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmUpdateLauncher.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-appstub.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-helper.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-previewer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-redir-client.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-remotemks.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view-usbloader.exe	Horizon

Đường dẫn	VMware Solution
C:\Program Files\VMware\VMware Horizon View Client\ClientService\horizon_client_service.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\DCT\ws_diag.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\cef\HTML5VideoPlayer.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib64.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlping.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlsv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\diagutil.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\ftscanmgrhv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan64.exe	Horizon
C:\Program Files\Common Files\VMware\SerialPortRedirection\Client\vmwsprrdpwks.exe	Horizon

Khử trùng lặp dữ liệu trong Microsoft Windows Server

Nếu tính năng chống trùng lặp dữ liệu được bật trên hệ điều hành Microsoft Windows Server có Kaspersky Endpoint Security được cài đặt, bạn cần thêm một ứng dụng được tin tưởng định sẵn vào danh sách các ứng dụng được tin tưởng để tối ưu hóa Kaspersky Endpoint Security và giảm tải cho CPU.

Các ứng dụng được tin tưởng định sẵn

Đường dẫn	Phiên bản Microsoft Windows Server
%SystemRoot%\system32\fsdmhost.exe	Tất cả các phiên bản được hỗ trợ

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 của các tập tin được lưu trữ trong thư mục `C:\ProgramData\Kaspersky Lab\KES.14.2\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.

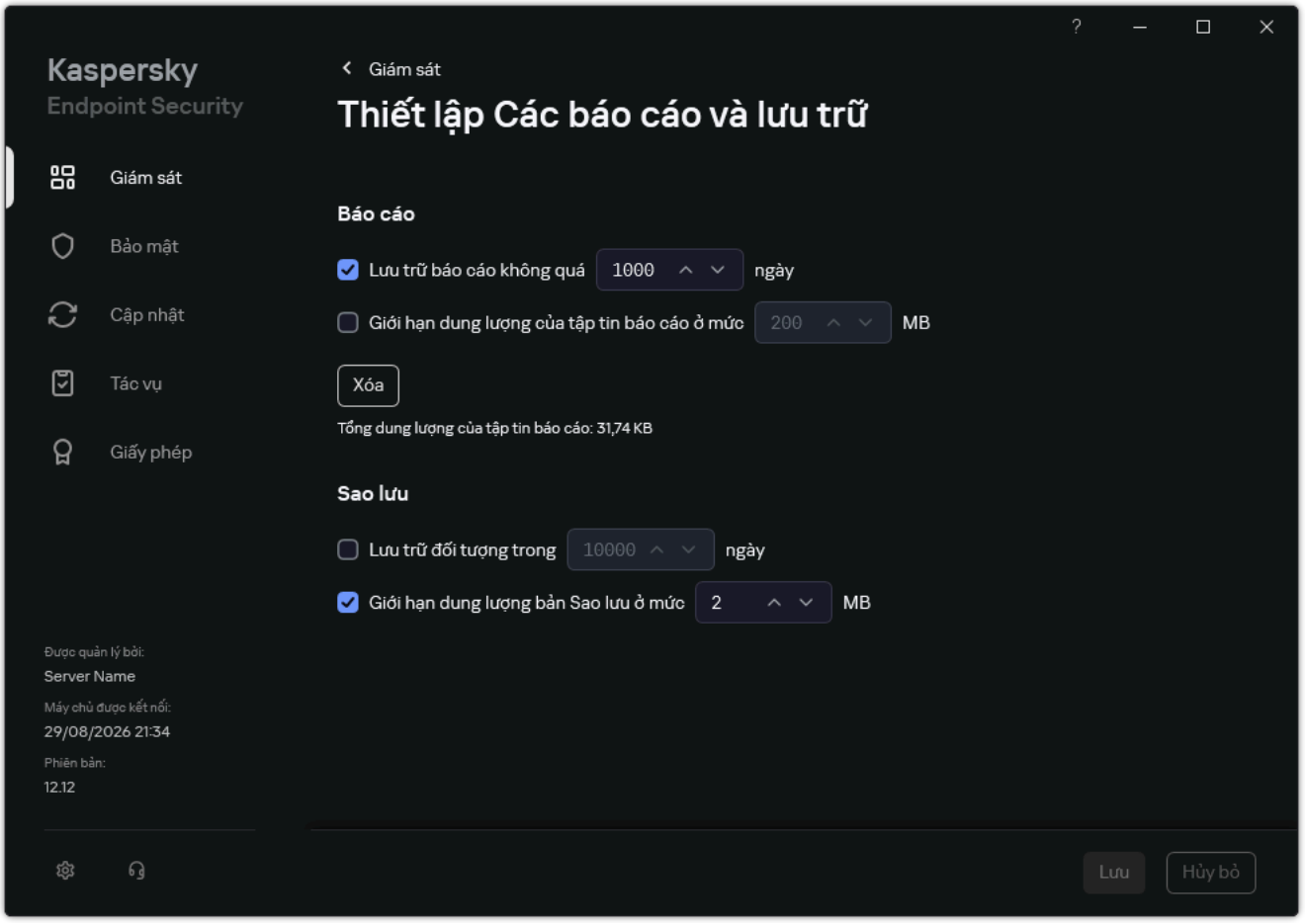
Nếu Kaspersky Endpoint Security đang được quản lý bởi Kaspersky Security Center, các bản sao lưu tập tin có thể được truyền tải đến Kaspersky Security Center Administration Server. Để biết thêm chi tiết về việc quản lý các bản sao lưu tập tin trong Kaspersky Security Center, vui lòng tham khảo hệ thống 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 cài đặt ứng dụng, trong mục **Thiết lập tổng quát** hãy nhấn vào ô **Các báo cáo và lưu trữ**.



Thiết lập sao lưu

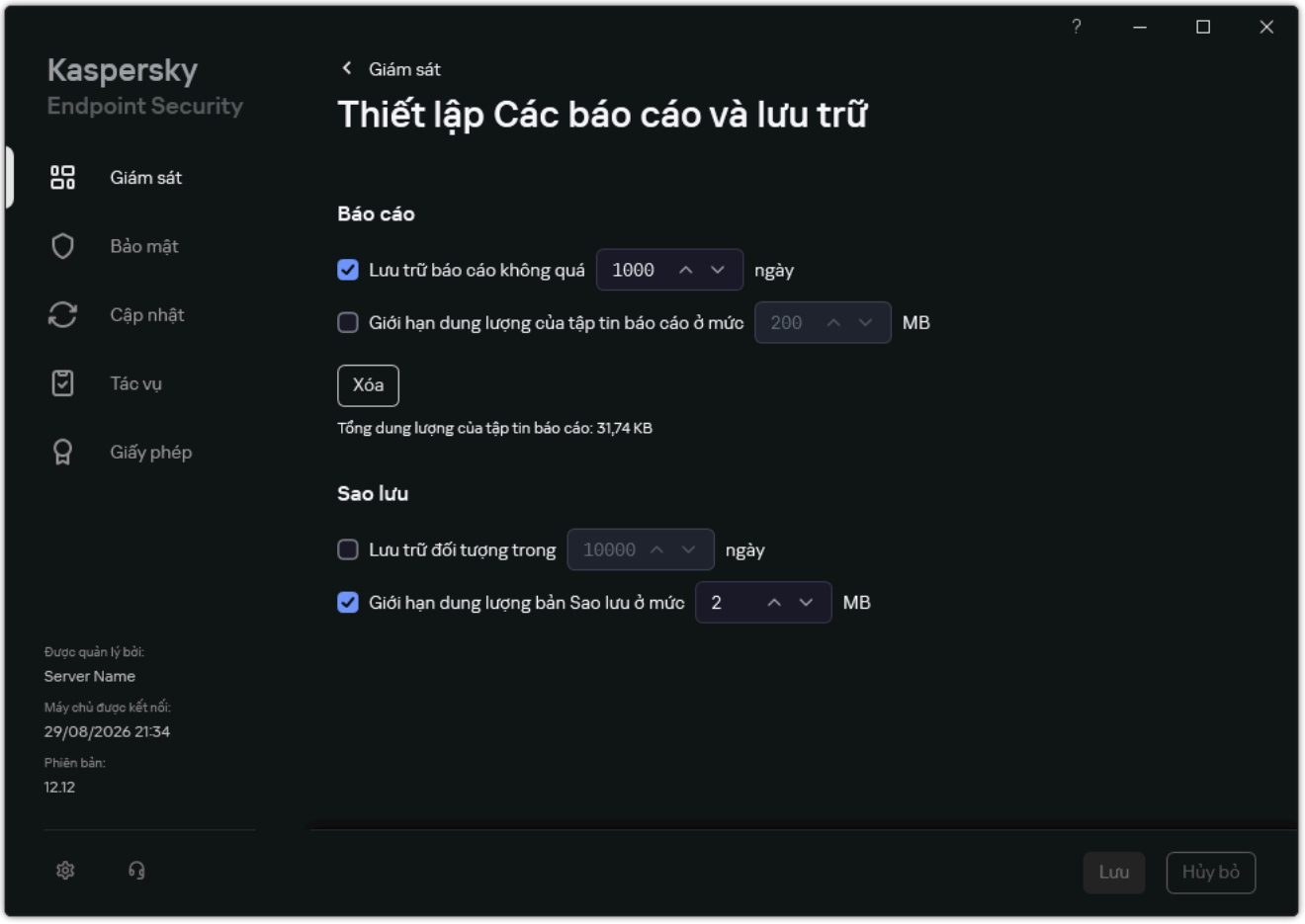
3. Nếu bạn muốn giới hạn thời gian lưu trữ cho các bản sao của tập tin trong Sao lưu, hãy chọn hộp kiểm **Lưu trữ đối tượng trong N ngày** trong mục **Sao lưu**. Nhập thời gian lưu trữ tối đa cho các bản sao tập tin trong Sao lưu.
4. Lưu các thay đổi của bạn.

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 cài đặt ứng dụng, trong mục **Thiết lập tổng quát** hãy nhấn vào ô **Các báo cáo và lưu trữ**.



Thiết lập sao lưu

3. Trong mục **Sao lưu**, hãy chọn hộp kiểm **Giới hạn dung lượng bản Sao lưu ở mức N MB**. 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 1024 MB. Để tránh vượt quá kích thước lưu trữ 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.
4. Lưu các thay đổi của bạn.

Khôi phục các tập tin từ Sao lưu

Nếu phát hiện mã độc trong tập tin, Kaspersky Endpoint Security sẽ chặn tập tin đó, gán trạng thái *Không khử được mã độc* cho tập tin, đặt một bản sao của tập tin vào Sao lưu, và cố gắng khử mã độc 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 *Đã 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 tập tin có trạng thái *Sẽ bị xóa khi máy tính khởi động lại*. Hãy khởi động lại máy tính, khi đó trạng thái tập tin sẽ đổi thành *Đã khử mã độc* hoặc *Đã 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 (xem tập tin trợ giúp của Microsoft Windows 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.

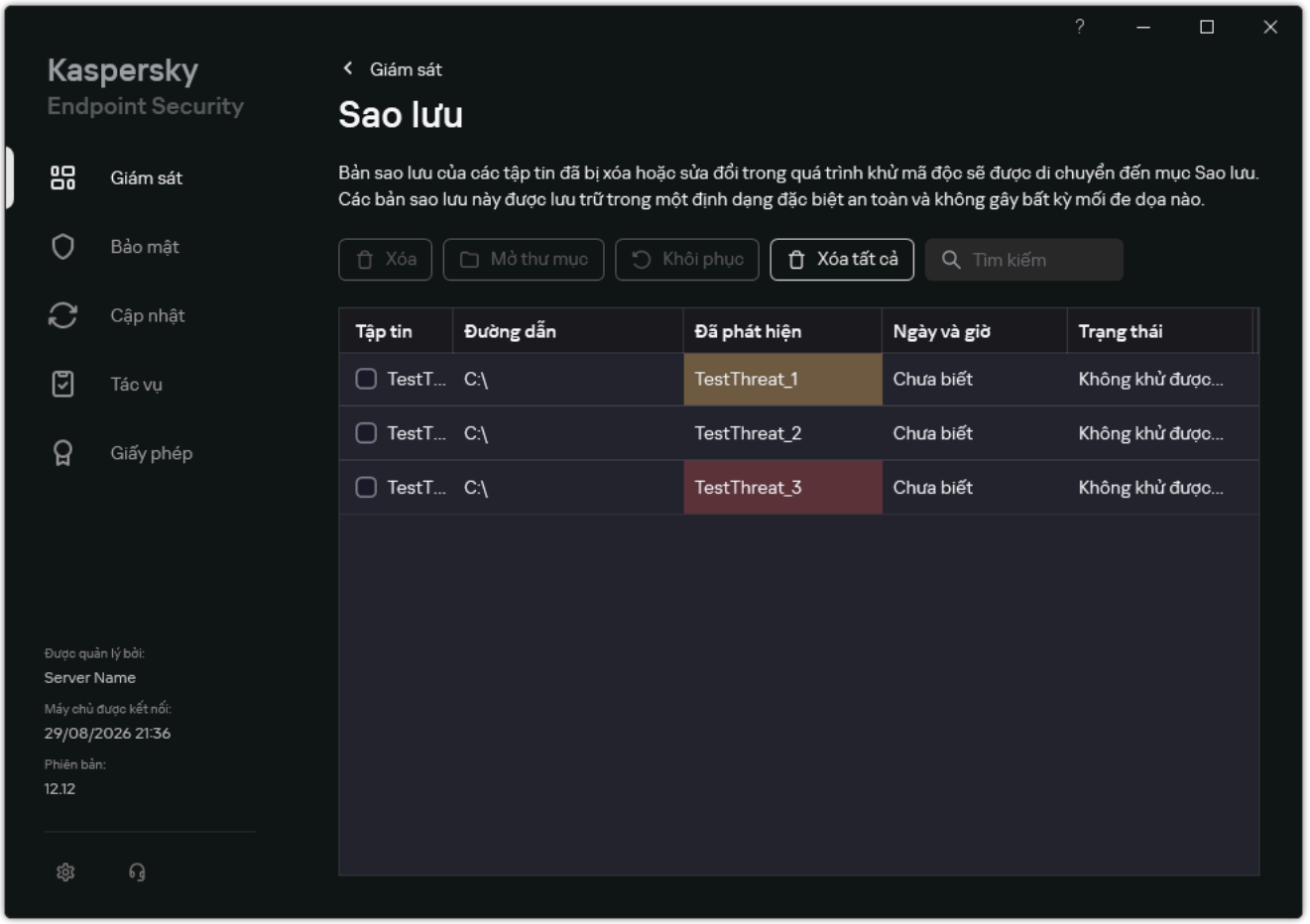
Nếu nhiều tập tin có tên giống nhau và nội dung khác nhau được đặt trong cùng một thư mục được di chuyển đến Sao lưu, chỉ tập tin có vị trí cuối cùng trong Sao lưu mới có thể được khôi phục.

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.



Sao lưu

Xóa bản sao lưu của tập tin khỏi Sao lưu

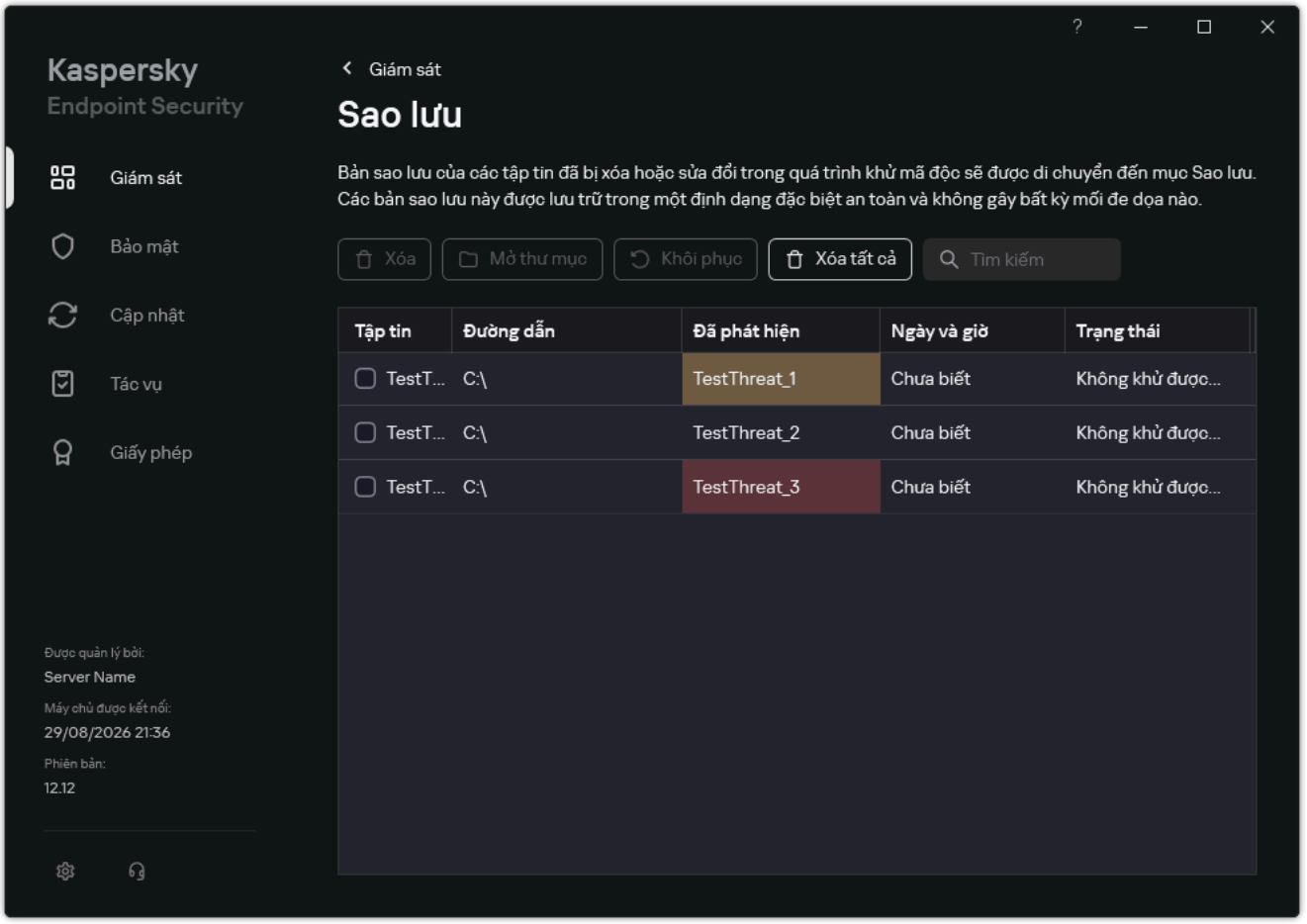
Kaspersky Endpoint Security sẽ tự động xóa các bản sao lưu của các tập tin thuộc bất cứ trạng thái nào khỏi Sao lưu sau khi thời hạn lưu trữ được cấu hình trong thiết lập của ứng dụng đã trôi qua. Bạn cũng có thể xóa thủ công bất kỳ bản sao nào của một tập tin khỏi Sao lưu.

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.



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, hãy chọn **Thiết lập tổng quát** → **Giao diện**.
3. Trong mục **Thông báo**, hãy nhấn nút **Cấu hình 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, hãy chọn **Thiết lập tổng quát → Giao diện**.

3. Trong mục **Thông báo**, hãy nhấn nút **Cấu hình 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 vào **OK**.

8. Nếu bạn đã bật thông báo qua email, hãy cấu hình thiết lập để gửi email:

   a. Nhấn vào **Cấu hình thông báo qua 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.

d. Nhấn vào **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, hãy 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.14.2\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:

ⓘ **Thông báo thông tin**. 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.

ⓘ **Sự kiện nghiêm trọng**. Các sự kiện có tầm quan trọng thiết yếu thể hiện các vấn đề trong hoạt động của Kaspersky Endpoint Security, hoặc lỗ hổng bảo mật trong tính năng bảo vệ máy tính của người dùng.

Để xử lý các báo cáo một cách tiện lợi, bạn có thể thay đổi việc trình bày dữ liệu trên màn hình theo các cách sau:

- Lọc danh sách sự kiện theo nhiều tiêu chí khác nhau.
- Sử dụng chức năng tìm kiếm để tìm một sự kiện cụ thể.
- Xem sự kiện được chọn trong một phần riêng.
- Sắp xếp danh sách sự kiện theo mỗi cột báo cáo.
- Hiển thị và ẩn các sự kiện được 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.

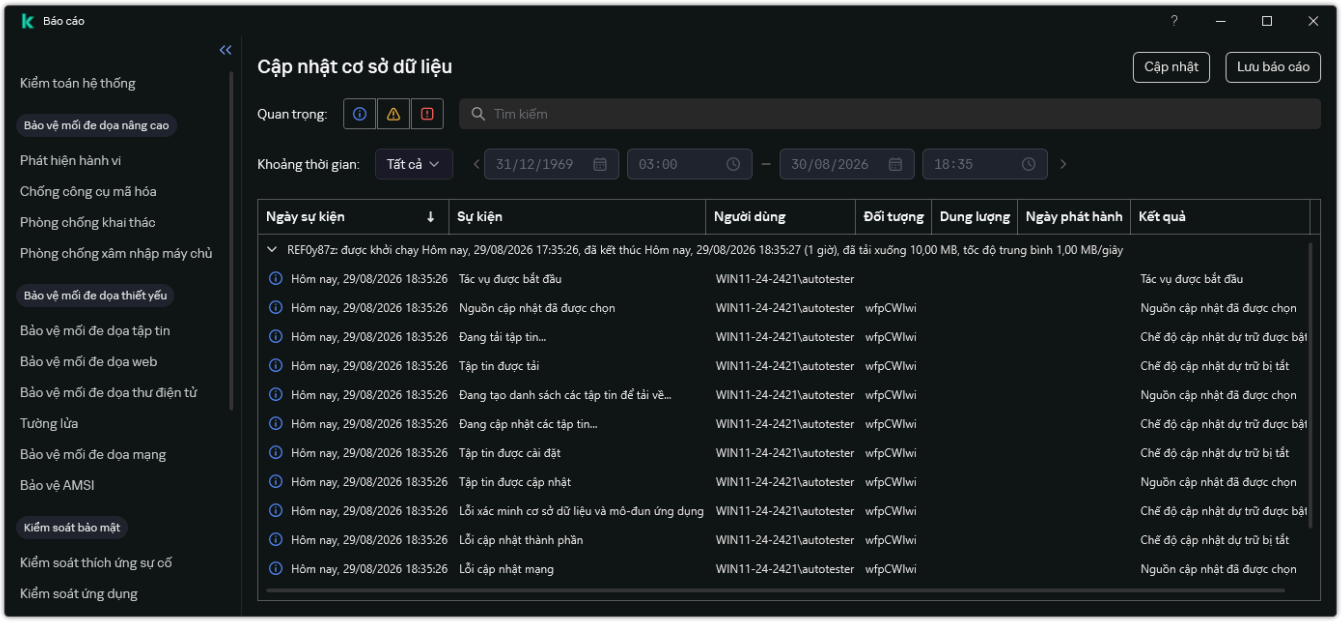
Nếu Kaspersky Endpoint Security đang chạy dưới sự quản lý của Kaspersky Security Center, thông tin về các sự kiện có thể được chuyển tiếp đến Máy chủ quản trị Kaspersky Security Center (để biết thêm chi tiết, vui lòng tham khảo Trợ giúp của Kaspersky Security Center).

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**.



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.

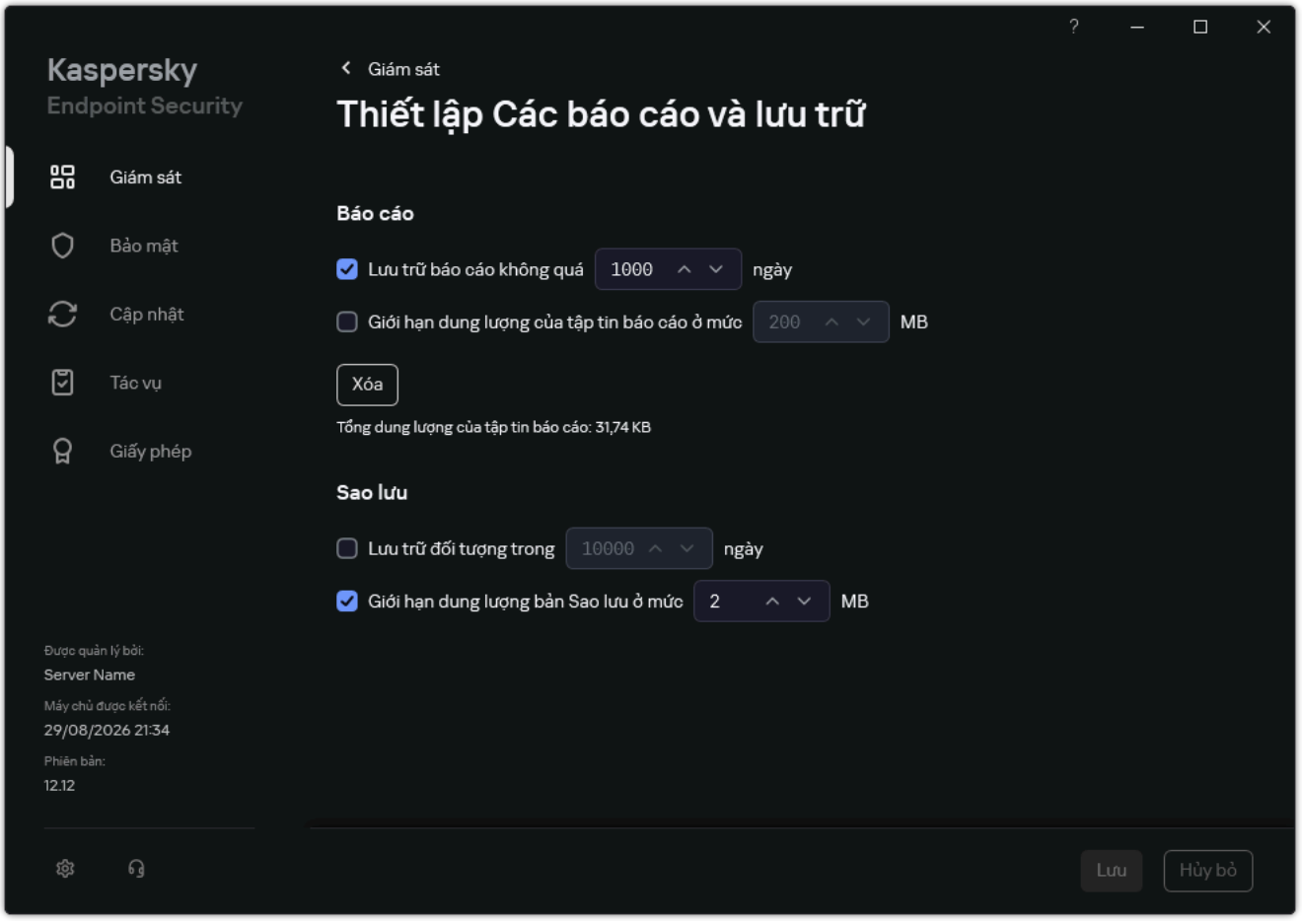
Cấu hình thời gian lưu trữ báo cáo tối đa

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 cài đặt ứng dụng, trong mục **Thiết lập tổng quát** hãy nhấn vào ô **Các báo cáo và lưu trữ**.



Thiết lập báo cáo

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.

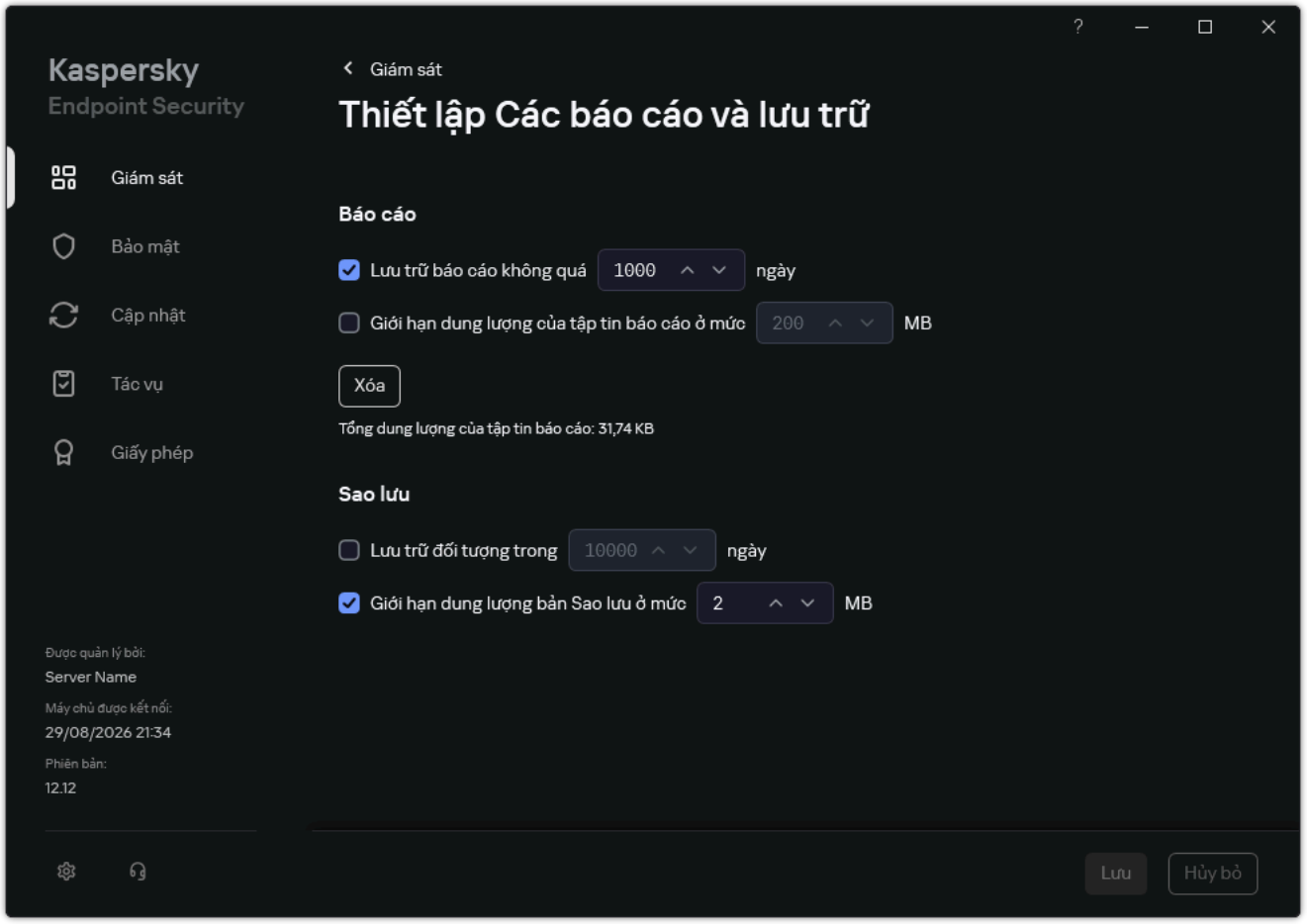
4. Lưu các thay đổi của bạn.

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 cài đặt ứng dụng, trong mục **Thiết lập tổng quát** hãy nhấn vào ô **Các báo cáo và lưu trữ**.



Thiết lập báo cáo

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

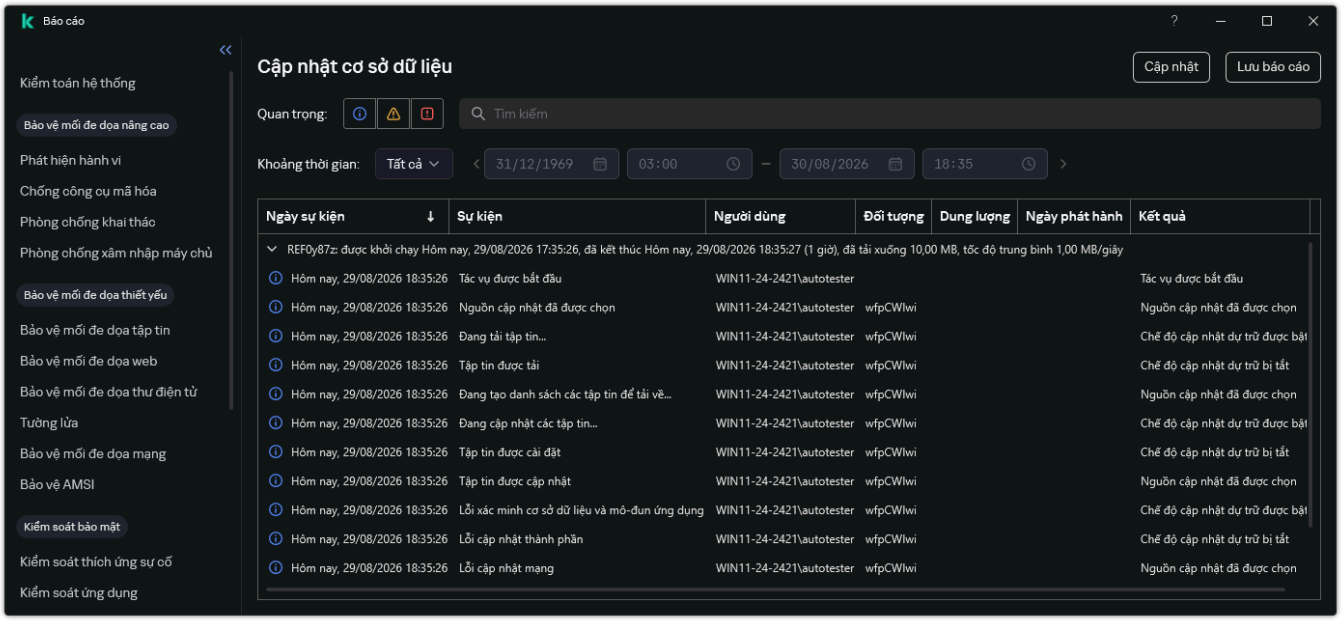
Người dùng có trách nhiệm đảm bảo sự bảo mật của thông tin từ một báo cáo được lưu ra tập tin, cụ thể là kiểm soát và hạn chế truy cập đến thông tin này.

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**.



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

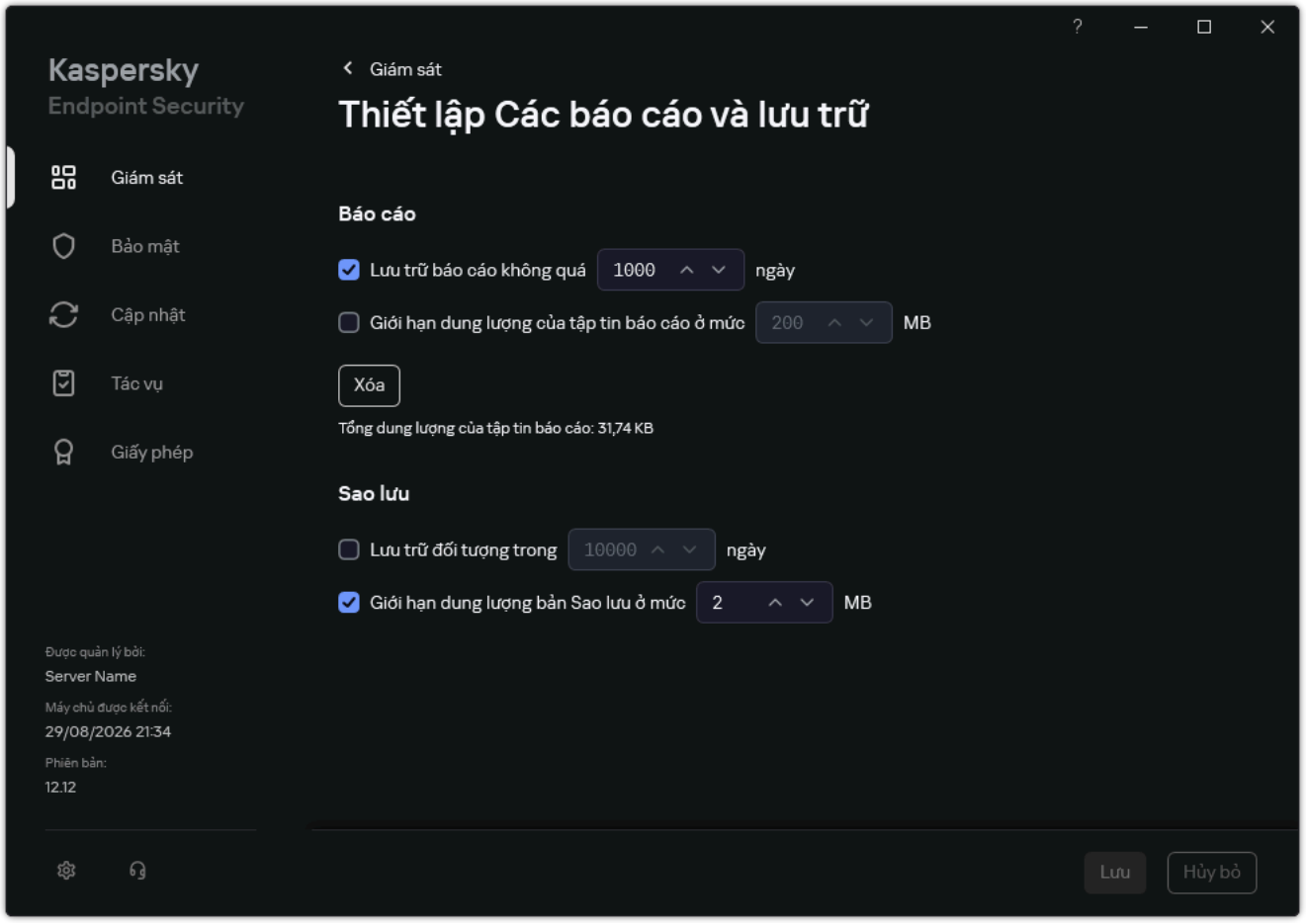
4. Nhấn vào nút **Lưu báo cáo** ở góc phải trên của cửa sổ.

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 cài đặt ứng dụng, trong mục **Thiết lập tổng quát** hãy nhấn vào ô **Các báo cáo và lưu trữ**.



Thiết lập báo cáo

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). Tính năng Tự bảo vệ cũng bao gồm khả năng bảo vệ bằng mật khẩu và bảo vệ kết nối Máy chủ quản trị.

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).

Bảo vệ kết nối Máy chủ quản trị ngăn kết nối lại trái phép máy tính tới máy chủ không đáng tin cậy.

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: • 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 khác (ví dụ: TeamViewer hoặc RemotelyAnywhere) lấy quyền truy cập vào Kaspersky Endpoint Security.	✓	– (trừ Windows 7)

Bật và tắt Tự bảo vệ

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.

Công nghệ này sẽ chặn quyền truy cập vào các thành phần sau của ứng dụng:

- 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.

Các cơ chế Tự bảo vệ không áp dụng cho các tiến trình Kaspersky Endpoint Security được khởi tạo bởi các tiến trình cha không được tin tưởng.

Cơ cấu Tự bảo vệ của Kaspersky Endpoint Security được bật theo mặc định.

Cách bật hoặc tắt thành phần Tự bảo vệ trong Bảng điều khiển quản trị (MMC)

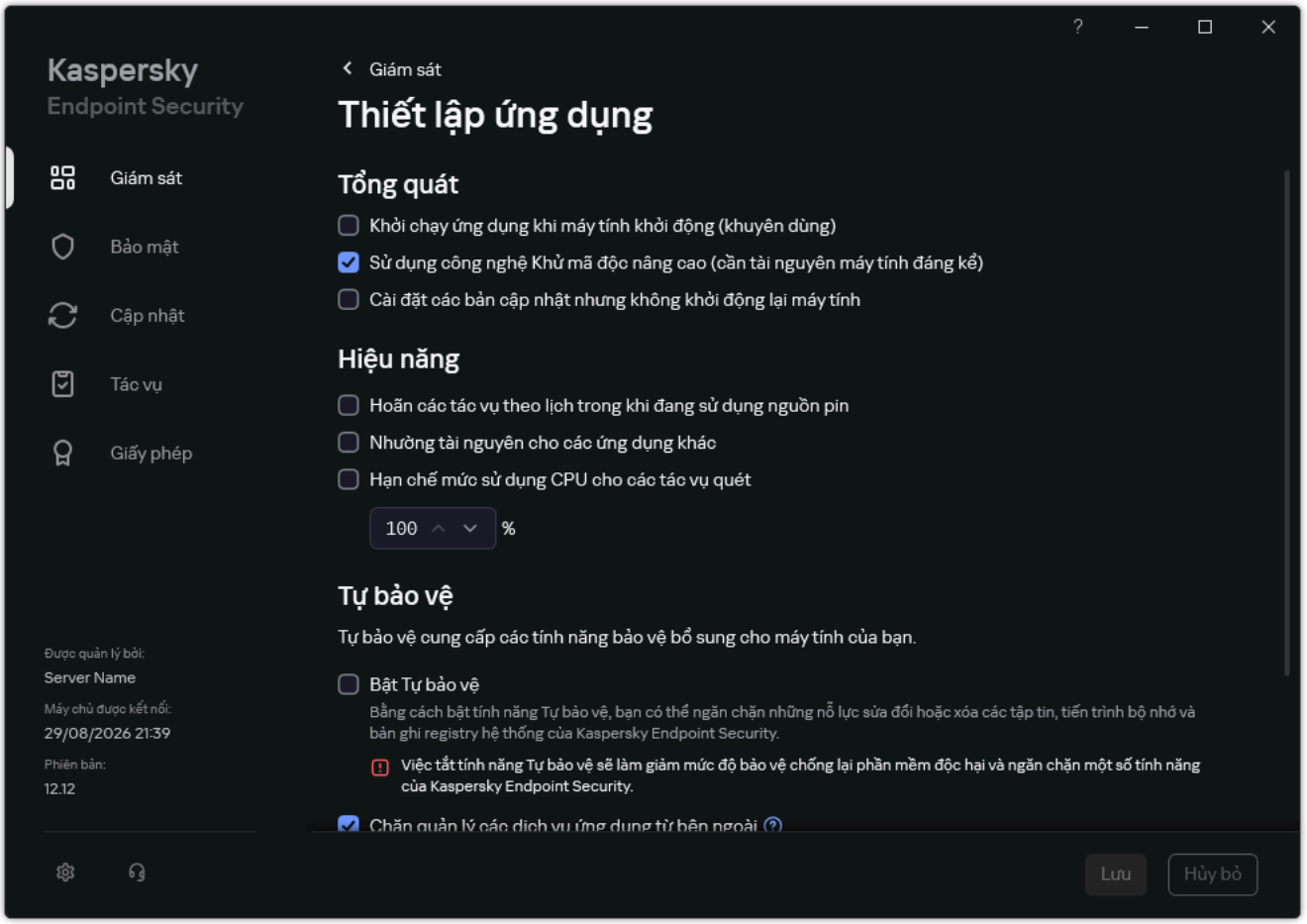
1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Thiết lập ứng dụng**.
4. Sử dụng hộp kiểm **Bật Tự bảo vệ** để bật hoặc tắt cơ chế Tự bảo vệ.
5. Lưu các thay đổi của bạn.

Cách bật hoặc tắt thành phần Tự 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 **Asset management** → **Policies**.
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** → **Self-Defense**.
5. Sử dụng công tắc bật/tắt **Self-Defense ENABLED** để bật hoặc tắt cơ chế Tự bảo vệ.
6. Lưu các thay đổi của bạn.

Cách bật hoặc tắt thành phần Tự 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 **Thiết lập tổng quát → Thiết lập ứng dụng**.



Thiết lập Kaspersky Endpoint Security cho Windows

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.

Sử dụng công nghệ AM-PPL liên tục. AM-PPL là một thành phần bảo vệ quan trọng của hệ điều hành. Vô hiệu hóa hỗ trợ AM-PPL có thể khiến một số tính năng của Kaspersky Endpoint Security không hoạt động (ví dụ: khả năng tích hợp của ứng dụng với Windows Security Center). Chỉ được phép tắt hỗ trợ AM-PPL trong môi trường thử nghiệm tách biệt, cho mục đích khắc phục sự cố.

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.

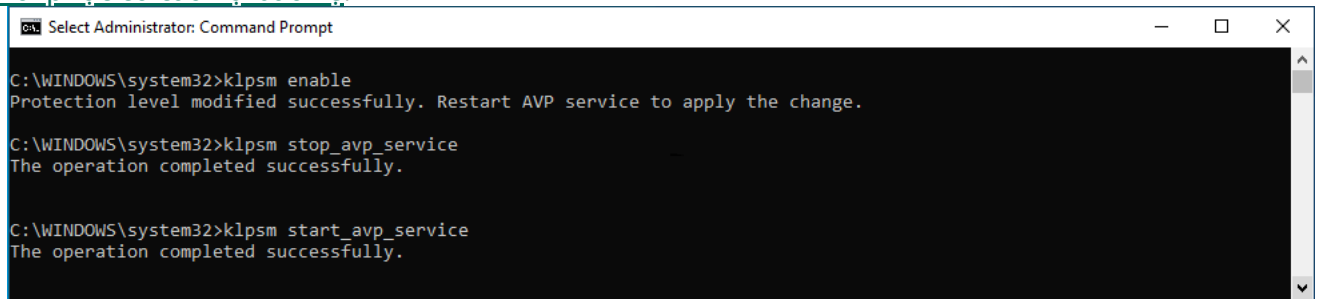
   Bạn có thể thêm đường dẫn đến tập tin thực thi vào biến hệ thống %PATH% trong khi cài đặt ứng dụng.

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.



Bật hỗ trợ cho công nghệ AM-PPL

Bảo vệ các dịch vụ ứng dụng trước hoạt động quản lý bên ngoài

Bảo vệ các dịch vụ ứng dụng trước các khối quản lý bên ngoài do người dùng và các ứng dụng khác cố gắng dừng các dịch vụ của Kaspersky Endpoint Security. Chức năng bảo vệ đảm bảo hoạt động của các dịch vụ sau:

- Dịch vụ Kaspersky Endpoint Security (AVP.KES.14.2)
- Dịch vụ Kaspersky Seamless Update Service (AVPSUS.KES.14.2)

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.

Bạn chỉ có thể cho phép quản lý từ bên ngoài các dịch vụ của ứng dụng trên các máy tính không hỗ trợ công nghệ AM-PPL hoặc trên các máy tính có công nghệ này bị tắt.

Cách bật hoặc tắt Bảo vệ dịch vụ ứng dụng trước sự quản lý bên ngoài trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Thiết lập ứng dụng**.
4. Sử dụng hộp kiểm **Chặn quản lý các dịch vụ ứng dụng từ bên ngoài** để bật hoặc 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.

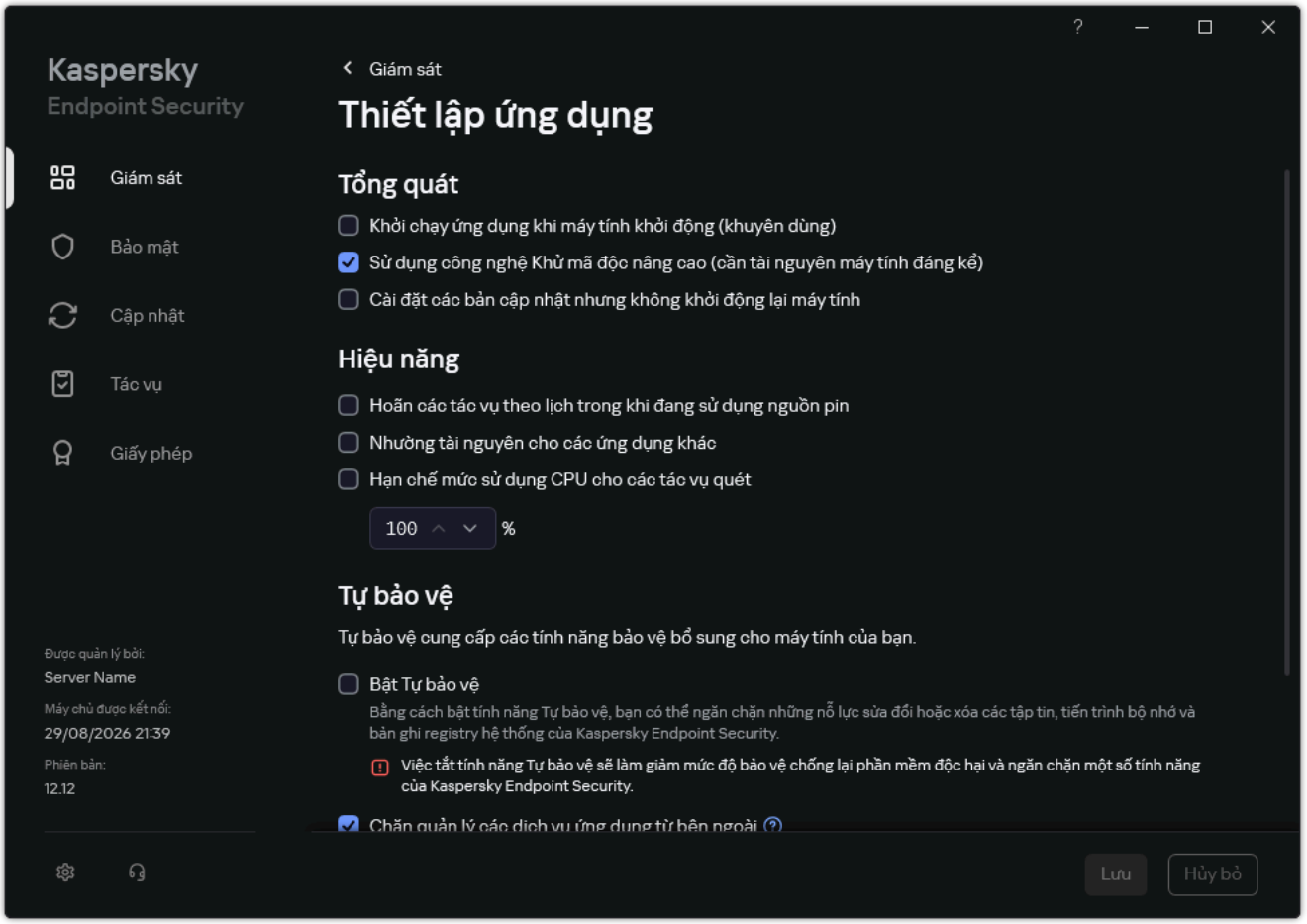
Cách bật hoặc tắt Bảo vệ dịch vụ ứng dụng trước sự quản lý bên ngoài trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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** → **Self-Defense**.
5. Sử dụng hộp kiểm **Block external management of application services** để bật hoặc tắt tính năng bảo vệ của các dịch vụ Kaspersky Endpoint Security trước sự quản lý từ bên ngoài.
6. Lưu các thay đổi của bạn.

Cách bật hoặc tắt Bảo vệ dịch vụ ứng dụng trước sự quản lý bên ngoài 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**.

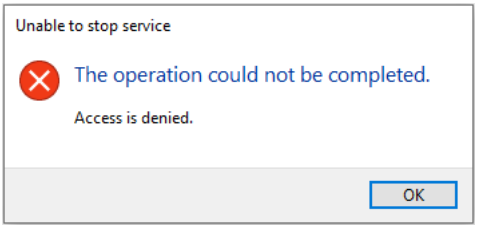


Thiết lập Kaspersky Endpoint Security cho Windows

3. Sử dụng hộp kiểm **Chặn quản lý các dịch vụ ứng dụng từ bên ngoài** để bật hoặc tắt tính năng bảo vệ của các dịch vụ Kaspersky Endpoint Security trước sự quản lý từ bên ngoài.

4. Lưu các thay đổi của bạn.

Do đó, khi người dùng cố gắng dừng các dịch vụ của ứng dụng thì một cửa sổ hệ thống kèm thông báo lỗi sẽ xuất hiện. Người dùng chỉ có thể quản lý các dịch vụ ứng dụng từ giao diện của Kaspersky Endpoint Security.



Lỗi truy cập dịch vụ ứng dụng

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 → Loại trừ và loại đối tượng được phát hiện**.
3. Trong mục **Loại trừ**, hãy nhấn liên kết **Chỉ định ứng dụng được tin tưởng**.
4. Trong cửa sổ mở ra, hãy nhấn nút **Thêm**.
5. Chọn tập tin thực thi của ứng dụng quản trị từ xa.

   Bạn cũng có thể nhập đường dẫn này 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 **Cho phép tương tác với giao diện của Kaspersky Endpoint Security**.
7. 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 thì có thể sử dụng tài khoản KLAdmin hoặc tài khoản được thêm theo cách thủ công.

- Nhập một mật khẩu tạm thời.

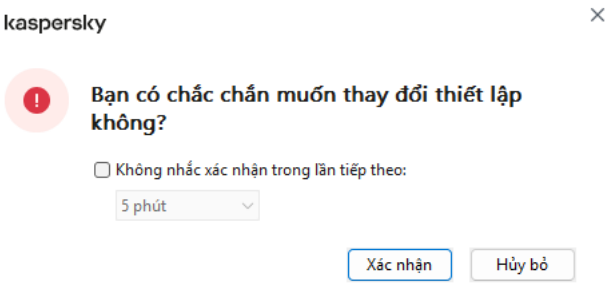
  Phương thức này phù hợp để cấp quyền truy cập tạm thời để thực hiện hành động bị chặn (ví dụ, thoát ứng dụng) cho người dùng bên ngoài mạng doanh nghiệp. Khi một mật khẩu tạm thời hết hạn hoặc một phiên kết thúc, Kaspersky Endpoint Security sẽ hoàn tác các thiết lập về trạng thái trước đó.

- Token.

  Phương pháp này phù hợp với người dùng có quyền truy cập đặc biệt (chẳng hạn như nhân viên hỗ trợ kỹ thuật). Xác thực bằng token cho phép sử dụng chế độ đăng nhập bằng thẻ thông minh trong Active Directory. Điều này giúp tăng tính bảo mật của cơ sở hạ tầng tổ chức.

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, mật khẩu token 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.



Hỏi mật khẩu truy cập Kaspersky Endpoint Security

Tên người dùng và mật khẩu

Để truy cập Kaspersky Endpoint Security, bạn nên nhập thông tin tài khoản. 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.

- **Tài khoản được thêm theo cách thủ công**. Một tài khoản bên ngoài miền Active Directory. Bạn có thể sử dụng tài khoản dịch vụ này thay vì tài khoản KLAdmin nếu không muốn chia sẻ mật khẩu quản trị viên. Bạn có thể đặt bất kỳ tên người dùng và mật khẩu nào cũng như cấu hình từng quyền riêng lẻ.

- **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.

Token

Để truy cập chức năng của Kaspersky Endpoint Security, bạn phải chọn chứng chỉ người dùng phù hợp từ danh sách chứng chỉ được lưu trữ trên thiết bị token đã kết nối và nhập mã PIN của mình. Xác thực dựa trên token chỉ khả dụng đối với người dùng thuộc miền Active Directory. Quản trị viên có thể cấu hình quyền truy cập cho từng người dùng hoặc từng nhóm. Để tính năng xác thực dựa token hoạt động, bạn phải triển khai cơ sở hạ tầng PKI được tin tưởng và cài đặt phần mềm chuyên dụng để quản lý token.

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).

Cách bật Bảo vệ bằng mật khẩu trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Giao diện**.
4. Trong mục **Bảo vệ bằng mật khẩu**, hãy nhấn nút **Thiết lập**.
   Thao tác này sẽ mở ra một cửa sổ chứa thiết lập Bảo vệ bằng mật khẩu.
5. Sử dụng hộp kiểm **Bật bảo vệ bằng mật khẩu** để bật hoặc tắt thành phần.
6. Trong mục **Quyền**, hãy chọn tài khoản KLAdmin.
7. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy nhấn vào **Mật khẩu** và đặt mật khẩu cho tài khoản KLAdmin.
   Tài khoản KLAdmin có quyền thực hiện mọi hành động được bảo vệ bởi mật khẩu.

> Nếu quên mật khẩu tài khoản KLAdmin thì bạn có thể đặt lại mật khẩu trong thuộc tính chính sách.

8. Quay lại danh sách tài khoản.

9. Thiết lập quyền truy cập cho tất cả người dùng trong mạng doanh nghiệp:

   a. Trong mục **Quyền**, hãy chọn nhóm "Mọi người".

      Nhóm Mọi người là một nhóm Windows tích hợp bao gồm tất cả người dùng trong mạng doanh nghiệp.

   b. Trong cửa sổ đã được mở, hãy 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 KLAdmin, 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.

10. Lưu các thay đổi của bạn.

Cách bật Bảo vệ bằng mật khẩu trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.

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** → **Self-Defense**.

5. Trong mục **Password Protection**, hãy sử dụng công tắc gạt **Password Protection ENABLED** để bật hoặc tắt thành phần.

6. Quy định mật khẩu cho tài khoản KLAdmin và xác nhận nó.

   Tài khoản KLAdmin có quyền thực hiện mọi hành động được bảo vệ bởi mật khẩu.

   > Nếu quên mật khẩu tài khoản KLAdmin thì bạn có thể đặt lại mật khẩu trong thuộc tính chính sách.

7. Quay lại danh sách tài khoản.

8. Thiết lập quyền truy cập cho tất cả người dùng trong mạng doanh nghiệp:

   a. Trong bảng tài khoản, hãy chọn nhóm "Mọi người".

      Nhóm Mọi người là một nhóm Windows tích hợp bao gồm tất cả người dùng trong mạng doanh nghiệp.

   b. Trong cửa sổ đã được mở, hãy 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 **Exit the application** bị xóa, bạn sẽ chỉ có thể thoát ứng dụng nếu bạn đăng nhập là KLAdmin, 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.

9. Lưu các thay đổi của bạn.

Cách bật Bảo vệ bằng mật khẩu 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 → Giao diện**.
3. Sử dụng nút bật/tắt **Bảo vệ bằng mật khẩu** để bật hoặc tắt thành phần này.
4. Quy định mật khẩu cho tài khoản KLAdmin và xác nhận nó.

   Tài khoản KLAdmin 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 KLAdmin 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 KLAdmin, 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 KLAdmin, 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 KLAdmin, 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 KLAdmin. Bạn không thể tắt bảo vệ bằng mật khẩu nếu bạn đang sử dụng một tài khoản người dùng khác hoặc một mật khẩu tạm thời.

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

Bảo vệ bằng mật khẩu cho phép cấp quyền truy cập Kaspersky Endpoint Security cho những tài khoản người dùng Active Directory cá nhân và tài khoản người dùng được thêm theo cách thủ công.

Tài khoản người dùng Active Directory

Bạn có thể cấp quyền truy cập Kaspersky Endpoint Security cho từng người dùng hoặc các nhóm bên trong miền Active Directory. 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 KLAdmin.

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 KLAdmin hoặc mật khẩu tạm thời.

Tài khoản người dùng được thêm theo cách thủ công

Bạn có thể tạo một tài khoản người dùng không có trong Active Directory và gán các quyền riêng lẻ cho tài khoản người dùng đó. Có nghĩa là bạn có thể tạo *tài khoản người dùng dịch vụ* và sử dụng nó thay vì KLAdmin. Bằng cách này, bạn không cần chia sẻ mật khẩu KLAdmin của mình với người dùng khác hoặc tạo tài khoản người dùng Active Directory mới. Bạn có thể chỉ định bất kỳ tên người dùng và mật khẩu nào. Ví dụ: bạn có thể cấp quyền **Xem báo cáo** cho tài khoản người dùng dịch vụ. Kết quả là, nếu xem báo cáo bị cấm với nhóm 'Tất cả' thì bạn có thể mở báo cáo bằng tài khoản người dùng dịch vụ hoặc tài khoản người dùng KLAdmin.

Cấp quyền truy cập cho người dùng cá nhân hoặc nhóm

Cách cấp quyền cho từng người dùng hoặc nhóm trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Giao diện**.
4. Trong mục **Bảo vệ bằng mật khẩu**, hãy nhấn nút **Thiết lập**.
   Thao tác này sẽ mở ra một cửa sổ chứa thiết lập Bảo vệ bằng mật khẩu.
5. Trong bảng tài khoản, hãy nhấn vào **Thêm**.
6. Chọn loại tài khoản người dùng mà bạn muốn thêm:
   - **Chọn một người dùng/nhóm trong Active Directory** – Tài khoản người dùng Active Directory.
     Để chọn tài khoản người dùng, hãy nhấn vào **Lựa chọn**. Chọn một người dùng hoặc nhóm trong Active Directory và xác nhận lựa chọn của bạn.
   - **Thêm người dùng / nhóm người dùng theo cách thủ công** dành cho tài khoản người dùng dịch vụ được thêm thủ công.
     Để thêm tài khoản người dùng dịch vụ, hãy nhập tên người dùng và mật khẩu (ví dụ: SecureAdmin).

     > Bạn có thể đặt lại mật khẩu tài khoản người dùng dịch vụ trong phần thiết lập chính sách. Mật khẩu tài khoản người dùng dịch vụ phải được đặt lại giống như mật khẩu KLAdmin. Nếu cho phép chỉnh sửa thiết lập Bảo vệ bằng mật khẩu ("ổ khóa" được mở) hoặc không áp dụng chính sách nào trên máy tính, bạn có thể đặt lại mật khẩu của tài khoản người dùng dịch vụ trong giao diện ứng dụng. Để thực hiện, hãy xác nhận các thay đổi thông tin tài khoản người dùng dịch vụ bằng mật khẩu KLAdmin.
7. 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 KLAdmin, 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.
8. Lưu các thay đổi của bạn.

Cách cấp quyền cho từng người dùng hoặc nhóm trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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** → **Self-Defense**.
5. Trong mục **Password Protection**, hãy nhấn liên kết **User permissions**.
   Thao tác này sẽ mở biểu mẫu để cấp quyền Kích hoạt mật khẩu.
6. Nhấn vào **Add**.
7. Chọn loại tài khoản người dùng mà bạn muốn thêm:
   - **Select from Active Directory** – Tài khoản người dùng Active Directory.
     Để chọn tài khoản người dùng, hãy nhấn vào **Edit**. Chọn một người dùng hoặc nhóm trong Active Directory và xác nhận lựa chọn của bạn.
   - **Add manually** dành cho tài khoản người dùng dịch vụ được thêm thủ công.
     Để thêm tài khoản người dùng dịch vụ, hãy nhập tên người dùng và mật khẩu (ví dụ: SecureAdmin).

     > Bạn có thể đặt lại mật khẩu tài khoản người dùng dịch vụ trong phần thiết lập chính sách. Mật khẩu tài khoản người dùng dịch vụ phải được đặt lại giống như mật khẩu KLAdmin. Nếu cho phép chỉnh sửa thiết lập Bảo vệ bằng mật khẩu ("ổ khóa" được mở) hoặc không áp dụng chính sách nào trên máy tính, bạn có thể đặt lại mật khẩu của tài khoản người dùng dịch vụ trong giao diện ứng dụng. Để thực hiện, hãy xác nhận các thay đổi thông tin tài khoản người dùng dịch vụ bằng mật khẩu KLAdmin.
8. Trong danh sách **Permissions**, 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 **Exit the application** bị xóa, bạn sẽ chỉ có thể thoát ứng dụng nếu bạn đăng nhập là KLAdmin, 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.
9. Nhấn vào **Add**.
10. Lưu các thay đổi của bạn.

Cách cấp quyền cho từng người dùng hoặc nhóm trong giao diện người dùng 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** → **Giao diện**.

3. Trong bảng tài khoản, hãy nhấn vào **Thêm**.

4. Chọn loại tài khoản người dùng mà bạn muốn thêm:

   - **Chọn một người dùng/nhóm trong Active Directory** – Tài khoản người dùng Active Directory.

     Để chọn tài khoản người dùng, hãy nhấn vào **Chọn người dùng hoặc nhóm**. Chọn một người dùng hoặc nhóm trong Active Directory và xác nhận lựa chọn của bạn.

   - **Thêm người dùng theo cách thủ công** dành cho tài khoản người dùng dịch vụ được thêm thủ công.

     Để thêm tài khoản người dùng dịch vụ, hãy nhập tên người dùng và mật khẩu (ví dụ: SecureAdmin).

     > Bạn có thể đặt lại mật khẩu tài khoản người dùng dịch vụ trong phần thiết lập chính sách. Mật khẩu tài khoản người dùng dịch vụ phải được đặt lại giống như mật khẩu KLAdmin. Nếu cho phép chỉnh sửa thiết lập Bảo vệ bằng mật khẩu ("ổ khóa" được mở) hoặc không áp dụng chính sách nào trên máy tính, bạn có thể đặt lại mật khẩu của tài khoản người dùng dịch vụ trong giao diện ứng dụng. Để thực hiện, hãy xác nhận các thay đổi thông tin tài khoản người dùng dịch vụ bằng mật khẩu KLAdmin.

5. 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 KLAdmin, 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 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 KLAdmin. 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)

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. Nhấn đúp để mở cửa sổ thuộc tính máy tính.

5. Trong cửa sổ thuộc tính máy tính, chọn phần **Applications**.

6. Trong danh sách các ứng dụng Kaspersky được cài đặt trên máy tính, hãy chọn **Kaspersky Endpoint Security cho Windows (14.2)** và nhấn đúp để mở thuộc tính ứng dụng.

7. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát → Giao diện**.

8. Trong mục **Bảo vệ bằng mật khẩu**, hãy nhấn nút **Thiết lập**.

9. Trong cửa sổ mở ra, trong mục **Mật khẩu tạm thời**, hãy nhấn vào nút **Danh sách mật khẩu tạm thời**.

   Cửa sổ quản lý mật khẩu tạm thời sẽ mở ra.

10. Nhấn vào **Thêm**.

11. Trong trường **Ngày hết hạn**, quy định ngày hết hạn của mật khẩu tạm thời.

12. 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.

13. Nhấn vào **Tạo**.

    Một cửa sổ chứa mật khẩu tạm thời sẽ được mở ra (xem hình dưới đây).

14. 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

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Assets (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 **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. Trong cửa sổ thiết lập ứng dụng, hãy chọn **General settings → Interface**.

7. Trong mục **Temporary passwords**, hãy nhấn nút **Add**.

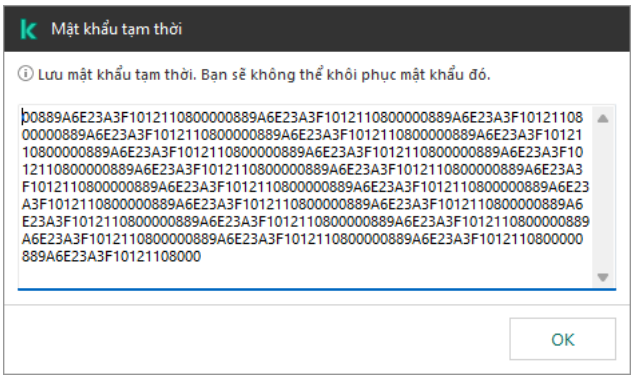
8. Trong trường **Ngày hết hạn**, quy định ngày hết hạn của mật khẩu tạm thời.

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.

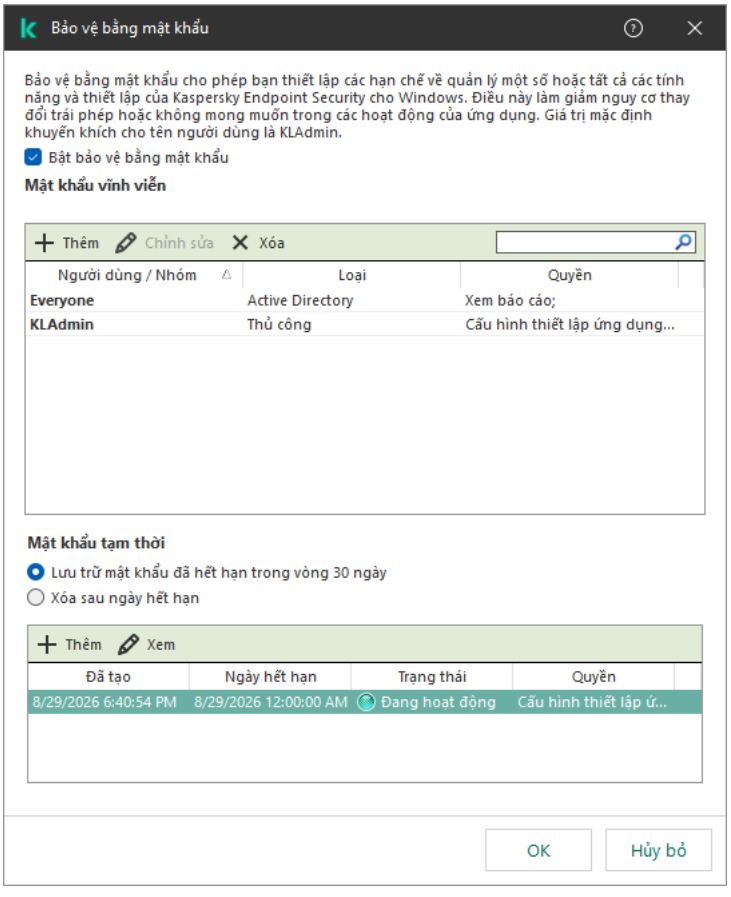


Mật khẩu tạm thời

Thu hồi mật khẩu tạm thời

Kể từ phiên bản 12.9, Kaspersky Endpoint Security for Windows bao gồm việc *quản lý chức năng mật khẩu tạm thời*. Quản lý mật khẩu tạm thời cho phép bạn thực hiện các hành động sau:

- Lưu lịch sử mật khẩu (tối đa 30 ngày).
- Theo dõi trạng thái mật khẩu tạm thời: *Đang hoạt động*, *Hết hạn*, *Đã thu hồi*.
- Thu hồi mật khẩu tạm thời.



Quản lý mật khẩu tạm thời

Quản lý mật khẩu tạm thời sẽ cập nhật trạng thái của mật khẩu và chỉ thu hồi mật khẩu sau khi đồng bộ hóa máy tính với Kaspersky Security Center.

Cách thu hồi mật khẩu tạm thời 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, hãy chọn thẻ **Devices**.
4. Nhấn đúp để mở cửa sổ thuộc tính máy tính.
5. Trong cửa sổ thuộc tính máy tính, chọn phần **Applications**.
6. Trong danh sách các ứng dụng Kaspersky được cài đặt trên máy tính, hãy chọn **Kaspersky Endpoint Security cho Windows (14.2)** và nhấn đúp để mở thuộc tính ứng dụng.
7. Trong cửa sổ thiết lập ứng dụng, hãy chọn **Thiết lập tổng quát → Giao diện**.
8. Trong mục **Bảo vệ bằng mật khẩu**, hãy nhấn nút **Thiết lập**.
9. Thao tác này mở ra một cửa sổ; trong cửa sổ đó, trong mục **Mật khẩu tạm thời**, hãy cấu hình thiết lập lưu trữ cho mật khẩu đã hết hạn.
10. Nhấn vào **Danh sách mật khẩu tạm thời**.

    Cửa sổ quản lý mật khẩu tạm thời sẽ mở ra. Quản lý mật khẩu tạm thời sẽ hiển thị ngày hết hạn của mật khẩu, trạng thái của mật khẩu và danh sách các quyền.
11. Chọn mật khẩu tạm thời đang hoạt động mà bạn muốn thu hồi và nhấn đúp vào mật khẩu để mở thuộc tính của mật khẩu.
12. Trong cửa sổ mở ra, hãy nhấn nút **Thu hồi**.
13. Lưu các thay đổi của bạn. Để áp dụng chính sách trên máy tính, hãy đóng ổ khóa .

Cách thu hồi mật khẩu tạm thời bằng cách sử dụng Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Assets (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 **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. Trong cửa sổ thiết lập ứng dụng, hãy chọn **General settings → Interface**.
7. Trong mục **Temporary passwords**, hãy cấu hình lưu trữ mật khẩu đã hết hạn.

8. Nhấn vào liên kết **Temporary password**.

   Cửa sổ quản lý mật khẩu tạm thời sẽ mở ra. Quản lý mật khẩu tạm thời sẽ hiển thị ngày hết hạn của mật khẩu, trạng thái của mật khẩu và danh sách các quyền.

9. Chọn mật khẩu tạm thời đang hoạt động mà bạn muốn thu hồi.

10. Trong cửa sổ mở ra, hãy nhấn nút **Revoke password**.

11. Lưu các thay đổi của bạn. Để áp dụng chính sách trên máy tính, hãy đóng ổ khóa .

Kết quả là, Quản lý mật khẩu tạm thời sẽ đặt trạng thái của mật khẩu thành *Đang thu hồi (đồng bộ với máy chủ)*. Sau khi đồng bộ hóa máy tính với Kaspersky Security Center, ứng dụng sẽ thu hồi mật khẩu tạm thời và chặn ngay lập tức các quyền đã cấp.

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.

Cấu hình 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 KLAdmin 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 ứng dụng**.
- Để tắt các thành phần bảo vệ từ menu ngữ cảnh (bằng cách sử dụng mục menu **Tạm dừng bảo vệ**), 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 KLAdmin 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 ứng dụng**.
- Để tắt các thành phần kiểm soát từ menu ngữ cảnh (bằng cách sử dụng mục menu **Tạm dừng bảo vệ**), 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 KLAdmin 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 dữ liệu trên ổ đĩa được 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 KLAdmin. 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.

Xuất thiết lập

Theo mặc định, việc xuất thiết lập ứng dụng bị từ chối đối với nhóm "Tất cả". Bạn có thể xuất thiết lập ứng dụng bằng tài khoản người dùng KLAdmin. Xuất thiết lập ứng dụng chỉ bao gồm tạo tập tin cấu hình với thiết lập Kaspersky Endpoint Security trong giao diện ứng dụng. Quyền này không hạn chế việc xuất danh sách loại trừ quét, địa chỉ web được tin tưởng, thiết bị được tin tưởng hoặc các danh sách khác do các thành phần ứng dụng duy trì.

Đặt lại mật khẩu KLAdmin

Nếu quên mật khẩu tài khoản KLAdmin 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 KLAdmin.

Nếu máy tính không được kết nối với Kaspersky Security Center và bạn đã quên mật khẩu cho tài khoản KLAdmin, bạn sẽ không thể phục hồi mật khẩu.

Cách đặt lại mật khẩu tài khoản KLAdmin bằng Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Giao diện**.
4. Trong mục **Bảo vệ bằng mật khẩu**, hãy nhấn nút **Thiết lập**.
5. Trong cửa sổ mở ra, hãy xóa hộp kiểm **Bật bảo vệ bằng mật khẩu**.
6. Lưu các thay đổi của bạn.
7. Chọn lại hộp kiểm **Bật bảo vệ bằng mật khẩu**.
8. Nhấn vào **OK**.
   Thao tác này sẽ mở ra cửa sổ mật khẩu quản trị viên.
9. Đặt mật khẩu mới cho tài khoản KLAdmin và xác nhận mật khẩu đó.
10. 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 **Asset management** → **Assets (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 14.2**.
   Việc này sẽ mở ra thiết lập cục bộ của ứng dụng.
5. Chọn thẻ **Application settings**.
6. Vào **General Settings** → **Self-Defense**.
7. Trong mục **Bảo vệ bằng mật khẩu**, hãy tắt nút gạt **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.

Bảo vệ kết nối Máy chủ quản trị

Kết nối máy tính với Máy chủ quản trị được thực hiện bằng cách sử dụng thành phần *Network Agent* của Kaspersky Security Center. Nếu kẻ xâm nhập có đủ quyền để sửa đổi thiết lập kết nối máy chủ thì sẽ có nguy cơ kết nối máy tính với máy chủ không được tin tưởng. Điều này sẽ cho phép kẻ xâm nhập áp dụng các chính sách nhóm của riêng chúng ví dụ như vô hiệu hóa khả năng tự bảo vệ của ứng dụng. Kaspersky Endpoint Security có thể ngăn kết nối lại trái phép máy tính với một máy chủ khác. Để bảo vệ kết nối máy chủ, ứng dụng đề xuất đặt mật khẩu và sử dụng Password-Based key Derivation Function (PBKDF2). Kết quả là không thể truy cập ứng dụng mà không cần mật khẩu.

> Để đảm bảo khả năng bảo vệ toàn diện cho Kaspersky Endpoint Security và Network Agent không bị truy cập trái phép, bạn nên kích hoạt tính năng bảo vệ bổ sung. Đối với Kaspersky Endpoint Security, bạn nên bật Bảo vệ bằng mật khẩu. Để bảo vệ Network Agent, bạn nên đặt mật khẩu ngăn gỡ cài đặt. Để biết thông tin chi tiết về bảo vệ chống gỡ bỏ Network Agent, vui lòng tham khảo Trợ giúp của Kaspersky Security Center.

Quản lý kết nối của máy tính với Máy chủ quản trị được thực hiện bằng cách sử dụng tác vụ *Bảo vệ kết nối Máy chủ quản trị*. Tác vụ này sẽ cho phép bạn thực hiện các hành động sau:

- Đặt mật khẩu để bảo vệ kết nối máy chủ.
- Thay đổi mật khẩu.

- Kết nối lại máy tính với một máy chủ khác.
- Vô hiệu hóa bảo vệ kết nối máy chủ.

Xác thực máy tính khi kết nối với Máy chủ quản trị

Sau khi đặt mật khẩu, ứng dụng sẽ tạo một mảng dữ liệu bằng cách sử dụng phép biến đổi PBKDF2 cho mật khẩu. Sau đó, ứng dụng sẽ mã hóa mảng dữ liệu này bằng khóa của Network Agent. Ứng dụng sử dụng mảng dữ liệu được mã hóa để kiểm tra quyền và đặc quyền của Máy chủ quản trị cho các kết nối tiếp theo.

Sau này, nếu có bất cứ nỗ lực kết nối lại máy tính với Máy chủ quản trị, ứng dụng sẽ giải mã mảng dữ liệu bằng khóa của Network Agent và so sánh nó với bản sao cục bộ. Nếu chúng không khớp, quyền truy cập ứng dụng sẽ bị hạn chế.

Bảo vệ kết nối Máy chủ quản trị

Cách đặt mật khẩu bảo vệ kết nối máy chủ trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Tasks**.

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **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 (14.2)** → **Bảo vệ kết nối Máy chủ quản trị**.

Bước 2. Bảo vệ kết nối với Máy chủ quản trị

Đặt mật khẩu bảo vệ kết nối với Máy chủ quản trị:

1. Trong mục **Bảo vệ kết nối Máy chủ quản trị**, hãy chọn **Bảo vệ bằng mật khẩu**.
2. Trong danh sách thả xuống **Máy chủ quản trị**, hãy chọn **Máy chủ mới**.
3. Trong trường **Mật khẩu để kết nối với Máy chủ quản trị**, hãy đặt mật khẩu kết nối với Máy chủ quản trị và xác nhận lại mật khẩu.

   Nếu quên mật khẩu, bạn có thể thay đổi mật khẩu bằng một tác vụ.

4. Nếu bạn đã triển khai Kaspersky Endpoint Security 12.7 hoặc phiên bản cũ hơn của ứng dụng, hãy chọn hộp kiểm **Bật khả năng tương thích mã hóa mật khẩu cho các phiên bản trước của ứng dụng (12.7 trở xuống)**.

   Kể từ Kaspersky Endpoint Security 12.8 cho Windows, ứng dụng này sử dụng mã hóa mật khẩu mạnh hơn. Nếu đã triển khai Kaspersky Endpoint Security 12.8 trở lên, bạn nên bỏ chọn hộp kiểm này và sử dụng mã hóa mật khẩu mạnh hơn. Các phiên bản trước của ứng dụng không hỗ trợ mã hóa mật khẩu mạnh. Để chạy tác vụ, bạn phải chọn hộp kiểm này.

Bước 3. Chọn tài khoản để chạy tác vụ

Chọn **Default account**. Theo mặc định, Kaspersky Endpoint Security sẽ khởi chạy tác vụ dưới quyền tài khoản người dùng hệ thống (SYSTEM).

Bước 4. Cấu hình lịch khởi chạy tác vụ

Trong mục **Scheduled start**, hãy chọn **Manually**.

Bước 5. Xác định tên tác vụ

Nhập tên cho tác vụ, ví dụ: *Mật khẩu kết nối máy chủ chính*.

Bước 6. Hoàn tất việc tạo tác vụ

Hoàn tất trình hướng dẫn. Chọn hộp kiểm **Run the task after the wizard finishes** hoặc chạy tác vụ theo cách thủ công. Bạn có thể giám sát tiến độ của tác vụ trong thuộc tính tác vụ.

Cách đặt mật khẩu bảo vệ kết nối với 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 **Tasks**.

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **Add**.

   Trình hướng dẫn Tác vụ sẽ được bắt đầu.

3. Cấu hình các thiết lập của tác vụ:

   a. Trong danh sách thả xuống **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.

   b. Trong danh sách thả xuống **Task type**, hãy chọn **Administration Server connection protection**.

c. Trong trường **Task name**, hãy nhập mô tả ngắn gọn, ví dụ: *Mật khẩu kết nối máy chủ chính*.

d. Trong phần **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. Chọn một tài khoản người dùng mặc định. 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.

   Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ.

7. Nhấn vào tác vụ **Administration Server connection protection** của Kaspersky Endpoint Security.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

8. Chọn thẻ **Application settings**.

9. Trong mục **Administration Server connection protection**, hãy chọn **Protect with a password**.

10. Trong danh sách thả xuống **Connection to the Administration Server**, hãy chọn **New password**.

11. Trong trường **Password for connection to the Administration Server**, hãy đặt mật khẩu kết nối với Máy chủ quản trị và xác nhận lại mật khẩu.

    Nếu quên mật khẩu, bạn có thể thay đổi mật khẩu bằng một tác vụ.

12. Nếu bạn đã triển khai Kaspersky Endpoint Security 12.7 hoặc phiên bản cũ hơn của ứng dụng, hãy chọn hộp kiểm **Enable password encryption compatibility for previous application versions (12.7 and lower)**.

    Kể từ Kaspersky Endpoint Security 12.8 cho Windows, ứng dụng này sử dụng mã hóa mật khẩu mạnh hơn. Nếu đã triển khai Kaspersky Endpoint Security 12.8 trở lên, bạn nên bỏ chọn hộp kiểm này và sử dụng mã hóa mật khẩu mạnh hơn. Các phiên bản trước của ứng dụng không hỗ trợ mã hóa mật khẩu mạnh. Để chạy tác vụ, bạn phải chọn hộp kiểm này.

13. Lưu các thay đổi của bạn.

14. Chọn hộp kiểm cạnh tác vụ.

15. Nhấn vào **Start**.

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 nối lại máy tính với Máy chủ quản trị khác

Quy trình kết nối lại máy tính với Máy chủ quản trị khác bao gồm các bước sau:

1. Trong bảng điều khiển của máy chủ `[KSC1]` hiện tại, hãy chạy tác vụ *Change Administration Server* cho Network Agent.

   Sau khi chạy xong tác vụ, máy tính sẽ được kết nối lại với máy chủ `[KSC2]` mới.

   Máy tính sẽ được hiển thị trong bảng điều khiển máy chủ `[KSC1]` với trạng thái *Critical*. Không thể cấu hình ứng dụng bằng các chính sách hoặc tác vụ chạy từ xa trên máy tính.

2. Trong bảng điều khiển của máy chủ [KSC2] mới, hãy tạo một tác vụ *Bảo vệ kết nối Máy chủ quản trị* mới cho Kaspersky Endpoint Security. Trong thuộc tính tác vụ, hãy nhập mật khẩu của máy chủ trước đó và đặt mật khẩu cho máy chủ mới.

Cách đặt mật khẩu mới để kết nối lại với máy chủ mới trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Tasks**.

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **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 (14.2)** → **Bảo vệ kết nối Máy chủ quản trị**.

Bước 2. Bảo vệ kết nối với Máy chủ quản trị

Đặt mật khẩu để bảo vệ kết nối đến Máy chủ quản trị mới:

1. Trong mục **Bảo vệ kết nối Máy chủ quản trị**, hãy chọn **Bảo vệ bằng mật khẩu**.

2. Trong danh sách thả xuống **Máy chủ quản trị**, hãy chọn **Kết nối lại từ máy chủ khác**.

3. Trong trường **Mật khẩu hiện tại**, hãy nhập mật khẩu đã đặt cho kết nối đến máy chủ được tin tưởng đã sử dụng trước đó.

4. Trong trường **Mật khẩu mới**, hãy đặt mật khẩu để kết nối với Máy chủ quản trị mới và xác nhận mật khẩu.

   Nếu quên mật khẩu, bạn có thể thay đổi mật khẩu bằng một tác vụ.

5. Nếu bạn đã triển khai Kaspersky Endpoint Security 12.7 hoặc phiên bản cũ hơn của ứng dụng, hãy chọn hộp kiểm **Bật khả năng tương thích mã hóa mật khẩu cho các phiên bản trước của ứng dụng (12.7 trở xuống)**.

   Kể từ Kaspersky Endpoint Security 12.8 cho Windows, ứng dụng này sử dụng mã hóa mật khẩu mạnh hơn. Nếu đã triển khai Kaspersky Endpoint Security 12.8 trở lên, bạn nên bỏ chọn hộp kiểm này và sử dụng mã hóa mật khẩu mạnh hơn. Các phiên bản trước của ứng dụng không hỗ trợ mã hóa mật khẩu mạnh. Để chạy tác vụ, bạn phải chọn hộp kiểm này.

Bước 3. Chọn tài khoản để chạy tác vụ

Chọn **Default account**. Theo mặc định, Kaspersky Endpoint Security sẽ khởi chạy tác vụ dưới quyền tài khoản người dùng hệ thống (SYSTEM).

Bước 4. Cấu hình lịch khởi chạy tác vụ

Trong mục **Scheduled start**, hãy chọn **Manually**.

Bước 5. Xác định tên tác vụ

Nhập tên cho tác vụ, ví dụ: *Mật khẩu kết nối máy chủ chính*.

Bước 6. Hoàn tất việc tạo tác vụ

Hoàn tất trình hướng dẫn. Chọn hộp kiểm **Run the task after the wizard finishes** hoặc chạy tác vụ theo cách thủ công. Bạn có thể giám sát tiến độ của tác vụ trong thuộc tính tác vụ.

Cách đặt mật khẩu mới để kết nối lại với máy chủ mới trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Tasks**.
   Danh sách tác vụ sẽ mở.
2. Nhấn vào **Add**.
   Trình hướng dẫn Tác vụ sẽ được bắt đầu.
3. Cấu hình các thiết lập của tác vụ:
   a. Trong danh sách thả xuống **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.
   b. Trong danh sách thả xuống **Task type**, hãy chọn **Administration Server connection protection**.
   c. Trong trường **Task name**, hãy nhập mô tả ngắn gọn, ví dụ: *Mật khẩu kết nối máy chủ chính*.
   d. Trong phần **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. Chọn một tài khoản người dùng mặc định. 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.
   Một tác vụ mới sẽ được hiển thị trong danh sách các tác vụ.
7. Nhấn vào tác vụ **Administration Server connection protection** của Kaspersky Endpoint Security.
   Cửa sổ thuộc tính tác vụ sẽ được mở ra.
8. Chọn thẻ **Application settings**.

9. Trong mục **Administration Server connection protection**, hãy chọn **Protect with a password**.

10. Trong danh sách thả xuống **Connection to the Administration Server**, hãy chọn **Reconnect from another server**.

11. Trong trường **Current password**, hãy nhập mật khẩu đã đặt cho kết nối đến máy chủ được tin tưởng đã sử dụng trước đó.

12. Trong trường **New password**, hãy đặt mật khẩu để kết nối với Máy chủ quản trị mới và xác nhận mật khẩu.

    Nếu quên mật khẩu, bạn có thể thay đổi mật khẩu bằng một tác vụ.

13. Nếu bạn đã triển khai Kaspersky Endpoint Security 12.7 hoặc phiên bản cũ hơn của ứng dụng, hãy chọn hộp kiểm **Enable password encryption compatibility for previous application versions (12.7 and lower)**.

    Kể từ Kaspersky Endpoint Security 12.8 cho Windows, ứng dụng này sử dụng mã hóa mật khẩu mạnh hơn. Nếu đã triển khai Kaspersky Endpoint Security 12.8 trở lên, bạn nên bỏ chọn hộp kiểm này và sử dụng mã hóa mật khẩu mạnh hơn. Các phiên bản trước của ứng dụng không hỗ trợ mã hóa mật khẩu mạnh. Để chạy tác vụ, bạn phải chọn hộp kiểm này.

14. Lưu các thay đổi của bạn.

15. Chọn hộp kiểm cạnh tác vụ.

16. Nhấn vào **Start**.

    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.

Sau khi hoàn thành tác vụ, đảm bảo rằng trong bảng điều khiển của máy chủ `[KSC2]` mới, máy tính có trạng thái *OK*🖥️. Kiểm tra xem bạn có thể chạy các tác vụ từ xa và cấu hình ứng dụng bằng các chính sách hay không.

Đặt lại mật khẩu của kết nối Máy chủ quản trị

Nếu bạn quên mật khẩu của kết nối Máy chủ quản trị hoặc mật khẩu bị xâm nhập, bạn có thể đặt lại mật khẩu trong thuộc tính tác vụ. Bạn cũng có thể đặt lại mật khẩu và đặt mật khẩu mới cho nhóm máy tính có các trạng thái bảo vệ kết nối Máy chủ quản trị khác nhau. Có nghĩa là, nếu một số máy tính đã bật chức năng bảo vệ và một số máy tính đã tắt tính năng này thì tác vụ sẽ đặt mật khẩu cho tất cả các máy tính.

> Bạn chỉ có thể đặt lại mật khẩu của kết nối Máy chủ quản trị trong bảng điều khiển của máy chủ được tin tưởng mà máy tính được kết nối.

Cách đặt lại mật khẩu của kết nối Máy chủ quản trị bằng Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.

2. Trong cây bảng điều khiển, hãy chọn **Tasks**.

3. Chọn tác vụ **Bảo vệ kết nối Máy chủ quản trị** và nhấn đúp để mở thuộc tính tác vụ.

4. Trong cửa sổ thuộc tính tác vụ, hãy chọn mục **Thiết lập**.
5. Trong mục **Bảo vệ kết nối Máy chủ quản trị**, hãy chọn **Bảo vệ và thay đổi mật khẩu**.
6. Trong trường **Mật khẩu để kết nối với Máy chủ quản trị**, hãy đặt mật khẩu mới để kết nối với máy chủ được tin tưởng hiện tại và xác nhận mật khẩu.
7. Lưu các thay đổi của bạn.
8. Chạy tác vụ.

Cách đặt lại mật khẩu kết nối của 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 **Tasks**.
   Danh sách tác vụ sẽ mở.
2. Nhấn vào tác vụ **Administration Server connection protection** của Kaspersky Endpoint Security.
   Cửa sổ thuộc tính tác vụ sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Trong mục **Administration Server connection protection**, hãy chọn **Protect and change password**.
5. Trong trường **Password for connection to the Administration Server**, hãy đặt mật khẩu mới để kết nối với máy chủ được tin tưởng hiện tại và xác nhận mật khẩu.
6. Lưu các thay đổi của bạn.
7. Chọn hộp kiểm cạnh tác vụ.
8. Nhấn vào **Start**.

Kết quả là mật khẩu của kết nối Máy chủ quản trị được đặt lại sau khi tác vụ kết thúc.

Tắt chức năng bảo vệ kết nối Máy chủ quản trị

Bạn chỉ có thể tắt từ xa chức năng bảo vệ kết nối Máy chủ quản trị trong bảng điều khiển của máy chủ được tin tưởng mà máy tính được kết nối. Bạn cũng có thể tắt chức năng bảo vệ theo cách cục bộ trên dòng lệnh.

Cách tắt chức năng bảo vệ kết nối máy chủ trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Tasks**.
3. Chọn tác vụ **Bảo vệ kết nối Máy chủ quản trị** và nhấn đúp để mở thuộc tính tác vụ.
4. Trong cửa sổ thuộc tính tác vụ, hãy chọn mục **Thiết lập**.

5. Trong mục **Bảo vệ kết nối Máy chủ quản trị**, hãy chọn **Không bảo vệ**.

6. Lưu các thay đổi của bạn.

7. Chạy tác vụ.

   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.

Cách tắt chức năng bảo vệ kết nối của 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 **Tasks**.

   Danh sách tác vụ sẽ mở.

2. Nhấn vào tác vụ **Administration Server connection protection** của Kaspersky Endpoint Security.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

3. Chọn thẻ **Application settings**.

4. Trong mục **Administration Server connection protection**, hãy chọn **Do not protect with a password**.

5. Lưu các thay đổi của bạn.

6. Chọn hộp kiểm cạnh tác vụ.

7. Nhấn vào **Start**.

   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.

Cách tắt chức năng bảo vệ kết nối của máy chủ trên 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 SERVERBINDINGDISABLE [/password=<password>]
   ```

   trong đó `<password>` là mật khẩu của tài khoản người dùng KLAdmin hoặc mật khẩu từ tác vụ *Bảo vệ kết nối Máy chủ quản trị*. Nếu không chỉ định tham số này, Kaspersky Endpoint Security sẽ nhắc bạn nhập mật khẩu ở dòng tiếp theo.

   > Để thực thi lệnh này, Bảo vệ bằng mật khẩu phải được bật.

Ví dụ

```
avp.com SERVERBINDINGDISABLE /password=samplePassword
```

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 Advanced Encryption Standard (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 Kaspersky Endpoint Security được cài đặt trên máy tính sử dụng kiến trúc Arm, chỉ có tính năng Mã hóa ổ đĩa BitLocker khả dụng. Ứng dụng này không hỗ trợ các thành phần mã hóa dữ liệu khác.

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 Trusted Platform Module (TPM), BitLocker sẽ sử dụng mô-đun đó 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 lôgic 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 *Quản lý tài khoản Authentication Agent*. Những tài khoản này đều dựa trên các tài khoản Microsoft Windows được người dùng sử dụng để đăng nhập vào hệ điều hành. Bạn 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. Lượt mã hóa đầu tiên bao gồm các khu vực chứa tập tin tại thời điểm mã hóa được bắt đầu. Lượt mã hóa thứ hai bao gồm các khu vực được ghi sau khi quá trình mã hóa được bắt đầu. Sau khi quá trình mã hóa được hoàn tất, tất cả các khu vực chứa dữ liệu đều sẽ được mã hóa.

Sau khi quá trình mã hóa được hoàn tất và người dùng xóa một tập tin, các khu vực chứa tập tin bị xóa sẽ có thể được sử dụng để lưu trữ thông tin mới ở cấp hệ thống tập tin, nhưng vẫn được mã hóa. Vì vậy, khi các tập tin 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.

- Nếu Kaspersky Endpoint Security được cài đặt trên máy tính sử dụng kiến trúc Arm thì chỉ có tính năng Mã hóa toàn bộ ổ đĩa bằng công nghệ BitLocker Drive Encryption là khả dụng, các thành phần mã hóa khác không được hỗ trợ.

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, IEEE1934, 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, và 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 ThinkCentre 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 10O
- 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 Encryption không được hỗ trợ trên các máy tính chạy trên kiến trúc Arm.

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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu → Mã hóa toàn bộ ổ đĩa**.
4. 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.

5. Trong danh sách thả xuống **Chế độ mã hóa**, hãy chọn **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.

6. Cấu hình tùy chọn Kaspersky Disk Encryption nâng cao (xem bảng bên dưới).
7. 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 **Asset management** → **Policies**.
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 **Data Encryption** → **Full Disk Encryption**.
5. Chọn công nghệ **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.

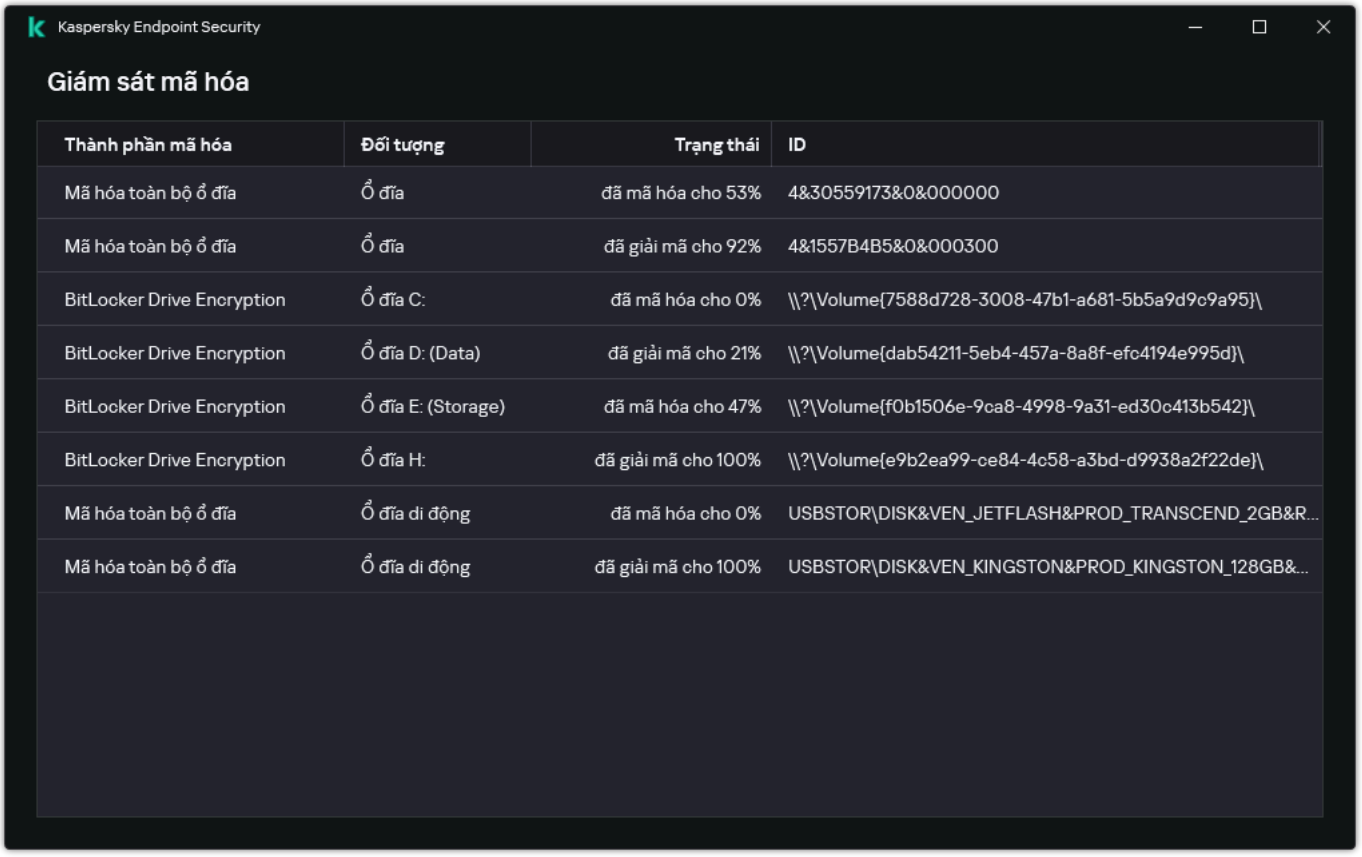
6. Trong mục **Action on devices**, hãy chọn **Encrypt all hard drives**.

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.

7. Cấu hình tùy chọn Kaspersky Disk Encryption nâng cao (xem bảng bên dưới).
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.



Giám sát mã hóa

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 Authentication Agent cho mọi người dùng của máy tính này sau khi đăng nhập	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 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 *Quản lý tài khoản Authentication Agent* cho máy tính có ổ đĩa đã được mã hóa.
Lưu tên người dùng đã nhập vào Authentication Agent	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.

Tham số	Mô tả
Chỉ mã hóa dung lượng ổ đĩa được sử dụng (giảm thời gian mã hóa)	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. Việc bật hoặc tắt tính năng **Chỉ mã hóa dung lượng ổ đĩa được sử dụng (giảm thời gian mã hóa)** 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. Theo mặc định, hộp kiểm này bị xóa.
Sử dụng Hỗ trợ USB chuẩn cũ (không khuyên dùng)	Hộp kiểm này bật hoặc tắt chức năng Legacy USB Support. *Hỗ trợ USB chuẩn cũ* **là** 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). Legacy USB Support không ảnh hưởng đến hỗ trợ cho các thiết bị USB sau khi hệ điều hành đã được khởi động. 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. Khi chức năng Legacy USB Support 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.

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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu → Mã hóa toàn bộ ổ đĩa**.
4. 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.

5. Để thêm ổ cứng vào danh sách các ổ cứng được loại trừ khỏi tác vụ mã hóa:

   a. Nhấn vào **Thêm**.

   b. Trong cửa sổ mở ra, hãy chỉ định các giá trị cho **Tên thiết bị**, **Máy tính**, **Kiểu ổ đĩa**, **Kaspersky Disk Encryption**.

   c. Nhấn vào **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 vào **OK**.

   Các ổ cứng được chọn sẽ xuất hiện trong bảng **Không mã hóa ổ đĩa cứng sau đây**.

6. 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Mã hóa toàn bộ ổ đĩa**.

4. 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**.

5. 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 nút → **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.

6. Để nhập danh sách quy tắc:

   a. Nhấn nút → **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.

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 **Asset management** → **Policies**.

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 **Data Encryption** → **Full Disk Encryption**.

   Chọn công nghệ **Kaspersky Disk Encryption**.

5. Nhấn vào liên kết **Exclusions**.

   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 nút → **Export**.

      Kaspersky Endpoint Security sẽ xuất danh sách các loại trừ vào tập tin JSON trong thư mục tải xuống mặc định.

7. Để nhập danh sách loại trừ:

   a. Nhấn nút → **Import**.

      Trong cửa sổ mở ra, hãy chọn tập tin JSON mà bạn muốn nhập danh sách các loại trừ.

   b. 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 JSON.

8. 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. Điều này có nghĩa là người dùng chỉ cần nhập mật khẩu một lần khi đăng nhập vào Windows (mật khẩu tài khoản Authentication Agent). Công nghệ Đăng nhập một lần cũng cho phép bạn tự động cập nhật mật khẩu tài khoản Authentication Agent khi mật khẩu tài khoản Windows được thay đổi.

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.

Bật công nghệ Đăng nhập một lần (SSO)

Cách bật sử dụng công nghệ Single Sign-On trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu → Thiết lập mã hóa chung**.
4. Trong mục **Thiết lập mật khẩu**, hãy nhấn nút **Thiết lập**.
5. Trong cửa sổ mở ra, trên thẻ **Authentication Agent**, chọn hộp kiểm **Sử dụng công nghệ Single Sign-On (SSO)**.
6. Nếu bạn đang sử dụng nhà cung cấp thông tin xác thực bên thứ ba, hãy chọn hộp kiểm **Chồng lên các nhà cung cấp dịch vụ thông tin xác thực bên thứ ba**.
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.

Cách bật sử dụng Single Sign-On trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Policies**.
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 **Data Encryption → Full Disk Encryption**.
5. Chọn công nghệ **Kaspersky Disk Encryption**.
6. Trong mục **Password settings**, hãy chọn hộp kiểm **Use Single Sign-On (SSO) technology**.

7. Nếu bạn đang sử dụng nhà cung cấp thông tin xác thực bên thứ ba, hãy chọn hộp kiểm **Wrap third-party credential providers**.

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.

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. Bạn chỉ cần thực hiện những hành động này một lần để đồng bộ hóa mật khẩu. Sau đó, Kaspersky Endpoint Security sẽ thay thế mật khẩu của tài khoản Authentication Agent bằng mật khẩu của tài khoản Windows. Khi mật khẩu tài khoản Windows được thay đổi, ứng dụng sẽ tự động cập nhật mật khẩu cho tài khoản Authentication Agent.

Nhà cung cấp dịch vụ thông tin xác thực bên thứ ba

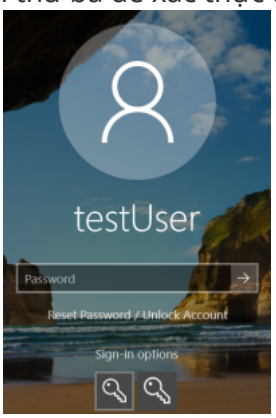
Kaspersky Endpoint Security hỗ trợ nhà cung cấp thông tin xác thực bên thứ ba ADSelfService Plus.

Khi làm việc với các nhà cung cấp dịch vụ thông tin xác thực bên thứ ba, Authentication Agent sẽ chặn mật khẩu trước khi hệ điều hành được nạp. Điều này có nghĩa là người dùng chỉ cần nhập mật khẩu một lần khi đăng nhập vào Windows. Sau khi đăng nhập vào Windows, người dùng có thể sử dụng các khả năng của nhà cung cấp dịch vụ thông tin xác thực bên thứ ba, ví dụ như để xác thực trong các dịch vụ của công ty. Các nhà cung cấp dịch vụ thông tin xác thực bên thứ ba cũng cho phép người dùng đặt lại mật khẩu của riêng họ một cách độc lập. Trong trường hợp này, Kaspersky Endpoint Security sẽ tự động cập nhật mật khẩu cho Authentication Agent.

Nếu đang sử dụng nhà cung cấp dịch vụ thông tin xác thực bên thứ ba không được ứng dụng hỗ trợ, bạn có thể gặp một số hạn chế trong hoạt động công nghệ Đăng nhập một lần. Khi đăng nhập vào Windows, người dùng sẽ có hai hồ sơ: nhà cung cấp dịch vụ thông tin xác thực trong hệ thống và nhà cung cấp dịch vụ thông tin xác thực bên thứ ba. Biểu tượng của các hồ sơ này sẽ giống hệt nhau (xem hình bên dưới). Người dùng sẽ có các tùy chọn sau để tiếp tục:

- Nếu người dùng chọn *nhà cung cấp dịch vụ thông tin xác thực bên thứ ba*, Authentication Agent sẽ không thể đồng bộ hóa mật khẩu với tài khoản Windows. Do đó, nếu người dùng đã thay đổi mật khẩu tài khoản Windows, Kaspersky Endpoint Security sẽ không thể cập nhật mật khẩu cho tài khoản Authentication Agent. Kết quả là người dùng cần thực hiện quy trình xác thực hai lần: trong giao diện của Authentication Agent và trước khi nạp hệ điều hành. Trong trường hợp này, người dùng có thể sử dụng các khả năng của nhà cung cấp dịch vụ thông tin xác thực bên thứ ba, ví dụ như để xác thực trong các dịch vụ của công ty.

- Nếu người dùng chọn *nhà cung cấp dịch vụ thông tin xác thực trong hệ thống*, Authentication Agent sẽ đồng bộ hóa mật khẩu với tài khoản Windows. Trong trường hợp này, người dùng không thể sử dụng các khả năng của nhà cung cấp bên thứ ba để xác thực trong các dịch vụ của công ty.



Hồ sơ xác thực hệ thống và hồ sơ xác thực của bên thứ ba để đăng nhập 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 *Manage Authentication Agent accounts* 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 *Manage Authentication Agent accounts*. 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 cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Tasks**.

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **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 (14.2)** → **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

Hoàn tất 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.

Cách tạo tác vụ Quản lý tài khoản Authentication Agent trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Tasks**.
   Danh sách tác vụ sẽ mở.
2. Nhấn vào **Add**.

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 **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.
2. Trong danh sách thả xuống **Task type**, hãy chọn **Manage Authentication Agent accounts**.
3. Trong trường **Task name**, hãy nhập một mô tả ngắn, ví dụ như *Tài khoản quản trị viên*.
4. Trong phần **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

Hoàn tất 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 **Start**.

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 *Manage Authentication Agent accounts*. 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)

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 **Tasks**.

   Danh sách tác vụ sẽ mở.

2. Nhấn vào tác vụ **Manage Authentication Agent accounts** của Kaspersky Endpoint Security.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

3. Chọn thẻ **Application settings**.

4. Trong danh sách các tài khoản Authentication Agent, hãy nhấn vào nút **Add** và chọn loại lệnh **Add account**.

5. 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 định danh bảo mật tài khoản (Security Identifier, 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.

6. 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.

   - **User name**. Tên người dùng mặc định của tài khoản Authentication Agent tương ứng với tên miền của người dùng.

   - **Allow password-based authentication**. 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.

   - **Allow certificate-based authentication**. 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.

   - **Comment**. Nếu cần, hãy nhập mô tả tài khoản.

7. Lưu các thay đổi của bạn.

8. Hãy chọn hộp kiểm cạnh tác vụ đó và nhấn nút **Start**.

   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 *Manage Authentication Agent accounts*. 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 **Tasks**.

   Danh sách tác vụ sẽ mở.

2. Nhấn vào tác vụ **Manage Authentication Agent accounts** của Kaspersky Endpoint Security.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.

3. Chọn thẻ **Application settings**.

4. Trong danh sách các tài khoản Authentication Agent, hãy nhấn vào nút **Add** và chọn loại lệnh **Edit account**.

5. 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 định danh bảo mật tài khoản (Security Identifier, 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.

6. Chọn các hộp kiểm cạnh thiết lập bạn muốn chỉnh sửa.

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.

   - **User name**. Tên người dùng mặc định của tài khoản Authentication Agent tương ứng với tên miền của người dùng.

   - **Allow password-based authentication**. 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.

   - **Allow certificate-based authentication**. 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.

   - **Comment**. 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 **Start**.

Để xóa tài khoản Authentication Agent, bạn cần thêm một lệnh đặc biệt vào tác vụ *Manage Authentication Agent accounts*. 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 **Tasks**.

   Danh sách tác vụ sẽ mở.
2. Nhấn vào tác vụ **Manage Authentication Agent accounts** của Kaspersky Endpoint Security.

   Cửa sổ thuộc tính tác vụ sẽ được mở ra.
3. Chọn thẻ **Application settings**.
4. Trong danh sách các tài khoản Authentication Agent, hãy nhấn vào nút **Add** và chọn loại lệnh **Remove account**.
5. 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.
6. Lưu các thay đổi của bạn.
7. Hãy chọn hộp kiểm cạnh tác vụ đó và nhấn nút **Start**.

   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 cây bảng điều khiển, hãy chọn **Devices**.
3. Nhấn đúp để mở cửa sổ thuộc tính máy tính.
4. Trong cửa sổ thuộc tính máy tính, chọn phần **Tasks**.
5. Trong danh sách tác vụ, hãy chọn **Quản lý tài khoản Authentication Agent** và mở thuộc tính tác vụ bằng cách nhấn đúp.
6. 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.

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Assets (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 **Tasks**.
4. Trong danh sách tác vụ, hãy chọn **Manage Authentication Agent accounts**.
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 kể cả khi không có giấy phép hiện tại cho phép mã hóa dữ liệu.

Để giải mã các ổ cứng:

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu → Mã hóa toàn bộ ổ đĩa**.

4. Trong danh sách thả xuống **Công nghệ mã hóa**, chọn công nghệ đã được sử dụng để mã hóa ổ cứng.

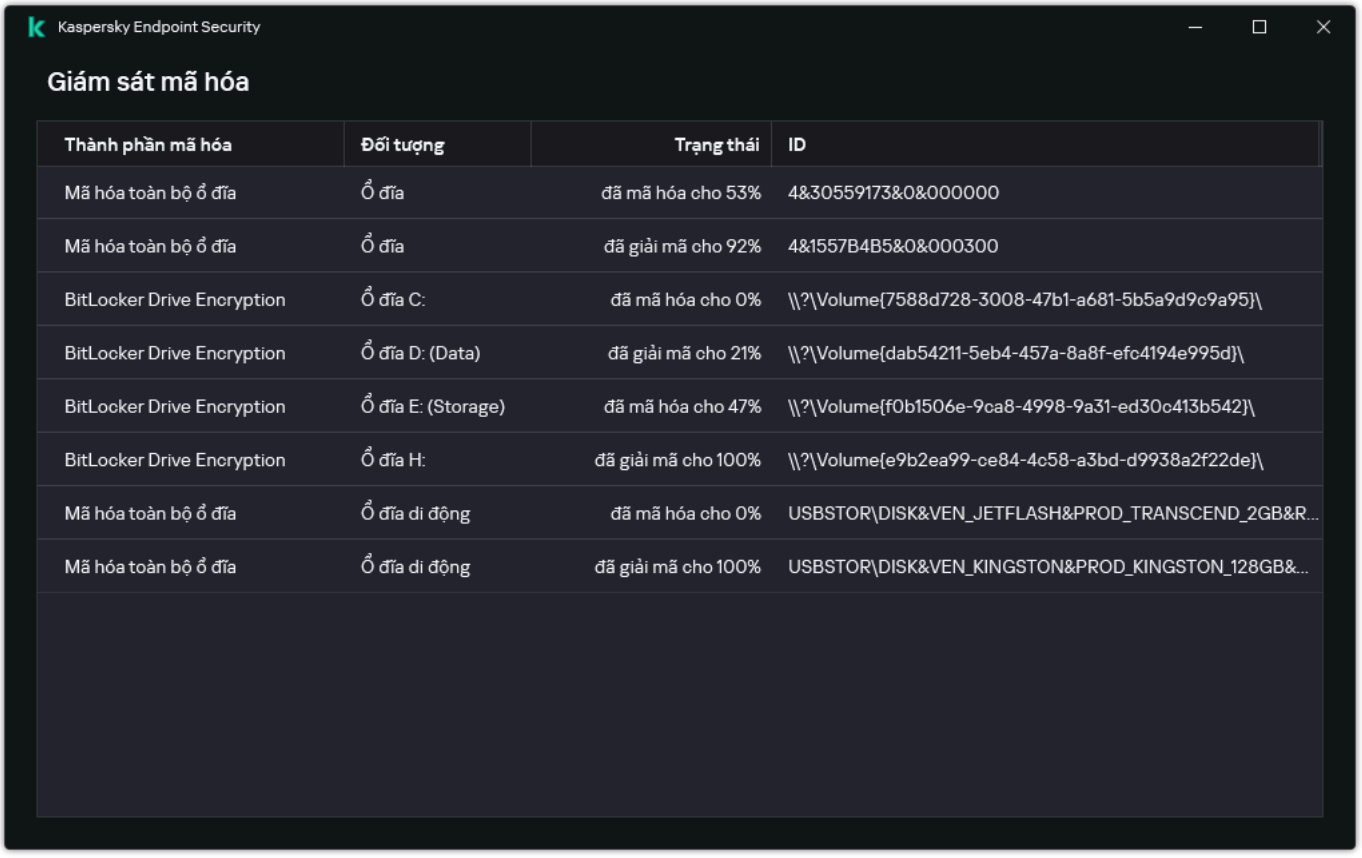
5. Thực hiện một trong các thao tác sau:

   - 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.

6. 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.



Giám sát mã hóa

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.

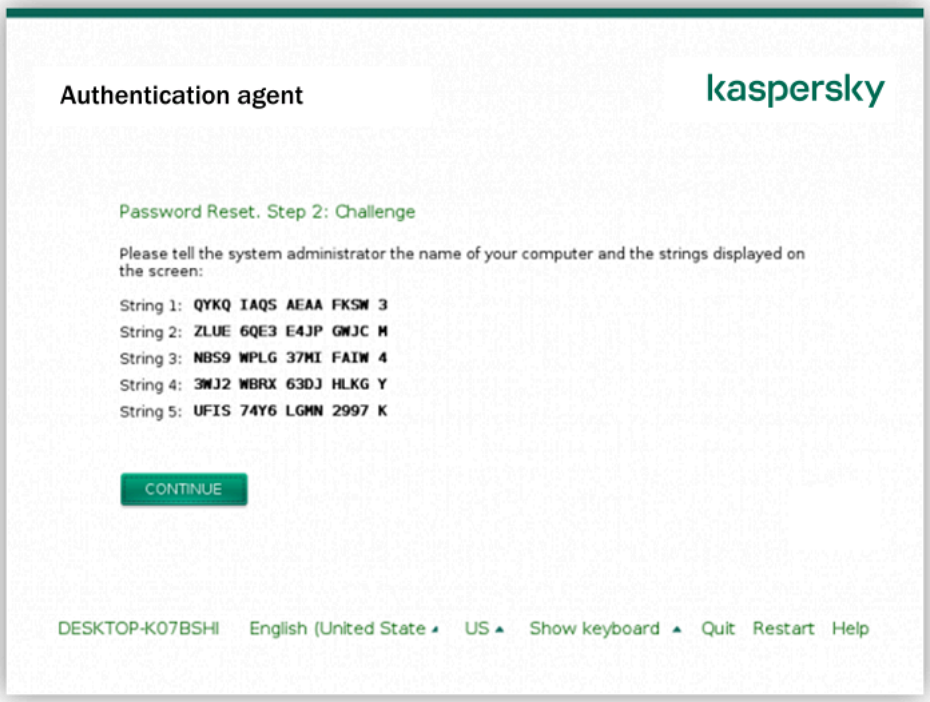
Khôi phục quyền truy cập vào ổ đĩa được bảo vệ bởi công nghệ Kaspersky Disk Encryption

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 cây bảng điều khiển, hãy chọn **Devices**.

3. 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.

4. Trong menu ngữ cảnh, hãy chọn **Cấp quyền truy cập trong chế độ ngoại tuyến**.

5. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy chọn thẻ **Authentication Agent**.

6. Trong mục **Thuật toán mã hóa được sử dụng**, hãy chọn thuật toán mã hóa: **AES56** hoặc **AES256**.

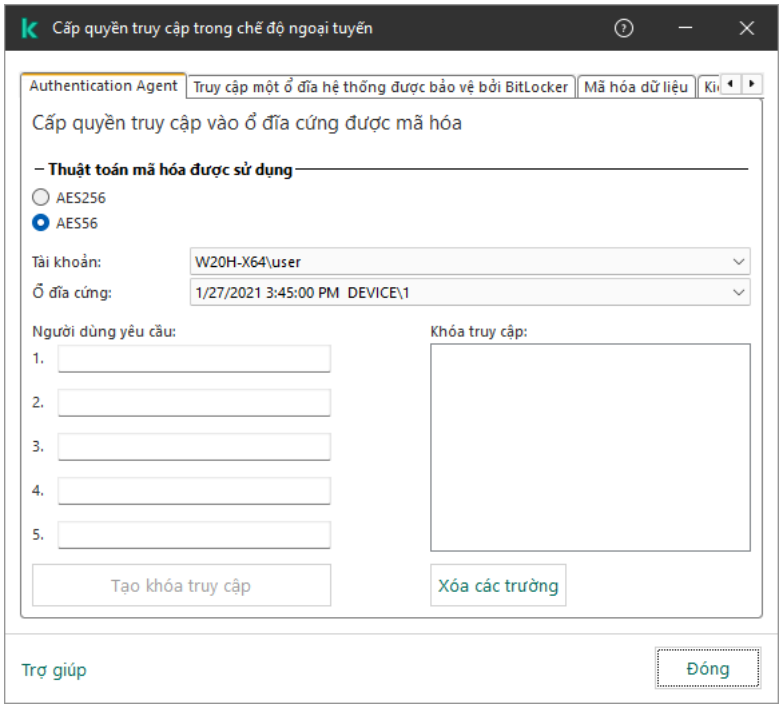
   Thuật toán mã hóa dữ liệu phụ thuộc vào thư viện mã hóa AES, được kèm theo gói phân phối: *Strong encryption (AES256)* hoặc *Lite encryption (AES56)*. Thư viện mã hóa AES được cài đặt cùng với ứng dụng.

7. 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.

8. Trong danh sách thả xuống **Ổ đĩa cứng**, chọn ổ cứng được mã hóa mà bạn cần khôi phục truy cập.

9. 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.



Cấp quyền truy cập trong chế độ ngoại tuyến

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 **Asset management** → **Assets (Devices)**.
2. Chọn hộp kiểm cạnh tên của máy tính có ổ đĩa mà bạn muốn khôi phục quyền truy cập.
3. Nhấn vào **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 **Account**, 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.

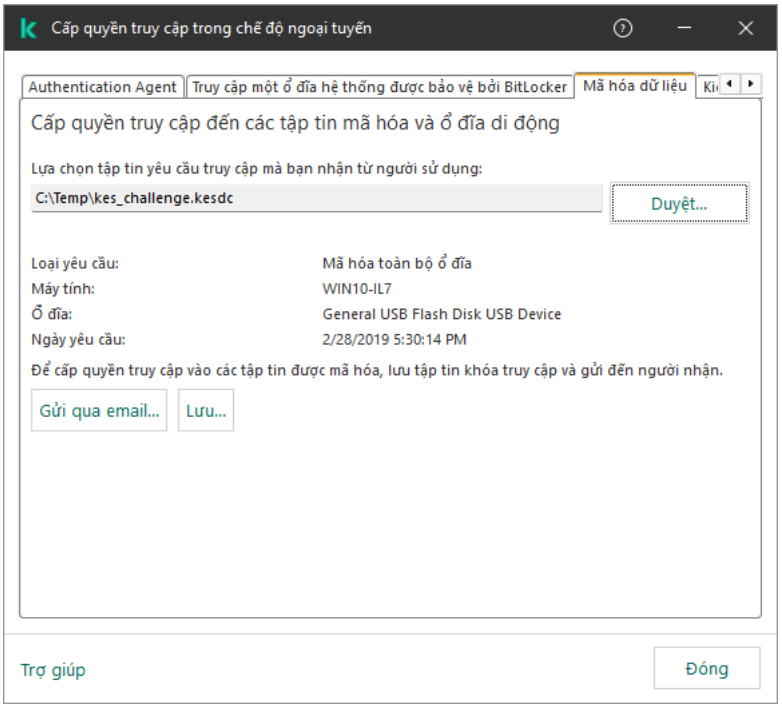
Cách lấy tập tin khóa truy cập cho ổ đĩa cứng không thuộc hệ thống được mã hóa trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Devices**.
3. 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.
4. Trong menu ngữ cảnh, hãy chọn **Cấp quyền truy cập trong chế độ ngoại tuyến**.
5. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy chọn thẻ **Mã hóa dữ liệu**.

6. Trên thẻ **Mã hóa dữ liệu**, hãy nhấn nút **Duyệt**.

7. 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.



Cấp quyền truy cập trong chế độ ngoại tuyến

Cách lấy tập tin khóa truy cập ổ đĩa cứng không thuộc hệ thống được mã hóa trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Assets (Devices)**.

2. Chọn hộp kiểm bên cạnh tên của máy tính có dữ liệu bạn muốn khôi phục quyền truy cập.

3. Nhấn vào **Grant access to the device in offline mode**.

4. Chọn **Data Encryption**.

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 cây bảng điều khiển, hãy chọn **Devices**.
3. Nhấn đúp để mở cửa sổ thuộc tính máy tính.
4. Trong cửa sổ thuộc tính máy tính, chọn phần **Tasks**.
5. Trong danh sách tác vụ, hãy chọn **Quản lý tài khoản Authentication Agent** và mở thuộc tính tác vụ bằng cách nhấn đúp.
6. Trong cửa sổ thuộc tính tác vụ, hãy chọn mục **Thiết lập**.
7. Trong danh sách tài khoản, hãy chọn tài khoản dịch vụ Authentication Agent (ví dụ: `WIN10-USER\ServiceAccount`).
8. Trong danh sách thả xuống **Hành động**, hãy chọn **Xem tài khoản**.
9. Trong thuộc tính tài khoản, hãy chọn hộp kiểm **Hiển thị mật khẩu ban đầu**.
10. 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 **Asset management → Assets (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 **Tasks**.
4. Trong danh sách tác vụ, hãy chọn **Manage Authentication Agent accounts**.
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 **Show password**.
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.

Các tính năng của bản cập nhật hệ điều hành:

- **Cập nhật HĐH thông qua WSUS**. Bạn có thể cập nhật hệ điều hành theo cách thông thường.
- **Cập nhật HĐH từ tập tin ISO**. Để cập nhật hệ điều hành, bạn phải chỉ định thư mục chứa trình điều khiển mã hóa đĩa Kaspersky. Ứng dụng sẽ tự động sao chép trình điều khiển vào một thư mục riêng. Làm các bước sau:

  1. Gắn tập tin ảnh ISO.
  2. Bắt đầu cài đặt bản cập nhật hệ thống bằng khóa sau:

     ```
     setup.exe /ReflectDrivers %ProgramFiles(x86)%\Kaspersky Lab\KES.14.2\reflect_drivers
     ```

Tính năng cập nhật HĐH tự động chỉ khả dụng nếu máy tính đang chạy Windows 10 1607 (RS1) trở lên. Để nâng cấp các phiên bản hệ điều hành cũ hơn, bạn nên giải mã ổ đĩa trước, thực hiện nâng cấp HĐH rồi mã hóa ổ đĩa.

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 14.2.

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,

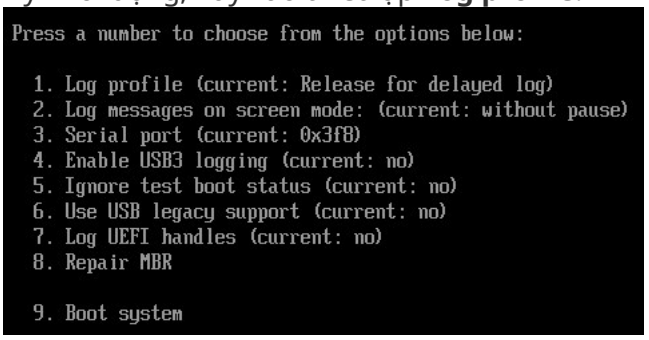
khôi phục quyền truy cập đến các thiết bị được mã hóa sử dụng Tiện ích khôi phục.

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.

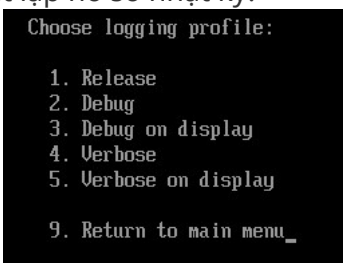
Để bật truy vết Authentication Agent:

1. Bật truy vết của Kaspersky Endpoint Security.
2. Khởi động lại máy tính.
3. 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.
4. Sau khi bộ nạp khởi động FDE khởi chạy, hãy chọn trình quản lý khởi động **KES (FDE <version>)**.
5. Trong menu của trình quản lý khởi động, hãy vào thiết lập **Log profile**.



Menu của trình quản lý khởi động

6. Chọn cấp độ truy vết trong cửa sổ thiết lập hồ sơ nhật ký:



Các cấp độ truy vết của Authentication Agent

- **Release**. Nếu chọn tùy chọn này, ứng dụng sẽ không ghi lại thông tin về các sự kiện Authentication Agent trong tập tin dấu vết.
- **Debug**. 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.
- **Debug on display**. 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.
- **Verbose**. 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.

  > Mức độ chi tiết của các mục trong tùy chọn này cao hơn so với mức độ của tùy chọn **Debug**. Một cấp độ chi tiết cao có thể làm chậm việc khởi động của Authentication Agent và hệ điều hành.
- **Verbose on display**. 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.

  > Mức độ chi tiết của các mục trong tùy chọn này cao hơn so với mức độ của tùy chọn **Debug on display**. Một cấp độ chi tiết cao có thể làm chậm việc khởi động của Authentication Agent và hệ điều hành.

Sau khi bạn chọn cấp độ truy vết, trình quản lý khởi động sẽ hiển thị lại menu.

7. Trong menu của trình quản lý khởi động, hãy chọn **Boot system**.

   Bộ tải khởi động FDE sẽ khởi chạy Authentication Agent.

   Tái diễn sự cố.

   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.

8. Để dừng truy vết tiến trình, hãy quay lại cửa sổ Công cụ hỗ trợ và tắt truy vết.

Kết quả là các tập tin dấu vết hoạt động KES.SRV của Authentication Agent sẽ được tạo trong thư mục `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu → Thiết lập mã hóa chung**.
4. Trong mục **Mẫu**, hãy nhấn nút **Trợ giúp**.
5. 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.
6. 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.
7. 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 sử dụng một Tiện ích khôi phục và xóa các đối tượng và dữ liệu còn sót lại sau hoạt động thử nghiệm của Authentication Agent:

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 cần thiết.

3. Nhấn vào **Quét**.

4. Nếu sau khi chẩn đoán ổ cứng hệ thống, bạn nhận được thông báo cho biết vẫn còn các đối tượng và dữ liệu từ quá trình kiểm tra của Tác nhân xác thực, hãy nhấn vào **Xóa các đối tượng AA và dữ liệu**.

   Nút **Xóa các đối tượng AA và dữ liệu** chỉ khả dụng nếu phát hiện thấy các đối tượng và dữ liệu còn lại sau khi thực hiện thao tác kiểm thử của Tác nhân xác thực.

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 cơ sở hạ tầng của Kaspersky Next. 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.

Khi mã hóa ổ đĩa, BitLocker sẽ đặt bộ tải khởi động và các tập tin phụ khác vào system partition. Phân vùng này không được mã hóa. Hệ điều hành sẽ tự động tạo phân vùng hệ thống trong quá trình cài đặt Windows. Nếu ổ đĩa được phân vùng đầy đủ trước khi cài đặt Windows, hệ điều hành không thể tạo phân vùng hệ thống. Trong trường hợp này, khi bạn tiến hành mã hóa đĩa BitLocker, hệ điều hành sẽ nhắc bạn phân vùng lại đĩa và tạo một phân vùng hệ thống. Sau khi tạo phân vùng hệ thống, hệ điều hành sẽ tiến hành mã hóa BitLocker.

Thuật toán mã hóa BitLocker không phụ thuộc vào phiên bản Thư viện AES kèm theo gói phân phối (AES256 hoặc AES56). Quá trình mã hóa sử dụng thư viện mã hóa tích hợp của hệ điều hành.

Theo mặc định, ứng dụng sử dụng thuật toán mã hóa BitLocker với độ dài khóa hiệu quả là 256 bit để mã hóa các thiết bị chưa từng được mã hóa trước đó. Đối với thiết bị đã được mã hóa trước khi cài đặt ứng dụng, thuật toán mã hóa có thể sẽ khác. Để biết thông tin chi tiết về cách chọn thuật toán mã hóa, vui lòng tham khảo Trang web hỗ trợ kỹ thuật của Microsoft. Kể từ phiên bản 12.9, Kaspersky Endpoint Security sẽ gửi khóa khôi phục gốc cho các thiết bị đã được các ứng dụng của bên thứ ba mã hóa trước đó đến Kaspersky Security Center.

BitLocker cung cấp ổ lưu trữ an toàn các khóa truy cập bằng mô-đun nền tảng được tin tưởng. *Trusted Platform Module* (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 cứng hệ thống, người dùng cần thực hiện xác thực BitLocker để khởi động hệ điều hành. Sau khi xác thực, BitLocker sẽ cho phép người dùng đăng nhập. BitLocker không hỗ trợ công nghệ đăng nhập một lần (SSO).

Sau khi mã hóa ổ đĩa, BitLocker sẽ tạo khóa khôi phục. Kaspersky Endpoint Security sẽ gửi khóa khôi phục 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 khóa khôi phục và thông tin về mã hóa ổ đĩa đến Kaspersky Security Center.

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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu → Mã hóa toàn bộ ổ đĩa**.
4. Trong danh sách thả xuống **Công nghệ mã hóa**, hãy chọn **BitLocker Drive Encryption**.

5. Trong danh sách thả xuống **Chế độ mã hóa**, hãy chọn **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.

6. Cấu hình tùy chọn BitLocker Drive Encryption nâng cao (xem bảng bên dưới).
7. Lưu các thay đổi của bạn.

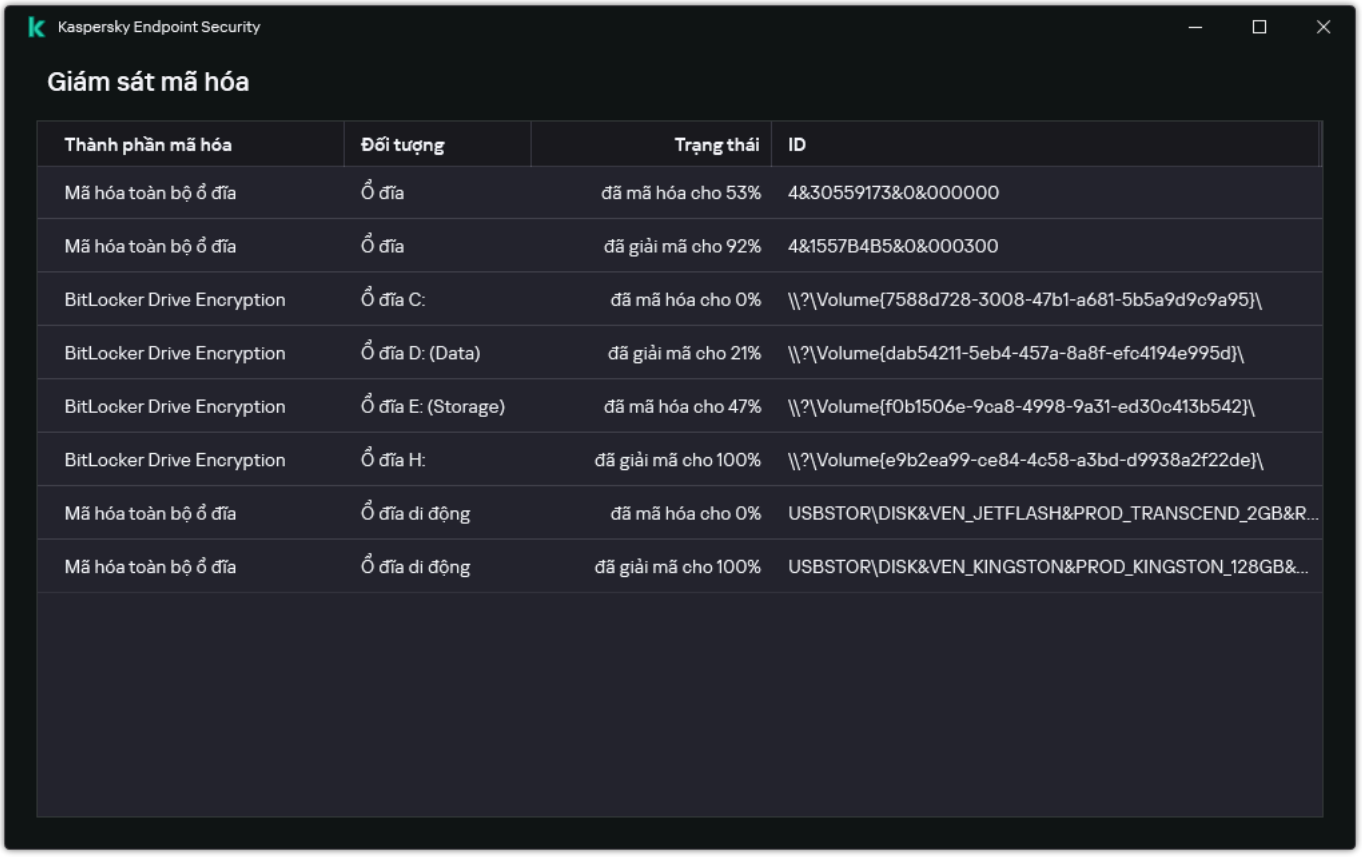
Cách chạy BitLocker Drive Encryption thông qua Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Data Encryption** → **Full Disk Encryption**.
5. Chọn công nghệ **BitLocker Disk Encryption**.
6. Trong mục **Action on devices**, hãy chọn **Encrypt all hard drives**.

> 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.

7. Cấu hình tùy chọn BitLocker Drive Encryption nâng cao (xem bảng bên dưới).
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.



Giám sát mã hóa

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
Cần nhập liệu bàn phím trong quá trình tiền khởi động để bật xác thực BitLocker trên máy tính bảng	Sử dụng 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). 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. 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. Nếu hộp kiểm bị xóa thì BitLocker Drive Encryption không khả dụng trên máy tính bảng.
Sử dụng mã hóa phần cứng (Windows 8 và các phiên bản mới hơn)	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.
Chỉ mã hóa dung lượng ổ đĩa được sử dụng (Windows 8 và các phiên bản mới hơn)	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. Việc bật hoặc tắt tính năng **Chỉ mã hóa dung lượng ổ đĩa được sử dụng (giảm thời gian mã hóa)** 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. Theo mặc định, hộp kiểm này bị xóa.

Tham số	Mô tả
Phương thức xác thực	**Chỉ 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. **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). *Trusted Platform Module* (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: • **Sử dụng mã PIN cho TPM**. Nếu hộp kiểm này được chọn, người dùng có thể sử dụng 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. • **Mô-đun nền tảng tin tưởng (TPM), hoặc mật khẩu nếu TPM không khả dụng**. Nếu chọn tùy chọn này, 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. Phương thức xác thực đã chọn phải được cấu hình bằng cách chỉ định các yêu cầu về mật khẩu hoặc mã PIN: • **Độ dài tối thiểu của mã PIN (ký tự)** (giá trị mặc định là 6). • **Độ dài mật khẩu tối thiểu (ký tự)** (giá trị mặc định là 8). • **Số lượng tối đa mật khẩu / mã PIN được lưu trữ** (giá trị mặc định là 5). • **Giới hạn thời gian hiệu lực của mật khẩu/mã PIN cho TPM (ngày)** (bị tắt theo mặc định). • **Sử dụng mã PIN tăng cường (chứa chữ và số)**. *Mã PIN cải tiến* cho phép sử dụng các ký tự khác ngoài ký tự số: chữ cái La-tinh viết hoa và viết thường, ký tự đặc biệt và dấu cách. Bị tắt theo mặc định.
Tự động tạo lại khóa khôi phục (ngày)	Tự động cập nhật mật khẩu thành khôi phục quyền truy cập ổ đĩa được bảo vệ bằng BitLocker. Nếu hộp kiểm được chọn, hãy chỉ định khoảng thời gian hiệu lực của mật khẩu khóa khôi phục. Điều này giúp ngăn sử dụng lại mật khẩu khóa khôi phục.

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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu → Mã hóa toàn bộ ổ đĩa**.
4. Trong danh sách thả xuống **Công nghệ mã hóa**, hãy chọn **BitLocker Drive Encryption**.

5. Trong danh sách thả xuống **Chế độ mã hóa**, hãy chọn **Giải mã tất cả đĩa cứng**.

6. 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 **Asset management → Policies**.

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**.

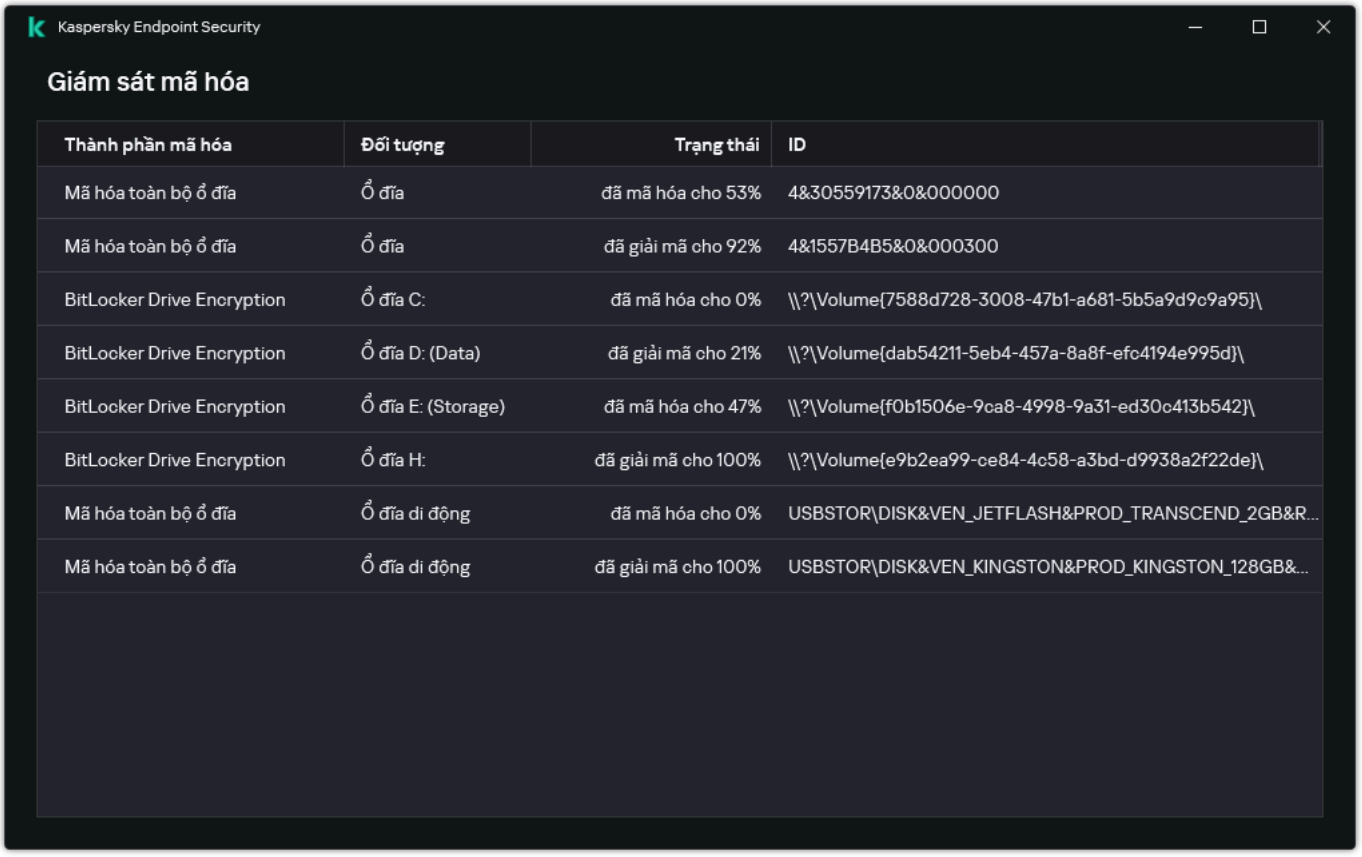
4. Vào **Data Encryption → Full Disk Encryption**.

5. Chọn công nghệ **BitLocker Disk Encryption**.

6. Trong mục **Action on devices**, hãy chọn **Decrypt all hard drives**.

7. 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.



Giám sát mã hóa

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.

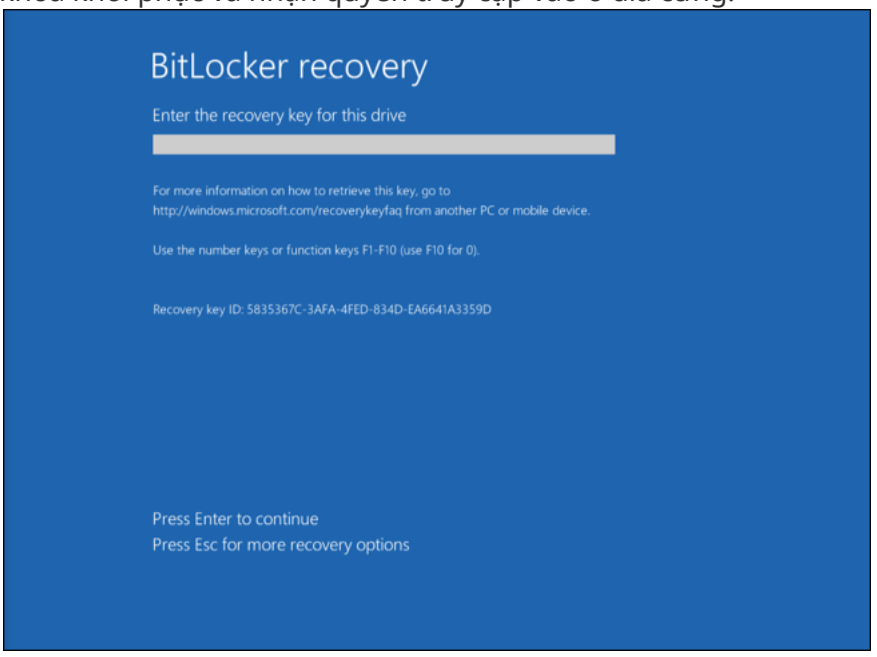
   Tập tin khóa khôi phục được sử dụng cho các máy tính chạy các hệ điều hành sau:

   - 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.

   Để ngăn sử dụng lại mật khẩu khóa khôi phục, bạn có thể cấu hình cập nhật mật khẩu tự động trong thiết lập chính sách.

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

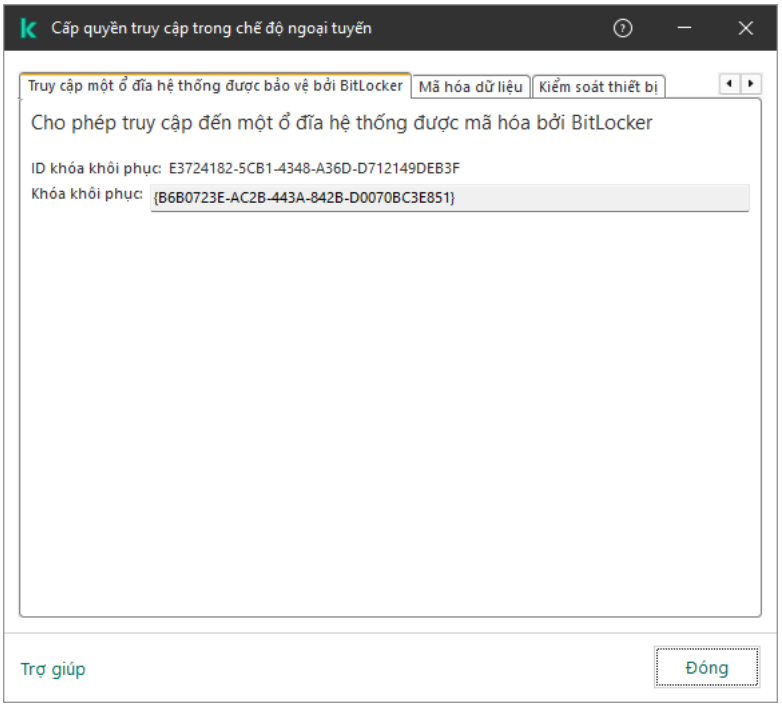
Để bắt đầu quy trình khôi phục, người dùng cần nhấn phím **Esc** ở giai đoạn xác thực tiền khởi động.

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 cây bảng điều khiển, hãy chọn **Managed devices**.
3. 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.
4. Trong menu ngữ cảnh, hãy chọn **Cấp quyền truy cập trong chế độ ngoại tuyến**.
5. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy chọn thẻ **Truy cập một ổ đĩa hệ thống được bảo vệ bởi BitLocker**.
6. 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 khôi phục**.

> 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.



Khôi phục quyền truy cập vào ổ đĩa được mã hóa bằng BitLocker

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 **Asset management** → **Assets (Devices)**.
2. Chọn hộp kiểm cạnh tên của máy tính có ổ đĩa mà bạn muốn khôi phục quyền truy cập.
3. Nhấn vào **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 vào **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 khôi phục 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

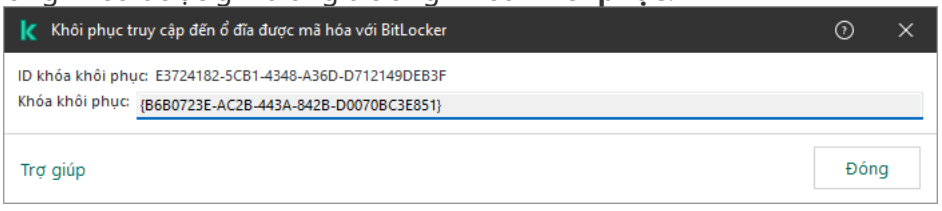
Để bắt đầu quy trình khôi phục, người dùng cần nhấn vào liên kết **Forgot your password** trong cửa sổ cung cấp quyền truy cập vào ổ đĩa. Sau khi có quyền truy cập vào ổ đĩa được mã hóa, người dùng có thể kích hoạt tự động mở khóa ổ đĩa trong khi xác thực Windows trong thiết lập của BitLocker.

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 **Advanced** → **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 thiết bị trong Kaspersky Endpoint Security**.
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 khôi phục**.

   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 khôi phục**.



Khôi phục quyền truy cập vào ổ đĩa được mã hóa bằng BitLocker

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 **Operations** → **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 vào **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 for 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 vào **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 cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Tasks**.

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **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 (14.2)** → **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

Hoàn tất 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 **Asset management → Tasks**.

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **Add**.

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 **Application**, hãy chọn **Kaspersky Endpoint Security cho Windows**.
2. Trong danh sách thả xuống **Task type**, hãy chọn **BitLocker Protection Management**.
3. Trong trường **Task name**, nhập một mô tả ngắn, ví dụ như *Cập nhật lên Windows 10*.
4. Trong phần **Devices to which the task will be assigned**, chọn phạm vi tác vụ.

Bước 2. Quản lý bảo vệ bằng BitLocker

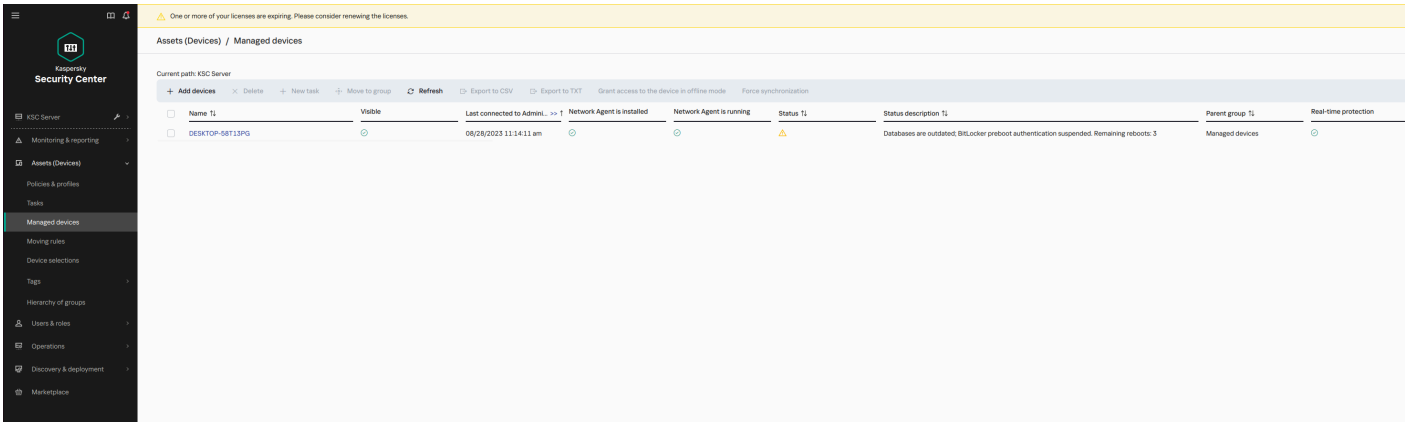
Cấu hình xác thực BitLocker. Để tạm dừng bảo vệ bằng BitLocker, hãy chọn **Temporarily allow skipping BitLocker authentication** và nhập số lần khởi động lại mà không cần xác thực BitLocker (1 đến 15 lần). Nếu cần, hãy nhập ngày và giờ hết hạn cho tác vụ. Tại thời điểm được chỉ định, tác vụ sẽ tự động 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

Hoàn tất 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 **Start**.

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 xem số lần khởi động lại còn lại trong thư mục **Managed devices** của bảng điều khiển Kaspersky Security Center trong phần mô tả trạng thái thiết bị.



Danh sách các thiết bị được quản lý

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

Mã hóa tập tin không được hỗ trợ trên các máy tính chạy trên kiến trúc Arm.

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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Data Encryption → File Level Encryption**.
4. Trong danh sách thả xuống **Chế độ mã hóa**, hãy chọn **Theo các quy tắc**.
5. 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.

   - **Tài liệu**. 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.

     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.

   - **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.

6. 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

Theo mặc định, tất cả các ứng dụng đều hoạt động với các tập tin được mã hóa ở trạng thái được giải mã. Nếu bạn thường xuyên sử dụng một số ứng dụng nhất định (ví dụ: trình duyệt hoặc trình soạn thảo văn bản), bạn có thể tạo các quy tắc truy cập tập tin được mã hóa để bảo vệ thông tin.

Bạn nên tạo quy tắc truy cập tập tin được mã hóa cho trình duyệt Microsoft Internet Explorer và Microsoft Edge. Do cách thức hoạt động của các trình duyệt này, nếu bạn tải tập tin được mã hóa lên một trang web (ví dụ: ổ lưu trữ đám mây), tập tin đó sẽ tự động được giải mã. Điều này có thể gây rò rỉ dữ liệu. Không thể tải lên tập tin được mã hóa bằng các trình duyệt này. Bạn nên thiết lập quy tắc **Chỉ cấp quyền truy cập vào các tập tin được mã hóa ở dạng bản mã**. Bạn không cần phải tạo quy tắc cho các trình duyệt khác (như Google Chrome).

Để tạo quy tắc truy cập tập tin được mã hóa cho ứng dụng:

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Data Encryption → File Level Encryption**.
4. 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.

5. Ở phần bên phải của cửa sổ, chọn thẻ **Quy tắc cho các ứng dụng**.
6. 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 thực hiện, hãy 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 **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 xuất hiện trong bảng trên thẻ **Quy tắc cho các ứng dụng**.

7. 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 xuất hiện trong bảng trên thẻ **Quy tắc cho các ứng dụng**.

8. 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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Data Encryption → File Level Encryption**.

4. 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.

5. Ở phần bên phải của cửa sổ, chọn thẻ **Quy tắc cho các ứng dụng**.

6. 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 thực hiện, hãy 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 **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**, hãy 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 các ứng dụng**.

7. 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**, hãy 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 các ứng dụng**.

8. Lưu các thay đổi của bạn.

Tạo một quy tắc giải mã

Để tạo một quy tắc giải mã:

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Data Encryption → File Level Encryption**.

4. Trong danh sách thả xuống **Chế độ mã hóa**, hãy chọn **Theo các quy tắc**.

5. Trên thẻ **Giải mã**, nhấn nút **Thêm**, và trong danh sách thả xuống chọn một trong các đề mục sau:

   a. Chọn mục **Các thư mục được xác định trước** để thêm tập tin từ các thư mục của hồ sơ người dùng cục bộ theo khuyến nghị của các chuyên gia Kaspersky vào quy tắc giải mã.

   b. Chọn đề mục **Thư mục tùy chỉnh** để thêm một đường dẫn thư mục được nhập thủ công vào quy tắc giải mã.

   c. 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.

   d. 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.

6. 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:

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Data Encryption → File Level Encryption**.

4. Ở phần bên phải của cửa sổ, chọn thẻ **Mã hóa**.

5. 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 **Xóa**.

   Các tập tin và thư mục được xóa khỏi danh sách mã hóa sẽ tự động được thêm vào danh sách giải mã.

6. Tạo một danh sách giải mã tập tin.

7. 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`.

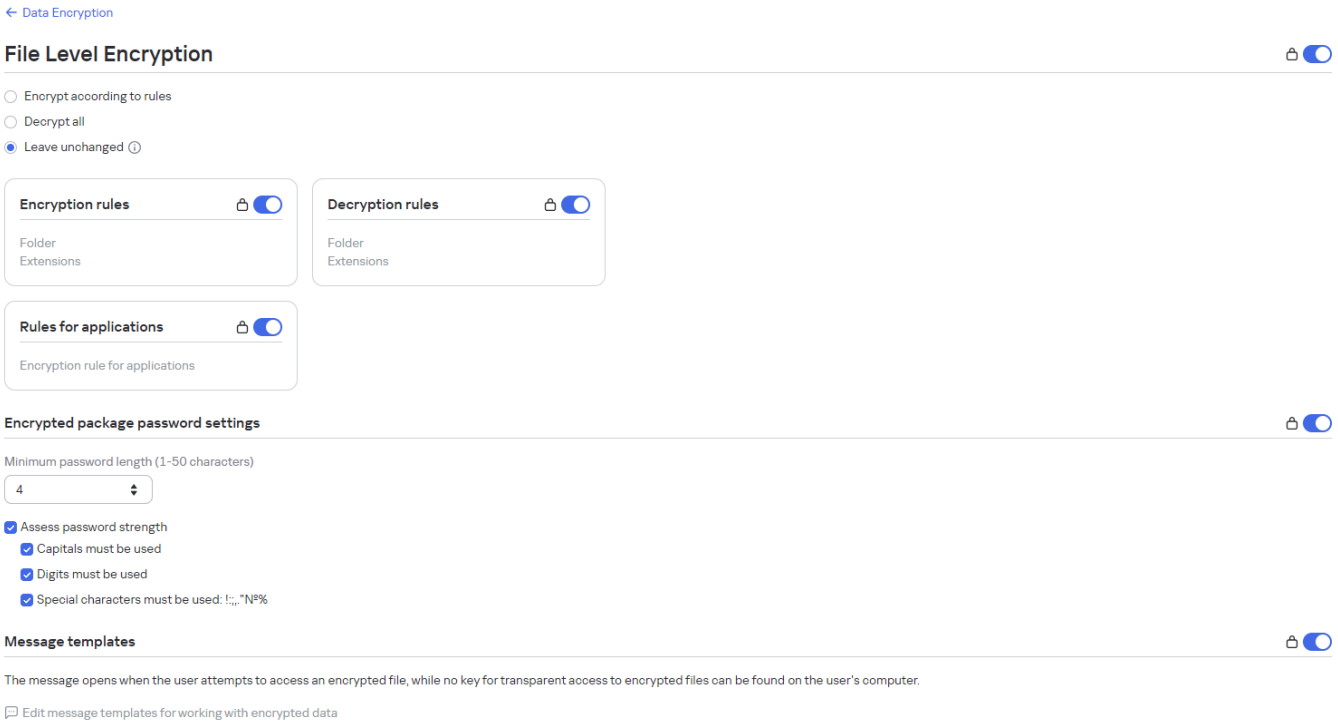
Cách bật kiểm tra độ mạnh mật khẩu khi tạo một các tập tin nén được mã hóa trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Thiết lập mã hóa chung**.
4. Trong mục **Thiết lập mật khẩu**, hãy nhấn nút **Thiết lập**.
5. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy chọn thẻ **Gói mã hóa**.
6. 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 **Asset management** → **Policies**.
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 **Data Encryption** → **File Level Encryption**.

5. Trong mục **Encrypted package password settings**, hãy cấu hình tiêu chí độ mạnh mật khẩu cần thiết khi tạo các gói được mã hóa.



Thiết lập Mã hóa tập tin

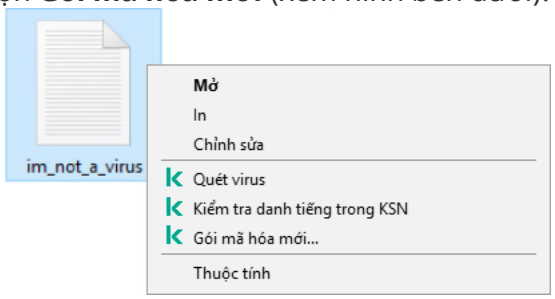
Bạn có thể tạo các gói mã hóa trên các máy tính được cài đặt Kaspersky Endpoint Security khi có tính năng Mã hóa mức độ tập tin.

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).



Tạo một gói mã hóa

3. 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.

4. Nhấn vào **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.

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.

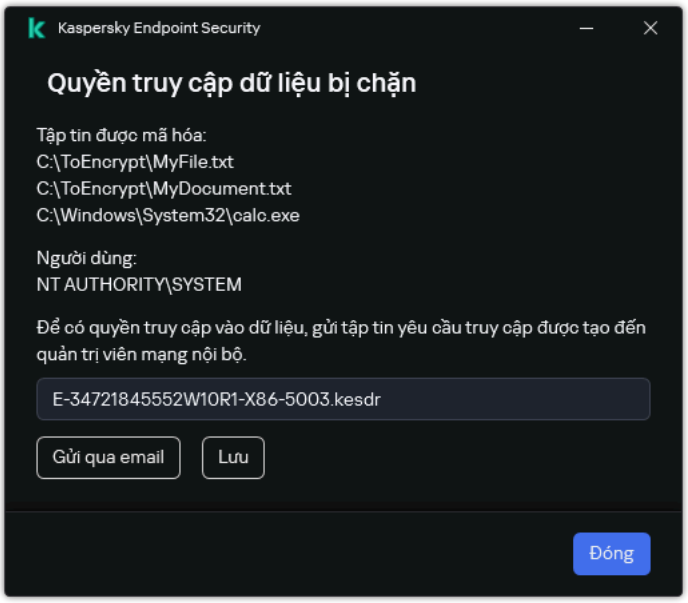
Để có quyền truy cập vào các tập tin được mã hóa, người dùng cần bắt đầu quy trình khôi phục (Yêu cầu-Phản hồi).

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

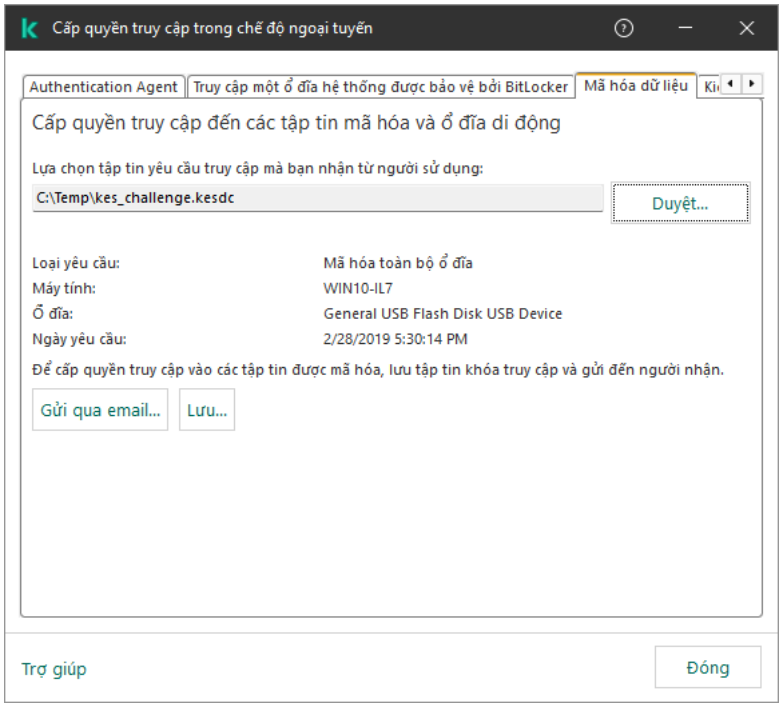
Để bắt đầu quy trình khôi phục, người dùng cần cố truy cập vào một tập tin. Kết quả là Kaspersky Endpoint Security sẽ tạo một tập tin yêu cầu truy cập (tập tin có phần mở rộng là KESDC) mà người dùng cần gửi cho quản trị viên, ví dụ như gửi qua email.

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 cây bảng điều khiển, hãy chọn **Devices**.
3. 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.
4. Trong menu ngữ cảnh, hãy chọn **Cấp quyền truy cập trong chế độ ngoại tuyến**.
5. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy chọn thẻ **Mã hóa dữ liệu**.
6. Trên thẻ **Mã hóa dữ liệu**, hãy nhấn nút **Duyệt**.
7. 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.



Cấp quyền truy cập trong chế độ ngoại tuyến

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 **Asset management** → **Assets (Devices)**.
2. Chọn hộp kiểm bên cạnh tên của máy tính có dữ liệu bạn muốn khôi phục quyền truy cập.
3. Nhấn vào **Grant access to the device in offline mode**.
4. Chọn **Data Encryption**.
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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu → Thiết lập mã hóa chung**.
4. Trong mục **Mẫu**, hãy nhấn nút **Mẫu**.
5. 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 sau 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 (xem hình bên dưới). Nhấn vào nút **Gửi qua email** sẽ tự động tạo một thư của 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.

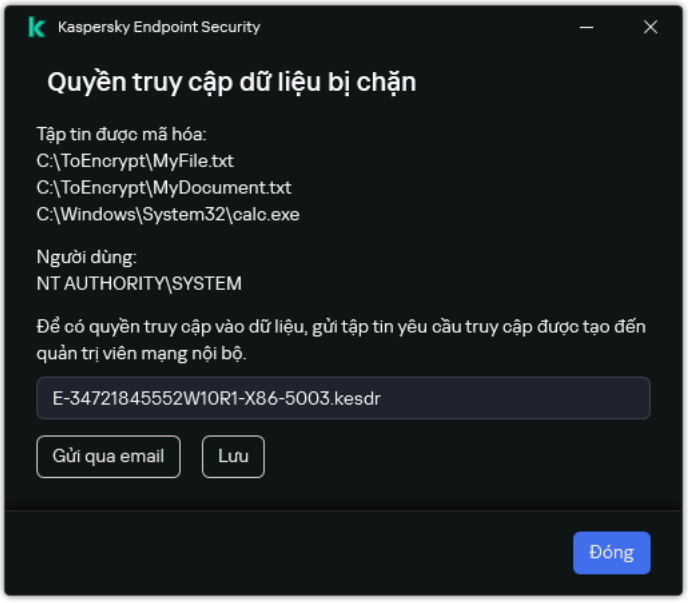
   - Nếu bạn muốn sửa mẫu thông điệp quản trị viên, chọn thẻ **Thông điệp của người quản trị**. Người dùng nhận được thư này sau khi được cấp quyền truy cập vào các tập tin được mã hóa.

6. Sửa mẫu thông điệp.

   Để thêm biến vào văn bản mẫu, hãy đặt con trỏ vào vị trí mong muốn, nhấn vào **Biến số** và chọn biến cần dùng trong danh sách các tùy chọn có sẵn.

   Bạn cũng có thể khôi phục văn bản mẫu mặc định bằng cách sử dụng nút **Theo mặc định**.

7. Lưu các thay đổi của bạn.



Khôi phục quyền truy cập vào các tập tin được mã hóa

Mã hóa ổ đĩa di động

Tính năng mã hóa ổ đĩa di động không được hỗ trợ trên máy tính chạy trên kiến trúc Arm.

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:

- Full Disk Encryption (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).

- File Level Encryption (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 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.

Trước khi mã hóa tập tin trên ổ đĩa di động, hãy đảm bảo rằng ổ đĩa đó đã được định dạng và không có phân vùng ẩn (chẳng hạn như phân vùng hệ thống EFI). Nếu ổ đĩa chứa các phân vùng chưa được định dạng hoặc bị ẩn thì quá trình mã hóa tập tin có thể không thành công và gây ra lỗi.

Để mã hóa ổ đĩa di động:

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu → Mã hóa ổ đĩa di động**.
4. 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.

5. 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.

6. 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.

7. Nếu bạn muốn cấu hình mã hóa cho từng ổ đĩa di động, hãy xác định quy tắc mã hóa.

8. 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.

9. Lưu các thay đổi của bạn.

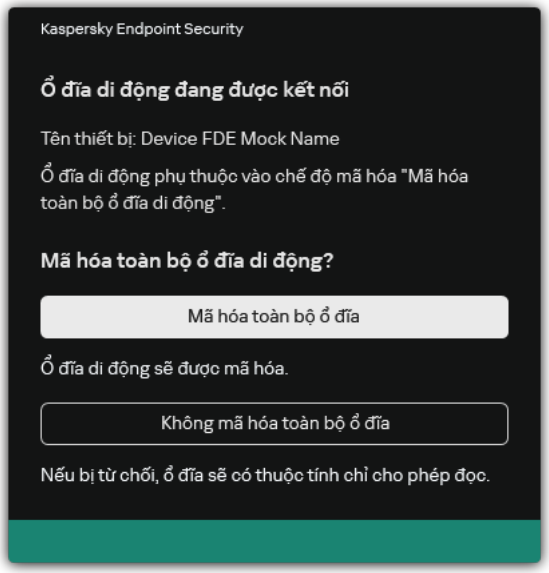
Sau khi áp dụng chính sách, khi người dùng kết nối một ổ đĩa di động hoặc nếu ổ đĩa di động đã được kết nối, Kaspersky Endpoint Security sẽ yêu cầu người dùng xác nhận thực hiện hoạt động mã hóa (xem hình bên dưới).

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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu → Mã hóa ổ đĩa di động**.
4. 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, hãy chọn **Từ danh sách thiết bị của Kaspersky Security Center**.
5. 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.

6. 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.

7. 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 có thể truy xuất. 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** thì các sector không chứa tập tin vẫn sẽ không được mã hóa.

8. 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**.

9. 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. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Data Encryption** → **Encryption of removable drives**.

5. Trong mục **Encryption rules for selected devices**, hãy nhấn liên kết **<N> rules**.

   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 **Export**.

   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 vào liên kết **Import**.

      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.

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu → Mã hóa ổ đĩa di động**.

4. 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 vào 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.

5. Để nhập danh sách các quy tắc mã hóa cho ổ đĩa di động:

   a. Nhấn vào 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.

6. 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:

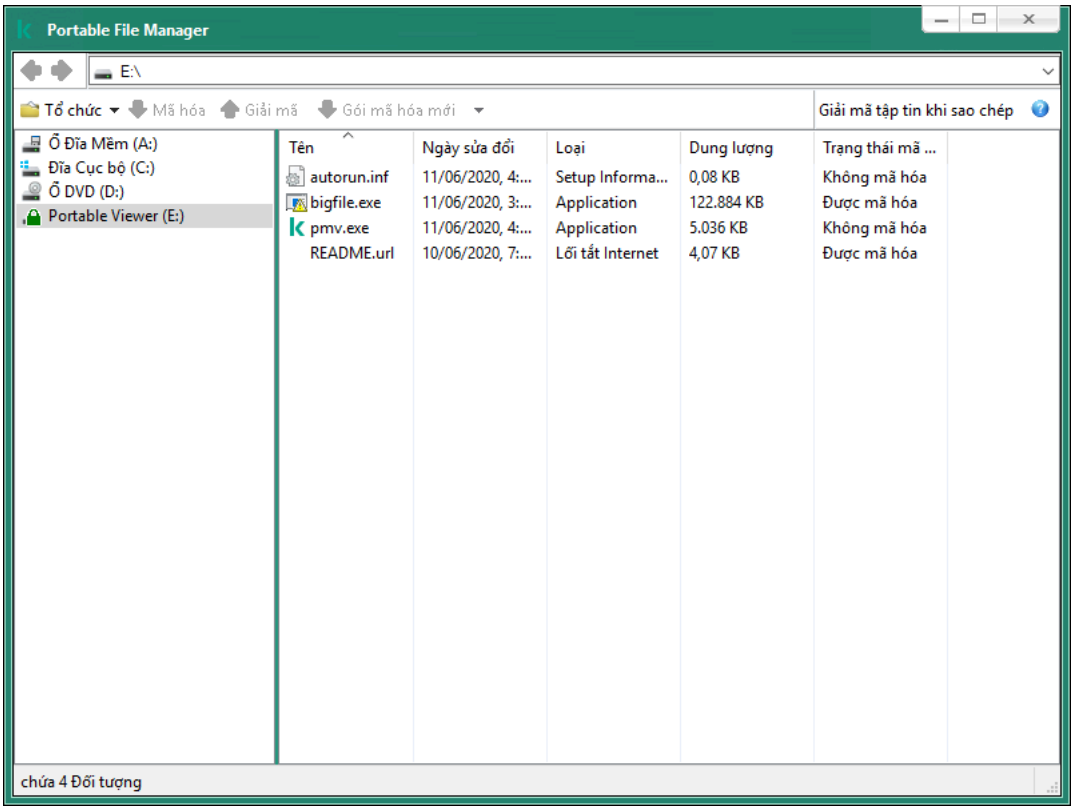
- Không có kết nối giữa máy tính và Máy chủ quản trị Kaspersky Security Center.
- Cơ sở hạ tầng đã thay đổi với sự thay đổi của Máy chủ quản trị Kaspersky Security Center.
- Kaspersky Endpoint Security không được cài đặt trên máy tính.

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

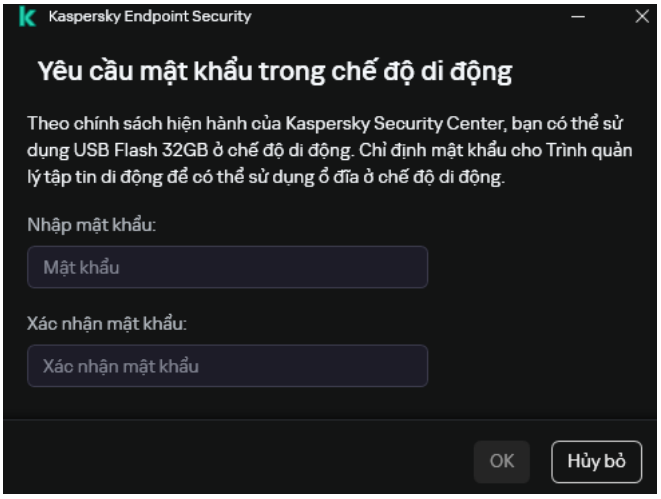
Cách bật hỗ trợ chế độ di động để làm việc với các tập tin được mã hóa trên các ổ đĩa di động trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu** → **Mã hóa ổ đĩa di động**.
4. 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).

5. Chọn hộp kiểm **Chế độ di động**.
6. Nếu cần, hãy thêm quy tắc mã hóa cho từng ổ đĩa di động.
7. Lưu các thay đổi của bạn.
8. Sau khi áp dụng chính sách, hãy kết nối ổ đĩa di động với máy tính.
9. 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.



Yêu cầu mật khẩu trong chế độ di động

10. Nhập vào một mật khẩu đáp ứng được yêu cầu về độ bảo mật và xác nhận nó.
11. Lưu các thay đổi của bạn.

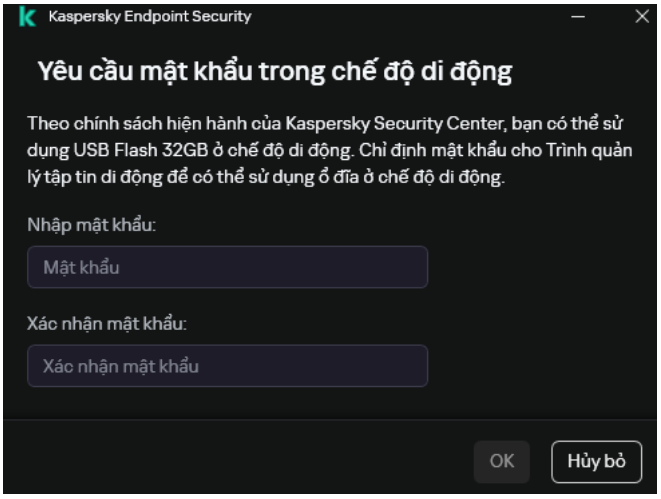
Cách bật hỗ trợ chế độ di động để làm việc với các tập tin được mã hóa trên các ổ đĩa di động trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Data Encryption** → **Encryption of removable drives**.
5. Trong mục **Default action**, hãy chọn **Encrypt all files** hoặc **Encrypt new files only**.

   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 **Portable mode**.
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.



Yêu cầu mật khẩu trong chế độ 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.

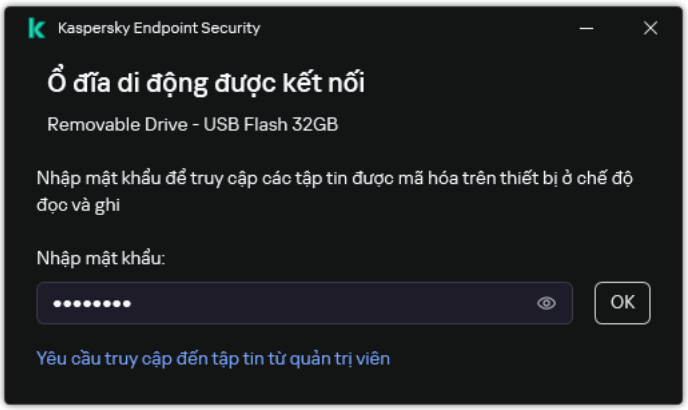
Truy cập các tập tin được mã hóa trên ổ đĩa di động

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 (xem hình bên dưới).

- 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.



Truy cập các tập tin được mã hóa trên ổ đĩa di động

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 cây bảng điều khiển, hãy chọn **Devices**.

3. 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.

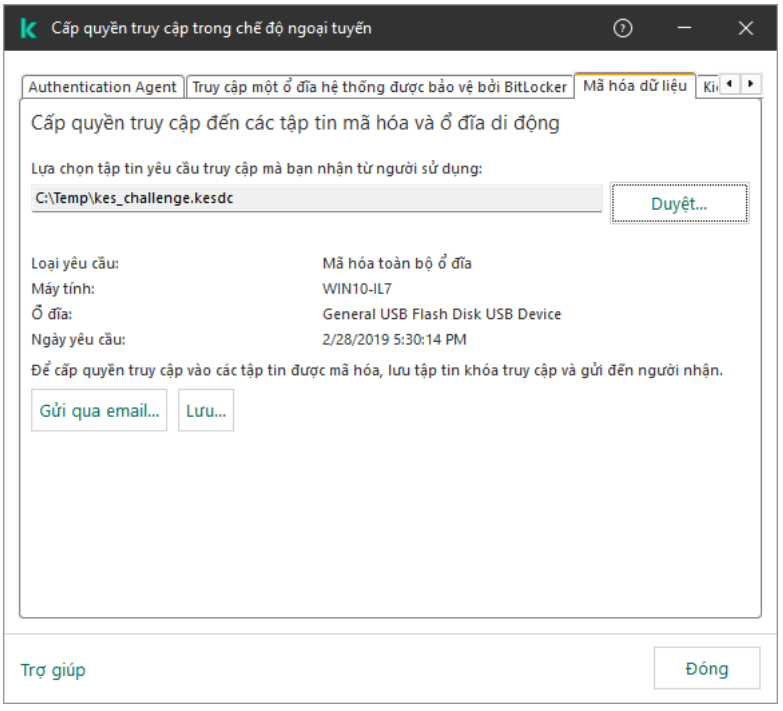
4. Trong menu ngữ cảnh, hãy chọn **Cấp quyền truy cập trong chế độ ngoại tuyến**.

5. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy chọn thẻ **Mã hóa dữ liệu**.

6. Trên thẻ **Mã hóa dữ liệu**, hãy nhấn nút **Duyệt**.

7. 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.



Cấp quyền truy cập trong chế độ ngoại tuyến

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 **Asset management → Assets (Devices)**.
2. Chọn hộp kiểm bên cạnh tên của máy tính có dữ liệu bạn muốn khôi phục quyền truy cập.
3. Nhấn vào **Grant access to the device in offline mode**.
4. Chọn **Data Encryption**.
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. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Mã hóa dữ liệu → Mã hóa ổ đĩa di động**.
4. 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**.

5. 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 nút **Thiết lập quy tắc**, hãy chọn mục **Giải mã toàn bộ ổ đĩa di động**.

6. 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.

Xem trạng thái mã hóa

Bạn có thể nhìn vào trạng thái để theo dõi quá trình mã hóa dữ liệu. Kaspersky Endpoint Security sẽ gán các trạng thái mã hóa sau:

- **Does not meet the policy; canceled by user**. Người dùng đã hủy mã hóa dữ liệu.
- **Does not meet the policy due to an error**. Lỗi mã hóa dữ liệu, ví dụ như thiếu giấy phép.
- **Applying the policy; restart is required**. Quá trình mã hóa dữ liệu đang diễn ra trên máy tính. Khởi động lại máy tính để hoàn tất quá trình mã hóa dữ liệu.
- **No encryption policy specified**. Mã hóa dữ liệu bị tắt trong thiết lập chính sách.
- **Not supported**. Các thành phần mã hóa dữ liệu không được cài đặt trên máy tính.
- **Applying the policy**. Tiến trình mã hóa và / hoặc giải mã dữ liệu đang diễn ra trên máy tính.

Để xem trạng thái mã hóa của dữ liệu máy tính:

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Managed devices**.
3. Trên thẻ **Devices** trong không gian làm việc, vuốt thanh cuộn sang tận cùng bên phải. Nếu cột **Encryption status** không được hiển thị, hãy thêm cột này trong thiết lập bảng điều khiển của Kaspersky Security Center.

   Cột **Encryption status** 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.
4. Nếu trạng thái mã hóa dữ liệu cho máy tính là **Applying policy** thì bạn có thể theo dõi bảng tiến trình mã hóa:
   a. Mở các thuộc tính của máy tính có trạng thái **Applying policy** bằng cách nhấn đúp vào nó.
   b. Trong cửa sổ thuộc tính máy tính, chọn phần **Applications**.
   c. Trong danh sách các ứng dụng Kaspersky đã cài đặt trên máy tính, hãy chọn **Kaspersky Endpoint Security for Windows**.
   d. Nhấn vào **Statistics**.
   e. Trong mục **Encryption of devices** bạn có thể thấy tiến trình mã hóa dữ liệu hiện tại dưới dạng tỷ lệ phần trăm.

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**, hãy nhấn nút **Customize view**.
   b. Trong cửa sổ mở ra, hãy nhấn nút **Add**.
   c. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, trong mục **General**, hãy nhập tên của trang.
   d. Trong mục **Information panels**, hãy chọn nút **Add**.
   e. Trong cửa sổ mở ra trong nhóm **Protection status**, hãy chọn mục **Encryption of devices**.
   f. Nhấn vào **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 vào **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 vào **OK**.

Tên của trang với khung chi tiết được tạo ở bước trước sẽ xuất hiện trong danh sách **Pages**.

k. Nhấn nút **Close**.

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 cây bảng điều khiển, hãy chọn **Managed devices**.

3. Trên thẻ **Devices**, chọn tên của máy tính trong danh sách và nhấn phải chuột để mở menu ngữ cảnh.

4. Trong menu ngữ cảnh của máy tính, chọn mục **Properties**. Trong cửa sổ mở ra, hãy chọn mục **Protection**.

5. 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

Kaspersky Security Center cho phép bạn tạo các báo cáo mã hóa dữ liệu:

- **Report on encryption status of managed devices**. Báo cáo sẽ bao gồm thông tin về việc trạng thái mã hóa của máy tính có tuân thủ chính sách mã hóa hay không.

- **Report on encryption status of mass storage devices**. Báo cáo sẽ bao gồm thông tin về trạng thái mã hóa của thiết bị ngoại vi và thiết bị lưu trữ.

- **Report on rights to access encrypted drives**. Báo cáo sẽ bao gồm thông tin về trạng thái của các tài khoản có quyền truy cập vào các ổ đĩa được mã hóa.

- **Report on file encryption errors**. Báo cáo sẽ bao gồm thông tin về các lỗi xảy ra trong quá trình thực hiện các tác vụ mã hóa hoặc giải mã dữ liệu trên máy tính.
- **Report on blockage of access to encrypted files**. Báo cáo bao gồm thông tin về các ứng dụng bị chặn truy cập các tập tin được mã hóa.

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 báo cáo mã hóa dữ liệu.

   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.

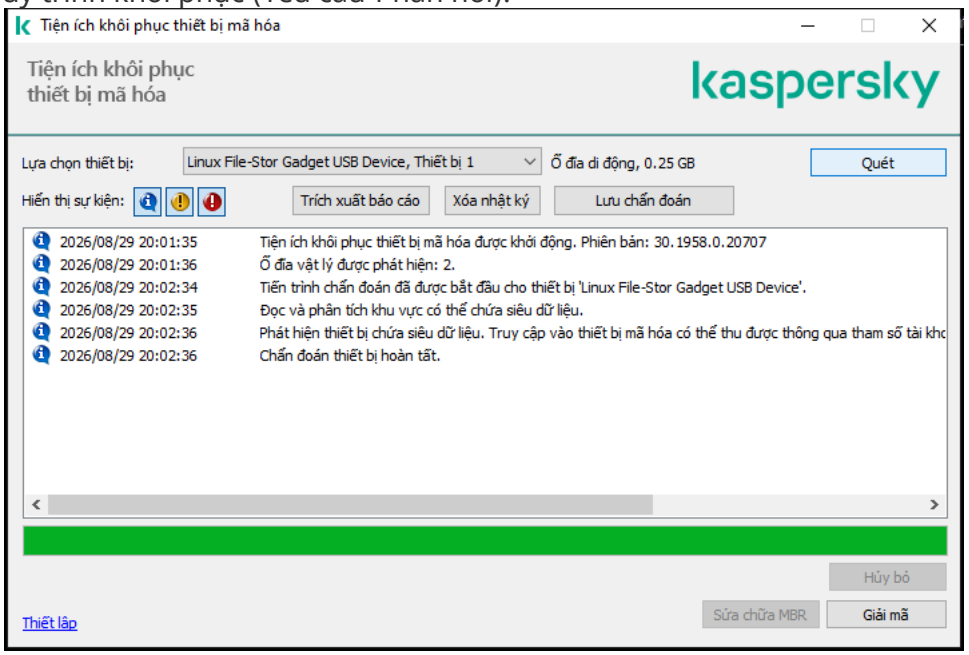
Trước khi khôi phục dữ liệu trên các thiết bị được mã hóa, bạn nên hủy bỏ chính sách Kaspersky Security Center hoặc tắt mã hóa trong thiết lập chính sách Kaspersky Security Center trên máy tính được thực hiện hoạt động này. Điều này sẽ ngăn thiết bị được mã hóa lại một lần nữa.

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. Hãy chọn tùy chọn **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 vào **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 **Advanced → 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 thiết bị trong Kaspersky Endpoint Security**.

> Nếu bạn không chắc chắn việc tập tin yêu cầu truy cập đã được tạo cho máy tính nào, trong cây Bảng điều khiển quản trị, hãy chọn thư mục **Advanced → Data encryption and protection** và trong không gian làm việc, hãy nhấn **Nhận khóa mã hóa thiết bị trong Kaspersky Endpoint Security**.

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: *Strong encryption (AES256)* hoặc *Lite encryption (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 vào **Mở khóa**.

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 **Operations → 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 vào **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: *Strong encryption (AES256)* hoặc *Lite encryption (AES56)*. Thư viện mã hóa AES được cài đặt cùng với ứng dụng.

   c. Chọn tập tin yêu cầu truy cập nhận được từ người dùng (tập tin có phần mở rộng là FDERTC).

   d. Chọn thư mục để lưu tập tin khóa 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

Các giải pháp Kaspersky Detection and Response là các hệ thống bảo mật để phát hiện các mối đe dọa nâng cao và chỉ báo tấn công ở các cấp độ khác nhau trong cơ sở hạ tầng của một tổ chức. Các giải pháp Detection and Response cung cấp thông tin về mối đe dọa được phát hiện và cho phép quản lý các hành động Ứng phó với mối đe dọa.

Do đó, giải pháp Detection and Response thực hiện như sau:

- Nhận thông tin về hoạt động của máy tính, máy chủ hoặc các thiết bị khác (đo từ xa).
- Tự động phân tích thông tin để phát hiện các mối đe dọa.
- Tạo chi tiết cảnh báo dưới dạng các cột của chuỗi phát triển mối đe dọa để phân tích và chọn các hành động Ứng phó với mối đe dọa.
- Thực hiện các hành động Ứng phó với mối đe dọa (ví dụ: cách ly mạng của máy tính).

Kaspersky Endpoint Security hỗ trợ các giải pháp Detection and Response bằng một tác nhân được tích hợp. Tác nhân tích hợp gửi phép đo từ xa đến máy chủ của các giải pháp và thực hiện các hành động Ứng phó với mối đe dọa. 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 Anti Targeted Attack Platform:
  - Endpoint Detection and Response (EDR) phiên bản 7.1 trở lên
  - Network Detection and Response (NDR)
  - KATA Sandbox
- Kaspersky Endpoint Detection and Response Expert (on-premises)
- Kaspersky Sandbox 2.0

Bạn có thể sử dụng giải pháp Kaspersky Endpoint Security với giải pháp Detection and Response theo nhiều cấu hình khác nhau, ví dụ: [EDR Optimum+MDR].

Cấp phép cho MDR và EDR Optimum

Kaspersky Endpoint Security hỗ trợ chức năng của giải pháp Kaspersky Managed Detection and Response (MDR) và Kaspersky Endpoint Detection and Response Optimum (EDR Optimum). Bạn có thể sử dụng Kaspersky Endpoint Security với các giải pháp này trong nhiều cấu hình khác nhau và xây dựng một hệ thống bảo vệ tùy chỉnh, đáp ứng các yêu cầu cụ thể của mình. Để làm như vậy, bạn phải mua giấy phép cho từng giải pháp. Giấy phép có thể bao gồm quyền sử dụng một giải pháp duy nhất (ví dụ: chỉ Phần bổ trợ MDR) hoặc vài giải pháp, Phần bổ trợ [EDR Optimum+MDR].

MDR và EDR Optimum hỗ trợ các phương thức cấp phép sau:

- Chức năng MDR hoặc EDR Optimum được hỗ trợ bởi giấy phép Kaspersky Endpoint Security cho Windows.

  Chức năng này khả dụng ngay sau khi kích hoạt Kaspersky Endpoint Security cho Windows. Bạn chỉ cần thêm một khóa.

- Các giấy phép riêng cho MDR hoặc EDR Optimum (MDR Add-on, EDR Optimum Add-on, [EDR Optimum+MDR] Add-on).

  Chức năng này sẽ khả dụng sau khi thêm một khóa riêng cho Tiện ích bổ trợ MDR, Tiện ích bổ trợ EDR Optimum hoặc Tiện ích bổ trợ [EDR Optimum+MDR]. Kết quả là hai khóa được thêm trên máy tính: một khóa dành cho Kaspersky Endpoint Security và một khóa dành cho MDR hoặc EDR Optimum. Khóa Kaspersky Endpoint Security phải là khóa được thêm đầu tiên.

Kaspersky Endpoint Security chỉ cho phép thêm một *khóa hiện hoạt* để cấp phép cho MDR và EDR Optimum. Do đó, nếu bạn cần kích hoạt cả hai giải pháp này, bạn phải thêm một khóa Tiện ích bổ trợ [EDR Optimum+MDR] Add-on thay vì một khóa riêng cho mỗi giải pháp. Bạn cũng có thể thêm một *khóa dự trữ*.

Nếu bạn đã sử dụng tập tin BLOB khi triển khai MDR, bạn không cần khóa riêng để kích hoạt MDR. Tập tin BLOB đã chứa thông tin giấy phép.

Cấp phép ban đầu cho các giải pháp

Khi triển khai MDR và EDR Optimum lần đầu tiên, các giải pháp sẽ được kích hoạt theo cách tương tự như ứng dụng Kaspersky Endpoint Security. Bạn có thể thêm khóa bằng cách sử dụng tác vụ *Thêm khóa* hoặc sử dụng chức năng phân phối khóa tự động. Khóa giấy phép sẽ được thêm vào ứng dụng dưới dạng khóa hiện hoạt thứ hai hoặc dưới dạng khóa dự trữ nếu bạn chọn hộp kiểm liên quan.

Chuyển từ một giấy phép này sang giấy phép khác

Nếu tổ chức của bạn đã triển khai một trong những giải pháp này và khóa tương ứng đã được thêm vào ứng dụng thì sẽ có một vài điểm đặc biệt cần cân nhắc liên quan đến việc cấp phép cho cấu hình mới. Khi chuyển sang giấy phép khác, ứng dụng không thêm khóa mới vào ứng dụng mà thay thế khóa hiện tại bằng khóa mới. Lý do là chức năng hạn chế chỉ cho phép ứng dụng thêm một khóa để kích hoạt MDR và EDR Optimum.

Ví dụ: giả sử tổ chức của bạn đã triển khai giải pháp [EDR Optimum+MDR] và bạn quyết định chuyển sang cấu hình Tiện ích bổ trợ MDR. Để chuyển sang cấu hình mới, bạn phải thay thế khóa Tiện ích bổ trợ [EDR Optimum+MDR] Add-on bằng khóa Tiện ích bổ trợ MDR.

Giấy phép riêng cho EDR Optimum và MDR (Tiện ích bổ trợ [EDR Optimum+MDR]) không còn khả dụng. Nếu muốn sử dụng cả hai giải pháp này, bạn phải kích hoạt MDR bằng tập tin BLOB và EDR Optimum bằng khóa giấy phép.

Với tính năng phân phối khóa tự động, ứng dụng sẽ từ chối các khóa giấy phép hỗ trợ cùng một số giải pháp. Có nghĩa là nếu bạn đã thêm khóa Tiện ích bổ trợ EDR Optimum, bạn không thể thay thế khóa này bằng khóa Tiện ích bổ trợ MDR. Tuy nhiên, bạn có thể thay thế khóa Tiện ích bổ trợ EDR Optimum bằng khóa Tiện ích bổ trợ [EDR Optimum+MDR]. Ứng dụng cũng từ chối các khóa nếu bạn cố gắng thay thế khóa Tiện ích bổ trợ MDR bằng khóa Tiện ích bổ trợ EDR. Để thay thế khóa, bạn có thể chạy tác vụ *Thêm khóa*. Tác vụ *Thêm khóa* cho phép thay thế khóa giấy phép với bất kỳ giải pháp nào.

Nếu bạn đã thêm khóa dự trữ Tiện ích bổ trợ [EDR Optimum+MDR] Add-on, để thêm đúng cách một khóa hiện hoạt cho Tiện ích bổ trợ EDR Optimum hoặc MDR, trước tiên bạn phải thay thế khóa dự trữ bằng khóa Tiện ích bổ trợ EDR Optimum hoặc Tiện ích bổ trợ MDR, hoặc cách khác là xóa khóa dự trữ rồi thay thế khóa hiện hoạt.

Khả năng tương thích với các giải pháp EDR của bên thứ ba

Bạn có thể sử dụng Kaspersky Endpoint Security để bảo vệ máy trạm và máy chủ cùng với các giải pháp EDR của bên thứ ba. Để loại bỏ các cảnh báo nhầm, bạn nên thêm các tập tin thực thi của Kaspersky Endpoint Security và Network Agent vào khu vực tin tưởng của giải pháp EDR bên thứ ba.

Khu vực tin tưởng để tương thích với các giải pháp EDR của bên thứ ba

	Kaspersky Endpoint Security cho Windows	Kaspersky Security Center Network Agent
Thư mục làm việc	`C:\Program Files (x86)\Kaspersky Lab\KES.14.2.0`	`C:\Program Files (x86)\Kaspersky Lab\NetworkAgent`

Tập tin thực thi	`avp.exe`
	`avp.com`
	`avpsus.exe`
	`avpui.exe`
	`dump_writer_agent.exe`
	`kescli.exe`
	`kesdr.exe`
	`kldw.exe`
	`klpsm.exe`
	`kvdb_upgrader.exe`
	`modify_watcher.exe`
	`pmv.exe`
	`remediation.exe`
	`service_stub.exe`
		`AVPDTAgt.exe`
		`fix_gflags.exe`
		`getsysteminfo.exe`
		`integrity_checker.exe`
		`klcpuld.exe`
		`klcsldcl.exe`
		`klcsngtgui.exe`
		`klcspxy.exe`
		`kldumper.exe`
		`klmover.exe`
		`klnagchk.exe`
		`klnagent.exe`
		`klnagntf.exe`
		`klnagwds.exe`
		`klosprep.exe`
		`klrbtagt.exe`
		`klscflag.exe`
		`klscmodchk.exe`
		`klshwmsg.exe`
		`klwd.exe`
		`ksnproxy.exe`
		`Patch.exe`
		`tslauncher.exe`
		`Up2Date.exe`
		`vapm.exe`

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 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

Gói phân phối cho các phiên bản Kaspersky Endpoint Security 11.2.0 – 11.8.0 bao gồm Kaspersky Endpoint Agent. Bạn có thể chọn Kaspersky Endpoint Agent khi cài đặt Kaspersky Endpoint Security cho Windows. Kết quả là hai ứng dụng sẽ được cài đặt trên máy tính của bạn: KEA và KES. Trong Kaspersky Endpoint Security 11.9.0, gói phân phối Kaspersky Endpoint Agent không còn thuộc gói phân phối Kaspersky Endpoint Security.

Sự tương ứng của các phiên bản KEA (thuộc KES) với các phiên bản KES

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

Kaspersky đang chuyển tất cả tính năng Detection and Response sang hoạt động với tác nhân tích hợp của Kaspersky Endpoint Security thay vì Kaspersky Endpoint Agent. Kaspersky đang dần bổ sung hỗ trợ cho các giải pháp này và dần loại bỏ Kaspersky Endpoint Agent (xem bảng bên dưới). Kể từ phiên bản 12.1, ứng dụng sẽ hỗ trợ tất cả các giải pháp Detection and Response. Ngoài ra, kể từ phiên bản 12.1, ứng dụng này không còn tương thích với Kaspersky Endpoint Agent và không thể cài đặt cùng lúc hai ứng dụng trên cùng một máy tính.

Phiên bản của Kaspersky Endpoint Security	Kaspersky Managed Detection and Response	Kaspersky Sandbox	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Endpoint Detection and Response Expert	Kaspersky Anti Targeted Attack Platform (thành phần Endpoint Detection and Response)	Kaspersky Anti Targeted Attack Platform (thành phần Network Detection and Response)
11.5.0	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.6.0	**Tác nhân tích hợp**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.7.0	**Tác nhân tích hợp**	**Tác nhân tích hợp**	**Tác nhân tích hợp**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.8.0	**Tác nhân tích hợp**	**Tác nhân tích hợp**	**Tác nhân tích hợp**	**Tác nhân tích hợp**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.9.0	**Tác nhân tích hợp**	**Tác nhân tích hợp**	**Tác nhân tích hợp**	**Tác nhân tích hợp**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.10.0	**Tác nhân tích hợp**	**Tác nhân tích hợp**	**Tác nhân tích hợp**	**Tác nhân tích hợp**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.11.0	**Tác nhân tích hợp**	**Tác nhân tích hợp**	**Tác nhân tích hợp**	**Tác nhân tích hợp**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12	**Tác nhân tích hợp**	**Tác nhân tích hợp**	**Tác nhân tích hợp**	**Tác nhân tích hợp**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12.1	**Tác nhân tích hợp**	**Tác nhân tích hợp**	**Tác nhân tích hợp**	**Tác nhân tích hợp**	**Tác nhân tích hợp**	Kaspersky Endpoint Agent
12.6	**Tác nhân tích hợp**	**Tác nhân tích hợp**	**Tác nhân tích hợp**	**Tác nhân tích hợp**	**Tác nhân tích hợp**	**Tác nhân tích hợp**

Chuyển cấu hình [KES+KEA] sang cấu hình [KES+built-in agent]

Kaspersky Endpoint Security có các tác nhân tích hợp để làm việc với các giải pháp Managed Detection and Response. Bạn không còn cần một ứng dụng Kaspersky Endpoint Agent riêng để hoạt động với các giải pháp này. Khi bạn triển khai Kaspersky Endpoint Security trên các máy tính đã cài đặt Kaspersky Endpoint Agent thì các giải pháp Detection and Response sẽ tiếp tục hoạt động với Kaspersky Endpoint Security. Ngoài ra, Kaspersky Endpoint Agent sẽ bị gỡ bỏ khỏi máy tính.

Gói phân phối cho các phiên bản Kaspersky Endpoint Security 11.2.0 – 11.8.0 bao gồm Kaspersky Endpoint Agent. Bạn có thể chọn Kaspersky Endpoint Agent khi cài đặt Kaspersky Endpoint Security cho Windows. Kết quả là hai ứng dụng sẽ được cài đặt trên máy tính của bạn: KEA và KES. Trong Kaspersky Endpoint Security 11.9.0, gói phân phối Kaspersky Endpoint Agent không còn thuộc gói phân phối Kaspersky Endpoint Security.

Việc chuyển cấu hình [KES+KEA] sang [KES+tác nhân tích hợp] 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 trở lên, bao gồm Network 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 trở lên. Bạn phải sử dụng Bảng điều khiển web để quản lý các thành phần EDR Optimum và Kaspersky Sandbox.

Để sử dụng Kaspersky Anti Targeted Attack Platform (EDR), bạn sẽ cần một tiện ích web dành cho Kaspersky Endpoint Security phiên bản 12.1 trở lên.

Để sử dụng Kaspersky Anti Targeted Attack Platform (NDR), bạn sẽ cần một tiện ích web dành cho Kaspersky Endpoint Security phiên bản 12.7 trở lên.

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 *Inactive*. Để áp dụng chính sách, hãy mở các thuộc tính chính sách, chấp nhận Tuyên bố Kaspersky Security Network và đặt trạng thái thành *Active*.

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 Tiện ích bổ trợ 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 *Add key*.

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.

Chỉ có thể sử dụng giấy phép Kaspersky Anti Targeted Attack Platform để kích hoạt Kaspersky Endpoint Security như một phần của giải pháp Kaspersky Anti Targeted Attack Platform. Sau khi bạn nâng cấp ứng dụng lên phiên bản 12.1, chức năng EDR (KATA) sẽ được kích hoạt tự động. Bạn không cần phải làm gì khác.

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 cho giải pháp Detection and Response trong phần thiết lập của gói cài đặt.
- Loại trừ thành phần Kaspersky Endpoint Agent trong thiết lập của gói cài đặt (đối với Kaspersky Endpoint Security cho Windows phiên bản 11.2.0 – 11.8.0).
- Nếu Bảo vệ bằng Mật khẩu được bật để hạn chế quyền truy cập vào Kaspersky Endpoint Agent, hãy nhập mật khẩu gỡ trong thiết lập của tác vụ *Install application remotely*. Bạn có thể nhập mật khẩu gỡ bỏ kể từ Kaspersky Security Center Linux 15.1.

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.

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 hiện tại 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 hiện tại của các giải pháp Kaspersky. Trong trường hợp này, Kaspersky Endpoint Security sẽ tự động chọn các thành phần dựa trên cấu hình của Kaspersky Endpoint Agent. Sau đó khiến Kaspersky Endpoint Security sẽ 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 *Critical* trong bảng điều khiển Kaspersky Security Center:

- Đảm bảo rằng máy tính được cài đặt Network Agent phiên bản 13.2 trở lên.
- Kiểm tra trạng thái hoạt động của tác nhân tích hợp bằng cách xem *Report on status of application components*. Nếu một thành phần có trạng thái *Not installed* thì hãy cài đặt thành phần này bằng cách sử dụng tác vụ *Change application components*.
- 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 *Report on status of application components*. 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.

Chuyển đổi chính sách và tác vụ cho Kaspersky Endpoint Agent

Kaspersky Endpoint Security cho Windows bao gồm một trình hướng dẫn để chuyển 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 Anti Targeted Attack Platform

Trình hướng dẫn chuyển từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security chỉ hoạt động trong Bảng điều khiển web và Bảng điều khiển đám mây. Trong Bảng điều khiển quản trị (MMC), bạn chỉ có thể chuyển thiết lập cho giải pháp Kaspersky Anti Targeted Attack Platform (EDR) bằng Trình hướng dẫn chuyển đổi tác vụ và chính sách tiêu chuẩn của Kaspersky Security Center.

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 **Operations → Migration from 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 chính sách Kaspersky Endpoint Agent để chọn chính sách Kaspersky Endpoint Security mà bạn muốn gộp thiết lập. 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

Hoàn tất trình hướng dẫn. Kết quả là trình hướng dẫn thực hiện như sau:

- 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 *Inactive*. Để tiếp tục, hãy thay đổi trạng thái của chính sách Kaspersky Endpoint Agent và Kaspersky Endpoint Security thành *Inactive* 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 mối đe dọa). Các giá trị thông số truyền dữ liệu không được chuyển từ một chính sách của Kaspersky Endpoint Agent.

  Bạn có thể gặp lỗi khi kết nối máy tính với máy chủ Central Node khi chuyển từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security cho giải pháp Kaspersky Anti Targeted Attack Platform (EDR). Lý do là trình hướng dẫn chuyển đổi trong Bảng điều khiển web sẽ bỏ qua các thiết lập chính sách sau và không chuyển chúng:

  - Cấm sửa đổi thiết lập **Connection to KATA servers** ("khóa").

    Theo mặc định, bạn có thể sửa đổi thiết lập ("khóa" đang mở). Do đó, thiết lập không được áp dụng trên máy tính đó. Bạn phải cấm sửa đổi thiết lập và đóng "khóa".

  - Bộ chứa mã hóa.

    Nếu đang sử dụng xác thực hai chiều để kết nối với máy chủ Central Node thì bạn phải thêm lại bộ chứa mã hóa. Trình hướng dẫn chuyển đổi sẽ chuyển chính xác chứng chỉ TLS của máy chủ.

  Trình hướng dẫn chuyển đổi chính sách và tác vụ trong Bảng điều khiển quản trị (MMC) sẽ chuyển tất cả các thiết lập cho giải pháp Kaspersky Anti Targeted Attack Platform (EDR).

- 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.

Cách chuyển thiết lập chính sách và tác vụ từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security trong Bảng điều khiển quản trị (MMC) (chỉ dành cho KATA (EDR))

1. Trong Bảng điều khiển quản trị, chọn Máy chủ quản trị và nhấn chuột phải để mở menu ngữ cảnh.
2. Chọn **All tasks** → **Policies and tasks batch conversion wizard**.

Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ sẽ khởi chạy. Làm theo chỉ dẫn của Trình hướng dẫn.

Bước 1. Chọn ứng dụng mà bạn cần chuyển đổi chính sách và tác vụ

Tại bước này, bạn cần chọn Kaspersky Endpoint Security cho Windows. Chuyển sang bước tiếp theo.

Bước 2. Chuyển đổi chính sách

Trình hướng dẫn chuyển đổi sẽ tạo một chính sách Kaspersky Endpoint Security mới trong đó các thiết lập chính sách của Kaspersky Endpoint Agent sẽ được chuyển. Trong danh sách chính sách, hãy chọn các chính sách Kaspersky Endpoint Agent có thiết lập mà bạn muốn chuyển sang chính sách Kaspersky Endpoint Security. Chuyển sang bước tiếp theo.

Khi đó, Trình hướng dẫn chuyển đổi sẽ bắt đầu chuyển đổi các chính sách. Trong quá trình chuyển đổi chính sách, Trình hướng dẫn chuyển đổi sẽ nhắc bạn chấp nhận Tuyên bố Kaspersky Security Network. Các chính sách mới sẽ được đặt tên *<Tên chính sách> (được chuyển đổi)*.

Bước 3. Chuyển đổi tác vụ

Bỏ qua bước này. Trình hướng dẫn chỉ hỗ trợ các tác vụ dành cho Kaspersky Endpoint Detection and Response Optimum và Kaspersky Sandbox. Việc quản lý các thành phần này chỉ khả dụng trong Bảng điều khiển web. Chuyển sang bước tiếp theo.

Bước 4. Hoàn tất Trình hướng dẫn

Hoàn tất trình hướng dẫn. Nhờ trình hướng dẫn này, một chính sách Kaspersky Endpoint Security mới sẽ được tạo.

Endpoint Detection and Response Agent (EDR Agent)

Kể từ Kaspersky Endpoint Security 12.3 cho Windows, ứng dụng đã có cấu hình Endpoint Detection and Response Agent (EDR Agent). *Endpoint Detection and Response Agent* là một ứng dụng được cài đặt trên các máy trạm và máy chủ riêng lẻ trong cơ sở hạ tầng CNTT của tổ chức để hỗ trợ các giải pháp Detection and Response của Kaspersky:

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack Platform (EDR)
- Kaspersky Unified Monitoring and Analysis Platform (KUMA) (kể từ phiên bản 12.6)

- Kaspersky Anti Targeted Attack Platform (NDR) (kể từ phiên bản 12.7)
- Kaspersky Endpoint Detection and Response Expert (on-premises) (bắt đầu từ phiên bản 12.11)

EDR Agent không hỗ trợ tích hợp với các giải pháp Kaspersky Endpoint Detection and Response Expert (cloud).

EDR Agent liên tục giám sát các tiến trình đang chạy trên những máy tính này, các kết nối mạng mở và các tập tin đang bị sửa đổi. Các thành phần bảo vệ và kiểm soát của ứng dụng không khả dụng cho EDR Agent.

EDR Agent tương thích với các ứng dụng EPP của bên thứ ba. Điều này cho phép bạn sử dụng các công cụ bảo mật cơ sở hạ tầng của bên thứ ba cùng với tính năng Detection and Response by Kaspersky.

Để triển khai EDR Agent, máy tính phải được cài đặt Network Agent và máy tính phải được thêm vào bảng điều khiển Kaspersky Security Center. Để kích hoạt khả năng tương tác của EDR Agent với Kaspersky Security Center, bạn phải cài đặt tiện ích quản lý Kaspersky Endpoint Security cho Windows. Bạn có thể chỉ định thiết lập EDR Agent bằng chính sách nhóm. Để tích hợp EDR Agent, bạn phải cấu hình tích hợp trong các phần chính sách thích hợp.

Các ứng dụng Kaspersky sau đây phải được cài đặt trên cơ sở hạ tầng để hỗ trợ các giải pháp của Kaspersky Detection and Response:

	• Network Agent • EDR Agent
Điểm cuối	
	Tiện ích quản lý Kaspersky Endpoint Security cho Windows
Kaspersky Security Center	
	
Các giải pháp Detection and Response: MDR, KATA (EDR), KATA (NDR), KUMA, EDR Expert (on-premises)	

Cài đặt EDR Agent

Kaspersky Endpoint Security trong cấu hình Endpoint Detection and Response Agent (EDR Agent) cho các giải pháp Kaspersky Detection and Response được cài đặt theo cùng cách.

Có thể cài đặt EDR Agent trên máy tính theo một trong các cách sau:

- Từ xa thông qua Kaspersky Security Center.
- Cài đặt cục bộ bằng Trình hướng dẫn cài đặt.
- Thực hiện cục bộ trên dòng lệnh (chỉ dành cho KATA (EDR) và EDR Expert (on-premises)).

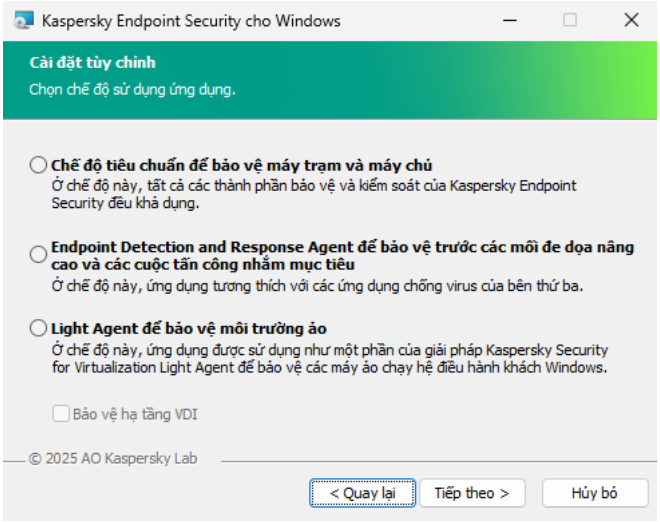
Để cài đặt EDR Agent, bạn phải chọn cấu hình thích hợp trong thiết lập gói cài đặt hoặc trong Trình hướng dẫn cài đặt.

Cách cài đặt EDR Agent bằng 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.

Cấu hình của Kaspersky Endpoint Security



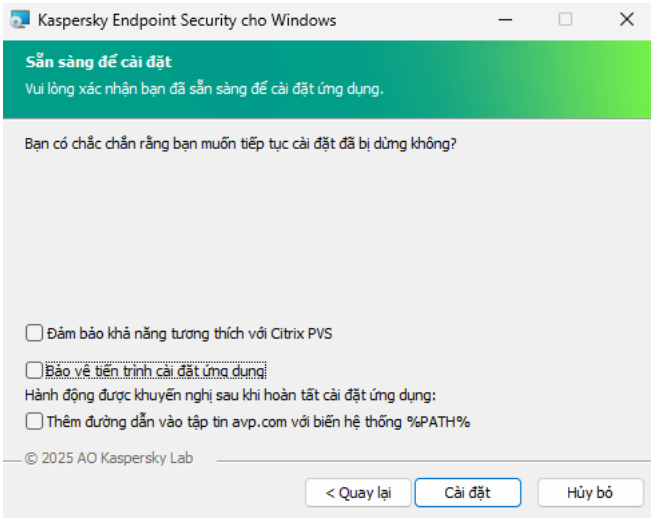
Lựa chọn cấu hình ứng dụng

Chọn cấu hình **Endpoint Detection and Response Agent**. Trong cấu hình này, bạn chỉ có thể cài đặt các thành phần hỗ trợ các giải pháp Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), cũng như KUMA. Đây là cấu hình cần thiết nếu Endpoint Protection Platform (EPP) của bên thứ ba được triển khai trong tổ chức của bạn cùng với giải pháp Kaspersky Detection and Response. Điều này làm cho Kaspersky Endpoint Security trong cấu hình Endpoint Detection and Response Agent tương thích với các ứng dụng EPP của bên thứ ba.

Các thành phần Kaspersky Endpoint Security

Chọn các thành phần mà bạn muốn cài đặt. 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.

Thiết lập nâng cao



Thiết lập cài đặt ứng dụng 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 khả năng tương thích với Citrix PVS. Bạn có thể bật hỗ trợ Citrix Provisioning Services để cài đặt Kaspersky Endpoint Security lên một máy tính ảo.

Thêm đường dẫn vào tập tin avp.com với biến hệ thống %PATH%. Bạn có thể thêm đường dẫn cài đặt vào biến số %PATH% để tiện sử dụng giao diện dòng lệnh.

Cách cài đặt EDR Agent trên dòng lệnh (chỉ dành cho KATA (EDR) và EDR Expert (on-premises))

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 /pSTANDALONEMODE=1 [/s]
   ```

   hoặc

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 STANDALONEMODE=1 [/qn]
   ```

   Kết quả là ứng dụng EDR Agent để tích hợp với Kaspersky Anti Targeted Attack Platform (EDR) hoặc Kaspersky Endpoint Detection and Response Expert (on-premises) sẽ 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`.

Cách cài đặt EDR Agent trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn thư mục **Advanced** → **Remote installation** → **Installation packages**.

   Thao tác này sẽ mở danh sách các gói cài đặt đã được tải về Kaspersky Security Center.
3. Mở thuộc tính của gói cài đặt.

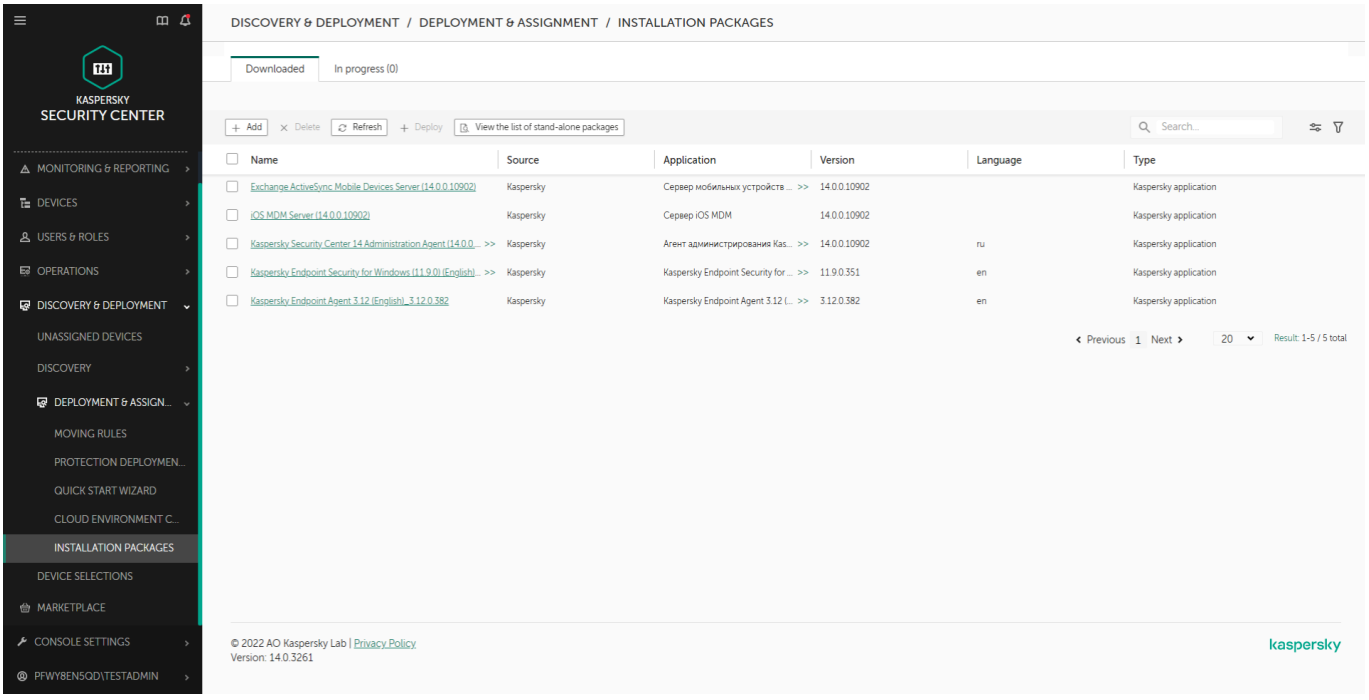
   Nếu cần, hãy tạo gói cài đặt mới.
4. Vào mục **Protection components**.
5. Chọn cấu hình **Endpoint Detection and Response Agent để bảo vệ trước các mối đe dọa nâng cao và các cuộc tấn công nhắm mục tiêu**. Trong cấu hình này, bạn chỉ có thể cài đặt các thành phần hỗ trợ các giải pháp Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), cũng như KUMA. Đây là cấu hình cần thiết nếu Endpoint Protection Platform (EPP) của bên thứ ba được triển khai trong tổ chức của bạn cùng với giải pháp Kaspersky Detection and Response. Điều này làm cho Kaspersky Endpoint Security trong cấu hình Endpoint Detection and Response Agent tương thích với các ứng dụng EPP của bên thứ ba.
6. Chọn các thành phần mà bạn muốn cài đặt.

   Bạn có thể thay đổi các thành phần ứng dụng khả dụng sau khi ứng dụng được cài đặt.
7. Lưu các thay đổi của bạn.
8. Tạo tác vụ cài đặt từ xa. Trong thuộc tính tác vụ, hãy chọn gói cài đặt bạn đã tạo.

Cách cài đặt EDR Agent bằng Bảng điều khiển web

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.



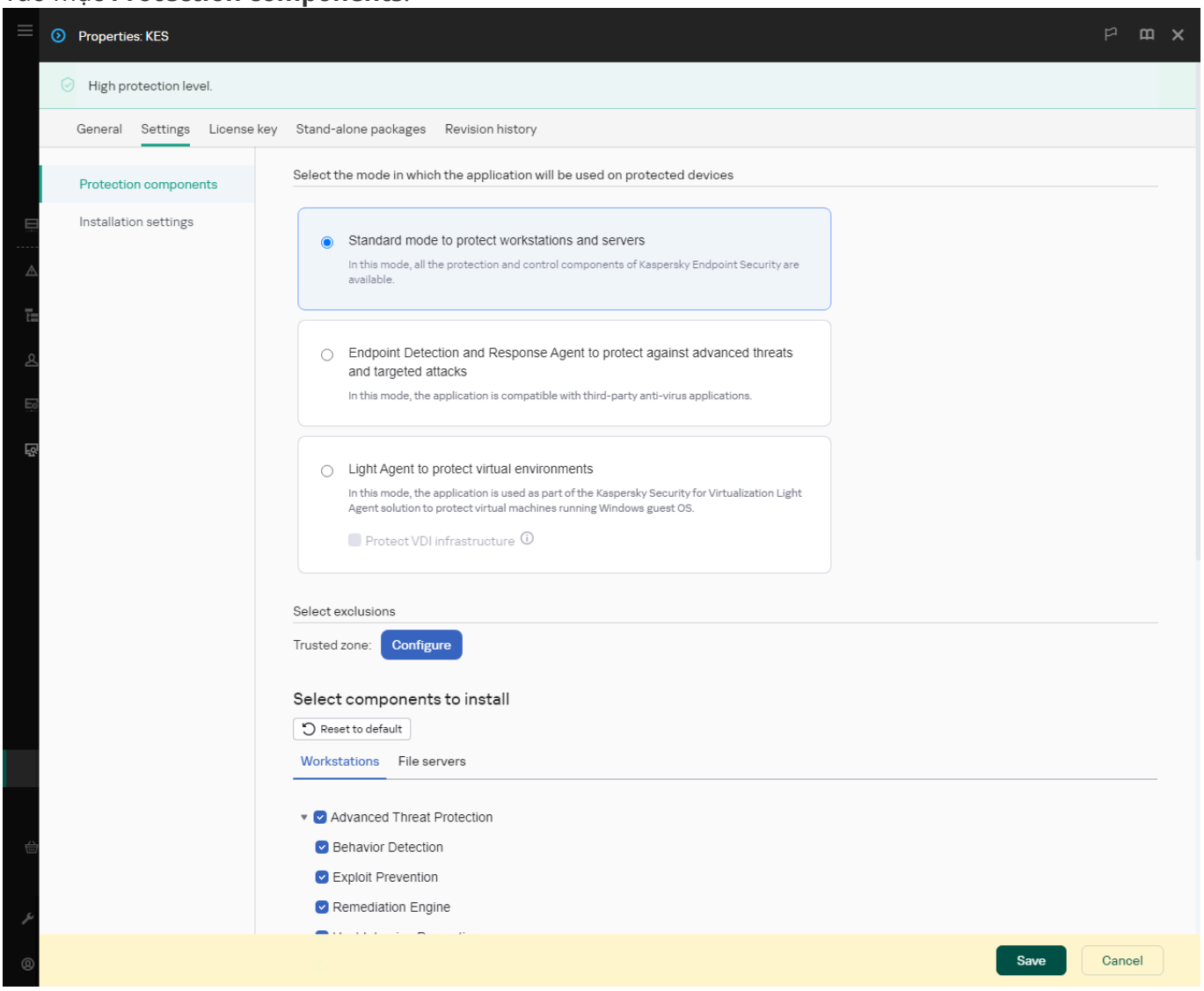
Danh sách gói cài đặt

2. Mở thuộc tính của gói cài đặt.

   Nếu cần, hãy tạo gói cài đặt mới.

3. Chọn thẻ **Settings**.

4. Vào mục **Protection components**.



Các thành phần có trong gói cài đặt

5. Chọn cấu hình **Endpoint Detection and Response Agent**. Trong cấu hình này, bạn chỉ có thể cài đặt các thành phần hỗ trợ các giải pháp Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), cũng như KUMA. Đây là cấu hình cần thiết nếu Endpoint Protection Platform (EPP) của bên thứ ba được triển khai trong tổ chức của bạn cùng với giải pháp Kaspersky Detection and Response. Điều này làm cho Kaspersky Endpoint Security trong cấu hình Endpoint Detection and Response Agent tương thích với các ứng dụng EPP của bên thứ ba.

6. Chọn các thành phần mà bạn muốn cài đặt.

   Bạn có thể thay đổi các thành phần ứng dụng khả dụng sau khi ứng dụng được cài đặt.

7. Lưu các thay đổi của bạn.

8. Tạo tác vụ cài đặt từ xa. Trong thuộc tính tác vụ, hãy chọn gói cài đặt bạn đã tạo.

Kết quả là EDR Agent được cài đặt trên máy tính của người dùng. Bạn có thể sử dụng giao diện của ứng dụng và biểu tượng của ứng dụng được hiển thị trong vùng thông báo .

Trong Kaspersky Security Center, máy tính có ứng dụng được cài đặt trong cấu hình EDR Agent có trạng thái *Critical* – . Máy tính có trạng thái này là vì thiếu thành phần Bảo vệ mối đe dọa tập tin. Bạn không cần thực hiện hành động nào.

Nếu không thể cài đặt EDR Agent trên máy tính có ứng dụng EPP của bên thứ ba vì trình cài đặt tìm thấy phần mềm không tương thích trên máy tính thì bạn có thể bỏ qua việc kiểm tra phần mềm không tương thích.



Cửa sổ chính của EDR Agent

Bây giờ bạn phải cấu hình tích hợp với giải pháp Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack (EDR) hoặc Kaspersky Anti Targeted Attack (NDR). Bạn cũng có thể chỉ định thiết lập nâng cao của ứng dụng, ví dụ: tạo một khu vực tin tưởng hoặc ẩn giao diện ứng dụng. Thiết lập trong các phần sau khả dụng:

- Kaspersky Security Network
- Thiết lập ứng dụng
- Thiết lập mạng
- Loại trừ
- Báo cáo

- Giao diện
- Quản lý thiết lập

Tích hợp EDR Agent với MDR

EDR Agent được cài đặt trên các máy trạm và máy chủ trong cơ sở hạ tầng CNTT của tổ chức. EDR Agent xử lý dữ liệu và gửi dữ liệu đó qua các luồng của Kaspersky Security Network tới Kaspersky Managed Detection and Response.

Để Kaspersky Managed Detection and Response 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 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.

Thiết lập một kết nối nền trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Settings** → **Integration**.
2. Vào mục **Integration**.
3. Bật nút bật/tắt **Background connection for integration Enabled**.
4. Lưu các thay đổi của bạn.

Việc tích hợp với thành phần Managed Detection and Response của Kaspersky bao gồm các bước sau:

1. **Cài đặt thành phần Managed Detection and Response**

   Bạn có thể chọn thành phần MDR trong quá trình cài đặt hoặc nâng cấp, cũng như sử dụng tác vụ *Thay đổi thành phần ứng dụng*.

   > Để cài đặt thành phần Managed Detection and Response mà không cần khởi động lại máy tính bằng cách sử dụng tác vụ *Thay đổi thành phần ứng dụng*, bạn cần vô hiệu hóa tùy chọn **Kiểm tra các ứng dụng không tương thích của bên thứ ba** trong thiết lập tác vụ.

2. **Cấu hình Kaspersky Private Security Network**

   > 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 Private Security Network khi cài đặt tiện ích MDR.

   Kaspersky Private Security Network (KPSN) 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 và truy cập các dữ liệu thống kê khác mà không cần gửi dữ liệu cho Kaspersky từ máy tính của riêng họ.

   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 Kaspersky Private Security Network, vui lòng tham khảo Trợ giúp của Kaspersky Security Center. 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 Private Security Network 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 <file name>
```

trong đó `<file name>` là tên của tập tin cấu hình chứa thiết lập Kaspersky Private Security Network (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 Kaspersky Private Security Network để xác định danh tiếng của các tập tin, ứng dụng và website. Mục **Kaspersky Security Network** của thiết lập chính sách sẽ hiển thị trạng thái hoạt động sau: *Cơ sở hạ tầng: Kaspersky Private Security Network*.

Bạn phải bật chế độ KSN mở rộng để Managed Detection and Response hoạt động.

3 Kích hoạt Kaspersky Managed Detection and Response

Kể từ Kaspersky Endpoint Security cho Windows 12.10, để kích hoạt chức năng Managed Detection and Response, làm giải pháp thay thế cho mã kích hoạt, bạn cũng có thể sử dụng một tập tin khóa.

Bạn cần mua một giấy phép riêng cho MDR (Tiện ích bổ trợ Kaspersky Managed Detection and Response).

Chức năng này sẽ khả dụng sau khi thêm một khóa riêng cho Phần bổ trợ Kaspersky Managed Detection and Response. Việc cấp giấy phép cho chức năng Managed Detection and Response độc lập cũng giống như việc cấp giấy phép cho Kaspersky Endpoint Security.

Đảm bảo rằng chức năng MDR được gộp trong giấy phép và đang hoạt động trong giao diện cục bộ của ứng dụng.

4 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.

Kể từ Kaspersky Endpoint Security 12.6 cho Windows, việc thêm tập tin BLOB trở thành tùy chọn cho Kaspersky Managed Detection and Response mà không cần thuê nếu bạn có giấy phép hiện tại.

Cách bật thành phần Managed Detection and Response trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**.

4. Chọn hộp kiểm **Managed Detection and Response (Industrial CyberSecurity)**.

5. Trong mục **Thiết lập**, hãy nhấn **Tải lên** và chọn tập tin BLOB nhận được trong Bảng điều khiển Managed Detection and Response của Kaspersky. Tập tin có đuôi mở rộng P7.

   Theo mặc định, người dùng được phép quản lý thiết lập của ứng dụng ("ổ khóa" được mở). Để áp dụng chính sách trên máy tính, hãy đóng ổ khóa .

6. 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 **Asset management** → **Policies**.

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 **Built-in Agents Configuration** → **Managed Detection and Response**.

5. Bật nút bật/tắt **Managed Detection and Response ENABLED**.

6. Nhấn vào **Upload** và chọn tập tin BLOB được lấy trong Bảng điều khiển Managed Detection and Response của Kaspersky. Tập tin có đuôi mở rộng P7.

   Theo mặc định, người dùng được phép quản lý các thiết lập chính sách ("ổ khóa" được mở). Để áp dụng chính sách trên máy tính, hãy đóng ổ khóa .

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 <file name> /login=<user name> /password=<password>
```

   Để thực thi lệnh này, Bảo vệ bằng mật khẩu phải được bật. Người dùng phải có quyền **Cấu hình thiết lập 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 xuống 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 *Report on status of application components*. 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.

5. **Cấu hình các thành phần khác của ứng dụng để nhận đo từ xa**

   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.
   - Phòng chống khai thác.
   - Bảo vệ mối đe dọa web.
   - Bảo vệ mối đe dọa thư điện tử.
   - Bảo vệ mối đe dọa tập tin.
   - Bảo vệ mối đe dọa mạng.
   - Tường lửa.
   - Bảo vệ AMSI.
   - Quét trong nền.

   1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
   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 **Built-in Agents Configuration** → **Managed Detection and Response**.
   5. Bật nút bật/tắt **Managed Detection and Response ENABLED**.
   6. Lưu các thay đổi của bạn.

   1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
   2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
   3. Trong cửa sổ chính sách, hãy chọn **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
   4. Chọn hộp kiểm **Managed Detection and Response (Industrial CyberSecurity)**.
   5. Lưu các thay đổi của bạn.

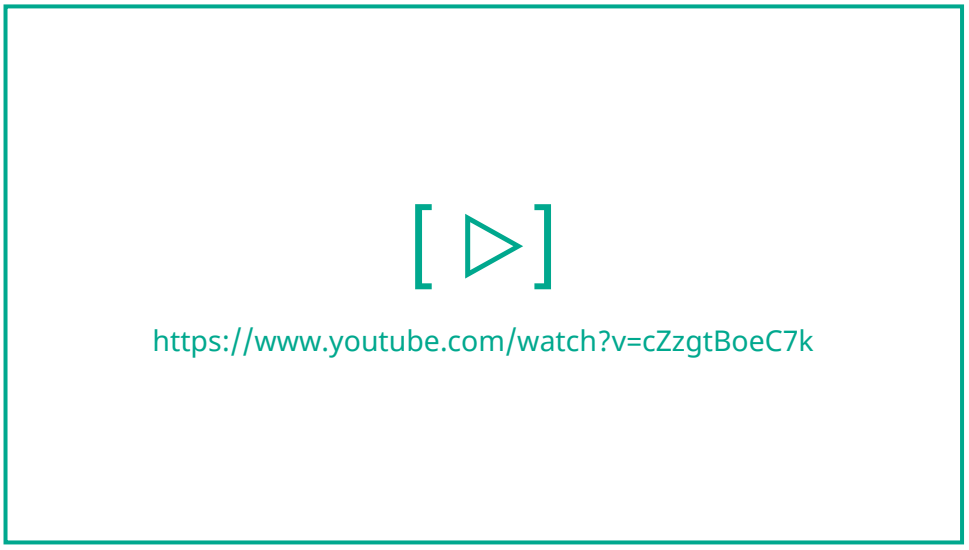
Tích hợp EDR Agent với EDR (KATA)

EDR Agent được cài đặt trên các máy trạm và máy chủ trong cơ sở hạ tầng CNTT của tổ chức. Trên các máy tính này, EDR Agent sẽ liên tục giám sát các tiến trình, kết nối mạng mở và các tập tin đang bị sửa đổi, đồng thời gửi dữ liệu giám sát đến máy chủ có thành phần Central Node.

Để tích hợp với EDR (KATA), bạn phải bật thành phần Endpoint Detection and Response (KATA) và cấu hình EDR Agent.

Phải đáp ứng các điều kiện sau đây để Endpoint Detection and Response (KATA) hoạt động:

- Kaspersky Anti Targeted Attack Platform phiên bản 5.0–7.1.
- Kaspersky Security Center phiên bản 14.2 trở lên. Không thể kích hoạt tính năng Endpoint Detection and Response (KATA) trong các phiên bản trước của Kaspersky Security Center.



https://www.youtube.com/watch?v=cZzgtBoeC7k

Tích hợp với thành phần Endpoint Detection and Response (KATA) liên quan tới các bước sau:

1. **Kích hoạt Endpoint Detection and Response (KATA)**

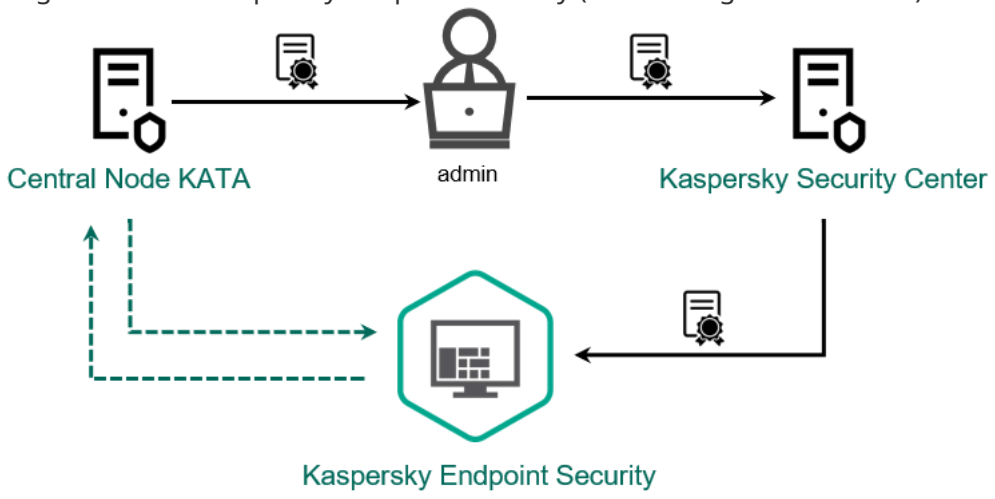
   Bạn cần mua một giấy phép riêng cho EDR (KATA) (Phần bổ trợ Kaspersky Endpoint Detection and Response (KATA)).

   Chức năng này sẽ khả dụng sau khi thêm một khóa riêng cho Kaspersky Endpoint Detection and Response (KATA). Việc cấp giấy phép cho chức năng Endpoint Detection and Response (KATA) độc lập cũng giống như việc cấp giấy phép cho Kaspersky Endpoint Security.

   Đảm bảo rằng chức năng EDR (KATA) được gộp trong giấy phép và đang chạy trong giao diện cục bộ của ứng dụng.

2. **Kết nối với Central Node**

Kaspersky Anti Targeted Attack Platform yêu cầu thiết lập kết nối được tin tưởng giữa Kaspersky Endpoint Security và thành phần Central Node. Để cấu hình kết nối được tin tưởng, bạn phải sử dụng chứng chỉ TLS. Bạn có thể lấy chứng chỉ TLS trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform). Sau đó, bạn phải thêm chứng chỉ TLS vào Kaspersky Endpoint Security (xem hướng dẫn bên dưới).



Thêm chứng chỉ TLS vào Kaspersky Endpoint Security

Theo mặc định, Kaspersky Endpoint Security chỉ kiểm tra chứng chỉ TLS của Central Node. Để cho kết nối bảo mật hơn, bạn có thể kích hoạt thêm xác minh máy tính trên Central Node (xác thực hai chiều). Để bật cơ chế xác minh này, bạn phải bật xác thực hai chiều trong thiết lập của Central Node và Kaspersky Endpoint Security. Để sử dụng xác thực hai chiều, bạn cũng sẽ cần một bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể nhận một bộ chứa mã hóa trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform).

Cách kết nối máy tính Kaspersky Endpoint Security với Central Node bằng Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Detection and Response → Endpoint Detection and Response Expert (on-premises)**.
5. Chọn hộp kiểm **Endpoint Detection and Response Expert (on-premises)**.
6. Nhấn vào **Thiết lập kết nối máy chủ**.
7. Cấu hình kết nối máy chủ:
   - **Thời gian chờ (giây)**. Thời gian chờ phản hồi tối đa của máy chủ Central Node. Khi hết thời gian chờ, Kaspersky Endpoint Security sẽ cố gắng kết nối với một máy chủ Central Node khác.
   - **Chứng chỉ TLS máy chủ**. Chứng chỉ TLS để thiết lập kết nối được tin tưởng với máy chủ Central Node. Bạn có thể lấy chứng chỉ TLS trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform).

- **Sử dụng xác thực hai chiều**. Xác thực hai chiều khi thiết lập kết nối bảo mật giữa Kaspersky Endpoint Security và máy chủ Central Node. Để sử dụng xác thực hai chiều, bạn cần bật xác thực hai chiều trong cài đặt máy chủ Central Node, sau đó lấy bộ chứa mã hóa và đặt mật khẩu để bảo vệ bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể nhận một bộ chứa mã hóa trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform). Sau khi cấu hình thiết lập Central Node, bạn cũng cần bật xác thực hai chiều trong thiết lập của Kaspersky Endpoint Security và tải bộ chứa mã hóa được bảo vệ bằng mật khẩu.

  Bộ chứa mã hóa phải được bảo vệ bằng mật khẩu. Không thể thêm bộ chứa mã hóa có mật khẩu trống.

8. Nhấn vào **OK**.
9. Thêm máy chủ Central Node. Để thực hiện, hãy chỉ định địa chỉ máy chủ (IPv4, IPv6) và cổng để kết nối với máy chủ.

   Bạn có thể thêm nhiều địa chỉ máy chủ Central Node. Kaspersky Endpoint Security sẽ cố gắng kết nối với máy chủ bằng địa chỉ IP đầu tiên. Nếu không thể thiết lập kết nối, Kaspersky Endpoint Security sẽ cố gắng kết nối bằng địa chỉ IP thứ hai trong danh sách, v.v.
10. Nếu cần, hãy cấu hình đo từ xa.
11. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách kết nối máy tính Kaspersky Endpoint Security với Central Node bằng Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)**.
5. Bật nút bật/tắt **Endpoint Detection and Response Expert (on-premises) ENABLED**.
6. Để cấu hình EDR (KATA), hãy chọn **Endpoint Detection and Response Expert (version 7.1 or earlier)** trong danh sách các giải pháp.
7. Nhấn vào **Connection settings**.
8. Cấu hình kết nối máy chủ:

   - **Timeout (sec)**. Thời gian chờ phản hồi tối đa của máy chủ Central Node. Khi hết thời gian chờ, Kaspersky Endpoint Security sẽ cố gắng kết nối với một máy chủ Central Node khác.
   - **Server certificate**. Chứng chỉ TLS để thiết lập kết nối được tin tưởng với máy chủ Central Node. Bạn có thể lấy chứng chỉ TLS trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform).

- **Use two-way authentication**. Xác thực hai chiều khi thiết lập kết nối bảo mật giữa Kaspersky Endpoint Security và máy chủ Central Node. Để sử dụng xác thực hai chiều, bạn cần bật xác thực hai chiều trong cài đặt máy chủ Central Node, sau đó lấy bộ chứa mã hóa và đặt mật khẩu để bảo vệ bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể nhận một bộ chứa mã hóa trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform). Sau khi cấu hình thiết lập Central Node, bạn cũng cần bật xác thực hai chiều trong thiết lập của Kaspersky Endpoint Security và tải bộ chứa mã hóa được bảo vệ bằng mật khẩu.

  Bộ chứa mã hóa phải được bảo vệ bằng mật khẩu. Không thể thêm bộ chứa mã hóa có mật khẩu trống.

9. Nhấn vào **OK**.
10. Thêm máy chủ Central Node. Để thực hiện, hãy chỉ định địa chỉ máy chủ (IPv4, IPv6) và cổng để kết nối với máy chủ.

    Bạn có thể thêm nhiều địa chỉ máy chủ Central Node. Kaspersky Endpoint Security sẽ cố gắng kết nối với máy chủ bằng địa chỉ IP đầu tiên. Nếu không thể thiết lập kết nối, Kaspersky Endpoint Security sẽ cố gắng kết nối bằng địa chỉ IP thứ hai trong danh sách, v.v.
11. Nếu cần, hãy cấu hình đo từ xa.
12. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Kết quả là máy tính được thêm vào bảng điều khiển Kaspersky Anti Targeted Attack Platform. Kiểm tra trạng thái hoạt động của thành phần bằng cách xem *Report on status of application components*. 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 Expert (on-premises)** sẽ được thêm vào danh sách các thành phần của Kaspersky Endpoint Security.

Tích hợp EDR Agent với NDR (KATA)

EDR Agent được cài đặt trên các máy trạm và máy chủ trong cơ sở hạ tầng CNTT của tổ chức. Trên các máy tính này, EDR Agent sẽ liên tục giám sát các tiến trình, kết nối mạng mở và các tập tin đang bị sửa đổi, đồng thời gửi dữ liệu giám sát đến máy chủ có thành phần Central Node.

Để tích hợp với NDR (KATA), bạn phải bật thành phần Network Detection and Response (KATA) và cấu hình EDR Agent.

Phải đáp ứng các điều kiện sau đây để Network Detection and Response (KATA) hoạt động:

- Kaspersky Anti Targeted Attack Platform phiên bản 7.0 trở lên.
- Kaspersky Security Center phiên bản 14.2 trở lên. Không thể kích hoạt tính năng Network Detection and Response (KATA) trong các phiên bản trước của Kaspersky Security Center.

https://www.youtube.com/watch?v=gd-rySv0ThQ

Tích hợp với thành phần Network Detection and Response (KATA) liên quan tới các bước sau:

1. **Kích hoạt Network Detection and Response (KATA)**

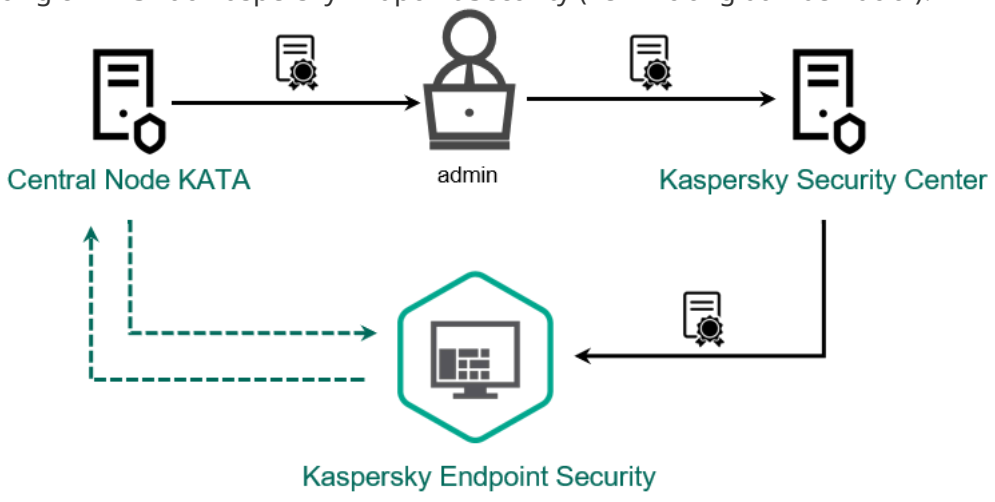
   Bạn cần mua một giấy phép riêng cho NDR (KATA) (Phần bổ trợ Kaspersky Network Detection and Response (KATA)).

   Chức năng này sẽ khả dụng sau khi thêm một khóa riêng cho Kaspersky Network Detection and Response (KATA). Việc cấp giấy phép cho chức năng Network Detection and Response (KATA) độc lập cũng giống như việc cấp giấy phép cho Kaspersky Endpoint Security.

   Đảm bảo rằng chức năng NDR (KATA) được gộp trong giấy phép và đang chạy trong giao diện cục bộ của ứng dụng.

2. **Kết nối với Central Node**

   Kaspersky Anti Targeted Attack Platform yêu cầu thiết lập kết nối được tin tưởng giữa Kaspersky Endpoint Security và thành phần Central Node. Để cấu hình kết nối được tin tưởng, bạn phải sử dụng chứng chỉ TLS. Bạn có thể lấy chứng chỉ TLS trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform). Sau đó, bạn phải thêm chứng chỉ TLS vào Kaspersky Endpoint Security (xem hướng dẫn bên dưới).



Thêm chứng chỉ TLS vào Kaspersky Endpoint Security

Theo mặc định, Kaspersky Endpoint Security chỉ kiểm tra chứng chỉ TLS của Central Node. Để cho kết nối bảo mật hơn, bạn có thể kích hoạt thêm xác minh máy tính trên Central Node (xác thực hai chiều). Để bật cơ chế xác minh này, bạn phải bật xác thực hai chiều trong thiết lập của Central Node và Kaspersky Endpoint Security. Để sử dụng xác thực hai chiều, bạn cũng sẽ cần một bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể nhận một bộ chứa mã hóa trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform).

Cách kết nối máy tính Kaspersky Endpoint Security với Central Node bằng Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Detection and Response → Network Detection and Response (KATA)**.
4. Chọn hộp kiểm **Network Detection and Response (KATA)**.
5. Nhấn vào **Connection settings**.
6. Cấu hình kết nối máy chủ:
   - **Timeout (sec)**. Thời gian chờ phản hồi tối đa của máy chủ Central Node. Khi hết thời gian chờ, Kaspersky Endpoint Security sẽ cố gắng kết nối với một máy chủ Central Node khác.
   - **Server certificate**. Chứng chỉ TLS để thiết lập kết nối được tin tưởng với máy chủ Central Node. Bạn có thể lấy chứng chỉ TLS trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform).
   - **Use two-way authentication**. Xác thực hai chiều khi thiết lập kết nối bảo mật giữa Kaspersky Endpoint Security và máy chủ Central Node. Để sử dụng xác thực hai chiều, bạn cần bật xác thực hai chiều trong cài đặt máy chủ Central Node, sau đó lấy bộ chứa mã hóa và đặt mật khẩu để bảo vệ bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể nhận một bộ chứa mã hóa trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform). Sau khi cấu hình thiết lập Central Node, bạn cũng cần bật xác thực hai chiều trong thiết lập của Kaspersky Endpoint Security và tải bộ chứa mã hóa được bảo vệ bằng mật khẩu.

     Bộ chứa mã hóa phải được bảo vệ bằng mật khẩu. Không thể thêm bộ chứa mã hóa có mật khẩu trống.
7. Nhấn vào **OK**.
8. Thêm máy chủ Central Node. Để thực hiện, hãy chỉ định địa chỉ máy chủ (IPv4, IPv6) và cổng để kết nối với máy chủ.
9. Bạn có thể thêm nhiều địa chỉ máy chủ Central Node. Kaspersky Endpoint Security sẽ cố gắng kết nối với máy chủ bằng địa chỉ IP đầu tiên. Nếu không thể thiết lập kết nối, Kaspersky Endpoint Security sẽ cố gắng kết nối bằng địa chỉ IP thứ hai trong danh sách, v.v.
10. Nếu cần, hãy cấu hình đo từ xa.
11. Lưu các thay đổi của bạn.

Cách kết nối máy tính Kaspersky Endpoint Security với Central Node bằng Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Network Detection and Response (KATA)**.
5. Bật nút bật/tắt **Network Detection and Response (KATA) ENABLED**.
6. Nhấn vào **Connection settings**.
7. Cấu hình kết nối máy chủ:
   - **Timeout (sec)**. Thời gian chờ phản hồi tối đa của máy chủ Central Node. Khi hết thời gian chờ, Kaspersky Endpoint Security sẽ cố gắng kết nối với một máy chủ Central Node khác.
   - **Server certificate**. Chứng chỉ TLS để thiết lập kết nối được tin tưởng với máy chủ Central Node. Bạn có thể lấy chứng chỉ TLS trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform).
   - **Use two-way authentication**. Xác thực hai chiều khi thiết lập kết nối bảo mật giữa Kaspersky Endpoint Security và máy chủ Central Node. Để sử dụng xác thực hai chiều, bạn cần bật xác thực hai chiều trong cài đặt máy chủ Central Node, sau đó lấy bộ chứa mã hóa và đặt mật khẩu để bảo vệ bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể nhận một bộ chứa mã hóa trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform). Sau khi cấu hình thiết lập Central Node, bạn cũng cần bật xác thực hai chiều trong thiết lập của Kaspersky Endpoint Security và tải bộ chứa mã hóa được bảo vệ bằng mật khẩu.

     Bộ chứa mã hóa phải được bảo vệ bằng mật khẩu. Không thể thêm bộ chứa mã hóa có mật khẩu trống.
8. Nhấn vào **OK**.
9. Thêm máy chủ Central Node. Để thực hiện, hãy chỉ định địa chỉ máy chủ (IPv4, IPv6) và cổng để kết nối với máy chủ.
10. Bạn có thể thêm nhiều địa chỉ máy chủ Central Node. Kaspersky Endpoint Security sẽ cố gắng kết nối với máy chủ bằng địa chỉ IP đầu tiên. Nếu không thể thiết lập kết nối, Kaspersky Endpoint Security sẽ cố gắng kết nối bằng địa chỉ IP thứ hai trong danh sách, v.v.
11. Nếu cần, hãy cấu hình đo từ xa.
12. Lưu các thay đổi của bạn.

Kết quả là máy tính được thêm vào bảng điều khiển Kaspersky Anti Targeted Attack Platform. Kiểm tra trạng thái hoạt động của thành phần bằng cách xem *Report on status of application components*. 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 **Network Detection and Response (KATA)** sẽ được thêm vào danh sách các thành phần của Kaspersky Endpoint Security.

Tích hợp Tác nhân EDR với EDR Expert (on-premises)

EDR Agent được cài đặt trên các máy trạm và máy chủ trong cơ sở hạ tầng CNTT của tổ chức. Trên các máy tính này, EDR Agent sẽ liên tục giám sát các tiến trình, kết nối mạng mở và các tập tin đang bị sửa đổi, đồng thời gửi dữ liệu giám sát đến máy chủ EDR Expert (on-premises).

Để tích hợp với EDR Expert (on-premises), bạn phải bật thành phần Endpoint Detection and Response Expert (on-premises) và cấu hình EDR Agent.

Việc tích hợp với thành phần Endpoint Detection and Response Expert (on-premises) bao gồm các bước sau:

1. **Kích hoạt Kaspersky Endpoint Detection and Response Expert (on-premises)**

   Bạn cần mua một giấy phép riêng cho EDR Expert (on-premises) (Phần bổ trợ Kaspersky Endpoint Detection and Response Expert (on-premises)).

   Chức năng này sẽ khả dụng sau khi thêm một khóa riêng cho Kaspersky Endpoint Detection and Response Expert (on-premises). Việc cấp giấy phép cho chức năng Endpoint Detection and Response Expert (on-premises) độc lập cũng giống như việc cấp giấy phép cho Kaspersky Endpoint Security.

   Đảm bảo rằng chức năng EDR Expert (on-premises) được gộp trong giấy phép và đang chạy trong giao diện cục bộ của ứng dụng.

2. **Kết nối với máy chủ thu thập dữ liệu đo từ xa và máy chủ phản hồi**

   Kaspersky Endpoint Detection and Response Expert (on-premises) yêu cầu kết nối tin cậy giữa Kaspersky Endpoint Security và hai máy chủ:

   - *Máy chủ thu thập đo từ xa* là một máy chủ thuộc giải pháp SIEM, có chức năng thu thập, chuẩn hóa, tương quan, phân tích và lưu trữ thông tin về các sự kiện xảy ra trên máy tính.
   - *Máy chủ phản hồi* là một máy chủ dùng để tiếp nhận và quét dữ liệu, nghiên cứu hành vi của các đối tượng và công bố kết quả của các nghiên cứu đó.

   Để cấu hình kết nối được tin tưởng, bạn phải sử dụng chứng chỉ TLS. Bạn có thể lấy chứng chỉ TLS trên Open Single Management Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises)). Sau đó, bạn phải thêm chứng chỉ TLS vào Kaspersky Endpoint Security (xem hướng dẫn bên dưới).

   Theo mặc định, Kaspersky Endpoint Security chỉ kiểm tra chứng chỉ TLS của máy chủ. Để cho kết nối bảo mật hơn, bạn có thể kích hoạt thêm xác minh máy tính trên máy chủ (xác thực hai chiều). Để bật cơ chế xác minh này, bạn phải bật xác thực hai chiều trong thiết lập của máy chủ và Kaspersky Endpoint Security. Để sử dụng xác thực hai chiều, bạn cũng sẽ cần một bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể lấy container mã hóa trên Open Single Management Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises)).

   Cách kết nối máy tính Kaspersky Endpoint Security với EDR Expert (on-premises) bằng Bảng điều khiển web

   1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.
   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 **Built-in Agents Configuration → Endpoint Detection and Response Expert (on-premises)**.

5. Bật nút bật/tắt **Endpoint Detection and Response Expert (on-premises) ENABLED**.

6. Để cấu hình EDR Expert (on-premises), hãy chọn **Endpoint Detection and Response Expert (version 8.0 or later)** trong danh sách các giải pháp.

7. Cấu hình kết nối của *máy chủ thu thập dữ liệu đo từ xa*:

   a. Trong mục **Connection to telemetry collection servers**, hãy nhấn liên kết **Connection settings**.

   b. Cấu hình kết nối của máy chủ thu thập dữ liệu đo từ xa:

   - **Timeout (sec)**. Thời gian chờ phản hồi tối đa của máy chủ. Khi hết thời gian chờ, Kaspersky Endpoint Security sẽ cố gắng kết nối với một máy chủ khác.
   - **Server certificate**. Chứng chỉ TLS để thiết lập kết nối được tin tưởng với máy chủ. Bạn có thể lấy chứng chỉ TLS trên Open Single Management Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises)).
   - **Use two-way authentication**. Xác thực hai chiều khi thiết lập kết nối bảo mật giữa Kaspersky Endpoint Security và máy chủ. Để sử dụng xác thực hai chiều, bạn cần bật xác thực hai chiều trong thiết lập máy chủ, sau đó lấy bộ chứa mã hóa và đặt mật khẩu để bảo vệ bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể lấy container mã hóa trên Open Single Management Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises)). Sau khi cấu hình thiết lập máy chủ, bạn cũng cần bật xác thực hai chiều trong thiết lập của Kaspersky Endpoint Security và tải bộ chứa mã hóa được bảo vệ bằng mật khẩu.

     Bộ chứa mã hóa phải được bảo vệ bằng mật khẩu. Không thể thêm bộ chứa mã hóa có mật khẩu trống.

   c. Nhấn vào **OK**.

   d. Thêm máy chủ thu thập dữ liệu đo từ xa. Để thực hiện, hãy chỉ định địa chỉ máy chủ (IPv4, IPv6) và cổng để kết nối với máy chủ.

   Bạn có thể thêm nhiều địa chỉ máy chủ thu thập đo từ xa. Kaspersky Endpoint Security sẽ cố gắng kết nối với máy chủ bằng địa chỉ IP đầu tiên. Nếu không thể thiết lập kết nối, Kaspersky Endpoint Security sẽ cố gắng kết nối bằng địa chỉ IP thứ hai trong danh sách, v.v.

   e. Nếu cần, hãy cấu hình đo từ xa.

8. Cấu hình kết nối *máy chủ phản hồi*:

   a. Trong mục **Connection to response servers**, hãy cấu hình thiết lập **Send sync request to server every (min)**. Tần suất yêu cầu đồng bộ được gửi đến máy chủ. Trong quá trình đồng bộ, Kaspersky Endpoint Security nhận các tác vụ phản hồi mối đe dọa và gửi kết quả tác vụ.

   b. Nhấn vào liên kết **Connection settings**.

c. Cấu hình kết nối máy chủ phản hồi:

- **Timeout (sec)**. Thời gian chờ phản hồi tối đa của máy chủ. Khi hết thời gian chờ, Kaspersky Endpoint Security sẽ cố gắng kết nối với một máy chủ khác.
- **Server certificate**. Chứng chỉ TLS để thiết lập kết nối được tin tưởng với máy chủ. Bạn có thể lấy chứng chỉ TLS trên Open Single Management Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises)).
- **Use two-way authentication**. Xác thực hai chiều khi thiết lập kết nối bảo mật giữa Kaspersky Endpoint Security và máy chủ. Để sử dụng xác thực hai chiều, bạn cần bật xác thực hai chiều trong thiết lập máy chủ, sau đó lấy bộ chứa mã hóa và đặt mật khẩu để bảo vệ bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể lấy container mã hóa trên Open Single Management Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises)). Sau khi cấu hình thiết lập máy chủ, bạn cũng cần bật xác thực hai chiều trong thiết lập của Kaspersky Endpoint Security và tải bộ chứa mã hóa được bảo vệ bằng mật khẩu.

  Bộ chứa mã hóa phải được bảo vệ bằng mật khẩu. Không thể thêm bộ chứa mã hóa có mật khẩu trống.

d. Nhấn vào **OK**.

e. Thêm máy chủ phản hồi. Để thực hiện, hãy chỉ định địa chỉ máy chủ (IPv4, IPv6) và cổng để kết nối với máy chủ.

Bạn có thể thêm nhiều địa chỉ máy chủ phản hồi. Kaspersky Endpoint Security sẽ cố gắng kết nối với máy chủ bằng địa chỉ IP đầu tiên. Nếu không thể thiết lập kết nối, Kaspersky Endpoint Security sẽ cố gắng kết nối bằng địa chỉ IP thứ hai trong danh sách, v.v.

9. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Kết quả là máy tính được thêm vào Open Single Management Platform (OSMP). Kiểm tra trạng thái hoạt động của thành phần bằng cách xem *Report on status of application components*. 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 Expert (on-premises)** sẽ được thêm vào danh sách các thành phần của Kaspersky Endpoint Security.

Khả năng tương thích với các ứng dụng EPP của bên thứ ba

EDR Agent hỗ trợ chức năng của các giải pháp Kaspersky Detection and Response. Các thành phần bảo vệ và kiểm soát không khả dụng cho EDR Agent. Cấu hình này cho phép cài đặt các ứng dụng EPP của bên thứ ba và triển khai các giải pháp Kaspersky Detection and Response trong cơ sở hạ tầng của tổ chức.

EDR Agent tương thích với ứng dụng EPP của các nhà cung cấp sau:

- **Dr.Web**

  EDR Agent tương thích với Dr.Web cho Windows phiên bản 13 và Dr.Web Server (x64) 13.0.0.10200.

- **Dallas Lock**

  EDR Agent tương thích với Dallas Lock 8.0-C phiên bản 843.2.

Để Tác nhân EDR chạy trên máy tính đã cài đặt phần mềm Dallas Lock, bạn phải cho phép kết nối với các dịch vụ bên ngoài của Kaspersky trong phần cài đặt của mô-đun Tường lửa.

- **Secret Net Studio**

  EDR Agent tương thích với Secret Net Studio phiên bản 8.11 (20851).

  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.

- **Trend Micro**

  EDR Agent tương thích với Trend Micro Vision One (bao gồm Security Agent phiên bản 14.0.20731).

  EDR Agent tương thích với Trend Micro Deep Security phiên bản 20.0.3-18160 (bao gồm Security Agent).

- **Windows Defender**

- **Sophos**

  EDR Agent tương thích với Sophos Intercept X phiên bản 2024.1.2 (bao gồm Endpoint Agent) và Sophos Core Agent phiên bản 2026.2.1.3.

- **Bitdefender**

  EDR Agent tương thích với Bitdefender Endpoint Security Tools phiên bản 8.26.7.647.

- **ESET**

  EDR Agent tương thích với ESET Endpoint Security phiên bản 13.0.2044.0 và ESET Management Agent phiên bản 13.2.1189.0.

Trên máy tính chạy Windows 11 cho Arm64, EDR Agent không tương thích với Bitdefender Endpoint Security Tools.

Các ứng dụng phải được cài đặt theo trình tự sau: đầu tiên, cài đặt ứng dụng EPP, sau đó là Kaspersky Security Center Network Agent, sau đó là EDR Agent. Đây là điều cần thiết vì trình cài đặt ứng dụng EPP có thể phát hiện EDR Agent và Network Agent là phần mềm không tương thích và xóa chúng. Hoạt động của EDR Agent và Network Agent cũng cần được kiểm tra sau khi cập nhật ứng dụng EPP của bên thứ ba vì trình cài đặt của giải pháp có thể quét lại máy tính để tìm phần mềm không tương thích và xóa ứng dụng.

Nếu không thể cài đặt EDR Agent trên máy tính có ứng dụng EPP của bên thứ ba vì trình cài đặt tìm thấy phần mềm không tương thích trên máy tính thì bạn có thể bỏ qua việc kiểm tra phần mềm không tương thích.

Managed Detection and Response



Kaspersky Endpoint Security cho Windows hỗ trợ tích hợp với giải pháp Managed Detection and Response được quản lý. 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.

Các cấu hình của Kaspersky Endpoint Security để tích hợp với MDR

Các cấu hình sau có thể được sử dụng để hoạt động với MDR:

- **[KES+tác nhân tích hợp]**. Trong cấu hình này, Kaspersky Endpoint Security đóng vai trò vừa là ứng dụng đảm bảo khả năng bảo mật của máy tính vừa là ứng dụng để làm việc với MDR.
- **[EPP bên thứ ba+EDR Agent]**. Trong cấu hình này, tính bảo mật của cơ sở hạ tầng CNTT được cung cấp bởi Endpoint Protection Platform (EPP) của bên thứ ba. Khả năng tương tác với MDR được cung cấp bởi Kaspersky Endpoint Security trong cấu hình Endpoint Detection and Response Agent (EDR Agent). Trong cấu hình này, EDR Agent tương thích với các ứng dụng EPP của bên thứ ba.

Tích hợp tác nhân 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.

Để Kaspersky Managed Detection and Response 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 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.

Thiết lập một kết nối nền trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Settings** → **Integration**.
2. Vào mục **Integration**.
3. Bật nút bật/tắt **Background connection for integration Enabled**.
4. Lưu các thay đổi của bạn.

Việc tích hợp với thành phần Managed Detection and Response của Kaspersky bao gồm các bước sau:

1. **Cài đặt thành phần Managed Detection and Response**

   Bạn có thể chọn thành phần MDR trong quá trình cài đặt hoặc nâng cấp, cũng như sử dụng tác vụ *Thay đổi thành phần ứng dụng*.

Để cài đặt thành phần Managed Detection and Response mà không cần khởi động lại máy tính bằng cách sử dụng tác vụ *Thay đổi thành phần ứng dụng*, bạn cần vô hiệu hóa tùy chọn **Kiểm tra các ứng dụng không tương thích của bên thứ ba** trong thiết lập tác vụ.

2 Cấu hình Kaspersky Private Security Network

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 Private Security Network khi cài đặt tiện ích MDR.

Kaspersky Private Security Network (KPSN) 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 và truy cập các dữ liệu thống kê khác mà không cần gửi dữ liệu cho Kaspersky từ máy tính của riêng họ.

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 Kaspersky Private Security Network, vui lòng tham khảo Trợ giúp của Kaspersky Security Center. 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 Private Security Network 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 <file name>
   ```

   trong đó `<file name>` là tên của tập tin cấu hình chứa thiết lập Kaspersky Private Security Network (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 Kaspersky Private Security Network để xác định danh tiếng của các tập tin, ứng dụng và website. Mục **Kaspersky Security Network** của thiết lập chính sách sẽ hiển thị trạng thái hoạt động sau: *Cơ sở hạ tầng: Kaspersky Private Security Network*.

Bạn phải bật chế độ KSN mở rộng để Managed Detection and Response hoạt động.

3 Kích hoạt Kaspersky Managed Detection and Response

Kể từ Kaspersky Endpoint Security cho Windows 12.10, để kích hoạt chức năng Managed Detection and Response, làm giải pháp thay thế cho mã kích hoạt, bạn cũng có thể sử dụng một tập tin khóa.

Kaspersky Managed Detection and Response hỗ trợ các phương thức cấp phép sau:

- Chức năng Managed Detection and Response được hỗ trợ bởi giấy phép Kaspersky Endpoint Security cho Windows.

  Chức năng này khả dụng ngay sau khi kích hoạt Kaspersky Endpoint Security cho Windows.

- Một giấy phép riêng cho MDR (Kaspersky Managed Detection and Response Add-on) được sử dụng.

  Chức năng này sẽ khả dụng sau khi thêm một khóa riêng cho Phần bổ trợ Kaspersky Managed Detection and Response. Kết quả là hai khóa được thêm trên máy tính: một khóa dành cho Kaspersky Endpoint Security và một khóa dành cho Kaspersky Managed Detection and Response.

  Việc cấp giấy phép cho chức năng Managed Detection and Response độc lập cũng giống như việc cấp giấy phép cho Kaspersky Endpoint Security.

Đảm bảo rằng chức năng MDR được gộp trong giấy phép và đang hoạt động trong giao diện cục bộ của ứng dụng.

4 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.

Kể từ Kaspersky Endpoint Security 12.6 cho Windows, việc thêm tập tin BLOB trở thành tùy chọn cho Kaspersky Managed Detection and Response mà không cần thuê nếu bạn có giấy phép hiện tại.

Cách bật thành phần Managed Detection and Response trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**.
4. Chọn hộp kiểm **Managed Detection and Response (Industrial CyberSecurity)**.
5. Trong mục **Thiết lập**, hãy nhấn **Tải lên** và chọn tập tin BLOB nhận được trong Bảng điều khiển Managed Detection and Response của Kaspersky. Tập tin có đuôi mở rộng P7.

   Theo mặc định, người dùng được phép quản lý thiết lập của ứng dụng ("ổ khóa" được mở). Để áp dụng chính sách trên máy tính, hãy đóng ổ khóa .

6. 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 **Asset management → Policies**.
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 **Built-in Agents Configuration** → **Managed Detection and Response**.
5. Bật nút bật/tắt **Managed Detection and Response ENABLED**.
6. Nhấn vào **Upload** và chọn tập tin BLOB được lấy trong Bảng điều khiển Managed Detection and Response của Kaspersky. Tập tin có đuôi mở rộng P7.

   Theo mặc định, người dùng được phép quản lý các thiết lập chính sách ("ổ khóa" được mở 🔓). Để áp dụng chính sách trên máy tính, hãy đóng ổ khóa 🔒.

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 <file name> /login=<user name> /password=<password>
   ```

   Để thực thi lệnh này, Bảo vệ bằng mật khẩu phải được bật. Người dùng phải có quyền **Cấu hình thiết lập 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 xuống 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 *Report on status of application components*. 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.

5 Cấu hình các thành phần khác của ứng dụng để nhận đo từ xa

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.
- Phòng chống khai thác.
- Bảo vệ mối đe dọa web.
- Bảo vệ mối đe dọa thư điện tử.
- Bảo vệ mối đe dọa tập tin.
- Bảo vệ mối đe dọa mạng.
- Tường lửa.

- Bảo vệ AMSI.
- Quét trong nền.

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Managed Detection and Response**.
5. Bật nút bật/tắt **Managed Detection and Response ENABLED**.
6. Lưu các thay đổi của bạn.

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
4. Chọn hộp kiểm **Managed Detection and Response (Industrial CyberSecurity)**.
5. Lưu các thay đổi của bạn.

Hướng dẫn chuyển KEA sang KES cho MDR

Kaspersky Endpoint Security for Windows bao gồm một tác nhân tích hợp cho giải pháp Kaspersky Managed Detection and Response. Bạn không còn cần một ứng dụng Kaspersky Endpoint Agent riêng để fhoạt động với MDR. Tất cả các chức năng của Kaspersky Endpoint Agent sẽ được thực hiện bởi Kaspersky Endpoint Security.

Khi bạn triển khai Kaspersky Endpoint Security trên các máy tính đã cài đặt Kaspersky Endpoint Agent thì giải pháp Kaspersky Managed Detection and Response sẽ tiếp tục hoạt động với Kaspersky Endpoint Security. Ngoài ra, Kaspersky Endpoint Agent sẽ bị gỡ bỏ khỏi máy tính. Hành vi tương tự trong hệ thống sẽ xảy ra khi bạn cập nhật Kaspersky Endpoint Security lên phiên bản 11.6.0 trở lên.

> Kaspersky Endpoint Security không tương thích với Kaspersky Endpoint Agent. Bạn không thể cài đặt cả hai ứng dụng này trên cùng một máy tính.

Các điều kiện sau phải được đáp ứng để Kaspersky Endpoint Security hoạt động như một phần của Kaspersky Managed Detection and Response:

- Kaspersky Security Center phiên bản 13.2 trở lên (bao gồm Network Agent). Không thể kích hoạt tính năng Managed Detection and Response trong các phiên bản trước của Kaspersky Security Center.
- Một kết nối trong nền giữa Bảng điều khiển web Kaspersky Security Center và Máy chủ quản trị được thiết lập. Để MDR 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*.

Các bước để chuyển cấu hình [KES KEA] sang [KES+Tác nhân tích hợp] cho MDR

1. **Nâng cấp Tiện ích quản lý Kaspersky Endpoint Security**

   Thành phần MDR có thể được quản lý bằng Tiện ích quản lý Kaspersky Endpoint Security phiên bản 11.6 trở lên. Tùy thuộc vào loại bảng điều khiển Kaspersky Security Center bạn đang sử dụng, hãy cập nhật tiện ích quản lý trong Bảng điều khiển quản trị (MMC) hoặc tiện ích web trong Bảng điều khiển web.

2. **Chuyển chính sách và tác vụ**

   Chuyển thiết lập của Kaspersky Endpoint Agent sang Kaspersky Endpoint Security cho Windows. Các tùy chọn sau có thể được sử dụng:

   - Một trình hướng dẫn để chuyển từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security. Trình hướng dẫn chuyển từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security chỉ hoạt động trong Bảng điều khiển web

     Cách chuyển thiết lập chính sách và tác vụ từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security trong Bảng điều khiển web

Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Operations → Migration from 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 chính sách Kaspersky Endpoint Agent để chọn chính sách Kaspersky Endpoint Security mà bạn muốn gộp thiết lập. 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 không hỗ trợ các tác vụ MDR. Bỏ qua bước này.

Bước 3. Hoàn tất Trình hướng dẫn

Hoàn tất trình hướng dẫn. Nhờ trình hướng dẫn này, một chính sách Kaspersky Endpoint Security mới sẽ được tạo. 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 *Inactive*. Để tiếp tục, hãy thay đổi trạng thái của chính sách Kaspersky Endpoint Agent và Kaspersky Endpoint Security thành *Inactive* và kích hoạt chính sách mới được gộp.

- Một trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ tiêu chuẩn. Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ chỉ khả dụng trong Bảng điều khiển quản trị (MMC). Để biết thêm chi tiết về Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ, vui lòng tham khảo Trợ giúp của Kaspersky Security Center.

3. **Cấp phép cho chức năng MDR**

   Để kích hoạt Kaspersky Endpoint Security thành một phần của giải pháp Kaspersky Managed Detection and Response, bạn cần có giấy phép riêng cho Phần bổ trợ Kaspersky Managed Detection and Response. Bạn có thể thêm khóa bằng tác vụ *Add key*. Kết quả là hai khóa sẽ được thêm vào ứng dụng: *Kaspersky Endpoint Security* và *Kaspersky Managed Detection and Response*.

4. **Cài đặt / nâng cấp ứng dụng Kaspersky Endpoint Security**

   Để chuyển chức năng MDR trong quá trình cài đặt hoặc nâng cấp ứng dụng, bạn nên sử dụng tác vụ cài đặt từ xa. Khi tạo tác vụ cài đặt từ xa, bạn cần chọn thành phần MDR 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.
   - Cục bộ bằng cách sử dụng Trình hướng dẫn cài đặt.

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 hiện tại của các giải pháp Kaspersky. Do đó, giả sử nếu máy tính được cài đặt Kaspersky Endpoint Agent và giải pháp MDR được kích hoạt thì bộ cài đặt Kaspersky Endpoint Security sẽ tự động cấu hình bộ thành phần và chọn thành phần MDR. 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 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 hiện tại của các giải pháp Kaspersky. Trong trường hợp này, Kaspersky Endpoint Security sẽ tự động chọn các thành phần dựa trên một bộ các thành phần của Kaspersky Endpoint Agent. Sau đó khiến Kaspersky Endpoint Security sẽ chuyển sang sử dụng tác nhân tích hợp và gỡ bỏ Kaspersky Endpoint Agent.

Kaspersky Endpoint Security hỗ trợ nâng cấp mà không cần khởi động lại máy tính. Bạn có thể chọn chế độ nâng cấp ứng dụng trong thuộc tính chính sách.

5. **Kiểm tra hoạt động của ứng dụng**

Nếu sau khi cài đặt hoặc nâng cấp ứng dụng, máy tính có trạng thái *Critical* trong bảng điều khiển Kaspersky Security Center:

- Đảm bảo rằng máy tính được cài đặt Network Agent phiên bản 13.2 trở lên.
- Kiểm tra trạng thái hoạt động của tác nhân tích hợp bằng cách xem *Report on status of application components*. Nếu một thành phần có trạng thái *Not installed* thì hãy cài đặt thành phần này bằng cách sử dụng tác vụ *Change application components*. Nếu một thành phần có trạng thái *Không được giấy phép hỗ trợ* thì hãy đảm bảo rằng bạn đã kích hoạt chức năng tác nhân tích hợp.
- Đảm bảo rằng bạn chấp nhận Tuyên bố Kaspersky Security Network trong chính sách mới của Kaspersky Endpoint Security cho Windows.

Endpoint Detection and Response

Kaspersky Endpoint Security for Windows bao gồm một tác nhân tích hợp cho giải pháp Kaspersky Endpoint Detection and Response Optimum (sau đây gọi là "EDR Optimum"). Kể từ phiên bản 11.8.0, Kaspersky Endpoint Security cho Windows 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.

Các công cụ Threat Intelligence

Kaspersky Endpoint Detection and Response sử dụng các công cụ Threat Intelligence sau:

- Tích hợp với 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.
- 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.
- Công nghệ Cloud Sandbox cho phép bạn chạy các tập tin được phát hiện trong một môi trường cách ly và kiểm tra danh tiếng của chúng.

Nguyên lý hoạt động của giải pháp

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. *Báo động* là một sự kiện trong cơ sở hạ tầng CNTT của công ty mà ứng dụng đã xác định là bất thường hoặc đáng ngờ và có thể gây ra mối đe dọa bảo mật cho cơ sở hạ tầng CNTT của công ty. *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.

Hỗ trợ cho các phiên bản trước của Kaspersky Endpoint Security

Nếu bạn đang sử dụng Kaspersky Endpoint Security 11.2.0–11.6.0, 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.

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).

Tích hợp tác nhân tích hợp với EDR Optimum / EDR Expert

Để thiết lập tích hợp với Kaspersky Endpoint Detection and Response, bạn phải thêm thành phần Endpoint Detection and Response Optimum hoặc thành phần Endpoint Detection and Response Expert (cloud) và cấu hình Kaspersky Endpoint Security.

Các thành phần Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud), và Endpoint Detection and Response Expert (on-premises) không tương thích với nhau.

Phải đáp ứng các điều kiện sau đây để Endpoint Detection and Response hoạt động:

- Kaspersky Security Center phiên bản 13.2 trở lên. Không thể kích hoạt tính năng Endpoint Detection and Response trong các phiên bản trước của Kaspersky Security Center.
- Tiện ích quản lý Kaspersky Endpoint Detection and Response.

  Kể từ Kaspersky Endpoint Security phiên bản 12.6, việc hiển thị thông tin chi tiết về cảnh báo đã được chuyển từ tiện ích quản lý Kaspersky Endpoint Security sang tiện ích quản lý EDR. Tiện ích quản lý EDR là một tiện ích duy nhất để làm việc với các tác nhân trên hệ điều hành Windows, Mac và Linux. Giờ đây, khi làm việc với EDR Optimum, bạn sẽ cần tiện ích quản lý Kaspersky Endpoint Security để tạo các tác vụ ứng phó với mối đe dọa và tiện ích quản lý EDR để xem thông tin chi tiết của cảnh báo.
- Thành phần Endpoint Detection and Response 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.
- 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 Endpoint Detection and Response Optimum hoặc thành phần Endpoint Detection and Response Expert (cloud) trong quá trình cài đặthoặc 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.

     Chức năng này 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).

     Chức năng này sẽ khả dụng sau khi thêm một khóa riêng cho Kaspersky Endpoint Detection and Response. Kết quả là hai khóa được thêm 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.

   Để biết thêm thông tin về Tthỏa thuận giấy phép người dùng cuối của EDR Optimum, hãy xem Trợ giúp của Kaspersky Endpoint Detection and Response Optimum.

3. **Bật các thành phần Endpoint Detection and Response**

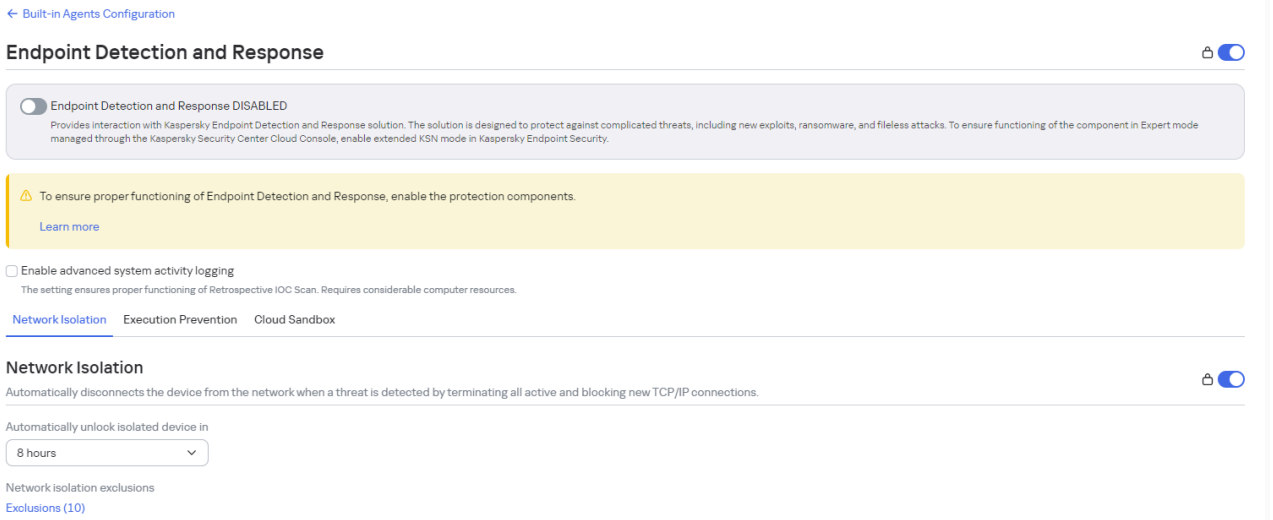
   Bạn có thể bật hoặc tắt thành phần này trong thiết lập chính sách của Kaspersky Endpoint Security cho Windows.

   Cách bật hoặc tắt thành phần Endpoint Detection and Response trong Bảng điều khiển web

   1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.
   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 **Built-in Agents Configuration** → **Endpoint Detection and Response**.
   5. Bật nút bật/tắt **Endpoint Detection and Response ENABLED**.

6. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.



Thiết lập tích hợp EDR

Thành phần Kaspersky Endpoint Detection and Response sẽ được bật. Kiểm tra trạng thái hoạt động của thành phần bằng cách xem *Report on status of application components*. 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 (cloud)** 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. Ví dụ: bạn có thể tải về một tập tin từ khu vực cách ly để phân tích trong Bảng điều khiển web.

- 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. Bạn có thể xem chi tiết về phát hiện và thực hiện các hành động ứng phó 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 **Asset management** → **Policies**.
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** → **KSC Integration**.
5. Trong mục **Data transfer to Administration Server**, hãy nhấn liên kết **Advanced settings**.

6. Trong cửa sổ mở ra, hãy chọn hộp kiểm sau:
   - **About Quarantine files**.
   - **About a threat development chain**.
7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

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 *IOC Scan* cho phép tìm các Dấu hiệu về sự xâm nhập trên máy tính và thực hiện các biện pháp ứng phó với mối 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 IOC Scan

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 tập tin IOC

Kể từ Kaspersky Endpoint Security 12.10 cho Windows, bạn có thể tạo tập tin IOC ngay trong thiết lập tác vụ. Để tạo tập tin IOC, bạn phải chuẩn bị tập tin TXT có danh sách các dấu hiệu xâm nhập. Bạn có thể thêm danh sách các đối tượng sau đây làm các dấu hiệu xâm nhập:

- Mã hash tập tin (MD5 / SHA256).

  Ứng dụng chuẩn bị một tập tin IOC có phạm vi quét FileItem/Md5sum hoặc FileItem/Sha256sum.

- Địa chỉ IP (IPv4, IPv6).
  Ứng dụng chuẩn bị một tập tin IOC có phạm vi quét PortItem/RemoteIP.
- Tên DNS.
  Ứng dụng chuẩn bị một tập tin IOC có phạm vi quét DnsEntryItem/RecordName.

Cách tạo tập tin IOC trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Tasks**.
   Danh sách tác vụ sẽ mở.
2. Chọn tác vụ **IOC Scan**.
   Cửa sổ thuộc tính tác vụ sẽ được mở ra. Nếu cần, hãy tạo tác vụ **IOC Scan**.
3. Chọn thẻ **Application settings**.
4. Vào mục **Threat Scan**.
5. Nhấn vào **Redefine IOC files**.
6. Thao tác này sẽ mở ra biểu mẫu để tạo tập tin IOC:
   a. Trong mục **IOC files source**, hãy chọn **Generate from file**.
   b. Nhập tên của tập tin IOC.
   c. Chọn tập tin TXT chứa danh sách các dấu hiệu xâm nhập.
   d. Chọn loại tập tin IOC: **DNS names**, **File hashes**, **IP addresses**.
   e. Nhấn vào **Upload**.

   Kaspersky Endpoint Security sẽ thêm các tập tin IOC vào bộ sưu tập IOC. Nếu cần, bạn có thể tạm thời loại trừ các tập tin IOC khỏi phạm vi tác vụ.
7. Lưu các thay đổi của bạn.

Tạo một tác vụ IOC Scan

Bạn có thể tạo các tác vụ *IOC Scan* 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.

Không thể chạy tác vụ nhóm *IOC Scan* nếu tích hợp với Kaspersky Endpoint Detection and Response Expert (on-premises) hoặc Kaspersky Endpoint Detection and Response Expert (cloud) được cấu hình trên các máy tính đang được quét. Trong trường hợp này, bạn nên sử dụng hành động phản hồi *Quét IOC* nhằm tìm kiếm các dấu hiệu xâm nhập. Để biết thêm chi tiết, vui lòng tham khảo mục trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises).

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 ra một tác vụ IOC Scan:

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

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **Add**.

   Trình hướng dẫn Tác vụ sẽ được bắt đầu.

3. Cấu hình các thiết lập của tác vụ:

   a. Trong danh sách thả xuống **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.

   b. Trong danh sách thả xuống **Task type**, hãy chọn **IOC Scan**.

   c. Trong trường **Task name**, hãy nhập một mô tả ngắn.

   d. Trong phần **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 *IOC Scan* 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. Hoàn tất 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 **Threat Scan**.

10. Tải lên các tập tin IOC để tìm kiếm các dấu hiệu xâm nhập.

    Sau khi bạn tải lên các tập tin IOC, ứng dụng sẽ hiển thị thông tin tóm tắt về tập tin, bao gồm danh sách các chỉ số không vượt qua kiểm tra. Sau khi tải lên các tập tin IOC, bạn có thể chỉnh sửa thủ công các tập tin đó trong trình chỉnh sửa tích hợp trực tiếp trong thuộc tính tác vụ. Kaspersky Endpoint Security hỗ trợ chỉnh sửa các tập tin IOC tuân thủ tiêu chuẩn OpenIOC 1.1. Không thể chỉnh sửa nội dung của các tập tin IOC tuân thủ phiên bản OpenIOC 1.0.

    Kaspersky Endpoint Security sẽ thêm các tập tin IOC vào bộ sưu tập IOC. Nếu cần, bạn có thể tạm thời loại trừ các tập tin IOC khỏi phạm vi tác vụ.

    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. Nếu cần, hãy chọn hộp kiểm **Retrospective IOC Scan**. *Quét IOC hồi cứu* là một chế độ của tác vụ *IOC Scan*, trong đó Kaspersky Endpoint Security sẽ quét để tìm dấu hiệu về sự xâm nhập bằng cách sử dụng dữ liệu trong một khoảng thời gian nhất định. Chế độ này được thiết kế để tìm kiếm các dấu hiệu xâm nhập thông qua dữ liệu đo từ xa của máy tính được bảo vệ, chẳng hạn như hoạt động mạng, các tiến trình, tập tin và các dữ liệu đo từ xa khác. Kaspersky Endpoint Security phân tích dữ liệu trong nhật ký hệ điều hành và nhật ký trình duyệt trên máy tính. Quét IOC hồi cứu sẽ phân tích nhật ký của các trình duyệt sau: Google Chrome, Mozilla Firefox, Microsoft Edge (phiên bản 79 trở lên).

12. Cấu hình các hành động khi phát hiện IOC:

    - **Isolate device 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.

      Nếu bỏ chọn hộp kiểm này, bạn có thể cô lập máy tính khỏi mạng sau khi chạy tác vụ theo cách thủ công. Nếu tác vụ *IOC Scan* phát hiện một IOC, bạn có thể cô lập máy tính khỏi mạng trực tiếp từ IOC (thuộc tính của tác vụ *IOC Scan* → **Application settings** → **IOC Scan results**). Kaspersky Endpoint Security cũng cho phép quản lý ngay lập tức các thiết lập bổ sung: Khoảng thời gian vô hiệu hóa cô lập mạng và Loại trừ cô lập mạng.

- **Move copy to Quarantine, delete object**. 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.

  Nếu bỏ chọn hộp kiểm này, bạn có thể cách ly tập tin theo cách thủ công sau khi chạy tác vụ theo cách thủ công. Nếu tác vụ *IOC Scan* phát hiện tập tin có thể gây nguy hiểm cho dữ liệu, bạn có thể cách ly tập tin này trực tiếp khỏi kết quả Quét IOC (**Application settings → IOC Scan results**). Kết quả là Kaspersky Endpoint Security sẽ khởi động trình hướng dẫn tạo tác vụ với dữ liệu có sẵn của tập tin đã phát hiện. Bạn chỉ cần quản lý các thiết lập tác vụ bổ sung, ví dụ như thiết lập lịch tác vụ.

  Nếu cần, hãy chọn hộp kiểm **Apply to system critical objects**. System Critical Object (SCO) bao gồm các tập tin mà hệ điều hành cần để hoạt động.

  > Chúng tôi không khuyến nghị áp dụng hành động đối với các tập tin SCO. Làm vậy có thể khiến hệ điều hành không ổn định hoặc không khởi động được.

- **Run Critical Areas Scan**. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ chạy tác vụ *Critical Areas Scan*. Theo mặc định, Kaspersky Endpoint Security sẽ quét nhân kernel, các tiến trình đang chạy, và phân vùng khởi động ổ đĩa.

13. Vào mục **Advanced**.

14. 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 *IOC Scan* 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 Log - 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.

      > Đối với thuật ngữ IOC EventLogItem\source, hãy sử dụng giá trị **Tên nhà cung cấp** từ lược đồ XML của sự kiện.

    - **Windows Registry - RegistryItem**. Cấu hình phạm vi quét IOC trong registry.

      Theo mặc định, Kaspersky Endpoint Security sẽ quét một tập hợp khóa registry.

15. Trong cửa sổ thuộc tính tác vụ, hãy chọn thẻ **Schedule**.

16. 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.

17. Lưu các thay đổi của bạn.

18. Chọn hộp kiểm cạnh tác vụ.

19. Nhấn vào **Start**.

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 **Results**. 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**. Trong kết quả quét IOC, bạn cũng có thể cách ly tập tin được phát hiện hoặc cô lập máy tính khỏi mạng theo cách thủ công.

Kaspersky Endpoint Security tìm kiếm các bản ghi trùng lặp được tạo cho cùng một tập tin IOC và chỉ giữ lại các bản ghi duy nhất trong kết quả tác vụ. Các bản ghi trùng lặp là các bản ghi cùng loại có cùng giá trị ở tất cả các trường được so sánh. Ứng dụng cũng có thể không tạo bản ghi nếu bản ghi đó thiếu giá trị trong một hoặc nhiều trường (xem bảng bên dưới).

Loại	So sánh các trường	Điều kiện để không tạo bản ghi
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• Thiếu giá trị của các trường FullPath, Md5sum, Sha256sum. • Thiếu giá trị của các trường FullPath và các giá trị giống hệt nhau của các trường Md5sum, Sha256sum.
RegistryItem	• Hive • KeyPath • ValueName • Text • Type	Thiếu giá trị ở ít nhất một trong các trường sau: Hive, KeyPath, ValueName.
ProcessItem	• startTime • PID	Thiếu giá trị của các trường startTime hoặc PID.

Cửa sổ **Alert Details** có thể hiển thị các bản ghi RegistryItem có các giá trị trường giống hệt nhau. Những bản ghi như vậy không phải là bản ghi trùng lặp vì chúng có giá trị khác nhau trong trường Văn bản, là điều không được hiển thị trên giao diện.

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.

Thông tin đo từ xa mở rộng cho tác vụ Quét IOC

Bạn nên bật tính năng đo từ xa mở rộng trên máy tính để quét IOC hồi cứu. Việc mở rộng đo từ xa giúp cải thiện độ chính xác của việc phát hiện IOC, nhưng lại tiêu tốn nhiều tài nguyên máy tính hơn.

Tính năng đo từ xa mở rộng bao gồm hỗ trợ các từ bổ sung sau:

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes

- FileItem/Created
- FileItem/Modified
- FileItem/Changed
- FileItem/Accessed
- FileItem/FileAttributes

Nếu tính đo từ xa mở rộng bị vô hiệu hóa, Kaspersky Endpoint Security có thể sẽ thay đổi thông tin về các dấu hiệu xâm nhập đã phát hiện.

Để kích hoạt đo từ xa mở rộng:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Chọn hộp kiểm **Enable advanced system activity logging**.
6. Lưu các thay đổi của bạn.

Di chuyển tập tin đến Khu vực cách ly

Khi phản ứng với các mối đe dọa, Kaspersky Endpoint Detection and Response có thể tạo các tác vụ *Move file to Quarantine*. 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 được tích hợp với các giải pháp của Kaspersky 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, Trợ giúp của Kaspersky Endpoint Detection and Response Expert, Trợ giúp của Kaspersky Anti Targeted Attack Platform và Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises).

Bạn có thể tạo các tác vụ *Move file to Quarantine* 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.

- Trong thiết lập tác vụ *IOC Scan*.

  Nếu tác vụ *IOC Scan* phát hiện tập tin có thể gây nguy hiểm cho dữ liệu, bạn có thể cách ly tập tin này trực tiếp khỏi kết quả Quét IOC (**Application settings → IOC Scan results**). Kết quả là Kaspersky Endpoint Security sẽ khởi động trình hướng dẫn tạo tác vụ với dữ liệu có sẵn của tập tin đã phát hiện. Bạn chỉ cần quản lý các thiết lập tác vụ bổ sung, ví dụ như thiết lập lịch tác vụ.

Tác vụ *Move file to Quarantine* có những hạn chế sau:

1. Kích thước tập tin không được vượt quá 100 MB.
2. Bạn không thể xóa các tập tin cần thiết cho hoạt động của Kaspersky Endpoint Security cho Windows:
   - Các tập tin trong phạm vi công nghệ tự bảo vệ của Kaspersky Endpoint Security cho Windows
   - Các tập tin được ký số bởi Kaspersky
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.
4. Bạn không thể quét một đối tượng bị cách ly do kết quả của tác vụ *Move file to Quarantine*.

Để tạo ra một tác vụ Move file to Quarantine:

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

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **Add**.

   Trình hướng dẫn Tác vụ sẽ được bắt đầu.

3. Cấu hình các thiết lập của tác vụ:

   a. Trong danh sách thả xuống **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.

   b. Trong danh sách thả xuống **Task type**, hãy chọn **Move file to Quarantine**.

   c. Trong trường **Task name**, hãy nhập một mô tả ngắn.

   d. Trong phần **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 vào **Next**.
5. Nhập thông tin đăng nhập tài khoản của người dùng có quyền mà bạn muốn sử dụng để chạy tác vụ. Nhấn vào **Next**.

   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 **Finish**.

   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. Nếu cần, hãy chọn hộp kiểm **Apply to system critical objects**.

   System Critical Object(SCO) bao gồm các tập tin mà hệ điều hành cần để hoạt động.

   > Chúng tôi không khuyến nghị áp dụng hành động đối với các tập tin SCO. Làm vậy có thể khiến hệ điều hành không ổn định hoặc không khởi động được.

10. Trong danh sách tập tin, hãy nhấn vào **Add**.

    Trình hướng dẫn thêm tập tin sẽ khởi chạy.

11. 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*.

12. Trong cửa sổ thuộc tính tác vụ, hãy chọn thẻ **Schedule**.

13. 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.

14. Lưu các thay đổi của bạn.

15. Chọn hộp kiểm cạnh tác vụ.

16. Nhấn vào **Start**.

    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 Done, nhưng bản thân tập tin chỉ được 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.

Nếu tập tin bị khóa bởi một tiến trình khác, tác vụ sẽ được hiển thị dưới dạng *Completed*, nhưng bản thân tập tin chỉ được 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 *Move file to Quarantine* có thể kết thúc kèm theo 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 *Move file to Quarantine* có thể kết thúc kèm theo lỗi *Không đủ không gian trống trong ổ lưu trữ của Khu vực cách ly* nếu bạn đang cố gắng 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. Kết quả của việc thực hiện tác vụ là một bản sao tập tin được lưu trong Khu vực cách ly. *Khu vực cách ly* là một kho lưu trữ cục bộ đặc biệt trên máy tính. Bạn có thể tải tập tin này từ Khu vực cách ly xuống máy tính của mình bằng Bảng điều khiển web (**Operations** → **Repositories** → **Quarantine**). Trên máy tính của người dùng, tập tin vẫn nằm trong thư mục gốc của nó.

Kích thước tập tin không được vượt quá 2 GB.

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 ra một tác vụ Lấy tập tin:

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

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **Add**.

   Trình hướng dẫn Tác vụ sẽ được bắt đầu.

3. Cấu hình các thiết lập của tác vụ:

   a. Trong danh sách thả xuống **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.

   b. Trong danh sách thả xuống **Task type**, hãy chọn **Get file**.

   c. Trong trường **Task name**, hãy nhập một mô tả ngắn.

   d. Trong phần **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 vào **Next**.

5. Nhập thông tin đăng nhập tài khoản của người dùng có quyền mà bạn muốn sử dụng để chạy tác vụ. Nhấn vào **Next**.

   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 **Finish**.
   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 **Add**.
   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 **Schedule**.
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. Lưu các thay đổi của bạn.
14. Chọn hộp kiểm cạnh tác vụ.
15. Nhấn vào **Start**.

    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 *Delete file*. Ví dụ: bạn có thể xóa từ xa một tập tin khi ứng phó với các mối đe dọa.

Bạn không thể xóa các tập tin cần thiết cho hoạt động của Kaspersky Endpoint Security cho Windows:

- Các tập tin trong phạm vi công nghệ tự bảo vệ của Kaspersky Endpoint Security cho Windows
- Các tập tin được ký số bởi Kaspersky

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 ra một tác vụ Delete file:

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

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **Add**.

   Trình hướng dẫn Tác vụ sẽ được bắt đầu.

3. Cấu hình các thiết lập của tác vụ:

   a. Trong danh sách thả xuống **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.

   b. Trong danh sách thả xuống **Task type**, hãy chọn **Delete file**.

   c. Trong trường **Task name**, hãy nhập một mô tả ngắn.

   d. Trong phần **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 vào **Next**.

5. Nhập thông tin đăng nhập tài khoản của người dùng có quyền mà bạn muốn sử dụng để chạy tác vụ. Nhấn vào **Next**.

   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 **Finish**.

   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 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*.

10. Nếu cần, hãy chọn hộp kiểm **Apply to system critical objects**.

    System Critical Object(SCO) bao gồm các tập tin mà hệ điều hành cần để hoạt động.

    Chúng tôi không khuyến nghị áp dụng hành động đối với các tập tin SCO. Làm vậy có thể khiến hệ điều hành không ổn định hoặc không khởi động được.

11. Trong cửa sổ thuộc tính tác vụ, hãy chọn thẻ **Schedule**.

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. Lưu các thay đổi của bạn.

14. Chọn hộp kiểm cạnh tác vụ.

15. Nhấn vào **Start**.

    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 *Done*, 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 *Delete file* có thể hoàn thành với lỗi *Access denied or file not found* 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 tập tin từ xa bằng cách sử dụng tác vụ *Process start*. 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 *Get file* 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 ra một tác vụ Process start:

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

   Danh sách tác vụ sẽ mở.

2. Nhấn vào **Add**.

   Trình hướng dẫn Tác vụ sẽ được bắt đầu.

3. Cấu hình các thiết lập của tác vụ:

   a. Trong danh sách thả xuống **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.

   b. Trong danh sách thả xuống **Task type**, hãy chọn **Process start**.

   c. Trong trường **Task name**, hãy nhập một mô tả ngắn.

   d. Trong phần **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 vào **Next**.

5. Nhập thông tin đăng nhập tài khoản của người dùng có quyền mà bạn muốn sử dụng để chạy tác vụ. Nhấn vào **Next**.

   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 **Finish**.

   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.

    Giả sử 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` trong thư mục hiện tại (theo mặc định). Tiện ích nằm ở thư mục `C:\Users\admin\Diagnostic\`. Bạn phải lưu tập tin cấu hình trong thư mục `C:\Users\admin\Documents\Configuration`. Nhập các giá trị sau:

    - **Executable command** – `C:\Users\admin\Diagnostic\utility.exe`
    - **Command line arguments (optional)** – `/R conf.txt`
    - **Path to the working folder (optional)** – `C:\Users\admin\Documents\Configuration`

11. Trong cửa sổ thuộc tính tác vụ, hãy chọn thẻ **Schedule**.

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. Lưu các thay đổi của bạn.

14. Chọn hộp kiểm cạnh tác vụ.

15. Nhấn vào **Start**.

    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 **Execution results**.

Chấm dứt tiến trình

Bạn có thể chấm dứt các tiến trình từ xa bằng cách sử dụng tác vụ *Terminate process*. Ví dụ: bạn có thể chấm dứt từ xa tiện ích kiểm tra tốc độ Internet đã được khởi chạy bằng tác vụ *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 *Terminate process* có những hạn chế sau:

Bạn không thể chấm dứt các tiến trình của tập tin cần thiết cho hoạt động của Kaspersky Endpoint Security cho Windows:

- Các tập tin trong phạm vi công nghệ tự bảo vệ của Kaspersky Endpoint Security cho Windows
- Các tập tin được ký số bởi Kaspersky

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 ra một tác vụ Terminate process:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Tasks**.
   Danh sách tác vụ sẽ mở.
2. Nhấn vào **Add**.
   Trình hướng dẫn Tác vụ sẽ được bắt đầu.
3. Cấu hình các thiết lập của tác vụ:
   a. Trong danh sách thả xuống **Application**, hãy chọn **Kaspersky Endpoint Security for Windows 14.2**.
   b. Trong danh sách thả xuống **Task type**, hãy chọn **Terminate process**.
   c. Trong trường **Task name**, hãy nhập một mô tả ngắn.
   d. Trong phần **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 vào **Next**.
5. Nhập thông tin đăng nhập tài khoản của người dùng có quyền mà bạn muốn sử dụng để chạy tác vụ. Nhấn vào **Next**.

   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 **Finish**.
   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. Nếu cần, hãy chọn hộp kiểm **Apply to system critical objects**.
   System Critical Object(SCO) bao gồm các tập tin mà hệ điều hành cần để hoạt động.

Chúng tôi không khuyến nghị áp dụng hành động đối với các tập tin SCO. Làm vậy có thể khiến hệ điều hành không ổn định hoặc không khởi động được.

10. 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*.

    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 *File not found*.

11. Trong cửa sổ thuộc tính tác vụ, hãy chọn thẻ **Schedule**.

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. Nhấn vào **Save**.

14. Chọn hộp kiểm cạnh tác vụ.

15. Nhấn vào **Start**.

    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 **Results**.

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 đường dẫn thư mục và giá trị hash của tập tin.

Bạn cũng có thể quản lý Phòng chống thực thi cục bộ bằng dòng lệnh.

Tính năng Phòng chống thực thi có các hạn chế sau:

1. 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.

2. Bạn không thể áp dụng quy tắc ngăn chặn cho các tập tin cần thiết cho hoạt động của Kaspersky Endpoint Security cho Windows:

   - Các tập tin trong phạm vi công nghệ tự bảo vệ của Kaspersky Endpoint Security cho Windows

   - Các tập tin được ký số bởi Kaspersky

3. Bạn không nên tạo nhiều hơn 5000 quy tắc ngăn chặn chạy vì điều này có thể khiến hệ thống không ổn định.

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 số liệu 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 **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Chọn thẻ **Execution Prevention**.
6. Bật nút bật/tắt **Execution Prevention ENABLED**.
7. Trong mục **Action on execution or opening of forbidden object**, hãy chọn chế độ hoạt động của thành phần:

   - **Block and add to event log**. 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.

     Nếu cần, hãy chọn hộp kiểm **Apply to system critical objects**. System Critical Object (SCO) bao gồm các tập tin mà hệ điều hành cần để hoạt động.

     Chúng tôi không khuyến nghị áp dụng hành động đối với các tập tin SCO. Làm vậy có thể khiến hệ điều hành không ổn định hoặc không khởi động được.

   - **Add to event log**. 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.
8. Tạo danh sách các quy tắc phòng chống thực thi:

   a. Nhấn vào **Add**.

   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 **Type**, hãy chọn đối tượng mà bạn muốn chặn: **Executable file**, **Script**, **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 giá trị hash và đường dẫn thư mục.

> 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.

9. 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 chạy. 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.

- Kết nối tới SVM và Máy chủ tích hợp nếu ứng dụng đang được sử dụng trong Chế độ Light Agent.
- Kết nối với KSN khi tích hợp ứng dụng với Kaspersky Managed Detection and Response.

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 **Asset management** → **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 *IOC Scan*.
3. Chọn thẻ **Application settings**.
4. Chọn phần **Response settings**.
5. Trong mục **Configure response actions on IOC detection**, hãy chọn **Alert and response** và chọn hộp kiểm **Isolate device from the network**.
6. 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.

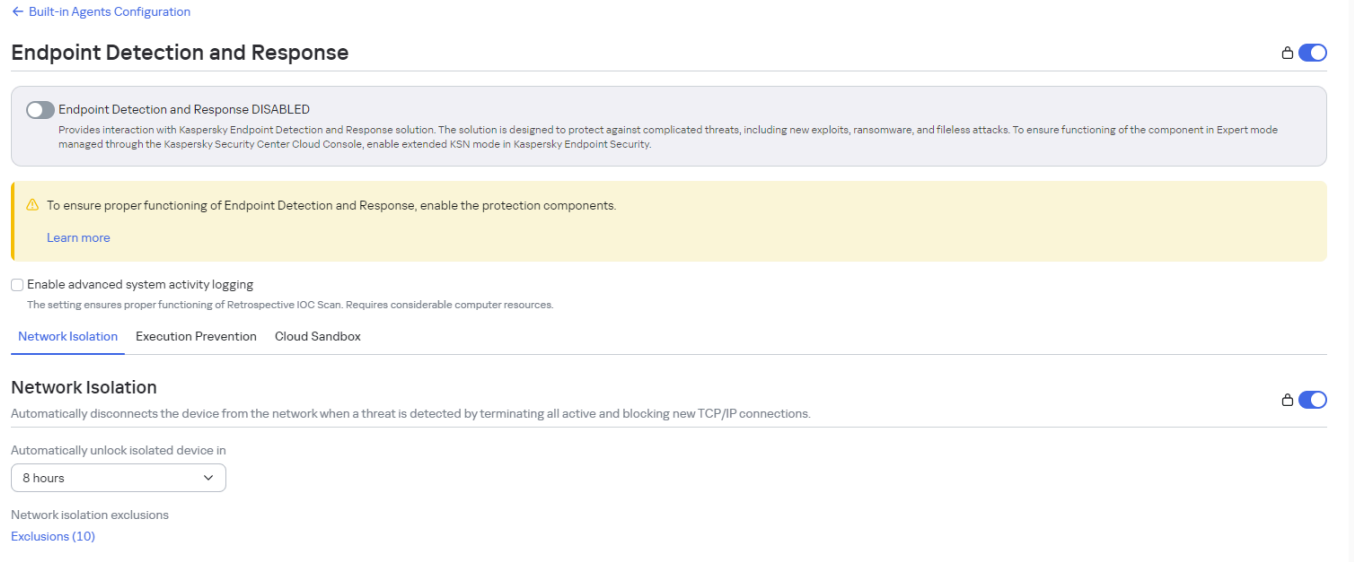
Bạn có thể cấu hình để tắt Cách ly mạng tự động sau một khoảng thời gian nhất định. Theo mặc định, ứng dụng sẽ tắt Cách ly mạng sau 8 giờ kể từ thời điểm tính năng này được bật. Bạn cũng có thể tắt Cách ly mạng theo cách thủ công (xem hướng dẫn bên dưới). Sau khi tắt Cách ly mạng, máy tính có thể sử 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 thẻ **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Chọn thẻ **Network Isolation**.

6. Chọn độ trễ để tắt Cách ly mạng.

7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.



Thiết lập tích hợp EDR

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.

- Trong thiết lập tác vụ *IOC Scan*.

  Nếu tác vụ *IOC Scan* phát hiện một IOC, bạn có thể cô lập máy tính khỏi mạng trực tiếp từ IOC (thuộc tính của tác vụ *IOC Scan* → **Application settings** → **IOC Scan results**). Kaspersky Endpoint Security cũng cho phép quản lý ngay lập tức các thiết lập bổ sung: Khoảng thời gian vô hiệu hóa cô lập mạng và Loại trừ cô lập mạng.

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 **Asset management** → **Assets (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 14.2**.
   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 để tắt Cách ly mạng tự động sau một khoảng thời gian nhất 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 **Asset management → Assets (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 **Asset management → Assets (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 14.2**.
   Việc này sẽ mở ra thiết lập cục bộ của ứng dụng.
5. Chọn thẻ **Application settings**.
6. Vào **Built-in Agents Configuration → 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.

Kể từ Kaspersky Endpoint Security 12.10 cho Windows, bạn có thể quản lý tính năng Cô lập mạng trong phần chi tiết cảnh báo. Ngoài ra, trong phần chi tiết cảnh báo, bạn có thể chỉ định khoảng thời gian cô lập mạng 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.

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 **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Chọn thẻ **Network Isolation**.
6. Trong mục **Network isolation exclusions**, hãy nhấn vào **Exclusions**.
7. Thao tác này mở ra một cửa sổ; trong cửa sổ này, hãy nhấn vào **Add** → **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** → **Add** và chỉnh sửa thiết lập kết nối mạng một cách thủ công.
9. 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 **Asset management** → **Assets (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.

Kể từ Kaspersky Endpoint Security 12.10 cho Windows, bạn có thể thêm tùy chọn loại trừ cô lập mạng vào chi tiết cảnh báo. 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.

Cloud Sandbox

Cloud Sandbox là công nghệ cho phép bạn phát hiện các mối đe dọa nâng cao trên máy tính. Kaspersky Endpoint Security sẽ tự động chuyển tiếp các tập tin được phát hiện tới Cloud Sandbox để phân tích. Cloud Sandbox sẽ chạy các tập tin này trong một môi trường cách ly để xác định hoạt động độc hại và quyết định danh tiếng của chúng. Sau đó, dữ liệu về các tập tin này sẽ được gửi đến Kaspersky Security Network. Do đó, nếu Cloud Sandbox đã phát hiện ra tập tin độc hại thì Kaspersky Endpoint Security sẽ thực hiện hành động thích hợp để loại bỏ mối đe dọa này trên tất cả các máy tính nơi tập tin này được phát hiện.

Để Cloud Sandbox hoạt động, bạn phải cho phép sử dụng Kaspersky Security Network.

Nếu bạn đang sử dụng Kaspersky Security Network Riêng thì công nghệ Cloud Sandbox sẽ không khả dụng.

Công nghệ Cloud Sandbox được bật vĩnh viễn và khả dụng cho tất cả người dùng Kaspersky Security Network bất kể họ đang sử dụng loại giấy phép nào. Nếu đã triển khai giải pháp Endpoint Detection and Response Optimum, bạn có thể bật một bộ đếm riêng cho các mối đe dọa được Cloud Sandbox phát hiện. Bạn có thể sử dụng bộ đếm này để biên soạn số liệu thống kê khi phân tích các mối đe dọa được phát hiện. Kaspersky Endpoint Security cho biết công nghệ phát hiện mối đe dọa Cloud Sandbox trong *Report on threats* trong bảng điều khiển Kaspersky Security Center.



Bộ đếm mối đe dọa

Để bật bộ đếm Cloud Sandbox:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Chọn thẻ **Cloud Sandbox**.
6. Bật nút bật/tắt **Cloud Sandbox ENABLED**.
7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Bất cứ khi nào có mối đe dọa, Kaspersky Endpoint Security sẽ kích hoạt bộ đếm các mối đe dọa được phát hiện bằng Cloud Sandbox trong cửa sổ chính của ứng dụng trong **Công nghệ phát hiện mối đe dọa**. Kaspersky Endpoint Security cũng sẽ chỉ báo công nghệ phát hiện mối đe dọa Cloud Sandbox trong *Report on threats* trong bảng điều khiển Kaspersky Security Center.

Hướng dẫn chuyển KEA sang KES cho EDR Optimum

Kaspersky Endpoint Security for Windows bao gồm một tác nhân tích hợp cho giải pháp Kaspersky Endpoint Detection and Response Optimum. Bạn không còn cần một ứng dụng Kaspersky Endpoint Agent riêng để fhoạt động với EDR Optimum. Tất cả các chức năng của Kaspersky Endpoint Agent sẽ được thực hiện bởi Kaspersky Endpoint Security.

Khi bạn triển khai Kaspersky Endpoint Security trên các máy tính đã cài đặt Kaspersky Endpoint Agent thì giải pháp Kaspersky Endpoint Detection and Response Optimum sẽ tiếp tục hoạt động với Kaspersky Endpoint Security. Ngoài ra, Kaspersky Endpoint Agent sẽ bị gỡ bỏ khỏi máy tính. Hành vi tương tự trong hệ thống sẽ xảy ra khi bạn cập nhật Kaspersky Endpoint Security lên phiên bản 11.7.0 trở lên.

> Kaspersky Endpoint Security không tương thích với Kaspersky Endpoint Agent. Bạn không thể cài đặt cả hai ứng dụng này trên cùng một máy tính.

Các điều kiện sau phải được đáp ứng để Kaspersky Endpoint Security hoạt động như một phần của Kaspersky Endpoint Detection and Response Optimum:

- Kaspersky Endpoint Detection and Response Optimum phiên bản 2.0 trở lên.
- Kaspersky Security Center phiên bản 13.2 trở lên (bao gồm Network Agent). Không thể kích hoạt tính năng EDR Optimum trong các phiên bản trước của Kaspersky Security Center.
- Chỉ có thể quản lý EDR Optimum bằng Bảng điều khiển web Kaspersky Security Center.
- Truyền dữ liệu đến Máy chủ quản trị 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.
- Một kết nối trong nền giữa Bảng điều khiển web Kaspersky Security Center và Máy chủ quản trị được thiết lập. Để EDR Optimum 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*.

Các bước để chuyển cấu hình [KES KEA] sang [KES+Tác nhân tích hợp] cho EDR Optimum

1. **Nâng cấp tiện ích web Kaspersky Endpoint Security**

   Thành phần EDR Optimum có thể được quản lý bằng Tiện ích Web Kaspersky Endpoint Security phiên bản 11.7.0 trở lên.

2. **Chuyển chính sách và tác vụ**

   Chuyển thiết lập của Kaspersky Endpoint Agent sang Kaspersky Endpoint Security cho Windows. Để thực hiện, hãy sử dụng trình hướng dẫn để chuyển từ Kaspersky Endpoint Agent trong Bảng điều khiển web.

   Cách chuyển thiết lập chính sách và tác vụ từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security trong Bảng điều khiển web

   Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Operations → Migration from 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 chính sách Kaspersky Endpoint Agent để chọn chính sách Kaspersky Endpoint Security mà bạn muốn gộp thiết lập. 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. Chuyển sang bước tiếp theo.

Bước 3. Hoàn tất Trình hướng dẫn

Hoàn tất trình hướng dẫn. Kết quả là trình hướng dẫn thực hiện như sau:

- 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 *Inactive*. Để tiếp tục, hãy thay đổi trạng thái của chính sách Kaspersky Endpoint Agent và Kaspersky Endpoint Security thành *Inactive* 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 mối 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 bản sao của các tác vụ Kaspersky Endpoint Agent. Đồng thời, Trình hướng dẫn sẽ giữ nguyên các tác vụ của Kaspersky Endpoint Agent.

3 Cấp phép cho chức năng EDR Optimum

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 trở lên. 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 trở lên 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 *Add key*.

4 Cài đặt / nâng cấp ứng dụng Kaspersky Endpoint Security

Để chuyển chức năng EDR Optimum trong quá trình cài đặt hoặc nâng cấp ứng dụng, bạn nên sử dụng tác vụ cài đặt từ xa. Khi tạo tác vụ cài đặt từ xa, bạn cần chọn thành phần EDR Optimum 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.
- Cục bộ bằng cách sử dụng Trình hướng dẫn cài đặt.

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 hiện tại 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 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 hiện tại của các giải pháp Kaspersky. Trong trường hợp này, Kaspersky Endpoint Security sẽ tự động chọn các thành phần dựa trên cấu hình của Kaspersky Endpoint Agent. Sau đó khiến Kaspersky Endpoint Security sẽ chuyển sang sử dụng tác nhân tích hợp và gỡ bỏ Kaspersky Endpoint Agent.

Kaspersky Endpoint Security hỗ trợ nâng cấp mà không cần khởi động lại máy tính. Bạn có thể chọn chế độ nâng cấp ứng dụng trong thuộc tính chính sách.

5 Kiểm tra hoạt động của ứng dụng

Nếu sau khi cài đặt hoặc nâng cấp ứng dụng, máy tính có trạng thái *Critical* trong bảng điều khiển Kaspersky Security Center:

- Đảm bảo rằng máy tính được cài đặt Network Agent phiên bản 13.2 trở lên.
- Kiểm tra trạng thái hoạt động của tác nhân tích hợp bằng cách xem *Report on status of application components*. Nếu một thành phần có trạng thái *Not installed* thì hãy cài đặt thành phần này bằng cách sử dụng tác vụ *Change application components*. Nếu một thành phần có trạng thái *Không được giấy phép hỗ trợ* thì hãy đảm bảo rằng bạn đã kích hoạt chức năng tác nhân tích hợp.
- Đảm bảo rằng bạn chấp nhận Tuyên bố Kaspersky Security Network trong chính sách mới của Kaspersky Endpoint Security cho Windows.

Kaspersky Sandbox

Kaspersky Endpoint Security for Windows bao gồm một tác nhân tích hợp sẵn để tích hợp với giải pháp Kaspersky Sandbox. Thành phần *Sandbox* phát hiện và tự động chặn các mối đe dọa nâng cao trên máy tính. 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. 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 (các máy chủ Sandbox). Để biết chi tiết về giải pháp này, vui lòng tham khảo Trợ giúp của Kaspersky Sandbox và Trợ giúp của Kaspersky Anti Targeted Attack Platform.

Tích hợp tác nhân tích hợp với Kaspersky Sandbox

Phải thêm thành phần Sandbox để tích hợp với Kaspersky Sandbox. Bạn có thể chọn thành phần 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 **Asset management** → **Policies**.
  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** → **KSC Integration**.
  5. Trong mục **Data transfer to Administration Server**, hãy chọn hộp kiểm **About Quarantine files**.
  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 **Settings** → **Integration**.
2. Vào mục **Integration**.
3. Bật nút bật/tắt **Background connection for integration Enabled**.
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.

- Để cấu hình kết nối được tin tưởng với máy chủ Sandbox, bạn phải chuẩn bị chứng chỉ TLS. Sau đó, bạn phải thêm chứng chỉ vào máy tính bằng chính sách. Bạn cũng cần thêm chứng chỉ vào máy chủ Sandbox.

  > Xác thực hai chiều sử dụng bộ chứa mã hóa không khả dụng với Kaspersky Sandbox.

  Bạn có thể thêm chứng chỉ TLS vào Bảng điều khiển web bằng cách sử dụng dòng lệnh.

- Thành phần Kaspersky Sandbox được bật.
- Các thành phần ứng dụng đảm bảo hoạt động của Sandbox được bật và hoạt động. Các thành phần sau đảm bảo hoạt động của Sandbox:
  - Bảo vệ mối đe dọa tập tin.
  - Phòng chống xâm nhập máy chủ.
  - Tường lửa.
  - Bảo vệ AMSI.
  - Quét trong nền.

Để bật hoặc tắt tích hợp với Kaspersky Sandbox:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Sandbox**.
5. Sử dụng nút bật/tắt **Integration with Sandbox ENABLED** để bật hoặc tắt thành phần này.

6. Trong mục **Integration mode**, hãy chọn chế độ hoạt động của thành phần: **Kaspersky Sandbox**.

7. Nhấn vào liên kết **Connection settings**.

   Thao tác này sẽ mở ra cửa sổ thiết lập kết nối máy chủ Sandbox.

8. Trong mục **Server TLS certificate**, hãy nhấn vào **Upload** và chọn tập tin chứng chỉ TLS.

   Kaspersky Endpoint Security chỉ có thể có một chứng chỉ TLS cho máy chủ 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.

9. Cấu hình thiết lập kết nối nâng cao cho máy chủ Sandbox:

   - **Timeout (msec)**. Thời gian chờ kết nối cho máy chủ 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 máy chủ 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.

   - **Request queue**. Kích thước của thư mục hàng chờ yêu cầu. Khi gửi nhiều đối tượng để quét trong Sandbox, 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, 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.

10. Trong mục **Connection to Sandbox servers**, hãy nhấn nút **Add**.

11. 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.

    Để biết chi tiết về việc triển khai ảnh máy ảo và cấu hình máy chủ Sandbox, hãy tham khảo Trợ giúp của Kaspersky Sandbox.

12. 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. Kiểm tra trạng thái hoạt động của thành phần bằng cách xem *Report on status of application components*. 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 **Sandbox** sẽ được thêm vào danh sách các thành phần của Kaspersky Endpoint Security.

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.

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.

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 *IOC Scan* cho phép tìm các Dấu hiệu về sự xâm nhập trên máy tính và thực hiện các biện pháp ứng phó với mối 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. Kaspersky Endpoint Security sẽ tự động tạo các tập tin IOC cho Kaspersky Sandbox.

Chế độ chạy tác vụ IOC Scan

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 IOC Scan

Kaspersky Sandbox có thể tự động tạo và chạy tác vụ *IOC Scan* 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 IOC Scan:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **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.
3. Chọn thẻ **Application settings**.
4. Vào mục **IOC Scan settings**.

5. Cấu hình các hành động khi phát hiện IOC:

   - **Move copy to Quarantine, delete object**. 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.

   - **Run Critical Areas Scan**. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ chạy tác vụ *Critical Areas Scan*. Theo mặc định, Kaspersky Endpoint Security sẽ quét nhân kernel, các tiến trình đang chạy, và phân vùng khởi động ổ đĩa.

   - **Run only when the computer is idle**. Hoãn bắt đầu tác vụ 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. Tùy chọn lịch này cho phép bạn bảo tiết kiệm nguyên máy tính khi máy tính đang được sử dụng.

6. Lưu các thay đổi của bạn.

   Bạn có thể xem kết quả tác vụ trong các thuộc tính tác vụ trong mục **Results**. 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.

Hướng dẫn chuyển KEA sang KES cho Kaspersky Sandbox

Kaspersky Endpoint Security for Windows bao gồm một tác nhân tích hợp sẵn cho giải pháp Kaspersky Sandbox. Bạn không còn cần một ứng dụng Kaspersky Endpoint Agent riêng để fhoạt động với Kaspersky Sandbox. Tất cả các chức năng của Kaspersky Endpoint Agent sẽ được thực hiện bởi Kaspersky Endpoint Security.

Khi bạn triển khai Kaspersky Endpoint Security trên các máy tính đã cài đặt Kaspersky Endpoint Agent thì giải pháp Kaspersky Sandbox sẽ tiếp tục hoạt động với Kaspersky Endpoint Security. Ngoài ra, Kaspersky Endpoint Agent sẽ bị gỡ bỏ khỏi máy tính. Hành vi tương tự trong hệ thống sẽ xảy ra khi bạn cập nhật Kaspersky Endpoint Security lên phiên bản 11.7.0 trở lên.

Kaspersky Endpoint Security không tương thích với Kaspersky Endpoint Agent. Bạn không thể cài đặt cả hai ứng dụng này trên cùng một máy tính.

Các điều kiện sau phải được đáp ứng để Kaspersky Endpoint Security hoạt động như một phần của Kaspersky Sandbox:

- Kaspersky Sandbox phiên bản 2.0 trở lên.
- Kaspersky Security Center phiên bản 13.2 trở lên (bao gồm Network Agent). Không thể kích hoạt tính năng Kaspersky Sandbox trong các phiên bản trước của Kaspersky Security Center.
- Chỉ có thể quản lý Kaspersky Sandbox bằng Bảng điều khiển web Kaspersky Security Center.

- Truyền dữ liệu đến Máy chủ quản trị 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.
- 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*.

Các bước để chuyển cấu hình [KES KEA] sang [KES+Tác nhân tích hợp] cho Kaspersky Sandbox

1. **Nâng cấp tiện ích web Kaspersky Endpoint Security**

   Có thể quản lý thành phần Kaspersky Sandbox bằng Tiện ích quản lý Kaspersky Endpoint Security phiên bản 11.7.0 trở lên.

2. **Chuyển chính sách và tác vụ**

   Chuyển thiết lập của Kaspersky Endpoint Agent sang Kaspersky Endpoint Security cho Windows. Để thực hiện, hãy sử dụng trình hướng dẫn để chuyển từ Kaspersky Endpoint Agent trong Bảng điều khiển web.

   Cách chuyển thiết lập chính sách và tác vụ từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security trong Bảng điều khiển web

   Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Operations → Migration from 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 chính sách Kaspersky Endpoint Agent để chọn chính sách Kaspersky Endpoint Security mà bạn muốn gộp thiết lập. 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. Chuyển sang bước tiếp theo.

Bước 3. Hoàn tất Trình hướng dẫn

Hoàn tất trình hướng dẫn. Kết quả là trình hướng dẫn thực hiện như sau:

- 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 *Inactive*. Để tiếp tục, hãy thay đổi trạng thái của chính sách Kaspersky Endpoint Agent và Kaspersky Endpoint Security thành *Inactive* 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 mối 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 bản sao của các tác vụ Kaspersky Endpoint Agent. Đồng thời, Trình hướng dẫn sẽ giữ nguyên các tác vụ của Kaspersky Endpoint Agent.

3 Cấp phép cho chức năng Kaspersky Sandbox

Để kích hoạt Kaspersky Endpoint Security thành một phần của giải pháp Kaspersky Sandbox, bạn cần có giấy phép riêng cho Phần bổ trợ Kaspersky Sandbox. Bạn có thể thêm khóa bằng tác vụ *Add key*. Kết quả là hai khóa sẽ được thêm vào ứng dụng: *Kaspersky Endpoint Security* và *Kaspersky Sandbox*.

4 Cài đặt / nâng cấp ứng dụng Kaspersky Endpoint Security

Để chuyển chức năng Kaspersky Sandbox trong quá trình cài đặt hoặc nâng cấp ứng dụng, bạn nên sử dụng tác vụ cài đặt từ xa. Khi tạo tác vụ cài đặt từ xa, bạn cần chọn thành phần Kaspersky Sandbox 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.
- Cục bộ bằng cách sử dụng Trình hướng dẫn cài đặt.

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 hiện tại của các giải pháp Kaspersky. Do đó, giả sử nếu máy tính được cài đặt Kaspersky Endpoint Agent và giải pháp Kaspersky Sandbox được kích hoạt thì bộ cài đặt Kaspersky Endpoint Security sẽ tự động cấu hình bộ thành phần và chọn thành phần Kaspersky Sandbox. 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 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 hiện tại của các giải pháp Kaspersky. Trong trường hợp này, Kaspersky Endpoint Security sẽ tự động chọn các thành phần dựa trên cấu hình của Kaspersky Endpoint Agent. Sau đó khiến Kaspersky Endpoint Security sẽ chuyển sang sử dụng tác nhân tích hợp và gỡ bỏ Kaspersky Endpoint Agent.

Kaspersky Endpoint Security hỗ trợ nâng cấp mà không cần khởi động lại máy tính. Bạn có thể chọn chế độ nâng cấp ứng dụng trong thuộc tính chính sách.

5. **Kiểm tra hoạt động của ứng dụng**

   Nếu sau khi cài đặt hoặc nâng cấp ứng dụng, máy tính có trạng thái *Critical* trong bảng điều khiển Kaspersky Security Center:

   - Đảm bảo rằng máy tính được cài đặt Network Agent phiên bản 13.2 trở lên.
   - Kiểm tra trạng thái hoạt động của tác nhân tích hợp bằng cách xem *Report on status of application components*. Nếu một thành phần có trạng thái *Not installed* thì hãy cài đặt thành phần này bằng cách sử dụng tác vụ *Change application components*. Nếu một thành phần có trạng thái *Không được giấy phép hỗ trợ* thì hãy đảm bảo rằng bạn đã kích hoạt chức năng tác nhân tích hợp.
   - Đảm bảo rằng bạn chấp nhận Tuyên bố Kaspersky Security Network trong chính sách mới của Kaspersky Endpoint Security cho Windows.

Kaspersky Anti Targeted Attack Platform



Kaspersky Endpoint Security cho Windows hỗ trợ làm việc với 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 ba đơn vị chức năng:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Bạn có thể mua tất cả các đơn vị chức năng hoặc mua riêng từng đơn vị chức năng. Để biết chi tiết về giải pháp này, vui lòng tham khảo Trợ giúp của Kaspersky Anti Targeted Attack Platform. Ứng dụng này bao gồm các tác nhân tích hợp cho các thành phần EDR, NDR. Ứng dụng này cũng hỗ trợ làm việc với thành phần Sandbox, là một phần của KATA.

Các công cụ Threat Intelligence

Kaspersky Endpoint Detection and Response sử dụng các công cụ Threat Intelligence sau:

- Tích hợp với 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.
- 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.

Nguyên lý hoạt động của giải pháp

Kaspersky Endpoint Security 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 (dữ liệu đo từ xa) được gửi đến máy chủ của Kaspersky Anti Targeted Attack Platform. Trong trường hợp này, Kaspersky Endpoint Security cũng gửi thông tin đến máy chủ của Kaspersky Anti Targeted Attack Platform về các mối đe dọa được phát hiện bởi ứng dụng, bao gồm cả thông tin về kết quả xử lý các mối đe dọa này.

Việc tích hợp EDR (KATA) và NDR (KATA) được cấu hình trong bảng điều khiển Kaspersky Security Center. Tác nhân tích hợp sau đó được quản lý bằng bảng điều khiển Kaspersky Anti Targeted Attack Platform, bao gồm hoạt động chạy các tác vụ, quản lý các đối tượng được cách ly, xem báo cáo và các hành động khác.

Các cấu hình Kaspersky Endpoint Security để làm việc với EDR / NDR (KATA)

Các cấu hình sau có thể được sử dụng để làm việc với EDR / NDR (KATA):

- **[KES+tác nhân tích hợp]**. Trong cấu hình này, Kaspersky Endpoint Security đóng vai trò vừa là ứng dụng đảm bảo khả năng bảo mật của máy tính vừa là ứng dụng để làm việc với EDR / NDR (KATA). Tác nhân tích hợp cho EDR (KATA) có trong Kaspersky Endpoint Security cho Windows phiên bản 12.1 trở lên. Tác nhân tích hợp cho NDR (KATA) có trong Kaspersky Endpoint Security cho Windows phiên bản 12.7 trở lên.
- **[EPP bên thứ ba+EDR Agent]**. Trong cấu hình này, tính bảo mật của cơ sở hạ tầng CNTT được cung cấp bởi Endpoint Protection Platform (EPP) của bên thứ ba. Khả năng tương tác với EDR / NDR (KATA) được cung cấp bởi Kaspersky Endpoint Security trong cấu hình Endpoint Detection and Response Agent (EDR Agent). Trong cấu hình này, EDR Agent tương thích với các ứng dụng EPP của bên thứ ba. EDR Agent EDR (KATA) có sẵn trong Kaspersky Endpoint Security cho Windows phiên bản 12.3 trở lên. EDR Agent cho NDR (KATA) có sẵn trong Kaspersky Endpoint Security cho Windows phiên bản 12.7 trở lên.

Hỗ trợ cho các phiên bản trước của Kaspersky Endpoint Security

Nếu bạn đang sử dụng Kaspersky Endpoint Security 11.2.0 – 11.8.0, để có khả năng tương tác với Kaspersky Anti Targeted Attack Platform (EDR), ứng dụng này sẽ bao gồm cả Kaspersky Endpoint Agent. Bạn có thể cài đặt Kaspersky Endpoint Agent để chạy cùng Kaspersky Endpoint Security.

Nếu bạn đang sử dụng Kaspersky Endpoint Security 11.9.0 – 12.0, bạn cần cài đặt riêng Kaspersky Endpoint Agent vì kể từ Kaspersky Endpoint Security 11.9.0, gói phân phối Kaspersky Endpoint Agent không còn là một phần của gói phân phối Kaspersky Endpoint Security.

Tích hợp tác nhân tích hợp với EDR / NDR (KATA)

Để tích hợp với EDR / NDR (KATA), bạn phải thêm thành phần liên quan: Endpoint Detection and Response (KATA) hoặc Network Detection and Response (KATA). Bạn có thể chọn các thành phần tích hợp với EDR / NDR (KATA) khi cài đặt hoặc nâng cấp ứng dụng, cũng như sử dụng tác vụ *Thay đổi thành phần ứng dụng*.

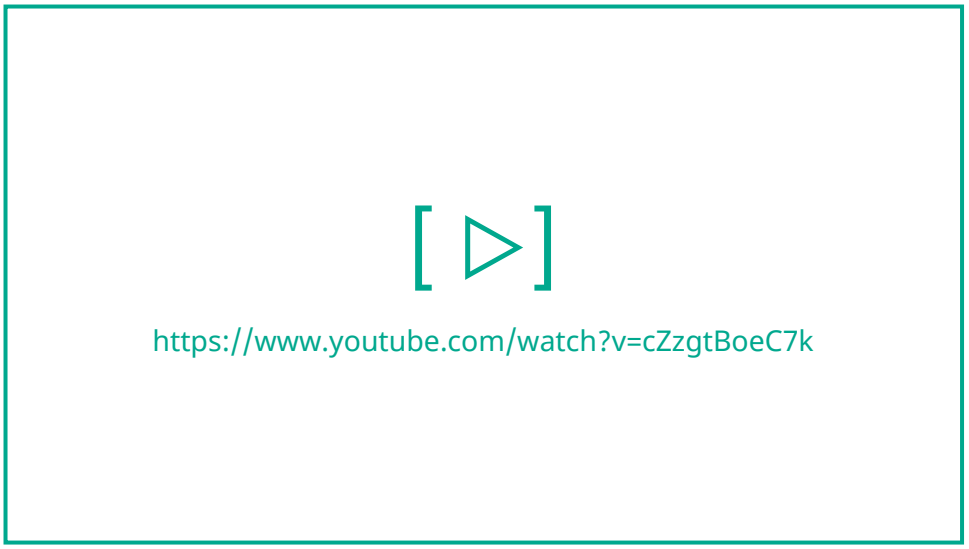
Kể đầu từ phiên bản 12.11 của Kaspersky Endpoint Security cho Windows, thành phần EDR (KATA) đã được đổi tên thành **Endpoint Detection and Response Expert (version 8.0 or later)**. Trong phiên bản ứng dụng này, thành phần tương thích với Kaspersky Anti Targeted Attack Platform 7.1 và các phiên bản trước đó và cả Kaspersky Endpoint Detection and Response Expert (on-premises).

Các thành phần Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud), và Endpoint Detection and Response Expert (on-premises) không tương thích với nhau.

Để sử dụng EDR / NDR (KATA), cần đáp ứng các điều kiện sau:

- EDR (KATA): Kaspersky Anti Targeted Attack Platform phiên bản 5.0–7.1.
- NDR (KATA): Kaspersky Anti Targeted Attack Platform phiên bản 7.0 trở lên.
- EDR (KATA): Kaspersky Endpoint Security cho Windows 12.1 trở lên. Để biết thêm chi tiết về khả năng tương thích của KATA với các phiên bản khác nhau của Kaspersky Endpoint Security, hãy tham khảo Trợ giúp của Kaspersky Anti Targeted Attack Platform.
- NDR (KATA): Kaspersky Endpoint Security cho Windows 12.7 trở lên.
- Kaspersky Security Center phiên bản 14.2 trở lên. Không thể kích hoạt chức năng tích hợp EDR / NDR (KATA) trong các phiên bản trước của Kaspersky Security Center.
- Ứng dụng được kích hoạt và chức năng được giấy phép hỗ trợ.
- Các thành phần Endpoint Detection and Response (KATA) và Network Detection and Response (KATA) được bật.

- Các thành phần ứng dụng đảm bảo hoạt động của EDR / NDR (KATA) được bật và hoạt động. Các thành phần sau đảm bảo hoạt động của EDR / NDR (KATA):
  - 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.
  - Bảo vệ AMSI.
  - Quét trong nền.
  - Kaspersky Security Network.



https://www.youtube.com/watch?v=cZzgtBoeC7k



https://www.youtube.com/watch?v=gd-rySv0ThQ

Tích hợp với thành phần Endpoint Detection and Response (KATA) liên quan tới các bước sau:

1. **Cài đặt các thành phần Endpoint Detection and Response (KATA) và Network Detection and Response (KATA)**

   Bạn có thể chọn các thành phần EDR (KATA) và NDR (KATA) 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 Endpoint Detection and Response (KATA) và Network Detection and Response (KATA)**

   Bạn cần mua một giấy phép riêng cho EDR (KATA) và NDR (KATA) (ví dụ: Phần bổ trợ Kaspersky Endpoint Detection and Response (KATA)).

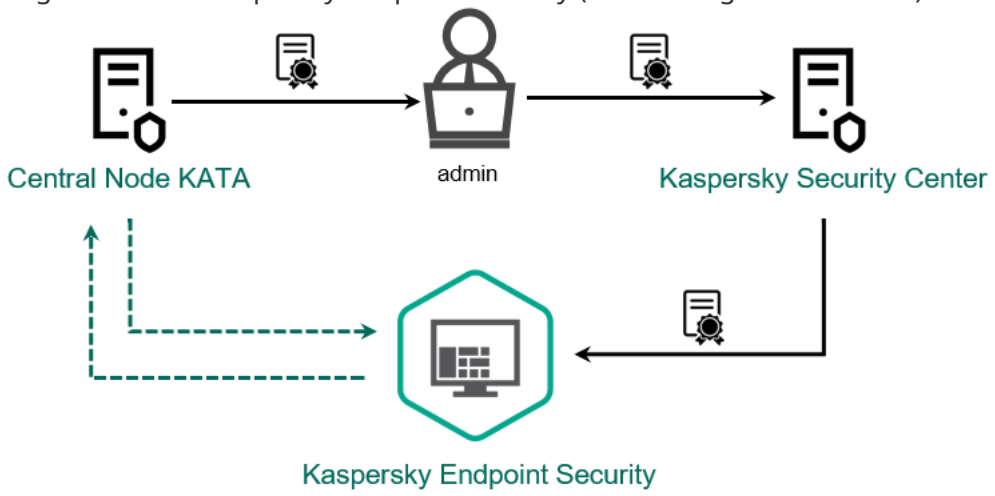
   Chức năng này sẽ khả dụng sau khi thêm khóa riêng hỗ trợ chức năng EDR (KATA) và NDR (KATA). Kết quả là nhiều khóa được thêm trên máy tính: một khóa dành cho Kaspersky Endpoint Security và một khóa dành cho Kaspersky Endpoint Detection and Response (KATA) và Network Detection and Response (KATA).

   Cấp giấy phép cho chức năng EDR (KATA) và NDR (KATA) độc lập cũng giống như cấp giấy phép cho Kaspersky Endpoint Security.

   Đảm bảo rằng cả chức năng EDR (KATA) và NDR (KATA) được gộp trong giấy phép và đang chạy trong giao diện cục bộ của ứng dụng.

3. **Kết nối với Central Node**

   Kaspersky Anti Targeted Attack Platform yêu cầu thiết lập kết nối được tin tưởng giữa Kaspersky Endpoint Security và thành phần Central Node. Để cấu hình kết nối được tin tưởng, bạn phải sử dụng chứng chỉ TLS. Bạn có thể lấy chứng chỉ TLS trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform). Sau đó, bạn phải thêm chứng chỉ TLS vào Kaspersky Endpoint Security (xem hướng dẫn bên dưới).



Thêm chứng chỉ TLS vào Kaspersky Endpoint Security

Theo mặc định, Kaspersky Endpoint Security chỉ kiểm tra chứng chỉ TLS của Central Node. Để cho kết nối bảo mật hơn, bạn có thể kích hoạt thêm xác minh máy tính trên Central Node (xác thực hai chiều). Để bật cơ chế xác minh này, bạn phải bật xác thực hai chiều trong thiết lập của Central Node và Kaspersky Endpoint Security. Để sử dụng xác thực hai chiều, bạn cũng sẽ cần một bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể nhận một bộ chứa mã hóa trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform).

Cách kết nối máy tính Kaspersky Endpoint Security với Central Node bằng Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Detection and Response** và chọn thành phần mà bạn muốn cấu hình: **Endpoint Detection and Response Expert (on-premises)** hoặc **Network Detection and Response (KATA)**.
5. Chọn hộp kiểm tương ứng: **Endpoint Detection and Response Expert (phiên bản 7.1 trở xuống)** hoặc **Network Detection and Response (KATA)**.
6. Nhấn vào **Thiết lập kết nối máy chủ**.
7. Cấu hình kết nối máy chủ:
   - **Thời gian chờ (giây)**. Thời gian chờ phản hồi tối đa của máy chủ Central Node. Khi hết thời gian chờ, Kaspersky Endpoint Security sẽ cố gắng kết nối với một máy chủ Central Node khác.
   - **Chứng chỉ TLS máy chủ**. Chứng chỉ TLS để thiết lập kết nối được tin tưởng với máy chủ Central Node. Bạn có thể lấy chứng chỉ TLS trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform).
   - **Sử dụng xác thực hai chiều**. Xác thực hai chiều khi thiết lập kết nối bảo mật giữa Kaspersky Endpoint Security và máy chủ Central Node. Để sử dụng xác thực hai chiều, bạn cần bật xác thực hai chiều trong cài đặt máy chủ Central Node, sau đó lấy bộ chứa mã hóa và đặt mật khẩu để bảo vệ bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể nhận một bộ chứa mã hóa trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform). Sau khi cấu hình thiết lập Central Node, bạn cũng cần bật xác thực hai chiều trong thiết lập của Kaspersky Endpoint Security và tải bộ chứa mã hóa được bảo vệ bằng mật khẩu.

     Bộ chứa mã hóa phải được bảo vệ bằng mật khẩu. Không thể thêm bộ chứa mã hóa có mật khẩu trống.
8. Nhấn vào **OK**.
9. Thêm máy chủ Central Node. Để thực hiện, hãy chỉ định địa chỉ máy chủ (IPv4, IPv6) và cổng để kết nối với máy chủ.

   Bạn có thể thêm nhiều địa chỉ máy chủ Central Node. Kaspersky Endpoint Security sẽ cố gắng kết nối với máy chủ bằng địa chỉ IP đầu tiên. Nếu không thể thiết lập kết nối, Kaspersky Endpoint Security sẽ cố gắng kết nối bằng địa chỉ IP thứ hai trong danh sách, v.v.
10. Nếu cần, hãy cấu hình đo từ xa.
11. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách kết nối máy tính Kaspersky Endpoint Security với Central Node bằng Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.
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 phần **Built-in Agents Configuration** và chọn thành phần mà bạn muốn cấu hình: **Endpoint Detection and Response Expert (on-premises)** hoặc **Network Detection and Response (KATA)**.
5. Bật nút bật/tắt tương ứng: **Endpoint Detection and Response Expert (on-premises) ENABLED** hoặc **Network Detection and Response (KATA) ENABLED**.
6. Để cấu hình EDR (KATA), hãy chọn **Endpoint Detection and Response Expert (version 7.1 or earlier)** trong danh sách các giải pháp.
7. Nhấn vào **Connection settings**.
8. Cấu hình kết nối máy chủ:

   - **Timeout (sec)**. Thời gian chờ phản hồi tối đa của máy chủ Central Node. Khi hết thời gian chờ, Kaspersky Endpoint Security sẽ cố gắng kết nối với một máy chủ Central Node khác.
   - **Server certificate**. Chứng chỉ TLS để thiết lập kết nối được tin tưởng với máy chủ Central Node. Bạn có thể lấy chứng chỉ TLS trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform).
   - **Use two-way authentication**. Xác thực hai chiều khi thiết lập kết nối bảo mật giữa Kaspersky Endpoint Security và máy chủ Central Node. Để sử dụng xác thực hai chiều, bạn cần bật xác thực hai chiều trong cài đặt máy chủ Central Node, sau đó lấy bộ chứa mã hóa và đặt mật khẩu để bảo vệ bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể nhận một bộ chứa mã hóa trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform). Sau khi cấu hình thiết lập Central Node, bạn cũng cần bật xác thực hai chiều trong thiết lập của Kaspersky Endpoint Security và tải bộ chứa mã hóa được bảo vệ bằng mật khẩu.

     Bộ chứa mã hóa phải được bảo vệ bằng mật khẩu. Không thể thêm bộ chứa mã hóa có mật khẩu trống.
9. Nhấn vào **OK**.
10. Thêm máy chủ Central Node. Để thực hiện, hãy chỉ định địa chỉ máy chủ (IPv4, IPv6) và cổng để kết nối với máy chủ.

    Bạn có thể thêm nhiều địa chỉ máy chủ Central Node. Kaspersky Endpoint Security sẽ cố gắng kết nối với máy chủ bằng địa chỉ IP đầu tiên. Nếu không thể thiết lập kết nối, Kaspersky Endpoint Security sẽ cố gắng kết nối bằng địa chỉ IP thứ hai trong danh sách, v.v.

11. Nếu cần, hãy cấu hình đo từ xa.

12. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Bạn cũng có thể thêm chứng chỉ TLS theo cách cục bộ bằng cách sử dụng dòng lệnh.

Kết quả là máy tính được thêm vào bảng điều khiển Kaspersky Anti Targeted Attack Platform. Kiểm tra trạng thái hoạt động của các thành phần bằng cách xem *Report on status of application components*. Bạn cũng có thể xem trạng thái hoạt động của các thành phần trong mục báo cáo trong giao diện cục bộ của Kaspersky Endpoint Security. Thành phần **Endpoint Detection and Response Expert (version 8.0 or later)** và **Network Detection and Response (KATA)** sẽ được thêm vào danh sách các thành phần của Kaspersky Endpoint Security.

Bạn có thể kiểm tra trạng thái của các thành phần trong bảng điều khiển Kaspersky Security Center trong thuộc tính máy tính trong phần **Components**. Hãy cân nhắc những điều sau khi kiểm tra trạng thái của thành phần trong bảng điều khiển. Nếu thành phần không được cài đặt và chức năng không được hỗ trợ theo giấy phép của bạn, bảng điều khiển sẽ hiển thị trạng thái **Not supported by license** thay vì **Not installed**.

Kể từ Kaspersky Endpoint Security 12.6 cho Windows, bạn có thể giám sát trạng thái của thành phần EDR (KATA) trong Bảng điều khiển quản trị Kaspersky Security Center (MMC). Trạng thái hiện tại của thành phần được hiển thị trong thuộc tính máy tính trong cột **Endpoint Sensor status** (*Running*, *Starting*, *Stopped*, *Paused*, *Failed*, *Unknown*). Bảng điều khiển web không hiển thị trạng thái của Cảm biến điểm cuối.

Cấu hình đo từ xa EDR (KATA)

Dữ liệu *đo từ xa* là danh sách các sự kiện đã xảy ra trên máy tính được bảo vệ. Kaspersky Endpoint Security sẽ phân tích dữ liệu đo lường từ xa và gửi nó tới Kaspersky Anti Targeted Attack Platform trong quá trình đồng bộ. Các sự kiện đo từ xa sẽ đến máy chủ gần như liên tục. Kaspersky Endpoint Security khởi tạo đồng bộ với máy chủ khi bất kỳ điều kiện nào sau đây được thỏa mãn:

- Khoảng thời gian đồng bộ đã hết.
- Số sự kiện trong bộ đệm vượt quá giới hạn trên.

Do đó, theo mặc định, ứng dụng sẽ đồng bộ sau mỗi 30 giây hoặc bất cứ khi nào bộ đệm chứa 1024 sự kiện. Bạn có thể cấu hình hành vi đồng bộ trong chính sách Kaspersky Endpoint Security và chọn các giá trị tối ưu để phù hợp với lượng tải mạng của bạn (xem hướng dẫn bên dưới).

Nếu không có kết nối giữa Kaspersky Endpoint Security và máy chủ, ứng dụng sẽ đặt các sự kiện mới vào hàng chờ. Khi kết nối được khôi phục, Kaspersky Endpoint Security sẽ gửi các sự kiện trong hàng chờ tới máy chủ theo đúng thứ tự. Để máy chủ không bị quá tải, Kaspersky Endpoint Security có thể bỏ qua một số sự kiện. Để bật tính năng này, bạn có thể tối ưu hóa thiết lập truyền sự kiện, chẳng hạn như đặt giá trị số sự kiện mỗi giờ tối đa (xem hướng dẫn bên dưới).

Nếu bạn đang sử dụng Kaspersky Anti Targeted Attack Platform cùng với một giải pháp khác cũng sử dụng phép đo lường từ xa, bạn có thể tắt đo lường từ xa cho KATA (EDR) (xem hướng dẫn bên dưới). Điều này cho phép bạn tối ưu hóa mức tải máy chủ cho các giải pháp này. Ví dụ: nếu bạn đã triển khai giải pháp Managed Detection and Response và KATA (EDR) thì bạn có thể sử dụng đo lường từ xa MDR và tạo các tác vụ Phản hồi về mối đe dọa trong KATA (EDR).

Cách cấu hình đo từ xa trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.

2. Trong cây bảng điều khiển, hãy chọn **Policies**.

3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

4. Trong cửa sổ chính sách, hãy chọn **Detection and Response** và chọn thành phần mà bạn muốn cấu hình: **Endpoint Detection and Response Expert (on-premises)** hoặc **Network Detection and Response (KATA)**.

5. Cấu hình thiết lập **Gửi yêu cầu đồng bộ đến máy chủ KATA sau mỗi (phút)**. Tần suất yêu cầu đồng bộ được gửi đến máy chủ. Trong quá trình đồng bộ, Kaspersky Endpoint Security sẽ gửi thông tin về các thiết lập và tác vụ ứng dụng được sửa đổi.

6. Đảm bảo rằng hộp kiểm **Gửi phép đo từ xa đến KATA** được chọn.

7. Nếu cần, hãy cấu hình đồng bộ hóa với thiết lập máy chủ trong mục **Thiết lập truyền dữ liệu**:

   - **Độ trễ truyền gửi sự kiện tối đa (giây)**. Ứng dụng sẽ đồng bộ với máy chủ để gửi các sự kiện sau khi hết khoảng thời gian đồng bộ. Thiết lập mặc định là 30 giây.

   - **Số lượng gói sự kiện tối đa**. Ứng dụng sẽ đồng bộ với máy chủ khi bộ đệm được lấp đầy bằng các sự kiện. Thiết lập mặc định là 1024 sự kiện.

8. Nếu cần, hãy chọn hộp kiểm **Cho phép làm nghẽn yêu cầu** trong mục **Làm nghẽn yêu cầu**.

   Tính năng này giúp tối ưu hóa mức tải trên máy chủ. Nếu chức năng này được kích hoạt, ứng dụng sẽ hạn chế việc truyền sự kiện. Nếu số lượng sự kiện vượt quá giới hạn được cấu hình thì Kaspersky Endpoint Security sẽ ngừng gửi sự kiện.

9. Cấu hình thiết lập tối ưu hóa để gửi sự kiện đến máy chủ:

   - **Số lượng sự kiện tối đa mỗi giờ**. Ứng dụng sẽ phân tích luồng dữ liệu đo từ xa và hạn chế gửi sự kiện nếu luồng sự kiện vượt quá giới hạn số sự kiện mỗi giờ đã được cấu hình. Kaspersky Endpoint Security sẽ tiếp tục gửi sự kiện sau một giờ. Thiết lập mặc định là 3000 sự kiện mỗi giờ. Nếu ứng dụng được cài đặt trên máy chủ, luồng dữ liệu đo từ xa sẽ cao hơn. Đối với máy chủ, bạn nên tăng giá trị lên 60.000 sự kiện mỗi giờ.

   - **Tỷ lệ vượt quá hạn mức sự kiện**. Ứng dụng sẽ sắp xếp sự kiện theo loại (ví dụ: sự kiện "thay đổi trong registry") và hạn chế truyền gửi sự kiện nếu tỷ lệ sự kiện cùng loại trên tổng số sự kiện vượt quá hạn mức được cấu hình theo tỷ lệ. Kaspersky Endpoint Security sẽ tiếp tục gửi sự kiện khi tỷ lệ của các sự kiện khác trên tổng số sự kiện trở lại đủ lớn. Thiết lập mặc định là 15%.

10. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách cấu hình đo từ xa trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management → Policies**.

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 **Built-in Agents Configuration → Endpoint Detection and Response Expert (on-premises)**.

5. Để cấu hình EDR (KATA), hãy chọn **Endpoint Detection and Response Expert (version 7.1 or earlier)** trong danh sách các giải pháp.

6. Đảm bảo rằng hộp kiểm **Send telemetry to KATA servers** được chọn trong mục **Data transmission settings**.

7. Cấu hình thiết lập **Send sync request to server every (min)**. Tần suất yêu cầu đồng bộ được gửi đến máy chủ. Trong quá trình đồng bộ, Kaspersky Endpoint Security sẽ gửi thông tin về các thiết lập và tác vụ ứng dụng được sửa đổi.

8. Đảm bảo rằng hộp kiểm **Send telemetry to KATA servers** được chọn.

9. Nếu cần, hãy cấu hình đồng bộ hóa với thiết lập máy chủ trong mục **Data transmission settings**:

   - **Maximum event transmission delay (sec)**. Ứng dụng sẽ đồng bộ với máy chủ để gửi các sự kiện sau khi hết khoảng thời gian đồng bộ. Thiết lập mặc định là 30 giây.

   - **Maximum number of event packages**. Ứng dụng sẽ đồng bộ với máy chủ khi bộ đệm được lấp đầy bằng các sự kiện. Thiết lập mặc định là 1024 sự kiện.

10. Nếu cần, hãy chọn hộp kiểm **Enable request throttling** trong mục **Request throttling**.

    Tính năng này giúp tối ưu hóa mức tải trên máy chủ. Nếu chức năng này được kích hoạt, ứng dụng sẽ hạn chế việc truyền sự kiện. Nếu số lượng sự kiện vượt quá giới hạn được cấu hình thì Kaspersky Endpoint Security sẽ ngừng gửi sự kiện.

11. Cấu hình thiết lập tối ưu hóa để gửi sự kiện đến máy chủ:

    - **Maximum number of events per hour**. Ứng dụng sẽ phân tích luồng dữ liệu đo từ xa và hạn chế gửi sự kiện nếu luồng sự kiện vượt quá giới hạn số sự kiện mỗi giờ đã được cấu hình. Kaspersky Endpoint Security sẽ tiếp tục gửi sự kiện sau một giờ. Thiết lập mặc định là 3000 sự kiện mỗi giờ. Nếu ứng dụng được cài đặt trên máy chủ, luồng dữ liệu đo từ xa sẽ cao hơn. Đối với máy chủ, bạn nên tăng giá trị lên 60.000 sự kiện mỗi giờ.

    - **Percentage of event limit excess**. Ứng dụng sẽ sắp xếp sự kiện theo loại (ví dụ: sự kiện "thay đổi trong registry") và hạn chế truyền gửi sự kiện nếu tỷ lệ sự kiện cùng loại trên tổng số sự kiện vượt quá hạn mức được cấu hình theo tỷ lệ. Kaspersky Endpoint Security sẽ tiếp tục gửi sự kiện khi tỷ lệ của các sự kiện khác trên tổng số sự kiện trở lại đủ lớn. Thiết lập mặc định là 15%.

12. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Policies**.

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 **Tích hợp KATA → Loại trừ đo lường từ xa**.

5. Trong mục **Thiết lập truyền dữ liệu**, hãy chọn hộp kiểm **Sử dụng loại trừ**.

6. Nhấn vào **Thêm** và cấu hình các loại trừ:

Các tiêu chí được kết hợp với *AND* logic.

- **Đường dẫn**. Đường dẫn đầy đủ đến tập tin, bao gồm tên và phần mở rộng của tập tin. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện. Để loại trừ hoạt động, đường dẫn đến tập tin phải được chỉ định.
- **Dòng lệnh**. Lệnh được dùng để chạy đối tượng.
- **Mô tả**. Giá trị của tham số FileDescription từ tài nguyên RT_VERSION (VersionInfo).
  Để biết thêm chi tiết về tài nguyên VersionInfo, vui lòng truy cập website của Microsoft.
- **Tên tập tin gốc**. Giá trị của tham số OriginalFilename từ tài nguyên RT_VERSION (VersionInfo).
- **Phiên bản**. Giá trị của tham số FileVersion từ tài nguyên RT_VERSION (VersionInfo).
- **MD5**. Giá trị hash MD5 của tập tin.
- **SHA256**. Giá trị hash SHA256 của tập tin.
- **Loại sự kiện**. Để loại trừ hoạt động, bạn phải chọn ít nhất một loại sự kiện.

7. Lưu các thay đổi của bạn.

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Tasks**.
   Danh sách tác vụ sẽ mở.
2. Nhấn vào **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

1. Chọn **Kaspersky Endpoint Security cho Windows (14.2)** → **Hoàn tác bản cập nhật**.

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 tác vụ, ví dụ như theo cách thủ công.

Bước 4. Xác định tên tác vụ

Nhập tên cho tác vụ.

Bước 7. Hoàn tất việc tạo tác vụ

Hoàn tất 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.

Loại trừ đo lường từ xa EDR (KATA)

Để nâng cao hiệu năng và tối ưu hóa việc truyền dữ liệu đến máy chủ Đo lường từ xa, bạn có thể cấu hình loại trừ đo lường từ xa. Ví dụ: bạn có thể chọn không gửi dữ liệu giao tiếp mạng cho từng ứng dụng.

Cách tạo loại trừ đo từ xa trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Loại trừ và loại đối tượng**.
4. Trong mục **Thiết lập đo lường từ xa → Đo lường từ xa EDR (KATA) / NDR (KATA)**, hãy nhấn nút **Thiết lập**.
5. Trong cửa sổ mở ra, hãy cấu hình các loại trừ dữ liệu đo từ xa (xem bảng bên dưới).

   Ứng dụng kết hợp các điều kiện loại trừ với toán tử logic AND. Để tạo một quy tắc, bạn phải chỉ định một giá trị trong trường **Đường dẫn đầy đủ** và chọn ít nhất một loại sự kiện trong danh sách **Sử dụng cho các loại sự kiện sau**.
6. Lưu các thay đổi của bạn.

Cách tạo loại trừ đo 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 **Asset management → Policies**.
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** → **Telemetry Settings**.

5. Chọn thẻ **EDR (KATA) / NDR (KATA) telemetry**.

6. Trong cửa sổ mở ra, hãy cấu hình các loại trừ dữ liệu đo từ xa (xem bảng bên dưới).

   Ứng dụng kết hợp các điều kiện loại trừ với toán tử logic AND. Để tạo một quy tắc, bạn phải chỉ định một giá trị trong trường **Full path** và chọn ít nhất một loại sự kiện.

7. Lưu các thay đổi của bạn.

Các tham số loại trừ đo từ xa

Tham số	Mô tả
Các tiến trình được loại trừ	**Tối ưu hóa dung lượng đo từ xa để gửi**. Kaspersky Endpoint Security cho phép tối ưu hóa lượng dữ liệu được truyền và loại trừ các sự kiện bằng một số mã nhất định khỏi dữ liệu đo lường từ xa: mã 102 (giao tiếp cơ bản) và 8 (hoạt động mạng của tiến trình) cho giao thức Microsoft SMB, dịch vụ WinRM và tiến trình klnagent.exe của Network Agent, cũng như thông tin mở rộng về các loại gói tin mạng cho tất cả các loại giao thức mạng. Kaspersky Endpoint Security kết hợp các tiêu chí kích hoạt quy tắc với toán tử AND logic. **Process** và **Parent process**: • **Full path**. Đường dẫn đầy đủ đến tập tin, bao gồm tên và phần mở rộng của tập tin. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện. • **Command line text**. Lệnh được dùng để chạy tập tin. • **Description**. Giá trị của tham số FileDescription từ tài nguyên RT_VERSION (VersionInfo). • **Original file name**. Giá trị của tham số OriginalFilename từ tài nguyên RT_VERSION (VersionInfo). • **Version**. Giá trị của tham số FileVersion từ tài nguyên RT_VERSION (VersionInfo). • **File checksums**. MD5 và SHA256. Bạn cũng có thể chọn tập tin theo cách thủ công và ứng dụng sẽ tự động điền vào các trường từ tập tin đã chọn. Trong hệ điều hành 64 bit, bạn phải nhập thủ công tham số của phiên bản 64 bit của tập tin thực thi của một tiến trình từ thư mục `C:\windows\system32` vì ứng dụng sẽ điền vào các trường tham số tập tin thực thi bằng dữ liệu từ các thuộc tính của phiên bản 32 bit của cùng một tập tin thực thi trong thư mục `C:\windows\syswow64`. Ví dụ: nếu bạn chọn `C:\windows\system32\cmd.exe`, tiện ích sẽ hiển thị các tham số của `C:\windows\syswow64\cmd.exe`. Hành vi như vậy được quyết định bởi đặc thù của hệ điều hành. **Sử dụng cho các loại sự kiện sau**: • **Sửa đổi tập tin**. • **Sự kiện mạng**. • **Tiến trình: đầu vào tương tác của bảng điều khiển**. • **Đã tải mô-đun**. • **Đã sửa đổi registry**. • **Nhật ký DNS**. • **Truy cập tiến trình**. • **Chèn mã**. • **Truy vấn WMI**. • **Đường ống**. • **LDAP**. • **AMSI**.

Tham số	Mô tả
Các giao tiếp mạng được loại trừ	**Tên quy tắc**. **Hướng**. **Giao thức**. **Socket thô**. **Số hiệu giao thức**. **Chứng chỉ TLS**. **Cổng hoặc dải cổng cục bộ**. **Cổng hoặc dải cổng từ xa**. **Địa chỉ nội bộ**. Địa chỉ mạng của máy tính mà Kaspersky Endpoint Security đang loại trừ đo lường từ xa khỏi lưu lượng mạng. **Địa chỉ từ xa**. Địa chỉ mạng của máy tính mà Kaspersky Endpoint Security đang loại trừ đo lường từ xa khỏi lưu lượng mạng. Chỉ hỗ trợ định dạng IPv4 cho địa chỉ IP. **Ứng dụng**. Danh sách các tập tin thực thi của ứng dụng mà Kaspersky Endpoint Security đang loại trừ đo lường từ xa EDR khỏi lưu lượng mạng.
Thao tác với tập tin được loại trừ	**Tên quy tắc**. **Tên tập tin hoặc tên đại diện**. Tên hoặc tên đại diện của tập tin hoặc thư mục; Kaspersky Endpoint Security sẽ áp dụng quy tắc loại trừ khi tập tin hoặc thư mục này được truy cập. Kaspersky Endpoint Security hỗ trợ các ký tự `*` và `?` khi nhập tên đại diện. **Loại hoạt động**. **Đường dẫn trước đó**. Kaspersky Endpoint Security kết hợp các tiêu chí kích hoạt quy tắc với toán tử AND logic. **Process** và **Parent process**: • **Full path**. Đường dẫn đầy đủ đến tập tin, bao gồm tên và phần mở rộng của tập tin. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện. • **Command line text**. Lệnh được dùng để chạy tập tin. • **Description**. Giá trị của tham số FileDescription từ tài nguyên RT_VERSION (VersionInfo). • **Original file name**. Giá trị của tham số OriginalFilename từ tài nguyên RT_VERSION (VersionInfo). • **Version**. Giá trị của tham số FileVersion từ tài nguyên RT_VERSION (VersionInfo). • **File checksums**. MD5 và SHA256. Bạn cũng có thể chọn tập tin theo cách thủ công và ứng dụng sẽ tự động điền vào các trường từ tập tin đã chọn. Trong hệ điều hành 64 bit, bạn phải nhập thủ công tham số của phiên bản 64 bit của tập tin thực thi của một tiến trình từ thư mục `C:\windows\system32` vì ứng dụng sẽ điền vào các trường tham số tập tin thực thi bằng dữ liệu từ các thuộc tính của phiên bản 32 bit của cùng một tập tin thực thi trong thư mục `C:\windows\syswow64`. Ví dụ: nếu bạn chọn `C:\windows\system32\cmd.exe`, tiện ích sẽ hiển thị các tham số của `C:\windows\syswow64\cmd.exe`. Hành vi như vậy được quyết định bởi đặc thù của hệ điều hành.

Tham số	Mô tả
Hoạt động DNS bị loại trừ	**Tên quy tắc**. Kaspersky Endpoint Security kết hợp các tiêu chí kích hoạt quy tắc với toán tử AND logic. **Process** và **Parent process**: • **Full path**. Đường dẫn đầy đủ đến tập tin, bao gồm tên và phần mở rộng của tập tin. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện. • **Command line text**. Lệnh được dùng để chạy tập tin. • **Description**. Giá trị của tham số FileDescription từ tài nguyên RT_VERSION (VersionInfo). • **Original file name**. Giá trị của tham số OriginalFilename từ tài nguyên RT_VERSION (VersionInfo). • **Version**. Giá trị của tham số FileVersion từ tài nguyên RT_VERSION (VersionInfo). • **File checksums**. MD5 và SHA256. Bạn cũng có thể chọn tập tin theo cách thủ công và ứng dụng sẽ tự động điền vào các trường từ tập tin đã chọn. Trong hệ điều hành 64 bit, bạn phải nhập thủ công tham số của phiên bản 64 bit của tập tin thực thi của một tiến trình từ thư mục `C:\windows\system32` vì ứng dụng sẽ điền vào các trường tham số tập tin thực thi bằng dữ liệu từ các thuộc tính của phiên bản 32 bit của cùng một tập tin thực thi trong thư mục `C:\windows\syswow64`. Ví dụ: nếu bạn chọn `C:\windows\system32\cmd.exe`, tiện ích sẽ hiển thị các tham số của `C:\windows\syswow64\cmd.exe`. Hành vi như vậy được quyết định bởi đặc thù của hệ điều hành. **DNS**: • **Địa chỉ IP máy chủ DNS**. • **Tùy chọn truy vấn**. • **Trạng thái**. • **Tên miền**. • **ID loại thiết lập**. • **Dữ liệu phản hồi**.
Hoạt động LDAP bị loại trừ	**Tên quy tắc**. **Phạm vi tìm kiếm LDAP**. **Lọc**. **Tên phân biệt để tìm kiếm đối tượng LDAP**. **Thuộc tính đối tượng**. Kaspersky Endpoint Security kết hợp các tiêu chí kích hoạt quy tắc với toán tử AND logic. **Process** và **Parent process**: • **Full path**. Đường dẫn đầy đủ đến tập tin, bao gồm tên và phần mở rộng của tập tin. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện. • **Command line text**. Lệnh được dùng để chạy tập tin. • **Description**. Giá trị của tham số FileDescription từ tài nguyên RT_VERSION (VersionInfo). • **Original file name**. Giá trị của tham số OriginalFilename từ tài nguyên RT_VERSION (VersionInfo). • **Version**. Giá trị của tham số FileVersion từ tài nguyên RT_VERSION (VersionInfo). • **File checksums**. MD5 và SHA256. Bạn cũng có thể chọn tập tin theo cách thủ công và ứng dụng sẽ tự động điền vào các trường từ tập tin đã chọn. Trong hệ điều hành 64 bit, bạn phải nhập thủ công tham số của phiên bản 64 bit của tập tin thực thi của một tiến trình từ thư mục `C:\windows\system32` vì ứng dụng sẽ điền vào các trường tham số tập tin thực thi bằng dữ liệu từ các thuộc tính của phiên bản 32 bit của cùng một tập tin thực thi trong thư mục `C:\windows\syswow64`. Ví dụ: nếu bạn chọn `C:\windows\system32\cmd.exe`, tiện ích sẽ hiển thị các tham số của `C:\windows\syswow64\cmd.exe`. Hành vi như vậy được quyết định bởi đặc thù của hệ điều hành.

Tham số	Mô tả
Truy vấn truy cập tiến trình bị loại trừ	**Tên quy tắc**. **Loại hoạt động**. **Đã yêu cầu quyền truy cập tiến trình**. **Dấu vết ngăn xếp gọi hàm**. Kaspersky Endpoint Security kết hợp các tiêu chí kích hoạt quy tắc với toán tử AND logic. **Process**, **Parent process**, **File of the target process**, **Handle to the source process** và **Handle to the target process**. • **Đường dẫn đầy đủ**. Đường dẫn đầy đủ đến tập tin, bao gồm tên và phần mở rộng của tập tin. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện. • **Văn bản dòng lệnh**. Lệnh được dùng để chạy tập tin. • **Chỉ định tiêu chí kích hoạt quy tắc và loại sự kiện để sử dụng quy tắc này**. Giá trị của tham số FileDescription từ tài nguyên RT_VERSION (VersionInfo). • **Tên tập tin gốc**. Giá trị của tham số OriginalFilename từ tài nguyên RT_VERSION (VersionInfo). • **Phiên bản**. Giá trị của tham số FileVersion từ tài nguyên RT_VERSION (VersionInfo). • **Giá trị tổng kiểm của tập tin**. MD5 và SHA256. Bạn cũng có thể chọn tập tin theo cách thủ công và ứng dụng sẽ tự động điền vào các trường từ tập tin đã chọn. Trong hệ điều hành 64 bit, bạn phải nhập thủ công tham số của phiên bản 64 bit của tập tin thực thi của một tiến trình từ thư mục `C:\windows\system32` vì ứng dụng sẽ điền vào các trường tham số tập tin thực thi bằng dữ liệu từ các thuộc tính của phiên bản 32 bit của cùng một tập tin thực thi trong thư mục `C:\windows\syswow64`. Ví dụ: nếu bạn chọn `C:\windows\system32\cmd.exe`, tiện ích sẽ hiển thị các tham số của `C:\windows\syswow64\cmd.exe`. Hành vi như vậy được quyết định bởi đặc thù của hệ điều hành.
Chèn mã bị loại trừ	**Tên quy tắc**. **Phương thức truy cập**. **Ngăn xếp gọi hàm**. **Dòng lệnh được sửa đổi**. **Địa chỉ chèn mã**. **Tên DLL được chèn**. Kaspersky Endpoint Security kết hợp các tiêu chí kích hoạt quy tắc với toán tử AND logic. **Process** và **Parent process**: • **Full path**. Đường dẫn đầy đủ đến tập tin, bao gồm tên và phần mở rộng của tập tin. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện. • **Command line text**. Lệnh được dùng để chạy tập tin. • **Description**. Giá trị của tham số FileDescription từ tài nguyên RT_VERSION (VersionInfo). • **Original file name**. Giá trị của tham số OriginalFilename từ tài nguyên RT_VERSION (VersionInfo). • **Version**. Giá trị của tham số FileVersion từ tài nguyên RT_VERSION (VersionInfo). • **File checksums**. MD5 và SHA256. Bạn cũng có thể chọn tập tin theo cách thủ công và ứng dụng sẽ tự động điền vào các trường từ tập tin đã chọn. Trong hệ điều hành 64 bit, bạn phải nhập thủ công tham số của phiên bản 64 bit của tập tin thực thi của một tiến trình từ thư mục `C:\windows\system32` vì ứng dụng sẽ điền vào các trường tham số tập tin thực thi bằng dữ liệu từ các thuộc tính của phiên bản 32 bit của cùng một tập tin thực thi trong thư mục `C:\windows\syswow64`. Ví dụ: nếu bạn chọn `C:\windows\system32\cmd.exe`, tiện ích sẽ hiển thị các tham số của `C:\windows\syswow64\cmd.exe`. Hành vi như vậy được quyết định bởi đặc thù của hệ điều hành.

Tham số	Mô tả
Các truy vấn WMI bị loại trừ	**Tên quy tắc**. **Loại hoạt động WMI**. **Truy vấn từ xa**. **Tên của máy tính đã thực thi lệnh WMI**. **Tài khoản người dùng WMI**. **Lệnh WMI đã thực thi**. **Tên của không gian WMI**. **Bộ lọc người dùng sự kiện WMI**. **Tên của người dùng sự kiện WMI đã tạo**. **Mã nguồn của người dùng sự kiện WMI**. Kaspersky Endpoint Security kết hợp các tiêu chí kích hoạt quy tắc với toán tử AND logic. **Process** và **Parent process**: • **Full path**. Đường dẫn đầy đủ đến tập tin, bao gồm tên và phần mở rộng của tập tin. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện. • **Command line text**. Lệnh được dùng để chạy tập tin. • **Description**. Giá trị của tham số FileDescription từ tài nguyên RT_VERSION (VersionInfo). • **Original file name**. Giá trị của tham số OriginalFilename từ tài nguyên RT_VERSION (VersionInfo). • **Version**. Giá trị của tham số FileVersion từ tài nguyên RT_VERSION (VersionInfo). • **File checksums**. MD5 và SHA256. Bạn cũng có thể chọn tập tin theo cách thủ công và ứng dụng sẽ tự động điền vào các trường từ tập tin đã chọn. Trong hệ điều hành 64 bit, bạn phải nhập thủ công tham số của phiên bản 64 bit của tập tin thực thi của một tiến trình từ thư mục `C:\windows\system32` vì ứng dụng sẽ điền vào các trường tham số tập tin thực thi bằng dữ liệu từ các thuộc tính của phiên bản 32 bit của cùng một tập tin thực thi trong thư mục `C:\windows\syswow64`. Ví dụ: nếu bạn chọn `C:\windows\system32\cmd.exe`, tiện ích sẽ hiển thị các tham số của `C:\windows\syswow64\cmd.exe`. Hành vi như vậy được quyết định bởi đặc thù của hệ điều hành.
Hoạt động đường ống bị loại trừ	**Tên quy tắc**. **Tên đường ống**. **Loại hoạt động**. Kaspersky Endpoint Security kết hợp các tiêu chí kích hoạt quy tắc với toán tử AND logic. **Process** và **Parent process**: • **Full path**. Đường dẫn đầy đủ đến tập tin, bao gồm tên và phần mở rộng của tập tin. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện. • **Command line text**. Lệnh được dùng để chạy tập tin. • **Description**. Giá trị của tham số FileDescription từ tài nguyên RT_VERSION (VersionInfo). • **Original file name**. Giá trị của tham số OriginalFilename từ tài nguyên RT_VERSION (VersionInfo). • **Version**. Giá trị của tham số FileVersion từ tài nguyên RT_VERSION (VersionInfo). • **File checksums**. MD5 và SHA256. Bạn cũng có thể chọn tập tin theo cách thủ công và ứng dụng sẽ tự động điền vào các trường từ tập tin đã chọn. Trong hệ điều hành 64 bit, bạn phải nhập thủ công tham số của phiên bản 64 bit của tập tin thực thi của một tiến trình từ thư mục `C:\windows\system32` vì ứng dụng sẽ điền vào các trường tham số tập tin thực thi bằng dữ liệu từ các thuộc tính của phiên bản 32 bit của cùng một tập tin thực thi trong thư mục `C:\windows\syswow64`. Ví dụ: nếu bạn chọn `C:\windows\system32\cmd.exe`, tiện ích sẽ hiển thị các tham số của `C:\windows\syswow64\cmd.exe`. Hành vi như vậy được quyết định bởi đặc thù của hệ điều hành.

Tham số	Mô tả
Thay đổi registry bị loại trừ	**Tên quy tắc**. **Loại hoạt động**. **Đường dẫn**. **Tên giá trị**. **Giá trị**. **Tên đầy đủ của tập tin registry**. Kaspersky Endpoint Security kết hợp các tiêu chí kích hoạt quy tắc với toán tử AND logic. **Process** và **Parent process**: • **Full path**. Đường dẫn đầy đủ đến tập tin, bao gồm tên và phần mở rộng của tập tin. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện. • **Command line text**. Lệnh được dùng để chạy tập tin. • **Description**. Giá trị của tham số FileDescription từ tài nguyên RT_VERSION (VersionInfo). • **Original file name**. Giá trị của tham số OriginalFilename từ tài nguyên RT_VERSION (VersionInfo). • **Version**. Giá trị của tham số FileVersion từ tài nguyên RT_VERSION (VersionInfo). • **File checksums**. MD5 và SHA256. Bạn cũng có thể chọn tập tin theo cách thủ công và ứng dụng sẽ tự động điền vào các trường từ tập tin đã chọn. Trong hệ điều hành 64 bit, bạn phải nhập thủ công tham số của phiên bản 64 bit của tập tin thực thi của một tiến trình từ thư mục `C:\windows\system32` vì ứng dụng sẽ điền vào các trường tham số tập tin thực thi bằng dữ liệu từ các thuộc tính của phiên bản 32 bit của cùng một tập tin thực thi trong thư mục `C:\windows\syswow64`. Ví dụ: nếu bạn chọn `C:\windows\system32\cmd.exe`, tiện ích sẽ hiển thị các tham số của `C:\windows\syswow64\cmd.exe`. Hành vi như vậy được quyết định bởi đặc thù của hệ điều hành.
Các hoạt động bị loại trừ với thiết bị	**Tên quy tắc**. **Loại thiết bị**. **ID thiết bị**. **Tên thiết bị**.

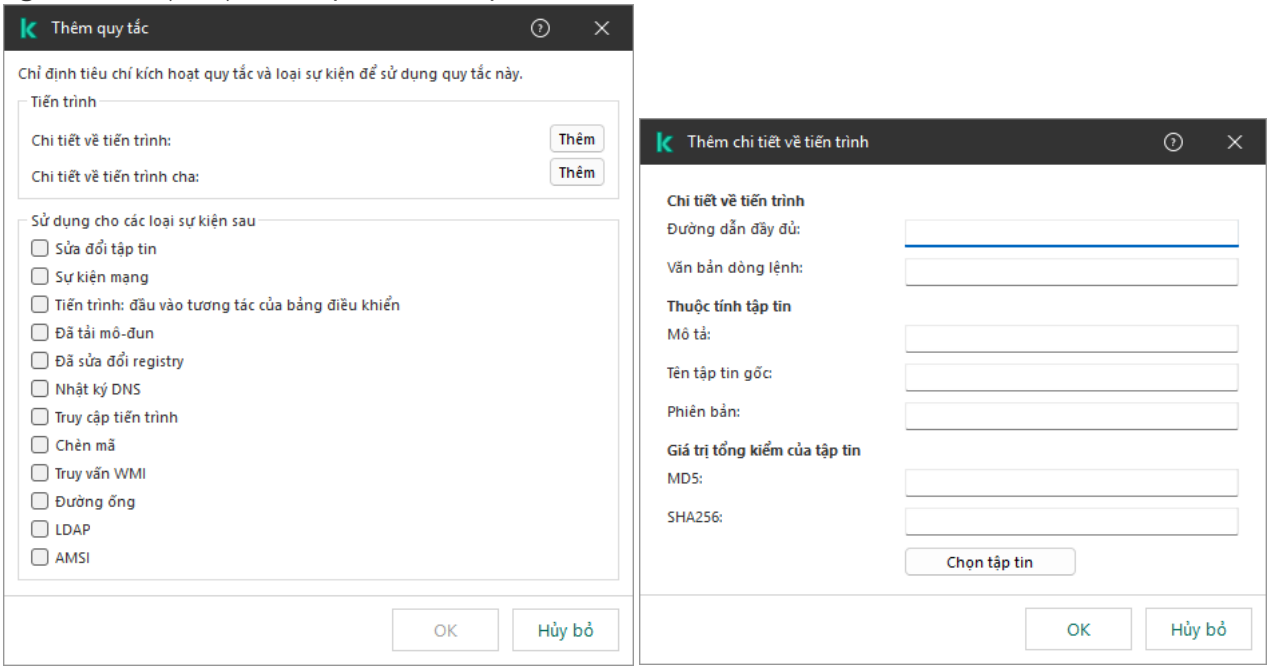
Ví dụ 1. Các tiến trình được loại trừ

Để loại trừ các sự kiện ứng dụng (tiến trình) của bên thứ ba khỏi đo từ xa, hãy mở cửa sổ loại trừ đo từ xa EDR trên thẻ **Các tiến trình được loại trừ** và thêm tập tin thực thi của ứng dụng.

Kaspersky Endpoint Security kết hợp các tiêu chí kích hoạt quy tắc với toán tử AND logic.

Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện. Ví dụ:

- `C:\Program Files\*\notepad++.exe`
- `%ProgramFiles(x86)%\Notepad++\notepad++.exe`



Loại trừ một tiến trình

Ví dụ 1. Sửa đổi tập tin

Nếu thường xuyên chỉnh sửa các tập lệnh trong ứng dụng Notepad++ và bạn muốn loại trừ các sự kiện sửa đổi cho các tập lệnh tương ứng, hãy thêm tập tin thực thi Notepad++ vào loại trừ đo từ xa.

Chỉ định các thiết lập như sau:

- **Đường dẫn đầy đủ**: `C:\Program Files\Notepad++\notepad++.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.
- **Sử dụng cho các loại sự kiện sau**: Sửa đổi tập tin.

Ví dụ 2. Sự kiện mạng

Nếu bạn sử dụng ứng dụng WinSCP để quản lý các tập tin trên máy chủ từ xa và bạn muốn loại trừ các sự kiện mạng, hãy thêm tập tin thực thi WinSCP vào loại trừ đo từ xa.

Chỉ định các thiết lập như sau:

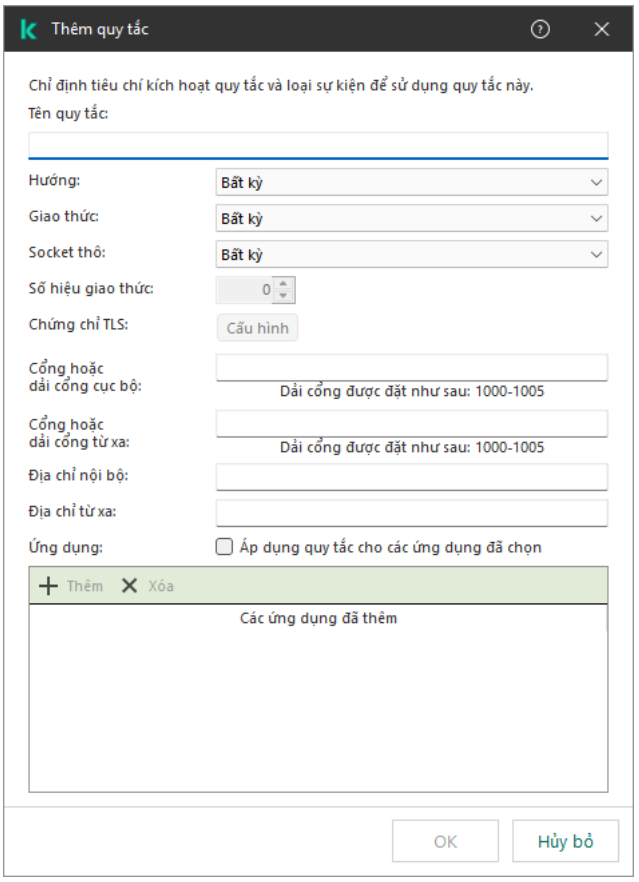
- **Đường dẫn đầy đủ**: `C:\Program Files (x86)\WinSCP\WinSCP.exe`.
- **SHA256**: 47204338f0e092057024c9186f228c02417e917777f3e841d52b58251a956a74 (không bắt buộc).
- **Sử dụng cho các loại sự kiện sau**: Sự kiện mạng.

Ví dụ 2. Các giao tiếp mạng được loại trừ

Để loại trừ các sự kiện kết nối dịch vụ đo từ xa khỏi đo từ xa, hãy mở cửa sổ loại trừ đo từ xa EDR trên thẻ **Các giao tiếp mạng được loại trừ** và thêm thiết lập kết nối: giao thức, cổng, hướng, địa chỉ IP, chứng chỉ TLS và các thiết lập khác.

Kaspersky Endpoint Security kết hợp các tiêu chí kích hoạt quy tắc với toán tử AND logic.

Bạn không thể chỉ định địa chỉ mạng con (ví dụ: 10.28.0.0/24). Ứng dụng chỉ cho phép chỉ định một địa chỉ IP (ví dụ: 10.28.0.105).



Loại trừ giao tiếp mạng

Nếu bạn sử dụng máy chủ web của công ty và muốn loại trừ các sự kiện trình duyệt khi kết nối với máy chủ web đó, hãy thêm địa chỉ IP của máy chủ và tập tin thực thi của trình duyệt vào mục loại trừ từ xa.

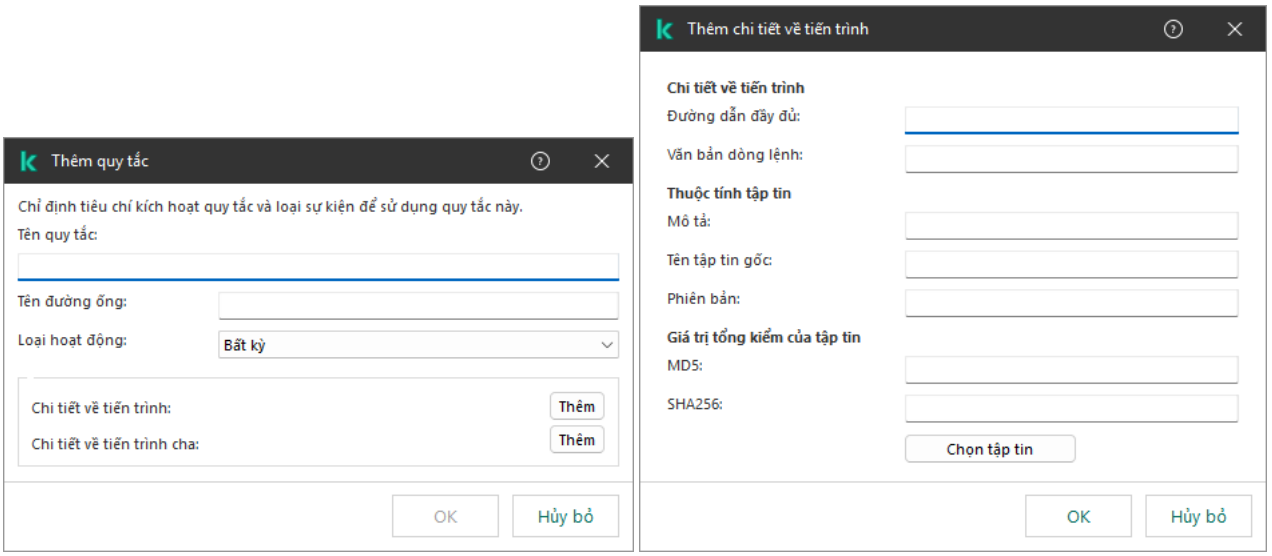
Chỉ định các thiết lập như sau:

- **Giao thức**: TCP.
- **Cổng hoặc dải cổng từ xa**: 443.
- **Địa chỉ từ xa**: 10.28.0.105.
- **Ứng dụng**: `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe`; `C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`.

Ví dụ 3. Các thao tác với tập tin được loại trừ

Để loại trừ các sự kiện liên quan đến hoạt động với các tập tin được tin tưởng khỏi đo từ xa, hãy mở cửa sổ loại trừ đo từ xa EDR trên thẻ **Thao tác với tập tin được loại trừ** thêm tập tin được tin tưởng.

Kaspersky Endpoint Security kết hợp các tiêu chí kích hoạt quy tắc với toán tử AND logic.



Loại trừ các thao tác với tập tin

Nếu một ứng dụng ghi vào nhật ký và bạn muốn loại trừ các sự kiện sửa đổi tập tin nhật ký thì hãy thêm tập tin nhật ký và tập tin thực thi của ứng dụng khỏi đo từ xa.

Chỉ định các thiết lập như sau:

- **Tên tập tin hoặc tên đại diện**: `C:\Apache24\logs\error.log`.
- **Loại hoạt động**: Sửa đổi tập tin.
- **Đường dẫn đầy đủ**: `C:\Apache24\bin\httpd.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

Ví dụ 4. Các sửa đổi registry được loại trừ

Để loại trừ các sự kiện sửa đổi registry khỏi đo từ xa, hãy mở cửa sổ loại trừ đo từ xa EDR trên thẻ **Thay đổi registry bị loại trừ** và thêm khóa registry.

Kaspersky Endpoint Security kết hợp các tiêu chí kích hoạt quy tắc với toán tử AND logic.

Nếu một ứng dụng thường xuyên sửa đổi các giá trị registry và bạn muốn loại trừ các sự kiện sửa đổi registry này khỏi đo từ xa, hãy thêm khóa registry và tập tin thực thi của ứng dụng vào mục loại trừ đo từ xa.

Chỉ định các thiết lập như sau:

- **Loại hoạt động**: Thay đổi.
- **Đường dẫn**: HKEY_LOCAL_MACHINE\SOFTWARE\SimonTatham\PuTTY64.
- **Đường dẫn đầy đủ**: `C:\Program Files\PuTTY\putty.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

KATA Sandbox

Kaspersky Anti Targeted Attack Platform bao gồm thành phần Sandbox (KATA Sandbox). *Sandbox* là công nghệ cho phép bạn phát hiện các mối đe dọa nâng cao trên máy tính. 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. 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 (các máy chủ Sandbox). Để biết chi tiết về giải pháp này, vui lòng tham khảo Trợ giúp của Kaspersky Anti Targeted Attack Platform.

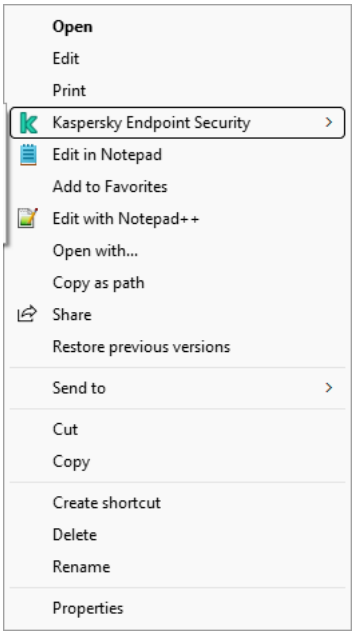
> Để kích hoạt KATA Sandbox, bạn cần có khóa giấy phép hỗ trợ chức năng KATA hoặc KEDR. Để biết chi tiết về các chức năng khả dụng, hãy tham khảo Trợ giúp của Kaspersky Anti Targeted Attack Platform.

KATA Sandbox cho phép quét các tập tin ở các chế độ sau:

- *Thủ công*. Người dùng gửi tập tin theo cách thủ công để quét từ menu ngữ cảnh (**Gửi đến Sandbox**). Khi gửi tập tin đến Sandbox, ứng dụng cũng sẽ quét tập tin bằng cơ sở dữ liệu chống virus.
- *Tự động*. Ứng dụng tự động phát hiện các đối tượng và gửi chúng đến Sandbox để quét.

Sau khi tập tin được gửi đến Sandbox, người dùng vẫn có thể truy cập được tập tin đó. Kaspersky Endpoint Security ghi lại sự kiện tương ứng và gửi sự kiện đó đến Kaspersky Security Center và bảng điều khiển Kaspersky Anti Targeted Attack Platform. Nếu Sandbox phát hiện hoạt động độc hại, Kaspersky Endpoint Security sẽ thực hiện Hành động phản hồi với mối đe dọa một cách tự động (ví dụ: xóa đối tượng và khởi tạo Quét khu vực quan trọng).

Để KATA Sandbox hoạt động ở chế độ thủ công, bạn phải triển khai Kaspersky Anti Targeted Attack Platform 7.0 trở lên. Để KATA Sandbox hoạt động ở chế độ tự động, bạn phải triển khai Kaspersky Anti Targeted Attack Platform 8.0 trở lên.



Quét trong KATA Sandbox từ menu ngữ cảnh

Tích hợp tác nhân tích hợp với KATA Sandbox

Phải thêm thành phần Sandbox để tích hợp với KATA Sandbox. Bạn có thể chọn thành phần Sandbox trong quá trình cài đặt hoặc nâng cấp, cũng như sử dụng tác vụ *Thay đổi thành phần ứng dụng*.

Để gửi tập tin để quét, bạn phải bật tích hợp với KATA Sandbox và thêm máy chủ Central Node được triển khai bên trong giải pháp. 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).

Để bật hoặc tắt tích hợp với KATA Sandbox:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Sandbox**.
5. Sử dụng nút bật/tắt **Integration with Sandbox ENABLED** để bật hoặc tắt thành phần này.

6. Chọn chế độ hoạt động của KATA Sandbox:

   - **Manually**. Người dùng gửi tập tin theo cách thủ công để quét từ menu ngữ cảnh (**Gửi đến Sandbox**).
   - **Automatically**. Ứng dụng tự động phát hiện các đối tượng và gửi chúng đến Sandbox để quét.
   - **Combined**.

7. Nhấn vào liên kết **Connection settings**.

8. Cấu hình thiết lập kết nối máy chủ Central Node:

   - **Timeout (msec)**. Hết thời gian kết nối cho máy chủ Central Node. 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 máy chủ 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.
   - **Request queue**. Kích thước của thư mục hàng chờ yêu cầu. Khi gửi nhiều đối tượng để quét trong Sandbox, 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, 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.
   - **Server TLS certificate**. Để cấu hình kết nối được tin tưởng với máy chủ Central Node, bạn phải chuẩn bị chứng chỉ TLS. Sau đó, bạn phải thêm chứng chỉ vào máy tính bằng chính sách. Bạn cũng cần thêm chứng chỉ vào máy chủ Central Node.
   - **Use two-way authentication**. Xác thực hai chiều khi thiết lập kết nối bảo mật giữa Kaspersky Endpoint Security và máy chủ Central Node. Để sử dụng xác thực hai chiều, bạn cần bật xác thực hai chiều trong cài đặt máy chủ Central Node, sau đó lấy bộ chứa mã hóa và đặt mật khẩu để bảo vệ bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể nhận một bộ chứa mã hóa trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform). Sau khi cấu hình thiết lập Central Node, bạn cũng cần bật xác thực hai chiều trong thiết lập của Kaspersky Endpoint Security và tải bộ chứa mã hóa được bảo vệ bằng mật khẩu.

9. Trong mục **Connection to Sandbox servers**, hãy nhấn nút **Add**.

10. Thao tác này sẽ mở ra một cửa sổ; trong cửa sổ đó, hãy nhập địa chỉ máy chủ Nút trung tâm (IPv4, IPv6, DNS) và cổng.

    Để biết chi tiết về việc triển khai ảnh máy ảo và cấu hình máy chủ Nút trung tâm, hãy tham khảo Trợ giúp của Kaspersky Anti Targeted Attack Platform.

11. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Kết quả là thành phần Sandbox được bật. Kiểm tra trạng thái hoạt động của thành phần bằng cách xem *Report on status of application components*. 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 **Sandbox** sẽ được thêm vào danh sách các thành phần của Kaspersky Endpoint Security.

Cấu hình các hành động Phản hồi với mối đe dọa

Nếu Sandbox phát hiện hoạt động độc hại, Kaspersky Endpoint Security sẽ thực hiện Hành động phản hồi với mối đe dọa một cách tự động (ví dụ: xóa đối tượng và khởi tạo Quét khu vực quan trọng).

Để cấu hình các hành động Phản hồi với mối đe dọa:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Sandbox**.
5. Chọn hành động liên quan trong mục **Action on threat detection**:
   - **Move copy to Quarantine, delete object**. 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.
   - **Run Critical Areas Scan**. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ chạy tác vụ *Critical Areas Scan*. Theo mặc định, Kaspersky Endpoint Security sẽ quét nhân kernel, các tiến trình đang chạy, và phân vùng khởi động ổ đĩa.
   - **Create IOC Scan task**. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ tự động tạo tác vụ *IOC Scan (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 (*Move copy to Quarantine, delete object* hoặc *Run Critical Areas Scan*). Để sửa đổi các thiết lập khác của tác vụ *IOC Scan*, hãy vào mục thiết lập tác vụ.
6. Nếu cần, hãy cấu hình thiết lập tác vụ *Quét IOC* trong mục **IOC Scan scope**.
   - **Critical file areas**. 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.
   - **File areas on system drive of the computer**. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ thực hiện quét IOC trên ổ đĩa hệ thống của máy tính.
7. Nếu cần, hãy cấu hình thiết lập tác vụ *Quét IOC* trong mục **Run IOC Scan task**.
   - **Manually**. Chế độ chạy trong đó bạn có thể tiến hành tác vụ *IOC Scan* theo cách thủ công tại một thời điểm thuận tiện cho bạn.
   - **Automatically**. Chế độ chạy trong đó Kaspersky Endpoint Security sẽ chạy tác vụ *IOC Scan* tự động sau khi phát hiện một mối đe dọa.
   - **Run only when the computer is idle**. Chế độ chạy trong đó Kaspersky Endpoint Security sẽ chạy *Quét IOC* 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.

8. Cấu hình thiết lập tác vụ nâng cao cho *Quét IOC*.

9. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Hướng dẫn chuyển KEA sang KES cho EDR (KATA)

Kể từ phiên bản 12.1, Kaspersky Endpoint Security cho Windows có một tác nhân tích hợp để quản lý thành phần Kaspersky Endpoint Detection and Response, thuộc giải pháp Kaspersky Anti Targeted Attack Platform (KATA EDR). Bạn không còn cần một ứng dụng Kaspersky Endpoint Agent riêng để fhoạt động với EDR (KATA). Tất cả các chức năng của Kaspersky Endpoint Agent sẽ được thực hiện bởi Kaspersky Endpoint Security. Mức tải trên các máy chủ của Kaspersky Anti Targeted Attack Platform sẽ không thay đổi.

Khi bạn triển khai Kaspersky Endpoint Security trên các máy tính đã cài đặt Kaspersky Endpoint Agent thì giải pháp Kaspersky Anti Targeted Attack Platform (EDR) sẽ tiếp tục hoạt động với Kaspersky Endpoint Security. Ngoài ra, Kaspersky Endpoint Agent sẽ bị gỡ bỏ khỏi máy tính. Hành vi tương tự trong hệ thống sẽ xảy ra khi bạn cập nhật Kaspersky Endpoint Security lên phiên bản 12.1 trở lên.

> Kaspersky Endpoint Security không tương thích với Kaspersky Endpoint Agent. Bạn không thể cài đặt cả hai ứng dụng này trên cùng một máy tính.

Các điều kiện sau phải được đáp ứng để Kaspersky Endpoint Security hoạt động như một phần của Endpoint Detection and Response (KATA):

- Kaspersky Anti Targeted Attack Platform phiên bản 5.0 trở lên.
- Kaspersky Security Center phiên bản 14.2 trở lên (bao gồm Network Agent). Không thể kích hoạt tính năng Endpoint Detection and Response (KATA) trong các phiên bản trước của Kaspersky Security Center.

Các bước để chuyển cấu hình [KES KEA] sang [KES+Tác nhân tích hợp] cho EDR (KATA)

1. **Nâng cấp Tiện ích quản lý Kaspersky Endpoint Security**

   Thành phần EDR (KATA) có thể được quản lý bằng Tiện ích quản lý Kaspersky Endpoint Security phiên bản 12.1 trở lên. Tùy thuộc vào loại bảng điều khiển Kaspersky Security Center bạn đang sử dụng, hãy cập nhật tiện ích quản lý trong Bảng điều khiển quản trị (MMC) hoặc tiện ích web trong Bảng điều khiển web.

2. **Chuyển chính sách và tác vụ**

   Chuyển thiết lập của Kaspersky Endpoint Agent sang Kaspersky Endpoint Security cho Windows. Các tùy chọn sau có thể được sử dụng:

   - Một trình hướng dẫn để chuyển từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security. Trình hướng dẫn chuyển từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security chỉ hoạt động trong Bảng điều khiển web

     Cách chuyển thiết lập chính sách và tác vụ từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security trong Bảng điều khiển web

Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Operations → Migration from 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 chính sách Kaspersky Endpoint Agent để chọn chính sách Kaspersky Endpoint Security mà bạn muốn gộp thiết lập. 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 không hỗ trợ các tác vụ EDR (KATA). Bỏ qua bước này.

Bước 3. Hoàn tất Trình hướng dẫn

Hoàn tất trình hướng dẫn. Nhờ trình hướng dẫn này, một chính sách Kaspersky Endpoint Security mới sẽ được tạo. 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 *Inactive*. Để tiếp tục, hãy thay đổi trạng thái của chính sách Kaspersky Endpoint Agent và Kaspersky Endpoint Security thành *Inactive* và kích hoạt chính sách mới được gộp.

Trình hướng dẫn chuyển đổi trong Bảng điều khiển web sẽ bỏ qua các thiết lập chính sách sau và không chuyển chúng:

- Cấm sửa đổi thiết lập **Connection settings** ("khóa").

  Theo mặc định, bạn có thể sửa đổi thiết lập ("khóa" đang mở). Do đó, thiết lập không được áp dụng trên máy tính đó. Bạn phải cấm sửa đổi thiết lập và đóng "khóa".

- Bộ chứa mã hóa.

  Nếu đang sử dụng xác thực hai chiều để kết nối với máy chủ Central Node thì bạn phải thêm lại bộ chứa mã hóa.

Bởi vì Trình hướng dẫn chuyển đổi không chuyển các thiết lập này nên bạn có thể gặp lỗi khi kết nối máy tính với máy chủ Central Node. Để sửa lỗi, bạn cần chuyển đến thuộc tính chính sách và cấu hình thiết lập kết nối.

- Một trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ tiêu chuẩn. Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ chỉ khả dụng trong Bảng điều khiển quản trị (MMC). Để biết thêm chi tiết về Trìnhh hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ, vui lòng tham khảo Trợ giúp của Kaspersky Security Center.

Để đảm bảo Kaspersky Endpoint Security hoạt động đúng trên các máy chủ, bạn nên thêm các tập tin quan trọng cho hoạt động của máy chủ vào khu vực tin tưởng. Đối với máy chủ SQL, bạn phải thêm tập tin cơ sở dữ liệu MDF và LDF. Đối với máy chủ Microsoft Exchange, bạn phải thêm các tập tin CHK, EDB, JRS, LOG và JSL. Bạn có thể sử dụng tên đại diện, ví dụ: `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

Kể từ Kaspersky Endpoint Security 12.6 cho Windows, loại trừ quét và ứng dụng được tin tưởng được thêm vào khu vực tin tưởng. Các ứng dụng được tin tưởng và loại trừ quét được xác định trước giúp nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager. Điều này có nghĩa là bạn không cần thiết lập khu vực tin tưởng theo cách thủ công cho ứng dụng trên máy chủ.

Các loại trừ đo lường từ xa EDR sẽ không chuyển từ chính sách Kaspersky Endpoint Agent sang chính sách Kaspersky Endpoint Security. Kaspersky Endpoint Security có các công cụ loại trừ riêng - ứng dụng được tin tưởng. Hoạt động của Kaspersky Endpoint Security được tối ưu hóa để việc không có các loại trừ đo từ xa EDR riêng lẻ sẽ không tạo thêm bất kỳ mức tải nào trên máy tính của bạn so với Kaspersky Endpoint Agent. Kaspersky Endpoint Security sử dụng đo từ xa không chỉ cho EDR (KATA), mà còn cho hoạt động của các thành phần bảo vệ của ứng dụng. Do đó, không cần chuyển các loại trừ đo lường từ xa EDR riêng lẻ. Nếu bạn thấy hiệu năng máy tính giảm, hãy kiểm tra hoạt động của ứng dụng (xem bước 7 Kiểm tra hiệu năng).

3 Cấp phép chức năng EDR (KATA)

Để kích hoạt Kaspersky Endpoint Security thành một phần của giải pháp Kaspersky Anti Targeted Attack Platform, bạn cần có giấy phép riêng cho Phần bổ trợ Kaspersky Endpoint Detection and Response (KATA). Bạn có thể thêm khóa bằng tác vụ *Add key*. Kết quả là hai khóa sẽ được thêm vào ứng dụng: *Kaspersky Endpoint Security* và *Kaspersky Endpoint Detection and Response (KATA)*.

Việc cấp giấy phép cho Phần bổ trợ Kaspersky Endpoint Detection and Response (KATA) trên các máy tính có các tính năng EDR Optimum hoặc EDR Expert đã kích hoạt trước đó liên quan đến những cân nhắc đặc biệt sau:

- Nếu bạn đang sử dụng một *tập tin khóa* để cấp phép cho Kaspersky Endpoint Security có các tính năng EDR Optimum hoặc EDR Expert thì bạn không thể thêm một khóa riêng cho Phần bổ trợ Kaspersky Endpoint Detection and Response (KATA). Bạn có thể chuyển sang sử dụng mã kích hoạt để cấp phép hoặc liên hệ với nhà cung cấp dịch vụ của mình để nhận tập tin khóa mới để kích hoạt các tính năng EDR và Kaspersky Endpoint Security. Nhà cung cấp dịch vụ sẽ cung cấp một hoặc nhiều tập tin khóa để cấp phép.

- Nếu bạn đang sử dụng một *tập tin khóa* để cấp phép cho Kaspersky Endpoint Security mà không có các tính năng EDR Optimum hoặc EDR Expert thì bạn có thể thêm một khóa riêng cho Phần bổ trợ Kaspersky Endpoint Detection and Response (KATA) mà không cần cấp lại các tập tin khóa.

- Nếu bạn đang sử dụng một *mã kích hoạt* để cấp phép thì máy chủ kích hoạt Kaspersky sẽ tự động cấp lại khóa và các tính năng EDR (KATA) sẽ tự động khả dụng. Trong trường hợp này, EDR Optimum và EDR Expert sẽ bị tắt.

- Kaspersky Endpoint Security cho phép bạn thêm tối đa hai khóa hiện hoạt: khóa Kaspersky Endpoint Security và khóa loại Phần bổ trợ. Bạn cũng có thể thêm tối đa hai khóa dự trữ. Một khóa dự trữ cho Kaspersky Endpoint Security và một khóa dự trữ cho loại Phần bổ trợ.

4 Cài đặt / nâng cấp ứng dụng Kaspersky Endpoint Security

Để chuyển chức năng EDR (KATA) trong quá trình cài đặt hoặc nâng cấp ứng dụng, bạn nên sử dụng tác vụ cài đặt từ xa. Khi tạo tác vụ cài đặt từ xa, bạn cần chọn thành phần EDR (KATA) 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.
- Cục bộ bằng cách sử dụng Trình hướng dẫn cài đặt.

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 hiện tại của các giải pháp Kaspersky. Do đó, giả sử nếu máy tính được cài đặt Kaspersky Endpoint Agent và giải pháp EDR (KATA) được kích hoạt thì bộ cài đặt Kaspersky Endpoint Security sẽ tự động cấu hình bộ thành phần và chọn thành phần EDR (KATA). 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 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 hiện tại của các giải pháp Kaspersky. Trong trường hợp này, Kaspersky Endpoint Security sẽ tự động chọn các thành phần dựa trên một bộ các thành phần của Kaspersky Endpoint Agent. Sau đó khiến Kaspersky Endpoint Security sẽ chuyển sang sử dụng tác nhân tích hợp và gỡ bỏ Kaspersky Endpoint Agent.

Kaspersky Endpoint Security hỗ trợ nâng cấp mà không cần khởi động lại máy tính. Bạn có thể chọn chế độ nâng cấp ứng dụng trong thuộc tính chính sách.

5 Kiểm tra hoạt động của ứng dụng

Nếu sau khi cài đặt hoặc nâng cấp ứng dụng, máy tính có trạng thái *Critical* trong bảng điều khiển Kaspersky Security Center:

- Đảm bảo rằng máy tính được cài đặt Network Agent phiên bản 13.2 trở lên.
- Kiểm tra trạng thái hoạt động của tác nhân tích hợp bằng cách xem *Report on status of application components*. Nếu một thành phần có trạng thái *Not installed* thì hãy cài đặt thành phần này bằng cách sử dụng tác vụ *Change application components*. Nếu một thành phần có trạng thái *Không được giấy phép hỗ trợ* thì hãy đảm bảo rằng bạn đã kích hoạt chức năng tác nhân tích hợp.
- Đảm bảo rằng bạn chấp nhận Tuyên bố Kaspersky Security Network trong chính sách mới của Kaspersky Endpoint Security cho Windows.

6 Kiểm tra kết nối đến máy chủ Kaspersky Anti Targeted Attack Platform

Kiểm tra kết nối đến máy chủ Kaspersky Anti Targeted Attack Platform. Để làm điều này:

1. Kiểm tra để đảm bảo bạn có chứng chỉ hợp lệ.
2. Kiểm tra thiết lập kết nối máy chủ.
3. Kiểm tra nhật ký sự kiện.

   Nếu kết nối đến máy chủ được thiết lập, ứng dụng sẽ gửi sự kiện *Successful connection to the EDR Expert server*. Nếu không có sự kiện kết nối thành công và không có sự kiện nào có lỗi kết nối thì hãy kiểm tra thiết lập nhật ký sự kiện và bật tính năng gửi sự kiện cho Endpoint Detection and Response (KATA).

Trạng thái kết nối máy chủ không ảnh hưởng đến trạng thái máy tính trong bảng điều khiển Kaspersky Security Center. Do đó, nếu không có kết nối với máy chủ, máy tính vẫn có thể có trạng thái *OK*. Kiểm tra nhật ký sự kiện để xác minh kết nối đến máy chủ.

7 Kiểm tra hiệu năng

Nếu hiệu năng máy tính của bạn bị chậm lại sau khi cài đặt hoặc cập nhật một ứng dụng, bạn có thể tối ưu hóa việc truyền dữ liệu. Để làm điều này:

1. Tắt thành phần EDR (KATA) và kiểm tra xem sự suy giảm hiệu năng có phải do EDR (KATA) không.
2. Với các ứng dụng được tin tưởng, hãy tắt thu thập phép đo từ xa trên thao tác nhập của bảng điều khiển (được bật theo mặc định).
3. Thêm các ứng dụng làm giảm hiệu năng máy tính vào danh sách các ứng dụng được tin tưởng.
4. Liên hệ với bộ phận Hỗ trợ Kỹ thuật của Kaspersky. Các chuyên gia hỗ trợ sẽ giúp bạn cấu hình lọc đo từ xa trong Kaspersky Anti Targeted Attack Platform. Điều này sẽ làm giảm lượng truy cập. Nếu hiệu năng máy tính của bạn bị ảnh hưởng bởi một ứng dụng nhất định, hãy đính kèm gói phân phối của ứng dụng đó vào yêu cầu.

Endpoint Detection and Response Expert (on-premises)



Kaspersky Endpoint Security cho Windows hỗ trợ tích hợp với giải pháp Kaspersky Endpoint Detection and Response Expert (on-premises). *Kaspersky Endpoint Detection and Response Expert (on-premises)* là giải pháp bảo mật mạng doanh nghiệp bao gồm các ứng dụng Kaspersky cho phép tổ chức phòng vệ trước hầu hết các loại rủi ro mạng và xử lý các tình huống phát tán mối đe dọa quan trọng nhất. Các thành phần của EDR Expert (on-premises) được triển khai trên Open Single Management Platform (OSMP). Nền tảng này chạy các kịch bản đa nền tảng trong một giao diện duy nhất và cho phép tích hợp các ứng dụng Kaspersky với ứng dụng của bên thứ ba thành một hệ thống bảo mật toàn diện.

Một trong những yếu tố cốt lõi của giải pháp là *SIEM*. SIEM theo dõi các sự kiện đến từ tất cả các thành phần và liên kết các sự kiện này với nhau bằng cách sử dụng các quy tắc do nhà cung cấp và người dùng định nghĩa. EDR Expert (on-premises) xem xét nhật ký và dữ liệu đo từ xa nhận được từ cơ sở hạ tầng của doanh nghiệp để tự động phát hiện các cuộc tấn công và cho phép điều tra sự cố bằng cách sử dụng biểu đồ điều tra thống nhất, kết hợp tất cả các sự kiện được thu thập trong EDR Expert (on-premises), bao gồm các sự kiện từ các ứng dụng Kaspersky và các sản phẩm bảo mật thông tin của bên thứ ba.

Để ứng phó với các sự cố phức tạp, EDR Expert (on-premises) sử dụng các kịch bản được thiết lập sẵn và do người dùng định nghĩa. Bạn cũng có thể sử dụng hành động phản hồi từ ứng dụng của bên thứ ba và kịch bản phản hồi liên quan đến nhiều ứng dụng.

Các công cụ Threat Intelligence

Kaspersky Endpoint Detection and Response sử dụng các công cụ Threat Intelligence sau:

- Tích hợp với 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.
- 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.

Nguyên lý hoạt động của giải pháp

Kaspersky Endpoint Security 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.

Khi được cài đặt ở chế độ tiêu chuẩn trong hạ tầng VDI, Kaspersky Endpoint Security hỗ trợ tích hợp với EDR Expert (on-premises). Tuy nhiên, không đảm bảo tính hoạt động của các chức năng khác của ứng dụng. Để bảo vệ các máy ảo trong hạ tầng VDI, chúng tôi khuyến nghị sử dụng Kaspersky Endpoint Security ở chế độ Light Agent.

Thông tin về các sự kiện trên máy tính (đo từ xa) được gửi đến máy chủ EDR Expert (on-premises). Trong trường hợp này, Kaspersky Endpoint Security cũng gửi thông tin về các mối đe dọa được phát hiện bởi ứng dụng, bao gồm cả thông tin về kết quả xử lý các mối đe dọa này đến các máy chủ thu tập từ xa.

Việc tích hợp EDR Expert (on-premises) được cấu hình trong bảng điều khiển Kaspersky Security Center. Tác nhân tích hợp sau đó được quản lý bằng Open Single Management Platform (OSMP), bao gồm hoạt động chạy các tác vụ, quản lý các đối tượng được cách ly, xem báo cáo và các hành động khác.

Các cấu hình Kaspersky Endpoint Security để làm việc với EDR Expert (on-premises)

Các cấu hình sau có thể được sử dụng để làm việc với EDR Expert (on-premises):

- **[KES+tác nhân tích hợp]**. Trong cấu hình này, Kaspersky Endpoint Security đóng vai trò vừa là ứng dụng đảm bảo khả năng bảo mật của máy tính vừa là ứng dụng để làm việc với EDR Expert (on-premises). Tác nhân tích hợp cho EDR Expert (on-premises) có trong Kaspersky Endpoint Security cho Windows phiên bản 12.11 trở lên.

- **[EPP bên thứ ba+EDR Agent]**. Trong cấu hình này, tính bảo mật của cơ sở hạ tầng CNTT được cung cấp bởi Endpoint Protection Platform (EPP) của bên thứ ba. Khả năng tương tác với EDR Expert (on-premises) được cung cấp bởi Kaspersky Endpoint Security trong cấu hình Endpoint Detection and Response Agent (EDR Agent). Trong cấu hình này, EDR Agent tương thích với các ứng dụng EPP của bên thứ ba. EDR Agent cho EDR Expert (on-premises) có sẵn trong Kaspersky Endpoint Security cho Windows phiên bản 12.11 trở lên.

Tích hợp tác nhân tích hợp với EDR Expert (on-premises)

Để tích hợp với giải pháp Kaspersky Endpoint Detection and Response Expert (on-premises), bạn cần thêm thành phần Endpoint Detection and Response Expert (on-premises) và cấu hình Kaspersky Endpoint Security.

Các thành phần Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud), và Endpoint Detection and Response Expert (on-premises) không tương thích với nhau.

Phải đáp ứng các điều kiện sau đây để Endpoint Detection and Response Expert (on-premises) hoạt động:

- OSMP (Open Single Management Platform) được cài đặt.
- Ứng dụng được kích hoạt và chức năng được giấy phép hỗ trợ.
- Thành phần Endpoint Detection and Response Expert (on-premises) được bật.
- Các thành phần ứng dụng đảm bảo hoạt động của EDR Expert (on-premises) được bật và hoạt động. Các thành phần sau đảm bảo hoạt động của EDR Expert (on-premises):
  - 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.

Thiết lập tích hợp EDR Expert (on-premises) bao gồm các bước sau:

1. **Cài đặt thành phần EDR Expert (on-premises)**

   Bạn có thể chọn thành phần EDR Expert (on-premises) 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 thành phần mới.

2. **Kích hoạt Kaspersky Endpoint Detection and Response Expert (on-premises)**

   Bạn cần mua một giấy phép riêng cho EDR Expert (on-premises) (Phần bổ trợ Kaspersky Endpoint Detection and Response Expert (on-premises)).

   Chức năng này sẽ khả dụng sau khi thêm một khóa riêng cho Kaspersky Endpoint Detection and Response Expert (on-premises). Kết quả là hai khóa được thêm trên máy tính: một khóa dành cho Kaspersky Endpoint Security và một khóa dành cho Kaspersky Endpoint Detection and Response Expert (on-premises).

   Việc cấp giấy phép cho chức năng Endpoint Detection and Response Expert (on-premises) độc lập cũng giống như việc cấp giấy phép cho Kaspersky Endpoint Security.

   Đảm bảo rằng chức năng EDR Expert (on-premises) được gộp trong giấy phép và đang chạy trong giao diện cục bộ của ứng dụng.

3. **Kết nối với máy chủ thu thập dữ liệu đo từ xa và máy chủ phản hồi**

   Kaspersky Endpoint Detection and Response Expert (on-premises) yêu cầu kết nối tin cậy giữa Kaspersky Endpoint Security và hai máy chủ:

   - *Máy chủ thu thập đo từ xa* là một máy chủ thuộc giải pháp SIEM, có chức năng thu thập, chuẩn hóa, tương quan, phân tích và lưu trữ thông tin về các sự kiện xảy ra trên máy tính.
   - *Máy chủ phản hồi* là một máy chủ dùng để tiếp nhận và quét dữ liệu, nghiên cứu hành vi của các đối tượng và công bố kết quả của các nghiên cứu đó.

   Để cấu hình kết nối được tin tưởng, bạn phải sử dụng chứng chỉ TLS. Bạn có thể lấy chứng chỉ TLS trên Open Single Management Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises)). Sau đó, bạn phải thêm chứng chỉ TLS vào Kaspersky Endpoint Security (xem hướng dẫn bên dưới).

   Theo mặc định, Kaspersky Endpoint Security chỉ kiểm tra chứng chỉ TLS của máy chủ. Để cho kết nối bảo mật hơn, bạn có thể kích hoạt thêm xác minh máy tính trên máy chủ (xác thực hai chiều). Để bật cơ chế xác minh này, bạn phải bật xác thực hai chiều trong thiết lập của máy chủ và Kaspersky Endpoint Security. Để sử dụng xác thực hai chiều, bạn cũng sẽ cần một bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể lấy container mã hóa trên Open Single Management Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises)).

Cách kết nối máy tính Kaspersky Endpoint Security với EDR Expert (on-premises) bằng Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.

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 **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)**.

5. Bật nút bật/tắt **Endpoint Detection and Response Expert (on-premises) ENABLED**.

6. Để cấu hình EDR Expert (on-premises), hãy chọn **Endpoint Detection and Response Expert (version 8.0 or later)** trong danh sách các giải pháp.

7. Cấu hình kết nối của *máy chủ thu thập dữ liệu đo từ xa*:

   a. Trong mục **Connection to telemetry collection servers**, hãy nhấn liên kết **Connection settings**.

   b. Cấu hình kết nối của máy chủ thu thập dữ liệu đo từ xa:

   - **Timeout (sec)**. Thời gian chờ phản hồi tối đa của máy chủ. Khi hết thời gian chờ, Kaspersky Endpoint Security sẽ cố gắng kết nối với một máy chủ khác.

   - **Server certificate**. Chứng chỉ TLS để thiết lập kết nối được tin tưởng với máy chủ. Bạn có thể lấy chứng chỉ TLS trên Open Single Management Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises)).

   - **Use two-way authentication**. Xác thực hai chiều khi thiết lập kết nối bảo mật giữa Kaspersky Endpoint Security và máy chủ. Để sử dụng xác thực hai chiều, bạn cần bật xác thực hai chiều trong thiết lập máy chủ, sau đó lấy bộ chứa mã hóa và đặt mật khẩu để bảo vệ bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể lấy container mã hóa trên Open Single Management Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises)). Sau khi cấu hình thiết lập máy chủ, bạn cũng cần bật xác thực hai chiều trong thiết lập của Kaspersky Endpoint Security và tải bộ chứa mã hóa được bảo vệ bằng mật khẩu.

     Bộ chứa mã hóa phải được bảo vệ bằng mật khẩu. Không thể thêm bộ chứa mã hóa có mật khẩu trống.

   c. Nhấn vào **OK**.

   d. Thêm máy chủ thu thập dữ liệu đo từ xa. Để thực hiện, hãy chỉ định địa chỉ máy chủ (IPv4, IPv6) và cổng để kết nối với máy chủ.

   Bạn có thể thêm nhiều địa chỉ máy chủ thu thập đo từ xa. Kaspersky Endpoint Security sẽ cố gắng kết nối với máy chủ bằng địa chỉ IP đầu tiên. Nếu không thể thiết lập kết nối, Kaspersky Endpoint Security sẽ cố gắng kết nối bằng địa chỉ IP thứ hai trong danh sách, v.v.

   e. Nếu cần, hãy cấu hình đo từ xa.

8. Cấu hình kết nối *máy chủ phản hồi*:

   a. Trong mục **Connection to response servers**, hãy cấu hình thiết lập **Send sync request to server every (min)**. Tần suất yêu cầu đồng bộ được gửi đến máy chủ. Trong quá trình đồng bộ, Kaspersky Endpoint Security nhận các tác vụ phản hồi mối đe dọa và gửi kết quả tác vụ.

   b. Nhấn vào liên kết **Connection settings**.

   c. Cấu hình kết nối máy chủ phản hồi:

   - **Timeout (sec)**. Thời gian chờ phản hồi tối đa của máy chủ. Khi hết thời gian chờ, Kaspersky Endpoint Security sẽ cố gắng kết nối với một máy chủ khác.
   - **Server certificate**. Chứng chỉ TLS để thiết lập kết nối được tin tưởng với máy chủ. Bạn có thể lấy chứng chỉ TLS trên Open Single Management Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises)).
   - **Use two-way authentication**. Xác thực hai chiều khi thiết lập kết nối bảo mật giữa Kaspersky Endpoint Security và máy chủ. Để sử dụng xác thực hai chiều, bạn cần bật xác thực hai chiều trong thiết lập máy chủ, sau đó lấy bộ chứa mã hóa và đặt mật khẩu để bảo vệ bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể lấy container mã hóa trên Open Single Management Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises)). Sau khi cấu hình thiết lập máy chủ, bạn cũng cần bật xác thực hai chiều trong thiết lập của Kaspersky Endpoint Security và tải bộ chứa mã hóa được bảo vệ bằng mật khẩu.

     > Bộ chứa mã hóa phải được bảo vệ bằng mật khẩu. Không thể thêm bộ chứa mã hóa có mật khẩu trống.

   d. Nhấn vào **OK**.

   e. Thêm máy chủ phản hồi. Để thực hiện, hãy chỉ định địa chỉ máy chủ (IPv4, IPv6) và cổng để kết nối với máy chủ.

      Bạn có thể thêm nhiều địa chỉ máy chủ phản hồi. Kaspersky Endpoint Security sẽ cố gắng kết nối với máy chủ bằng địa chỉ IP đầu tiên. Nếu không thể thiết lập kết nối, Kaspersky Endpoint Security sẽ cố gắng kết nối bằng địa chỉ IP thứ hai trong danh sách, v.v.

9. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Bạn có thể kiểm tra trạng thái thành phần bằng cách sử dụng*Report on status of application components*. 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 Expert (on-premises)** sẽ được thêm vào danh sách các thành phần của Kaspersky Endpoint Security.

Cấu hình thiết lập đo lường từ xa của EDR Expert (on-premises)

Dữ liệu *đo từ xa* là danh sách các sự kiện đã xảy ra trên máy tính được bảo vệ. Kaspersky Endpoint Security sẽ phân tích dữ liệu đo lường từ xa và gửi nó tới máy chủ thu thập đo từ xa trong quá trình đồng bộ. Để biết thêm thông tin về các sự kiện đo từ xa được truyền tải, hãy xem Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises).

Các sự kiện đo từ xa sẽ đến máy chủ gần như liên tục. Kaspersky Endpoint Security khởi tạo đồng bộ với máy chủ khi bất kỳ điều kiện nào sau đây được thỏa mãn:

- Khoảng thời gian đồng bộ đã hết.
- Số sự kiện trong bộ đệm vượt quá giới hạn trên.

Do đó, theo mặc định, ứng dụng sẽ đồng bộ sau mỗi 30 giây hoặc bất cứ khi nào bộ đệm chứa 1024 sự kiện. Bạn có thể cấu hình hành vi đồng bộ trong chính sách Kaspersky Endpoint Security và chọn các giá trị tối ưu để phù hợp với lượng tải mạng của bạn (xem hướng dẫn bên dưới).

Nếu không có kết nối giữa Kaspersky Endpoint Security và máy chủ, ứng dụng sẽ đặt các sự kiện mới vào hàng chờ. Khi kết nối được khôi phục, Kaspersky Endpoint Security sẽ gửi các sự kiện trong hàng chờ tới máy chủ theo đúng thứ tự. Để máy chủ không bị quá tải, Kaspersky Endpoint Security có thể bỏ qua một số sự kiện. Để bật tính năng này, bạn có thể tối ưu hóa thiết lập truyền sự kiện, chẳng hạn như đặt giá trị số sự kiện mỗi giờ tối đa (xem hướng dẫn bên dưới).

Để cấu hình thiết lập đo từ xa, hãy thực hiện các bước sau:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management → Policies**.
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 **Built-in Agents Configuration → Endpoint Detection and Response Expert (on-premises)**.
5. Để cấu hình EDR Expert (on-premises), hãy chọn **Endpoint Detection and Response Expert (version 8.0 or later)** trong danh sách các giải pháp.
6. Đảm bảo rằng hộp kiểm **Send telemetry to telemetry collection servers** được chọn trong mục **Data transmission settings**.
7. Nếu cần, hãy chọn hộp kiểm **Send telemetry with IOA only**. *Dấu hiệu tấn công (IOA)* là một quy tắc chứa mô tả về hành vi đáng ngờ trong hệ thống có thể cho biết một cuộc tấn công có chủ đích. Ứng dụng so sánh hành vi đang diễn ra trong hệ thống với các quy tắc này và ghi lại các sự kiện cho thấy có cuộc tấn công có chủ đích. Ứng dụng sử dụng công nghệ *quét luồng* cho phép theo dõi các sự kiện như vậy theo thời gian thực.
8. Nếu cần, hãy cấu hình đồng bộ hóa với thiết lập máy chủ trong mục **Data transmission settings**:

   - **Maximum event transmission delay (sec)**. Ứng dụng sẽ đồng bộ với máy chủ để gửi các sự kiện sau khi hết khoảng thời gian đồng bộ. Thiết lập mặc định là 30 giây.
   - **Maximum number of event packages**. Ứng dụng sẽ đồng bộ với máy chủ khi bộ đệm được lấp đầy bằng các sự kiện. Thiết lập mặc định là 1024 sự kiện.
9. Nếu cần, hãy xóa hộp kiểm **Enable request throttling** trong mục **Request throttling**.

   Tính năng này giúp tối ưu hóa mức tải trên máy chủ. Nếu chức năng này được kích hoạt, ứng dụng sẽ hạn chế việc truyền sự kiện. Nếu số lượng sự kiện vượt quá giới hạn được cấu hình thì Kaspersky Endpoint Security sẽ ngừng gửi sự kiện. Tùy chọn này được bật theo mặc định.

10. Cấu hình thiết lập tối ưu hóa để gửi sự kiện đến máy chủ:

    - **Maximum number of events per hour**. Ứng dụng sẽ phân tích luồng dữ liệu đo từ xa và hạn chế gửi sự kiện nếu luồng sự kiện vượt quá giới hạn số sự kiện mỗi giờ đã được cấu hình. Kaspersky Endpoint Security sẽ tiếp tục gửi sự kiện sau một giờ. Thiết lập mặc định là 3000 sự kiện mỗi giờ. Nếu ứng dụng được cài đặt trên máy chủ, luồng dữ liệu đo từ xa sẽ cao hơn. Đối với máy chủ, bạn nên tăng giá trị lên 60.000 sự kiện mỗi giờ.

    - **Percentage of event limit excess**. Ứng dụng sẽ sắp xếp sự kiện theo loại (ví dụ: sự kiện "thay đổi trong registry") và hạn chế truyền gửi sự kiện nếu tỷ lệ sự kiện cùng loại trên tổng số sự kiện vượt quá hạn mức được cấu hình theo tỷ lệ. Kaspersky Endpoint Security sẽ tiếp tục gửi sự kiện khi tỷ lệ của các sự kiện khác trên tổng số sự kiện trở lại đủ lớn. Thiết lập mặc định là 15%.

11. Trong mục **Connection to response servers**, hãy giá trị cho tham số **Send sync request to server every (min)**.

12. Tần suất yêu cầu đồng bộ được gửi đến máy chủ. Trong quá trình đồng bộ, Kaspersky Endpoint Security sẽ gửi thông tin về các thiết lập và tác vụ ứng dụng được sửa đổi.

13. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Loại trừ đo từ xa của EDR Expert (on-premises)

Để nâng cao hiệu năng và tối ưu hóa việc truyền dữ liệu đến máy chủ thu thập dữ liệu đo lường từ xa, bạn có thể thêm loại trừ dữ liệu đo lường từ xa. Ví dụ: bạn có thể chọn không gửi dữ liệu giao tiếp mạng cho từng ứng dụng.

Sử dụng quá nhiều quy tắc có thể làm tăng lượng tải cho máy chủ thu thập Đo từ xa và làm giảm hiệu năng của máy tính. Bạn chỉ nên thêm những quy tắc cần thiết.

Để tạo loại trừ dữ liệu đo lường 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 thẻ **Asset management** → **Policies**.

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** → **Telemetry Settings**.

5. Chọn thẻ **EDR Expert (on-premises) telemetry**.

6. Trong mục **General exclusions**, hãy nhấn nút **Add**.
   Cửa sổ **Add exclusion rule** sẽ mở ra.

7. Nếu cần, hãy thay đổi trạng thái của quy tắc. Theo mặc định, quy tắc đã được bật.

8. Nhập tên cho quy tắc.

9. Chọn hành động sẽ được thực hiện khi quy tắc được kích hoạt:

   - **Do not collect**. Sự kiện đã được lọc sẽ bị loại trừ khỏi dữ liệu đo lường từ xa được gửi đi.
   - **Exclude IOA**. Sự kiện kích hoạt quy tắc IOA sẽ bị loại trừ khỏi dữ liệu đo lường từ xa được gửi đi.

10. Nếu chọn tùy chọn **Exclude IOA**, hãy chỉ định các quy tắc IOA sẽ được thêm vào danh sách loại trừ:

    - **Exclude all**. Khi điều kiện được chỉ định được đáp ứng, ứng dụng sẽ loại trừ các sự kiện được tạo dựa trên tất cả quy tắc IOA khỏi dữ liệu đo lường từ xa.
    - **Exclude by GUID**. Hãy chỉ định GUID của quy tắc IOA. Bạn có thể chỉ định nhiều GUID bằng cách sử dụng `,`. Để biết thêm chi tiết về các quy tắc IOA, vui lòng tham khảo Trợ giúp EDR Expert (on-premises).

11. Hãy chỉ định điều kiện lọc:

    a. Chọn tên trường sẽ được dùng để lọc.

    b. Chọn một toán tử (xem bảng bên dưới) và chỉ định giá trị mà giá trị trường từ sự kiện sẽ được so sánh với.

Danh sách các toán tử điều kiện

Toán tử	Mô tả
<	Nếu giá trị của trường nhỏ hơn giá trị được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ.
≤	Nếu giá trị của trường nhỏ hơn hoặc bằng giá trị được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ.
=	Nếu giá trị của trường bằng với giá trị được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ.
≥	Nếu giá trị của trường lớn hơn hoặc bằng giá trị được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ.
>	Nếu giá trị của trường lớn hơn giá trị được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ.
≠	Nếu giá trị của trường không bằng giá trị được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ.
is like	Nếu giá trị trường khớp với tên đại diện được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ. Ứng dụng này hỗ trợ các ký tự `*` và `?` khi nhập tên đại diện:
is not like	Nếu giá trị trường không khớp với tên đại diện được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ. Ứng dụng này hỗ trợ các ký tự `*` và `?` khi nhập tên đại diện:
one of	Nếu giá trị của trường khớp với một trong các giá trị trong danh sách được chỉ định trong điều kiện, sự kiện đó được coi là đã được lọc.
none of	Nếu giá trị trường không khớp với bất kỳ giá trị nào trong danh sách được chỉ định trong điều kiện, sự kiện đó được coi là đã được lọc.
is like one of	Nếu giá trị trường khớp với một trong các tên đại diện được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ. Ứng dụng này hỗ trợ các ký tự * và ? khi nhập tên đại diện.
is not like one of	Nếu giá trị trường không khớp với bất kỳ tên đại diện nào được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ. Ứng dụng này hỗ trợ các ký tự * và ? khi nhập tên đại diện.
exists	Nếu trường được chỉ định trong điều kiện có trong sự kiện, sự kiện đó sẽ bị loại bỏ.
not exists	Nếu trường được chỉ định trong điều kiện không có trong sự kiện, sự kiện đó sẽ bị lọc bỏ.
contains	Nếu giá trị được chỉ định trong điều kiện có trong giá trị trường, sự kiện sẽ bị lọc bỏ.
is equal to	Nếu giá trị của trường bằng với giá trị được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ. Quá trình quét không phân biệt chữ hoa chữ thường.
bitwise AND	Nếu kết quả của phép toán Bitwise AND (&) giữa giá trị trường và giá trị được chỉ định trong điều kiện là 1, sự kiện sẽ bị loại trừ.

12. Nếu cần, bạn có thể tạo các tiêu chí lọc phức tạp bằng cách thêm nhiều điều kiện và nhóm điều kiện. Bạn cũng có thể thêm điều kiện lồng nhau và nhóm điều kiện vào một nhóm điều kiện. Bạn có thể sử dụng các toán tử sau:

    - **AND** là bộ lọc sẽ chọn các sự kiện đáp ứng tất cả các điều kiện đã được chỉ định.
    - **OR** là bộ lọc sẽ chọn các sự kiện đáp ứng một trong các điều kiện đã được chỉ định.
    - **NOT** (để sử dụng toán tử này, hãy chọn tùy chọn **Add NOT before**) nghĩa là bộ lọc chọn các sự kiện không thỏa mãn bất kỳ điều kiện nào đã chỉ định.

    Các điều kiện và nhóm điều kiện cấp đầu tiên được kết hợp bằng toán tử **AND**.

13. Nếu máy tính của bạn đang chạy Open Single Management Platform (OSMP), bạn có thể kiểm tra quy tắc lọc đã tạo. Để chạy quá trình quét, hãy nhấp vào nút **Check rule**.

    Trong cửa sổ mở ra, sẽ hiển thị bảng các sự kiện được lọc bởi quy tắc đã tạo. Để biết thêm chi tiết, vui lòng tham khảo Trợ giúp EDR Expert (on-premises).

14. Nếu cần, trong mục **All event types**, hãy thêm các ngoại lệ về đo từ xa theo loại sự kiện.

    a. Nhấp vào tên loại sự kiện.

    b. Trong cửa sổ mở ra, hãy nhấn nút **Set up manually**.

    c. Nếu cần, cấu hình việc truyền dữ liệu đo lường từ xa cho loại sự kiện đã chọn bằng công tắc bật/tắt **Send event**. Theo mặc định, việc truyền dữ liệu đo lường từ xa được bật cho tất cả các loại sự kiện.

    d. Trong mục **Exclusion rules**, hãy nhấn nút **Add**.

    Cửa sổ **Add exclusion rule** sẽ mở ra.

    e. Thực hiện các hành động được mô tả trong các bước từ 7–13 cho mỗi quy tắc bạn thêm.

15. Đối với một số loại sự kiện, bạn cũng có thể thêm quy tắc bao gồm để mở rộng dữ liệu đo lường từ xa được thu thập:

    a. Trong mục **Inclusion rules**, hãy nhấn nút **Add**.

    Cửa sổ **Add inclusion rules** sẽ mở ra.

    b. Nhập tên cho quy tắc.

    c. Trong **Condition**, nhập các giá trị cho các trường hiển thị. Loại trường khả dụng phụ thuộc vào sự kiện được chọn.

    > Các quy tắc loại trừ được ưu tiên hơn các quy tắc bao gồm.

16. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Xuất và nhập bộ lọc sự kiện EDR Expert (on-premises)

Bạn có thể xuất danh sách loại trừ ra tập tin JSON. Sau đó, bạn có thể sửa đổi tập tin, ví dụ như thêm một số lượng lớn các ID sự kiện. Bạn cũng có thể sử dụng chức năng xuất/nhập để sao lưu bộ lọc sự kiện hoặc để chuyển danh sách sang máy chủ khác.

Sử dụng quá nhiều quy tắc có thể làm tăng lượng tải cho máy chủ thu thập Đo từ xa và làm giảm hiệu năng của máy tính. Bạn chỉ nên thêm những quy tắc cần thiết.

Cách xuất và nhập bộ lọc sự kiện trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Loại trừ và loại đối tượng**.
5. Trong mục **Thiết lập đo lường từ xa → Đo lường từ xa EDR Expert (on-premises)**, hãy nhấn nút **Thiết lập**.
6. Để xuất bộ lọc sự kiện:
   a. Nhấn vào **Xuất**.
      Trong cửa sổ mở ra, hãy chỉ định tên của tập tin JSON mà bạn muốn xuất bộ lọc sự kiện vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
   b. Lưu tập tin.
      Kaspersky Endpoint Security sẽ xuất bộ lọc sự kiện vào tập tin JSON.
7. Để nhập bộ lọc sự kiện:
   a. Nhấn vào **Nhập**.
   b. Trong cửa sổ mở ra, hãy chọn tập tin JSON mà bạn muốn nhập bộ lọc sự kiện.
   c. Mở tập tin.
      Nếu các quy tắc lọc sự kiện đã tồn tại trên máy tính, Kaspersky Endpoint Security sẽ thay thế các quy tắc này khi nhập.
8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách xuất và nhập bộ lọc sự kiện trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management → Policies**.
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** → **Telemetry Settings**.

5. Chọn thẻ **EDR Expert (on-premises) telemetry**.

6. Để xuất bộ lọc sự kiện:

   a. Nhấn vào **Export**.

   b. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin JSON mà bạn muốn xuất bộ lọc sự kiện vào đó rồi chọn thư mục bạn muốn lưu tập tin này.

   c. Lưu tập tin.

   Kaspersky Endpoint Security sẽ xuất bộ lọc sự kiện vào tập tin JSON.

7. Để nhập bộ lọc sự kiện:

   a. Nhấn vào **Import**.

   b. Trong cửa sổ mở ra, hãy chọn tập tin JSON mà bạn muốn nhập bộ lọc sự kiện.

   c. Chọn cách bạn muốn nhập các quy tắc lọc sự kiện: bằng cách thêm vào các quy tắc hiện có hoặc bằng cách loại bỏ các quy tắc hiện có và thay thế bằng các quy tắc mới.

   d. Mở tập tin.

8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Bạn cũng có thể xuất hoặc nhập bộ lọc sự kiện trên dòng lệnh.

Những lưu ý đặc biệt khi sử dụng cấu hình chính sách để thiết lập tích hợp với EDR Expert (on-premises) và EDR (KATA)

Để cấu hình tích hợp với EDR (KATA) đối với một số nhóm quản lý nhất định và với EDR Expert (on-premises) đối với các trường hợp khác như một phần của chính sách duy nhất, bạn sẽ cần sử dụng hồ sơ chính sách. Bạn phải cấu hình các thiết lập tích hợp EDR (KATA) trong thuộc tính chính sách và cấu hình tích hợp EDR Expert (on-premises) cho các nhóm quản trị đã chọn trong thuộc tính hồ sơ chính sách.

Việc sử dụng cấu hình chính sách để cấu hình tích hợp với EDR Expert (on-premises) có những hạn chế sau:

- Nếu bạn cấu hình tích hợp với EDR Expert (on-premises) trong thuộc tính chính sách, các thiết lập này sẽ được áp dụng cho tất cả các nhóm quản trị; các thiết lập tích hợp từ hồ sơ chính sách sẽ không được áp dụng.
- Khi sử dụng cấu hình chính sách để thiết lập tích hợp với EDR Expert (on-premises), bạn không thể sử dụng Bảng điều khiển quản trị (MMC) để quản lý các chính sách. Khi bạn mở thuộc tính chính sách trong Bảng điều khiển quản trị, các thiết lập tích hợp EDR Expert (on-premises) trong hồ sơ chính sách sẽ bị ghi đè bởi các thiết lập từ chính sách, khiến thành phần hoạt động không chính xác. Bạn sẽ cần phải đặt lại thiết lập thành phần Endpoint Detection and Response Expert (on-premises) theo hướng dẫn bên dưới.
- Khi sử dụng cấu hình chính sách để thiết lập tích hợp với EDR Expert (on-premises), bạn không thể sử dụng các chính sách con.

Nếu đã cấu hình chính sách trong phiên bản trước của tiện ích web, bạn phải đặt lại thiết lập dành cho thành phần Endpoint Detection and Response Expert (on-premises) để áp dụng các thiết lập tích hợp EDR Expert (on-premises) cho các thiết bị được quản lý từ các cấu hình chính sách.

Để đặt lại thiết lập thành phần:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)**.
5. Thay đổi chế độ hoạt động từ **Endpoint Detection and Response Expert (version 7.1 or earlier)** sang **Endpoint Detection and Response Expert (từ phiên bản 8.0 trở lên)**.
6. Chuyển về **Endpoint Detection and Response Expert (version 7.1 or earlier)**.
7. Lưu các thay đổi của bạn.

Endpoint Detection and Response Expert (cloud)

Việc tích hợp Kaspersky Endpoint Security với Kaspersky Endpoint Detection and Response Expert (cloud) hiện tạm thời không khả dụng. Chức năng này dự kiến sẽ được hỗ trợ vào cuối năm 2026. Hãy theo dõi Ghi chú phát hành của chúng tôi để biết về các nâng cấp ứng dụng và tính năng mới.



Kaspersky Endpoint Security hỗ trợ tích hợp với các giải pháp Kaspersky Endpoint Detection and Response Expert (cloud). *Kaspersky Endpoint Detection and Response Expert (cloud)* là giải pháp bảo mật mạng doanh nghiệp sử dụng đám mây bao gồm các ứng dụng Kaspersky cho phép tổ chức phòng vệ trước hầu hết các loại rủi ro mạng và xử lý các tình huống phát tán mối đe dọa quan trọng nhất. Các thành phần EDR Expert (cloud) được triển khai trên Open Single Management Platform (OSMP). Nền tảng này chạy các kịch bản đa nền tảng trong một giao diện duy nhất và cho phép tích hợp các ứng dụng Kaspersky với ứng dụng của bên thứ ba thành một hệ thống bảo mật toàn diện.

Một trong những yếu tố cốt lõi của giải pháp là *SIEM*. SIEM theo dõi các sự kiện đến từ tất cả các thành phần và liên kết các sự kiện này với nhau bằng cách sử dụng các quy tắc do nhà cung cấp và người dùng định nghĩa. EDR Expert (cloud) xem xét nhật ký và dữ liệu đo từ xa nhận được từ cơ sở hạ tầng của doanh nghiệp để tự động phát hiện các cuộc tấn công và cho phép điều tra sự cố bằng cách sử dụng biểu đồ điều tra thống nhất, kết hợp tất cả các sự kiện được thu thập trong EDR Expert (cloud), bao gồm các sự kiện từ các ứng dụng Kaspersky và các sản phẩm bảo mật thông tin của bên thứ ba.

Để ứng phó với các sự cố phức tạp, EDR Expert (cloud) sử dụng các kịch bản được thiết lập sẵn và do người dùng định nghĩa. Bạn cũng có thể sử dụng hành động phản hồi từ ứng dụng của bên thứ ba và kịch bản phản hồi liên quan đến nhiều ứng dụng.

Các công cụ Threat Intelligence

Kaspersky Endpoint Detection and Response sử dụng các công cụ Threat Intelligence sau:

- Tích hợp với 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.
- 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.

Nguyên lý hoạt động của giải pháp

Kaspersky Endpoint Security 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 (dữ liệu đo lường từ xa) được gửi đến máy chủ EDR Expert (cloud). Trong trường hợp này, Kaspersky Endpoint Security cũng gửi thông tin về các mối đe dọa được phát hiện bởi ứng dụng, bao gồm cả thông tin về kết quả xử lý các mối đe dọa này đến các máy chủ thu tập từ xa.

Việc tích hợp EDR Expert (cloud) được cấu hình trong bảng điều khiển Kaspersky Security Center. Tác nhân tích hợp sau đó được quản lý bằng Open Single Management Platform (OSMP), bao gồm hoạt động chạy các tác vụ, quản lý các đối tượng được cách ly, xem báo cáo và các hành động khác.

Tích hợp tác nhân tích hợp với EDR Expert (cloud)

Để thiết lập tích hợp với giải pháp Kaspersky Endpoint Detection and Response (đám mây), bạn phải cài đặt thành phần Endpoint Detection and Response Expert (cloud) và cấu hình Kaspersky Endpoint Security.

Các thành phần Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud), và Endpoint Detection and Response Expert (on-premises) không tương thích với nhau.

Điều kiện hoạt động của EDR Expert (cloud)

Để EDR Expert (cloud) hoạt động, cần đáp ứng các điều kiện sau:

- Cơ sở hạ tầng Kaspersky Endpoint Detection and Response Expert (cloud) khả dụng tại khu vực của bạn. Để biết thông tin về việc cơ sở hạ tầng EDR Expert (cloud) có khả dụng tại khu vực của bạn hay không, vui lòng liên hệ Bộ phận Hỗ trợ kỹ thuật.
- OSMP (Open Single Management Platform) được cài đặt.
- Kaspersky Endpoint Security đã được cài đặt ở chế độ tiêu chuẩn.
- Ứng dụng Kaspersky Endpoint Security được kích hoạt và chức năng được giấy phép hỗ trợ.
- Bạn đã chấp nhận các điều khoản của Thỏa thuận Xử lý Dữ liệu Kaspersky Endpoint Detection and Response Expert (cloud).
- Thành phần Endpoint Detection and Response Expert (cloud) đang được bật.
- Các thành phần ứng dụng đảm bảo hoạt động của EDR Expert (cloud) được bật và hoạt động:
  - 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.

Các bước tích hợp với EDR Expert (cloud)

Thiết lập tích hợp EDR Expert (cloud) bao gồm các bước sau:

1. **Cài đặt thành phần Endpoint Detection and Response Expert (cloud)**

   Bạn có thể chọn thành phần Endpoint Detection and Response Expert (cloud) 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 thành phần mới.

2. **Kích hoạt Kaspersky Endpoint Detection and Response Expert (cloud)**

   Bạn cần mua một giấy phép riêng cho Kaspersky Endpoint Detection and Response Expert (cloud).

   Chức năng này sẽ khả dụng sau khi thêm một khóa riêng cho Kaspersky Endpoint Detection and Response Expert (cloud). Kết quả là hai khóa được thêm trên máy tính: một khóa dành cho Kaspersky Endpoint Security và một khóa dành cho Kaspersky Endpoint Detection and Response Expert (cloud).

   Việc cấp giấy phép cho chức năng Endpoint Detection and Response Expert (cloud) độc lập cũng giống như việc cấp giấy phép cho Kaspersky Endpoint Security.

   Đảm bảo rằng chức năng EDR Expert (cloud) được gộp trong giấy phép và đang chạy trong giao diện cục bộ của ứng dụng.

3. **Kết nối với máy chủ thu thập dữ liệu đo từ xa và máy chủ phản hồi**

   Kaspersky Endpoint Detection and Response Expert (cloud) yêu cầu kết nối tin cậy giữa Kaspersky Endpoint Security và hai máy chủ:

   - *Máy chủ thu thập đo từ xa* là một máy chủ thuộc giải pháp SIEM, có chức năng thu thập, chuẩn hóa, tương quan, phân tích và lưu trữ thông tin về các sự kiện xảy ra trên máy tính.
   - *Máy chủ phản hồi* là một máy chủ dùng để tiếp nhận và quét dữ liệu, nghiên cứu hành vi của các đối tượng và công bố kết quả của các nghiên cứu đó.

   Cách kết nối máy tính Kaspersky Endpoint Security với EDR Expert (cloud) bằng Bảng điều khiển web

   1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.
   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 **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (cloud)**.
   5. Kích hoạt thành phần bằng cách sử dụng công tắc bật/tắt **Endpoint Detection and Response Expert (cloud) DISABLED**.

6. Nếu chính sách hiện tại là chính sách con và chính sách cha không cho phép thay đổi cài đặt tích hợp EDR Expert (cloud) (biểu tượng "ổ khóa" đóng), bạn có thể cấu hình kế thừa cài đặt trong mục **Inheritance**:

   - **Inherit connection settings from the policy** (giá trị mặc định). Các thiết lập kết nối sẽ được kế thừa từ chính sách của chính sách cha. Bạn sẽ không thể chỉnh sửa các cài đặt.
   - **Use custom connection settings**. Bạn có thể cấu hình cài đặt kết nối thủ công.

7. Thẻ **Response server** hiển thị tên miền đầy đủ và cổng của máy chủ phản hồi, được tự động truy xuất. Nếu chính sách bảo mật trong cơ sở hạ tầng của bạn không cho phép kết nối trực tiếp tới các máy chủ EDR Expert (cloud), bạn có thể thiết lập kết nối thông qua đường hầm TCP:

   a. Chọn hộp kiểm **Use a TCP tunnel for response**.

   b. Nhập địa chỉ máy chủ (IPv4, IPv6) và cổng để kết nối với đường hầm.

8. Nếu cần, hãy đặt tần suất gửi yêu cầu đồng bộ tới máy chủ trong trường **Send sync request to server every (min)**. Trong quá trình đồng bộ, Kaspersky Endpoint Security nhận các tác vụ phản hồi mối đe dọa và gửi kết quả tác vụ.

9. Vào thẻ **Telemetry collection server**.

10. Cấu hình cài đặt kết nối của máy chủ thu thập dữ liệu đo từ xa:

    a. Nhấn vào liên kết **Edit**.

    b. Trong cửa sổ hiện ra, hãy chọn máy chủ thu thập dữ liệu đo từ xa trong danh sách. Bộ thu thập KUMA đóng vai trò là máy chủ thu thập dữ liệu đo lường từ xa trong EDR Expert (cloud). Để biết thêm chi tiết, vui lòng tham khảo Trợ giúp của Kaspersky Unified Monitoring and Analysis Platform.

    Nếu xảy ra lỗi trong quá trình kết nối với máy chủ thu thập dữ liệu đo từ xa, hãy chọn một máy chủ khác. Nếu bạn không thể kết nối với máy chủ thu thập dữ liệu đo lường từ xa, vui lòng liên hệ với Bộ phận Hỗ trợ kỹ thuật.

    c. Nếu cần, bạn có thể cấu hình kết nối đến máy chủ thu thập dữ liệu đo từ xa thông qua đường hầm TCP, như cách bạn làm với máy chủ phản hồi.

11. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Bạn có thể kiểm tra trạng thái thành phần bằng cách sử dụng*Report on status of application components*. 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 Expert (cloud)** sẽ được thêm vào danh sách các thành phần của Kaspersky Endpoint Security.

Cấu hình thiết lập dữ liệu đo lường từ xa của EDR Expert (cloud)

Dữ liệu *đo từ xa* là danh sách các sự kiện đã xảy ra trên máy tính được bảo vệ. Kaspersky Endpoint Security sẽ phân tích dữ liệu đo lường từ xa và gửi nó tới máy chủ thu thập đo từ xa trong quá trình đồng bộ. Các sự kiện đo từ xa sẽ đến máy chủ gần như liên tục. Kaspersky Endpoint Security khởi tạo đồng bộ với máy chủ khi bất kỳ điều kiện nào sau đây được thỏa mãn:

- Khoảng thời gian đồng bộ đã hết.
- Số sự kiện trong bộ đệm vượt quá giới hạn trên.

Do đó, theo mặc định, ứng dụng sẽ đồng bộ sau mỗi 30 giây hoặc bất cứ khi nào bộ đệm chứa 1024 sự kiện. Bạn có thể cấu hình hành vi đồng bộ trong chính sách Kaspersky Endpoint Security và chọn các giá trị tối ưu để phù hợp với lượng tải mạng của bạn (xem hướng dẫn bên dưới).

Nếu không có kết nối giữa Kaspersky Endpoint Security và máy chủ, ứng dụng sẽ đặt các sự kiện mới vào hàng chờ. Khi kết nối được khôi phục, Kaspersky Endpoint Security sẽ gửi các sự kiện trong hàng chờ tới máy chủ theo đúng thứ tự. Để máy chủ không bị quá tải, Kaspersky Endpoint Security có thể bỏ qua một số sự kiện. Để bật tính năng này, bạn có thể tối ưu hóa thiết lập truyền sự kiện, chẳng hạn như đặt giá trị số sự kiện mỗi giờ tối đa (xem hướng dẫn bên dưới).

Để cấu hình thiết lập đo từ xa, hãy thực hiện các bước sau:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management → Policies**.
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 **Built-in Agents Configuration → Endpoint Detection and Response Expert (cloud)**.
5. Trong cửa sổ mở ra, hãy chọn thẻ **Data transmission settings**.
6. Đảm bảo rằng hộp kiểm **Sending telemetry ENABLED** được chọn.
7. Nếu cần, hãy bật chức năng **Send telemetry with IOA only**. *Dấu hiệu tấn công (IOA)* là một quy tắc chứa mô tả về hành vi đáng ngờ trong hệ thống có thể cho biết một cuộc tấn công có chủ đích. Ứng dụng so sánh hành vi đang diễn ra trong hệ thống với các quy tắc này và ghi lại các sự kiện cho thấy có cuộc tấn công có chủ đích. Ứng dụng sử dụng công nghệ *quét luồng* cho phép theo dõi các sự kiện như vậy theo thời gian thực. Chức năng này bị tắt theo mặc định.
8. Nếu cần, hãy cấu hình cài đặt đồng bộ hóa máy chủ:
   - **Maximum event transmission delay (sec)**. Ứng dụng sẽ đồng bộ với máy chủ để gửi các sự kiện sau khi hết khoảng thời gian đồng bộ. Thiết lập mặc định là 30 giây.
   - **Maximum number of event packages**. Ứng dụng sẽ đồng bộ với máy chủ khi bộ đệm được lấp đầy bằng các sự kiện. Thiết lập mặc định là 1024 sự kiện.
9. Vào thẻ **Request throttling**.

10. Nếu cần, hãy tắt làm nghẽn yêu cầu bằng cách sử dụng nút bật/tắt **Request throttling ENABLED**.

    Tính năng này giúp tối ưu hóa mức tải trên máy chủ. Nếu chức năng này được kích hoạt, ứng dụng sẽ hạn chế việc truyền sự kiện. Nếu số lượng sự kiện vượt quá giới hạn được cấu hình thì Kaspersky Endpoint Security sẽ ngừng gửi sự kiện. Tùy chọn này được bật theo mặc định.

11. Cấu hình thiết lập tối ưu hóa để gửi sự kiện đến máy chủ:

    - **Maximum number of events per hour**. Ứng dụng sẽ phân tích luồng dữ liệu đo từ xa và hạn chế gửi sự kiện nếu luồng sự kiện vượt quá giới hạn số sự kiện mỗi giờ đã được cấu hình. Kaspersky Endpoint Security sẽ tiếp tục gửi sự kiện sau một giờ. Thiết lập mặc định là 3000 sự kiện mỗi giờ. Nếu ứng dụng được cài đặt trên máy chủ, luồng dữ liệu đo từ xa sẽ cao hơn. Đối với máy chủ, bạn nên tăng giá trị lên 60.000 sự kiện mỗi giờ.

    - **Percentage of event limit excess (%)**. Ứng dụng sẽ sắp xếp sự kiện theo loại (ví dụ: sự kiện "thay đổi trong registry") và hạn chế truyền gửi sự kiện nếu tỷ lệ sự kiện cùng loại trên tổng số sự kiện vượt quá hạn mức được cấu hình theo tỷ lệ. Kaspersky Endpoint Security sẽ tiếp tục gửi sự kiện khi tỷ lệ của các sự kiện khác trên tổng số sự kiện trở lại đủ lớn. Thiết lập mặc định là 15%.

12. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Loại trừ dữ liệu đo lường từ xa của EDR Expert (cloud)

Để nâng cao hiệu năng và tối ưu hóa việc truyền dữ liệu đến máy chủ thu thập dữ liệu đo lường từ xa, bạn có thể thêm loại trừ dữ liệu đo lường từ xa. Ví dụ: bạn có thể chọn không gửi dữ liệu giao tiếp mạng cho từng ứng dụng.

> Sử dụng quá nhiều quy tắc có thể làm tăng lượng tải cho máy chủ thu thập Đo từ xa và làm giảm hiệu năng của máy tính. Bạn chỉ nên thêm những quy tắc cần thiết.

Để tạo loại trừ dữ liệu đo lường 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 thẻ **Asset management** → **Policies**.

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** → **Telemetry Settings**.

5. Chọn thẻ **EDR Expert (cloud) telemetry**.

6. Trong mục **General exclusions**, hãy nhấn nút **Add**.

   Cửa sổ **Add exclusion rule** sẽ mở ra.

7. Nếu cần, hãy thay đổi trạng thái của quy tắc. Theo mặc định, quy tắc đã được bật.

8. Nhập tên cho quy tắc.

9. Chọn hành động sẽ được thực hiện khi quy tắc được kích hoạt:

   - **Do not collect**. Sự kiện đã được lọc sẽ bị loại trừ khỏi dữ liệu đo lường từ xa được gửi đi.
   - **Exclude IOA**. Sự kiện kích hoạt quy tắc IOA sẽ bị loại trừ khỏi dữ liệu đo lường từ xa được gửi đi.

10. Nếu chọn tùy chọn **Exclude IOA**, hãy chỉ định các quy tắc IOA sẽ được thêm vào danh sách loại trừ:

    - **Exclude all**. Khi điều kiện được chỉ định được đáp ứng, ứng dụng sẽ loại trừ các sự kiện được tạo dựa trên tất cả quy tắc IOA khỏi dữ liệu đo lường từ xa.
    - **Exclude by GUID**. Hãy chỉ định GUID của quy tắc IOA. Bạn có thể chỉ định nhiều GUID bằng cách sử dụng `,`. Để biết thêm chi tiết về quy tắc IOA, vui lòng tham khảo Trợ giúp của EDR Center (đám mây).

11. Hãy chỉ định điều kiện lọc:

    a. Chọn tên trường sẽ được dùng để lọc.

    b. Chọn một toán tử (xem bảng bên dưới) và chỉ định giá trị mà giá trị trường từ sự kiện sẽ được so sánh với.

Danh sách các toán tử điều kiện

Toán tử	Mô tả
<	Nếu giá trị của trường nhỏ hơn giá trị được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ.
≤	Nếu giá trị của trường nhỏ hơn hoặc bằng giá trị được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ.
=	Nếu giá trị của trường bằng với giá trị được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ.
≥	Nếu giá trị của trường lớn hơn hoặc bằng giá trị được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ.
>	Nếu giá trị của trường lớn hơn giá trị được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ.
≠	Nếu giá trị của trường không bằng giá trị được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ.
is like	Nếu giá trị trường khớp với tên đại diện được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ. Ứng dụng này hỗ trợ các ký tự `*` và `?` khi nhập tên đại diện:
is not like	Nếu giá trị trường không khớp với tên đại diện được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ. Ứng dụng này hỗ trợ các ký tự `*` và `?` khi nhập tên đại diện:
one of	Nếu giá trị của trường khớp với một trong các giá trị trong danh sách được chỉ định trong điều kiện, sự kiện đó được coi là đã được lọc.
none of	Nếu giá trị trường không khớp với bất kỳ giá trị nào trong danh sách được chỉ định trong điều kiện, sự kiện đó được coi là đã được lọc.
is like one of	Nếu giá trị trường khớp với một trong các tên đại diện được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ. Ứng dụng này hỗ trợ các ký tự * và ? khi nhập tên đại diện.
is not like one of	Nếu giá trị trường không khớp với bất kỳ tên đại diện nào được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ. Ứng dụng này hỗ trợ các ký tự * và ? khi nhập tên đại diện.
exists	Nếu trường được chỉ định trong điều kiện có trong sự kiện, sự kiện đó sẽ bị loại bỏ.
not exists	Nếu trường được chỉ định trong điều kiện không có trong sự kiện, sự kiện đó sẽ bị lọc bỏ.
contains	Nếu giá trị được chỉ định trong điều kiện có trong giá trị trường, sự kiện sẽ bị lọc bỏ.
is equal to	Nếu giá trị của trường bằng với giá trị được chỉ định trong điều kiện, sự kiện sẽ bị lọc bỏ. Quá trình quét không phân biệt chữ hoa chữ thường.
bitwise AND	Nếu kết quả của phép toán Bitwise AND (&) giữa giá trị trường và giá trị được chỉ định trong điều kiện là 1, sự kiện sẽ bị loại trừ.

12. Nếu cần, bạn có thể tạo các tiêu chí lọc phức tạp bằng cách thêm nhiều điều kiện và nhóm điều kiện. Bạn cũng có thể thêm điều kiện lồng nhau và nhóm điều kiện vào một nhóm điều kiện. Bạn có thể sử dụng các toán tử sau:

    - **AND** là bộ lọc sẽ chọn các sự kiện đáp ứng tất cả các điều kiện đã được chỉ định.
    - **OR** là bộ lọc sẽ chọn các sự kiện đáp ứng một trong các điều kiện đã được chỉ định.
    - **NOT** (để sử dụng toán tử này, hãy chọn tùy chọn **Add NOT before**) nghĩa là bộ lọc chọn các sự kiện không thỏa mãn bất kỳ điều kiện nào đã chỉ định.

    Các điều kiện và nhóm điều kiện cấp đầu tiên được kết hợp bằng toán tử **AND**.

13. Để quét quy tắc lọc bạn đã tạo, hãy nhấp vào nút **Check rule**.

    Trong cửa sổ mở ra, sẽ hiển thị bảng các sự kiện được lọc bởi quy tắc đã tạo. Để biết thêm chi tiết, vui lòng tham khảo Trợ giúp của EDR Expert (cloud).

14. Nếu cần, trong mục **All event types**, hãy thêm các ngoại lệ về đo từ xa theo loại sự kiện.

    a. Nhấp vào tên loại sự kiện.

    b. Trong cửa sổ mở ra, hãy nhấn nút **Set up manually**.

    c. Nếu cần, cấu hình việc truyền dữ liệu đo lường từ xa cho loại sự kiện đã chọn bằng công tắc bật/tắt **Send event**. Theo mặc định, việc truyền dữ liệu đo lường từ xa được bật cho tất cả các loại sự kiện.

    d. Trong mục **Exclusion rules**, hãy nhấn nút **Add**.

    Cửa sổ **Add exclusion rule** sẽ mở ra.

    e. Thực hiện các hành động được mô tả trong các bước từ 7–13 cho mỗi quy tắc bạn thêm.

15. Đối với một số loại sự kiện, bạn cũng có thể thêm quy tắc bao gồm để mở rộng dữ liệu đo lường từ xa được thu thập:

    a. Trong mục **Inclusion rules**, hãy nhấn nút **Add**.

    Cửa sổ **Add inclusion rules** sẽ mở ra.

    b. Nhập tên cho quy tắc.

    c. Trong **Condition**, nhập các giá trị cho các trường hiển thị. Loại trường khả dụng phụ thuộc vào sự kiện được chọn.

    > Các quy tắc loại trừ được ưu tiên hơn các quy tắc bao gồm.

16. Để áp dụng chính sách này cho máy tính, hãy đảm bảo rằng các ổ khóa đã được đóng (🔒) và lưu lại các thay đổi của bạn.

Các xuất và nhập bộ lọc sự kiện EDR Expert (cloud)

Bạn có thể xuất danh sách loại trừ ra tập tin JSON. Sau đó, bạn có thể sửa đổi tập tin, ví dụ như thêm một số lượng lớn các ID sự kiện. Bạn cũng có thể sử dụng chức năng xuất/nhập để sao lưu bộ lọc sự kiện hoặc để chuyển danh sách sang máy chủ khác.

Sử dụng quá nhiều quy tắc có thể làm tăng lượng tải cho máy chủ thu thập Đo từ xa và làm giảm hiệu năng của máy tính. Bạn chỉ nên thêm những quy tắc cần thiết.

Để xuất hoặc nhập bộ lọc sự kiện trong Bảng điều khiển web:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.
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** → **Telemetry Settings**.
5. Chọn thẻ **EDR Expert (cloud) telemetry**.
6. Để xuất bộ lọc sự kiện:
   a. Nhấn vào **Export**.
   b. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin JSON mà bạn muốn xuất bộ lọc sự kiện vào đó rồi chọn thư mục bạn muốn lưu tập tin này.
   c. Lưu tập tin.
      Kaspersky Endpoint Security sẽ xuất bộ lọc sự kiện vào tập tin JSON.
7. Để nhập bộ lọc sự kiện:
   a. Nhấn vào **Import**.
   b. Trong cửa sổ mở ra, hãy chọn tập tin JSON mà bạn muốn nhập bộ lọc sự kiện.
   c. Chọn cách bạn muốn nhập các quy tắc lọc sự kiện: bằng cách thêm vào các quy tắc hiện có hoặc bằng cách loại bỏ các quy tắc hiện có và thay thế bằng các quy tắc mới.
   d. Mở tập tin.
8. Để áp dụng chính sách này cho máy tính, hãy đảm bảo rằng các ổ khóa đã được đóng (🔒) và lưu lại các thay đổi của bạn.
   1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.
   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** → **Telemetry Settings**.

5. Chọn thẻ **EDR Expert (cloud) telemetry**.

6. Để xuất bộ lọc sự kiện:

   a. Nhấn vào **Export**.

   b. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin JSON mà bạn muốn xuất bộ lọc sự kiện vào đó rồi chọn thư mục bạn muốn lưu tập tin này.

   c. Lưu tập tin.

   Kaspersky Endpoint Security sẽ xuất bộ lọc sự kiện vào tập tin JSON.

7. Để nhập bộ lọc sự kiện:

   a. Nhấn vào **Import**.

   b. Trong cửa sổ mở ra, hãy chọn tập tin JSON mà bạn muốn nhập bộ lọc sự kiện.

   c. Chọn cách bạn muốn nhập các quy tắc lọc sự kiện: bằng cách thêm vào các quy tắc hiện có hoặc bằng cách loại bỏ các quy tắc hiện có và thay thế bằng các quy tắc mới.

   d. Mở tập tin.

8. Để áp dụng chính sách này cho máy tính, hãy đảm bảo rằng các ổ khóa đã được đóng (🔒) và lưu lại các thay đổi của bạn.

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 được tích hợp với các giải pháp của Kaspersky 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, Trợ giúp của Kaspersky Endpoint Detection and Response Expert, Trợ giúp của Kaspersky Anti Targeted Attack Platform và Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises).

Kaspersky Endpoint Security sử dụng tài khoản hệ thống (SYSTEM) để cách ly các tập tin.

Bạn chỉ có thể cấu hình các thiết lập cách ly trong Bảng điều khiển Kaspersky Security Center. Bạn cũng có thể sử dụng Bảng điều khiển Kaspersky Security Center 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 1024 MB. Khi Khu vực cách ly đạt đến kích thước tối đa, Kaspersky Endpoint Security sẽ ngừng gửi các tập tin và tạo sự kiện *Không đủ không gian trống trong ổ lưu trữ của Khu vực cách ly*. Để ngăn khu vực cách ly hết dung lượng ổ đĩa, bạn có thể đặt ngưỡng mà Kaspersky Endpoint Security tạo sự kiện *Ổ lưu trữ của Khu vực cách lý sắp hết không gian trống*. Bạn không thể cấu hình thời gian lưu giữ cho các tập tin bị cách ly để tự động xóa chúng.

Nếu giải pháp Kaspersky Anti Targeted Attack Platform (EDR) được triển khai trong tổ chức của bạn, chúng tôi khuyên bạn nên tăng dung lượng của Khu vực cách ly. Khi thực hiện quét YARA, ứng dụng có thể gặp phải tập tin kết xuất bộ nhớ lớn. Nếu kích thước của tập tin kết xuất bộ nhớ vượt quá kích thước của Khu vực cách ly thì tác vụ quét YARA sẽ kết thúc với lỗi và tập tin kết xuất bộ nhớ sẽ không được cách ly. Bạn nên đặt kích thước của Khu vực cách ly bằng tổng dung lượng của RAM trên máy tính (ví dụ: 8 GB) hoặc tắt giới hạn kích thước của Khu vực cách ly.

Cách cấu hình dung lượng tối đa của khu vực cách ly trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Các báo cáo và lưu trữ**.
4. 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**. Nếu hộp kiểm được chọn, kích thước tối đa của Khu vực cách ly sẽ bị giới hạn theo giá trị mặc định. Theo mặc định, kích cỡ tối đa là 1024 MB. Khi Khu vực cách ly đạt dung lượng tối đa, Kaspersky Endpoint Security sẽ gửi sự kiện *Không đủ không gian trống trong ổ lưu trữ của Khu vực cách ly* đến Kaspersky Security Center và phát 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.

     Nếu bỏ chọn hộp kiểm, kích thước của Khu vực cách ly sẽ bị giới hạn bởi dung lượng ổ đĩa trống có sẵn.

   - **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.

     Nếu bỏ chọn hộp kiểm này, ứng dụng sẽ không tạo sự kiện khi đạt đến ngưỡng của khu vực cách ly.

5. Lưu các thay đổi của bạn.

Cách cấu hình kích thước tối đa cho Khu vực cách ly trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Policies**.
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** → **Reports and Storage**.

5. Trong mục **Quarantine**, hãy cấu hình kích thước của Khu vực cách ly:

   - **Limit the size of Quarantine**. Nếu hộp kiểm được chọn, kích thước của Khu vực cách ly sẽ bị giới hạn theo giá trị mặc định. Nếu bỏ chọn hộp kiểm, kích thước của Khu vực cách ly sẽ bị giới hạn bởi dung lượng ổ đĩa trống có sẵn. Đây là điều có thể cần thiết cho quá trình quét YARA vì ứng dụng có thể lưu một tập tin kết xuất bộ nhớ lớn.

   - **Maximum size of Quarantine (MB)**. Nếu hộp kiểm được chọn, kích thước tối đa của Khu vực cách ly sẽ bị giới hạn theo giá trị mặc định. Theo mặc định, kích cỡ tối đa là 1024 MB. Khi Khu vực cách ly đạt dung lượng tối đa, Kaspersky Endpoint Security sẽ gửi sự kiện *Không đủ không gian trống trong ổ lưu trữ của Khu vực cách ly* đến Kaspersky Security Center và phát 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.

     Nếu bỏ chọn hộp kiểm, kích thước của Khu vực cách ly sẽ bị giới hạn bởi dung lượng ổ đĩa trống có sẵn.

   - **Notify when the Quarantine storage reaches (%)**. 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.

Cách bật chuyển dữ liệu tập tin được cách ly trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Các báo cáo và lưu trữ**.

4. Trong mục **Truyền dữ liệu đến Máy chủ quản trị**, hãy nhấn nút **Thiết lập**.

5. Trong cửa sổ mở ra, hãy chọn hộp kiểm **Các tập tin trong Khu vực cách ly**.

6. Lưu các thay đổi của bạn.

Cách bật chuyển dữ liệu tập tin được cách ly trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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** → **KSC Integration**.
5. Trong mục **Data transfer to Administration Server**, hãy chọn hộp kiểm **About Quarantine files**.
6. Lưu các thay đổi của bạn.

Do đó, bạn có thể xem danh sách các tập tin, được cách ly trên máy tính của mình, trong Bảng điều khiển Kaspersky Security Center. Bạn có thể sử dụng Bảng điều khiển Kaspersky Security Center để quản lý các đối tượng đã cách ly (khôi phục, xóa, thêm, v.v.). Để biết thêm chi tiết về thao tác với Khu vực cách ly, hãy tham khảo Trợ giúp của Kaspersky Security Center.

Khôi phục các tập tin từ Khu vực cách ly

Theo mặc định, Kaspersky Endpoint Security sẽ khôi phục các tập tin về thư mục gốc của chúng. Nếu thư mục đích đã bị xóa hoặc người dùng không có quyền truy cập vào thư mục đó, ứng dụng sẽ đặt tập tin vào thư mục `%DataRoot%\QB\Restored`. Sau đó bạn phải di chuyển tập tin vào thư mục đích theo cách thủ công.

Để khôi phục các tập tin từ Khu vực cách ly:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Operations** → **Repositories** → **Quarantine**.
2. Thao tác này sẽ mở danh sách các tập tin trong Khu vực cách ly; trong danh sách đó, hãy chọn các tập tin mà bạn muốn khôi phục và nhấn vào **Restore**.

   Kaspersky Endpoint Security sẽ khôi phục tập tin đó. Nếu thư mục đích đã có một tập tin có cùng tên, ứng dụng sẽ hủy khôi phục tập tin đó. Ứng dụng sẽ lưu một bản sao của tập tin vào Khu vực cách ly sau khi khôi phục tập tin. Để xóa tập tin, bạn phải xóa Khu vực cách ly theo cách thủ công.

Giám sát các hành động EDR

Kaspersky Endpoint Security cho Windows 12.9 ra mắt trung tâm giám sát hành động EDR. *Trung tâm giám sát hành động EDR* là bảng điều khiển, nơi bạn có thể xem lịch sử Phản hồi mối đe dọa cho tất cả các giải pháp Detection and Response của Kaspersky. Nếu tổ chức của bạn triển khai nhiều giải pháp Detection and Response (ví dụ: EDR Optimum và MDR), Kaspersky Endpoint Security sẽ hiển thị lịch sử Phản hồi mối đe dọa cho tất cả các giải pháp. Tính năng này cho phép bạn phân tích hiệu quả của các giải pháp Detection and Response trên một máy tính riêng biệt và tối ưu hóa cài đặt của các giải pháp này.

Trung tâm giám sát cung cấp những thông tin sau:

- Thông tin về các tác vụ Phản hồi mối đe dọa (ví dụ: tác vụ *Chấm dứt tiến trình*)
- Thay đổi quy tắc cô lập mạng và ngăn chặn thực thi

Nếu phản hồi mối đe dọa gặp phải lỗi liên quan đến quyền truy cập vào chia sẻ mạng, lỗi đó sẽ bị bỏ qua khỏi lịch sử Phản hồi mối đe dọa được hiển thị.

Để điều hướng đến trung tâm giám sát hành động EDR:

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Assets (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 14.2**.
   Việc này sẽ mở ra thiết lập cục bộ của ứng dụng.
5. Chọn thẻ **Application settings**.
6. Vào **Detection and Response** → **Response history**.

Thao tác này sẽ mở bảng điều khiển trung tâm giám sát hành động EDR. Bạn có thể sử dụng bảng điều khiển để xem trạng thái tác vụ Phản hồi mối đe dọa, thời lượng tác vụ, thay đổi quy tắc và thông tin chi tiết về người khởi tạo.

Kaspersky Unified Monitoring and Analysis Platform (KUMA)



Kaspersky Endpoint Security cho Windows hỗ trợ giải pháp Kaspersky Unified Monitoring and Analysis Platform. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* là giải pháp quản lý sự kiện và thông tin bảo mật (SIEM) dành cho hạ tầng CNTT của các tổ chức. KUMA cho phép phát hiện, phân tích và giảm thiểu các mối đe dọa bảo mật trước khi chúng có thể gây hại.

Kaspersky Endpoint Security 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 (đo từ xa) được gửi đến máy chủ Kaspersky Unified Monitoring and Analysis Platform (KUMA). Trong bảng điều khiển của mình, KUMA sẽ hiển thị các sự kiện dưới dạng danh sách không đánh dấu, tương tự như nhật ký sự kiện của Windows.

Kaspersky Endpoint Security không cung cấp đầy đủ chức năng của một tác nhân cho KUMA. Ứng dụng chỉ gửi sự kiện đến KUMA mà không đánh dấu. Để truy cập tất cả chức năng của KUMA, bạn cần mua giấy phép và triển khai giải pháp theo Hướng dẫn dành cho quản trị viên KUMA.

Tích hợp Kaspersky Endpoint Security với KUMA

Thiết lập tích hợp KES với KUMA bao gồm các bước sau:

1. Trong bảng điều khiển KUMA, hãy thêm một bộ thu thập.
2. Trong bảng điều khiển KUMA, hãy cấu hình một bộ kết nối cho bộ thu thập để nhận sự kiện từ KES.
3. Trong bảng điều khiển KUMA, hãy bật xác thực hai chiều (không bắt buộc).
4. Trong chính sách Kaspersky Endpoint Security cho Windows, hãy cấu hình các thiết lập để kết nối KES với KUMA.
5. Trong bảng điều khiển KUMA, hãy đảm bảo rằng các sự kiện từ KES được chuyển đến đúng khách thuê và được xử lý bởi các quy tắc tương quan chính xác.

Chuẩn bị cho tích hợp KES với KUMA

Để sử dụng KUMA, cần đáp ứng các điều kiện sau:

- Kaspersky Security Center phiên bản 14.2 trở lên. Không thể kích hoạt chức năng tích hợp KUMA trong các phiên bản trước của Kaspersky Security Center.
- Ứng dụng được kích hoạt và chức năng được giấy phép hỗ trợ.
- Thành phần tích hợp KUMA được bật.

Việc chuẩn bị cho quá trình tích hợp KES với KUMA bao gồm các bước sau:

1. **Cài đặt thành phần tích hợp KUMA**

   Bạn có thể chọn thành phần tích hợp KUMA khi cài đặt hoặc nâng cấp ứng dụng, 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 thành phần mới.

2. **Kích hoạt KUMA**

   Ngoài giấy phép ứng dụng Kaspersky Endpoint Security (ví dụ: Kaspersky Endpoint Security for Business Standard), bạn cần có giấy phép riêng để tích hợp Kaspersky Endpoint Security với KUMA (Phần bổ trợ tích hợp KUMA Kaspersky Endpoint Security cho Windows).

   Nếu bạn đang cài đặt ứng dụng ở chế độ EDR Agent, bạn cần có giấy phép tích hợp Kaspersky Endpoint Security với KUMA và giấy phép Kaspersky Anti Targeted Attack Platform (KATA) hoặc giấy phép Kaspersky Managed Detection and Response (MDR). Bạn không thể triển khai EDR Agent chỉ cho KUMA.

   Chức năng này sẽ khả dụng sau khi thêm khóa KUMA riêng. Do đó, sẽ có một khóa hiện hoạt khác trên máy tính để tích hợp Kaspersky Endpoint Security với KUMA.

   Việc cấp giấy phép cho chức năng KUMA độc lập cũng giống như việc cấp giấy phép cho Kaspersky Endpoint Security.

   Đảm bảo rằng chức năng KUMA được gộp trong giấy phép và đang hoạt động trong giao diện cục bộ của ứng dụng.

Kết nối KES với KUMA

Để kết nối máy tính có ứng dụng Kaspersky Endpoint Security với giải pháp KUMA:

1. Trong bảng điều khiển KUMA, hãy thêm bộ thu thập có bộ nối loại **tcp**, **udp** hoặc **http** và chỉ định thiết lập mạng cơ bản của kết nối. Để biết chi tiết về cách quản lý bộ thu thập, vui lòng tham khảo Trợ giúp của Kaspersky Unified Monitoring and Analysis Platform.

2. Trong chính sách của Kaspersky Endpoint Security, hãy thêm địa chỉ bộ thu thập KUMA và chỉ định thiết lập mạng của kết nối.

Cách kết nối máy tính Kaspersky Endpoint Security với KUMA bằng Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.

2. Trong cây bảng điều khiển, hãy chọn **Policies**.

3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

4. Trong cửa sổ chính sách, hãy chọn **Tích hợp KUMA**.

5. Chọn hộp kiểm **Tích hợp KUMA**.

6. Trong mục **Thiết lập tích hợp**, hãy chọn hộp kiểm **$IsKUMATelemetry ? "Cho phép truyền sự kiện của Windows đến máy chủ KUMA": "Cho phép truyền sự kiện của Windows đến máy chủ SIEM**.

7. Thêm máy chủ KUMA:

   a. Nhấn vào **Thêm**.

   Thao tác này sẽ mở biểu mẫu cho phép bạn thêm các máy chủ KUMA.

   b. Chọn giao thức để kết nối với máy chủ KUMA: **HTTP / HTTPS**, **TCP**, **UDP**.

   Giao thức kết nối với bộ thu thập trong Kaspersky Endpoint Security phải khớp với loại bộ kết nối trong KUMA: **http**, **tcp** hoặc **udp**.

   > Khi sử dụng giao thức UDP, dữ liệu có thể bị mất do hiện tượng suy giảm lưu lượng vốn có của giao thức này.

   c. Nhập địa chỉ máy chủ (IPv4, IPv6, FQDN) và cổng để kết nối với máy chủ (cổng 443 được chỉ định theo mặc định).

   Khi nhập địa chỉ máy chủ, hãy lưu ý những điều sau:

   - **TCP**:
     - **Không có TLS**. Bạn có thể chỉ định địa chỉ IP hoặc tên miền đầy đủ (FQDN) của máy chủ.
     - **Có TLS**. Bạn chỉ cần chỉ định tên miền đầy đủ (FQDN) của máy chủ.
   - **HTTP / HTTPS**:
     - **Không có TLS**. Bạn phải chỉ định rõ ràng giao thức HTTP trong địa chỉ máy chủ (ví dụ: `http://server.com` hoặc `http://10.10.10.100`).
     - **Có TLS**. Bạn không cần phải chỉ định giao thức (ví dụ: `https://server.com` hoặc `server.com`).
   - **UDP**. Giao thức UDP không hỗ trợ mã hóa TLS. Bạn có thể chỉ định địa chỉ IP hoặc tên miền đầy đủ (FQDN) của máy chủ.

   Bạn có thể xem địa chỉ máy chủ trong thuộc tính bộ kết nối trong bảng điều khiển KUMA. Để biết thêm thông tin về bộ kết nối KUMA, vui lòng xem Trợ giúp của Kaspersky Unified Monitoring and Analysis Platform.

   d. Nhấn vào **OK**.

Kaspersky Endpoint Security sẽ kết nối với máy chủ KUMA đầu tiên trong danh sách. Nếu kết nối không thành công, Kaspersky Endpoint Security sẽ kết nối với máy chủ KUMA thứ hai trong danh sách, v.v.

8. Nếu cần, hãy cấu hình thiết lập **Độ trễ truyền gửi sự kiện tối đa (giây)** trong mục **Thiết lập truyền dữ liệu**. Khi hết thời gian được chỉ định, Kaspersky Endpoint Security sẽ cố gắng kết nối với cùng một bộ thu thập hoặc kết nối với bộ thu thập tiếp theo trong danh sách, nếu có nhiều bộ thu thập. Thiết lập mặc định là 30 giây.

9. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách kết nối máy tính Kaspersky Endpoint Security với KUMA bằng Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.

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 **Built-in Agents Configuration** → **KUMA Integration**.

5. Bật nút bật/tắt **KUMA Integration ENABLED**.

6. Thêm máy chủ KUMA:

   a. Nhấn vào **Add**.

      Thao tác này sẽ mở biểu mẫu cho phép bạn thêm các máy chủ KUMA.

   b. Chọn giao thức để kết nối với máy chủ KUMA: **HTTP/HTTPS**, **TCP**, **UDP**.

      Giao thức kết nối với bộ thu thập trong Kaspersky Endpoint Security phải khớp với loại bộ kết nối trong KUMA: **http**, **tcp** hoặc **udp**.

      > Khi sử dụng giao thức UDP, dữ liệu có thể bị mất do hiện tượng suy giảm lưu lượng vốn có của giao thức này.

   c. Nhập địa chỉ máy chủ (IPv4, IPv6, FQDN) và cổng để kết nối với máy chủ (cổng 443 được chỉ định theo mặc định).

      Khi nhập địa chỉ máy chủ, hãy lưu ý những điều sau:

      - **TCP**:
        - **Không có TLS**. Bạn có thể chỉ định địa chỉ IP hoặc tên miền đầy đủ (FQDN) của máy chủ.
        - **Có TLS**. Bạn chỉ cần chỉ định tên miền đầy đủ (FQDN) của máy chủ.
      - **HTTP/HTTPS**:
        - **Không có TLS**. Bạn phải chỉ định rõ ràng giao thức HTTP trong địa chỉ máy chủ (ví dụ: `http://server.com` hoặc `http://10.10.10.100`).
        - **Có TLS**. Bạn không cần phải chỉ định giao thức (ví dụ: `https://server.com` hoặc `server.com`).
      - **UDP**. Giao thức UDP không hỗ trợ mã hóa TLS. Bạn có thể chỉ định địa chỉ IP hoặc tên miền đầy đủ (FQDN) của máy chủ.

Bạn có thể xem địa chỉ máy chủ trong thuộc tính bộ kết nối trong bảng điều khiển KUMA. Để biết thêm thông tin về bộ kết nối KUMA, vui lòng xem Trợ giúp của Kaspersky Unified Monitoring and Analysis Platform.

d. Nhấn vào **OK**.

Kaspersky Endpoint Security sẽ kết nối với máy chủ KUMA đầu tiên trong danh sách. Nếu kết nối không thành công, Kaspersky Endpoint Security sẽ kết nối với máy chủ KUMA thứ hai trong danh sách, v.v.

7. Nếu cần, hãy cấu hình thiết lập **Maximum delay when sending events (sec)** trong mục **Server connection settings**. Khi hết thời gian được chỉ định, Kaspersky Endpoint Security sẽ cố gắng kết nối với cùng một bộ thu thập hoặc kết nối với bộ thu thập tiếp theo trong danh sách, nếu có nhiều bộ thu thập. Thiết lập mặc định là 30 giây.

8. Lưu các thay đổi của bạn.

Bạn có thể xác minh rằng việc tích hợp KUMA được cấu hình đúng trong bảng điều khiển KUMA (để biết chi tiết, hãy xem Trợ giúp của Kaspersky Unified Monitoring and Analysis Platform). Kiểm tra trạng thái hoạt động của thành phần bằng cách xem *Report on status of application components* trong bảng điều khiển Kaspersky Security Center. 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 **Tích hợp KUMA** sẽ được thêm vào danh sách các thành phần của Kaspersky Endpoint Security.

Thiết lập một kết nối được tin tưởng giữa KES và KUMA

Bạn có thể thiết lập một kết nối được tin tưởng giữa Kaspersky Endpoint Security và bộ thu thập KUMA bằng bộ kết nối loại TCP hoặc HTTP. Không thể thiết lập kết nối được tin tưởng với bộ kết nối thuộc loại UDP.

Để thiết lập kết nối được tin tưởng, bạn cần cấu hình chế độ TLS trong phần thiết lập của bộ kết nối. Có thể sử dụng các chế độ TLS sau đây:

- **Disabled**: Không sử dụng mã hóa TLS. Tùy chọn này được chọn mặc định.
- **Enabled** Sử dụng mã hóa TLS, nhưng không cần xác minh chứng chỉ.
- **Custom PFX with client authentication** Sử dụng mã hóa TLS với khóa bí mật PFX. Ở chế độ này, máy khách được xác thực bằng chứng chỉ.

Kaspersky Endpoint Security không hỗ trợ chế độ **Custom PFX** TLS. Khi tích hợp KES với KUMA bằng PFX, xác thực người dùng bằng mật khẩu là điều bắt buộc.

Để thiết lập kết nối được tin tưởng, bạn cần chứng chỉ TLS - là *chứng chỉ CA cho dịch vụ vi mô*. Bạn có thể lấy chứng chỉ TLS trong bảng điều khiển KUMA. Để biết chi tiết về cách tải xuống chứng chỉ TLS, vui lòng tham khảo Trợ giúp của Kaspersky Unified Monitoring and Analysis Platform. Sau đó, bạn phải thêm chứng chỉ TLS vào Kaspersky Endpoint Security (xem hướng dẫn bên dưới).

Để cho kết nối bảo mật hơn, bạn có thể kích hoạt xác thực bổ sung cho máy tính trong KUMA (xác thực hai chiều). Để kích hoạt xác thực theo cách đó, bạn cần tạo một bộ chứa mã hóa trong cơ quan chứng nhận bên ngoài. Một *bộ chứa mã hóa* là tập tin nén PFX có chứng chỉ và khóa riêng ở định dạng PKCS#12. Tiếp theo, bạn cần bật xác thực hai chiều trong thiết lập KUMA (chế độ TLS **Custom PFX with client authentication**), bật xác thực hai chiều trong Kaspersky Endpoint Security và thêm tập tin nén PFX vào bảng điều khiển KUMA và Kaspersky Endpoint Security.

Cách cấu hình kết nối được tin tưởng giữa KES và KUMA trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Tích hợp KUMA**.
5. Chọn hộp kiểm **Tích hợp KUMA**.
6. Trong mục **Thiết lập để kết nối với máy chủ KUMA**, hãy chọn hộp kiểm **Sử dụng mã hóa TLS**.
7. Cấu hình kết nối tin tưởng:

   a. Nhấn vào **Thiết lập để kết nối với máy chủ KUMA**.

   b. Cấu hình kết nối máy chủ:

   - **Thời gian chờ (giây)**. Thời gian tối đa để chờ phản hồi từ máy chủ KUMA (mặc định là 5 giây). Khi hết thời gian chờ, Kaspersky Endpoint Security sẽ cố gắng kết nối với một máy chủ KUMA khác.
   - **Chứng chỉ TLS máy chủ**. Chứng chỉ TLS để thiết lập kết nối được tin tưởng với máy chủ KUMA. Bạn có thể lấy chứng chỉ TLS trong bảng điều khiển Kaspersky Unified Monitoring and Analysis Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Unified Monitoring and Analysis Platform).

     Để thiết lập kết nối được tin tưởng, bạn cần chọn chế độ TLS **Enabled** trong bảng điều khiển KUMA.
   - **Sử dụng xác thực hai chiều**. Xác thực hai chiều khi thiết lập kết nối bảo mật giữa KES và KUMA. Để sử dụng xác thực hai chiều, trong bảng điều khiển KUMA, trong thiết lập bộ nối, bạn phải chọn chế độ TLS **Custom PFX with client authentication** (xem thiết lập cho bộ nối trong phần Trợ giúp của Kaspersky Unified Monitoring and Analysis Platform). Sau đó, bạn phải tải xuống một chứng chỉ máy chủ và đặt mật khẩu để bảo vệ container mật mã.

     > Bộ chứa mã hóa phải được bảo vệ bằng mật khẩu. Không thể thêm bộ chứa mã hóa có mật khẩu trống.

   c. Nhấn vào **OK**.
8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách cấu hình kết nối được tin tưởng giữa KES và KUMA trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **KUMA Integration**.
5. Bật nút bật/tắt **KUMA Integration ENABLED**.
6. Trong mục **Server connection settings**, hãy bật nút gạt **Use TLS encryption**.
7. Cấu hình kết nối tin tưởng:
   a. Nhấn vào **Connection settings**.
   b. Cấu hình kết nối máy chủ:
   - **Timeout (sec)**. Thời gian tối đa để chờ phản hồi từ máy chủ KUMA (mặc định là 5 giây). Khi hết thời gian chờ, Kaspersky Endpoint Security sẽ cố gắng kết nối với một máy chủ KUMA khác.
   - **Server TLS certificate**. Chứng chỉ TLS để thiết lập kết nối được tin tưởng với máy chủ KUMA. Bạn có thể lấy chứng chỉ TLS trong bảng điều khiển Kaspersky Unifield Monitoring and Analysis Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Unified Monitoring and Analysis Platform).
     Để thiết lập kết nối được tin tưởng, bạn cần chọn chế độ TLS **Enabled** trong bảng điều khiển KUMA.
   - **Use two-way authentication**. Xác thực hai chiều khi thiết lập kết nối bảo mật giữa KES và KUMA. Để sử dụng xác thực hai chiều, trong bảng điều khiển KUMA, trong thiết lập bộ nối, bạn phải chọn chế độ TLS **Custom PFX with client authentication** (xem thiết lập cho bộ nối trong phần Trợ giúp của Kaspersky Unified Monitoring and Analysis Platform). Sau đó, bạn phải tải xuống một chứng chỉ máy chủ và đặt mật khẩu để bảo vệ container mật mã.

     > Bộ chứa mã hóa phải được bảo vệ bằng mật khẩu. Không thể thêm bộ chứa mã hóa có mật khẩu trống.

   c. Nhấn vào **OK**.
8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cho phép gửi dữ liệu đo từ xa đến máy chủ KUMA

Theo mặc định, việc gửi sự kiện đến máy chủ KUMA bị vô hiệu hóa. Để đảm bảo KUMA hoạt động đúng, bạn phải bật tính năng gửi dữ liệu đo từ xa. Bạn có thể chọn một nguồn sự kiện trong số các nhật ký tiêu chuẩn: *Application*, *Security* hoặc *System*.

Cách cho phép gửi dữ liệu đo từ xa đến KUMA trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Loại trừ và loại đối tượng**.
5. Trong mục **Thiết lập đo lường từ xa → Đo lường từ xa KUMA**, hãy nhấn nút **Thiết lập**.
6. Chọn nhật ký sự kiện mà bạn muốn sử dụng làm nguồn sự kiện: *Application*, *Security* hoặc *System*. Ngoài các nhật ký tiêu chuẩn, bạn có thể chỉ định nhật ký của ứng dụng bên thứ ba.
7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách cho phép gửi dữ liệu từ xa đến KUMA trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management → Policies**.
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 → Telemetry Settings**.
5. Chọn thẻ **KUMA telemetry**.
6. Chọn nhật ký sự kiện mà bạn muốn sử dụng làm nguồn sự kiện: *Application*, *Security* hoặc *System*. Ngoài các nhật ký tiêu chuẩn, bạn có thể chỉ định nhật ký của ứng dụng bên thứ ba.
7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Lọc các sự kiện được gửi đến KUMA

Theo mặc định, việc gửi sự kiện đến máy chủ KUMA bị vô hiệu hóa. Để đảm bảo KUMA hoạt động đúng, bạn phải bật tính năng gửi dữ liệu đo từ xa. Bạn có thể chọn một nguồn sự kiện trong số các nhật ký tiêu chuẩn: *Application*, *Security* hoặc *System*. Để nâng cao hiệu năng và tối ưu hóa việc truyền dữ liệu đến máy chủ KUMA, bạn có thể thêm hoặc loại trừ thủ công từng sự kiện khỏi dữ liệu đo từ xa. Ví dụ: bạn có thể loại trừ các sự kiện Sysmon.

Cách tạo danh sách sự kiện sẽ được gửi đến KUMA trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Loại trừ và loại đối tượng**.

5. Trong mục **Thiết lập đo lường từ xa → Đo lường từ xa KUMA**, hãy nhấn nút **Thiết lập**.

6. Trong cửa sổ được hiển thị, hãy cấu hình bộ lọc sự kiện sẽ được gửi đến KUMA.

   Bạn có thể cấu hình lọc sự kiện cho nhật k *Application*, *Security*, *System* tiêu chuẩn hoặc thêm nhật ký khác theo cách thủ công:

   a. Mở thuộc tính nhật ký hoặc nhấp vào nút **Thêm** và nhập tên nhật ký.

   b. Chọn chế độ gửi sự kiện:

   - **Gửi tất cả các sự kiện**. Ở chế độ này, ứng dụng sẽ gửi tất cả các sự kiện từ nhật ký Windows, ngoại trừ các sự kiện được thêm vào quy tắc loại trừ.
   - **Chỉ gửi các sự kiện được chọn**. Ở chế độ này, ứng dụng chỉ gửi các sự kiện được thêm vào các quy tắc bao gồm.

   c. Tạo danh sách quy tắc loại trừ hoặc quy tắc bao gồm cho chế độ gửi sự kiện liên quan.

   Để thêm quy tắc, bạn cần chỉ định ID của sự kiện trong nhật ký sự kiện Windows. Bạn có thể liệt kê nhiều ID sự kiện trong một quy tắc. Để chỉ định nhiều ID sự kiện, hãy sử dụng ký tự dấu phẩy (,).

   d. Nếu cần, hãy bật tính năng ghi nhật ký sự kiện bằng cách chọn hộp kiểm bên cạnh tên nhật ký.

7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách tạo danh sách các sự kiện sẽ được gửi đến KUMA trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management → Policies**.

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 → Telemetry Settings**.

5. Chọn thẻ **KUMA telemetry**.

6. Trong cửa sổ được hiển thị, hãy cấu hình bộ lọc sự kiện sẽ được gửi đến KUMA.

   Bạn có thể cấu hình lọc sự kiện cho nhật k *Application*, *Security*, *System* tiêu chuẩn hoặc thêm nhật ký khác theo cách thủ công:

   a. Mở thuộc tính nhật ký hoặc nhấp vào nút **Add** và nhập tên nhật ký.

   b. Chọn chế độ gửi sự kiện:

   - **Send all events**. Ở chế độ này, ứng dụng sẽ gửi tất cả các sự kiện từ nhật ký Windows, ngoại trừ các sự kiện được thêm vào quy tắc loại trừ.
   - **Send only selected events**. Ở chế độ này, ứng dụng chỉ gửi các sự kiện được thêm vào các quy tắc bao gồm.

c. Tạo danh sách quy tắc loại trừ hoặc quy tắc bao gồm cho chế độ gửi sự kiện liên quan.

Để thêm quy tắc, bạn cần chỉ định ID của sự kiện trong nhật ký sự kiện Windows. Bạn có thể liệt kê nhiều ID sự kiện trong một quy tắc. Để chỉ định nhiều ID sự kiện, hãy sử dụng ký tự dấu phẩy (`,`).

d. Nếu cần, hãy bật tính năng ghi nhật ký sự kiện bằng cách sử dụng công tắc bật/tắt bên cạnh tên nhật ký.

7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Xuất và nhập bộ lọc sự kiện KUMA

Bạn có thể xuất danh sách loại trừ ra tập tin JSON. Sau đó, bạn có thể sửa đổi tập tin, ví dụ như thêm một số lượng lớn các ID sự kiện. Bạn cũng có thể sử dụng chức năng xuất/nhập để sao lưu bộ lọc sự kiện hoặc để chuyển danh sách sang máy chủ khác.

Sử dụng quá nhiều quy tắc có thể làm tăng lượng tải cho máy chủ KUMA và làm giảm hiệu năng của máy tính. Bạn chỉ nên thêm những quy tắc cần thiết.

Cách xuất và nhập bộ lọc sự kiện trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Loại trừ và loại đối tượng**.
5. Trong mục **Thiết lập đo lường từ xa → Đo lường từ xa KUMA**, hãy nhấn nút **Thiết lập**.
6. Để xuất bộ lọc sự kiện:

a. Chọn nhật ký sự kiện có bộ lọc mà bạn muốn xuất.

b. Nhấn nút → **Xuất**.

c. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin JSON mà bạn muốn xuất bộ lọc sự kiện vào đó rồi chọn thư mục bạn muốn lưu tập tin này.

d. Lưu tập tin.

Kaspersky Endpoint Security sẽ xuất bộ lọc sự kiện vào tập tin JSON.

7. Để nhập bộ lọc sự kiện:

a. Nhấn nút → **Nhập**.

b. Trong cửa sổ mở ra, hãy chọn tập tin JSON mà bạn muốn nhập bộ lọc sự kiện.

c. Mở tập tin.

Nếu các quy tắc lọc sự kiện đã tồn tại trên máy tính, Kaspersky Endpoint Security sẽ thay thế các quy tắc này khi nhập.

8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách xuất và nhập bộ lọc sự kiện trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn thẻ **Asset management** → **Policies**.
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** → **Telemetry Settings**.
5. Chọn thẻ **KUMA telemetry**.
6. Để xuất bộ lọc sự kiện:

   a. Chọn nhật ký sự kiện có bộ lọc mà bạn muốn xuất.

   b. Nhấn nút → **Export**.

   c. Trong cửa sổ mở ra, hãy chỉ định tên của tập tin JSON mà bạn muốn xuất bộ lọc sự kiện vào đó rồi chọn thư mục bạn muốn lưu tập tin này.

   d. Lưu tập tin.

   Kaspersky Endpoint Security sẽ xuất bộ lọc sự kiện vào tập tin JSON.
7. Để nhập bộ lọc sự kiện:

   a. Nhấn nút → **Import**.

   b. Trong cửa sổ mở ra, hãy chọn tập tin JSON mà bạn muốn nhập bộ lọc sự kiện.

   c. Mở tập tin.

   Nếu các quy tắc lọc sự kiện đã tồn tại trên máy tính, Kaspersky Endpoint Security sẽ thay thế các quy tắc này khi nhập.
8. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Bạn cũng có thể xuất hoặc nhập bộ lọc sự kiện trên dòng lệnh.

Hướng dẫn chuyển từ KSWS sang KES

Kể từ phiên bản 11.8.0, Kaspersky Endpoint Security cho Windows hỗ trợ chức năng cơ bản của giải pháp Kaspersky Security for Windows Server (KSWS). *Kaspersky Security for 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 hoạt động của giải pháp này, vui lòng tham khảo Trợ giúp của Kaspersky Security for Windows Server. Kể từ Kaspersky Endpoint Security 11.8.0, bạn có thể chuyển từ Kaspersky Security for Windows Server sang Kaspersky Endpoint Security cho Windows và sử dụng cùng một giải pháp để bảo vệ máy trạm và máy chủ.

Yêu cầu về phần mềm

Trước khi bạn bắt đầu chuyển từ KSWS sang KES, hãy đảm bảo rằng máy chủ của bạn đáp ứng các yêu cầu về phần cứng và phần mềm của Kaspersky Endpoint Security cho Windows. Danh sách các phiên bản hệ điều hành được hỗ trợ sẽ khác nhau đối với KES và KSWS. Ví dụ: KES không hỗ trợ máy chủ chạy Windows Server 2003.

Yêu cầu về phần mềm tối thiểu để chuyển từ KSWS sang KES:

- Kaspersky Endpoint Security cho Windows 12.0.
- Kaspersky Security 11.0.1 for Windows Server.

  Nếu bạn đã cài đặt phiên bản cũ hơn của Kaspersky Security for Windows Server thì bạn nên nâng cấp ứng dụng lên phiên bản mới nhất. Trình hướng dẫn chuyển đổi chính sách và tác vụ không hỗ trợ các phiên bản cũ hơn của Kaspersky Security for Windows Server.
- Kaspersky Security Center 14.2

  Nếu bạn đã cài đặt phiên bản cũ hơn của Kaspersky Security Center, hãy cập nhật đó lên phiên bản 14.2 trở lên. Trong phiên bản Kaspersky Security Center này, Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ cho phép bạn chuyển các chính sách vào một cấu hình thay vì vào một chính sách. Trong phiên bản Kaspersky Security Center này, Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ cũng cho phép bạn chuyển một dải thiết lập chính sách rộng hơn.
- Kaspersky Endpoint Agent 3.10.

  Nếu bạn đã cài đặt phiên bản cũ hơn của Kaspersky Endpoint Agent thì bạn nên nâng cấp ứng dụng lên phiên bản mới nhất. Kaspersky Endpoint Security hỗ trợ chuyển cấu hình [KSWS+KEA] sang [KES+tác nhân tích hợp] kể từ Kaspersky Endpoint Agent 3.10.

Các khuyến nghị di chuyển

Khi di chuyển từ KSWS sang KES, hãy tuân thủ các khuyến nghị sau:

- Lên lịch chuyển từ KSWS sang KES từ trước. Chọn thời điểm khi các máy chủ đang hoạt động ở mức tải nhẹ nhất, như vào cuối tuần.
- Sau khi chuyển, hãy bật dần các thành phần ứng dụng. Ví dụ: bắt đầu bằng cách bật riêng thành phần Bảo vệ mối đe dọa tập tin, sau đó bật các thành phần bảo vệ khác, sau đó bật các thành phần kiểm soát, v.v. Ở mỗi bước, bạn phải đảm bảo ứng dụng hoạt động đúng và theo dõi hiệu năng của máy chủ. Kiến trúc của KES khác với KSWS, do đó hệ điều hành cũng có thể hoạt động khác.
- Tiến hành chuyển dần. Đầu tiên chuyển một máy chủ, sau đó là nhiều máy chủ, sau đó thực hiện chuyển trên tất cả các máy chủ của tổ chức.
- Chuyển các loại máy chủ khác nhau riêng rẽ. Ví dụ: đầu tiên hãy chuyển máy chủ cơ sở dữ liệu, sau đó là máy chủ thư, v.v.
- Chuyển trên các máy chủ có mức tải cao liên quan đến một số điều cần cân nhắc đặc biệt.

Các bước chuyển

Quá trình chuyển từ KSWS sang KES được thực hiện bán tự động. Đây là điều cần thiết vì các kiến trúc khác nhau của các ứng dụng. Để chuyển thiết lập chính sách, bạn phải chạy Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ (trình hướng dẫn chuyển đổi). Sau khi chuyển các thiết lập chính sách, bạn phải cấu hình các thiết lập theo cách thủ công mà trình hướng dẫn chuyển đổi không thể tự động chuyển (ví dụ: Thiết lập bảo vệ bằng mật khẩu). Sau khi chuyển, bạn cũng nên kiểm tra xem trình hướng dẫn chuyển đổi có chuyển đúng tất cả các thiết lập hay không.

Chuyển từ KSWS sang KES theo thứ tự sau:

1. **Chuyển các tác vụ và chính sách của KSWS**

   Sau khi chuyển các chính sách và tác vụ, bạn phải thực hiện các bước cấu hình bổ sung. Bạn cũng nên đảm bảo rằng Kaspersky Endpoint Security cung cấp mức độ bảo mật cần thiết sau khi chuyển từ KSWS.

   > Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ cho Kaspersky Security for Windows Server chỉ khả dụng trong Bảng điều khiển quản trị (MMC). Không thể di chuyển thiết lập chính sách và tác vụ trong Bảng điều khiển web và Bảng điều khiển đám mây của Kaspersky Security Center.

2. **Cài đặt Kaspersky Endpoint Security**

Bạn có thể cài đặt Kaspersky Endpoint Security theo các cách sau:

- Cài đặt KES sau khi gỡ bỏ KSWS (khuyên dùng).

  > Tiện ích kavremover không hỗ trợ quản lý KSWS.

- Cài đặt KES trên KSWS.

3. **Kích hoạt KES bằng khóa KSWS**

4. **Xác nhận rằng ứng dụng đang hoạt động tốt sau khi chuyển**

   Sau khi chuyển từ KSWS sang KES, hãy đảm bảo rằng ứng dụng đang hoạt động đúng. Kiểm tra trạng thái của máy chủ trong bảng điều khiển (nên có trạng thái *OK*). Đảm bảo không có lỗi nào được báo cáo cho ứng dụng, đồng thời kiểm tra thời gian kết nối lần cuối với Máy chủ quản trị, thời điểm cập nhật cơ sở dữ liệu lần cuối và trạng thái bảo vệ máy chủ.

   > Đặc biệt chú ý đến việc chuyển danh sách loại trừ, ứng dụng được tin tưởng, địa chỉ web được tin tưởng, quy tắc Kiểm soát ứng dụng.

Sự tương hợp của thành phần của KSWS và KES

Khi chuyển từ KSWS sang KES, nhóm thành phần chỉ được chuyển khi ứng dụng đang được cài đặt cục bộ.

Sự tương hợp của các thành phần Kaspersky Security for Windows Server và Kaspersky Endpoint Security cho Windows

Thành phần của Kaspersky Security for Windows Server	Thành phần của Kaspersky Endpoint Security cho Windows
Basic functionality	Nhân ứng dụng
Log Inspection	Kiểm tra nhật ký
Device Control	Kiểm soát thiết bị
Firewall Management	*(không được hỗ trợ)* Các chức năng của Tường lửa KSWS được thực hiện bởi Tường lửa cấp hệ thống. Trong KES, một thành phần riêng biệt chịu trách nhiệm cho chức năng Tường lửa. Sau khi chuyển đổi, bạn có thể cấu hình Tường lửa của Kaspersky Endpoint Security.
File Integrity Monitor	Giám sát tính toàn vẹn của hệ thống
Exploit Prevention	Phòng chống khai thác
System Tray Icon	*(không được hỗ trợ)* Bạn có thể cấu hình tương tác của người dùng trong thiết lập giao diện ứng dụng.
Integration with Kaspersky Security Center	Network Agent Connector
Endpoint Agent	*(không được hỗ trợ)* 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.
Network Threat Protection	Bảo vệ mối đe dọa mạng
Anti-Cryptor	Phát hiện hành vi
Anti-Cryptor for NetApp	*(không được hỗ trợ)*

Thành phần của Kaspersky Security for Windows Server	Thành phần của Kaspersky Endpoint Security cho Windows
Traffic Security	Bảo vệ mối đe dọa web Bảo vệ mối đe dọa thư điện tử Kiểm soát Web
On-Demand Scan	Nhân ứng dụng
ICAP Network Storage Protection	*(không được hỗ trợ)* Kaspersky Endpoint Security không hỗ trợ các thành phần Bảo vệ ổ lưu trữ nối mạng. Nếu cần những thành phần này, bạn có thể tiếp tục sử dụng Kaspersky Security for Windows Server.
RPC Network Storage Protection	*(không được hỗ trợ)* Kaspersky Endpoint Security không hỗ trợ các thành phần Bảo vệ ổ lưu trữ nối mạng. Nếu cần những thành phần này, bạn có thể tiếp tục sử dụng Kaspersky Security for Windows Server.
Real-Time File Protection	Bảo vệ mối đe dọa tập tin
Script Monitoring	*(không được hỗ trợ)* Giám sát tập lệnh được xử lý bởi các thành phần khác, ví dụ như Bảo vệ AMSI.
KSN Usage	Kaspersky Security Network
Applications Launch Control	Kiểm soát ứng dụng
Performance counters	*(không được hỗ trợ)*

Sự tương hợp của thiết lập KSWS và KES

Khi chuyển đổi các chính sách và tác vụ, KES sẽ được cấu hình theo thiết lập của KSWS. Thiết lập của các thành phần ứng dụng mà KSWS không có sẽ được đặt thành giá trị mặc định.

Application settings

Scalability, interface and scanning settings

Thiết lập ứng dụng không được hỗ trợ trong Kaspersky Endpoint Security cho Windows.

Thiết lập ứng dụng

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Scalability settings	*(không chuyển)* Kaspersky Endpoint Security sẽ quản lý tất cả các quy trình làm việc.
Show System Tray Icon	*(không chuyển)* 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 theo mặc định. 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. Bạn có thể cấu hình tương tác của người dùng trong thiết lập giao diện ứng dụng.
Restore file attributes after scanning	*(không chuyển)* Kaspersky Endpoint Security sẽ tự động khôi phục các thuộc tính tập tin sau khi quét tập tin.
Limit CPU usage for scanning threads	*(không chuyển)* Kaspersky Endpoint Security sẽ không giới hạn mức sử dụng CPU khi quét. Bạn có thể cấu hình tác vụ để chạy khi máy tính đang hoạt động dưới mức tải tối thiểu.

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Folder for temporary files created during scanning	*(không chuyển)* Kaspersky Endpoint Security sẽ đặt các tập tin tạm thời vào thư mục `C:\Windows\Temp`.
HSM system settings	*(không chuyển)* Kaspersky Endpoint Security sẽ không hỗ trợ các hệ thống HSM.

Security and reliability

Thiết lập bảo mật KSWS được chuyển sang mục **Thiết lập tổng quát**, **Thiết lập ứng dụng** và các tiểu mục của **Giao diện**.

Thiết lập bảo mật ứng dụng

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Protect application processes from external threats	**Bật Tự bảo vệ** (tiểu mục **Thiết lập ứng dụng**)
Apply password protection	*(không chuyển)* Kaspersky Endpoint Security có tính năng Bảo vệ bằng mật khẩu tích hợp (mục con **Giao diện**).
Perform task recovery	*(không chuyển)* Kaspersky Endpoint Security chỉ tự động khôi phục các tác vụ *Quét phần mềm độc hại*. Kaspersky Endpoint Security sẽ chạy các tác vụ khác theo lịch.
Do not start scheduled scan tasks	**Hoãn các tác vụ theo lịch trong khi đang sử dụng nguồn pin** (tiểu mục **Thiết lập ứng dụng**)
Stop current scan tasks	*(không chuyển)* Khi máy tính được cấp nguồn bởi thiết bị UPS, Kaspersky Endpoint Security sẽ không dừng các tác vụ quét đang chạy.

Connection settings

Thiết lập tương tác của Máy chủ quản trị được chuyển sang mục **Thiết lập tổng quát**, **Thiết lập mạng** và các tiểu mục **Thiết lập ứng dụng**.

Thiết lập tương tác Máy chủ quản trị

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Proxy server settings	**Thiết lập máy chủ Proxy** (tiểu mục **Thiết lập mạng**)
Do not use proxy server for local addresses	**Bỏ qua máy chủ proxy đối với các địa chỉ cục bộ** (tiểu mục **Thiết lập mạng**)
Proxy server authentication settings	**Sử dụng chứng thực máy chủ proxy** (tiểu mục **Thiết lập mạng**) Mật khẩu xác thực máy chủ proxy không được chuyển sang. Sau khi chuyển một chính sách, mật khẩu phải được nhập theo cách thủ công.
Use Kaspersky Security Center as a proxy server when activating the application	**Sử dụng Kaspersky Security Center như máy chủ proxy để kích hoạt** (tiểu mục **Thiết lập ứng dụng**)

Run local system tasks

Kaspersky Endpoint Security sẽ bỏ qua các thiết lập để chạy các tác vụ hệ thống cục bộ của Kaspersky Security for Windows Server. Bạn có thể cấu hình việc sử dụng các tác vụ KES cục bộ trong **Tác vụ cục bộ**, **Quản lý tác vụ**. Bạn cũng có thể cấu hình lịch để chạy tác vụ *Quét phần mềm độc hại* và *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* trong thuộc tính của các tác vụ này.

Supplementary

Trusted zone

Thiết lập khu vực tin tưởng của KSWS được chuyển sang mục **Thiết lập tổng quát**, mục con **Loại trừ**.

Thiết lập khu vực tin tưởng

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Object to scan (Exclusions)	**Loại trừ quét** (Loại trừ quét) Các phương thức được KSWS và KES sử dụng để chọn đối tượng sẽ khác nhau. Khi chuyển đổi, KES sẽ hỗ trợ các loại trừ được xác định là các tập tin riêng lẻ hoặc đường dẫn đến tập tin / thư mục. Nếu KSWS có các loại trừ được cấu hình làm khu vực định trước hoặc một tập lệnh URL, thì các loại trừ đó sẽ không được chuyển đổi. Sau khi chuyển đổi, bạn phải thêm các loại trừ đó theo cách thủ công. Các loại trừ dưới dạng khu vực được định trước phải được định cấu hình trong tác vụ *Quét phần mềm độc hại*. Các loại trừ dưới dạng địa chỉ web tập lệnh phải được thêm vào các địa chỉ web được tin tưởng cho Bảo vệ mối đe dọa web.
Apply also to subfolders (Exclusions)	**Bao gồm các thư mục con** (Loại trừ quét)
Objects to detect (Exclusions)	**Loại đối tượng được phát hiện** (Loại trừ quét)
Exclusion usage scope (Exclusions)	**Thành phần bảo vệ** (Loại trừ quét) Nếu ít nhất một thành phần được chọn trong KSWS thì KES sẽ áp dụng các loại trừ cho tất cả các thành phần ứng dụng.
Comment (Exclusions)	**Bình luận** (Loại trừ quét)
Trusted process (Trusted process)	**Ứng dụng được tin tưởng** Phương thức lựa chọn tiến trình / ứng dụng được tin tưởng sẽ khác nhau trong KSWS và KES. Khi chuyển sang, KES sẽ hỗ trợ các ứng dụng tin tưởng được cấu hình làm đường dẫn đến tập tin thực thi hoặc tên đại diện. Nếu KSWS có các tiến trình tin tưởng được cấu hình như hash tập tin thì các tiến trình tin tưởng đó sẽ không được chuyển đổi. Sau khi chuyển đổi, bạn phải thêm các tiến trình tin tưởng như vậy theo cách thủ công.
Do not check file backup operations (Trusted process)	**Không giám sát hoạt động ứng dụng** (Ứng dụng được tin tưởng)

Removable drives scan

Thiết lập Quét ổ đĩa di động được chuyển sang mục **Tác vụ cục bộ**, tiểu mục **Quét ổ đĩa di động**.

Thiết lập quét ổ đĩa di động

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Scan removable drives on connection via USB	**Hành động khi kết nối ổ đĩa di động**
Scan removable drives if its stored data volume does not exceed (MB)	**Dung lượng tối đa của ổ đĩa di động**

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Scan with security level: • **Maximum protection** • **Recommended** • **Maximum performance**	**Hành động khi kết nối ổ đĩa di động**: • **Bảo vệ tối đa**. • **Khuyên dùng**. Mức độ bảo mật của KSWS tương ứng với các chế độ quét KES như sau: • Maximum protection – Bảo vệ tối đa • Recommended – Khuyên dùng • Maximum performance – Khuyên dùng

User permissions for application management

Kaspersky Endpoint Security không hỗ trợ gán quyền truy cập của người dùng để quản lý ứng dụng và quản lý dịch vụ ứng dụng. Bạn có thể cấu hình thiết lập truy cập cho người dùng và nhóm người dùng để quản lý ứng dụng trong Kaspersky Security Center.

User access permissions for Kaspersky Security Service management

Kaspersky Endpoint Security không hỗ trợ gán quyền truy cập của người dùng để quản lý ứng dụng và quản lý dịch vụ ứng dụng. Bạn có thể cấu hình thiết lập truy cập cho người dùng và nhóm người dùng để quản lý ứng dụng trong Kaspersky Security Center.

Storages

Thiết lập kho lưu trữ KSWS được chuyển sang mục **Thiết lập tổng quát**, tiểu mục **Các báo cáo và lưu trữ** và sang mục **Bảo vệ mối đe dọa thiết yếu**, tiểu mục **Bảo vệ mối đe dọa mạng**.

Thiết lập kho lưu trữ

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Backup folder	*(không chuyển)* Kaspersky Endpoint Security lưu các bản sao lưu của tập tin trong thư mục `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.
Maximum Backup size (MB)	**Giới hạn dung lượng của bản Sao lưu ở mức N MB** (mục **Thiết lập tổng quát → Các báo cáo và lưu trữ**)
Threshold value for space available (MB)	*(không chuyển)* Kaspersky Endpoint Security ghi nhật ký sự kiện *Ổ lưu trữ của Khu vực cách lý sắp hết không gian trống* khi đạt đến ngưỡng 50%.
Target folder for restoring objects	*(không chuyển)* Kaspersky Endpoint Security sẽ khôi phục các tập tin về thư mục gốc của chúng.
Quarantine folder	*(không chuyển)* Kaspersky Endpoint Security lưu các bản sao lưu của tập tin trong thư mục `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.
Maximum Quarantine size (MB)	*(không chuyển)* Kaspersky Endpoint Security sẽ sử dụng Sao lưu để lưu trữ các đối tượng có thể đã bị nhiễm mã độc. Trong quá trình chuyển đổi, Kaspersky Endpoint Security sẽ bỏ qua thiết lập của Khu vực cách ly.
Threshold value for space available (MB)	*(không chuyển)* Kaspersky Endpoint Security sẽ sử dụng Sao lưu để lưu trữ các đối tượng có thể đã bị nhiễm mã độc. Trong quá trình chuyển đổi, Kaspersky Endpoint Security sẽ bỏ qua thiết lập của Khu vực cách ly.
Target folder for restoring objects	*(không chuyển)* Kaspersky Endpoint Security sẽ khôi phục các tập tin về thư mục gốc của chúng.
Unblock automatically in N	**Chặn các thiết bị tấn công cho N phút** (Mục **Bảo vệ mối đe dọa thiết yếu → Bảo vệ mối đe dọa mạng**)

Real-time server protection

Real-Time File Protection

Thiết lập Bảo vệ tập tin theo thời gian thực của KSWS được chuyển sang mục **Bảo vệ mối đe dọa thiết yếu**, mục con **Bảo vệ mối đe dọa tập tin**.

Thiết lập Bảo vệ tập tin theo thời gian thực

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Objects protection mode: • **Smart mode** • **When run** • **On access** • **On access and modification**	**Chế độ quét**: • **Chế độ thông minh**. • **Khi thực thi**. • **Khi truy cập**. • **Khi truy cập và sửa đổi**.
Deeper analysis of launching processes	*(không chuyển)* Kaspersky Endpoint Security chỉ hỗ trợ một chế độ phân tích, là chế độ Optimal.
Heuristic analyzer: • **Light** • **Medium** • **Deep**	**Phân tích hành vi**: • **Quét nhanh**. • **Quét vừa**. • **Quét sâu**.
Apply Trusted Zone	*(không chuyển)* Kaspersky Endpoint Security áp dụng khu vực tin tưởng cho tất cả các thành phần. Bạn có thể cấu hình các loại trừ trong Thiết lập khu vực tin tưởng.
Use KSN for protection	*(không chuyển)* Kaspersky Endpoint Security sử dụng KSN cho tất cả các thành phần ứng dụng.
Block access to network shared resources for the hosts that show malicious activity	*(không chuyển)* Theo mặc định, Kaspersky Endpoint Security sẽ chặn truy cập vào các tài nguyên được chia sẻ trên mạng đối với các máy chủ có hoạt động độc hại.
Launch critical areas scan when active infection is detected	*(không chuyển)* Kaspersky Endpoint Security không khởi chạy tác vụ quét khu vực quan trọng khi phát hiện sự cố nhiễm mã độc đang hoạt động.
Use Kaspersky Sandbox for protection	*(không chuyển)* Theo mặc định, Kaspersky Endpoint Security sẽ gửi các đối tượng để quét tới Kaspersky Sandbox.
Protection scope	**Phạm vi bảo vệ**
Schedule settings	*(không chuyển)* Kaspersky Endpoint Security sử dụng lịch của chính ứng dụng để tạm dừng Bảo vệ mối đe dọa tập tin.

KSN Usage

Thiết lập KSWS cho Kaspersky Security Network được chuyển sang mục **Bảo vệ mối đe dọa nâng cao**, tiểu mục **Kaspersky Security Network**.

Cấu hình của Kaspersky Security Network

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
I confirm that I have fully read, understood, and accept the terms of participation in Kaspersky Security Network	**Tuyên bố Kaspersky Security Network** Kaspersky Endpoint Security yêu cầu sự đồng ý với Tuyên bố Kaspersky Security Network khi cài đặt ứng dụng, tạo chính sách hoặc bật sử dụng Kaspersky Security Network.
Send data about scanned files	*(không chuyển)* Kaspersky Endpoint Security sẽ tự động gửi dữ liệu về các tập tin được quét nếu KSN được bật.
Send data about requested URLs	*(không chuyển)* Kaspersky Endpoint Security sẽ tự động gửi dữ liệu về các URL được yêu cầu nếu KSN được bật.
Send Kaspersky Security Network statistics	**Bật chế độ KSN mở rộng**
Accept the terms of the Kaspersky Managed Protection Statement	*(không chuyển)* Kaspersky Endpoint Security không bao gồm dịch vụ KMP.
Action to perform on KSN untrusted objects	*(không chuyển)* Bạn có thể cấu hình Hành động khi phát hiện mối đe dọa trong thiết lập Thành phần bảo vệ và thiết lập tác vụ Quét.
Do not calculate checksum before sending to KSN if file size exceeds N MB	*(không chuyển)* Bạn có thể cấu hình các hạn chế quét tập tin lớn trong thiết lập Thành phần bảo vệ và thiết lập tác vụ Quét.
Use Kaspersky Security Center as KSN Proxy	**Sử dụng Máy chủ quản trị làm máy chủ proxy KSN**
Schedule settings	*(không chuyển)* Không thể cấu hình lịch riêng cho thành phần. Thành phần này luôn bật khi Kaspersky Endpoint Security đang hoạt động.

Traffic Security

Thiết lập Bảo vệ lưu lượng KSWS được chuyển sang mục **Bảo vệ mối đe dọa thiết yếu**, **Bảo vệ mối đe dọa web** và tiểu mục **Bảo vệ mối đe dọa thư điện tử**, mục **Kiểm soát bảo mật**, tiểu mục **Kiểm soát Web**, mục **Thiết lập tổng quát**, tiểu mục **Thiết lập mạng**.

Thiết lập bảo mật lưu lượng

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Apply URL-based rules	**Kiểm soát Web** (tiểu mục **Kiểm soát Web**) Các quy tắc dựa trên URL được chuyển sang các quy tắc riêng trong Kaspersky Endpoint Security.
Apply certificate-based rules	*(không chuyển)* Kaspersky Endpoint Security sẽ không hỗ trợ quy tắc dựa trên chứng chỉ.
Apply rules for web traffic category control	**Kiểm soát Web** (tiểu mục **Kiểm soát Web**) Các quy tắc chặn để kiểm soát danh mục lưu lượng truy cập web được chuyển sang một quy tắc chặn duy nhất trong Kaspersky Endpoint Security. Kaspersky Endpoint Security bỏ qua việc cho phép các quy tắc kiểm soát danh mục. Sự tương hợp của các danh mục KSWS và KES được liệt kê dưới đây.
Allow access if the web page can not be categorized	*(không chuyển)* Kaspersky Endpoint Security cho phép truy cập nếu không thể phân loại trang web.
Allow access to legitimate web resources that can be used to damage a protected device	*(không chuyển)* Kaspersky Endpoint Security cho phép truy cập vào các tài nguyên web hợp pháp có thể được sử dụng để làm hư hại thiết bị được bảo vệ.
Allow access to legitimate advertisement	*(không chuyển)* Bạn có thể quản lý truy cập vào quảng cáo hợp pháp bằng cách sử dụng danh mục tài nguyên web *Bảng quảng cáo* trong thiết lập Kiểm soát web.

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Operation mode: • **Driver Interceptor** • **Redirector** • **External Proxy**	*(không chuyển)* Kaspersky Endpoint Security chỉ hỗ trợ chế độ Driver Interceptor.
ICAP-service connection settings	*(không chuyển)* Kaspersky Endpoint Security không hỗ trợ ICAP Network Storage Protection.
Check safe connections through the HTTPS protocol	Chế độ **Quét các kết nối mã hóa** / **Luôn luôn quét các kết nối mã hóa** (tiểu mục **Thiết lập mạng**)
Use TLS protocol version	*(không chuyển)* Kaspersky Endpoint Security sẽ quét lưu lượng mạng mã hóa được truyền qua các giao thức sau: • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Ngoài ra, bạn có thể chặn các kết nối SSL 2.0 trong thiết lập quét các kết nối được mã hóa.
Do not trust web-servers with invalid certificate	**Địa chỉ** (tiểu mục **Thiết lập mạng**)
Intercept ports (Interception area)	**Giám sát các cổng** (tiểu mục **Thiết lập mạng**) Trong quá trình chuyển sang, KES sẽ xóa các hộp kiểm **Giám sát tất cả các cổng cho ứng dụng từ danh sách được khuyến nghị bởi Kaspersky** và **Theo dõi tất cả các cổng của những ứng dụng được chỉ định**.
Exclude ports (Interception area)	*(không chuyển)*
Exclude IP addresses (Interception area)	**Cấu hình địa chỉ được tin tưởng** (tiểu mục **Thiết lập mạng**)
Exclude processes (Interception area)	**Cấu hình ứng dụng được tin tưởng** (tiểu mục **Thiết lập mạng**) Trong quá trình di chuyển, KES sẽ cấu hình các thiết lập sau cho ứng dụng được tin tưởng: • Hộp kiểm **Không quét lưu lượng mạng** được chọn. KES sẽ không quét lưu lượng mạng để tìm bất kỳ địa chỉ IP từ xa và cổng nào. • Các hộp kiểm khác trong thiết lập ứng dụng được tin tưởng sẽ bị xóa.
Security port	*(không chuyển)*
Use malicious URL database to scan web links	**Kiểm tra địa chỉ web bằng cách đối chiếu với cơ sở dữ liệu địa chỉ web độc hại** (tiểu mục **Bảo vệ mối đe dọa web**)
Use anti-phishing database to scan web pages	**Kiểm tra địa chỉ web bằng cách đối chiếu với cơ sở dữ liệu địa chỉ web lừa đảo** (tiểu mục **Bảo vệ mối đe dọa web**)
Use KSN for protection	*(không chuyển)* Kaspersky Endpoint Security sử dụng KSN cho tất cả các thành phần ứng dụng.
Use Trusted Zone	*(không chuyển)* Kaspersky Endpoint Security áp dụng khu vực tin tưởng cho tất cả các thành phần. Bạn có thể cấu hình các loại trừ trong Thiết lập khu vực tin tưởng.
Use heuristic analyzer	**Sử dụng phân tích hành vi** (**Bảo vệ mối đe dọa web** và tiểu mục **Bảo vệ mối đe dọa thư điện tử**)
Security level	*(không chuyển)* Kaspersky Endpoint Security có các mức độ bảo mật riêng cho các thành phần Bảo vệ mối đe dọa web và Bảo vệ mối đe dọa thư điện tử. Theo mặc định, Kaspersky Endpoint Security đặt mức độ bảo mật được khuyến nghị.
Enable mail threat protection	**Bảo vệ mối đe dọa thư điện tử** (tiểu mục **Bảo vệ mối đe dọa thư điện tử**) **Kết nối phần mở rộng Microsoft Outlook** **Chỉ tin nhắn gửi đến** (Phạm vi bảo vệ) **Quét khi nhận** (Bảo vệ email)
Schedule settings	*(không chuyển)* Không thể cấu hình lịch riêng cho thành phần. Thành phần này luôn bật khi Kaspersky Endpoint Security đang hoạt động.

Exploit Prevention

Thiết lập Phòng chống khai thác của KSWS được chuyển sang mục **Bảo vệ mối đe dọa nâng cao**, tiểu mục **Phòng chống khai thác**.

Thiết lập Phòng chống khai thác

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Prevent vulnerable processes exploit: • **Terminate on exploit** • **Notify only**	**Khi phát hiện khai thác**: • **Chặn**. • **Thông báo**.
Notify about abused processes via Terminal Service	*(không chuyển)* Kaspersky Endpoint Security sẽ không hỗ trợ các dịch vụ đầu cuối.
Prevent vulnerable processes exploit even if Kaspersky Security Service is disabled	*(không chuyển)* Kaspersky Endpoint Security liên tục ngăn việc khai thác tiến trình dễ bị tấn công.
Protected processes	**Bật bảo vệ bộ nhớ tiến trình hệ thống** Kaspersky Endpoint Security sẽ không hỗ trợ chọn các tiến trình được bảo vệ. Bạn chỉ có thể bật bảo vệ bộ nhớ tiến trình hệ thống.
Exploit prevention techniques: • **Apply all available exploit prevention techniques** • **Apply selected exploit prevention techniques**	*(không chuyển)* Kaspersky Endpoint Security áp dụng tất cả các kỹ thuật phòng chống khai thác hiện có.

Network Threat Protection

Thiết lập Bảo vệ mối đe dọa mạng của KSWS được chuyển sang mục **Bảo vệ mối đe dọa thiết yếu**, tiểu mục **Bảo vệ mối đe dọa mạng**.

Thiết lập Bảo vệ mối đe dọa mạng

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Operation mode: • **Pass-through** • **Only inform about network attacks** • **Block connections when attack is detected**	**Bảo vệ mối đe dọa mạng** Nếu chế độ **Pass-through** được chọn thì Bảo vệ mối đe dọa mạng bị tắt. Nếu chế độ **Only inform about network attacks** hoặc chế độ **Block connections when attack is detected** được chọn thì Bảo vệ mối đe dọa mạng được bật. Kaspersky Endpoint Security luôn hoạt động ở chế độ **Block connections when attack is detected**.
Do not stop traffic analysis when the task is not running	*(không chuyển)* Kaspersky Endpoint Security sẽ phân tích lưu lượng liên tục nếu thành phần được kích hoạt.
Do not control excluded IP addresses	**Loại trừ**
Schedule settings	*(không chuyển)* Không thể cấu hình lịch riêng cho thành phần. Thành phần này luôn bật khi Kaspersky Endpoint Security đang hoạt động.

Script Monitoring

Kaspersky Endpoint Security sẽ không hỗ trợ thành phần Giám sát tập lệnh. Giám sát tập lệnh được xử lý bởi các thành phần khác, ví dụ như Bảo vệ AMSI.

Website categories

Kaspersky Endpoint Security không hỗ trợ tất cả các danh mục của Kaspersky Security for Windows Server. Các danh mục không tồn tại trong Kaspersky Endpoint Security sẽ không được chuyển đổi. Do đó, các quy tắc phân loại tài nguyên web có các danh mục không được hỗ trợ sẽ không được chuyển đổi.

Các danh mục của Kaspersky Security for Windows Server	Các danh mục của Kaspersky Endpoint Security cho Windows
Wargaming	Trò chơi điện tử
Abortion	*(không chuyển)*
Lotteries (extended)	Đánh bạc, xổ số, rút thăm
Alcohol	Cồn, thuốc lá, ma túy
Anonymous proxy servers	Trình ẩn danh
Anorexia	*(không chuyển)*
Rentals for real estate	*(không chuyển)*
Audio, video and software	Phần mềm, âm thanh, video
Banks	Ngân hàng
Blogs	Blog
Military	Vũ khí, thuốc nổ, quân sự
For children	*(không chuyển)*
Discrimination	Bạo lực, không khoan dung
Home and family	*(không chuyển)*
Hosting and domain services	Giao tiếp trên Internet
Pets and animals	*(không chuyển)*
Law and politics	Bị cấm bởi luật pháp khu vực
Restricted by Roskomnadzor (RF)	Bị cấm bởi luật pháp của Liên bang Nga
Restricted by Federal Law 436 (RF)	Bị cấm bởi luật pháp của Liên bang Nga
Restricted by RF legislation	Bị cấm bởi luật pháp của Liên bang Nga
Restricted by global legislation	Bị cấm bởi luật pháp khu vực
Adult dating	Nội dung người lớn
Internet services	*(không chuyển)*
Sex shops	Nội dung người lớn
Information technologies	*(không chuyển)*
Casinos, card games	Đánh bạc, xổ số, rút thăm
Books and writing	*(không chuyển)*
Computer games	Trò chơi điện tử
Health and beauty	*(không chuyển)*
Culture and society	*(không chuyển)*
LGBT	Nội dung người lớn
Lotteries	Đánh bạc, xổ số, rút thăm
Medicine	*(không chuyển)*
Fashion	*(không chuyển)*
Music	*(không chuyển)*
Drugs	Cồn, thuốc lá, ma túy
Violence	Bạo lực, không khoan dung
Discontent	*(không chuyển)*
Illegal drugs	Cồn, thuốc lá, ma túy
Hate and discrimination	Bạo lực, không khoan dung

Các danh mục của Kaspersky Security for Windows Server	Các danh mục của Kaspersky Endpoint Security cho Windows
Obscene vocabulary	Báng bổ, tục tĩu
Lingerie	Nội dung người lớn
News	Tin tức truyền thông
Nudism	Nội dung người lớn
Education	*(không chuyển)*
Online shopping	Cửa hàng trực tuyến
All communication media	Giao tiếp trên Internet
Payment by credit cards	Hệ thống thanh toán
Online shopping (own payment system)	Cửa hàng trực tuyến
Online encyclopedias	*(không chuyển)*
Online banking	Ngân hàng
Weapons	Vũ khí, thuốc nổ, quân sự
Fishing and hunting	*(không chuyển)*
Payment systems	Hệ thống thanh toán
Job search	Tìm kiếm việc làm
Search engines	*(không chuyển)*
Police decision (JP)	Bị cấm bởi Cảnh sát Nhật Bản
Trusted by KPSN	*(không chuyển)*
Untrusted by KPSN	*(không chuyển)*
Porn	Nội dung người lớn
Media hosting and streaming	Tin tức truyền thông
Web Mail	Email trên web
Traveling	*(không chuyển)*
TV and radio	Tin tức truyền thông
Teasers and ads services	Bảng quảng cáo
Religion	Tôn giáo, tổ chức tín ngưỡng
Restaurants, cafe and food	*(không chuyển)*
Dating sites	Trang hẹn hò
Sex education	Nội dung người lớn
Social networks	Mạng xã hội
Sport	*(không chuyển)*
Betting	Đánh bạc, xổ số, rút thăm
Suicide	Bạo lực, không khoan dung
Tobacco	Cồn, thuốc lá, ma túy
Torrents	Torrent
Mentioned in Federal list of extremists (RF)	Bị cấm bởi luật pháp của Liên bang Nga
File sharing	Chia sẻ tập tin
Pharmacy	*(không chuyển)*
Hobby and entertainment	*(không chuyển)*
Chats and forums	Trò chuyện, diễn đàn, tin nhắn nhanh
Schools and universities pages	*(không chuyển)*

Các danh mục của Kaspersky Security for Windows Server	Các danh mục của Kaspersky Endpoint Security cho Windows
Astrology and esoterica	*(không chuyển)*
Extremism and racism	Bạo lực, không khoan dung
E-commerce	Cửa hàng trực tuyến
Erotic	Nội dung người lớn
Humor	*(không chuyển)*

Local activity control

Applications Launch Control

Thiết lập Kiểm soát ứng dụng của KSWS được chuyển sang mục **Kiểm soát bảo mật**, tiểu mục **Kiểm soát ứng dụng**.

Thiết lập Kiểm soát khởi chạy ứng dụng

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Operation mode: • **Statistics only** • **Active**	**Hành động** (Kiểm soát ứng dụng): • **Kiểm tra quy tắc**. • **Áp dụng quy tắc**.
Repeat action taken for the first file launch on all the subsequent launches for this file	*(không chuyển)* Kaspersky Endpoint Security sẽ quét ứng dụng mỗi khi ứng dụng cố gắng chạy.
Deny the command interpreters launch with no command to execute	*(không chuyển)* Kaspersky Endpoint Security cho phép chạy trình thông dịch lệnh nếu chúng không bị thành phần Kiểm soát ứng dụng cấm.
Rules	**Quy tắc Kiểm soát ứng dụng** *(được hỗ trợ nhưng có các hạn chế)* Kaspersky Endpoint Security 11.11.0 ra mắt khả năng hỗ trợ di chuyển các quy tắc Kiểm soát khởi chạy ứng dụng. Chức năng di chuyển quy tắc Kiểm soát khởi chạy ứng dụng có một số hạn chế. Theo mặc định, Kiểm soát khởi chạy ứng dụng KSWS bao gồm hai quy tắc: • **Allow scripts and MSI by OS-trusted certificate** • **Allow executable by OS-trusted certificate** Nếu ít nhất một quy tắc KSWS nguồn có loại **Allow** thì trong quá trình di chuyển, KES sẽ tạo ra một quy tắc cho phép mới, **Applications with trusted root certificates**. Tức là Kiểm soát ứng dụng KES sẽ sử dụng một quy tắc duy nhất để cho phép chạy các tập lệnh, gói MSI và các tập tin thực thi được tin tưởng. Nếu cả hai quy tắc KSWS nguồn đều có loại **Deny** thì KES không thêm quy tắc quản lý ứng dụng có chứng chỉ gốc được tin tưởng.
Apply rules to executable files	*(không chuyển)* Không thể cấu hình phạm vi áp dụng quy tắc trong thiết lập Kiểm soát ứng dụng KES. Kiểm soát ứng dụng KES sẽ áp dụng các quy tắc cho tất cả các loại tập tin: tập tin thực thi, tập lệnh và gói MSI. Nếu tất cả các loại tập tin được thêm trong phạm vi áp dụng quy tắc trong KSWS, thì trong quá trình di chuyển, KES sẽ thực hiện các quy tắc KSWS. Nếu một số loại tập tin bị loại trừ khỏi phạm vi áp dụng quy tắc trong KSWS, thì trong quá trình di chuyển KES cũng chuyển các quy tắc KSWS, nhưng **Kiểm tra quy tắc** sẽ được chọn làm hành động Kiểm soát ứng dụng.
Monitor loading of DLL modules	**Giám sát việc tải các mô-đun DLL (tăng mức tải đáng kể lên hệ thống)**
Apply rules to scripts and MSI packages	*(không chuyển)* Không thể cấu hình phạm vi áp dụng quy tắc trong thiết lập Kiểm soát ứng dụng KES. Kiểm soát ứng dụng KES sẽ áp dụng các quy tắc cho tất cả các loại tập tin: tập tin thực thi, tập lệnh và gói MSI. Nếu tất cả các loại tập tin được thêm trong phạm vi áp dụng quy tắc trong KSWS, thì trong quá trình di chuyển, KES sẽ thực hiện các quy tắc KSWS. Nếu một số loại tập tin bị loại trừ khỏi phạm vi áp dụng quy tắc trong KSWS, thì trong quá trình di chuyển KES sẽ chuyển các quy tắc KSWS, nhưng **Kiểm tra quy tắc** sẽ được chọn làm hành động Kiểm soát ứng dụng.

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Deny applications untrusted by KSN	*(không chuyển)* Kaspersky Endpoint Security không xem xét danh tiếng của các ứng dụng và cho phép hoặc từ chối các ứng dụng đang chạy theo các quy tắc.
Allow applications trusted by KSN	Trong quá trình di chuyển, KES sẽ thêm một quy tắc cho phép mới. Danh mục KL **Phần mềm khác\Các ứng dụng được tin tưởng theo danh tiếng trong KSN** được chỉ định làm điều kiện kích hoạt quy tắc.
Users and / or user groups allowed to run applications trusted by KSN	**Người dùng và quyền của họ** trong một quy tắc cho phép Kiểm soát ứng dụng bao gồm danh mục KL **Phần mềm khác\Các ứng dụng được tin tưởng theo danh tiếng trong KSN**.
Automatically allow software distribution via applications and packages listed	Kiểm soát phân phối phần mềm trong KSWS và KES hoạt động khác nhau. Trong quá trình di chuyển, KES sẽ bổ sung các quy tắc cho phép mới cho các ứng dụng được phép phân phối phần mềm tự động. Giá trị băm tập tin được chỉ định làm điều kiện kích hoạt quy tắc.
Always allow software distribution via Windows Installer	Kiểm soát phân phối phần mềm trong KSWS và KES hoạt động khác nhau. Trong quá trình di chuyển, KES sẽ bổ sung các quy tắc cho phép mới cho các ứng dụng được phép phân phối phần mềm tự động (**Software distribution applications and packages allowed**). Giá trị băm tập tin được chỉ định làm điều kiện kích hoạt quy tắc. Trong thuộc tính tài khoản, hộp kiểm **Trình cập nhật được tin tưởng** được chọn.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(không chuyển)*
Software distribution applications and packages allowed	Kiểm soát phân phối phần mềm trong KSWS và KES hoạt động khác nhau. Trong quá trình di chuyển, KES sẽ bổ sung các quy tắc cho phép mới cho các ứng dụng được phép phân phối phần mềm tự động. Giá trị băm tập tin được chỉ định làm điều kiện kích hoạt quy tắc. Trong thuộc tính tài khoản, hộp kiểm **Trình cập nhật được tin tưởng** được chọn.
Schedule settings	*(không chuyển)* Nếu lịch được cấu hình cho thành phần trong cài đặt KSWS thì thành phần Kiểm soát ứng dụng sẽ được bật khi di chuyển. Nếu lịch không được cấu hình cho thành phần trong cài đặt KSWS thì thành phần Kiểm soát ứng dụng sẽ bị tắt khi di chuyển. Không thể cấu hình lịch riêng cho thành phần. Thành phần này luôn bật khi Kaspersky Endpoint Security đang hoạt động.

Device Control

Thiết lập Kiểm soát thiết bị của KSWS được chuyển sang mục **Kiểm soát bảo mật**, tiểu mục **Kiểm soát thiết bị**.

Thiết lập Kiểm soát thiết bị

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Operation mode: • **Active** • **Statistics only**	*(không chuyển)* Kiểm soát ứng dụng hoạt động ở chế độ *Active*. Số liệu thống kê về kết nối thiết bị được Kiểm toán liên tục cung cấp.
Allow using all external devices when the Device Control task is not running	*(không chuyển)* Kiểm soát thiết bị luôn bật trong khi Kaspersky Endpoint Security đang chạy.
Device Control rules	**Thiết bị được tin tưởng** Trong quá trình chuyển đổi, Kaspersky Endpoint Security sẽ bỏ qua các quy tắc KSWS bị tắt.
Schedule settings	*(không chuyển)* Kaspersky Endpoint Security sử dụng lịch riêng của ứng dụng để giành quyền truy cập vào một số loại thiết bị nhất định.

Network-Attached Storages Protection

RPC Network Storage Protection

Kaspersky Endpoint Security không hỗ trợ các thành phần Bảo vệ ổ lưu trữ nối mạng. Nếu cần những thành phần này, bạn có thể tiếp tục sử dụng Kaspersky Security for Windows Server.

ICAP Network Storage Protection

Kaspersky Endpoint Security không hỗ trợ các thành phần Bảo vệ ổ lưu trữ nối mạng. Nếu cần những thành phần này, bạn có thể tiếp tục sử dụng Kaspersky Security for Windows Server.

Anti-Cryptor for NetApp

Kaspersky Endpoint Security không hỗ trợ Anti-Cryptor for NetApp. Chức năng Anti-Cryptor được cung cấp bởi các thành phần ứng dụng khác, chẳng hạn như Phát hiện hành vi.

Network activity control

Firewall Management

Kaspersky Endpoint Security không hỗ trợ Quản lý tường lửa của KSWS. Các chức năng của Tường lửa KSWS được thực hiện bởi Tường lửa cấp hệ thống. Sau khi chuyển đổi, bạn có thể cấu hình Tường lửa của Kaspersky Endpoint Security.

Anti-Cryptor

Thiết lập Network Anti-Cryptor được chuyển sang mục **Bảo vệ mối đe dọa nâng cao**, tiểu mục **Phát hiện hành vi**.

Thiết lập Anti-Cryptor

Thiết lập KSWS	Thiết lập KES
Operation mode: • **Statistics only** • **Active**	**Khi phát hiện mã hóa từ bên ngoài các thư mục được chia sẻ**: • **Thông báo**. • **Chặn**.
Heuristic analyzer	*(không chuyển)* Kaspersky Endpoint Security không sử dụng Phân tích hành vi để Phát hiện hành vi.
Configuration of protection scope: • **All shared network folders on the protected device** • **Only specified shared folders**	*(không chuyển)* Kaspersky Endpoint Security ngăn mã hóa tất cả các thư mục mạng được chia sẻ của máy tính được bảo vệ.
Exclusions	*(không chuyển)* Kaspersky Endpoint Security có các loại trừ riêng cho thành phần Phát hiện hành vi. Bạn có thể thêm các loại trừ sau khi chuyển sang theo cách thủ công.
Schedule settings	*(không chuyển)* Không thể cấu hình lịch riêng cho thành phần. Thành phần này luôn bật khi Kaspersky Endpoint Security đang hoạt động.

System Inspection

File Integrity Monitor

Thiết lập Giám sát tính toàn vẹn của tập tin từ KSWS được chuyển sang mục **Kiểm soát bảo mật** tiết diện, tiểu mục **Giám sát tính toàn vẹn của hệ thống**.

Thiết lập Giám sát tính toàn vẹn của tập tin

Thiết lập KSWS	Thiết lập KES
Log information about file operations that appear during the monitor interruption period	*(không chuyển)* Kaspersky Endpoint Security không ghi lại các sự kiện cho các hoạt động tập tin được thực hiện trong thời gian gián đoạn màn hình.
Block attempts to compromise the USN log	*(không chuyển)* Kaspersky Endpoint Security không chặn các nỗ lực xâm nhập nhật ký USN.
Monitoring scope	**Phạm vi giám sát → Tập tin** *(được hỗ trợ nhưng có các hạn chế)* Bản ghi phạm vi giám sát bị vô hiệu hóa sẽ không được di chuyển sang KES. Kaspersky Endpoint Security chỉ thêm các bản ghi được bật vào phạm vi giám sát.
Trusted users	**Người dùng và / hoặc nhóm người dùng được tin tưởng**
File operation markers	**Bộ đánh dấu thao tác với tập tin**
Calculate checksum for the file if possible	**Tạo giá trị băm**
Exclusions	**Loại trừ → Tập tin**

Log Inspection

Thiết lập Kiểm tra nhật ký của KSWS được chuyển sang mục **Kiểm soát bảo mật**, tiểu mục **Kiểm tra nhật ký**.

Thiết lập Kiểm tra nhật ký

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Apply custom rules for log inspection	*(không chuyển)* Kaspersky Endpoint Security sẽ áp dụng tất cả các quy tắc tùy chỉnh đã kích hoạt.
Custom rules	**Quy tắc tùy chỉnh** Quy tắc định trước **A service was installed in the system (for Server 2003 OS)** không được di chuyển sang KES.
Apply predefined rules for log inspection	*(không chuyển)* Kaspersky Endpoint Security sẽ áp dụng tất cả các quy tắc định trước đã kích hoạt.
Predefined rules	**Các quy tắc định trước**
Password brute-force detection	**Phát hiện tấn công vét cạn**
Network logon detection	**Phát hiện đăng nhập mạng**
Exclusions (IP addresses)	**Loại trừ** (Địa chỉ IP)
Exclusions (users)	**Loại trừ** (Người dùng)
Schedule settings	*(không chuyển)* Không thể cấu hình lịch riêng cho thành phần. Thành phần này luôn bật khi Kaspersky Endpoint Security đang hoạt động.

Logs and notifications

Task logs

Thiết lập Nhật ký KSWS được chuyển sang mục **Thiết lập tổng quát**, **Giao diện** và các tiểu mục của **Các báo cáo và lưu trữ**.

Thiết lập nhật ký

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Event logging	**Thông báo** (tiểu mục **Giao diện**)
Logs folder	*(không chuyển)* Kaspersky Endpoint Security lưu các báo cáo trong thư mục `C:\ProgramData\Kaspersky Lab\KES.14.2\Report`.
Remove task logs older than N day(s)	*(không chuyển)* Bạn có thể cấu hình thời gian lưu trữ cho báo cáo của KES trong **Thiết lập tổng quát**, **Các báo cáo và lưu trữ**.
Remove from the audit log events N day(s)	*(không chuyển)* Kaspersky Endpoint Security sẽ áp dụng các giới hạn lưu trữ báo cáo cho tất cả các báo cáo, bao gồm báo cáo kiểm toán hệ thống.
SIEM Integration	*(không chuyển)* Bạn có thể cấu hình tích hợp SIEM trong Kaspersky Security Center.

Event notifications

Thiết lập thông báo của KSWS được chuyển sang mục **Thiết lập tổng quát**, tiểu mục **Giao diện**.

Thiết lập thông báo

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Notifications	**Thông báo**
Notify users: • **By using terminal service** • **By using Windows Messenger Service command**	*(không chuyển)* Kaspersky Endpoint Security không hỗ trợ chỉnh sửa văn bản thông báo. Kaspersky Endpoint Security sẽ hiển thị các thông báo tiêu chuẩn.
Notify administrators: • **By using Windows Messenger Service command** • **By running executable file** • **By sending email**	Chỉ thiết lập thông báo email mới được chuyển sang Kaspersky Endpoint Security - **Thiết lập thông báo email** (mục **Thông báo**). Không hỗ trợ các phương thức thông báo khác cho quản trị viên.
Application database is out of date	**Gửi thông báo "Cơ sở dữ liệu đã lỗi thời" nếu cơ sở dữ liệu không được cập nhật**
Application database is extremely out of date	**Gửi thông báo "Cơ sở dữ liệu đã rất lỗi thời" nếu cơ sở dữ liệu không được cập nhật**
Critical areas scan has not been performed for a long time	*(không chuyển)* Kaspersky Endpoint Security sẽ tạo một sự kiện Quét khu vực quan trọng bị bỏ lỡ sau ba ngày.

Interaction with Administration Server

Thiết lập tương tác Máy chủ quản trị KSWS được chuyển sang mục **Thiết lập tổng quát**, tiểu mục **Các báo cáo và lưu trữ**.

Thiết lập tương tác Máy chủ quản trị

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Quarantined files	**Các tập tin trong Khu vực cách ly**
Backed up files	**Các tập tin sao lưu**
Blocked hosts	*(không chuyển)* Kaspersky Endpoint Security sẽ tự động gửi dữ liệu về các máy chủ bị chặn.

Tasks

Activating the application

Kaspersky Endpoint Security không hỗ trợ tác vụ *Application activation* (KSWS). Bạn có thể tạo một tác vụ *Thêm khóa* (KES), thêm khóa giấy phép vào Gói cài đặt hoặc bật tự động phân phối khóa giấy phép.

Copying Updates

Các thiết lập tác vụ *Copying Updates* (KSWS) được chuyển sang tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* (KES).

Thiết lập tác vụ Sao chép bản cập nhật

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Nguồn cập nhật**: • **Kaspersky Security Center**. • **Các máy chủ cập nhật của Kaspersky**. • **Được chỉ định bởi người dùng**.
Use Kaspersky update servers if specified servers are not available	*(không chuyển)* Kaspersky Endpoint Security cho phép chọn nhiều nguồn cập nhật, bao gồm các máy chủ cập nhật của Kaspersky. Nếu nguồn cập nhật đầu tiên không khả dụng, Kaspersky Endpoint Security sẽ cho phép bạn tải các bản cập nhật từ một nguồn khác trong danh sách.
Use proxy server settings to connect to Kaspersky update servers	*(không chuyển)* Kaspersky Endpoint Security sẽ sử dụng máy chủ proxy cho tất cả các thành phần. Bạn có thể cấu hình kết nối máy chủ proxy trong các tùy chọn mạng của ứng dụng.
Use proxy server settings to connect to other servers	*(không chuyển)* Kaspersky Endpoint Security sẽ sử dụng máy chủ proxy cho tất cả các thành phần. Bạn có thể cấu hình kết nối máy chủ proxy trong các tùy chọn mạng của ứng dụng.
Copying updates settings: • **Copy database updates** • **Copy critical software modules updates** • **Copy database updates and critical updates of application modules**	*(không chuyển)* Kaspersky Endpoint Security sẽ sao chép các bản cập nhật cơ sở dữ liệu và các bản cập nhật quan trọng của mô-đun ứng dụng dưới dạng một gói duy nhất.
Folder for local storage of copied updates	**Sao chép các bản cập nhật vào thư mục**

Baseline File Integrity Monitor

Các thiết lập tác vụ *Baseline File Integrity Monitor* (KSWS) được chuyển sang tác vụ *Kiểm tra tính toàn vẹn của hệ thống* và sang mục chính sách **Kiểm soát bảo mật**, mục con **Giám sát tính toàn vẹn của hệ thống**.

Thiết lập tác vụ Giám sát tính toàn vẹn của tập tin cơ sở

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Hash calculation algorithm: • **MD5** • **SHA256**.	*(không chuyển)* Kaspersky Endpoint Security sử dụng thuật toán SHA256 để tính giá trị tổng kiểm.
Scan scope	**Phạm vi giám sát** (tiểu mục **Giám sát tính toàn vẹn của hệ thống**)

Database Update

Các thiết lập tác vụ *Database Update* (KSWS) được chuyển sang tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* (KES).

Thiết lập tác vụ cập nhật cơ sở dữ liệu

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Nguồn cập nhật**: • **Kaspersky Security Center**. • **Các máy chủ cập nhật của Kaspersky**. • **Được chỉ định bởi người dùng**.
Use Kaspersky update servers if specified servers are not available	*(không chuyển)* Kaspersky Endpoint Security cho phép chọn nhiều nguồn cập nhật, bao gồm các máy chủ cập nhật của Kaspersky. Nếu nguồn cập nhật đầu tiên không khả dụng, Kaspersky Endpoint Security sẽ cho phép bạn tải các bản cập nhật từ một nguồn khác trong danh sách.
Use proxy server settings to connect to Kaspersky update servers	*(không chuyển)* Kaspersky Endpoint Security sẽ sử dụng máy chủ proxy cho tất cả các thành phần. Bạn có thể cấu hình kết nối máy chủ proxy trong các tùy chọn mạng của ứng dụng.
Use proxy server settings to connect to other servers	*(không chuyển)* Kaspersky Endpoint Security sẽ sử dụng máy chủ proxy cho tất cả các thành phần. Bạn có thể cấu hình kết nối máy chủ proxy trong các tùy chọn mạng của ứng dụng.
Lower the load on the disk I/O	*(không chuyển)*

Software modules updates

Các thiết lập tác vụ *Software Modules Update* (KSWS) được chuyển sang tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* (KES).

Thiết lập tác vụ Cập nhật mô-đun phần mềm

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Nguồn cập nhật**: • **Kaspersky Security Center**. • **Các máy chủ cập nhật của Kaspersky**. • **Được chỉ định bởi người dùng**.
Use Kaspersky update servers if specified servers are not available	*(không chuyển)* Kaspersky Endpoint Security cho phép chọn nhiều nguồn cập nhật, bao gồm các máy chủ cập nhật của Kaspersky. Nếu nguồn cập nhật đầu tiên không khả dụng, Kaspersky Endpoint Security sẽ cho phép bạn tải các bản cập nhật từ một nguồn khác trong danh sách.
Use proxy server settings to connect to Kaspersky update servers	*(không chuyển)* Kaspersky Endpoint Security sẽ sử dụng máy chủ proxy cho tất cả các thành phần. Bạn có thể cấu hình kết nối máy chủ proxy trong các tùy chọn mạng của ứng dụng.
Use proxy server settings to connect to other servers	*(không chuyển)* Kaspersky Endpoint Security sẽ sử dụng máy chủ proxy cho tất cả các thành phần. Bạn có thể cấu hình kết nối máy chủ proxy trong các tùy chọn mạng của ứng dụng.

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Copy and install critical software modules updates	**Cài đặt các bản cập nhật quan trọng và được phê duyệt**
Only check for critical software updates available	*(không chuyển)* Kaspersky Endpoint Security liên tục kiểm tra tính khả dụng của các bản cập nhật rất quan trọng cho các mô-đun ứng dụng.
Allow operating system restart	*(không chuyển)* Kaspersky Endpoint Security sẽ nhắc người dùng cấp quyền khởi động lại máy tính.
Receive information about available scheduled software modules updates	*(không chuyển)* Kaspersky Endpoint Security sẽ hiển thị thông báo về các bản cập nhật mô-đun phần mềm.

Rollback of Application Database Update

Các thiết lập tác vụ *Rollback of Application Database Update* (KSWS) được chuyển sang tác vụ *Hoàn tác bản cập nhật* (KES). Tác vụ *Hoàn tác bản cập nhật* mới (KES) có lịch bắt đầu tác vụ – *Manually*.

On-Demand Scan

Các thiết lập tác vụ *On-Demand Scan* (KSWS) được chuyển sang tác vụ *Quét phần mềm độc hại* (KES).

Thiết lập tác vụ Quét virus

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Scan scope	**Phạm vi quét**
Protection level: • **Maximum protection** • **Recommended** • **Maximum performance**	**Mức độ bảo mật**: • **Cao**. • **Khuyên dùng**. • **Thấp**. Thiết lập mức độ bảo mật sẽ khác nhau trong KSWS và KES.
Objects to scan: • **All objects** • **Objects scanned by format** • **Objects scanned according to list of extensions specified in anti-virus database** • **Objects scanned by specified list of extensions**	**Loại tập tin**: • **Tất cả tập tin**. • **Quét các tập tin theo định dạng**. • **Quét các tập tin theo phần mở rộng**. Kaspersky Endpoint Security không cho phép tạo danh sách phần mở rộng tùy chỉnh. Kaspersky Endpoint Security sẽ thay thế giá trị **Objects scanned by specified list of extensions** bằng giá trị **Quét các tập tin theo phần mở rộng**.
Subfolders	**Bao gồm các thư mục con**
Subfiles	*(không chuyển)*
Scan disk boot sectors and MBR	*(không chuyển)*
Scan alternate NTFS streams	*(không chuyển)*
Scan only new and modified files	**Chỉ quét các tập tin mới và bị chỉnh sửa**
Scan of compound objects: • **All archives** • **All SFX archives** • **All email databases** • **All packed objects** • **All plain email** • **All embedded OLE objects**	**Quét các tập tin hỗn hợp**: • **Quét tập tin nén**. • **Quét tập tin nén có mật khẩu bảo vệ**. • **Quét các gói phân phối**. • **Quét các tập tin có định dạng email**. • **Quét các tập tin có định dạng Microsoft Office**.
Action to perform on infected and other objects: • **Disinfect** • **Disinfect. Remove if disinfection fails** • **Remove** • **Perform recommended action** • **Notify only**	**Hành động khi phát hiện mối đe dọa**: • **Khử mã độc, xóa nếu không thể khử mã độc**. • **Khử mã độc; thông báo nếu không thể khử mã độc**. • **Thông báo**.

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Action to perform on probably infected objects: • **Quarantine** • **Remove** • **Perform recommended action** • **Notify only**	*(không chuyển)* Kaspersky Endpoint Security sẽ áp dụng hành động nếu phát hiện thấy bất kỳ mối đe dọa nào.
Perform actions depending on the type of object detected	*(không chuyển)*
Entirely remove compound file that cannot be modified by the application in case of embedded object detection	*(không chuyển)*
Exclude files	*(không chuyển)* Kaspersky Endpoint Security áp dụng khu vực tin tưởng cho tất cả các thành phần. Bạn có thể cấu hình các loại trừ trong Thiết lập khu vực tin tưởng.
Do not detect	*(không chuyển)*
Stop scanning if it takes longer than N sec	**Bỏ qua các tập tin quét trong thời gian dài hơn N giây**
Do not scan compound objects larger than N MB	**Không giải nén các tập tin hỗn hợp lớn**
Use iSwift technology	**Công nghệ iSwift**
Use iChecker technology	**Công nghệ iChecker**
Action on the offline files: • **Do not scan** • **Scan resident part of file only** • **Scan entire file** • **Only if the file has been accessed within the specified period (days)** • **Do not copy file to a local hard drive, if possible**	*(không chuyển)* Kaspersky Endpoint Security sẽ quét toàn bộ các tập tin ngoại tuyến của chúng.

Application Integrity Check

Các thiết lập tác vụ *Application Integrity Control* (KSWS) được chuyển sang tác vụ *Kiểm tra tính toàn vẹn của ứng dụng* (KES).

Rule Generator for Applications Launch Control

Kaspersky Endpoint Security không hỗ trợ tác vụ *Applications Launch Control Generator*. Bạn có thể tạo các quy tắc trong Thiết lập Kiểm soát ứng dụng.

Rule Generator for Device Control

Kaspersky Endpoint Security không hỗ trợ tác vụ *Rule Generator for Device Control*. Bạn có thể tạo các quy tắc truy cập trong Thiết lập Kiểm soát thiết bị.

Chuyển các thành phần KSWS

Trước khi cài đặt cục bộ, Kaspersky Endpoint Security sẽ kiểm tra máy tính để xác định sự hiện diện của các ứng dụng Kaspersky. Nếu Kaspersky Security for Windows Server được cài đặt trên máy tính, KES sẽ phát hiện bộ thành phần KSWS đã được cài đặt và chọn các thành phần giống nhau để cài đặt.

Các thành phần KES mà KSWS không có sẽ được cài đặt như sau:

- Bảo vệ AMSI, Phòng chống xâm nhập máy chủ, Công cụ khắc phục được cài đặt theo thiết lập mặc định.
- Các thành phần Phòng chống Tấn công BadUSB, Kiểm soát thích ứng sự cố, Mã hóa dữ liệu, Detection and Response đều bị bỏ qua.

Khi được cài đặt từ xa, ứng dụng KES sẽ bỏ qua nhóm thành phần KSWS đã cài đặt. Trình cài đặt sẽ cài đặt các thành phần mà bạn chọn trong thuộc tính của gói cài đặt. Sau khi cài đặt Kaspersky Endpoint Security và chuyển chính sách và tác vụ, thiết lập KES sẽ được cấu hình theo thiết lập KSWS.

Chuyển đổi các tác vụ và chính sách của KSWS

Bạn có thể chuyển đổi thiết lập chính sách và tác vụ KSWS theo các cách sau:

- Sử dụng Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ (sau đây gọi là Trình hướng dẫn chuyển đổi).

  > Trình hướng dẫn chuyển đổi cho KSWS chỉ khả dụng trong Bảng điều khiển quản trị (MMC). Không thể chuyển thiết lập chính sách và tác vụ trong Bảng điều khiển web và Bảng điều khiển đám mây.

  Trình hướng dẫn chuyển đổi hàng loạt sẽ hoạt động khác nhau tùy theo các phiên bản khác nhau của Kaspersky Security Center. Bạn nên nâng cấp giải pháp lên phiên bản 14.2 trở lên. Trong phiên bản Kaspersky Security Center này, Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ cho phép bạn chuyển các chính sách vào một cấu hình thay vì vào một chính sách. Trong phiên bản Kaspersky Security Center này, Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ cũng cho phép bạn chuyển một dải thiết lập chính sách rộng hơn.

- Sử dụng Trình hướng dẫn chính sách mới cho Kaspersky Endpoint Security cho Windows.

  Trình hướng dẫn chính sách mới cho phép bạn tạo chính sách KES dựa trên chính sách KSWS.

Các quy trình chuyển chính sách KSWS sẽ khác nhau khi sử dụng Trình hướng dẫn chuyển đổi và Trình hướng dẫn chính sách mới.

Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ

Trình hướng dẫn chuyển đổi sẽ chuyển thiết lập chính sách KSWS vào bộ cấu hình chính sách thay vì thiết lập chính sách KES. *Bộ cấu hình chính sách* là một tập hợp các thiết lập chính sách được kích hoạt trên máy tính nếu máy tính đáp ứng các quy tắc kích hoạt được cấu hình. Thẻ thiết bị `UpgradedFromKSWS` được chọn làm tiêu chí kích hoạt của bộ cấu hình chính sách. Kaspersky Security Center sẽ tự động thêm thẻ `UpgradedFromKSWS` vào tất cả các máy tính mà bạn cài đặt KES lên trên KSWS bằng tác vụ cài đặt từ xa. Nếu chọn phương thức cài đặt khác, bạn có thể gán thẻ cho thiết bị theo cách thủ công.

Để thêm thẻ vào thiết bị:

1. Tạo thẻ mới cho máy chủ — `UpgradedFromKSWS`.

   Để biết thêm chi tiết về việc tạo thẻ cho các thiết bị, hãy tham khảo Trợ giúp của Kaspersky Security Center.

2. Tạo một nhóm quản trị mới trong bảng điều khiển Kaspersky Security Center và thêm các máy chủ mà bạn muốn gán thẻ cho nhóm này.

   Bạn có thể nhóm các máy chủ bằng công cụ lựa chọn. Để biết thêm chi tiết về thao tác với các lựa chọn, hãy tham khảo Trợ giúp của Kaspersky Security Center.

3. Chọn tất cả các máy chủ của nhóm quản trị trong bảng điều khiển Kaspersky Security Center, mở thuộc tính của các máy chủ đã chọn rồi gán thẻ.

Nếu bạn đang chuyển nhiều chính sách KSWS, thì mỗi chính sách sẽ được chuyển đổi thành một cấu hình trong một chính sách tổng thể. Nếu chính sách KSWS đã có bộ cấu hình thì những cấu hình này cũng được chuyển dưới dạng cấu hình. Kết quả là bạn sẽ nhận được một chính sách duy nhất bao gồm các bộ cấu hình tương ứng với tất cả các chính sách KSWS.

Cách sử dụng Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ để chuyển đổi thiết lập chính sách KSWS

1. Trong Bảng điều khiển quản trị, chọn Máy chủ quản trị và nhấn chuột phải để mở menu ngữ cảnh.

2. Chọn **All tasks** → **Policies and tasks batch conversion wizard**.

   Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ sẽ khởi chạy. Làm theo chỉ dẫn của Trình hướng dẫn.

Bước 1. Chọn ứng dụng mà bạn cần chuyển đổi chính sách và tác vụ

Tại bước này, bạn cần chọn Kaspersky Endpoint Security cho Windows. Chuyển sang bước tiếp theo.

Bước 2. Chuyển đổi chính sách

Trình hướng dẫn chuyển đổi sẽ tạo bộ cấu hình chính sách KSWS bên trong chính sách KES. Chọn chính sách Kaspersky Security for Windows Server mà bạn muốn chuyển đổi sang bộ cấu hình chính sách. Chuyển sang bước tiếp theo.

Khi đó, Trình hướng dẫn chuyển đổi sẽ bắt đầu chuyển đổi các chính sách. Tên của các bộ cấu hình chính sách mới sẽ tương ứng với các chính sách KSWS ban đầu.

Bước 3. Báo cáo chuyển đổi chính sách

Trình hướng dẫn chuyển đổi sẽ tạo báo cáo chuyển đổi chính sách. Báo cáo chuyển chính sách chứa ngày và giờ khi các chính sách được chuyển đổi, tên của chính sách KSWS ban đầu, tên của chính sách KES đích và tên của bộ cấu hình chính sách mới.

Bước 4. Chuyển đổi tác vụ

Trình hướng dẫn chuyển đổi sẽ tạo các tác vụ mới cho Kaspersky Endpoint Security cho Windows. Trong danh sách tác vụ, hãy chọn các tác vụ KSWS mà bạn muốn tạo cho Kaspersky Endpoint Security. Tác vụ mới sẽ được đặt tên *<tên tác vụ KSWS> (được chuyển đổi)*. Chuyển sang bước tiếp theo.

Bước 5. Hoàn tất Trình hướng dẫn

Hoàn tất trình hướng dẫn. Kết quả là trình hướng dẫn thực hiện như sau:

- Các bộ cấu hình chính sách mới được thêm vào chính sách Kaspersky Endpoint Security.

  Chính sách này bao gồm các cấu hình có thiết lập của Kaspersky Security for Windows Server. Chính sách mới có trạng thái *Active*. Trình hướng dẫn không thay đổi các chính sách KSWS.

- Sẽ tạo các tác vụ Kaspersky Endpoint Security mới.

  Các tác vụ mới là bản sao của các tác vụ KSWS. Trình hướng dẫn không thay đổi các tác vụ KSWS.

Bộ cấu hình chính sách mới có thiết lập KSWS sẽ được đặt tên *UpgradedFromKSWS <Tên chính sách Kaspersky Security for Windows Server>*. Trong thuộc tính cấu hình, trình hướng dẫn chuyển đổi sẽ tự động chọn thẻ thiết bị `UpgradedFromKSWS` làm tiêu chí kích hoạt. Do đó, các thiết lập từ bộ cấu hình chính sách sẽ tự động được áp dụng cho các máy chủ.

Trình hướng dẫn để tạo chính sách dựa trên chính sách KSWS

Khi chính sách KES được tạo dựa trên chính sách KSWS, trình hướng dẫn sẽ chuyển thiết lập sang chính sách mới tương ứng. Nghĩa là, một chính sách KES sẽ tương ứng với một chính sách KSWS. Trình hướng dẫn không chuyển đổi chính sách thành cấu hình.

Cách sử dụng Trình hướng dẫn chính sách mới để chuyển đổi thiết lập chính sách KSWS

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, hãy chọn thẻ **Policies**.

4. Nhấn vào **New policy**.
   Trình hướng dẫn Chính sách sẽ được bắt đầu.
5. Làm theo chỉ dẫn của Trình hướng dẫn Chính sách.

Bước 1. Chọn ứng dụng để tạo chính sách nhóm

Chọn ứng dụng **Kaspersky Endpoint Security for Windows (14.2)**.

Bước 2. Đặt tên cho chính sách nhóm

Nhập tên cho chính sách nhóm, ví dụ: *Chính sách cho văn phòng*.

Chọn hộp kiểm **Use policy settings for an earlier version of the application**. Nhấn vào **Browse** và chọn chính sách KSWS.

Bước 3. Tham gia Kaspersky Security Network

Vui lòng đọc và chấp nhận các điều khoản của Tuyên bố Kaspersky Security Network (KSN).

Bước 4. Chọn chế độ sử dụng ứng dụng trên máy tính

Chọn **Chế độ tiêu chuẩn để bảo vệ máy chủ**. Kaspersky Endpoint Security cung cấp một chính sách chung cho tất cả chế độ ứng dụng và các loại HĐH.

> Bạn nên sử dụng các chính sách khác nhau cho các chế độ và loại hệ điều hành khác nhau.

Bước 5. Nhập thiết lập

> Bước này khả dụng nếu bạn chọn cấu hình chính sách thủ công ở bước 4.

Bạn có thể tạo chính sách dựa trên thiết lập Kaspersky Endpoint Security từ tập tin cấu hình CFG. Trình hướng dẫn chính sách mới không hỗ trợ các tập tin cấu hình được mã hóa. Khi xuất tập tin cấu hình, hãy bỏ qua bước mã hóa tập tin.

Khi nhập tập tin cấu hình CFG ứng dụng, không phải tất cả các thiết lập chính sách đều có sẵn cho trình hướng dẫn. Ví dụ: các hồ sơ chính sách bị thiếu trong thiết lập ứng dụng. Nếu bạn muốn chuyển tất cả thiết lập và hồ sơ sang chính sách, bạn có thể nhập một chính sách khác từ tập tin KLP.

Khi nhập tập tin cấu hình, Kaspersky Endpoint Security sẽ không chuyển mật khẩu bộ chứa mã hóa. Nếu bạn sử dụng xác thực hai chiều khi kết nối với máy chủ, bạn cần phải chỉ định mật khẩu của bộ chứa mã hóa lại từ đầu.

Bước 6 - 10. Cấu hình thiết lập chính sách

Bước này khả dụng nếu bạn chọn cấu hình chính sách thủ công ở bước 4.

Làm theo các bước sau để quản lý thiết lập chính sách.

Bước 11. Cấu hình khu vực tin tưởng

Cấu hình vùng tin tưởng. Bạn có thể thêm loại trừ quét được định sẵn và ứng dụng được tin tưởng. Các ứng dụng được tin tưởng và loại trừ quét được xác định trước giúp nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager. Điều này có nghĩa là bạn không cần thiết lập khu vực tin tưởng theo cách thủ công cho ứng dụng trên máy chủ. Các loại trừ quét được định sẵn và các ứng dụng được tin tưởng cũng có thể giúp bạn nhanh chóng cấu hình Kaspersky Endpoint Security ở chế độ Light Agent trong môi trường ảo Citrix và VMware.

Bước 12. Chọn trạng thái chính sách

- **Active**. Sau lần đồng bộ tiếp theo, chính sách sẽ được sử dụng làm chính sách hoạt động trên máy tính.

  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.

- **Inactive**. Chính sách sao lưu. Nếu cần thiết, một chính sách không hoạt động có thể được chuyển trạng thái thành hoạt động.

  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.

- **Out-of-office**. Chính sách này được kích hoạt khi máy tính rời khỏi mạng doanh nghiệp.

Hoàn tất trình hướng dẫn.

Cấu hình bổ sung của các chính sách và tác vụ sau khi chuyển đổi

KSWS và KES có các nhóm thành phần và thiết lập chính sách khác nhau, vì vậy, sau khi chuyển, bạn phải xác minh rằng thiết lập chính sách đáp ứng các yêu cầu bảo mật của công ty bạn.

Kiểm tra các thiết lập chính sách cơ bản sau:

- Bảo vệ bằng mật khẩu. Thiết lập bảo vệ bằng mật khẩu KSWS sẽ không được chuyển. Kaspersky Endpoint Security có tính năng Bảo vệ bằng mật khẩu được tích hợp sẵn. Nếu cần, hãy bật Bảo vệ bằng mật khẩu.

- Khu vực tin tưởng. Các phương thức được KSWS và KES sử dụng để chọn đối tượng sẽ khác nhau. Khi chuyển đổi, KES sẽ hỗ trợ các loại trừ được xác định là các tập tin riêng lẻ hoặc đường dẫn đến tập tin / thư mục. Nếu KSWS có các loại trừ được cấu hình làm khu vực định trước hoặc một tập lệnh URL, thì các loại trừ đó sẽ không được chuyển đổi. Sau khi chuyển đổi, bạn phải thêm các loại trừ đó theo cách thủ công.

  > Để đảm bảo Kaspersky Endpoint Security hoạt động đúng trên các máy chủ, bạn nên thêm các tập tin quan trọng cho hoạt động của máy chủ vào khu vực tin tưởng. Đối với máy chủ SQL, bạn phải thêm tập tin cơ sở dữ liệu MDF và LDF. Đối với máy chủ Microsoft Exchange, bạn phải thêm các tập tin CHK, EDB, JRS, LOG và JSL. Bạn có thể sử dụng tên đại diện, ví dụ: `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

  > Kể từ Kaspersky Endpoint Security 12.6 cho Windows, loại trừ quét và ứng dụng được tin tưởng được thêm vào khu vực tin tưởng. Các ứng dụng được tin tưởng và loại trừ quét được xác định trước giúp nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager. Điều này có nghĩa là bạn không cần thiết lập khu vực tin tưởng theo cách thủ công cho ứng dụng trên máy chủ.

- Tường lửa. Các chức năng của Tường lửa KSWS được thực hiện bởi Tường lửa cấp hệ thống. Trong KES, một thành phần riêng biệt chịu trách nhiệm cho chức năng Tường lửa. Sau khi chuyển đổi, bạn có thể cấu hình Tường lửa của Kaspersky Endpoint Security.

- Kaspersky Security Network. Kaspersky Endpoint Security không hỗ trợ cấu hình KSN cho các thành phần riêng lẻ. Kaspersky Endpoint Security sử dụng KSN cho tất cả các thành phần ứng dụng. Để sử dụng KSN, bạn phải chấp nhận các điều khoản và điều kiện mới của Tuyên bố Kaspersky Security Network.

- Kiểm soát Web. Các quy tắc chặn để kiểm soát danh mục lưu lượng truy cập web được chuyển sang một quy tắc chặn duy nhất trong Kaspersky Endpoint Security. Kaspersky Endpoint Security bỏ qua việc cho phép các quy tắc kiểm soát danh mục. Kaspersky Endpoint Security không hỗ trợ tất cả các danh mục của Kaspersky Security for Windows Server. Các danh mục không tồn tại trong Kaspersky Endpoint Security sẽ không được chuyển đổi. Do đó, các quy tắc phân loại tài nguyên web có các danh mục không được hỗ trợ sẽ không được chuyển đổi. Nếu cần, thêm quy tắc Kiểm soát web.

- Máy chủ proxy. Mật khẩu kết nối máy chủ proxy không được chuyển sang. Nhập mật khẩu được sử dụng để kết nối với máy chủ proxy theo cách thủ công.

- Lịch của các thành phần riêng lẻ. Kaspersky Endpoint Security không hỗ trợ cấu hình lịch cho các thành phần riêng lẻ. Các thành phần này luôn bật khi Kaspersky Endpoint Security đang hoạt động.

- Nhóm thành phần. Nhóm tính năng Kaspersky Endpoint Security khả dụng tùy thuộc vào loại hệ điều hành: máy trạm hoặc máy chủ. Ví dụ: trong số các công cụ mã hóa, chỉ có BitLocker Drive Encryption khả dụng trên máy chủ.

- Thuộc tính . Trạng thái của thuộc tính không được chuyển. Thuộc tính sẽ có giá trị mặc định. Theo mặc định, hầu hết tất cả các thiết lập trong chính sách mới đều có lệnh cấm áp dụng đối với việc sửa đổi thiết lập trong chính sách con và trong giao diện ứng dụng cục bộ. Thuộc tính đó có giá trị cho thiết lập chính sách trong mục **Managed Detection and Response (Industrial CyberSecurity)** và trong nhóm thiết lập **Hỗ trợ người dùng** (mục **Giao diện**). Nếu cần, hãy cấu hình kế thừa thiết lập từ chính sách cha.

- Làm việc với các mối đe dọa đang hoạt động. 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 phần mềm độc hại* và trong thiết lập ứng dụng.

- Nâng cấp ứng dụng. Để cài đặt các bản cập nhật và bản vá lớn mà không cần khởi động lại, bạn phải thay đổi chế độ nâng cấp ứng dụng. Theo mặc định, tính năng Cài đặt các bản cập nhật ứng dụng mà không cần khởi động lại bị tắt.

- Kaspersky Endpoint Agent. Kaspersky Endpoint Security có một tác nhân tích hợp để làm việc với các giải pháp Managed Detection and Response. Nếu cần, chuyển thiết lập chính sách Kaspersky Endpoint Agent sang chính sách Kaspersky Endpoint Security.

- Các tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*. Đảm bảo rằng các thiết lập của tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* đã được chuyển một cách chính xác. Thay vì ba tác vụ của KSWS, KES sử dụng một tác vụ KES duy nhất. Bạn có thể tối ưu hóa các tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* và loại bỏ các tác vụ không cần thiết.

- Các tác vụ khác. Các thành phần Kiểm soát ứng dụng, Kiểm soát thiết bị và Giám sát tính toàn vẹn của tập tin hoạt động khác nhau trong KSWS và KES. KES không sử dụng tác vụ *Baseline File Integrity Monitor*, *Applications Launch Control Generator*, *Rule Generator for Device Control*. Do đó, các tác vụ này không được chuyển. Sau khi chuyển, bạn có thể cấu hình các thành phần Giám sát tính toàn vẹn của tập tin, Kiểm soát ứng dụng, Kiểm soát thiết bị.

Chuyển vùng được tin tưởng của KSWS

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. Bạn có thể chuyển các đối tượng của vùng được tin tưởng từ KSWS sang KES bằng cách sử dụng *Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ* hoặc *trình hướng dẫn tạo chính sách KES mới dựa trên chính sách KSWS*. KSWS và KES có các bộ thành phần và tính năng khác nhau, vì vậy, sau khi chuyển, bạn phải xác minh rằng các loại trừ đáp ứng các yêu cầu bảo mật của công ty bạn. Các phương thức thêm loại trừ vào vùng được tin tưởng cũng khác nhau đối với KES và KSWS. Trình hướng dẫn chuyển đổi không có công cụ để chuyển tất cả các loại trừ KSWS. Điều này có nghĩa là sau khi chuyển đổi, bạn phải thêm một số loại trừ KSWS theo cách thủ công.

Để đảm bảo Kaspersky Endpoint Security hoạt động đúng trên các máy chủ, bạn nên thêm các tập tin quan trọng cho hoạt động của máy chủ vào khu vực tin tưởng. Đối với máy chủ SQL, bạn phải thêm tập tin cơ sở dữ liệu MDF và LDF. Đối với máy chủ Microsoft Exchange, bạn phải thêm các tập tin CHK, EDB, JRS, LOG và JSL. Bạn có thể sử dụng tên đại diện, ví dụ: `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

Kể từ Kaspersky Endpoint Security 12.6 cho Windows, loại trừ quét và ứng dụng được tin tưởng được thêm vào khu vực tin tưởng. Các ứng dụng được tin tưởng và loại trừ quét được xác định trước giúp nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager. Điều này có nghĩa là bạn không cần thiết lập khu vực tin tưởng theo cách thủ công cho ứng dụng trên máy chủ.

Phương thức tạo vùng được tin tưởng của KES và KSWS.

KSWS		KES
Object to scan		
• Predefined scope	*(không chuyển)*	
• Disk, folder or network location	→	**Tập tin hoặc thư mục**
• File	→	**Tập tin hoặc thư mục**
• Script file or web address	*(không chuyển)*	
Detected object	→	**Loại đối tượng được phát hiện**
Trusted processes	→	**Ứng dụng được tin tưởng**

Chuyển các đối tượng được quét

Các loại trừ của KSWS có phương thức **Object to scan** được chọn trong thuộc tính của chúng sẽ được chuyển sang loại trừ KES có phương thức **Tập tin hoặc thư mục** được lựa chọn trong thuộc tính của chúng, kèm một số hạn chế. Việc chuyển một loại trừ phụ thuộc vào phương thức lựa chọn đối tượng:

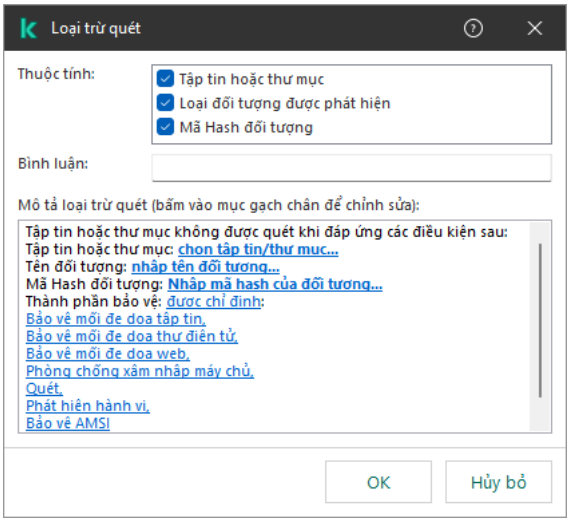
- Predefined scope – *không chuyển*.

  Sau khi chuyển đổi, bạn phải thêm các loại trừ đó theo cách thủ công. Các loại trừ dưới dạng khu vực được định trước phải được định cấu hình trong tác vụ *Quét phần mềm độc hại*.

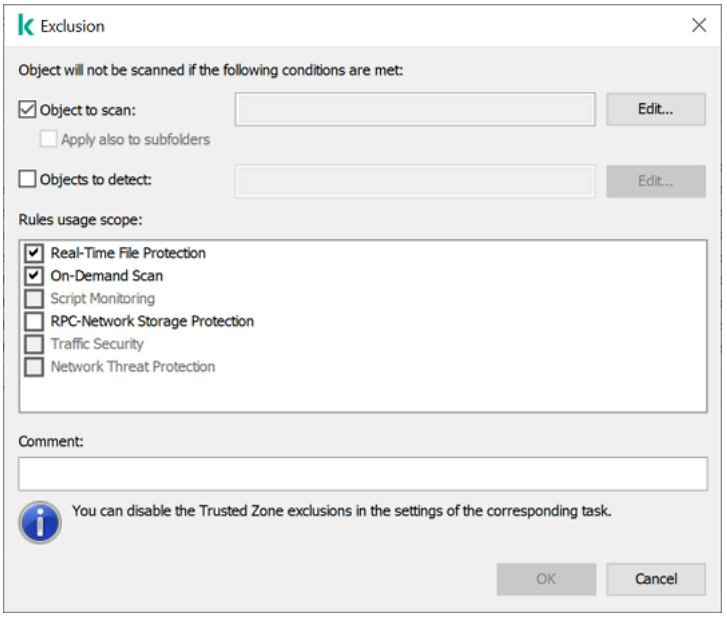
- Disk, folder or network location – chuyển sang loại trừ KES có phương thức "Tập tin hoặc thư mục" được chọn trong thuộc tính.
- File – chuyển sang loại trừ KES có phương thức "Tập tin hoặc thư mục" được chọn trong thuộc tính.
- Script file or web address – *không chuyển*.

  Sau khi chuyển đổi, bạn phải thêm các loại trừ đó theo cách thủ công. Các loại trừ dưới dạng địa chỉ web tập lệnh phải được thêm vào các địa chỉ web được tin tưởng cho Bảo vệ mối đe dọa web.

Nếu hộp kiểm **Apply also to subfolders** được chọn cho đối tượng được quét thì thiết lập này sẽ được chuyển sang loại trừ KES (hộp kiểm **Bao gồm các thư mục con**).



Thiết lập loại trừ KES



Thiết lập loại trừ KSWS

Chuyển các đối tượng được phát hiện

Các loại trừ của KSWS có phương thức **Detected object** được chọn trong thuộc tính của chúng sẽ được chuyển sang loại trừ KES có phương thức **Loại đối tượng được phát hiện** được lựa chọn trong thuộc tính của chúng. Tên của đối tượng được phát hiện tương ứng với phân loại của Bách khoa toàn thư của Kaspersky (Ví dụ: `Email-Worm`, `Rootkit` hoặc `RemoteAdmin`). Kaspersky Endpoint Security hỗ trợ chuỗi đại diện có dấu chấm hỏi `?` (khớp với bất kỳ một ký tự nào) và dấu hoa thị `*` (khớp với bất kỳ chuỗi ký tự nào).

Chuyển phạm vi sử dụng loại trừ

Phạm vi sử dụng của một loại trừ là một bộ thành phần mà loại trừ đó áp dụng. KES và KSWS có các bộ thành phần khác nhau do đó Trình hướng dẫn chuyển đổi không thể chuyển phạm vi sử dụng loại trừ. Do đó, nếu ít nhất một thành phần được chọn trong phạm vi sử dụng KSWS thì KES sẽ áp dụng loại trừ cho tất cả các thành phần ứng dụng.

Bạn có thể cấu hình phạm vi sử dụng KSWS trong thiết lập khu vực tin tưởng cũng như trong thiết lập của các thành phần bảo vệ KSWS. Để thực hiện, bạn có thể chọn hoặc xóa hộp kiểm **Apply Trusted Zone** trong phần tương ứng của chính sách. Thiết lập của các thành phần bảo vệ KES không bao gồm hộp kiểm như vậy. Điều này có nghĩa là trạng thái vùng được tin tưởng trong thiết lập của thành phần riêng lẻ sẽ bị mất khi chuyển. Sau khi hoàn tất quá trình chuyển đổi, hãy chọn các thành phần áp dụng loại trừ trong thiết lập vùng được tin tưởng trong chính sách KES.

Chuyển nhận xét

Nhận xét từ vùng được tin tưởng của KSWS được chuyển sang nhận xét loại trừ KES mà không sửa đổi.

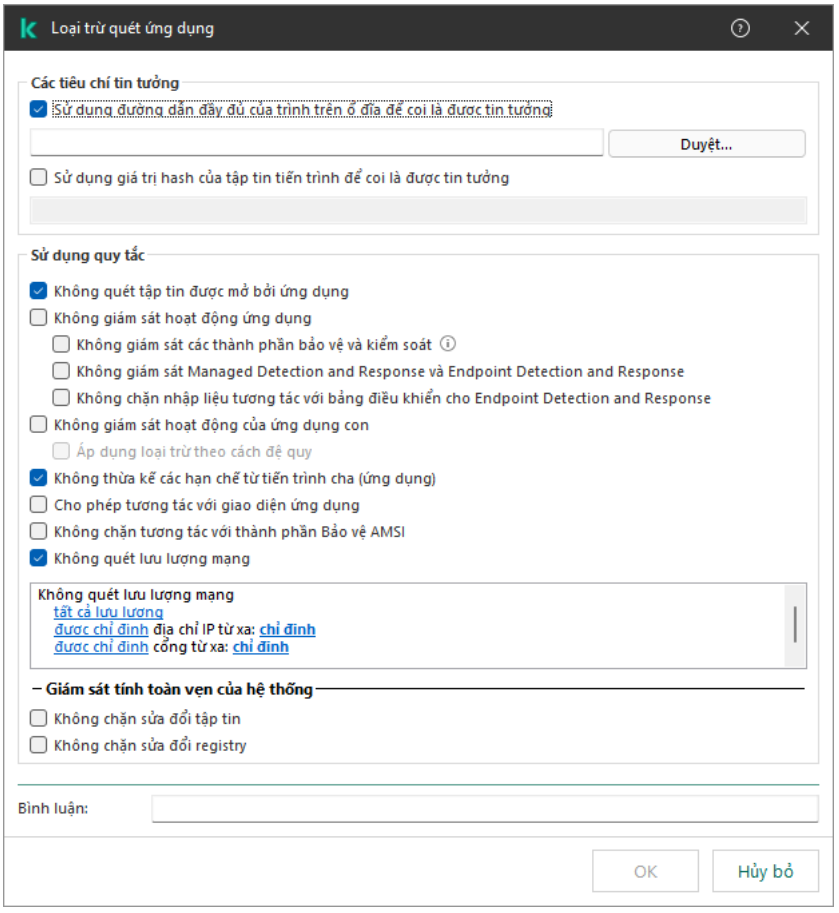
Chuyển các tiến trình được tin tưởng

Các tiến trình được tin tưởng của KSWS được chuyển sang các tiến trình được tin tưởng của KES kèm một số hạn chế. Việc chuyển các tiến trình được tin tưởng phụ thuộc vào phương thức chọn đối tượng:

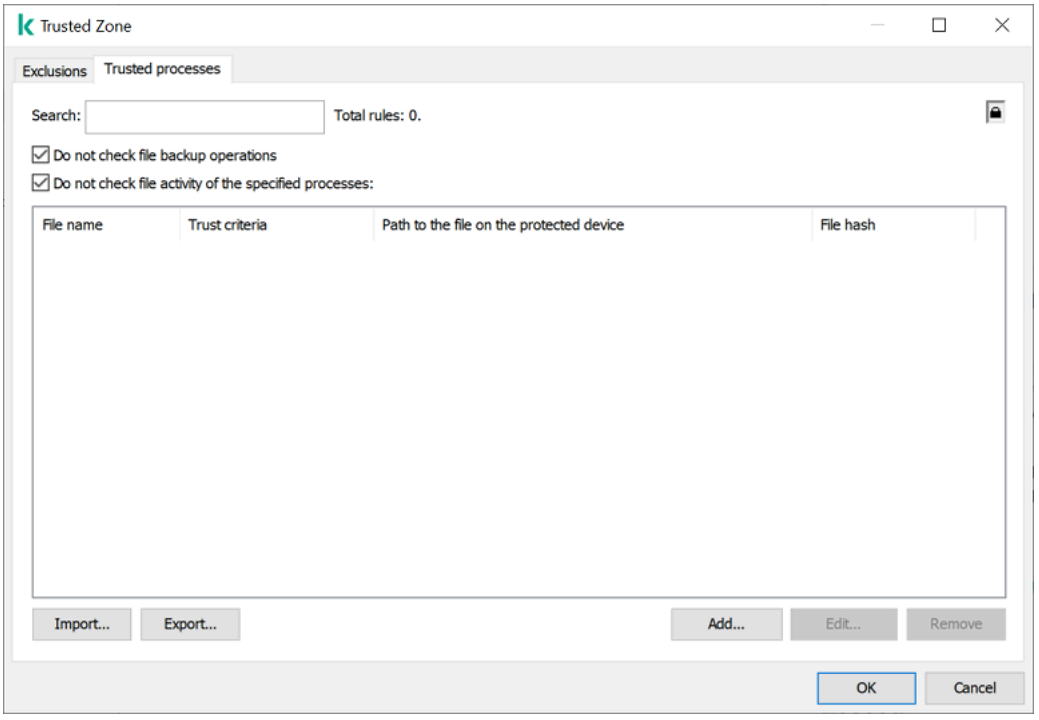
- Path to the file on the protected device – chuyển sang các ứng dụng được tin tưởng của KES.
- File hash – *không chuyển*.

Nếu KSWS có các tiến trình tin tưởng được cấu hình như hash tập tin thì các tiến trình tin tưởng đó sẽ không được chuyển đổi. Sau khi chuyển đổi, bạn phải thêm các tiến trình tin tưởng như vậy theo cách thủ công.

Nếu hộp kiểm **Do not check file backup operations** được chọn trong thiết lập tiến trình được tin tưởng thì thiết lập này sẽ được chuyển sang các ứng dụng được tin tưởng của KES (hộp kiểm **Không giám sát hoạt động ứng dụng**).



Thiết lập ứng dụng được tin tưởng của KES



Thiết lập tiến trình được tin tưởng của KSWS

Chuyển các quy tắc Kiểm soát khởi chạy ứng dụng KSWS

Kiểm soát khởi chạy ứng dụng KSWS bị chặn theo mặc định. Tức là Kiểm soát khởi chạy ứng dụng sẽ tự động chặn tất cả các ứng dụng không được chỉ định trong các ứng dụng được cho phép. Do đó, trình hướng dẫn chuyển đổi cho Kiểm soát ứng dụng KES sẽ tự động đặt chế độ kiểm soát **Danh sách được phép**, tương ứng với nguyên tắc chặn theo mặc định.

Bạn có thể chuyển các quy tắc từ KSWS sang KES bằng cách sử dụng *Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ* hoặc *trình hướng dẫn tạo chính sách KES mới dựa trên chính sách KSWS*.

Chuyển chế độ Kiểm soát khởi chạy ứng dụng

Chế độ Kiểm soát khởi chạy ứng dụng KSWS chuyển sang Kiểm soát ứng dụng KES như sau:

- **Statistics only → Kiểm tra quy tắc**;
- **Active → Áp dụng quy tắc**.

Chuyển các quy tắc định trước của Kiểm soát khởi chạy ứng dụng KSWS

Theo mặc định, Kiểm soát khởi chạy ứng dụng KSWS bao gồm hai quy tắc:

- **Allow scripts and MSI by OS-trusted certificate**
- **Allow executable by OS-trusted certificate**

Các quy tắc được định trước cho phép chạy *các tập lệnh*, *các gói MSI* và *tập tin thực thi* được ký bởi chứng chỉ gốc được tin tưởng. Nếu ít nhất một quy tắc KSWS được định sẵn có loại **Allow** thì trình hướng dẫn chuyển đổi sẽ tạo ra một quy tắc cho phép mới, **Applications with trusted root certificates**. Tức là Kiểm soát ứng dụng KES sẽ sử dụng một quy tắc duy nhất để cho phép chạy các tập lệnh, gói MSI và các tập tin thực thi được tin tưởng.

Nếu cả hai quy tắc KSWS được định sẵn đều có loại **Deny** thì KES sẽ bỏ qua các quy tắc được định sẵn.

Chuyển các quy tắc tùy chỉnh của Kiểm soát khởi chạy ứng dụng KSWS

Các quy tắc Kiểm soát khởi chạy ứng dụng KSWS sẽ điều chỉnh thực thi các tập tin theo các tiêu chí sau:

- chữ ký có chứng chỉ số;
- hash SHA256;
- đường dẫn đến tập tin.

Các quy tắc được tạo theo cách khác nhau trong KSWS và KES, do đó trình hướng chuyển đổi sẽ tạo *các danh mục ứng dụng*, bao gồm các điều kiện và loại trừ khỏi các quy tắc KSWS và thêm các danh mục ứng dụng này vào các quy tắc KES. Trình hướng dẫn sử dụng các điều kiện **Chứng chỉ**, **Đường dẫn thư mục** và **Giá trị băm tập tin** trong các loại ứng dụng. Các danh mục ứng dụng mới có trong Bảng điều khiển quản trị Kaspersky Security Center trong phần **Application management → Application categories**.

Trình hướng dẫn chuyển đổi sẽ nhóm các quy tắc KSWS theo loại và theo người dùng. Tiếp theo, trình hướng dẫn sẽ tạo các danh mục ứng dụng, bao gồm các điều kiện và loại trừ khỏi các quy tắc KSWS và thêm các danh mục ứng dụng vào các quy tắc KES mới. Trình hướng dẫn sẽ chỉ định tên của các quy tắc KSWS trong trường **Mô tả** của quy tắc KES.

Chuyển các thiết lập nâng cao của Kiểm soát khởi chạy ứng dụng của KSWS

Nguyên lý hoạt động của Kiểm soát khởi chạy ứng dụng của KSWS và Kiểm soát ứng dụng của KES là khác nhau nên trình hướng dẫn chuyển đổi có thể chuyển một nhóm nhỏ các thiết lập.

Thiết lập Kiểm soát khởi chạy ứng dụng

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Repeat action taken for the first file launch on all the subsequent launches for this file	*(không chuyển)* Kaspersky Endpoint Security sẽ quét ứng dụng mỗi khi ứng dụng cố gắng chạy.
Deny the command interpreters launch with no command to execute	*(không chuyển)* Kaspersky Endpoint Security cho phép chạy trình thông dịch lệnh nếu chúng không bị thành phần Kiểm soát ứng dụng cấm.
Apply rules to executable files	*(không chuyển)* Không thể cấu hình phạm vi áp dụng quy tắc trong thiết lập Kiểm soát ứng dụng KES. Kiểm soát ứng dụng KES sẽ áp dụng các quy tắc cho tất cả các loại tập tin: tập tin thực thi, tập lệnh và gói MSI. Nếu tất cả các loại tập tin được thêm trong phạm vi áp dụng quy tắc trong KSWS, thì trong quá trình di chuyển, KES sẽ thực hiện các quy tắc KSWS. Nếu một số loại tập tin bị loại trừ khỏi phạm vi áp dụng quy tắc trong KSWS, thì trong quá trình di chuyển KES cũng chuyển các quy tắc KSWS, nhưng **Kiểm tra quy tắc** sẽ được chọn làm hành động Kiểm soát ứng dụng.
Monitor loading of DLL modules	**Giám sát việc tải các mô-đun DLL (tăng mức tải đáng kể lên hệ thống)**
Apply rules to scripts and MSI packages	*(không chuyển)* Không thể cấu hình phạm vi áp dụng quy tắc trong thiết lập Kiểm soát ứng dụng KES. Kiểm soát ứng dụng KES sẽ áp dụng các quy tắc cho tất cả các loại tập tin: tập tin thực thi, tập lệnh và gói MSI. Nếu tất cả các loại tập tin được thêm trong phạm vi áp dụng quy tắc trong KSWS, thì trong quá trình di chuyển, KES sẽ thực hiện các quy tắc KSWS. Nếu một số loại tập tin bị loại trừ khỏi phạm vi áp dụng quy tắc trong KSWS, thì trong quá trình di chuyển KES sẽ chuyển các quy tắc KSWS, nhưng **Kiểm tra quy tắc** sẽ được chọn làm hành động Kiểm soát ứng dụng.

Thiết lập Kaspersky Security for Windows Server	Thiết lập Kaspersky Endpoint Security cho Windows
Deny applications untrusted by KSN	*(không chuyển)* Kaspersky Endpoint Security không xem xét danh tiếng của các ứng dụng và cho phép hoặc từ chối các ứng dụng đang chạy theo các quy tắc.
Allow applications trusted by KSN	Trong quá trình di chuyển, KES sẽ thêm một quy tắc cho phép mới. Danh mục KL **Phần mềm khác\Các ứng dụng được tin tưởng theo danh tiếng trong KSN** được chỉ định làm điều kiện kích hoạt quy tắc.
Users and / or user groups allowed to run applications trusted by KSN	**Người dùng và quyền của họ** trong một quy tắc cho phép Kiểm soát ứng dụng bao gồm danh mục KL **Phần mềm khác\Các ứng dụng được tin tưởng theo danh tiếng trong KSN**.
Automatically allow software distribution via applications and packages listed	Kiểm soát phân phối phần mềm trong KSWS và KES hoạt động khác nhau. Trong quá trình di chuyển, KES sẽ bổ sung các quy tắc cho phép mới cho các ứng dụng được phép phân phối phần mềm tự động. Giá trị băm tập tin được chỉ định làm điều kiện kích hoạt quy tắc.
Always allow software distribution via Windows Installer	Kiểm soát phân phối phần mềm trong KSWS và KES hoạt động khác nhau. Trong quá trình di chuyển, KES sẽ bổ sung các quy tắc cho phép mới cho các ứng dụng được phép phân phối phần mềm tự động (**Software distribution applications and packages allowed**). Giá trị băm tập tin được chỉ định làm điều kiện kích hoạt quy tắc. Trong thuộc tính tài khoản, hộp kiểm **Trình cập nhật được tin tưởng** được chọn.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(không chuyển)*
Software distribution applications and packages allowed	Kiểm soát phân phối phần mềm trong KSWS và KES hoạt động khác nhau. Trong quá trình di chuyển, KES sẽ bổ sung các quy tắc cho phép mới cho các ứng dụng được phép phân phối phần mềm tự động. Giá trị băm tập tin được chỉ định làm điều kiện kích hoạt quy tắc. Trong thuộc tính tài khoản, hộp kiểm **Trình cập nhật được tin tưởng** được chọn.
Schedule settings	*(không chuyển)* Nếu lịch được cấu hình cho thành phần trong cài đặt KSWS thì thành phần Kiểm soát ứng dụng sẽ được bật khi di chuyển. Nếu lịch không được cấu hình cho thành phần trong cài đặt KSWS thì thành phần Kiểm soát ứng dụng sẽ bị tắt khi di chuyển. Không thể cấu hình lịch riêng cho thành phần. Thành phần này luôn bật khi Kaspersky Endpoint Security đang hoạt động.

Cài đặt KES thay vì KSWS

Bạn có thể cài đặt Kaspersky Endpoint Security theo các cách sau:

- Cài đặt KES sau khi gỡ bỏ KSWS (khuyên dùng).
- Cài đặt KES trên KSWS.

Gỡ bỏ Kaspersky Security for Windows Server

Bạn có thể gỡ bỏ ứng dụng từ xa bằng cách sử dụng tác vụ *Uninstall application remotely* hoặc gỡ bỏ cục bộ trên máy chủ. Bạn có thể cần phải khởi động lại máy chủ sau khi gỡ bỏ KSWS. Nếu bạn muốn cài đặt Kaspersky Endpoint Security mà không cần khởi động lại, hãy đảm bảo rằng Kaspersky Security for Windows Server được gỡ bỏ hoàn toàn. Nếu ứng dụng không được gỡ bỏ hoàn toàn, việc cài đặt Kaspersky Endpoint Security có thể khiến máy chủ hoạt động trục trặc. Bạn cũng nên đảm bảo rằng ứng dụng đã được gỡ bỏ hoàn toàn nếu bạn đã sử dụng tiện ích kavremover. Tiện ích kavremover không hỗ trợ quản lý KSWS.

Nếu Bảo vệ bằng mật khẩu được bật để hạn chế quyền truy cập vào KSWS, hãy nhập mật khẩu gỡ bỏ vào thiết lập cho gói cài đặt KES.

Sau khi gỡ bỏ KSWS, hãy cài đặt Kaspersky Endpoint Security cho Windows bằng bất kỳ phương thức nào khả dụng.

Cài đặt Kaspersky Endpoint Security

Khi bạn cài đặt KES từ xa, các thành phần mà bạn đã chọn trong thuộc tính gói cài đặt sẽ được cài đặt trên máy chủ. Chúng tôi khuyến nghị bạn nên chọn các thành phần mặc định trong thuộc tính gói cài đặt. Không cần khởi động lại khi cài đặt KES lên trên KSWS.

Trước khi cài đặt cục bộ, Kaspersky Endpoint Security sẽ kiểm tra máy tính để xác định sự hiện diện của các ứng dụng Kaspersky. Nếu Kaspersky Security for Windows Server được cài đặt trên máy tính, KES sẽ phát hiện bộ thành phần KSWS đã được cài đặt và chọn các thành phần giống nhau để cài đặt. Không cần khởi động lại khi cài đặt KES lên trên KSWS.

Nếu cài đặt KES lên trên KSWS không thành công, bạn có thể hoàn tác quá trình cài đặt. Sau khi hoàn tác quá trình cài đặt, bạn nên khởi động lại máy chủ và thử lại.

Thiết lập và tác vụ KSWS không được chuyển đổi khi Kaspersky Endpoint Security cho Windows được cài đặt. Để chuyển đổi thiết lập và tác vụ, hãy chạy Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ.

Bạn có thể kiểm tra danh sách các thành phần đã cài đặt trong phần **Bảo mật** của giao diện ứng dụng, sử dụng lệnh `status` hoặc trong bảng điều khiển Kaspersky Security Center trong thuộc tính máy tính. Bạn có thể thay đổi nhóm thành phần sau khi cài đặt bằng cách sử dụng *Thay đổi thành phần ứng dụng*.

Chuyển cấu hình [KSWS+KEA] sang cấu hình [KES+built-in agent]

Một tác nhân tích hợp đã được thêm vào ứng dụng để hỗ trợ sử dụng Kaspersky Endpoint Security cho Windows như một phần của EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA và MDR. Bạn không còn cần một ứng dụng Kaspersky Endpoint Agent riêng để hoạt động với các giải pháp này.

Khi chuyển từ KSWS sang KES, các giải pháp EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA và MDR sẽ tiếp tục hoạt động với các tác nhân tích hợp của Kaspersky Endpoint Security. Ngoài ra, Kaspersky Endpoint Agent sẽ bị gỡ bỏ khỏi máy tính.

Việc chuyển cấu hình [KSWS+KEA] sang [KES+tác nhân tích hợp] liên quan đến các bước sau:

1. **Chuyển từ KSWS sang KES**

   Chuyển từ KSWS sang KES liên quan đến cài đặt Kaspersky Endpoint Security thay vì Kaspersky Security for Windows Server.

   Quản trị viên thường bật Bảo vệ bằng mật khẩu để hạn chế quyền truy cập KSWS và KEA. Kể từ Kaspersky Security Center Linux 15.1, bạn có thể nhập mật khẩu gỡ bỏ ứng dụng trong thiết lập tác vụ *Install application remotely*. Tac svụ này chỉ cho phép nhập một mật khẩu gỡ bỏ. Tức là, nếu đặt cùng một mật khẩu cho KSWS và KEA thì các ứng dụng KSWS và KEA sẽ được gỡ bỏ thành công. Nếu mật khẩu khác nhau, việc gỡ bỏ một trong các ứng dụng sẽ không thành công do lỗi truy cập. Để hoàn tất quá trình chuyển đổi, bạn phải tắt Bảo vệ bằng mật khẩu cho ứng dụng có mật khẩu mà bạn không thể nhập trong thiết lập của tác vụ *Install application remotely*.

   Để thực hiện việc chuyển đổi, bạn phải chọn các thành phần cần thiết để hỗ trợ các giải pháp Detection and Response như một phần của Kaspersky Endpoint Security. Sau khi cài đặt ứng dụng, Kaspersky Endpoint Security sẽ chuyển sang sử dụng tác nhân tích hợp và gỡ bỏ Kaspersky Endpoint Agent.

2. **Chuyển chính sách và các tác vụ**

   Chuyển chính sách và tác vụ [KSWS+KEA] sang [KES+tác nhân tích hợp] liên quan đến các bước sau:

   1. Chuyển các chính sách và tác vụ từ KSWS sang KES bằng Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ (chỉ khả dụng trên Bảng điều khiển quản trị (MMC)).

      Kết quả là, một hồ sơ chính sách có tên *UpgradedFromKSWS <Tên của chính sách Kaspersky Security for Windows Server>* sẽ được thêm vào chính sách KES. Các tác vụ KES mới cũng được tạo bằng tên *<tên tác vụ KSWS> (được chuyển đổi)*.

   2. Chuyển các chính sách và tác vụ từ KEA sang KES bằng trình hướng dẫn chuyển đổi từ Kaspersky Endpoint Agent (chỉ khả dụng trong Bảng điều khiển web và Bảng điều khiển đám mây).

      Kết quả là, một chính sách mới được tạo với tên *<Tên của chính sách Kaspersky Endpoint Security> & <Tên của chính sách Kaspersky Endpoint Agent>*. Các tác vụ mới và tác vụ KES cũng được tạo.

3. **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 Tiện ích bổ trợ 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 *Add key*.

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.

Chỉ có thể sử dụng giấy phép Kaspersky Anti Targeted Attack Platform để kích hoạt Kaspersky Endpoint Security như một phần của giải pháp Kaspersky Anti Targeted Attack Platform. Sau khi bạn nâng cấp ứng dụng lên phiên bản 12.1, chức năng EDR (KATA) sẽ được kích hoạt tự động. Bạn không cần phải làm gì khác.

4. **Kiểm tra tình trạng của Kaspersky Endpoint Detection and Response Optimum và Kaspersky Sandbox**

   Nếu sau khi nâng cấp, máy tính có trạng thái *Critical* trong bảng điều khiển Kaspersky Security Center:

   - Đảm bảo rằng máy tính được cài đặt Network Agent phiên bản 13.2 trở lên.
   - Kiểm tra trạng thái hoạt động của tác nhân tích hợp bằng cách xem *Report on status of application components*. Nếu một thành phần có trạng thái *Not installed* thì hãy cài đặt thành phần này bằng cách sử dụng tác vụ *Change application components*.
   - 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 *Report on status of application components*. 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.

Đảm bảo rằng Kaspersky Security for Windows Server đã được gỡ bỏ thành công

Đảm bảo rằng Kaspersky Security for Windows Server đã được gỡ bỏ hoàn toàn:

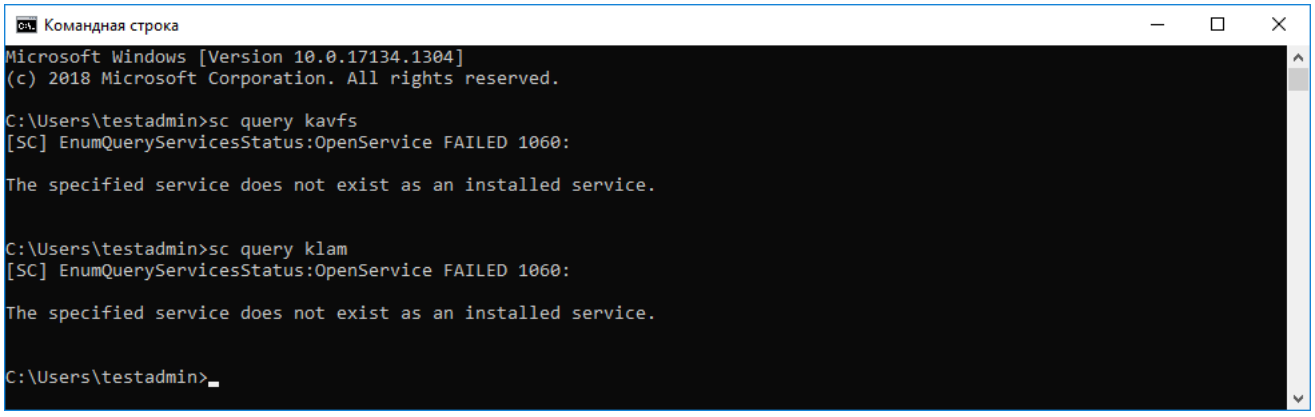
- Thư mục `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\` không tồn tại.
- Các dịch vụ sau không hiện diện:
  - Kaspersky Security Service (KAVFS)
  - Dịch vụ Kaspersky Security Management (KAVFSGT)

- Dịch vụ Kaspersky Security Exploit Prevention (KAVFSSLP)
- Dịch vụ Kaspersky Security Script Checker (KAVFSSCS)

Bạn có thể kiểm tra các dịch vụ đang chạy trong Trình quản lý tác vụ hoặc bằng cách thực thi lệnh `sc query` (xem hình bên dưới).

- Các trình điều khiển sau đây không hiện diện:
  - 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 thực thi lệnh `sc query`. Nếu thiếu một dịch vụ hoặc trình điều khiển thì bạn sẽ nhận được phản hồi sau đây:



Đảm bảo các dịch vụ và trình điều khiển của Kaspersky Security for Windows Server đã được gỡ bỏ thành công

Nếu các tập tin ứng dụng hoặc trình điều khiển vẫn còn trên máy chủ, hãy xóa các tập tin liên quan theo cách thủ công. Nếu các dịch vụ Kaspersky Security for Windows Server vẫn đang chạy trên máy chủ, hãy dừng (`sc stop`) và xóa (`sc delete`) các dịch vụ 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 for Windows Server (KSWS). Quá trình kích hoạt sau khi chuyển đổi phụ thuộc vào phương thức kích hoạt KSWS (xem bảng bên dưới).

Kaspersky Endpoint Security không hỗ trợ *Giấy phép Kaspersky Security for Storage*. Để làm việc với giấy phép này, bạn cần sử dụng Kaspersky Security for Windows Server.

Bạn chỉ có thể sử dụng mã kích hoạt để kích hoạt KES bằng khóa KSWS. Nếu bạn đang sử dụng tập tin khóa để kích hoạt ứng dụng, bạn cần liên hệ với bộ phận Hỗ trợ kỹ thuật để nhận tập tin khóa Kaspersky Endpoint Security.

Kích hoạt Kaspersky Endpoint Security cho Windows bằng khóa của Kaspersky Security for Windows Server

Phương thức kích hoạt Kaspersky Security for 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 được thêm vào bởi một tác vụ.	Nếu KSWS của bạn được kích hoạt bằng tác vụ đó 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.
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.
Ảnh máy ảo trả phí (Amazon Machine Image – AMI) trong Amazon Web Services (AWS).	Nếu bạn đã mua Kaspersky Security Center dưới dạng ảnh máy ảo trả phí (Amazon Machine Image – AMI) trong Amazon Web Services (AWS) thì bạn không cần kích hoạt KES. Trong trường hợp này, Kaspersky Security Center sẽ sử dụng gói đăng ký AWS đã được thêm vào ứng dụng.
Ảnh Kaspersky Security Center miễn phí được tạo sẵn kèm giấy phép của riêng bạn (mô hình Bring Your Own License – BYOL).	Nếu bạn đang sử dụng ảnh Kaspersky Security Center miễn phí sẵn dùng kèm giấy phép của riêng bạn trong môi trường đám mây (mô hình Bring Your Own License – BYOL) thì bạn phải kích hoạt ứng dụng bằng bất kỳ phương pháp khả dụng nào. Bạn sẽ cần một giấy phép Kaspersky Hybrid Cloud Security.

Các cân nhắc đặc biệt để chuyển các máy chủ có mức tải cao

Trên các máy chủ có mức tải cao, điều quan trọng là phải theo dõi hiệu năng và tránh lỗi. Sau khi chuyển sang Kaspersky Endpoint Security cho Windows, bạn nên tạm thời tắt các thành phần ứng dụng sử dụng nhiều tài nguyên máy chủ so với các thành phần khác. Sau khi đảm bảo rằng máy chủ đang hoạt động như bình thường, bạn có thể bật lại các thành phần của ứng dụng.

Bạn nên chuyển các máy chủ có mức tải cao như sau:

1. Tạo chính sách Kaspersky Endpoint Security với 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.

2. Trong thiết lập chính sách, hãy tắt các thành phần sau: Bảo vệ mối đe dọa mạng, Phát hiện hành vi, Phòng chống khai thác, Công cụ khắc phục, Kiểm soát ứng dụng.

   Nếu tổ chức của bạn đã triển khai giải pháp Kaspersky Managed Detection and Response (MDR), hãy tải tập tin cấu hình BLOB lên chính sách Kaspersky Endpoint Security.

3. Gỡ bỏ Kaspersky Security for Windows Server khỏi máy chủ.

4. Cài đặt Kaspersky Endpoint Security cho Windows với nhóm thành phần mặc định.

   Nếu tổ chức của bạn đã triển khai các giải pháp Detection and Response, hãy chọn các thành phần liên quan trong thuộc tính của gói cài đặt.

5. Kiểm tra thiết lập của ứng dụng:

   - Ứng dụng được kích hoạt bằng khóa giấy phép KSWS.
   - Chính sách mới được áp dụng. Các thành phần đã chọn trước đó bị tắt.

6. Đảm bảo máy chủ đang hoạt động. Đảm bảo rằng Kaspersky Endpoint Security cho Windows không sử dụng trên 1% tài nguyên của máy chủ.

7. Nếu cần, tạo loại trừ quét, thêm các ứng dụng được tin tưởng, tạo danh sách các địa chỉ web được tin tưởng.

8. Bật các thành phần Phát hiện hành vi, Phòng chống khai thác, Công cụ khắc phục. Đảm bảo rằng Kaspersky Endpoint Security cho Windows không sử dụng trên 1% tài nguyên của máy chủ.

9. Bật thành phần Bảo vệ mối đe dọa mạng. Đảm bảo rằng Kaspersky Endpoint Security cho Windows không sử dụng trên 2% tài nguyên của máy chủ.

10. Bật thành phần Kiểm soát ứng dụng trong chế độ kiểm tra quy tắc.

11. Đảm bảo thành phần Kiểm soát ứng dụng đang hoạt động. Nếu cần, thêm quy tắc Kiểm soát ứng dụng mới và tắt chế độ kiểm tra quy tắc sau khi xác nhận rằng thành phần Kiểm soát ứng dụng đang hoạt động.

Sau khi chuyển từ KSWS sang KES, hãy đảm bảo rằng ứng dụng đang hoạt động đúng. Kiểm tra trạng thái của máy chủ trong bảng điều khiển (nên có trạng thái *OK*). Đảm bảo không có lỗi nào được báo cáo cho ứng dụng, đồng thời kiểm tra thời gian kết nối lần cuối với Máy chủ quản trị, thời điểm cập nhật cơ sở dữ liệu lần cuối và trạng thái bảo vệ máy chủ.

Quản lý ứng dụng trên máy chủ ở chế độ Server Core

Máy chủ ở chế độ Server 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 ở chế độ Server 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 ở chế độ Server 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 ở chế độ Server Core liên quan đến các lưu ý đặc biệt sau:

- Máy chủ ở chế độ Server 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 phần mềm độc hại*. Sau đó bạn cần khởi chạy tác vụ *Quét phần mềm độc hại*.

- 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 trên máy chủ ở chế độ Core Server, 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 <activation code or key file>
```

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
```

Chuyển từ [KSWS+KEA] sang [KES+tác nhân tích hợp]

Khi chuyển từ Kaspersky Security for Windows Server (KSWS) sang Kaspersky Endpoint Security (KES), bạn có thể sử dụng các đề xuất sau để cấu hình bảo vệ máy chủ và tối ưu hóa hiệu năng. Ở đây chúng ta sẽ xem xét một ví dụ về quá trình chuyển đổi cho một tổ chức.

Cơ sở hạ tầng của tổ chức

Công ty đã lắp đặt các thiết bị sau:

- Kaspersky Security Center 14.2

  Quản trị viên quản lý các giải pháp của Kaspersky bằng Bảng điều khiển quản trị (MMC). Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) cũng được kiểm tra

  Trong Kaspersky Security Center, ba nhóm quản trị sẽ được tạo, chứa các máy chủ của tổ chức: hai nhóm quản trị dành cho máy chủ SQL và một nhóm quản trị dành cho máy chủ Microsoft Exchange. Mỗi nhóm quản trị được quản lý bởi chính sách riêng của mình. Tác vụ *Database Update* và *On-demand scan* được tạo ra cho tất cả các máy chủ trong tổ chức.

  Khóa kích hoạt KSWS sẽ được thêm vào Kaspersky Security Center. Phân phối khóa tự động được bật.

- Các máy chủ SQL được cài đặt Kaspersky Security for Windows Server 11.0.1 và Kaspersky Endpoint Agent 3.11. Các máy chủ SQL được kết hợp thành hai cụm.

  KSWS được quản lý bởi chính sách *SQL_Policy(1)* và *SQL_Policy(2)*. Tác vụ *Database Update*, *On-demand scan* cũng sẽ được tạo ra.

- Máy chủ Microsoft Exchange được cài đặt Kaspersky Security for Windows Server 11.0.1 và Kaspersky Endpoint Agent 3.11.

  KSWS được quản lý bởi chính sách *Exchange_Policy*. Tác vụ *Database Update*, *On-demand scan* cũng sẽ được tạo ra.

Lập kế hoạch chuyển đổi

Quá trình chuyển đổi bao gồm các bước sau:

1. Chuyển các tác vụ và chính sách KSWS bằng Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ.
2. Chuyển chính sách Kaspersky Endpoint Agent bằng Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ.
3. Sử dụng thẻ để kích hoạt các bộ cấu hình chính sách trong thuộc tính của chính sách mới.
4. Cài đặt KES thay vì KSWS.
5. Kích hoạt EDR Optimum.
6. Xác nhận rằng KES đang hoạt động.

Kịch bản chuyển đổi ban đầu được thực hiện trên một trong các cụm máy chủ SQL. Sau đó, kịch bản chuyển đổi được thực hiện trên cụm máy chủ SQL khác. Sau đó, kịch bản chuyển đổi được thực hiện trên Microsoft Exchange.

Chuyển các tác vụ và chính sách KSWS bằng Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ

Để chuyển các tác vụ KSWS, bạn có thể sử dụng Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ (trình hướng dẫn chuyển đổi). Kết quả là, thay vì chính sách *SQL_Policy(1)*, *SQL_Policy(2)* và *Exchange_Policy*, bạn sẽ nhận được một chính sách với ba bộ cấu hình tương ứng cho các máy chủ SQL và Microsoft Exchange. Bộ cấu hình chính sách mới có thiết lập KSWS sẽ được đặt tên *UpgradedFromKSWS <Tên chính sách Kaspersky Security for Windows Server>*. Trong thuộc tính cấu hình, trình hướng dẫn chuyển đổi sẽ tự động chọn thẻ thiết bị `UpgradedFromKSWS` làm tiêu chí kích hoạt. Do đó, các thiết lập từ bộ cấu hình chính sách sẽ tự động được áp dụng cho các máy chủ.

Chuyển chính sách Kaspersky Endpoint Agent bằng Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ

Để chuyển các chính sách của Kaspersky Endpoint Agent, bạn có thể sử dụng Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ. Trình hướng dẫn chuyển đổi chính sách và tác vụ cho Kaspersky Endpoint Agent chỉ khả dụng trong Bảng điều khiển web.

Sử dụng thẻ để kích hoạt các bộ cấu hình chính sách trong thuộc tính của chính sách mới

Chọn thẻ thiết bị mà bạn đã chỉ định trước đó làm điều kiện kích hoạt cấu hình. Mở thuộc tính chính sách và chọn *General rules for policy profile activation* làm điều kiện kích hoạt cấu hình.

Cài đặt KES thay vì KSWS

Trước khi cài đặt KES, bạn phải tắt Bảo vệ bằng mật khẩu trong thuộc tính chính sách KSWS.

Việc cài đặt KES bao gồm các bước sau:

1. Chuẩn bị gói cài đặt. Trong thuộc tính gói cài đặt, hãy chọn gói phân phối Kaspersky Endpoint Security cho Windows 12.0 và chọn nhóm thành phần mặc định.

2. Tạo một tác vụ *Install application remotely* cho một trong các nhóm quản trị máy chủ SQL.

3. Trong thuộc tính tác vụ, hãy chọn gói cài đặt và tập tin khóa cấp phép.

4. Chờ cho đến khi nhiệm vụ hoàn tất thành công.

5. Lặp lại quá trình cài đặt KES cho các nhóm quản trị còn lại.

Kaspersky Security Center sẽ tự động thêm thẻ `UpgradedFromKSWS` vào tên của các máy tính trên bàn điều khiển sau khi cài đặt KES hoàn tất.

Để kiểm tra quá trình cài đặt KES, bạn có thể sử dụng *Report on protection deployment*. Bạn cũng có thể kiểm tra trạng thái thiết bị. Để xác nhận kích hoạt ứng dụng, bạn có thể sử dụng *Report on usage of license keys*.

Kích hoạt EDR Optimum

Bạn có thể kích hoạt chức năng EDR Optimum bằng giấy phép Tiện ích bổ trợ Kaspersky Endpoint Detection and Response Optimum độc lập. Bạn phải xác nhận rằng khóa EDR Optimum đã được thêm vào kho lưu trữ của Kaspersky Security Center và chức năng phân phối khóa giấy phép tự động được bật.

Để kiểm tra kích hoạt EDR Optimum, bạn có thể sử dụng *Report on status of application components*.

Xác nhận rằng KES đang hoạt động

Để xác nhận rằng KES đang hoạt động, bạn có thể kiểm tra và thấy không có lỗi nào được báo cáo. Trạng thái thiết bị phải là *OK*. Các tác vụ quét phần mềm độc hại và cập nhật đã hoàn tất thành công.

Chế độ Light Agent để bảo vệ máy ảo

Kể phiên bản 12.8, bạn có thể sử dụng Kaspersky Endpoint Security cho Windows như một phần của Kaspersky Security for Virtualization Light Agent. *Kaspersky Security for Virtualization Light Agent* là giải pháp tích hợp, cung cấp khả năng bảo vệ toàn diện cho máy ảo trước nhiều loại mối đe dọa bảo mật thông tin, tấn công mạng và tấn công lừa đảo. Để sử dụng giải pháp này, bạn phải cài đặt ứng dụng ở chế độ Light Agent.

Cài đặt Kaspersky Endpoint Security ở chế độ Light Agent trên máy ảo dựa trên kiến trúc Arm hiện không được hỗ trợ.

Bạn có thể sử dụng Kaspersky Endpoint Security ở chế độ Light Agent như một phần của Kaspersky Security for Virtualization Light Agent kể từ phiên bản 6.2.

Khi bạn khởi động Light Agent, chế độ này sẽ thiết lập và duy trì kết nối với máy ảo SVM (Secure Virtual Machine). Một Máy chủ bảo vệ được triển khai trên SVM. *Máy chủ bảo vệ* là thành phần của giải pháp Kaspersky Security for Virtualization Light Agent, có khả năng quét các tập tin để tìm virus và phần mềm độc hại khác, cập nhật cơ sở dữ liệu diệt virus và quản lý khóa cấp phép. Light Agent sẽ gửi các tập tin hoặc phân đoạn tập tin cần quét tới SVM. Kết quả quét có sẵn cho tất cả các máy ảo được cài đặt Light Agent (công nghệ SharedCache). Công nghệ này làm tăng hiệu quả giải pháp và phản ứng nhanh hơn với các mối đe dọa.

Cơ sở hạ tầng của tổ chức có thể chứa nhiều máy ảo được cài đặt Light Agent và nhiều SVM. Máy chủ tích hợp xử lý tương tác giữa các máy ảo và SVM. *Máy chủ tích hợp* - một thành phần của giải pháp Kaspersky Security for Virtualization Light Agent, giúp tạo danh sách các SVM khả dụng và chuyển dữ liệu này tới Light Agent, tham gia vào quá trình khám phá SVM của Light Agent, bảo vệ kết nối giữa Light Agent và SVM và thực hiện các chức năng khác.

Những cân nhắc đặc biệt cho chế độ Light Agent

Bạn có thể quản lý Kaspersky Endpoint Security ở Chế độ tiêu chuẩn và chế độ Light Agent bằng cách sử dụng các chính sách và tác vụ Kaspersky Endpoint Security. Ở chế độ Light Agent, một số thành phần và tính năng của ứng dụng không khả dụng.

Cập nhật cơ sở dữ liệu và các mô-đun phần mềm ứng dụng

Kaspersky Endpoint Security ở chế độ Light Agent sử dụng cơ sở dữ liệu phần mềm độc hại đặc biệt mà ứng dụng cần khi hoạt động như một phần của giải pháp Kaspersky Security for Virtualization Light Agent. Kaspersky Endpoint Security nhận các bản cập nhật cơ sở dữ liệu và mô-đun ứng dụng từ Máy chủ bảo vệ.

Cơ sở dữ liệu và mô-đun trên các máy ảo được bảo vệ được cập nhật bằng cách sử dụng một tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*, trong đó một thư mục trên SVM được chỉ định là nguồn cập nhật. Light Agent tự động chạy tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*. Bạn không thể chọn nguồn cập nhật khác, cấu hình lịch tác vụ hoặc xóa tác vụ.

Việc khôi phục bản cập nhật cơ sở dữ liệu phần mềm độc hại mới nhất cũng được xử lý ở phía Máy chủ bảo vệ. Sau khi khôi phục cơ sở dữ liệu và cập nhật mô-đun ứng dụng trên SVM, một tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* cục bộ đặc biệt được bắt đầu trên máy ảo được bảo vệ. Tác vụ này khiến Light Agent quay lại sử dụng bộ cơ sở dữ liệu phần mềm độc hại trước đó.

Kaspersky Endpoint Security ở chế độ Light Agent không hỗ trợ tác vụ *Hoàn tác bản cập nhật*.

Kích hoạt Light Agent

Để kích hoạt ứng dụng, bạn phải thêm khóa giấy phép vào SVM mà Light Agent được kết nối. Bạn không cần phải kích hoạt ứng dụng một cách riêng biệt.

Những cân nhắc đặc biệt khác cho chế độ Light Agent

- Khi tạo chính sách cho ứng dụng, bạn nên chọn chế độ Light Agent. Ở chế độ này, Trình hướng dẫn chính sách mới sẽ nhắc bạn cấu hình kết nối SVM. Những thiết lập này là bắt buộc để ứng dụng hoạt động ở chế độ Light Agent.
- Bạn không thể cài đặt các thành phần Mã hóa dữ liệu và Kiểm soát thích ứng sự cố ở chế độ Light Agent. Nhóm thành phần cũng phụ thuộc vào loại hệ điều hành khách: máy trạm hoặc máy chủ.
- Light Agent không hỗ trợ tích hợp với các giải pháp Kaspersky Endpoint Detection and Response Expert và Kaspersky Endpoint Detection and Response Expert (cloud).
- Bạn có thể quản lý Light Agent trong Bảng điều khiển quản trị (MMC) và Bảng điều khiển web của Kaspersky Security Center. Không thể quản lý Light Agent trong Bảng điều khiển đám mây Kaspersky Security Center.
- Không hỗ trợ việc thay đổi bộ thành phần ứng dụng trên máy ảo VDI.
- Kaspersky Endpoint Security giao tiếp với máy chủ KSN thông qua máy chủ proxy KSN. Không hỗ trợ giao tiếp trực tiếp với KSN.
- Không hỗ trợ Chế độ đám mây của Kaspersky Security Network.
- Không hỗ trợ sử dụng máy chủ proxy của ứng dụng khi kết nối với Máy chủ tích hợp (VIIS), Máy chủ bảo vệ (SVM) và máy chủ KSN.

Cấu hình sơ bộ của máy ảo

Bạn có thể cài đặt Kaspersky Endpoint Security trên máy ảo sử dụng công nghệ nền tảng ảo. Kaspersky Endpoint Security hỗ trợ các nền tảng ảo VMware, Microsoft Hyper-V, Citrix. Trước khi cài đặt, bạn phải thực hiện cấu hình sơ bộ cho máy ảo.

Khả năng tương thích với công nghệ Citrix App Layering

Nếu bạn dự định sử dụng Full User Layer để lưu trạng thái của máy ảo tạm thời, bạn phải thực hiện các bước sau trước khi cài đặt trên mẫu máy ảo:

1. Tạo tập tin C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txt và thêm các loại trừ sau vào đó:

   - `C:\ProgramData\KasperskyLab\`
   - `C:\ProgramData\Kaspersky Lab\`
   - `C:\Program Files (x86)\Kaspersky Lab\`

2. Trong registry của hệ điều hành trong khóa HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Unifltr, tạo một giá trị DWORD mới có tên là MiniFilterBypass và đặt thành 1.

3. Trong registry của hệ điều hành trong khóa HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd, tạo một giá trị MULTI_SZ mới có tên là ExcludeKey và đặt thành \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab.

4. Khởi động lại máy ảo.

Để cài đặt trên máy ảo trong cơ sở hạ tầng sử dụng Citrix App Layering, bạn phải thực hiện như sau:

1. Cài đặt Kaspersky Security Center Administration Agent và Kaspersky Endpoint Security cho Windows trên mẫu máy ảo trong Application Layer.

2. Tạo một ảnh máy ảo bao gồm nhiều lớp.

3. Triển khai ảnh đã tạo trên các trình quản lý ảo hỗ trợ giải pháp Citrix App Layering.

4. Cấu hình tạo máy ảo tạm thời từ hình ảnh đã tạo.

Để biết chi tiết về việc cài đặt phần mềm diệt virus cùng với Citrix App Layering, vui lòng tham khảo Tài liệu về Citrix App Layering.

Khả năng tương thích với công nghệ Citrix Provisioning (Citrix Provisioning Services)

Để đảm bảo ứng dụng tương thích với công nghệ Citrix Provisioning (Citrix Provisioning Services):

- Nếu phần mềm Citrix Provisioning Target Device được cài đặt trên máy ảo, bạn phải gỡ bỏ phần mềm này trước khi cài đặt ứng dụng Kaspersky Endpoint Security (để biết chi tiết, vui lòng truy cập trang web hỗ trợ kỹ thuật Citrix). Sau khi cài đặt ứng dụng, bạn phải cài đặt lại Citrix Provisioning Target Device. Bạn cũng cần cài đặt lại Citrix Provisioning Target Device khi khôi phục ứng dụng, bao gồm cả khi nâng cấp hệ điều hành.

Nâng cấp hệ điều hành bao gồm các bước sau:

1. Xóa Citrix Provisioning Target Device.
2. Nâng cấp hệ điều hành.
3. Sau khi khởi động máy ảo, hãy đảm bảo rằng ứng dụng Kaspersky Endpoint Security đang chạy và hoạt động bình thường.
4. Cài đặt lại Citrix Provisioning Target Device.

- Khi cài đặt ứng dụng bằng Trình hướng dẫn cài đặt hoặc từ xa bằng Kaspersky Security Center, bạn phải chọn hộp kiểm **Đảm bảo khả năng tương thích với Citrix PVS**.

Khả năng tương thích với công nghệ Omnissa App Volumes

Trước khi cài đặt trên mẫu máy ảo, bạn phải tạo tập tin %SVAgent%\Config\Custom\snapvol.cfg và thêm các loại trừ sau vào đó:

- `exclude_path=\ProgramData\Kaspersky Lab`
- `exclude_path=\ProgramData\KasperskyLab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Kaspersky Lab`
- `exclude_process_name=avp.exe`
- `exclude_process_name=klnagent.exe`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_arkmon`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klark`

- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klbg`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_mark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_swmon`

Để biết chi tiết, vui lòng tham khảo tài liệu của Omnissa.

Cài đặt Light Agent

Cài đặt Kaspersky Endpoint Security ở chế độ Light Agent trên máy ảo dựa trên kiến trúc Arm hiện không được hỗ trợ.

Cài đặt ứng dụng ở chế độ Light Agent cũng giống như ở Chế độ tiêu chuẩn. Trước khi cài đặt Light Agent trên máy ảo, bạn phải đảm bảo Kaspersky Security Center Network Agent đã được cài đặt. *Network Agent* giúp xúc tiến tương tác giữa Máy chủ quản trị và một máy ảo.

Có thể cài đặt Light Agent trên máy ảo theo một trong các cách sau:

- Từ xa thông qua Kaspersky Security Center.
- Cài đặt cục bộ bằng Trình hướng dẫn cài đặt.
- Cục bộ bằng cách sử dụng dòng lệnh.

Để cài đặt Light Agent, bạn phải chọn cấu hình thích hợp trong thiết lập gói cài đặt hoặc trong Trình hướng dẫn cài đặt.

Khi cài đặt Light Agent trên máy chủ, các thành phần bảo vệ nâng cao (Phát hiện hành vi, Phòng chống khai thác, Công cụ khắc phục) sẽ bị loại trừ khỏi cấu hình mặc định của ứng dụng. Thiết lập mặc định của ứng dụng sẽ cung cấp mức độ bảo vệ được đề xuất và sử dụng tối ưu tài nguyên máy chủ. Khi cài đặt Light Agent trên máy trạm, các thành phần bảo vệ nâng cao sẽ được thêm vào cấu hình mặc định của ứng dụng.

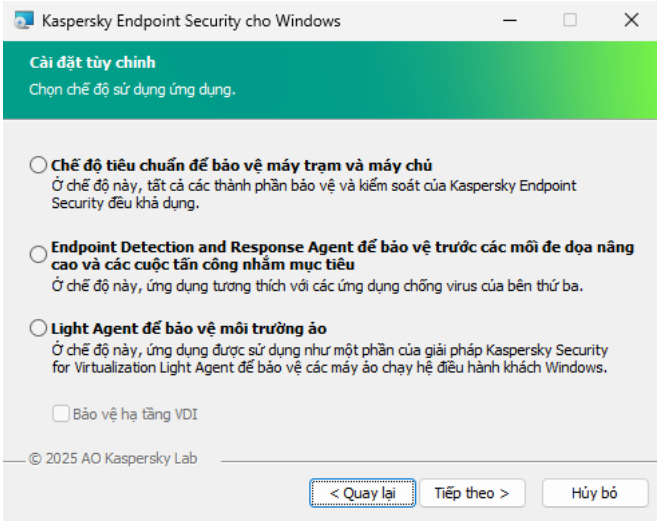
Khi cài đặt Light Agent, bạn nên chọn các loại trừ được định sẵn và các ứng dụng được tin tưởng cho môi trường ảo liên quan. Các loại trừ quét được định sẵn và các ứng dụng được tin tưởng sẽ giúp bạn thiết lập ứng dụng nhanh chóng và tránh các sự cố tương thích với môi trường ảo. Bạn cũng có thể cấu hình các loại trừ quét được định sẵn và các ứng dụng được tin tưởng sau khi cài đặt, trong chính sách.

Cách cài đặt Light Agent bằng Trình hướng dẫn cài đặt

1. Sao chép thư mục bộ phân phối vào máy ảo.
2. Chạy setup_kes.exe.

   Trình hướng dẫn cài đặt sẽ được bắt đầu.

Cấu hình của Kaspersky Endpoint Security



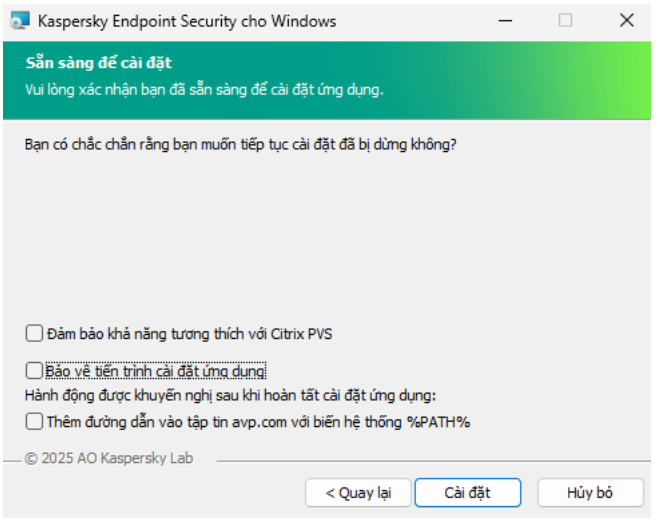
Lựa chọn cấu hình ứng dụng

Chọn cấu hình **Light Agent để bảo vệ môi trường ảo**. Cấu hình này được dành cho ứng dụng được sử dụng như một phần của giải pháp Kaspersky Security for Virtualization Light Agent. Phải cài đặt Light Agent trên mỗi máy ảo cần được bảo vệ bằng giải pháp này. Trong cấu hình này, bạn không thể sử dụng các thành phần các thành phần Mã hóa dữ liệu hoặc Kiểm soát thích ứng sự cố. Nếu bạn đang cài đặt Light Agent trên một mẫu máy ảo sẽ được sử dụng để tạo *máy ảo không lưu các thay đổi*, hãy chọn hộp kiểm **Bảo vệ hạ tầng VDI** (VDI chữ là viết tắt của Virtual Desktop Infrastructure). Chế độ bảo vệ VDI giúp tối ưu hóa hiệu năng của Kaspersky Endpoint Security trên các máy ảo không lưu các thay đổi. Ở chế độ này, Light Agent từ chối các bản cập nhật ứng dụng đòi hỏi khởi động lại máy ảo. Khi nhận được các bản cập nhật ứng dụng yêu cầu khởi động lại, Light Agent sẽ tạo một sự kiện về việc cần cập nhật mẫu của các máy ảo được bảo vệ.

Các thành phần Kaspersky Endpoint Security

Chọn các thành phần bạn muốn cài đặt (xem hình bên dưới). 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.

Thiết lập nâng cao



Thiết lập cài đặt ứng dụng 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 khả năng tương thích với Citrix PVS. Bạn có thể bật hỗ trợ Citrix Provisioning Services để cài đặt Kaspersky Endpoint Security lên một máy tính ảo.

Thêm đường dẫn vào tập tin avp.com với biến hệ thống %PATH%. Bạn có thể thêm đường dẫn cài đặt vào biến số %PATH% để tiện sử dụng giao diện dòng lệnh.

Cách cài đặt Light Agent bằng dòng lệnh

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 /pLIGHTAGENTMODE=1 [/pVDI=1] [/s]
   ```

   hoặc

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 LIGHTAGENTMODE=1 [VDI=1] [/qn]
   ```

   Tùy chọn `VDI` cho phép chế độ bảo vệ VDI (Virtual Desktop Infrastructure). Chế độ bảo vệ VDI giúp tối ưu hóa hiệu năng của Kaspersky Endpoint Security trên các máy ảo không lưu các thay đổi. Ở chế độ này, Light Agent từ chối các bản cập nhật ứng dụng đòi hỏi khởi động lại máy ảo. Khi nhận được các bản cập nhật ứng dụng yêu cầu khởi động lại, Light Agent sẽ tạo một sự kiện về việc cần cập nhật mẫu của các máy ảo được bảo vệ. Theo mặc định, chế độ bảo vệ VDI bị tắt.

Kết quả là Light Agent được cài đặt trên máy ảo bằng một nhóm thành phần mặc định. Bạn có thể chỉnh sửa nhóm thành phần và chỉ định thiết lập nâng cao bằng cách sử dụng tập tin setup.ini. Bạn cũng có thể chỉ định thiết lập trên dòng lệnh.

Cách cài đặt Light Agent trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.

2. Trong cây bảng điều khiển, hãy chọn thư mục **Advanced → Remote installation → Installation packages**.

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

3. Mở thuộc tính của gói cài đặt Kaspersky Endpoint Security cho Windows.

   Nếu cần, hãy tạo gói cài đặt mới.

4. Vào mục **Settings**.

5. Chọn cấu hình **Light Agent để bảo vệ môi trường ảo**. Cấu hình này được dành cho ứng dụng được sử dụng như một phần của giải pháp Kaspersky Security for Virtualization Light Agent. Phải cài đặt Light Agent trên mỗi máy ảo cần được bảo vệ bằng giải pháp này. Trong cấu hình này, bạn không thể sử dụng các thành phần các thành phần Mã hóa dữ liệu hoặc Kiểm soát thích ứng sự cố. Nếu bạn đang cài đặt Light Agent trên một mẫu máy ảo sẽ được sử dụng để tạo *máy ảo không lưu các thay đổi*, hãy chọn hộp kiểm **Bảo vệ hạ tầng VDI** (VDI chữ là viết tắt của Virtual Desktop Infrastructure). Chế độ bảo vệ VDI giúp tối ưu hóa hiệu năng của Kaspersky Endpoint Security trên các máy ảo không lưu các thay đổi. Ở chế độ này, Light Agent từ chối các bản cập nhật ứng dụng đòi hỏi khởi động lại máy ảo. Khi nhận được các bản cập nhật ứng dụng yêu cầu khởi động lại, Light Agent sẽ tạo một sự kiện về việc cần cập nhật mẫu của các máy ảo được bảo vệ.

6. Chọn các thành phần mà bạn muốn cài đặt.

   Bạn có thể thay đổi các thành phần ứng dụng khả dụng sau khi ứng dụng được cài đặt.

7. Cấu hình vùng tin tưởng. Chọn các loại trừ quét được định sẵn và các ứng dụng được tin tưởng cho môi trường ảo mà bạn đang cài đặt ứng dụng.

   Các loại trừ quét được định sẵn và các ứng dụng được tin tưởng sẽ giúp bạn thiết lập ứng dụng nhanh chóng và tránh các sự cố tương thích với môi trường ảo.

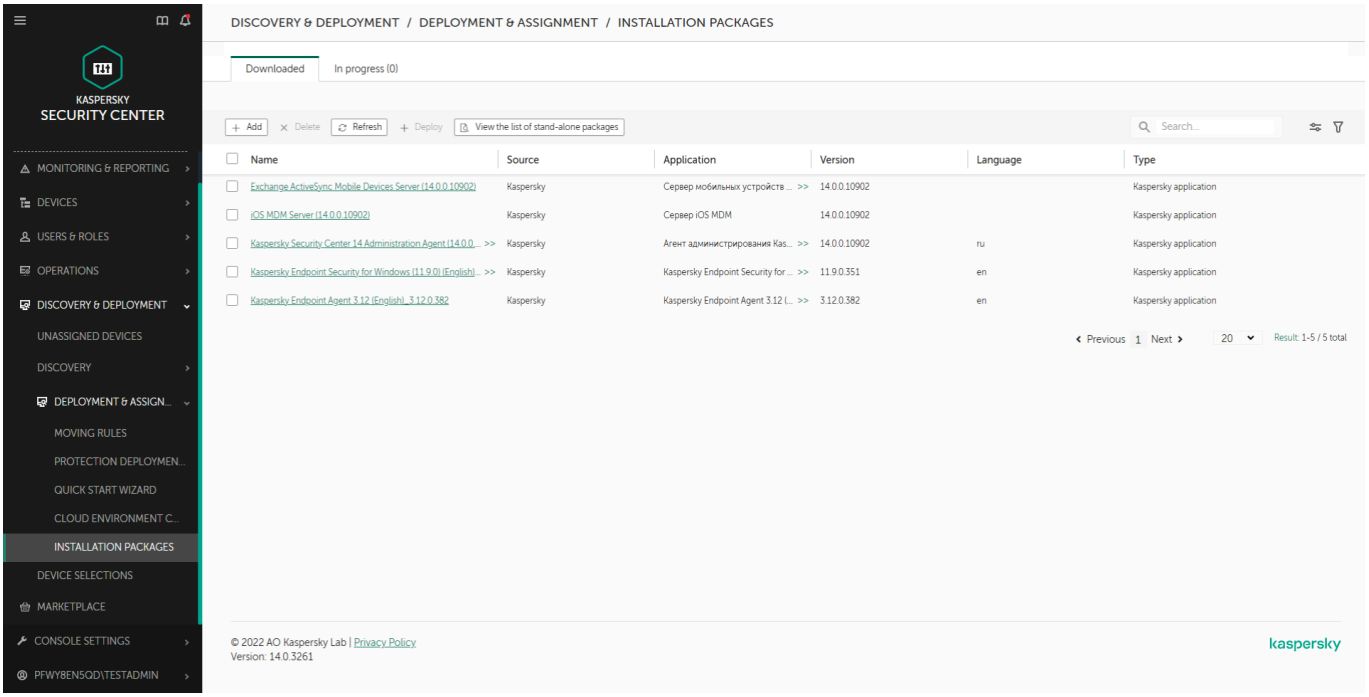
8. Lưu các thay đổi của bạn.

9. Tạo tác vụ cài đặt từ xa. Trong thuộc tính tác vụ, hãy chọn gói cài đặt bạn đã tạo.

Cách cài đặt Light Agent bằng Bảng điều khiển web

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.

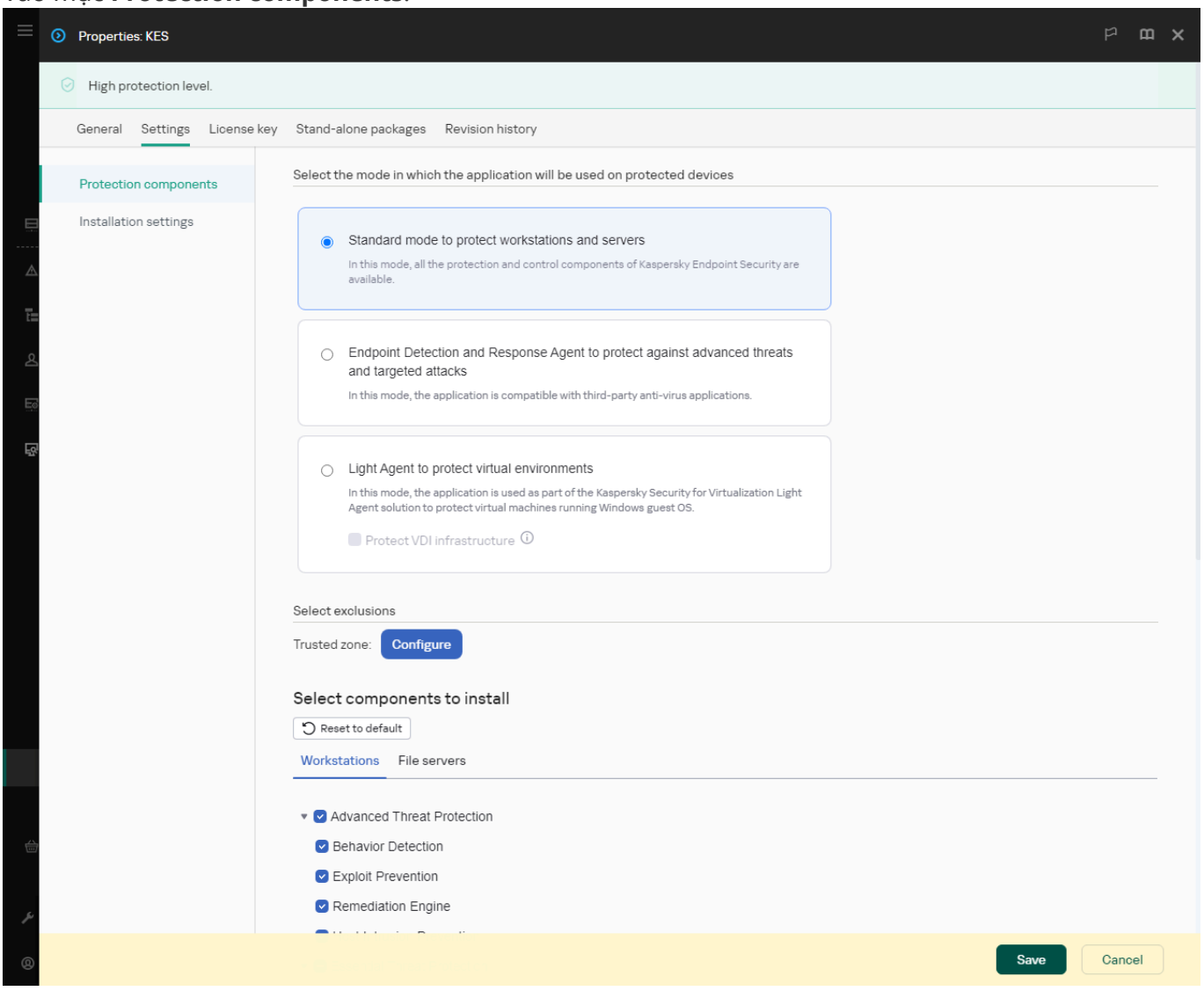


Danh sách gói cài đặt

2. Mở thuộc tính của gói cài đặt Kaspersky Endpoint Security cho Windows.
   Nếu cần, hãy tạo gói cài đặt mới.

3. Chọn thẻ **Settings**.

4. Vào mục **Protection components**.



Các thành phần có trong gói cài đặt

5. Chọn cấu hình **Light Agent to protect virtual environments**. Cấu hình này được dành cho ứng dụng được sử dụng như một phần của giải pháp Kaspersky Security for Virtualization Light Agent. Phải cài đặt Light Agent trên mỗi máy ảo cần được bảo vệ bằng giải pháp này. Trong cấu hình này, bạn không thể sử dụng các thành phần các thành phần Mã hóa dữ liệu hoặc Kiểm soát thích ứng sự cố. Nếu bạn đang cài đặt Light Agent trên một mẫu máy ảo sẽ được sử dụng để tạo *máy ảo không lưu các thay đổi*, hãy chọn hộp kiểm **Protect VDI infrastructure** (VDI chữ là viết tắt của Virtual Desktop Infrastructure). Chế độ bảo vệ VDI giúp tối ưu hóa hiệu năng của Kaspersky Endpoint Security trên các máy ảo không lưu các thay đổi. Ở chế độ này, Light Agent từ chối các bản cập nhật ứng dụng đòi hỏi khởi động lại máy ảo. Khi nhận được các bản cập nhật ứng dụng yêu cầu khởi động lại, Light Agent sẽ tạo một sự kiện về việc cần cập nhật mẫu của các máy ảo được bảo vệ.

6. Chọn các thành phần mà bạn muốn cài đặt.

   Bạn có thể thay đổi các thành phần ứng dụng khả dụng sau khi ứng dụng được cài đặt.

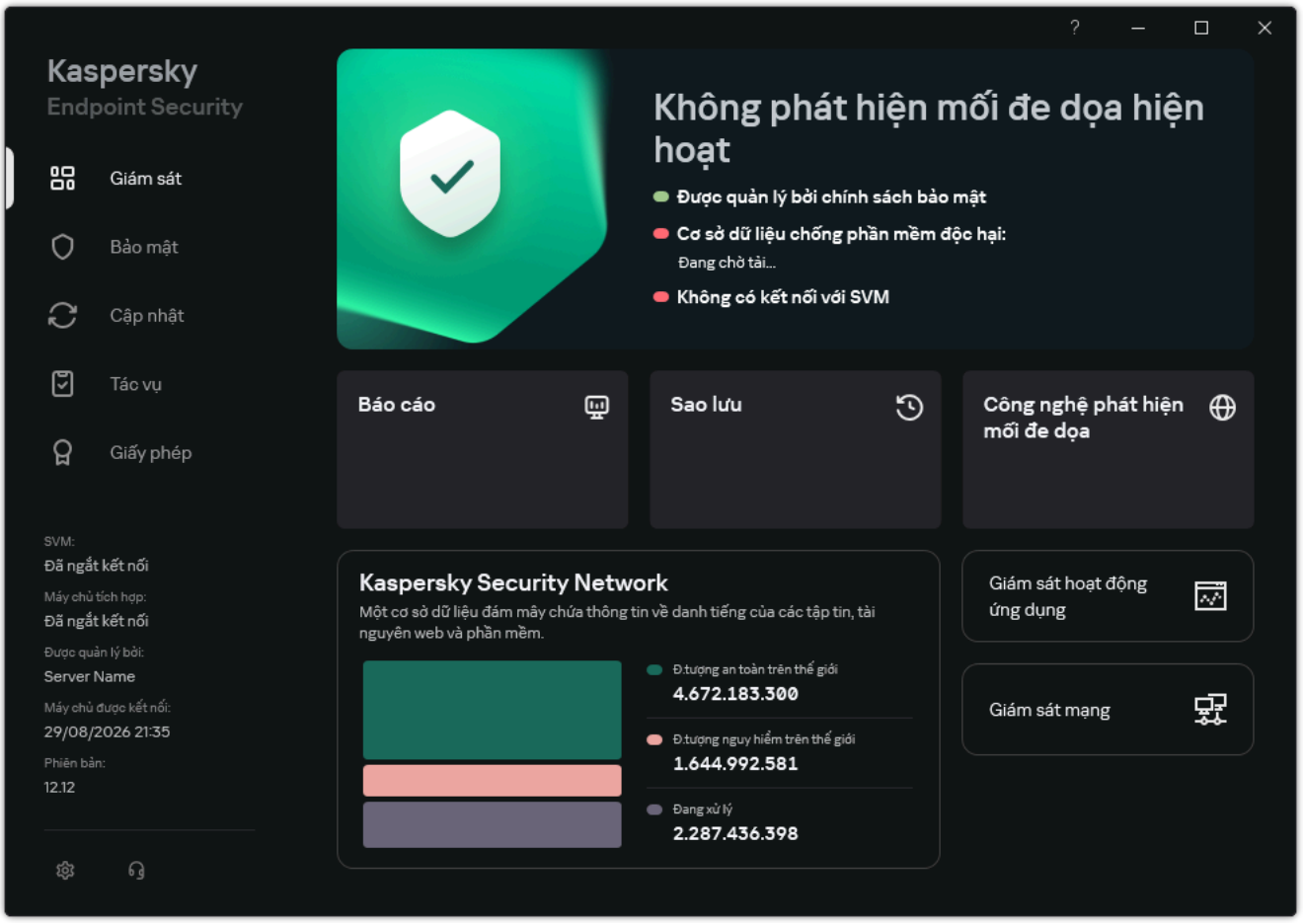
7. Cấu hình vùng tin tưởng. Chọn các loại trừ quét được định sẵn và các ứng dụng được tin tưởng cho môi trường ảo mà bạn đang cài đặt ứng dụng.

   Các loại trừ quét được định sẵn và các ứng dụng được tin tưởng sẽ giúp bạn thiết lập ứng dụng nhanh chóng và tránh các sự cố tương thích với môi trường ảo.

8. Lưu các thay đổi của bạn.

9. Tạo tác vụ cài đặt từ xa. Trong thuộc tính tác vụ, hãy chọn gói cài đặt bạn đã tạo.

Kết quả là Light Agent được cài đặt trên máy ảo. Bạn có thể sử dụng giao diện của ứng dụng và biểu tượng của ứng dụng được hiển thị trong vùng thông báo . Bây giờ bạn cần cấu hình kết nối của Light Agent với SVM.



Cửa sổ chính của Light Agent

Kết nối Light Agent với SVM

Giải pháp Kaspersky Security for Virtualization Light Agent đòi hỏi Light Agent và SVM phải liên lạc liên tục. Đây là điều cần thiết để quét các tập tin do Light Agent gửi đi để tìm virus và phần mềm độc hại khác. Nếu không có kết nối SVM, Light Agent không thể gửi tập tin để quét. Nếu không thể thiết lập kết nối trong hơn năm phút, quá trình quét sẽ kết thúc kèm theo.

Việc kết nối Light Agent với SVM bao gồm các bước sau:

1. Light Agent lấy danh sách các SVM có sẵn.
2. Light Agent xác định một Máy chủ bảo vệ (SVM) khả dụng, tối ưu cho kết nối theo Thuật toán chọn SVM.
3. Light Agent kiểm tra các thiết lập kết nối SVM bổ sung: thẻ, trạng thái bảo vệ kết nối, chức năng ứng dụng được giấy phép hỗ trợ.
4. Kết nối Light Agent với SVM.

Bạn có thể nhận thông tin về trạng thái kết nối của Light Agent với SVM trong Kaspersky Endpoint Security hoặc bằng cách sử dụng lệnh của ứng dụng. Ứng dụng sẽ tạo ra sự kiện bất cứ khi nào kết nối SVM của Light Agent bị mất hoặc được thiết lập và gửi những sự kiện này đến Kaspersky Security Center. Nếu đang sử dụng Máy chủ tích hợp để khám phá SVM, bạn có thể nhận thông tin về trạng thái của SVM và số lượng Light Agent được kết nối trong Bảng điều khiển Máy chủ tích hợp. Để biết chi tiết về giám sát trạng thái SVM, hãy xem Trợ giúp của Kaspersky Security for Virtualization Light Agent.

Khám phá SVM

Bạn có thể chọn một trong các phương thức khám phá SVM cho Light Agent:

- Sử dụng Máy chủ tích hợp (VIIS).

  Máy chủ tích hợp là thành phần giải pháp cho phép tương tác giữa Kaspersky Security for Virtualization Light Agent với cơ sở hạ tầng ảo và tạo một danh sách SVM có sẵn để kết nối. Light Agent thiết lập kết nối với Máy chủ tích hợp và lấy danh sách các địa chỉ SVM.

  Máy chủ tích hợp hữu ích nhất trong các cơ sở hạ tầng ảo quy mô lớn vì máy chủ sẽ tự động cân bằng tải giữa các SVM, thu thập thông tin về các SVM khả dụng, phân tích thông tin này và cung cấp cho các Light Agent danh sách các Máy chủ bảo vệ (SVM) tối ưu để kết nối.

  Để Light Agent có thể lấy được danh sách SVM, bạn chỉ cần nhập địa chỉ của Máy chủ tích hợp.

- Sử dụng cụm máy chủ tích hợp có tính khả dụng cao.

  Tính năng triển khai cụm máy chủ tích hợp có độ khả dụng cao được hỗ trợ trong Kaspersky Security for Virtualization Light Agent kể từ phiên bản 6.4. Cụm máy chủ tích hợp có tính khả dụng cao cho phép bảo vệ liên tục cho môi trường ảo nhờ vào cơ chế chuyển đổi dự phòng của SVM và Light Agent sang máy chủ tích hợp dự phòng bất cứ khi nào máy chủ tích hợp chính gặp sự cố. Một thành phần cụm đặc biệt là *bộ cân bằng tải* sẽ chịu trách nhiệm chuyển đổi dự phòng máy chủ. Để biết chi tiết cụm Máy chủ tích hợp có tính khả dụng cao, hãy xem Trợ giúp của Kaspersky Security for Virtualization Light Agent.

  Để Light Agent lấy được danh sách các SVM, bạn cần nhập địa chỉ của thiết bị được cài đặt bộ cân bằng tải.

- Sử dụng danh sách địa chỉ SVM.

  Nếu bạn cần chỉ định từng SVM mà bạn muốn Light Agent kết nối với, bạn có thể chuẩn bị danh sách theo cách thủ công.

  Bạn cần liệt kê địa chỉ của các SVM khả dụng mà Light Agent có thể kết nối với.

Cách cấu hình phát hiện SVM bằng Light Agent trong Bảng điều khiển quản trị (MMC)

1. Mở Bảng điều khiển quản trị Kaspersky Security Center.
2. Trong cây bảng điều khiển, hãy chọn **Policies**.
3. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
4. Trong cửa sổ chính sách, hãy chọn **Chế độ Light Agent → Thiết lập khám phá SVM**.

5. Chọn phương thức khám phá SVM.

   - **Sử dụng Máy chủ tích hợp**. Nhập các thiết lập để kết nối với Máy chủ tích hợp tùy theo cơ sở hạ tầng của bạn:

     - **Một Máy chủ tích hợp duy nhất**. Nhập các thiết lập kết nối Máy chủ tích hợp: địa chỉ IPv4 hoặc tên miền tên đầy đủ (FQDN) của thiết bị.

     - **Cụm máy chủ tích hợp có tính khả dụng cao**. Nhập địa chỉ IP và cổng của bộ cân bằng tải thuộc cụm máy chủ.

   - **Sử dụng danh sách địa chỉa SVM tùy chỉnh**. Tạo danh sách các SVM mà Light Agent có thể kết nối với. Chỉ định địa chỉ IP theo định dạng IPv4 hoặc tên miền đầy đủ (FQDN) của SVM. Mỗi mục trong danh sách phải được nhập trên một dòng mới hoặc được phân tách với mục trước đó bằng dấu chấm phẩy (`;`).

     > Trong danh sách địa chỉ SVM, chỉ được chỉ định tên miền đầy đủ (FQDN) khớp với một địa chỉ IP duy nhất. Việc sử dụng tên miền đầy đủ tương ứng với nhiều địa chỉ IP có thể dẫn đến lỗi trong giải pháp.

6. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách cấu hình khám phá SVM bằng Light Agent trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.

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 **Light Agent Mode** → **SVM discovery settings**.

5. Chọn phương thức khám phá SVM.

   - **Use Integration Server**. Nhập các thiết lập để kết nối với Máy chủ tích hợp tùy theo cơ sở hạ tầng của bạn:

     - **Một Máy chủ tích hợp duy nhất**. Nhập các thiết lập kết nối Máy chủ tích hợp: địa chỉ IPv4 hoặc tên miền tên đầy đủ (FQDN) của thiết bị.

     - **Cụm máy chủ tích hợp có tính khả dụng cao**. Nhập địa chỉ IP và cổng của bộ cân bằng tải thuộc cụm máy chủ.

- **Use a custom list of SVM addresses**. Tạo danh sách các SVM mà Light Agent có thể kết nối với. Chỉ định địa chỉ IP theo định dạng IPv4 hoặc tên miền đầy đủ (FQDN) của SVM. Mỗi mục trong danh sách phải được nhập trên một dòng mới hoặc được phân tách với mục trước đó bằng dấu chấm phẩy (;).

  > Trong danh sách địa chỉ SVM, chỉ được chỉ định tên miền đầy đủ (FQDN) khớp với một địa chỉ IP duy nhất. Việc sử dụng tên miền đầy đủ tương ứng với nhiều địa chỉ IP có thể dẫn đến lỗi trong giải pháp.

6. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách cấu hình khám phá SVM bằng Light Agent trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ cài đặt ứng dụng, trong mục **Chế độ Light Agent** hãy nhấn vào ô **Thiết lập khám phá SVM**.
3. Chọn phương thức khám phá SVM.
   - **Sử dụng máy chủ tích hợp**. Nhập các thiết lập để kết nối với Máy chủ tích hợp tùy theo cơ sở hạ tầng của bạn:
     - **Một Máy chủ tích hợp duy nhất**. Nhập các thiết lập kết nối Máy chủ tích hợp: địa chỉ IPv4 hoặc tên miền tên đầy đủ (FQDN) của thiết bị.
     - **Cụm máy chủ tích hợp có tính khả dụng cao**. Nhập địa chỉ IP và cổng của bộ cân bằng tải thuộc cụm máy chủ.
   - **Sử dụng danh sách địa chỉ SVM tùy chỉnh**. Tạo danh sách các SVM mà Light Agent có thể kết nối với. Chỉ định địa chỉ IP theo định dạng IPv4 hoặc tên miền đầy đủ (FQDN) của SVM. Mỗi mục trong danh sách phải được nhập trên một dòng mới hoặc được phân tách với mục trước đó bằng dấu chấm phẩy (;).

     > Trong danh sách địa chỉ SVM, chỉ được chỉ định tên miền đầy đủ (FQDN) khớp với một địa chỉ IP duy nhất. Việc sử dụng tên miền đầy đủ tương ứng với nhiều địa chỉ IP có thể dẫn đến lỗi trong giải pháp.

4. Lưu các thay đổi của bạn.

Cấu hình thuật toán chọn SVM cho Light Agent

Cơ sở hạ tầng của tổ chức có thể có nhiều SVM được triển khai mà Light Agent có thể kết nối. Để cân bằng tải trên mạng và tài nguyên của cơ sở hạ tầng ảo, bạn cần phân phối Light Agent giữa các SVM.

Thuật toán chọn SVM

Các Light Agent có thể áp dụng các thuật toán chọn SVM sau để kết nối: Thuật toán tiêu chuẩn (mặc định) và Thuật toán mở rộng.

Thuật toán tiêu chuẩn	Thuật toán mở rộng
Nếu thuật toán này được sử dụng, sau khi cài đặt và khởi động, Light Agent trên máy ảo sẽ chọn kết nối với một SVM *cục bộ* liên quan đến Light Agent đó. Nếu không tìm thấy SVM cục bộ nào phù hợp để kết nối, Light Agent sẽ chọn một SVM có số lượng Light Agent kết nối ít nhất, bất kể vị trí của SVM đó trong cơ sở hạ tầng ảo. Ứng dụng không xác định liệu SVM có cục bộ so với Light Agent hay không nếu chế độ bảo vệ cơ sở hạ tầng lớn được bật cho Máy chủ bảo vệ trên SVM. Trong trường hợp này, bạn nên sử dụng thuật toán lựa chọn SVM mở rộng và chọn Máy chủ tích hợp làm phương pháp khám phá SVM. Việc một SVM có được coi là cục bộ đối với Light Agent hay không phụ thuộc vào loại cơ sở hạ tầng ảo.	Nếu áp dụng thuật toán này, bạn có thể xác định các thiết lập lựa chọn SVM sau: • có nên cân nhắc hay bỏ qua vị trí của SVM trong cơ sở hạ tầng khi lựa chọn SVM cho kết nối • nếu cân nhắc vị trí của SVM, phương thức xác định tính chất cục bộ của SVM so với Light Agent Nếu các Light Agent bỏ qua vị trí của SVM trong cơ sở hạ tầng thì các Light Agent sẽ có thể kết nối với bất kỳ SVM nào có sẵn để kết nối. Nếu các Light Agent phải cân nhắc vị trí của SVM trong cơ sở hạ tầng, bạn cần chọn loại đường dẫn SVM cần được cân nhắc khi xác định tính chất cục bộ của SVM so với Light Agent. Việc một SVM có được coi là cục bộ đối với Light Agent hay không phụ thuộc vào loại cơ sở hạ tầng ảo. Nếu các Light Agent xem xét vị trí của SVM trong cơ sở hạ tầng khi lựa chọn SVM để kết nối với thì các Light Agent chỉ có thể kết nối với các SVM nằm trong cùng khu vực. Ví dụ: nếu bạn chỉ định một cụm hypervisor làm loại đường dẫn SVM thì tất cả các SVM được triển khai trên cụm hypervisor này sẽ được coi là cục bộ đối với Light Agent và Light Agent đó chỉ có thể kết nối với một trong số các SVM này. Nếu không có SVM nào khả dụng để kết nối trong cùng cụm có Light Agent đang chạy thì Light Agent đó sẽ không kết nối với SVM. Khi lựa chọn SVM, các Light Agent cũng xem xét số lượng Light Agent được kết nối để đảm bảo rằng các Light Agent được phân bổ đều giữa các SVM có sẵn để kết nối. Nếu Light Agent sử dụng thuật toán lựa chọn SVM mở rộng và phương thức phát hiện SVM được đặt thành danh sách địa chỉ SVM, đồng thời chế độ bảo vệ cơ sở hạ tầng lớn được bật trên SVM thì chỉ có thể kết nối Light Agent với SVM này nếu đường dẫn SVM bị bỏ qua.
Basis Dynamix Enterprise	
Trong cơ sở hạ tầng ảo dựa trên Basis Dynamix Enterprise, SVM được coi là cục bộ đối với Light Agent chính là SVM được triển khai trên cùng một nút với máy ảo đã cài đặt Light Agent.	Trong cơ sở hạ tầng ảo dựa trên Basis Dynamix Enterprise thì một SVM có thể được coi là cục bộ đối với Light Agent trong bất kỳ trường hợp nào sau đây: • Một SVM được triển khai trên cùng một nút với máy ảo có Light Agent được cài đặt. • Một SVM được triển khai trong cùng khu vực với máy ảo có Light Agent được cài đặt. • Một SVM được triển khai trong cùng trung tâm dữ liệu với máy ảo có Light Agent được cài đặt.
Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer, và Basis Dynamix Standard	

Thuật toán tiêu chuẩn	Thuật toán mở rộng
Trong cơ sở hạ tầng ảo dựa trên Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer hoặc Basis Dynamix Standard thì SVM được coi là cục bộ đối với Light Agent chính là SVM được triển khai trên cùng một hypervisor với máy ảo được cài đặt Light Agent.	Trong cơ sở hạ tầng ảo dựa trên Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer hoặc Basis Dynamix Standard thì một SVM có thể được coi là cục bộ đối với Light Agent trong bất kỳ trường hợp nào sau đây: • Một SVM được triển khai trên cùng một hypervisor với máy ảo có Light Agent được cài đặt. • Một SVM được triển khai trên cùng một cụm hypervisor với máy ảo có Light Agent được cài đặt. • Một SVM được triển khai trong cùng trung tâm dữ liệu với máy ảo có Light Agent được cài đặt.
OpenStack và VK Private Cloud SVM	
Trong cơ sở hạ tầng ảo chạy trên nền tảng OpenStack hoặc VK Private Cloud, bạn có thể chỉ định cách xác định tính chất cục bộ của SVM so với Light Agent bằng cách sử dụng tham số `StandardAlgorithmSvmLocality` trong phần `HypervisorSpecificSettings:Openstack` của tập tin cấu hình máy chủ tích hợp appsettings.json. Tùy thuộc vào phiên bản của Máy chủ tích hợp, tập tin này nằm ở một trong các đường dẫn sau: • /var/opt/kaspersky/viis/common/ đối với Máy chủ tích hợp dựa trên Linux • %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ đối với Máy chủ tích hợp dựa trên Windows Tham số `StandardAlgorithmSvmLocality` có thể nhận các giá trị sau: • `ServerGroup` – nếu giá trị này được chọn thì SVM được coi là cục bộ đối với Light Agent nếu SVM đó nằm trong cùng nhóm máy chủ với máy ảo có Light Agent được cài đặt. Giá trị này được bật theo mặc định. • `Project` – nếu giá trị này được chọn thì SVM được coi là cục bộ đối với Light Agent nếu SVM đó được triển khai trong cùng dự án OpenStack với máy ảo có Light Agent được cài đặt. • `AvailabilityZone` – nếu giá trị này được chọn thì SVM được coi là cục bộ đối với Light Agent nếu SVM đó nằm trong cùng vùng khả dụng với máy ảo có Light Agent được cài đặt.	Trong cơ sở hạ tầng ảo chạy trên nền tảng OpenStack hoặc VK Private Cloud thì một SVM có thể được coi là cục bộ đối với Light Agent trong bất kỳ trường hợp nào sau đây: • Máy ảo SVM nằm trong cùng nhóm máy chủ với máy ảo có Light Agent được cài đặt. • Một SVM được triển khai trong cùng một dự án OpenStack với máy ảo có Light Agent được cài đặt. • SVM nằm trong cùng vùng khả dụng cùng với máy ảo được cài đặt Light Agent.

Ngoài các thuật toán kết nối SVM, bạn có thể điều chỉnh kết nối của các Light Agent với SVM bằng cách sử dụng thẻ.

Cấu hình thuật toán chọn SVM

Cách cấu hình thuật toán lựa chọn SVM cho Light Agent trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Chế độ Light Agent → Thuật toán chọn SVM**.
4. Chọn thuật toán:
   - **Sử dụng thuật toán chọn SVM tiêu chuẩn**. Light Agent sẽ chọn các SVM được triển khai trong cùng một trình quản lý ảo.
   - **Sử dụng thuật toán chọn SVM mở rộng**. Light Agent sẽ chọn các SVM được triển khai trong loại đường dẫn SVM đã chọn (theo mặc định là **Hypervisor**).

5. Nếu cần, hãy chọn đường dẫn SVM cho thuật toán chọn SVM mở rộng:

- **Hypervisor**. Light Agent sẽ chọn một SVM để kết nối, SVM đó phải đáp ứng các tiêu chí (tùy thuộc vào loại cơ sở hạ tầng ảo):

  - SVM được triển khai trên cùng một hypervisor như máy ảo có thiết lập Light Agent (trong cơ sở hạ tầng ảo dựa trên Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer hoặc Basis Dynamix Standard).

  - SVM nằm trong cùng nhóm máy chủ với máy ảo có Light Agent được cài đặt (trong cơ sở hạ tầng ảo chạy trên nền tảng OpenStack, VK Private Cloud hoặc TIONIX Cloud).

  - SVM được đặt trên cùng một nút với máy ảo có Light Agent được cài đặt (trong cơ sở hạ tầng ảo Basis Dynamix Enterprise).

  Nếu không có SVM nào khả dụng cho kết nối trên cùng một hypervisor hoặc trong cùng một Nhóm máy chủ nơi đặt máy ảo có Light Agent thì Light Agent sẽ không kết nối với SVM.

- **Cluster**. Light Agent sẽ chọn một SVM để kết nối, SVM đó phải đáp ứng các tiêu chí (tùy thuộc vào loại cơ sở hạ tầng ảo):

  - Các SVM được triển khai trên cùng một cụm hypervisor như máy ảo có thiết lập Light Agent (trong cơ sở hạ tầng ảo dựa trên Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer hoặc Basis Dynamix Standard).

  - Các SVM được triển khai trong cùng dự án OpenStack với máy ảo có Light Agent được cài đặt (trong cơ sở hạ tầng ảo chạy trên nền tảng OpenStack, VK Private Cloud hoặc TIONIX Cloud).

  - SVM được đặt trong cùng một vùng với máy ảo có Light Agent được cài đặt (trong cơ sở hạ tầng ảo Basis Dynamix Enterprise).

  Nếu không có SVM nào khả dụng cho kết nối trong cùng một cụm hypervisor hoặc trong cùng một dự án OpenStack nơi đặt máy ảo có Light Agent thì Light Agent sẽ không kết nối với SVM.

- **Trung tâm dữ liệu**. Light Agent sẽ chọn một SVM để kết nối, SVM đó phải đáp ứng các tiêu chí (tùy thuộc vào loại cơ sở hạ tầng ảo):

  - Các SVM được triển khai trên cùng một trung tâm dữ liệu như máy ảo có thiết lập Light Agent (trong cơ sở hạ tầng ảo dựa trên Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer hoặc Basis Dynamix Standard).

  - Các SVM nằm trong cùng Khu vực khả dụng với máy ảo có Light Agent được cài đặt (trong cơ sở hạ tầng ảo chạy trên nền tảng OpenStack, VK Private Cloud hoặc TIONIX Cloud).

  - SVM được đặt trong cùng một trung tâm dữ liệu với máy ảo có Light Agent được cài đặt (trong cơ sở hạ tầng ảo Basis Dynamix Enterprise).

Nếu không có SVM nào khả dụng để kết nối trong cùng trung tâm dữ liệu hoặc Vùng khả dụng nơi đặt máy ảo có Light Agent thì Light Agent sẽ không kết nối với SVM.

- **Bỏ qua**. Light Agent bỏ qua đường dẫn SVM để kết nối với Máy chủ bảo vệ. Light Agents cân nhắc các tiêu chí khác: thẻ, số lượng Light Agent được kết nối với SVM, v.v.

6. Lưu các thay đổi của bạn.

Cách cấu hình thuật toán chọn SVM cho Light Agent trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.

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 **Light Agent Mode** → **SVM selection algorithm**.

5. Chọn thuật toán:

   - **Use the standard SVM selection algorithm**. Light Agent sẽ chọn các SVM được triển khai trong cùng một trình quản lý ảo.

   - **Use the extended SVM selection algorithm**. Light Agent sẽ chọn các SVM được triển khai trong loại đường dẫn SVM đã chọn (theo mặc định là **Hypervisor**).

6. Nếu cần, hãy chọn đường dẫn SVM cho thuật toán chọn SVM mở rộng:

   - **Hypervisor**. Light Agent sẽ chọn một SVM để kết nối, SVM đó phải đáp ứng các tiêu chí (tùy thuộc vào loại cơ sở hạ tầng ảo):

     - SVM được triển khai trên cùng một hypervisor như máy ảo có thiết lập Light Agent (trong cơ sở hạ tầng ảo dựa trên Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer hoặc Basis Dynamix Standard).

     - SVM nằm trong cùng nhóm máy chủ với máy ảo có Light Agent được cài đặt (trong cơ sở hạ tầng ảo chạy trên nền tảng OpenStack, VK Private Cloud hoặc TIONIX Cloud).

     - SVM được đặt trên cùng một nút với máy ảo có Light Agent được cài đặt (trong cơ sở hạ tầng ảo Basis Dynamix Enterprise).

     Nếu không có SVM nào khả dụng cho kết nối trên cùng một hypervisor hoặc trong cùng một Nhóm máy chủ nơi đặt máy ảo có Light Agent thì Light Agent sẽ không kết nối với SVM.

- **Cluster**. Light Agent sẽ chọn một SVM để kết nối, SVM đó phải đáp ứng các tiêu chí (tùy thuộc vào loại cơ sở hạ tầng ảo):

  - Các SVM được triển khai trên cùng một cụm hypervisor như máy ảo có thiết lập Light Agent (trong cơ sở hạ tầng ảo dựa trên Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer hoặc Basis Dynamix Standard).

  - Các SVM được triển khai trong cùng dự án OpenStack với máy ảo có Light Agent được cài đặt (trong cơ sở hạ tầng ảo chạy trên nền tảng OpenStack, VK Private Cloud hoặc TIONIX Cloud).

  - SVM được đặt trong cùng một vùng với máy ảo có Light Agent được cài đặt (trong cơ sở hạ tầng ảo Basis Dynamix Enterprise).

  Nếu không có SVM nào khả dụng cho kết nối trong cùng một cụm hypervisor hoặc trong cùng một dự án OpenStack nơi đặt máy ảo có Light Agent thì Light Agent sẽ không kết nối với SVM.

- **Data center**. Light Agent sẽ chọn một SVM để kết nối, SVM đó phải đáp ứng các tiêu chí (tùy thuộc vào loại cơ sở hạ tầng ảo):

  - Các SVM được triển khai trên cùng một trung tâm dữ liệu như máy ảo có thiết lập Light Agent (trong cơ sở hạ tầng ảo dựa trên Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer hoặc Basis Dynamix Standard).

  - Các SVM nằm trong cùng Khu vực khả dụng với máy ảo có Light Agent được cài đặt (trong cơ sở hạ tầng ảo chạy trên nền tảng OpenStack, VK Private Cloud hoặc TIONIX Cloud).

  - SVM được đặt trong cùng một trung tâm dữ liệu với máy ảo có Light Agent được cài đặt (trong cơ sở hạ tầng ảo Basis Dynamix Enterprise).

  Nếu không có SVM nào khả dụng để kết nối trong cùng trung tâm dữ liệu hoặc Vùng khả dụng nơi đặt máy ảo có Light Agent thì Light Agent sẽ không kết nối với SVM.

- **Ignore**. Light Agent bỏ qua đường dẫn SVM để kết nối với Máy chủ bảo vệ. Light Agents cân nhắc các tiêu chí khác: thẻ, số lượng Light Agent được kết nối với SVM, v.v.

7. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách cấu hình thuật toán chọn SVM cho Light Agent trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .

2. Trong cửa sổ cài đặt ứng dụng, trong mục **Chế độ Light Agent** hãy nhấn vào ô **Thiết lập khám phá SVM**.

3. Chọn thuật toán:

   - **Sử dụng thuật toán chọn SVM tiêu chuẩn**. Light Agent sẽ chọn các SVM được triển khai trong cùng một trình quản lý ảo.

   - **Sử dụng thuật toán chọn SVM mở rộng**. Light Agent sẽ chọn các SVM được triển khai trong loại đường dẫn SVM đã chọn (theo mặc định là **Hypervisor**).

4. Nếu cần, hãy chọn đường dẫn SVM cho thuật toán chọn SVM mở rộng:

- **Hypervisor**. Light Agent sẽ chọn một SVM để kết nối, SVM đó phải đáp ứng các tiêu chí (tùy thuộc vào loại cơ sở hạ tầng ảo):

  - SVM được triển khai trên cùng một hypervisor như máy ảo có thiết lập Light Agent (trong cơ sở hạ tầng ảo dựa trên Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer hoặc Basis Dynamix Standard).

  - SVM nằm trong cùng nhóm máy chủ với máy ảo có Light Agent được cài đặt (trong cơ sở hạ tầng ảo chạy trên nền tảng OpenStack, VK Private Cloud hoặc TIONIX Cloud).

  - SVM được đặt trên cùng một nút với máy ảo có Light Agent được cài đặt (trong cơ sở hạ tầng ảo Basis Dynamix Enterprise).

  Nếu không có SVM nào khả dụng cho kết nối trên cùng một hypervisor hoặc trong cùng một Nhóm máy chủ nơi đặt máy ảo có Light Agent thì Light Agent sẽ không kết nối với SVM.

- **Cụm**. Light Agent sẽ chọn một SVM để kết nối, SVM đó phải đáp ứng các tiêu chí (tùy thuộc vào loại cơ sở hạ tầng ảo):

  - Các SVM được triển khai trên cùng một cụm hypervisor như máy ảo có thiết lập Light Agent (trong cơ sở hạ tầng ảo dựa trên Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer hoặc Basis Dynamix Standard).

  - Các SVM được triển khai trong cùng dự án OpenStack với máy ảo có Light Agent được cài đặt (trong cơ sở hạ tầng ảo chạy trên nền tảng OpenStack, VK Private Cloud hoặc TIONIX Cloud).

  - SVM được đặt trong cùng một vùng với máy ảo có Light Agent được cài đặt (trong cơ sở hạ tầng ảo Basis Dynamix Enterprise).

  Nếu không có SVM nào khả dụng cho kết nối trong cùng một cụm hypervisor hoặc trong cùng một dự án OpenStack nơi đặt máy ảo có Light Agent thì Light Agent sẽ không kết nối với SVM.

- **Trung tâm dữ liệu**. Light Agent sẽ chọn một SVM để kết nối, SVM đó phải đáp ứng các tiêu chí (tùy thuộc vào loại cơ sở hạ tầng ảo):

  - Các SVM được triển khai trên cùng một trung tâm dữ liệu như máy ảo có thiết lập Light Agent (trong cơ sở hạ tầng ảo dựa trên Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer hoặc Basis Dynamix Standard).

  - Các SVM nằm trong cùng Khu vực khả dụng với máy ảo có Light Agent được cài đặt (trong cơ sở hạ tầng ảo chạy trên nền tảng OpenStack, VK Private Cloud hoặc TIONIX Cloud).

  - SVM được đặt trong cùng một trung tâm dữ liệu với máy ảo có Light Agent được cài đặt (trong cơ sở hạ tầng ảo Basis Dynamix Enterprise).

Nếu không có SVM nào khả dụng để kết nối trong cùng trung tâm dữ liệu hoặc Vùng khả dụng nơi đặt máy ảo có Light Agent thì Light Agent sẽ không kết nối với SVM.

- **Bỏ qua**. Light Agent bỏ qua đường dẫn SVM để kết nối với Máy chủ bảo vệ. Light Agents cân nhắc các tiêu chí khác: thẻ, số lượng Light Agent được kết nối với SVM, v.v.

5. Lưu các thay đổi của bạn.

Phân phối các kết nối của Light Agents tới SVM (thẻ)

Nhiều Light Agent có thể kết nối với một SVM. Để cân bằng các kết nối Light Agent, bạn có thể chỉ định một danh sách SVM riêng. Nếu bạn đang sử dụng máy chủ tích hợp để khám phá SVM, bạn có thể sử dụng *thẻ* để cân bằng các kết nối Light Agent với SVM. Tức là đối với Light Agent, bạn có thể chỉ định danh sách SVM để kết nối bằng cách sử dụng thẻ. Để thực hiện, bạn phải gán thẻ cho Light Agent và chỉ định thẻ này trong thiết lập SVM. Để biết chi tiết về việc chỉ định thẻ trong thiết lập SVM, hãy xem Trợ giúp của Kaspersky Security for Virtualization Light Agent.

Ví dụ: Giải pháp Kaspersky Endpoint Detection and Response Optimum được triển khai trong cơ sở hạ tầng của bạn cho các máy chủ ảo được chỉ định. Trong trường hợp này, bạn có thể chỉ định thẻ `[EDROptimum]` cho Light Agent để kết nối với SVM có thêm khóa giấy phép EDR Optimum (Tiện ích bổ trợ EDR Optimum). Do đó, bạn có thể sử dụng chức năng EDR Optimum trên máy ảo với Light Agent. Khi kết nối Light Agent với SVM mà không có khóa giấy phép EDR Optimum, chức năng Kaspersky Endpoint Detection and Response Optimum sẽ không khả dụng.

Cách gán thẻ kết nối SVM cho Light Agent trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Chế độ Light Agent → Thẻ kết nối SVM**.
4. Chọn hộp kiểm **Sử dụng thẻ kết nối** và nhập thẻ kết nối SVM.

   Đối với thẻ, bạn có thể nhập chuỗi văn bản dài tối đa 255 ký tự. Bạn có thể sử dụng bất kỳ ký tự nào ngoại trừ ký tự `;`.
5. Lưu các thay đổi của bạn.

Cách gán thẻ kết nối SVM cho Light Agent trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management → Policies**.
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 **Light Agent Mode → SVM connection tag**.

5. Chọn hộp kiểm **Use connection tag** và nhập thẻ kết nối SVM.

   Đối với thẻ, bạn có thể nhập chuỗi văn bản dài tối đa 255 ký tự. Bạn có thể sử dụng bất kỳ ký tự nào ngoại trừ ký tự `;`.

6. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách gán thẻ kết nối SVM cho Light Agent trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .

2. Trong cửa sổ cài đặt ứng dụng, trong mục **Chế độ Light Agent** hãy nhấn vào ô **Thẻ kết nối SVM**.

3. Chọn hộp kiểm **Sử dụng thẻ kết nối** và nhập thẻ kết nối SVM.

   Đối với thẻ, bạn có thể nhập chuỗi văn bản dài tối đa 255 ký tự. Bạn có thể sử dụng bất kỳ ký tự nào ngoại trừ ký tự `;`.

4. Lưu các thay đổi của bạn.

Bảo vệ kết nối giữa Light Agent và SVM

Bạn có thể cấu hình mã hóa của kết nối giữa Light Agents và Máy chủ bảo vệ. Để thực hiện việc này, bạn cần bật mã hóa kênh dữ liệu giữa Light Agent và Máy chủ bảo vệ trong thiết lập Máy chủ bảo vệ trên SVM và trong thiết lập Light Agent.

Light Agent được bật tính năng bảo vệ kết nối chỉ có thể kết nối với SVM được bật tính năng mã hóa kênh dữ liệu giữa Light Agent và Máy chủ bảo vệ. Light Agent bị vô hiệu hóa bảo vệ kết nối chỉ có thể kết nối với SVM bị vô hiệu hóa mã hóa kênh hoặc cho phép kết nối không bảo mật giữa Máy chủ bảo vệ và Light Agent.

Để biết chi tiết về cấu hình bảo vệ kết nối trên Máy chủ bảo vệ, hãy xem Trợ giúp của Kaspersky Security for Virtualization Light Agent.

Việc bảo vệ kết nối bằng mã hóa có thể làm giảm hiệu năng của Kaspersky Security for Virtualization Light Agent.

Cách cấu hình bảo vệ kết nối trong Light Agent trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.

2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.

3. Trong cửa sổ chính sách, hãy chọn **Chế độ Light Agent** → **Bảo vệ kết nối**.

4. Chọn hộp kiểm **Mã hóa kênh dữ liệu giữa Light Agent và Máy chủ bảo vệ**.

5. Lưu các thay đổi của bạn.

Cách cấu hình bảo vệ kết nối trong Light Agent trong Bảng điều khiển web

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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 **Light Agent Mode** → **Connection protection**.
5. Chọn hộp kiểm **Encrypt data channel between Light Agent and the Protection Server**.
6. Để áp dụng chính sách này cho máy tính, hãy đóng biểu tượng ổ khóa và lưu các thay đổi của bạn.

Cách cấu hình bảo vệ kết nối trong Light Agent trong giao diện ứng dụng

1. Trong cửa sổ chính của ứng dụng, hãy nhấn nút .
2. Trong cửa sổ cài đặt ứng dụng, trong mục **Chế độ Light Agent** hãy nhấn vào ô **Bảo vệ kết nối**.
3. Chọn hộp kiểm **Mã hóa kênh dữ liệu giữa Light Agent và Máy chủ bảo vệ**.
4. Lưu các thay đổi của bạn.

Kích hoạt Light Agent

Nếu Kaspersky Endpoint Security đang được sử dụng trong Chế độ Light Agent để bảo vệ môi trường ảo thì bạn không cần kích hoạt ứng dụng riêng. Để kích hoạt ứng dụng, bạn phải thêm khóa giấy phép vào SVM. Bạn có thể thêm khóa giấy phép vào SVM bằng tác vụ đặc biệt trong bảng điều khiển Kaspersky Security Center. Bạn không thể quản lý khóa giấy phép trong giao diện Light Agent, tuy nhiên, bạn có thể xem thông tin giấy phép (xem hình bên dưới). Bạn cũng có thể xem thông tin cấp phép Light Agent trên dòng lệnh (xem hướng dẫn bên dưới). Light Agent lấy thông tin này từ SVM. Để biết chi tiết về cách kích hoạt giải pháp và quản lý khóa giấy phép, hãy xem Trợ giúp của Kaspersky Security for Virtualization Light Agent.

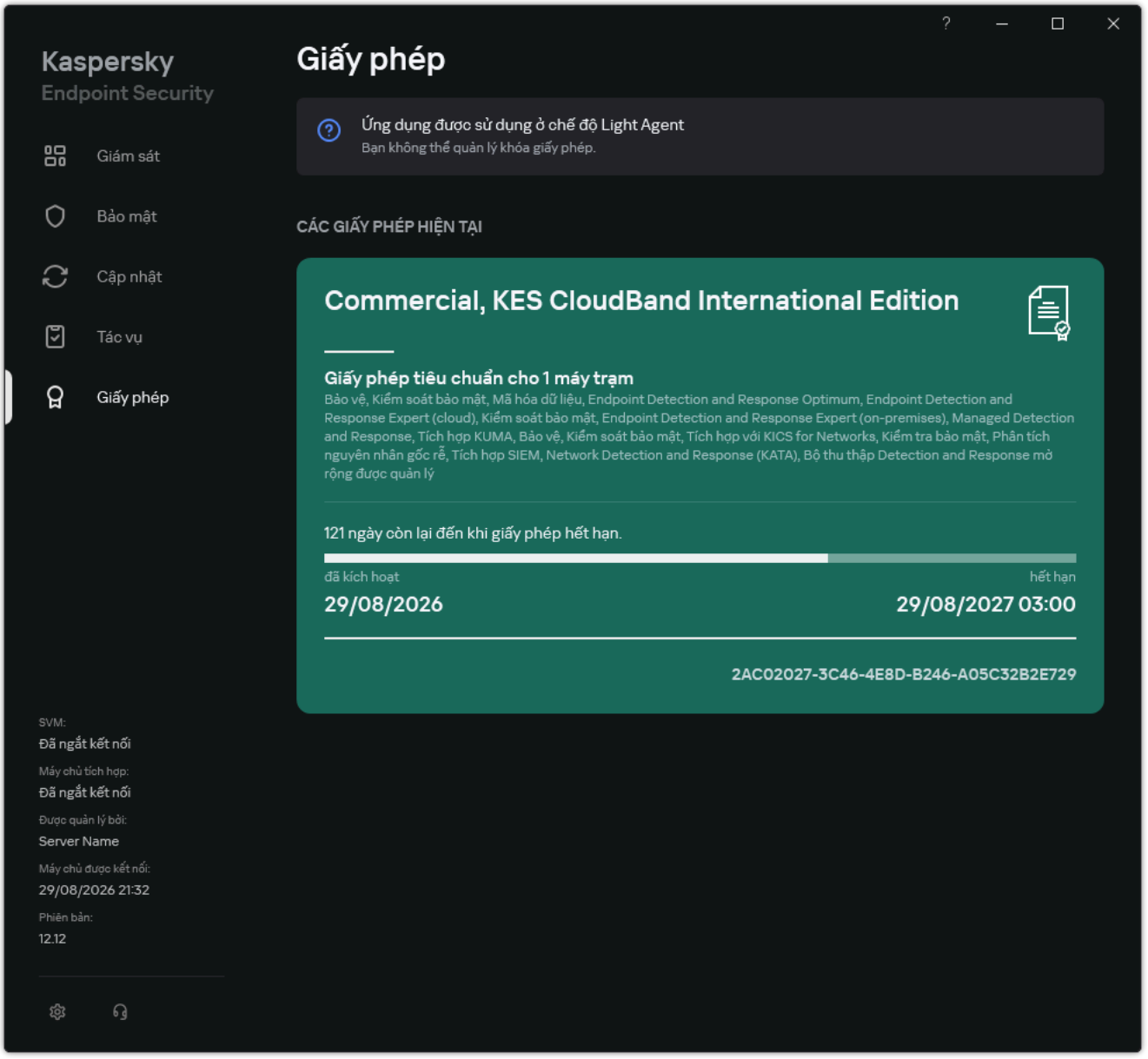
Để xem thông tin cấp phép Light Agent:

1. Chạy trình thông dịch dòng lệnh (cmd) 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 LICENSE /CHECK
```

Do đó, Kaspersky Endpoint Security hiển thị thông tin giấy phép: địa chỉ của SVM mà Light Agent được kết nối, số ngày cho đến khi giấy phép hết hạn và các thông tin khác. Nếu bạn gặp vấn đề gì khi kích hoạt Light Agent, vui lòng tham khảo Cơ sở kiến thức hỗ trợ kỹ thuật.



Cửa sổ Cấp giấy phép

Hướng dẫn chuyển từ KSVLA Light Agent sang KES Light Agent

Kaspersky Security for Virtualization 5.2 Light Agent bao gồm thành phần Light Agent cho Windows 5.2 (sau đây được gọi là "KSVLA Light Agent"). Trong Kaspersky Security for Virtualization Light Agent 6.2, Kaspersky Endpoint Security ở chế độ Light Agent được sử dụng làm thành phần Light Agent. Để cập nhật giải pháp lên phiên bản 6.2, bạn phải chuyển từ KSVLA Light Agent 5.2 sang Kaspersky Endpoint Security ở chế độ Light Agent (sau đây được gọi là "KES Light Agent"). Để biết thông tin chi tiết về việc cập nhật phiên bản giải pháp Kaspersky Security for Virtualization Light Agent, hãy xem Trợ giúp của Kaspersky Security for Virtualization Light Agent.

Yêu cầu về phần mềm

Trước khi bạn bắt đầu chuyển từ KSVLA Light Agent sang KES Light Agent, hãy đảm bảo rằng máy ảo của bạn đáp ứng các yêu cầu về phần cứng và phần mềm của Kaspersky Endpoint Security cho Windows. Danh sách các phiên bản hệ điều hành được hỗ trợ sẽ khác nhau đối với KES và KSWS. Ví dụ: KES không hỗ trợ máy chủ chạy Windows Server 2003.

Yêu cầu về phần mềm tối thiểu để chuyển từ KSVLA Light Agent sang KES Light Agent:

- Kaspersky Endpoint Security cho Windows 12.8.
- Kaspersky Security for Virtualization Light Agent 6.2 (bao gồm các thành phần Máy chủ bảo vệ và Máy chủ tích hợp).
- Kaspersky Security Center 14.2

  Nếu bạn đã cài đặt phiên bản cũ hơn của Kaspersky Security Center, hãy cập nhật đó lên phiên bản 14.2 trở lên. Trong phiên bản Kaspersky Security Center này, Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ cho phép bạn chuyển các chính sách vào một cấu hình thay vì vào một chính sách. Trong phiên bản Kaspersky Security Center này, Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ cũng cho phép bạn chuyển một dải thiết lập chính sách rộng hơn.

Các bước chuyển

Việc chuyển từ KSVLA Light Agent sang KES Light Agent được thực hiện bán tự động. Đây là điều cần thiết vì các kiến trúc khác nhau của các ứng dụng.

Chuyển từ KSVLA Light Agent sang KES Light Agent theo thứ tự sau:

1. **Chuyển các tác vụ và chính sách KSVLA Light Agent**

   Để chuyển thiết lập chính sách, bạn phải chạy Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ (trình hướng dẫn chuyển đổi). Sau khi chuyển các thiết lập chính sách, bạn phải cấu hình các thiết lập theo cách thủ công mà trình hướng dẫn chuyển đổi không thể tự động chuyển (ví dụ: thiết lập cập nhật cơ sở dữ liệu). Sau khi chuyển, bạn cũng nên kiểm tra xem trình hướng dẫn chuyển đổi có chuyển đúng tất cả các thiết lập hay không.

   > Nếu Bảo vệ bằng mật khẩu được bật để hạn chế quyền truy cập KSVLA Light Agent thì trước khi cài đặt KES Light Agent, bạn cần tắt Bảo vệ bằng mật khẩu trong chính sách của KSVLA Light Agent. Bạn không thể nhập mật khẩu gỡ cài đặt trong thiết lập gói cài đặt KES Light Agent. Sau khi hoàn tất cài đặt KES Light Agent lên trên KSVLA Light Agent, bạn phải bật Bảo vệ bằng mật khẩu trong chính sách KES.

2. **Cài đặt Kaspersky Endpoint Security ở chế độ Light Agent**

   Bạn có thể cài đặt KES Light Agent theo các cách sau:

   - Cài đặt KES Light Agent sau khi gỡ bỏ KSVLA Light Agent (khuyên dùng)
   - Cài đặt KES Light Agent trên KSVLA Light Agent

3. **Xác nhận rằng ứng dụng đang hoạt động tốt sau khi chuyển**

   Sau khi chuyển từ KSVLA Light Agent sang KES Light Agent, hãy đảm bảo rằng ứng dụng đang hoạt động đúng. Kích hoạt chính sách được chuyển đổi. Kiểm tra trạng thái của máy ảo trong bảng điều khiển Kaspersky Security Center (nên là *OK*). Đảm bảo không có lỗi nào được báo cáo cho ứng dụng, đồng thời kiểm tra thời gian kết nối cuối cùng tới SVM và trạng thái bảo vệ máy ảo. Bạn không cần phải kích hoạt Light Agent vì khóa giấy phép được thêm vào SVM.

Cài đặt KES Light Agent thay vì KSVLA Light Agent

Bạn có thể cài đặt KES Light Agent theo các cách sau:

- Cài đặt KES Light Agent sau khi gỡ bỏ KSVLA Light Agent (khuyên dùng)
- Cài đặt KES Light Agent trên KSVLA Light Agent

Gỡ bỏ KSVLA Light Agent

Bạn có thể gỡ bỏ ứng dụng từ xa bằng cách sử dụng tác vụ *Install application remotely*, cục bộ trên máy ảo hoặc trong mẫu máy ảo. Sau khi gỡ bỏ KSVLA Light Agent, bạn có thể cần phải khởi động lại máy ảo.

Sau khi gỡ bỏ KSVLA Light Agent, hãy cài đặt KES Light Agent bằng bất kỳ phương thức nào phù hợp.

Nếu Bảo vệ bằng mật khẩu được bật để hạn chế quyền truy cập KSVLA Light Agent thì trước khi cài đặt KES Light Agent, bạn cần tắt Bảo vệ bằng mật khẩu trong chính sách của KSVLA Light Agent. Bạn không thể nhập mật khẩu gỡ cài đặt trong thiết lập gói cài đặt KES Light Agent. Sau khi hoàn tất cài đặt KES Light Agent lên trên KSVLA Light Agent, bạn phải bật Bảo vệ bằng mật khẩu trong chính sách KES.

Khi cài đặt Kaspersky Endpoint Security, bạn phải chọn chế độ **Light Agent để bảo vệ môi trường ảo**. Trước khi cài đặt KES Light Agent trên một máy ảo, trình cài đặt sẽ phát hiện KSVLA Light Agent là phần mềm không tương thích và gỡ bỏ phần mềm này. Không hỗ trợ chuyển cấu hình KSVLA Light Agent. Tức là, khi bạn cài đặt KES Light Agent, bộ thành phần cần cài đặt sẽ được xác định theo lựa chọn của bạn trong thuộc tính gói cài đặt hoặc trong trình hướng dẫn cài đặt. Sau khi gỡ bỏ KSVLA Light Agent, bạn phải khởi động lại máy ảo.

Các thiết lập và tác vụ của KSVLA Light Agent sẽ không được chuyển khi bạn cài đặt KES Light Agent. Để chuyển đổi thiết lập và tác vụ, hãy chạy Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ.

Bạn có thể kiểm tra danh sách các thành phần đã cài đặt trong phần **Bảo mật** của giao diện ứng dụng, sử dụng lệnh `status` hoặc trong bảng điều khiển Kaspersky Security Center trong thuộc tính máy tính. Bạn có thể thay đổi nhóm thành phần sau khi cài đặt bằng cách sử dụng *Thay đổi thành phần ứng dụng*.

Tính tương ứng của các thành phần KSVLA Light Agent và KES Light Agent

Các nhóm thành phần của KSVLA Light Agent và KES Light Agent về cơ bản là giống nhau. KES Light Agent có nhiều thiết lập hơn KSVLA Light Agent. Sau khi chuyển, các thiết lập mới sẽ có giá trị mặc định.

Tính tương ứng của các thành phần KSVLA Light Agent và KES Light Agent

Light Agent 5.2	KES Light Agent
Scan kernel	Nhân ứng dụng
File Anti-Virus	Bảo vệ mối đe dọa tập tin
Mail Anti-Virus	Bảo vệ mối đe dọa thư điện tử
Web Anti-Virus	Bảo vệ mối đe dọa web
Firewall	Tường lửa
Network Attack Blocker	Bảo vệ mối đe dọa mạng
Application Privilege Control	Phòng chống xâm nhập máy chủ
Applications Launch Control	Kiểm soát ứng dụng
Web Control	Kiểm soát Web
Device Control	Kiểm soát thiết bị
System Watcher	Trong Kaspersky Endpoint Security, thành phần này được chia thành các thành phần sau: • Phòng chống khai thác • Phát hiện hành vi • Công cụ khắc phục
System Integrity Monitoring	Giám sát tính toàn vẹn của hệ thống

Light Agent 5.2	KES Light Agent
Integration with Kaspersky Endpoint Agent	*(không được hỗ trợ)* Kể từ Kaspersky Endpoint Security cho Windows 11.9.0, gói phân phối Kaspersky Endpoint Agent không còn thuộc bộ phân phối nữa.
AMSI Protection	Bảo vệ AMSI

Chuyển các tác vụ và chính sách KSVLA Light Agent

Bạn có thể chuyển các thiết lập của chính sách và tác vụ KSVLA Light Agent bằng Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ (sau đây còn gọi là "Trình hướng dẫn chuyển đổi").

Trình hướng dẫn chuyển đổi cho KSVLA Light Agent chỉ khả dụng trong Bảng điều khiển quản trị (MMC). Không thể chuyển thiết lập chính sách và tác vụ trong Bảng điều khiển web và Bảng điều khiển đám mây.

Những cân nhắc đặc biệt sau đây liên quan đến việc chuyển các chính sách và tác vụ:

- Một chính sách mới có tên *<Chính sách> (đã chuyển đổi)*.
- Chính sách mới có trạng thái *Inactive policy*.
- Việc cấm sửa đổi thiết lập (hình "ổ khóa") không được chuyển. Trình hướng dẫn chuyển đổi sẽ đặt các giá trị mặc định.
- Hồ sơ chính sách không được chuyển. Bạn phải thêm hồ sơ chính sách theo cách thủ công.
- Đã cải tiến quản lý vùng tin tưởng. Trong KSVLA Light Agent, bạn chỉ có thể thêm các loại trừ được định sẵn khi tạo chính sách. Sau đó, trong thuộc tính chính sách, bạn có thể cấu hình các loại trừ được định sẵn hoặc thêm các loại trừ theo cách thủ công. Bạn không thể thêm các loại trừ được định sẵn vào thuộc tính chính sách. Trong KES Light Agent, các loại trừ được định sẵn có trong quá trình tạo chính sách và trong các thuộc tính của chính sách đã tạo. Bạn cũng có thể chọn các loại trừ được định sẵn trong gói cài đặt.
- Cấu hình giao diện người dùng của ứng dụng trong Kaspersky Endpoint Security đã được chuyển từ trình cài đặt sang chính sách. Ví dụ: nếu bạn cần ẩn giao diện người dùng của ứng dụng, hãy quản lý thiết lập chính sách.
- Bộ chức năng để cấu hình kiểm soát truy cập theo quyền (RBAC) sẽ khác nhau trong Kaspersky Endpoint Security và KSVLA Light Agent. Bạn phải cấu hình quyền truy cập của người dùng vào các khu vực chức năng từ đầu.

Cách sử dụng Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ để chuyển đổi thiết lập chính sách KSVLA Light Agent

1. Trong Bảng điều khiển quản trị, chọn Máy chủ quản trị và nhấn chuột phải để mở menu ngữ cảnh.
2. Chọn **All tasks** → **Policies and tasks batch conversion wizard**.

Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ sẽ khởi chạy. Làm theo chỉ dẫn của Trình hướng dẫn.

Bước 1. Chọn ứng dụng mà bạn cần chuyển đổi chính sách và tác vụ

Tại bước này, bạn cần chọn Kaspersky Endpoint Security cho Windows. Chuyển sang bước tiếp theo.

Bước 2. Chuyển đổi chính sách

Chọn chính sách Kaspersky Security for Virtualization 5.2 Light Agent cho Windows mà bạn muốn chuyển đổi. Chuyển sang bước tiếp theo.

Khi đó, Trình hướng dẫn chuyển đổi sẽ bắt đầu chuyển đổi các chính sách. Trong quá trình chuyển đổi, Trình hướng dẫn chuyển đổi sẽ nhắc bạn chấp nhận các điều kiện của Tuyên bố KSN. Một chính sách mới có tên *<Chính sách> (đã chuyển đổi)*.

Bước 3. Chuyển đổi tác vụ

Trình hướng dẫn chuyển đổi sẽ tạo các tác vụ mới cho Kaspersky Endpoint Security cho Windows. Trong danh sách tác vụ, hãy chọn các tác vụ KSVLA Light Agent mà bạn muốn tạo cho Kaspersky Endpoint Security. Các tác vụ mới sẽ được đặt tên *<tên tác vụ> (được chuyển đổi)*. Chuyển sang bước tiếp theo.

Bước 4. Hoàn tất Trình hướng dẫn

Hoàn tất trình hướng dẫn.

Sau khi chuyển chính sách, bạn phải mở thuộc tính của chính sách, kiểm tra cài đặt và lưu chính sách. Nếu bạn không hoàn tất các bước này, KES Light Agent có thể bỏ qua chính sách đã chuyển đổi.

Đặc biệt chú ý đến việc chuyển thiết lập kết nối SVM của Light, danh sách loại trừ, ứng dụng được tin tưởng, địa chỉ web được tin tưởng, quy tắc Kiểm soát ứng dụng.

Chuyển cấu hình [KSVLA Light Agent+KEA] sang cấu hình [KES Light Agent+tác nhân tích hợp]

Một tác nhân tích hợp đã được thêm vào ứng dụng để hỗ trợ sử dụng Kaspersky Endpoint Security cho Windows như một phần của EDR (KATA), EDR Optimum, Kaspersky Sandbox. Bạn không còn cần một ứng dụng Kaspersky Endpoint Agent riêng để hoạt động với các giải pháp này.

Khi chuyển từ KSVLA Light Agent sang KES Light Agent, giải pháp EDR (KATA), EDR Optimum, Kaspersky Sandbox sẽ tiếp tục hoạt động với các tác nhân tích hợp của Kaspersky Endpoint Security. Ngoài ra, Kaspersky Endpoint Agent sẽ bị gỡ bỏ khỏi máy tính.

Trước khi chuyển từ KSVLA Light Agent sang KES Light Agent, bạn phải cập nhật tất cả các thành phần của Kaspersky Security for Virtualization lên phiên bản 6.2, bao gồm máy chủ Bảo vệ và Máy chủ tích hợp. Để biết thông tin chi tiết về việc cập nhật phiên bản giải pháp Kaspersky Security for Virtualization Light Agent, hãy xem Trợ giúp của Kaspersky Security for Virtualization Light Agent.

Việc chuyển cấu hình [KSVLA Light Agent+KEA] sang [KES Light Agent+tác nhân tích hợp] liên quan đến các bước sau:

1. **Chuyển chính sách và các tác vụ**

   Chuyển chính sách và tác vụ [KSVLA Light Agent+KEA] sang [KES Light Agent+tác nhân tích hợp] liên quan đến các bước sau:

   1. Chuyển các chính sách và tác vụ từ KSVLA Light Agent sang KES Light Agent bằng Trình hướng dẫn chuyển đổi hàng loạt chính sách và tác vụ (chỉ khả dụng trên Bảng điều khiển quản trị (MMC)).

      Kết quả là, một chính sách mới được tạo với tên *<Chính sách> (đã chuyển đổi)*. Các tác vụ KES mới cũng được tạo bằng tên *<Tên tác vụ> (được chuyển đổi)*.

   2. Chuyển các chính sách và tác vụ từ KEA sang KES bằng trình hướng dẫn chuyển đổi từ Kaspersky Endpoint Agent (chỉ khả dụng trong Bảng điều khiển web và Bảng điều khiển đám mây).

      Kết quả là, một chính sách mới được tạo với tên *<Tên của chính sách Kaspersky Endpoint Security> & <Tên của chính sách Kaspersky Endpoint Agent>*. Các tác vụ mới và tác vụ KES cũng được tạo.

2. **Chuyển từ KSVLA Light Agent sang KES Light Agent**

   Chuyển từ KSVLA Light Agent sang KES Light Agent liên quan đến cài đặt KES Light Agent thay vì KSVLA Light Agent.

   Quản trị viên thường bật Bảo vệ bằng mật khẩu để hạn chế quyền truy cập KSVLA Light Agent và KEA. Bạn chỉ có thể nhập mật khẩu gỡ cài đặt KEA vào thuộc tính của tác vụ *Install application remotely*. Khi chuyển, bạn phải tắt tính năng bảo vệ bằng mật khẩu cho KSVLA Light Agent.

   Để thực hiện việc chuyển đổi, bạn phải chọn các thành phần cần thiết để hỗ trợ các giải pháp Detection and Response như một phần của Kaspersky Endpoint Security. Sau khi cài đặt ứng dụng, Kaspersky Endpoint Security sẽ chuyển sang sử dụng tác nhân tích hợp và gỡ bỏ Kaspersky Endpoint Agent.

3. **Chức năng cấp giấy phép**

   Nếu ứng dụng đang được sử dụng trong chế độ Light Agent thì bạn không cần kích hoạt ứng dụng. Để kích hoạt ứng dụng, bạn phải thêm khóa giấy phép vào SVM. Bạn cũng phải thêm khóa giấy phép để kích hoạt chức năng bổ sung (ví dụ: EDR Optimum) vào SVM. Tức là, việc cấp phép chức năng sẽ diễn ra tự động như một phần của quá trình chuyển đổi.

4. **Kiểm tra tình trạng của Kaspersky Endpoint Detection and Response Optimum và Kaspersky Sandbox**

Nếu sau khi nâng cấp, máy tính có trạng thái *Critical* trong bảng điều khiển Kaspersky Security Center:

- Đảm bảo rằng máy tính được cài đặt Network Agent phiên bản 13.2 trở lên.
- Kiểm tra trạng thái hoạt động của tác nhân tích hợp bằng cách xem *Report on status of application components*. Nếu một thành phần có trạng thái *Not installed* thì hãy cài đặt thành phần này bằng cách sử dụng tác vụ *Change application components*.
- 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 *Report on status of application components*. 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.
- Kiểm tra trạng thái kết nối của máy ảo với SVM. Bạn có thể nhận thông tin về trạng thái kết nối của Light Agent với SVM trong Kaspersky Endpoint Security hoặc bằng cách sử dụng lệnh của ứng dụng.

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 chạy lệnh `avp.com HELP`. Để đọc về cú pháp của một lệnh cụ thể, nhập `avp.com HELP <command>`.

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 `%%`.

Các giá trị thay thế cho `1` là các giá trị `yes`, `on`, `enable`, `enabled`, và `true`. Các giá trị thay thế cho `0` là các giá trị `no`, `off`, `disable`, `disabled`, và `false`.

Setup. Cài đặt ứng dụng

Cài đặt ứng dụng từ dòng lệnh bao gồm các bước sau:

1. **Chọn gói phân phối**

   Kaspersky cung cấp các gói phân phối cho nhiều ngôn ngữ khác nhau, tương thích với các kiến trúc CPU khác nhau và bao gồm các mô-đun mã hóa khác nhau.

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

   - **AES256**

     Gói phân phối này được dùng để cài đặt trên các máy tính có kiến trúc x86/x64. Gói phân phối này chứa các công cụ mật mã để triển khai thuật toán mã hóa AES (Advanced Encryption Standard) với độ dài khóa hiệu quả là 256 bit.

   - **AES56**

     Gói phân phối này được dùng để cài đặt trên các máy tính có kiến trúc x86/x64. 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.

   - **Arm64**

     Gói phân phối này được thiết kế để cài đặt trên các máy tính chạy trên kiến trúc Arm. Gói phân phối này không được dùng để cài đặt trên máy chủ.

2. **Chuyển gói phân phối ứng dụng vào bộ nhớ của máy tính**

   Gói phân phối là một tệp lưu trữ tự giải nén ở định dạng EXE. Để xem nội dung của gói phân phối, bạn cần giải nén tệp lưu trữ vào một thư mục riêng. Để cài đặt ứng dụng, bạn cần tất cả các tập tin từ gói phân phối, bao gồm cả tập tin bases.cab.

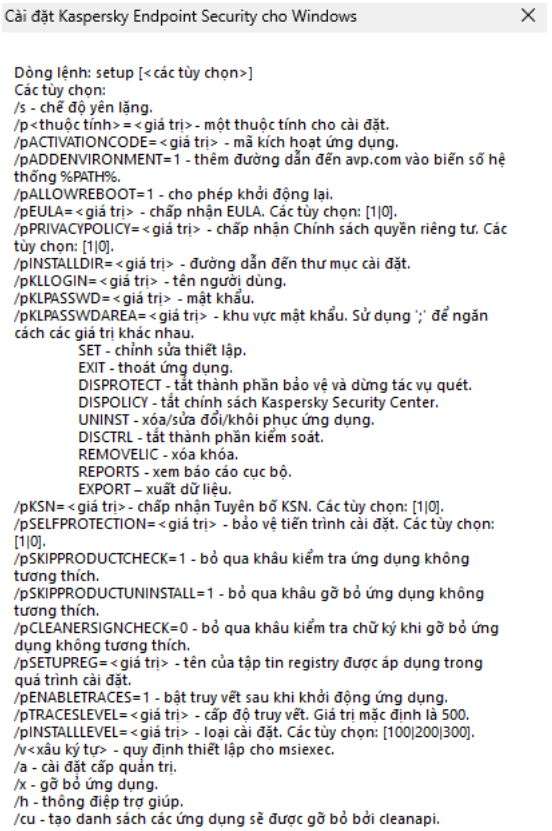
3. **Chạy lệnh cài đặt**

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 (cài đặt im lặng). 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.

Bạn có thể xem danh sách các lệnh để cài đặt ứng dụng bằng cách chạy lệnh `/h`. Để nhận trợ giúp về cú pháp lệnh cài đặt, hãy nhập `setup_kes.exe /h`. Kết quả là trình cài đặt sẽ hiển thị một cửa sổ kèm mô tả các tùy chọn lệnh (xem hình bên dưới).



Mô tả các tùy chọn lệnh cài đặt

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] [/pCONFIGPATH=<path to the configuration file>]
[/pALLOWREBOOT=1] [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<user name> /pKLPASSWD=
<password> /pKLPASSWDAREA=<password scope>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<tracing level>]
[/pSKIPKB5007186CHECK=1] [/s]
```

hoặc

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [CONFIGPATH=<path to the configuration
file>] [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<user name> KLPASSWD=<password> KLPASSWDAREA=<password
scope>] [ENABLETRACES=1|0 TRACESLEVEL=<tracing level>] [SKIPKB5007186CHECK=1] [/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`.

Thiết lập cài đặt ứng dụng

`EULA=1`	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. Việc chấp nhận các điều khoản của Thỏa thuận giấy phép người dùng cuối là cần thiết để cài đặt ứng dụng hoặc nâng cấp phiên bản ứng dụng.
`PRIVACYPOLICY=1`	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. Để cài đặt ứng dụng hoặc nâng cấp ứng dụng phiên bản ứng dụng, bạn phải chấp nhận Chính sách quyền riêng tư.
`KSN`	Đồng ý hoặc từ chối tham gia Kaspersky Security Network (KSN). Nếu không có giá trị nào được thiết lập cho tham số này, Kaspersky Endpoint Security sẽ nhắc bạn xác nhận sự đồng ý hoặc từ chối tham gia KSN khi Kaspersky Endpoint Security được khởi động lần đầu. Giá trị khả dụng: • `1` – đồng ý tham gia KSN. • `0` – từ chối tham gia KSN (giá trị mặc định). Gói phân phối Kaspersky Endpoint Security được tối ưu cho việc sử dụng với Kaspersky Security Network. Nếu bạn không chọn tham gia Kaspersky Security Network, bạn nên cập nhật Kaspersky Endpoint Security ngay sau khi hoàn tất cài đặt.
`CONFIGPATH=<path to the configuration file>`	Cài đặt ứng dụng bằng các thiết lập được định sẵn. Để thực hiện, bạn cần tải lên một tập tin định nghĩa thiết lập của Kaspersky Endpoint Security. Bạn có thể tạo một tập tin cấu hình trong giao diện cục bộ của ứng dụng.
`ALLOWREBOOT=1`	Tự động khởi động lại máy tính nếu cần thiết sau khi cài đặt hoặc nâng cấp ứng dụng. Nếu không có giá trị nào được đặt cho tham số này thì việc tự động khởi động lại máy tính sẽ bị chặn. Không cần khởi động lại khi cài đặt Kaspersky Endpoint Security. Chỉ cần khởi động lại nếu bạn 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.
`SKIPPRODUCTCHECK=1`	Tắt kiểm tra phần mềm đã cài đặt. Danh sách phần mềm có thể gây ra sự cố tương thích có trong tập tin incompatible.txt có trong gói phân phối. Nếu không có giá trị nào được đặt cho tham số này và phần mềm trong danh sách được phát hiện thì quá trình cài đặt Kaspersky Endpoint Security sẽ bị chấm dứt.
`SKIPPRODUCTUNINSTALL=1`	Tắt tính năng tự động gỡ bỏ phần mềm được phát hiện khỏi danh sách incompatible.txt. Nếu không có giá trị nào được đặt cho tham số này, Kaspersky Endpoint Security sẽ cố gắng gỡ bỏ phần mềm có thể gây ra sự cố tương thích. Không thể bật tính năng tự động gỡ bỏ phần mềm khi cài đặt Kaspersky Endpoint Security bằng trình cài đặt msiexec. Để tự động gỡ bỏ phần mềm có thể gây ra sự cố tương thích, hãy sử dụng tập tin setup_kes.exe.

CLEANERSIGNCHECK=0|1	Xác minh chữ ký số của các tập tin phần mềm được phát hiện từ danh sách incompatible.txt. Để gỡ bỏ phần mềm, Kaspersky Endpoint Security sẽ chạy tập tin cài đặt phần mềm. Nếu tập tin bộ cài đặt không có chữ ký số thì Kaspersky Endpoint Security sẽ coi tập tin đó là không được tin tưởng và sẽ tạm dừng việc gỡ bỏ phần mềm để tránh chạy mã độc hại tiềm ẩn. Nếu ứng dụng không thể xác minh chữ ký số của tập tin phần mềm được phát hiện thì quá trình cài đặt Kaspersky Endpoint Security sẽ bị dừng kèm một lỗi. Giá trị mặc định sẽ khác nhau, tùy thuộc vào phương thức cài đặt phần mềm: • 0 có nghĩa là khâu xác minh chữ ký số bị tắt (giá trị mặc định nếu được triển khai thông qua Kaspersky Security Center). • 1 có nghĩa là khâu xác minh chữ ký số được bật (giá trị mặc định nếu ứng dụng đang được cài đặt cục bộ).
STANDALONEMODE=1	Cài đặt ứng dụng trong cấu hình Endpoint Detection and Response Agent (EDR Agent) để tích hợp với giải pháp Kaspersky Endpoint Detection and Response (KATA) hoặc Kaspersky Endpoint Detection and Response Expert (on-premises). Đây là cấu hình cần thiết nếu Endpoint Protection Platform (EPP) của bên thứ ba được triển khai trong tổ chức của bạn cùng với giải pháp lớp Kaspersky Endpoint Detection and Response. Điều này làm cho Kaspersky Endpoint Security trong cấu hình Endpoint Detection and Response Agent tương thích với các ứng dụng EPP của bên thứ ba.
KLLOGIN	Thiết lập tên người dùng để truy cập các tính năng và thiết lập của Kaspersky Endpoint Security (thành phần Mật khẩu). Tên người dùng được quy định cùng với các thiết lập KLPASSWD và KLPASSWDAREA. Tên người dùng KLAdmin được sử dụng theo mặc định.
KLPASSWD	Quy định một mật khẩu để truy cập các tính năng và cấu hình của Kaspersky Endpoint Security (mật khẩu được quy định cùng với các tham số KLLOGIN và KLPASSWDAREA). Nếu bạn quy định một mật khẩu nhưng không quy định tên người dùng với tham số KLLOGIN, tên người dùng mặc định KLAdmin sẽ được sử dụng.
KLPASSWDAREA	Quy định phạm vi của mật khẩu để truy cập Kaspersky Endpoint Security. Khi người dùng cố gắng thực hiện một hành động có 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: • 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. • EXPORT – xuất thiết lập ứng dụng. Ví dụ: KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT. Tài khoản KLAdmin có quyền thực hiện mọi hành động được bảo vệ bởi mật khẩu. Do đó, cấu hình phạm vi mật khẩu cho tài khoản KLAdmin là điều không thể. Nếu bạn thử cấu hình phạm vi mật khẩu cho tài khoản KLAdmin, ứng dụng sẽ cấm các hành động được chỉ định cho nhóm "Mọi người".
PROTECTOSSERVICES	Bảo vệ chức năng của dịch vụ hệ điều hành. Tính năng bảo vệ dịch vụ hệ điều hành sẽ ngăn các ứng dụng của bên thứ ba can thiệp vào hoạt động của các dịch vụ hệ điều hành. Ví dụ: các dịch vụ đó bao gồm dịch vụ tự động khởi chạy ứng dụng. • 1 có nghĩa là tính năng bảo vệ dịch vụ hệ điều hành được bật (giá trị mặc định). • 0 có nghĩa là tính năng bảo vệ dịch vụ hệ điều hành bị tắt.
ENABLETRACES	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.14.2\Traces. Giá trị khả dụng: • 1 – truy vết được bật. • 0 – truy vết bị tắt (giá trị mặc định).
TRACESLEVEL	Cấp chi tiết dấu vết. Giá trị khả dụng: • 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). • 600 (thấp). Tất cả các thông báo.

ENABLEAZURESUPPORT	Bật hoặc tắt chế độ tương thích Azure WVD. Giá trị khả dụng: • 1 – Chế độ tương thích Azure WVD được bật. • 0 – Chế độ tương thích Azure WVD bị tắt (giá trị mặc định). Tính năng này đảm bảo hiển thị chính xác trạng thái máy ảo Azure trong bảng điều khiển Kaspersky Anti Targeted Attack Platform. Để theo dõi hiệu năng của máy tính, Kaspersky Endpoint Security sẽ gửi thông tin đo từ xa đến các máy chủ KATA. Thông tin đo từ xa chứa một ID của máy tính (Sensor ID). Chế độ tương thích Azure WVD cho phép gán Sensor ID duy nhất vĩnh viễn cho các máy ảo này. Nếu chế độ tương thích bị tắt thì Sensor ID có thể thay đổi sau khi máy tính được khởi động lại do cách máy ảo Azure hoạt động. Điều này có thể khiến các máy ảo trùng lặp xuất hiện trên bảng điều khiển.
AMPPL	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. Công nghệ AM-PPL có sẵn trên hệ điều hành Windows 10 phiên bản 1703 (RS2) hoặc mới hơn và Windows Server 2019. Giá trị khả dụng: • 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.
UPGRADEMODE	Chế độ nâng cấp ứng dụng: • Seamless nghĩa là nâng cấp ứng dụng bằng cách khởi động lại máy tính (giá trị mặc định). • Force có nghĩa là nâng cấp ứng dụng mà không cần khởi động lại. Bạn có thể nâng cấp ứng dụng mà không cần khởi động lại kể từ phiên bản 11.10.0. Bạn phải khởi động lại máy tính để nâng cấp phiên bản cũ hơn của ứng dụng. Bạn cũng có thể cài đặt các bản vá mà không cần khởi động lại kể từ phiên bản 11.11.0. Không cần khởi động lại khi cài đặt Kaspersky Endpoint Security. Vì vậy, chế độ nâng cấp của ứng dụng sẽ được chỉ định trong thiết lập ứng dụng. Bạn có thể thay đổi tham số này trong thiết lập ứng dụng hoặc trong chính sách. Khi nâng cấp ứng dụng đã được cài đặt, mức ưu tiên của tham số dòng lệnh thấp hơn mức ưu tiên của tham số được chỉ định trong thiết lập ứng dụng hoặc trong tập tin setup.ini. Ví dụ: nếu chế độ nâng cấp Force được chỉ định trong dòng lệnh và chế độ Seamless được chỉ định trong thiết lập ứng dụng thì bản nâng cấp sẽ được cài đặt khi khởi động lại máy tính (Seamless).
RESTAPI	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). Giá trị khả dụng: • 1 - quản lý thông qua REST API được cho phép. • 0 - quản lý thông qua REST API bị chặn (giá trị mặc định). 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.
RESTAPI_User	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>\<UserName> (ví dụ: RESTAPI_User=COMPANY\Administrator). Bạn chỉ có thể chọn một người dùng để làm việc với REST API. Thêm tên người dùng là điều kiện tiên quyết để quản lý ứng dụng thông qua REST API.
RESTAPI_Port	Cổng được sử dụng để quản lý ứng dụng thông qua REST API. Cổng 6782 được sử dụng theo mặc định. Đảm bảo rằng cổng chưa được sử dụng.
RESTAPI_Certificate	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.
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: • 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.

`EnableUniqueSensorID`	Tạo định danh máy tính duy nhất (Sensor ID) trong quá trình cài đặt hoặc cập nhật ứng dụng. Sensor ID được sử dụng trong giải pháp Kaspersky Anti Targeted Attack Platform để xác định các máy tính gửi dữ liệu từ xa đến máy chủ. Khi tạo Sensor ID, ứng dụng sẽ sử dụng một thuật toán có cân nhắc đến cấu hình của máy tính như số sê-ri của bo mạch chủ. Trong một số trường hợp, ví dụ như khi sử dụng ứng dụng trong môi trường ảo, Sensor ID có thể bị trùng lặp. Do đó, Kaspersky Anti Targeted Attack Platform không thể xác định được máy tính nào đã gửi dữ liệu từ xa. Để tạo một Sensor ID duy nhất, bạn cần đặt tham số `EnableUniqueSensorID=1`. Kết quả là ứng dụng sẽ sử dụng một thuật toán khác để tạo Sensor ID, thuật toán này sẽ cân nhắc đến các dữ liệu khác về máy tính. Làm vậy sẽ đảm bảo có một Sensor ID duy nhất. Theo mặc định, tham số này không được đặt. Ứng dụng kế thừa Sensor ID trong các trường hợp sau: • Cập nhật phiên bản của ứng dụng; • chuyển cấu hình [KES+KEA] sang cấu hình [KES+tác nhân tích hợp]. Là một phần của quá trình sửa ứng dụng, do đó trình cài đặt sẽ cố gắng kế thừa Sensor ID. Nếu không thể khôi phục Sensor ID, ứng dụng sẽ tạo ra một Sensor ID mới.
`SKIPKB5007186CHECK=1`	Tắt kiểm tra bản cập nhật hệ điều hành đã cài đặt KB5007186. Trước khi cài đặt ứng dụng, trình cài đặt sẽ kiểm tra các bản cập nhật hệ điều hành đã cài đặt. Bản cập nhật KB5007186 thuộc một trong các bản cập nhật hệ điều hành có thể gây ra sự cố cho ứng dụng. Để biết thông tin chi tiết, hãy tham khảo Cơ sở tri thức Hỗ trợ kỹ thuật. Do đó, trình cài đặt sẽ hủy quá trình cài đặt nếu phát hiện bản cập nhật này. Để tiếp tục quá trình cài đặt, hãy đặt `SKIPKB5007186CHECK=1`.

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 cho bản cài đặt ứng dụng.

  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.

- install.cfg – thiết lập hoạt động của Kaspersky Endpoint Security

  Để áp dụng thiết lập từ tập tin cấu hình install.cfg, bạn cần chỉ định đường dẫn đến tập tin trong lệnh cài đặt ứng dụng sau: `CONFIGPATH=<path to the configuration file>`.

- 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 tập tin setup.reg, hãy đặt 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=<path to the setup.reg file>`.

Setup /x. 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 quá trình gỡ bỏ được bắt đầu ở chế độ im lặng, bạn không cần tham gia vào quá trình gỡ bỏ (gỡ bỏ im lặng). 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 trong Cơ sở tri thức hỗ trợ kỹ thuật hoặc 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 /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
     ```

     hoặc

     ```
     msiexec.exe /x <GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

Bạn cũng có thể sử dụng tham số `SAVEQB` để lưu các tập tin được ứng dụng quét và đặt vào Sao lưu. Những bản sao lưu của các tập tin được lưu trữ trong thư mục `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`. Theo mặc định, việc lưu tập tin vào Sao lưu bị tắt (`SAVEQB=0`).

Ví dụ

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

msiexec /i. Phục hồi ứng dụng

Khi khôi phục, ứng dụng sẽ kiểm tra và khôi phục tính toàn vẹn của tất cả các mô-đun ứng dụng bị hỏng và khóa registry hệ thống được tạo trong quá trình cài đặt ứng dụng.

Có thể khôi phục Kaspersky Endpoint Security 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 hành khôi phục trong chế độ im lặng, bạn không cần tham gia vào quá trình khôi phục.

Nếu trình cài đặt Kaspersky Endpoint Security đang chạy ở chế độ khôi phục và ứng dụng không cần khôi phục thì trình cài đặt sẽ không thực hiện bất kỳ thay đổi nào.

Nếu trình cài đặt Kaspersky Endpoint Security đang chạy ở chế độ khôi phục và ứng dụng chưa được cài đặt thì trình cài đặt sẽ bắt đầu quá trình cài đặt.

Để khôi phục 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 quá trình khôi phục không được bảo vệ bằng mật khẩu:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL /qn
     ```

     <GUID> và ID duy nhất của ứng dụng. Bạn có thể tìm ra GUID của ứng dụng trong Cơ sở tri thức hỗ trợ kỹ thuật hoặc bằng lệnh sau:

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

   - Nếu quá trình khôi phục được bảo vệ bằng mật khẩu:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

Ví dụ

```
msiexec.exe /i {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} REINSTALL=ALL KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

Các lệnh AVP

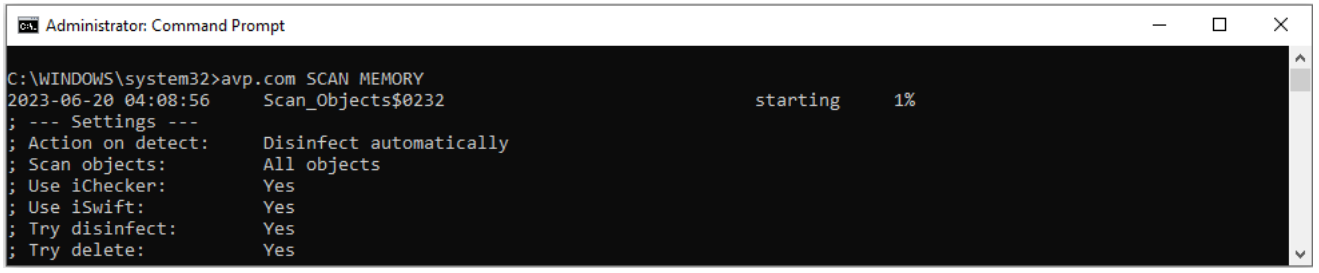
Để quản lý Kaspersky Endpoint Security từ dòng lệnh:

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.

   Bạn có thể thêm đường dẫn đến tập tin thực thi vào biến hệ thống %PATH% trong khi cài đặt ứng dụng.
3. Sử dụng mẫu sau để thực thi lệnh:

```
avp.com <command> [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 phần mềm độc hại

Chạy tác vụ *Quét phần mềm độc hại*.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com SCAN [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>] [/C:<file with scan settings>]
```

Phạm vi quét	
`<files to scan>`	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: • `"C:\Program Files (x86)\Example Folder"` – đường dẫn dài. • `C:\PROGRA~2\EXAMPL~1` – đường dẫn ngắn.

`/ALL`	Chạy tác vụ *Quét phần mềm độc hại*. 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 Trong Kaspersky Endpoint Security cho Windows 12.12, email không nằm trong phạm vi quét ứng dụng. Tác vụ quét các email đến và đi được thực hiện bởi Thành phần Bảo vệ mối đe dọa thư điện tử. Nếu bạn đang sử dụng phiên bản cũ hơn của tiện ích quản lý, ứng dụng sẽ loại trừ email khỏi phạm vi quét ngay cả khi chính sách bao gồm email.
`/MEMORY`	Quét bộ nhớ Kernel
`/STARTUP`	Quét các đối tượng được nạp lúc khởi động hệ điều hành
`/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>`	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: • `"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; 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 khử mã độc thất bại, 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 chọn tùy chọn này, ứng dụng sẽ tự động cố gắng khử mã độc tập tin bị nhiễm được phát hiện. Nếu không thể khử mã độc, ứng dụng sẽ xóa tập tin đó. Hành động này được chọn theo mặc định.
`/i3`	**Xóa nếu khử mã độc thất bại**. 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**. 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, ứng dụng 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, ứng dụng 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, ứng dụng sẽ kiểm tra tất cả các tập tin mà không có loại trừ (tất cả các định dạng và đuôi 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:<file mask>`	Các tập tin khớp với tên đại diện tập tin được loại trừ khỏi phạm vi quét. Ví dụ: • 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:<seconds>`	Các tập tin cần nhiều thời gian để quét hơn giới hạn quy định (tính theo giây) được loại trừ khỏi phạm vi quét.
`-es:<megabytes>`	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:<report file>`	Chỉ lưu các sự kiện nghiêm trọng đến tập tin báo cáo.
`/RA:<report file>`	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 tác vụ 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 tác vụ 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 iSwift được cải tiến từ công nghệ iChecker cho hệ thống tập tin NTFS.

Thiết lập nâng cao	
`/C:<file with scan settings>`	Tập tin chứa thiết lập cho tác vụ *Quét phần mềm độc hại*. Tập tin này phải được tạo thủ công và lưu trong định dạng TXT. Tập tin này có các nội dung sau: `[<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>].`

Ví dụ

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP "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 cơ sở dữ liệu và mô-đun ứng dụng*.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

> Không thể chạy lệnh này nếu ứng dụng được cài đặt ở chế độ Light Agent.

Cú pháp lệnh

```
avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<file with update settings>]
```

Cấu hình tác vụ cập nhật	
`local`	Bắt đầu tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* được tạo tự động sau khi ứng dụng được cài đặt. Bạn có thể thay đổi thiết lập của tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* 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 *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* bằng thiết lập mặc định hoặc bằng thiết lập được chỉ định trong lệnh. Bạn có thể cấu hình thiết lập tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* như sau: • `UPDATE` bắt đầu tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* 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 *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* được tạo tự động sau khi cài đặt (tác vụ được định nghĩa trước). • `UPDATE <update settings>` bắt đầu tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* bằng thiết lập được định nghĩa theo cách thủ công (xem bên dưới).

Nguồn cập nhật	
`"<update source>"`	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.

Lưu sự kiện vào chế độ tập tin báo cáo (chỉ dành cho cấu hình Quét, Trình cập nhật và Khôi phục)	
`/R:<report file>`	Chỉ lưu các sự kiện nghiêm trọng đến tập tin báo cáo.
`/RA:<report file>`	Lưu tất cả các sự kiện đến một tập tin báo cáo.

Thiết lập nâng cao	
`/C:<file with update settings>`	Tập tin chứa thiết lập cho tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*. Tập tin này phải được tạo thủ công và lưu trong định dạng TXT. Tập tin này có các nội dung sau: `["<update source>"] [/R[A]:<report file>]`.

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.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

> Không thể chạy lệnh này nếu ứng dụng được cài đặt ở chế độ Light Agent.

Cú pháp lệnh

```
avp.com ROLLBACK [/R[A]:<report file>]
```

Lưu sự kiện vào chế độ tập tin báo cáo (chỉ dành cho cấu hình Quét, Trình cập nhật và Khôi phục)	
`/R:<report file>`	Chỉ lưu các sự kiện nghiêm trọng đến tập tin báo cáo.
`/RA:<report file>`	Lưu tất cả các sự kiện đến một tập tin báo cáo.

Ví dụ

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. 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.14.2\Traces`. Theo mặc định, truy vết được tắt.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com TRACES on|off [<tracing level>] [<advanced settings>]
```

Cấp độ truy vết	
`<tracing level>`	Cấp chi tiết dấu vết. Giá trị khả dụng: • `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). • `600` (thấp). Tất cả các thông báo.

Thiết lập nâng cao	
`all`	Chạy một lệnh với các tham số `file` và `mem`.
`file`	Lưu một tập tin dấu vết (không có giới hạn kích cỡ).

`rot`	Lưu dấu vết vào một số bộ 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 off
```

```
avp.com TRACES on 500 mem
```

```
avp.com TRACES off file
```

START. Bắt đầu một hồ sơ

Bắt đầu một hồ sơ (ví dụ: bắt đầu cập nhật cơ sở dữ liệu hoặc bật một thành phần bảo vệ).

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com START <profile> [/R[A]:<report file>]
```

Hồ sơ	
`<profile>`	Tên hồ sơ. *Hồ sơ* 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 chạy lệnh `HELP START`.

Lưu sự kiện vào chế độ tập tin báo cáo (chỉ dành cho cấu hình Quét, Trình cập nhật và Khôi phục)	
`/R:<report file>`	Chỉ lưu các sự kiện nghiêm trọng đến tập tin báo cáo.
`/RA:<report file>`	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 thực thi hồ sơ (ví dụ: 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**.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com STOP <profile> /login=<user name> /password=<password>
```

Hồ sơ	
`<profile>`	Tên hồ sơ. *Hồ sơ* 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 chạy lệnh `HELP STOP`.

Xác thực	
`/login=<user name> /password=<password>`	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: `running` hoặc `completed`). Bạn có thể xem danh sách các hồ sơ khả dụng bằng cách chạy 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.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com STATUS [<profile>]
```

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

Hiển thị số liệu 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`.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com STATISTICS <profile>
```

RESTORE. Khôi phục các tập tin từ Sao lưu

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. Người dùng 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 của các tập tin được lưu trữ trong thư mục `C:\ProgramData\Kaspersky Lab\KES.14.2\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.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Thiết lập nâng cao	
`/REPLACE`	Ghi đè lên một tập tin hiện có.
`<file name>`	Tên của tập tin được khôi phục.

Xác thực	
`/login=<user name> /password=<password>`	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=samplePassword
```

EXPORT. Xuất thiết lập ứng dụng

Xuất thiết lập của Kaspersky Endpoint Security ra một tập tin. Nếu lệnh chỉ chứa tên của tập tin mà bạn muốn xuất thiết lập thì ứng dụng sẽ đặt tập tin như sau:

- Nếu đường dẫn đến avp.com được thêm vào biến hệ thống %PATH% thì ứng dụng sẽ đặt tập tin vào thư mục `C:\Windows\SysWOW64`.
- Nếu bạn chạy lệnh từ thư mục cài đặt ứng dụng, thao tác xuất sẽ không thành công vì tính năng tự bảo vệ của ứng dụng sẽ chặn tạo tập tin mới trong thư mục ứng dụng. Để xuất thiết lập ứng dụng ra tập tin, hãy nhập đường dẫn tập tin.

Để thực thi lệnh này, Bảo vệ bằng mật khẩu phải được bật. Người dùng phải có quyền **Xuất thiết lập**.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com EXPORT <profile> <file name> /login=<user name> /password=<password>
```

Hồ sơ	
`<profile>`	Tên hồ sơ. *Hồ sơ* 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 chạy lệnh `HELP EXPORT`.

Tập tin để xuất	
`<file name>`	Tên của tập tin mà thiết lập ứng dụng sẽ được xuất ra đó. Bạn cũng có thể nhập đường dẫn tập tin. 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.

Xác thực	
`/login=<user name> /password=<password>`	Thông tin đăng nhập vào tài khoản người dùng với các quyền Bảo vệ bằng mật khẩu cần thiết.

Ví dụ

```
avp.com EXPORT ids ids_C:\Users\Fred123\Documents\config.dat
```

```
avp.com EXPORT fm fm_config.txt
```

IMPORT. Nhập thiết lập ứng dụng

Nhập thiết lập Kaspersky Endpoint Security từ tập tin đã được tạo bằng lệnh `EXPORT`.

Để thực thi lệnh này, Bảo vệ bằng mật khẩu phải được bật. Người dùng phải có quyền **Cấu hình thiết lập ứng dụng**.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com IMPORT <file name> /login=<user name> /password=<password>
```

Tập tin để nhập	
`<file name>`	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.

Xác thực	
`/login=<user name> /password=<password>`	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=samplePassword
```

ADDKEY. Áp dụng một tập tin khóa

Kích hoạt Kaspersky Endpoint Security bằng một tập tin khóa. Nếu ứng dụng đã được kích hoạt, khóa sẽ được thêm làm khóa dự trữ.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

> Không thể chạy lệnh này nếu ứng dụng được cài đặt ở chế độ Light Agent.

Cú pháp lệnh

```
avp.com ADDKEY <file name> [/login=<user name> /password=<password>]
```

Key file	
<file name>	Tên tập tin khóa.

Xác thực	
/login=<user name> /password=<password>	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

Quản lý các khóa giấy phép của Kaspersky Endpoint Security, 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**.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

> Không thể chạy lệnh này nếu ứng dụng được cài đặt ở chế độ Light Agent.

Cú pháp lệnh

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

Hoạt động	
/ADD <file name>	Kích hoạt Kaspersky Endpoint Security bằng một tập tin khóa. Nếu ứng dụng đã được kích hoạt, khóa sẽ được thêm làm khóa dự trữ.
/ADD <activation code>	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 <license ID>`	Cập nhật trạng thái giấy phép bằng ID giấy phép. Sử dụng lệnh này, bạn có thể cập nhật trạng thái của Tiện ích bổ trợ EDR, Tiện ích bổ trợ MDR, Tiện ích bổ trợ KUMA hoặc các giấy phép khác. Bạn có thể lấy ID giấy phép từ giấy chứng nhận giấy phép. Do đó, ứng dụng nhận được thông tin trạng thái giấy phép cập nhật từ các máy chủ kích hoạt của Kaspersky.
`/CHECK`	Lấy thông tin giấy phép. Kaspersky Endpoint Security hiển thị thông tin về tất cả các khóa giấy phép được thêm, bao gồm khóa dự trữ, khóa Tiện ích bổ trợ EDR, khóa Tiện ích bổ trợ MDR, khóa Tiện ích bổ trợ KUMA và các khóa khác. Kaspersky Endpoint Security hiển thị các thông tin giấy phép sau: • tên giấy phép; • định danh giấy phép; • địa chỉ của Máy chủ bảo vệ (SVM) được máy ảo kết nối với và là máy ảo có ứng dụng được cài đặt ở chế độ Light Agent; • loại giấy phép: dùng thử, thương mại, beta, gói đăng ký; • ngày và thời gian kích hoạt ứng dụng; • ngày và thời gian hết hạn giấy phép; • số ngày đến khi hết hạn giấy phép.
`/CHECK <license ID>`	Lấy thông tin giấy phép theo ID. Bạn có thể sử dụng lệnh này để lấy thông tin giấy phép. Bạn có thể lấy ID giấy phép từ giấy chứng nhận giấy phép.
`/DEL /login=<user name> /password=<password>`	Xóa khóa giấy phép của ứng dụng. Khóa dự trữ cũng sẽ bị xóa.
`/DEL <license ID> /login=<user name> /password=<password>`	Xóa khóa bằng ID giấy phép. Sử dụng lệnh này, bạn có thể xóa khóa khỏi Tiện ích bổ trợ EDR, Tiện ích bổ trợ MDR, Tiện ích bổ trợ KUMA hoặc các giấy phép khác. Bạn có thể lấy ID giấy phép từ giấy chứng nhận giấy phép.

Xác thực	
`/login=<user name> /password=<password>`	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 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

Ví dụ

```
avp.com LICENSE /ADD file.key
```

```
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
```

```
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

RENEW. Mua giấy phép

Mở website Kaspersky để mua hoặc gia hạn giấy phép của bạn.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Không thể chạy lệnh này nếu ứng dụng được cài đặt ở chế độ Light Agent.

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.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

EXIT. Thoát 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**.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com EXIT /login=<user name> /password=<password>
```

EXITPOLICY. Tắt chính sách

Tắt 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**.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com EXITPOLICY /login=<user name> /password=<password>
```

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.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

DISABLE. Tắt bảo vệ

Tắt Bảo vệ mối 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.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

SPYWARE. Phát hiện phần mềm gián điệp

Quản lý phát hiện phần mềm gián điệp. Theo mặc định, tính năng phát hiện phần mềm gián điệp được bật.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com SPYWARE on|off
```

KSN. Chuyển qua lại giữa KSN / KPSN

Chọn một giải pháp Kaspersky để xác định danh tiếng của các tập tin hoặc trang web. Kaspersky Endpoint Security hỗ trợ các giải pháp cơ sở hạ tầng sau để làm việc với cơ sở dữ liệu danh tiếng của Kaspersky:

- *Kaspersky Security Network (KSN)* là giải pháp được hầu hết các ứng dụng Kaspersky sử dụng. Người tham gia vào KSN sẽ nhận thông tin từ Kaspersky 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.

- *Kaspersky Private Security Network (KPSN)* 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 và truy cập các dữ liệu thống kê khác mà không cần gửi dữ liệu cho Kaspersky từ máy tính của riêng họ. KPSN được thiết kế dành cho khách hàng doanh nghiệp, là những khách hàng 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.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Không thể chạy lệnh này nếu ứng dụng được cài đặt ở chế độ Light Agent.

Cú pháp lệnh

```
avp.com KSN /global | /private <file name>
```

Tập tin cấu hình Kaspersky Security Network	
`<file name>`	Tên của tập tin cấu hình chứa thiết lập Kaspersky Private Security Network. Tập tin này có phần mở rộng PKCS7 hoặc PEM.

Ví dụ

```
avp.com KSN /global
avp.com KSN /private C:\ksn_config.pkcs7
```

Ví dụ

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

SERVERBINDINGDISABLE. Tắt bảo vệ kết nối máy chủ

Chạy tác vụ *Bảo vệ kết nối Máy chủ quản trị*, giúp xóa bỏ mật khẩu kết nối của máy tính với Máy chủ quản trị. Bằng cách này, tác vụ đó sẽ tắt chức năng bảo vệ kết nối Máy chủ quản trị.

Để thực thi lệnh này, Bảo vệ bằng mật khẩu phải được bật.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com SERVERBINDINGDISABLE [/password=<password>]
```

Mật khẩu	
`/password=<password>`	Mật khẩu của tài khoản người dùng KLAdmin hoặc mật khẩu từ tác vụ *Bảo vệ kết nối Máy chủ quản trị*. Nếu không chỉ định tham số này, Kaspersky Endpoint Security sẽ nhắc bạn nhập mật khẩu ở dòng tiếp theo.

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 phần mềm độc hại* và *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*.

Bạn có thể xem danh sách các lệnh KESCLI bằng cách sử dụng lệnh `kescli --help` hoặc bằng cách sử dụng lệnh viết tắt `kescli -h`.

Để quản lý Kaspersky Endpoint Security từ dòng lệnh:

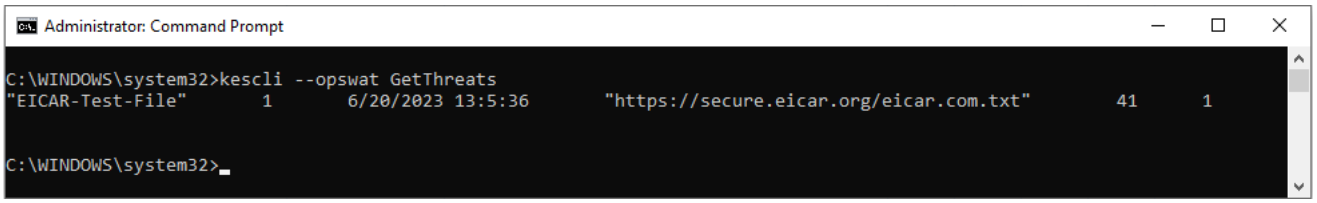
1. Chạy trình thông dịch dòng lệnh (cmd.exe) với tư cách quản trị viên.
2. Tới thư mục chứa tập tin thực thi Kaspersky Endpoint Security.

   Bạn có thể thêm đường dẫn đến tập tin thực thi vào biến hệ thống %PATH% trong khi cài đặt ứng dụng.

3. Sử dụng mẫu sau để thực thi lệnh:

```
kescli <lệnh> [tùy chọn]
```

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 phần mềm độc hại

Chạy tác vụ *Quét phần mềm độc hại* (Quét toàn bộ).

Để chạy tác vụ, quản trị viên phải Cho phép sử dụng tác vụ cục bộ trong chính sách.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security.

Cú pháp lệnh

```
kescli --opswat Scan "<scan scope>" <action on threat detection>
```

Bạn có thể kiểm tra trạng thái hoàn thành của tác vụ *Quét phần mềm độc hại* 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	
`<scan scope>`	Một danh sách các tập tin và thư mục được ngăn cách bởi dấu `;`. Ví dụ: `"C:\Program Files (x86)\Example Folder"`.

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 chọn tùy chọn này, ứng dụng sẽ tự động cố gắng khử mã độc tập tin bị nhiễm được phát hiện. Nếu không thể khử mã độc, ứng dụng sẽ xóa 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

Hiển thị thông tin về trạng thái hoàn thành tác vụ *Quét phần mềm độc hại* (*Quét toàn bộ*):

- `1` – tác vụ đang diễn ra.
- `0` – tác vụ đang không chạy.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security.

Cú pháp lệnh

```
kescli --opswat GetScanState
```

GetLastScanTime. Xác định thời gian hoàn thành tác vụ quét

Hiển thị thông tin về ngày tháng và thời gian hoàn thành tác vụ *Quét phần mềm độc hại* (*Quét toàn bộ*) gần đây nhất.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security.

Cú pháp lệnh

```
kescli --opswat GetLastScanTime
```

GetThreats. Nhận dữ liệu về các mối đe dọa được phát hiện

Hiển thị một danh sách các mối đe dọa được phát hiện (*Report on threats*). 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.

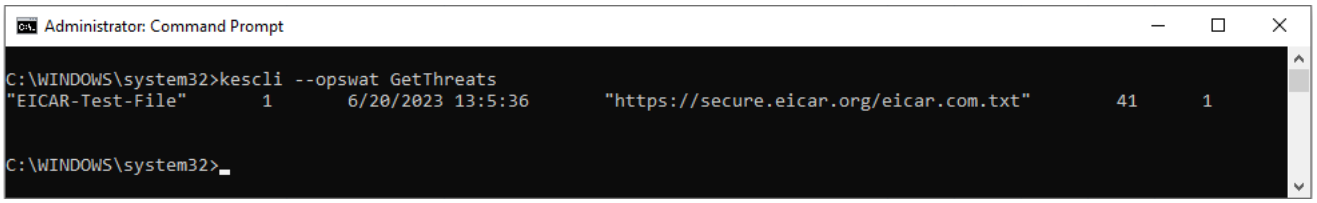
Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security.

Cú pháp lệnh

```
kescli --opswat GetThreats
```

Khi lệnh này được thực thi, Kaspersky Endpoint Security sẽ gửi một phản hồi theo định dạng sau:

<name of detected object> <type of object> <detection date and time> <path to file> <action on threat detection> <threat danger level>



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 hổng bảo mật (Vulnerability).
70	Lừa đảo (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 (Suspic 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 mối đe dọa	
`0`	Chưa biết
`1`	Cao
`2`	quét vừa
`4`	Thấp
`8`	Thông tin (ít hơn *Thấp*)

UpdateDefinitions. Cập nhật cơ sở dữ liệu và các mô-đun phần mềm ứng dụng

Chạy tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*. 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.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security.

> Không thể chạy lệnh này nếu ứng dụng được cài đặt ở chế độ Light Agent.

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 ngày tháng và thời gian cập nhật gần đây nhất của cơ sở dữ liệu

Hiển thị thông tin về ngày tháng và thời gian cập nhật gần đây nhất của cơ sở dữ liệu chống virus đang được sử dụng.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security.

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).

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security.

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

Hiển thị thông tin về trạng thái của thành phần Bảo vệ mối đe dọa tập tin:

- `1` – thành phần dang được bật.
- `0` – thành phần đang bị tắt.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security.

Cú pháp lệnh

```
kescli --opswat GetRealTimeProtectionState
```

GetEncryptionState. Trạng thái mã hóa ổ đĩa

Hiển thị thông tin về trạng thái mã hóa ổ đĩa:

- `1` có nghĩa là đĩa được bảo vệ bằng công nghệ mã hóa đĩa của Kaspersky hoặc BitLocker.
- `0` có nghĩa là đĩa không được mã hóa.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security.

Cú pháp lệnh

```
kescli --opswat GetEncryptionState
```

Version. Xác định phiên bản của ứng dụng

Hiển thị phiên bản của Kaspersky Endpoint Security cho Windows.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security.

Cú pháp lệnh

```
kescli --Version
```

Bạn cũng có thể sử dụng lệnh viết tắt `-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 chạy lệnh `HELP`. Để đọc về cú pháp của một lệnh cụ thể, nhập `HELP <command>`.

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. Sử dụng mẫu sau để thực thi lệnh:

```
avp.com <command> [options]
```

Kết quả là, Kaspersky Endpoint Security sẽ thực thi lệnh đó.

SANDBOX. Quản lý Sandbox

Các lệnh để quản lý thành phần Sandbox:

- Bật hoặc tắt thành phần Sandbox.

  Các thành phần của Sandbox cung cấp khả năng tương tác với giải pháp Kaspersky Sandbox và thành phần KATA Sandbox, là một phần của Kaspersky Anti Targeted Attack Platform.

- Cấu hình thành phần Kaspersky Sandbox:

  - Kết nối máy tính với máy chủ 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 ảo và cấu hình máy chủ Sandbox, hãy tham khảo Trợ giúp của Kaspersky Sandbox và Trợ giúp của Kaspersky Anti Targeted Attack Platform.

  - Cấu hình thời gian chờ kết nối cho máy chủ.

    Thời gian chờ kết nối cho máy chủ Sandbox (đối với Kaspersky Sandbox) hoặc máy chủ Central Node (đối với KATA). 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 máy chủ 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.

  - Cấu hình kết nối được tin tưởng giữa máy tính và máy chủ.

    Để cấu hình kết nối được tin tưởng với máy chủ Sandbox (đối với Kaspersky Sandbox) hoặc máy chủ Central Node (đối với KATA), bạn phải chuẩn bị chứng chỉ TLS. Sau đó, bạn phải thêm chứng chỉ vào máy tính bằng chính sách. Bạn cũng cần thêm chứng chỉ vào máy chủ Sandbox (đối với Kaspersky Sandbox) hoặc máy chủ Central Node (đối với KATA).

- Cấu hình chế độ tích hợp.

  Bạn cần chọn một giải pháp có tích hợp Sandbox: Kaspersky Sandbox hoặc KATA Sandbox. *Kaspersky Sandbox* là giải pháp Detection and Response solution độc lập của Kaspersky. *KATA Sandbox* là một thành phần của giải pháp Kaspersky Anti Targeted Attack Platform. Khi được tích hợp với KATA Sandbox, thành phần này có thể hoạt động ở các chế độ sau:

  - **Manually**. Người dùng gửi tập tin theo cách thủ công để quét từ menu ngữ cảnh (**Gửi đến Sandbox**).
  - **Automatically**. Ứng dụng tự động phát hiện các đối tượng và gửi chúng đến Sandbox để quét.
  - **Combined**.

- Hiển thị thiết lập hiện tại của thành phần.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com stop sandbox [/login=<user name> /password=<password>]
```

```
avp.com start sandbox
```

```
avp.com sandbox /set [--servers=<address:port>] [--pinned-certificate=<path to the TLS certificate>] [--client-certificate=<path to the PFX archive>] [--client-certificate-password=<password>] [--timeout=<Sandbox server connection timeout (ms)>] [--mode=<KSB|KATAManual|KATAAuto|KATAFull>] [/login=<user name> /password=<password>]
```

Hoạt động	
`stop`	Tắt thành phần Sandbox.
`start`	Bật thành phần Sandbox.

`set`	Cấu hình thành phần Sandbox. Bạn có thể cấu hình các thiết lập sau:
	• Thêm máy chủ Sandbox (`--servers`)
	• Thêm chứng chỉ TLS (`--pinned-certificate`)
	• Thêm một bộ chứa mã hóa (`--client-certificate`)
	• Chỉ định mật khẩu cho bộ chứa mã hóa (`--client-certificate-password`);
	• Đặt thời gian chờ kết nối máy chủ (`--timeout`)
	• Chọn chế độ tích hợp (`--mode`):
	  • `KSB` – tích hợp với Kaspersky Sandbox;
	  • `KATAManual` – tích hợp thủ công với KATA Sandbox;
	  • `KATAAuto` – tích hợp tự động với KATA Sandbox;
	  • `KATAFull` – tích hợp kết hợp với KATA Sandbox.

`show`	Hiển thị thiết lập hiện tại của thành phần. Bạn nhận được phản hồi sau:
	`sandbox.timeout=<Sandbox server connection timeout (ms)>`
	`sandbox.servers=<list of Sandbox servers>`
	`sanbox.mode=<integration mode>`
	`sandbox.tls=<trusted connection status>`

Xác thực	
`/login=<user name> /password=<password>`	Thông tin đăng nhập vào tài khoản người dùng với các quyền Bảo vệ bằng mật khẩu cần thiết.

Ví dụ

```
avp.com SANDBOX /SET --servers=127.0.0.1:8080;127.0.0.2:8080 --pinned-certificate=c:\my_certs\my.cer --mode=KSB
/login=login /password=password
```

PREVENTION. Quản lý phòng chống thực thi

Vô hiệu hóa thành phần Phòng chống thực thi hoặc hiển thị các thiết lập hiện tại của thành phần này, bao gồm danh sách các quy tắc phòng chống thực thi.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com prevention disable
```

```
avp.com 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: <MD5 hash of the file>
sha256: <SHA256 hash of the file>
pattern: <path to the object>
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).

ISOLATION. Quản lý cách ly mạng

Vô hiệu 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.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com isolation /OFF /login=<user name> /password=<password>
```

```
avp.com 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

Khôi phục một tập tin từ Khu vực cách ly đến thư mục gốc của nó. *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 được tích hợp với các giải pháp của Kaspersky 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, Trợ giúp của Kaspersky Endpoint Detection and Response Expert, Trợ giúp của Kaspersky Anti Targeted Attack Platform và Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises).

Để thực thi lệnh này, Bảo vệ bằng mật khẩu phải được bật. Người dùng phải có quyền **Khôi phục từ Sao lưu**.

Đối tượng được cách ly dưới quyền tài khoản hệ thống (SYSTEM).

Khôi phục các tập tin từ Khu vực cách ly liên quan đến những cân nhắc đặc biệt sau:

- Nếu thư mục đích đã bị xóa hoặc người dùng không có quyền truy cập vào thư mục đó, ứng dụng sẽ đặt tập tin vào thư mục `%DataRoot%\QB\Restored`. Sau đó bạn phải di chuyển tập tin vào thư mục đích theo cách thủ công.
- Ứng dụng phân biệt chữ viết hoa và chữ viết thường của tên của tập tin đang được khôi phục. Nếu bạn không quan sát trường hợp khi nhập tên tập tin, ứng dụng không khôi phục tập tin đó.

- Nếu thư mục đích đã có một tập tin có cùng tên, ứng dụng sẽ hủy khôi phục tập tin đó.
- Nếu bạn đang sử dụng giải pháp KATA (EDR), ứng dụng sẽ lưu một bản sao của tập tin trong Khu vực cách ly sau khi khôi phục tập tin. Bạn có thể xóa Khu vực cách ly theo cách thủ công. Đối với các giải pháp EDR Optimum và EDR Expert, ứng dụng sẽ xóa tập tin sau khi khôi phục.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Thiết lập nâng cao	
`/REPLACE`	Ghi đè lên một tập tin hiện có.
`<file name>`	Tên của tập tin được khôi phục.

Xác thực	
`/login=<user name> /password= <password>`	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=samplePassword
```

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 *IOC Scan*. 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 *IOC Scan* cho phép tìm các Dấu hiệu về sự xâm nhập trên máy tính và thực hiện các biện pháp ứng phó với mối đe dọa.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Quét IOC sẽ bị hủy sau 128 lần khớp với các dấu hiệu xâm nhập được mô tả trong tập tin IOC. Đây là điều cần thiết để hạn chế số lượng mục trong báo cáo tác vụ Quét IOC nhằm giúp phân tích dễ dàng hơn và bảo vệ báo cáo khỏi tình trạng tràn dữ liệu do dấu hiệu xâm nhập được xây dựng không chính xác có thể tạo ra số lượng lớn trùng khớp.

Cú pháp lệnh

```
avp.com IOCSCAN <full path to the IOC file>|/path=<path to the IOC files folder> [/process=on|off] [/hint=<full path to executable file of a process|full file path>] [/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=<all|system|critical|custom>] [/excludes=<list of exclusions>][/scope=<list of folders to scan>]
```

Tập tin IOC	
`<full path to the IOC file>`	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=<path to the folder with IOC files>`	Đường dẫn đến thư mục có tập tin IOC mà bạn muốn sử dụng để quét. *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. 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=<full path to the executable file of the process|full path to the file>`	Phân tích dữ liệu tập tin khi thực hiện quét IOC (từ ProcessItem và FileItem terms). Bạn có thể chọn một tập tin theo một trong những cách sau đây: • `<full path to the executable file of the process>` – từ ProcessItem; • `<full path to the file>` – từ 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 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 DnsEntryItem, chúng sẽ bị bỏ qua (được phát hiện là không khớp). 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.

`/arpentry=on|off`	Phân tích dữ liệu về các bản ghi trong bảng ARP khi thực hiện quét IOC (từ ArpEntryItem). Nếu giá trị của đối số là `off`, Kaspersky Endpoint Security không quét bảng ARP. Nếu tập tin IOC chứa các từ tài liệu ArpEntryItem, chúng sẽ bị bỏ qua (được phát hiện là không khớp). 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.
`/ports=on|off`	Phân tích dữ liệu về các cổng mở để nghe khi thực hiện quét IOC (từ PortItem). 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). 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.
`/services=on|off`	Phân tích dữ liệu về các dịch vụ được cài đặt trên thiết bị khi thực hiện quét IOC (từ ServiceItem). 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 ServiceItem, 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 dịch vụ nếu tài liệu IOC ServiceItem được mô tả trong tập tin IOC được cung cấp cho tác vụ quét.
`/system=on|off`	Phân tích dữ liệu môi trường khi thực hiện quét IOC (từ SystemInfoItem). 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 SystemInfoItem, 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 môi trường nếu tài liệu IOC SystemInfoItem được mô tả trong tập tin IOC được cung cấp cho tác vụ quét.
`/users=on|off`	Phân tích dữ liệu về người dùng khi thực hiện quét IOC (từ UserItem). 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 UserItem, 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 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.
`/volumes=on|off`	Phân tích dữ liệu về phân vùng khi thực hiện quét IOC (từ VolumeItem). Nếu giá trị của đối số là `off`, Kaspersky Endpoint Security không quét dữ liệu về các phân vùng trên thiết bị. Nếu tập tin IOC chứa các từ tài liệu VolumeItem, 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 phân vùng nếu tài liệu IOC VolumeItem được mô tả trong tập tin IOC được cung cấp cho tác vụ quét.
`/eventlog=on|off`	Phân tích dữ liệu về các bản ghi trong nhật ký sự kiện Windows khi thực hiện quét IOC (từ EventLogItem). Nếu giá trị của đối số là `off`, Kaspersky Endpoint Security không quét các bản ghi trong nhật ký sự kiện Windows. Nếu tập tin IOC chứa các từ tài liệu EventLogItem, chúng sẽ bị bỏ qua (được phát hiện là không khớp). 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. Đối với thuật ngữ IOC EventLogItem\source, hãy sử dụng giá trị **Tên nhà cung cấp** từ lược đồ XML của sự kiện.

`/datetime=<event publication date>`	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. 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. 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. 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`. 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.
`/channel=<list of channels>`	Danh sách tên kênh (nhật ký) mà bạn muốn thực hiện quét IOC. 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. 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 Full Name) 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. Nếu đối số không được chỉ định, Kaspersky Endpoint Security sẽ quét các bản ghi cho các kênh `Application`, `System`, `Security`.
`/files=on|off`	Phân tích dữ liệu tập tin khi thực hiện quét IOC (từ FileItem). Nếu giá trị của đối số là `off`, 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). 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.
`/drives=<all|system|critical|custom>`	Đặt phạm vi quét IOC khi phân tích dữ liệu cho tài liệu IOC FileItem. Bạn có thể đặt các giá trị sau cho phạm vi quét: • `<all>` cho tất cả các phạm vi tập tin khả dụng. • `<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=<list of folders to scan>`). Nếu đối số không được chỉ định, tác vụ quét sẽ được thực hiện cho các khu vực quan trọng.
`/excludes=<list of exclusions>`	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=<list of folders to scan>`	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.
`/retro /<number of days>`	*Quét IOC hồi cứu* là một chế độ của tác vụ *IOC Scan*, trong đó Kaspersky Endpoint Security sẽ quét để tìm dấu hiệu về sự xâm nhập bằng cách sử dụng dữ liệu trong một khoảng thời gian nhất định. Chế độ này được thiết kế để tìm kiếm các dấu hiệu xâm nhập thông qua dữ liệu đo từ xa của máy tính được bảo vệ, chẳng hạn như hoạt động mạng, các tiến trình, tập tin và các dữ liệu đo từ xa khác. Bạn có thể đặt khoảng thời gian từ 1 đến 14 ngày. Theo mặc định, ứng dụng sẽ quét các dấu hiệu xâm nhập trong vòng một ngày.
`/network=on|off`	Phân tích dữ liệu mạng (từ NetworkItem).
`/url=on|off`	Phân tích dữ liệu trong nhật ký trình duyệt (từ UrlHistoryItem). Quét IOC hồi cứu sẽ phân tích nhật ký của các trình duyệt sau: Google Chrome, Mozilla Firefox, Microsoft Edge (phiên bản 79 trở lên).
`/email`	Phân tích các đối tượng thư (từ EmailItem).
`/route`	Phân tích bảng định tuyến và chuyển tiếp (từ RouteEntryItem).

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="">`)
`Name`	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

Thêm 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 ( ).

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com MDRLICENSE <operation> [/login=<user name> /password=<password>]
```

Hoạt động	
`/ADD <file name>`	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.

Xác thực	
`/login=<user name> /password=<password>`	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=samplePassword
```

Ví dụ

```
avp.com MDRLICENSE /ADD file.key
```

```
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

EDRKATA. Tích hợp EDR (KATA)

Các lệnh để quản lý thành phần Endpoint Detection and Response component (KATA):

- Bật hoặc tắt thành phần EDR (KATA).

  Thành phần EDR (KATA) cung cấp khả năng tương tác với giải pháp Kaspersky Anti Targeted Attack Platform của Kaspersky.

- Cấu hình kết nối với máy chủ Kaspersky Anti Targeted Attack Platform.

- Hiển thị thiết lập hiện tại của thành phần.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com START EDRKATA
```

```
avp.com STOP EDRKATA
```

```
avp.com edrkata /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=<Central Node server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
```

```
avp.com edrkata /show
```

Hoạt động	
`stop`	Tắt thành phần EDR (KATA).
`start`	Bật thành phần EDR (KATA).
`set`	Cấu hình thành phần EDR (KATA). Bạn có thể cấu hình các thiết lập sau: • Thêm máy chủ Central Node (`servers=<server address>:<port>`) • Thêm chứng chỉ TLS (`server-certificate=<path to the TLS certificate>`) • Đặt thời gian chờ kết nối máy chủ Central Node (`/timeout=<Central Node server connection timeout (s)>`) • Đặt thời gian đồng bộ hóa với máy chủ Central Node (`/sync-period=<Central Node server synchronization period (min)>`)
`show`	Hiển thị thiết lập hiện tại của thành phần.

EDRExpertOnPrem. Tích hợp EDR Expert (on-premises)

Các lệnh để quản lý tác nhân tích hợp để cấu hình tích hợp Kaspersky Endpoint Detection and Response Expert (on-premises):

- Bật hoặc tắt tác nhân EDR Expert (on-premises) tích hợp.
- Cấu hình thiết lập kết nối cho máy chủ EDR Expert (on-premises).
- Hiển thị thiết lập hiện tại của tác nhân tích hợp.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com START EDRExpertOnPrem
```

```
avp.com STOP EDRExpertOnPrem
```

```
avp.com EDRExpertOnPrem /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate>
[/client-certificate=<path to the PFX archive> /client-certificate-password=<password to the PFX archive>]
[/timeout=<server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
/telemetry-servers=<server address:port> /telemetry-server-certificate=<path to the TLS certificat> [telemetry-
client-certificate=<path to the PFX archive> telemetry-client-certificate-password=<password to the PFX archive>]
[/telemetry-timeout=<server connection timeout (s)>] [/events-send-period=<seconds>] [/events-limit=<0|1>]
[/events-per-hour=<number of events>] [/max-packet-length=<number of packets>] [/telemetry-only-tagged-events=
<0|1>] login=<user name> password=<password>
```

```
avp.com EDRExpertOnPrem /show
```

Hoạt động	Mô tả
`stop`	Tắt tác nhân EDR Expert (on-premises) tích hợp.
`start`	Bật tác nhân EDR Expert (on-premises) tích hợp.

`set`	Cấu hình tác nhân EDR Expert (on-premises) tích hợp.
	Bạn có thể cấu hình các thiết lập kết nối sau cho *máy chủ phản hồi*:
	• `servers=<server address>:<port>`. Địa chỉ máy chủ phản hồi (FQDN, IPv4, IPv6).
	• `server-certificate=<path to the TLS certificate>`. Chứng chỉ TLS để thiết lập kết nối được tin tưởng với máy chủ. Bạn có thể lấy chứng chỉ TLS trên Open Single Management Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises)).
	• `client-certificate=<path to the PFX archive> client-certificate-password=<password to the PFX archive>`. Sử dụng bộ chứa mã hóa để xác thực hai chiều. Một *bộ chứa mã hóa* là tập tin nén PFX có chứng chỉ và khóa riêng ở định dạng PKCS#12. Để kích hoạt xác thực theo cách đó, bạn cần tạo một bộ chứa mã hóa trong cơ quan chứng nhận bên ngoài.
	• `timeout=<server connection timeout (s)>`. Thời gian chờ phản hồi tối đa của máy chủ. Khi hết thời gian chờ, Kaspersky Endpoint Security sẽ cố gắng kết nối với một máy chủ khác.
	• `sync-period=<server synchronization period (min)>`. Tần suất yêu cầu đồng bộ được gửi đến máy chủ. Trong quá trình đồng bộ, Kaspersky Endpoint Security nhận các tác vụ phản hồi mối đe dọa và gửi kết quả tác vụ.
	Bạn có thể cấu hình các thiết lập kết nối sau cho *máy chủ thu thập đo từ xa*:
	• `telemetry-servers=<server address:port>`. Địa chỉ máy chủ thu thập đo từ xa (FQDN, IPv4, IPv6).
	• `telemetry-server-certificate=<path to the TLS certificat>`. Chứng chỉ TLS để thiết lập kết nối được tin tưởng với máy chủ. Bạn có thể lấy chứng chỉ TLS trên Open Single Management Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises)).
	• `telemetry-client-certificate=<path to the PFX archive> telemetry-client-certificate-password=<password to the PFX archive>`. Sử dụng bộ chứa mã hóa để xác thực hai chiều. Một *bộ chứa mã hóa* là tập tin nén PFX có chứng chỉ và khóa riêng ở định dạng PKCS#12. Để kích hoạt xác thực theo cách đó, bạn cần tạo một bộ chứa mã hóa trong cơ quan chứng nhận bên ngoài.
	• `telemetry-timeout=<server connection timeout (s)>`. Thời gian chờ phản hồi tối đa của máy chủ. Khi hết thời gian chờ, Kaspersky Endpoint Security sẽ cố gắng kết nối với một máy chủ khác.
	• `events-send-period=<seconds>`. Độ trễ tối đa khi gửi sự kiện. Ứng dụng sẽ đồng bộ với máy chủ để gửi các sự kiện sau khi hết khoảng thời gian đồng bộ. Thiết lập mặc định là 30 giây.
	• `events-limit=<0|1>`. Giới hạn số lượng yêu cầu. Tính năng này giúp tối ưu hóa mức tải trên máy chủ. Nếu chức năng này được kích hoạt, ứng dụng sẽ hạn chế việc truyền sự kiện. Nếu số lượng sự kiện vượt quá giới hạn được cấu hình thì Kaspersky Endpoint Security sẽ ngừng gửi sự kiện.
	• `events-per-hour=<number of events>`. Số lượng sự kiện tối đa mỗi giờ. Ứng dụng sẽ phân tích luồng dữ liệu đo từ xa và hạn chế gửi sự kiện nếu luồng sự kiện vượt quá giới hạn số sự kiện mỗi giờ đã được cấu hình. Kaspersky Endpoint Security sẽ tiếp tục gửi sự kiện sau một giờ. Thiết lập mặc định là 3000 sự kiện mỗi giờ. Nếu ứng dụng được cài đặt trên máy chủ, luồng dữ liệu đo từ xa sẽ cao hơn. Đối với máy chủ, bạn nên tăng giá trị lên 60.000 sự kiện mỗi giờ.
	• `max-packet-length=<number of packets>`. Độ dài tối đa của gói tin. Ứng dụng sẽ đồng bộ với máy chủ khi bộ đệm được lấp đầy bằng các sự kiện. Thiết lập mặc định là 1024 sự kiện.
	• `telemetry-only-tagged-events=<0|1>`. Chỉ gửi dữ liệu đo từ xa có IOA. *Dấu hiệu tấn công (IOA)* là một quy tắc chứa mô tả về hành vi đáng ngờ trong hệ thống có thể cho biết một cuộc tấn công có chủ đích. Ứng dụng so sánh hành vi đang diễn ra trong hệ thống với các quy tắc này và ghi lại các sự kiện cho thấy có cuộc tấn công có chủ đích. Ứng dụng sử dụng công nghệ *quét luồng* cho phép theo dõi các sự kiện như vậy theo thời gian thực.
	Bạn có thể cấu hình các thiết lập chung sau:
	• `mode=EDRKATA | EDRExpertOnPrem`. Chuyển đổi giữa các giải pháp:
	  • `EDRKATA`. Endpoint Detection and Response Expert (version 7.1 or earlier).
	  • `EDRExpertOnPrem`. Endpoint Detection and Response Expert (version 8.0 or later). Giá trị mặc định.
	• `login=<user name> password=<password>`. Thông tin đăng nhập vào tài khoản người dùng với các quyền Bảo vệ bằng mật khẩu cần thiết.

`show`	Hiển thị thiết lập hiện tại của thành phần.

KUMA. Tích hợp KUMA

Các lệnh để quản lý tác nhân KUMA tích hợp:

- Bật hoặc tắt tích hợp KUMA.

  Tác nhân KUMA tích hợp cho phép tương tác với giải pháp Kaspersky Unified Monitoring and Analysis Platform.

- Cấu hình kết nối với máy chủ Kaspersky Unified Monitoring and Analysis Platform.

- Hiển thị thiết lập hiện tại của thành phần.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com START KUMA
```

```
avp.com STOP KUMA [/login=<user name> /password=<password>]
```

```
avp.com KUMA /SET /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=<KUMA server connection timeout (s)>] [/client-certificate=<path to the crypto-container>] [ /client-certificate-password=<password>] [/maximum-data-transfer-time=<maximum events transmission delay (sec)>]
```

```
avp.com KUMA /SHOW
```

Hoạt động	
`stop`	Tắt tích hợp KUMA.
`start`	Bật tích hợp KUMA.
`set`	Cấu hình tác nhân KUMA tích hợp. Bạn có thể cấu hình các thiết lập sau: • Thêm máy chủ KUMA (`/servers=<protocol>://<server address>:<port>`) Ứng dụng hỗ trợ các giao thức kết nối máy chủ sau: `tcp`, `udp`, `http`, `https`. • Thêm chứng chỉ TLS (`/server-certificate=<path to the TLS certificate>`) • Đặt thời gian chờ kết nối máy chủ (`/timeout=<KUMA server connection timeout (s)>`) • Thêm một bộ chứa mã hóa (`/client-certificate=<path to the crypto-container> /client-certificate-password=<password>`) • Cấu hình độ trễ truyền sự kiện (`/maximum-data-transfer-time=<maximum events transmission delay (sec)`)
`show`	Hiển thị thiết lập hiện tại của thành phần.

Xác thực	
`/login=<user name> /password=<password>`	Thông tin đăng nhập vào tài khoản người dùng với các quyền Bảo vệ bằng mật khẩu cần thiết.

Ví dụ

```
avp.com start kuma
```

```
avp.com KUMA /SET /servers=https://127.0.0.1:8080 /server-certificate=c:\\folder\\certificate.cer /timeout=15 /login=login /password=password
```

```
avp.com KUMA /SET /servers=https://kuma.server.com:8000 /server-certificate=c:\\folder\\certificate.cer /login=login /password=password
```

YARA. Chạy Quét YARA

Chạy tác vụ *Chạy quét YARA*. Ứng dụng sẽ quét các tập tin và đối tượng để tìm dấu hiệu tấn công có chủ đích vào cơ sở hạ tầng CNTT của công ty bằng cách sử dụng cơ sở dữ liệu các quy tắc YARA. *Quy tắc YARA* là những mô tả về các dấu hiệu nhận biết của các cuộc tấn công có chủ đích và các hành vi xâm nhập vào cơ sở hạ tầng CNTT của doanh nghiệp mà Kaspersky Endpoint Security sử dụng để quét các đối tượng.

Để chạy quét YARA, bạn phải chuẩn bị các tập tin YARA mô tả các quy tắc. Khi tạo tập tin YARA, hãy cân nhắc các yêu cầu sau:

- Kaspersky Endpoint Security hỗ trợ các tập tin YARA có phần mở rộng .YARA và .YAR tuân theo tiêu chuẩn mở YARA 4.2.3 để mô tả các dấu hiệu xâm nhập.
- Chỉ có thể chỉ định các tập tin có quy tắc YARA cho tác vụ. Tác vụ *Chạy quét YARA* không hỗ trợ các loại quy tắc khác.
- Nếu bạn đã thêm các tập tin YARA mà Kaspersky Endpoint Security không hỗ trợ hoặc các quy tắc chứa lỗi cú pháp thì tác vụ sẽ bị hủy bỏ kèm thông báo lỗi tương ứng.
- Các định danh của tất cả các tập tin IOC được sử dụng trong một tác vụ đơn phải có tính duy nhất. Nếu có các tập tin YARA có cùng số mã định danh thì điều đó có thể ảnh hưởng đến kết quả thực thi tác vụ.
- Quét YARA sẽ bị hủy sau 128 lần khớp với các chỉ số được mô tả trong quy tắc YARA. Đây là điều cần thiết để hạn chế số lượng mục trong báo cáo quét YARA nhằm giúp phân tích dễ dàng hơn và bảo vệ báo cáo khỏi tình trạng tràn dữ liệu do các quy tắc YARA được xây dựng không chính xác có thể tạo ra số lượng lớn trùng khớp.

Kaspersky khuyến nghị tạo một quy tắc cho mỗi tập tin YARA. Điều này làm cho kết quả quét dễ đọc hơn.

Quá trình quét YARA có thể mất khá nhiều thời gian. Tùy thuộc vào dung lượng ổ đĩa, thiết lập của tác vụ và số lượng đối tượng trên đĩa, quá trình quét YARA có thể kéo dài từ vài phút đến vài giờ. Ứng dụng không hiển thị chỉ báo tiến trình. Không thể dừng hoặc hủy quá trình quét YARA. Bạn nên đợi cho đến khi có kết quả quét YARA.

Cú pháp lệnh

```
avp.com YARA <full path to the YARA file>|/path=<path to the folder with YARA files> [<advanced settings>]
```

Tập tin YARA	
`<full path to the YARA file>`	Đường dẫn đầy đủ đến tập tin YARA mà bạn muốn sử dụng để quét. Bạn có thể chỉ định đường dẫn đến nhiều tập tin YARA được phân tách bằng dấu cách. Đối số bắt buộc nếu không chỉ định giá trị `/path=<path to the folder with YARA files>`. Ví dụ: `C:\Users\Admin\Desktop\YARA\file1.yar C:\Users\Admin\Desktop\YARA\file2.yar`
`/path=<path to the folder with YARA files>`	Đường dẫn đầy đủ đến thư mục có các tập tin YARA mà bạn muốn sử dụng để quét. Đối số bắt buộc nếu không chỉ định giá trị `<full path to the YARA file>`. Ví dụ: `/path=C:\Users\Admin\Desktop\YARA`

Thiết lập nâng cao	
`/fastScan=<on|off>`	Quét YARA nhanh. Đối với mỗi đối tượng, ứng dụng sẽ ghi lại một lần xuất hiện của chỉ báo được phát hiện. Ứng dụng này cũng ẩn các bản sao của các dấu hiệu được phát hiện trong nhật ký. Tính năng Quét YARA nhanh cho phép quét các tập tin lớn nhanh hơn. Nếu thiết lập này không được chỉ định, ứng dụng sẽ thực hiện quét YARA tiêu chuẩn. Ở chế độ này, ứng dụng sẽ ghi lại các bản sao của các dấu hiệu được phát hiện.
`/maxRules=<maximum number of scan rules>`	Hãy giới hạn số lượng các quy tắc được kích hoạt duy nhất khiến ứng dụng dừng quá trình quét YARA khi đạt đến. Nếu giá trị của thiết lập này không được chỉ định hoặc nếu chỉ định giá trị `0` thì ứng dụng sẽ thực hiện quét YARA mà không có giới hạn.
`/timeOut=<stop scan after the specified time in seconds>`	Thời lượng để quét YARA, tính bằng giây. Khi thời gian này hết, ứng dụng sẽ dừng quét YARA. Nếu giá trị của thiết lập này không được chỉ định hoặc nếu chỉ định giá trị `0` thì ứng dụng sẽ thực hiện quét YARA mà không có giới hạn.
`/recursive=<on|off>`	Đối số này khởi động quá trình quét đệ quy các thư mục con bên trong Quét tùy chỉnh `/scanFolders`.
`/scanFolders=<list of folders to be scanned>`	Đối số này khởi động quá trình quét tập tin bằng YARA trong danh sách thư mục được chỉ định. Bạn có thể chỉ định nhiều giá trị được phân tách bằng dấu cách. Kaspersky Endpoint Security hỗ trợ các ký tự `*` và `?` khi nhập tên đại diện đường dẫn thư mục. Nếu không chỉ định thiết lập này, ứng dụng sẽ thực hiện quét YARA trên tất cả các ổ đĩa cục bộ ngoại trừ các lượt chia sẻ mạng, ổ đĩa đám mây và thiết bị lưu trữ di động.
`/scanMemory=<on|off>`	Quét bộ nhớ của tất cả các tiến trình đang chạy.
`/scanProcess=<process name>`	Chỉ quét bộ nhớ cho những tiến trình được chỉ định. Hãy chỉ định đường dẫn đầy đủ, phân cách bằng dấu cách, đến tập tin thực thi của các tiến trình. Bạn cũng có thể sử dụng ký tự `*` và `?` nhập vào tên đại diện.
`/maxSize=<file size in bytes>`	Giới hạn kích thước tập tin cho tác vụ quét YARA. Ứng dụng bỏ qua các tập tin lớn hơn.
`/includes=<list of objects to be scanned>>`	Chỉnh sửa phạm vi quét. Bạn có thể chỉ định nhiều giá trị được phân tách bằng dấu cách. Các giá trị sau khả dụng: • Tên tập tin • Phần mở rộng tập tin Phạm vi quét phải được chỉ định bằng tham số `/scanFolders`. Ví dụ: `/scanFolders C:\*.* /includes=*.exe *.dll` – ứng dụng này quét tất cả các tập tin có phần mở rộng .EXE và .DLL trên ổ đĩa C.
`/excludes=<list of objects to be scanned>`	Loại trừ các tập tin khỏi tác vụ quét YARA. Bạn có thể chỉ định nhiều giá trị được phân tách bằng dấu cách. Các giá trị sau khả dụng: • Đường dẫn đến tập tin • Tên đại diện đường dẫn tập tin Các loại trừ phải được chỉ định bằng tham số `/scanFolders`. Ví dụ: `/scanFolders C:\*.* /excludes readme.txt C:\trusted\*.* *.xml` – ứng dụng bỏ qua tập tin readme.txt, mọi tập tin trong C:\trusted folder và tất cả các tập tin có phần mở rộng .XML trong thư mục gốc trên ổ đĩa C.
`/scanAutoruns=<on|off>`	Quét YARA các đối tượng điểm tự động chạy.
`/excludeAutoruns=<list of autorun point areas to skip>`	Loại trừ các đối tượng điểm tự động chạy khỏi phạm vi quét. Hãy chỉ định đường dẫn đầy đủ, phân cách bằng dấu cách, đến tập tin thực thi của các tiến trình. Bạn cũng có thể sử dụng ký tự `*` và `?` nhập vào tên đại diện.
`/logFolder=<path to the folder for saving the scan results in a TXT file>`	Nếu bạn chỉ định đường dẫn đến một thư mục, ứng dụng sẽ lưu kết quả quét tại đường dẫn đã chỉ định vào một tập tin có tên là yara_<tên máy tính>_<thời gian hoàn thành quét>.txt. Nếu bạn chỉ định đường dẫn đến một tập tin TXT cụ thể, ứng dụng sẽ lưu kết quả quét vào tập tin đó. Ví dụ: `/logFolder=C:\test` hoặc `/logFolder=C:\test\abc.txt`. Kết quả quét được xuất ra dòng lệnh bất kể có chỉ định tùy chọn `/logFolder` hay không.

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.
- `5` có nghĩa là không tìm thấy một hoặc nhiều tập tin có quy tắc YARA được chỉ định trong tham số.

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:

`Started at <time>` `Finished at <time>`	Thời gian bắt đầu và thời gian hoàn thành của quá trình quét.
`Host name: <computer name>`	Tên của máy tính đã phát hiện ra đối tượng.
`Result: <error>`	Mã lỗi cho lỗi xảy ra trong quá trình thực thi tác vụ. Nếu không có lỗi, ứng dụng sẽ xuất ra: `0x00000000`.
`Comment: <comment text>`	Mô tả lỗi cho lỗi xảy ra trong quá trình thực thi tác vụ. Ví dụ: `Operation timeout`.
`Object Name:` hoặc `Process:` (khi quét bộ nhớ tiến trình)	Tên của đối tượng hoặc tiến trình mà quy tắc YARA được kích hoạt.
`Md5: <md5 hash>` `Sha256: <sha256 hash>`	Giá trị băm của đối tượng mà quy tắc YARA được kích hoạt.
`Rule Name`	Tên của quy tắc YARA được kích hoạt.

`Meta:`
`Author: <author>`
`Date: <date>`
`Description: <description>`
	Siêu dữ liệu được chỉ định trong quy tắc YARA.

`Detects:`
`Offset : String name : String data`
`<offset> : <string name> : <string data>`
	Các kết quả phù hợp được tìm thấy trong đối tượng đáp ứng các điều kiện của quy tắc YARA:
	• Địa chỉ offset trong bộ nhớ tiến trình hoặc tập tin nơi phát hiện kết quả (`Offset`).
	• Tên của chuỗi trùng khớp trong quy tắc YARA (`String name`).
	• Chuỗi trùng khớp trong bộ nhớ tiến trình hoặc tập tin (`String data`).

BỘ LỌC ĐO LƯỜNG TỪ XA. Lọc các sự kiện được gửi đến KUMA

Theo mặc định, việc gửi sự kiện đến máy chủ KUMA bị vô hiệu hóa. Để đảm bảo KUMA hoạt động đúng, bạn phải bật tính năng gửi dữ liệu đo từ xa. Bạn có thể chọn một nguồn sự kiện trong số các nhật ký tiêu chuẩn: *Application*, *Security* hoặc *System*. Để nâng cao hiệu năng và tối ưu hóa việc truyền dữ liệu đến máy chủ KUMA, bạn có thể thêm hoặc loại trừ thủ công từng sự kiện khỏi dữ liệu đo từ xa. Ví dụ: bạn có thể loại trừ các sự kiện Sysmon.

Bạn có thể xuất danh sách loại trừ ra tập tin JSON từ dòng lệnh.

Nếu lệnh chỉ chứa tên của tập tin mà bạn muốn xuất thiết lập thì ứng dụng sẽ đặt tập tin như sau:

- Nếu đường dẫn đến avp.com được thêm vào biến hệ thống %PATH% thì ứng dụng sẽ đặt tập tin vào thư mục `C:\Windows\SysWOW64`.
- Nếu bạn chạy lệnh từ thư mục cài đặt ứng dụng, thao tác xuất sẽ không thành công vì tính năng tự bảo vệ của ứng dụng sẽ chặn tạo tập tin mới trong thư mục ứng dụng. Để xuất thiết lập ứng dụng ra tập tin, hãy nhập đường dẫn tập tin.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com TELEMETRYFILTERS /export <file name>
```

```
avp.com TELEMETRYFILTERS /import <file name>
```

Hoạt động	
`export`	Xuất bộ lọc sự kiện để gửi tới KUMA.
`import`	Nhập bộ lọc sự kiện để gửi tới KUMA. Nếu các quy tắc lọc sự kiện đã tồn tại trên máy tính, Kaspersky Endpoint Security sẽ thay thế các quy tắc này khi nhập.

Tập tin để xuất hoặc nhập	
`<file name>`	Tên của tập tin có bộ lọc sự kiện sẽ được gửi tới KUMA. Bạn cũng có thể nhập đường dẫn tập tin. Bạn có thể xuất bộ lọc để gửi tới KUMA thành tập tin JSON.

Các lệnh quản lý Light Agent

Bạn có thể quản lý ứng dụng trong chế độ Light Agent để bảo vệ môi trường ảo trên dòng lệnh. Bạn có thể quản lý ứng dụng ở chế độ Light Agent 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 chạy lệnh `HELP`. Để đọc về cú pháp của một lệnh cụ thể, nhập `HELP <command>`.

Để quản lý ứng dụng ở chế độ Light Agent 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. Sử dụng mẫu sau để thực thi lệnh:

   ```
   avp.com <command> [options]
   ```

   Kết quả là, Kaspersky Endpoint Security sẽ thực thi lệnh đó.

Ứng dụng được cài đặt ở chế độ Light Agent hỗ trợ hầu hết tất cả các lệnh AVP của ứng dụng được cài đặt ở Chế độ tiêu chuẩn. Ở chế độ Light Agent, các tác vụ cập nhật cơ sở dữ liệu diệt virus và tác vụ quản lý khóa giấy phép bị hạn chế.

KSVLAINFO. Xác định chế độ Light Agent

Xác định chế độ Light Agent.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com KSVLAINFO
```

Lệnh này sẽ xuất thông tin sau ra bảng điều khiển:

- Chế độ Light Agent để bảo vệ môi trường ảo: được bật hoặc bị tắt.

  Nếu chế độ Light Agent được bật, ứng dụng sẽ được sử dụng như một phần của giải pháp Kaspersky Security for Virtualization Light Agent.

- Chế độ bảo vệ VDI: bật hoặc tắt.

  Chế độ bảo vệ VDI giúp tối ưu hóa hiệu năng của Kaspersky Endpoint Security trên các máy ảo không lưu các thay đổi. Nếu chế độ bảo vệ VDI được bật, các bản cập nhật yêu cầu khởi động lại máy ảo được bảo vệ sẽ không được cài đặt trên các máy ảo không liên tục. Khi nhận được các bản cập nhật yêu cầu khởi động lại, Light Agent được cài đặt trên máy ảo không liên tục sẽ gửi thông báo đến Kaspersky Security Center để thông báo rằng mẫu máy ảo được bảo vệ cần được cập nhật.

- Loại máy ảo được bảo vệ: liên tục hoặc không liên tục.

- Vai trò của máy ảo được bảo vệ trong cơ sở hạ tầng ảo: máy chủ hay máy trạm.

- Định danh: UUID.

VIISINFO. Trạng thái kết nối Light Agent với Máy chủ tích hợp

Xem thông tin về kết nối Light Agent với Máy chủ tích hợp.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com VIISINFO
```

Lệnh này sẽ xuất thông tin sau ra bảng điều khiển:

- Địa chỉ và cổng của Máy chủ tích hợp mà Light Agent được kết nối.
- Trạng thái kết nối Máy chủ tích hợp.
- Ngày và thời gian kết nối cuối cùng của Light Agent với Máy chủ tích hợp.

SVMINFO. Trạng thái kết nối của Light Agent với Máychủ bảo vệ

Xem thông tin về kết nối Light Agent với Máy chủ bảo vệ.

Để chạy lệnh, hãy vào thư mục chứa tập tin thực thi Kaspersky Endpoint Security. Bạn cũng có thể thêm đường dẫn tập tin thực thi vào biến hệ thống %PATH% và chạy lệnh mà không cần điều hướng đến thư mục ứng dụng.

Cú pháp lệnh

```
avp.com SVMINFO
```

Lệnh này sẽ xuất thông tin sau ra bảng điều khiển:

- Địa chỉ của SVM mà Light Agent được kết nối và vị trí của SVM trong cơ sở hạ tầng ảo liên quan đến Light Agent: cục bộ hay không cục bộ.
- Phương thức khám phá SVM mà Light Agent sử dụng: sử dụng Máy chủ tích hợp hoặc sử dụng danh sách tùy chỉnh các địa chỉ SVM.
- Danh sách địa chỉ SVM nếu danh sách địa chỉ SVM được chọn làm phương thức khám phá SVM.
- Thẻ để kết nối Light Agent với SVM.
- Thuật toán chọn SVM: tiêu chuẩn hoặc mở rộng. Nếu thuật toán chọn SVM mở rộng đang được sử dụng, loại đường dẫn SVM trong cơ sở hạ tầng ảo cũng được hiển thị.
- Trạng thái bảo vệ của kết nối giữa Light Agent và Máy chủ bảo vệ.

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 `Error: Cannot start task 'EntAppControl'`. Kaspersky Endpoint Security cũng có thể hiển thị thông tin bổ sung dưới dạng mã, ví dụ như `error=8947906D` (xem bảng bên dưới).

Các mã lỗi

Mã lỗi	Mô tả
`09479001`	Khóa này đang được sử dụng
`0947901D`	Giấy phép đã hết hạn. Các bản cập nhật cơ sở dữ liệu không khả dụng nữa

Mã lỗi	Mô tả
89479002	Không tìm thấy khóa
89479003	Chữ ký số bị thiếu hoặc bị hỏng
89479004	Dữ liệu đã bị lỗi
89479005	Tập tin khóa bị hỏng
89479006	Giấy phép đã hết hạn
89479007	Tập tin khóa không được chỉ định
89479008	Tập tin khóa không hợp lệ
89479009	Không thể lưu dữ liệu
8947900A	Không thể đọc dữ liệu
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 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 của tập tin không khớp với chữ ký số của Kaspersky
89479015	Không thể sử dụng một khóa dành cho giấy phép dùng thử cho giấy phép thương mại
89479016	Phải có giấy phép dành cho thử nghiệm beta để sử dụng phiên bản beta của ứng dụng
89479017	Tập tin khóa không tương thích với ứng dụng này. Không thể kích hoạt Kaspersky Endpoint Security cho Windows bằng tập tin khóa dành cho ứng dụng khác. Vui lòng kiểm tra ứng dụng được cài đặt
89479018	Khóa giấy phép bị chặn bởi Kaspersky
89479019	Ứng dụng đã sử dụng giấy phép dùng thử. Không thể thêm khóa dành cho giấy phép dùng thử một lần nữa
8947901A	Tập tin khóa bị hỏng
8947901B	Chữ ký số bị thiếu, hỏng hoặc không khớp với chữ ký số của Kaspersky
8947901C	Không thể thêm khóa nếu giấy phép phi thương mại tương ứng đã hết hạn
8947901E	Ngày tạo hoặc sử dụng tập tin khóa không hợp lệ. Vui lòng kiểm tra ngày hệ thống
8947901F	Không thể thêm một khóa cho giấy phép dùng thử: một khóa khác cho giấy phép dùng thử đang hoạt động
89479020	Hỏng hoặc thiếu danh sách các khóa không được phép
89479021	Thiếu hoặc hỏng mô tả về bản cập nhật
89479022	Khóa không phù hợp cho ứng dụng này
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. Lý do có thể: Lỗi kết nối Internet hoặc vấn đề tạm thời trên máy chủ kích hoạt. Thử kích hoạt lại ứng dụng với mã kích hoạt sau (trong 1 đến 2 giờ). Nếu xuất hiện lỗi một lần nữa, liên hệ nhà cung cấp Internet của bạn
89479026	Mã kích hoạt có chứa yêu cầu không chính xác
89479027	Không thể truy xuất trạng thái phản hồi
89479028	Đã xảy ra lỗi khi lưu tập tin tạm thời
89479029	Mã kích hoạt được nhập không chính xác hoặc ngày hệ thống trên máy tính được thiết lập không hợp lệ. Vui lòng kiểm tra ngày hệ thống trên máy tính của bạn
8947902A	Khóa không tương thích với ứng dụng này hoặc giấy phép đã hết hạn

Mã lỗi	Mô tả
8947902B	Không nhận được tập tin khóa. Mã kích hoạt được nhập không chính xác
8947902C	Máy chủ kích hoạt đã trả về lỗi 400
8947902D	Máy chủ kích hoạt đã trả về lỗi 401
8947902E	Máy chủ kích hoạt đã trả về lỗi 403
8947902F	Tài nguyên cần thiết không có trên máy chủ kích hoạt. Máy chủ kích hoạt đã trả về lỗi 404. Vui lòng kiểm tra thiết lập kết nối Internet của bạn
89479030	Máy chủ kích hoạt đã trả về lỗi 405
89479031	Máy chủ kích hoạt đã trả về lỗi 406
89479032	Cần xác thực proxy. Vui lòng kiểm tra thiết lập mạng của bạn
89479033	Hết thời gian yêu cầu
89479034	Máy chủ kích hoạt đã trả về lỗi 409
89479035	Tài nguyên cần thiết không có trên máy chủ kích hoạt. Máy chủ kích hoạt đã trả về lỗi 410. Vui lòng kiểm tra thiết lập kết nối Internet của bạn
89479036	Máy chủ kích hoạt đã trả về lỗi 411
89479037	Máy chủ kích hoạt đã trả về lỗi 412
89479038	Máy chủ kích hoạt đã trả về lỗi 413
89479039	Máy chủ kích hoạt đã trả về lỗi 414
8947903A	Máy chủ kích hoạt đã trả về lỗi 415
8947903C	Lỗi máy chủ nội bộ
8947903D	Chức năng không được hỗ trợ
8947903E	Phản hồi cổng không hợp lệ. Vui lòng kiểm tra thiết lập mạng của bạn
8947903F	Tài nguyên tạm thời không khả dụng
89479040	Hết thời gian chờ phản hồi của cổng. Vui lòng kiểm tra thiết lập mạng của bạn
89479041	Giao thức không được máy chủ hỗ trợ
89479043	Lỗi HTTP không xác định
89479044	ID tài nguyên không hợp lệ
89479046	Liên kết không hợp lệ
89479047	Thư mục đích không hợp lệ
89479048	Lỗi cấp bộ nhớ
89479049	Đã xảy ra lỗi khi chuyển đổi các tham số thành chuỗi ANSI (URL, thư mục, tác nhân)
8947904A	Đã xảy ra lỗi khi tạo ra nhân làm việc
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 bị chặn
8947904F	Lỗi nội bộ trên máy chủ kích hoạt
89479050	Không đủ dữ liệu trong yêu cầu kích hoạt
89479053	Giấy phép tương ứng với khóa được thêm đã hết hạn
89479054	Ngày hệ thống không hợp lệ được thiết lập trên máy tính. Vui lòng kiểm tra giá trị ngày hệ thống
89479055	Giấy phép dùng thử đã hết hạn
89479056	Thời gian kích hoạt ứng dụng đã hết hạn

Mã lỗi	Mô tả
89479057	Đã vượt quá số lần kích hoạt cho ứng dụng của mã được chỉ định
89479058	Thủ tục kích hoạt hoàn tất với lỗi hệ thống
89479059	Không thể sử dụng một khóa dành cho giấy phép dùng thử cho giấy phép thương mại
8947905C	Phải có mã kích hoạt
89479062	Không thể kết nối với 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	Giấy phép đã hết hạn
89479066	Không thể thay thế khóa hiện hoạt bằng khóa đã hết hạn
89479067	Không thể thêm khóa dự trữ nếu giấy phép tương ứng hết hạn trước giấy phép hiện tại
89479068	Thiếu khóa gói đăng ký được cập nhật
8947906A	Mã kích hoạt không hợp lệ
8947906B	Khóa đang hoạt động
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 về lớp truyền dẫn
89479214	Không thể kết nối với máy chủ kích hoạt
89479215	Định dạng địa chỉ web không hợp lệ
89479216	Không thể chuyển đổi địa chỉ máy chủ proxy
89479217	Không thể chuyển đổi địa chỉ máy chủ. Vui lòng kiểm tra thiết lập kết nối Internet
89479218	Thử kết nối máy chủ không thành công
89479219	Quyền truy cập bị từ chối từ xa
8947921A	Hoạt động đã hết thời gian chờ
8947921B	Xảy ra lỗi khi gửi yêu cầu HTTP
8947921C	Lỗi kết nối SSL
8947921D	Hoạt động bị gián đoạn bởi lệnh gọi lại
8947921E	Quá nhiều lượt chuyển hướng
8947921F	Kiểm tra người nhận thất bại
89479220	Không có phản hồi từ máy chủ
89479221	Xảy ra lỗi khi gửi dữ liệu
89479222	Lỗi truy xuất dữ liệu
89479223	Chứng chỉ SSL liên quan đến vấn đề
89479224	Mã hóa SSL liên quan đến vấn đề
89479225	Trung tâm chứng chỉ SSL liên quan đến vấn đề
89479226	Gói tin mạng chứa nội dung không hợp lệ
89479227	Truy cập bị từ chối đối với tài khoản
89479228	Tập tin chứng chỉ SSL không hợp lệ
89479229	Không thể tắt kết nối SSL
8947922A	Lỗi tái diễn
8947922B	Tập tin không hợp lệ có chứng chỉ bị thu hồi

Mã lỗi	Mô tả
8947922C	Lỗi yêu cầu chứng chỉ SSL
89479401	Lỗi máy chủ không xác định
89479402	Lỗi máy chủ nội bộ
89479403	Không có khóa khả dụng cho mã kích hoạt được nhập
89479404	Khóa hiện hoạt bị chặn
89479405	Các thông số cần thiết để kích hoạt bị mất
89479406	Số hoặc mật khẩu của ứng dụng khách không hợp lệ
89479407	Mã kích hoạt không hợp lệ
89479408	Mã kích hoạt không tương thích với ứng dụng này. Không thể kích hoạt Kaspersky Endpoint Security cho Windows bằng một mã kích hoạt dành cho ứng dụng khác. Vui lòng kiểm tra ứng dụng được cài đặt
89479409	Phải có mã kích hoạt
8947940B	Thời gian kích hoạt đã hết hạn
8947940C	Đã vượt quá số lượt kích hoạt bằng mã này
8947940D	Định dạng ID yêu cầu không hợp lệ
8947940E	Mã kích hoạt đã được sử dụng
8947940F	Không thể gia hạn mã kích hoạt
89479410	Mã kích hoạt không hợp lệ đối với khu vực này
89479411	Không thể sử dụng mã kích hoạt này cho ngôn ngữ bản địa hóa của ứng dụng này
89479412	Mã kích hoạt được dành cho phiên bản mới của ứng dụng. Nhận mã kích hoạt khác để kích hoạt phiên bản cài đặt của ứng dụng
89479413	Máy chủ kích hoạt đã trả về lỗi 643
89479414	Máy chủ kích hoạt đã trả về lỗi 644
89479415	Máy chủ kích hoạt đã trả về lỗi 645
89479416	Máy chủ kích hoạt đã trả về lỗi 646
89479417	Phải có phiên bản máy chủ kích hoạt 1.0
89479418	Định dạng mã kích hoạt không chính xác
89479419	Thời gian máy tính không đồng bộ với thời gian máy chủ kích hoạt
8947941A	Sai phiên bản ứng dụng
8947941B	Gói đăng ký đã hết hạn
8947941C	Vượt quá số lần kích hoạt
8947941D	Chữ ký của phiếu không hợp lệ
8947941E	Cần dữ liệu bổ sung
8947941F	Không thể xác minh dữ liệu
89479420	Gói đăng ký không hoạt động
89479421	Máy chủ kích hoạt đang bảo trì
89479501	Sự cố bất ngờ
89479502	Đã truyền đi tham số không hợp lệ. Ví dụ như một danh sách địa chỉ máy chủ kích hoạt trống
89479503	Mã kích hoạt không hợp lệ (giá trị băm không hợp lệ)
89479504	ID người dùng không hợp lệ
89479505	Mật khẩu người dùng không hợp lệ
89479506	Phản hồi không hợp lệ từ máy chủ kích hoạt

Mã lỗi	Mô tả
89479507	Yêu cầu kích hoạt đã bị gián đoạn
89479509	Máy chủ kích hoạt trả về danh sách chuyển tiếp rỗng

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` và `EXPORT`. 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.
- `AntiCryptor`
- `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
- `LogInspector` – Kiểm tra nhật ký
- `Mail_Monitoring` hoặc `EM` – Bảo vệ mối đe dọa thư điện tử
- `Rollback` – Cập nhật khôi phục (không thể áp dụng hồ sơ nếu ứng dụng được cài đặt ở chế độ Light Agent)
- `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 (không thể áp dụng hồ sơ nếu ứng dụng được cài đặt ở chế độ Light Agent)
- `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 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 một 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=<user name>`

     Tên người dùng để quản lý ứng dụng thông qua REST API. Nhập tên người dùng theo định dạng `<DOMAIN>\<UserName>` (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=<port>`

     Cổng được sử dụng để quản lý ứng dụng thông qua REST API. Cổng 6782 được sử dụng theo mặc định. Đảm bảo rằng cổng chưa được sử dụng. Tham số tùy chọn.
   - `RESTAPI_Certificate=<path to certificate>`

     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\RestAp`
     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 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

Phần này mô tả các nguồn thông tin về ứng dụng.

Bạn có thể chọn nguồn thông tin tiện lợi nhất, tùy thuộc vào mức độ quan trọng và cấp bách của sự cố mình gặp phải.

Trang Kaspersky Endpoint Security trên website của 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 Cơ sở tri thức

Cơ sở tri thức là một khu vực trên website Hỗ trợ kỹ thuật.

Trên trang Kaspersky Endpoint Security trong Cơ sở tri thức, bạn có thể đọc các bài viết cung cấp thông tin hữu ích, khuyến nghị và câu trả lời cho các câu hỏi thường gặp về cách mua, cài đặt và sử dụng ứng dụng.

Các bài viết trong Cơ sở tri thức có thể giải đáp các thắc mắc không chỉ liên quan đến Kaspersky Endpoint Security mà còn liên quan đến các ứng dụng khác của Kaspersky. Các bài viết trong Cơ sở tri thức cũng có thể chứa tin tức từ đội ngũ Hỗ trợ kỹ thuật.

Phần thảo luận về các ứng dụng của Kaspersky trong Diễn đàn

Nếu không cần được giải đáp thắc mắc khẩn cấp, bạn có thể thảo luận với các chuyên gia của Kaspersky và những người dùng khác trong Diễn đàn của chúng tôi.

Trong Diễn đàn, bạn có thể xem các chủ đề hiện có, đăng bình luận của mình và tạo các chủ đề 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 nhập 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.14.2\Traces`.

Các tập tin dấu vết được đặt tên như sau: `KES<14.2_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.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.

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<14.2_dateXX.XX_timeXX.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 mối 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 `shellex.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-<type of trace file>.DESKTOP-<date of file update>.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. Trong quá trình truy vết, ứng dụng sẽ tạo một tập hợp các tập tin có dữ liệu về hoạt động của các thành phần ứng dụng khác nhau (ví dụ: SRV.log, WD.log, v.v.).

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 giới hạn dung lượng**. Lưu dấu vết vào một số bộ 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 bộ tập tin tối đa để luân phiên và dung lượng tối đa cho mỗi bộ tập tin.

     Theo mặc định, ứng dụng sẽ lưu năm bộ tập tin dấu vết. Dung lượng của mỗi bộ tập tin là 3072 MB. Như vậy, bạn cần 15 GB dung lượng đĩa trống để lưu các tập tin dấu vết.
   - **Không có giới hạn**. 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:
   - **Bình thường** có nghĩa là tập tin dấu vết sẽ lưu các thông báo về tất cả các lỗi, cảnh báo, cũng như thông tin về hoạt động bình thường của ứng dụng (mặc định).
   - **Chi tiết** có nghĩa là tập tin dấu vết sẽ lưu tất cả thông tin về hoạt động của ứng dụng.

   Bạn có thể thiết lập các cấp độ truy vết bổ sung nếu quản lý thiết lập truy vết của ứng dụng trên dòng lệnh. 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**.

Nếu tính năng truy vết của ứng dụng được bật trên dòng lệnh và cấp độ truy vết được đặt khác với cấp độ **Bình thường** hoặc **Chi tiết** thì danh sách thả xuống **Mức độ** sẽ được đặt thành **Bình thường**.

6. 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 các tập tin dấu vết hoạt động của ứng dụng sẽ được tạo trong thư mục `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. Sau khi các tập tin dấu vết được tạo, hãy gửi các 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 giới hạn dung lượng**. 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.

   - **Không có giới hạn**. 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.14.2\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.14.2\Traces`.

Cách bật ghi tập tin kết xuất trong Bảng điều khiển quản trị (MMC)

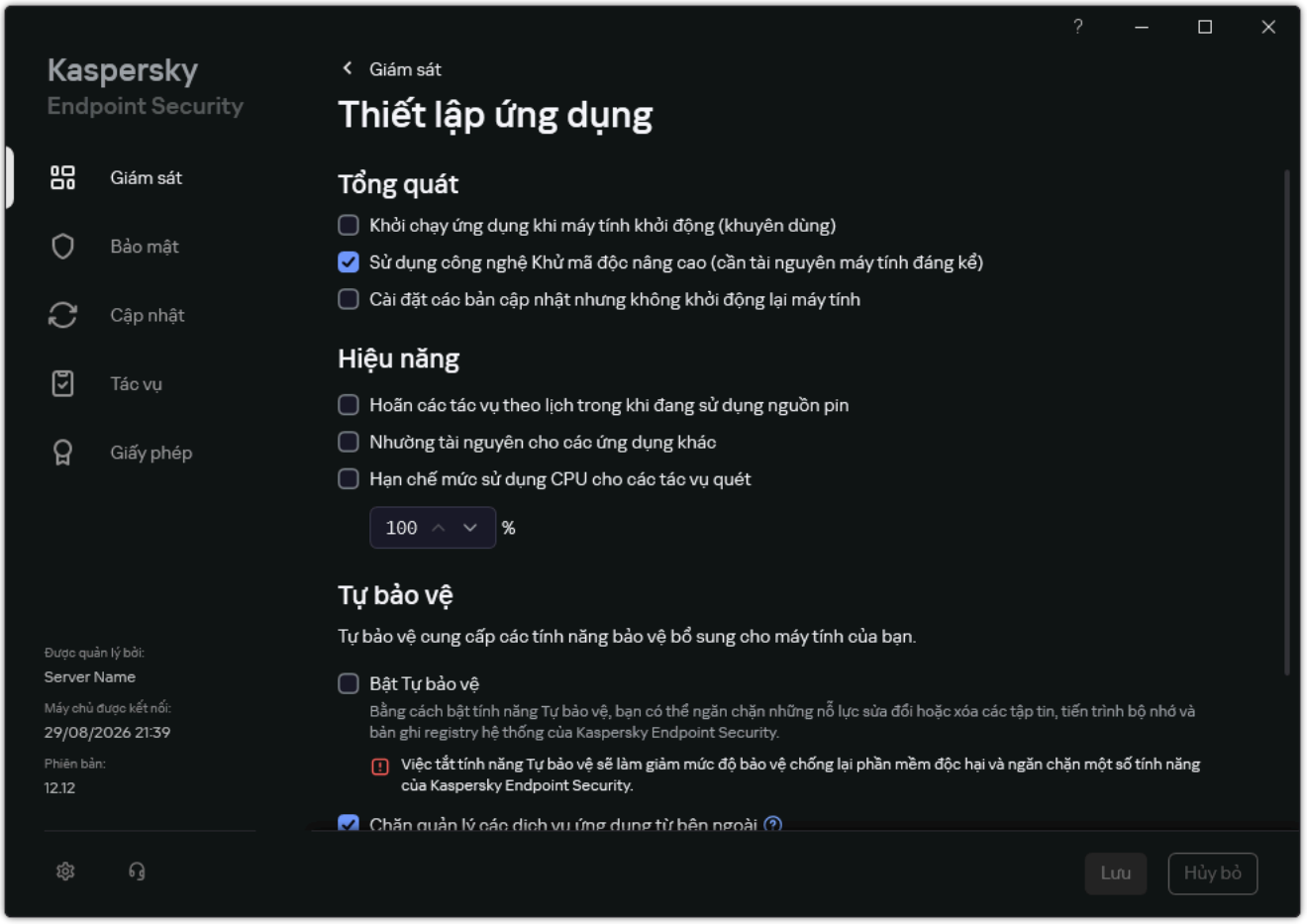
1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát → Thiết lập ứng dụng**.
4. Trong mục **Thông tin gỡ lỗi**, hãy nhấn nút **Thiết lập**.
5. Trong cửa sổ mở ra, hãy sử dụng hộp kiểm **Cho phép ghi tập tin dump** để bật hoặc tắt ghi tập tin kết xuất ứng dụng.
6. Lưu các thay đổi của bạn.

Cách bật ghi tập tin kết xuất trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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** → **Technical Support**.
5. Trong mục **Debug information**, sử dụng hộp kiểm **Dump writing ENABLED** để bật hoặc tắt ghi tập tin kết xuất của ứng dụng.
6. Lưu các thay đổi của bạn.

Cách bật ghi tập tin kết xuất 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**.



Thiết lập Kaspersky Endpoint Security cho Windows

3. Trong mục **Thông tin gỡ lỗi**, sử dụng hộp kiểm **Cho phép ghi tập tin kết xuất** 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.

Cách bật bảo vệ tập tin kết xuất và tập tin dấu vết trong Bảng điều khiển quản trị (MMC)

1. Trong cây Bảng điều khiển quản trị Kaspersky Security Center, hãy chọn **Policies**.
2. Chọn chính sách cần thiết và nhấn đúp để mở các thuộc tính chính sách.
3. Trong cửa sổ chính sách, hãy chọn **Thiết lập tổng quát** → **Thiết lập ứng dụng**.
4. Trong mục **Thông tin gỡ lỗi**, hãy nhấn nút **Thiết lập**.
5. Trong cửa sổ mở ra, hãy sử dụng hộp kiểm **Bật bảo vệ các tập tin kết xuất và dấu vết** để bật hoặc tắt bảo vệ tập tin.
6. Lưu các thay đổi của bạn.

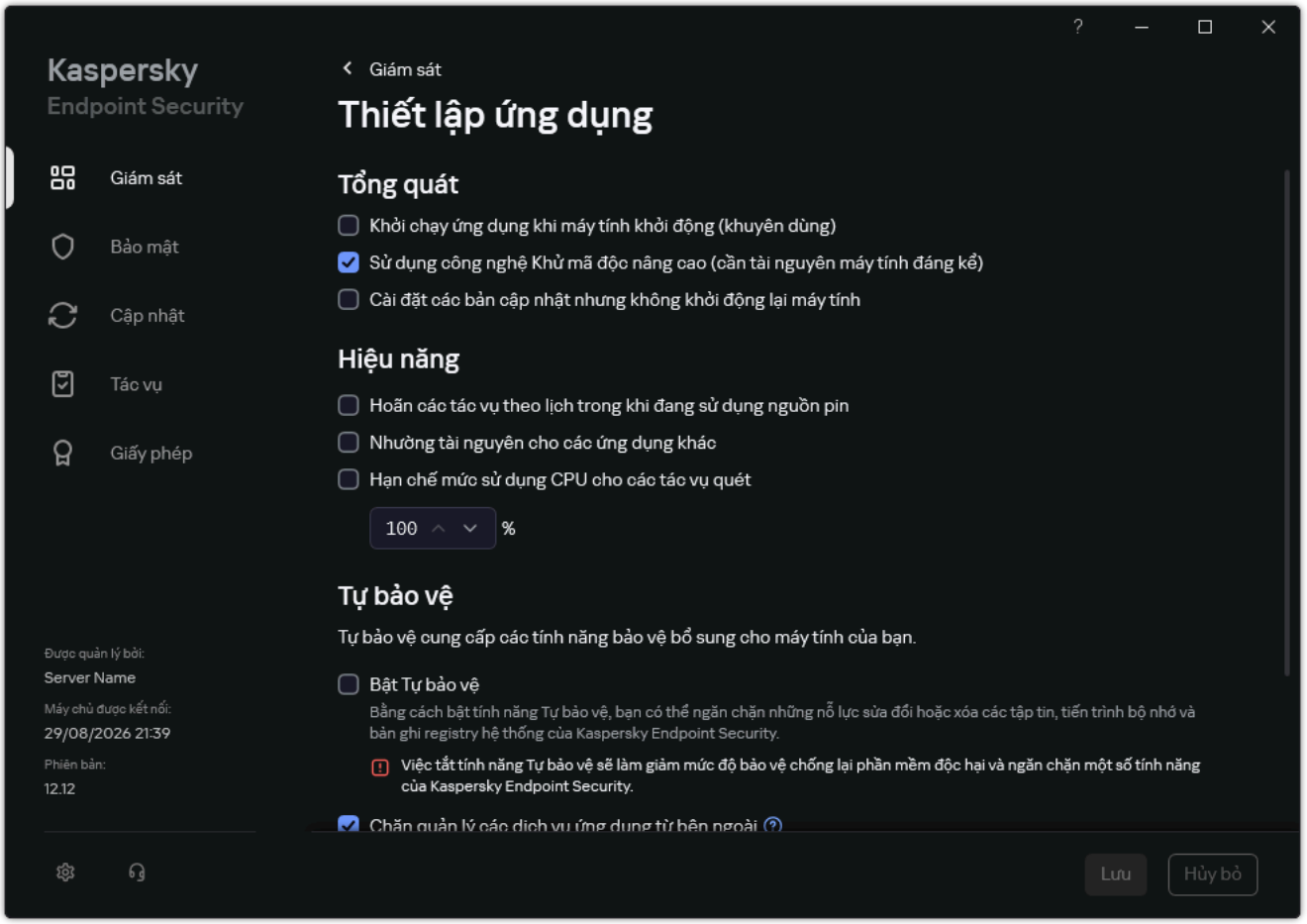
Cách bật bảo vệ tập tin kết xuất và tập tin dấu vết trong Bảng điều khiển web và Bảng điều khiển đám mây

1. Trong cửa sổ chính của Bảng điều khiển web, hãy chọn **Asset management** → **Policies**.
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** → **Technical Support**.
5. Trong mục **Debug information**, hãy sử dụng hộp kiểm **Dump and trace files protection ENABLED** để bật hoặc tắt bảo vệ tập tin.
6. Lưu các thay đổi của bạn.

Cách bật bảo vệ tập tin kết xuất và tập tin dấu vết 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**.



Thiết lập Kaspersky Endpoint Security cho Windows

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.

Thu thập dữ liệu hệ điều hành (Kaspersky Get System Info)

Sau khi cài đặt ứng dụng Kaspersky Endpoint Security, hệ điều hành hoặc một ứng dụng nào đó có thể không hoạt động đúng cách. Xảy ra xung đột giữa ứng dụng và phần mềm hoặc trình điều khiển của các thành phần máy tính.

Để xác định nguyên nhân của sự cố, bộ phận hỗ trợ kỹ thuật của Kaspersky yêu cầu báo cáo từ tiện ích Kaspersky Get System Info (sau đây gọi tắt là GSI). Để biết thông tin chi tiết về việc sử dụng tiện ích này, hãy tham khảo Cơ sở tri thức của Kaspersky.

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 gỡ bỏ từng thành phần ứng dụng riêng lẻ (ví dụ: sử dụng tác vụ *Thay đổi thành phần ứng dụng*) thì bạn có thể cần khởi động lại máy tính.
- Trong các thuộc tính của tác vụ *Thay đổi thành phần ứng dụng*, khi chuyển đổi chế độ cài đặt (**Chế độ riêng** / **Chế độ kết hợp**), việc đồng bộ hóa nhóm thành phần giữa các chế độ không được hỗ trợ. Ứng dụng sẽ đồng bộ hóa nhóm thành phần giữa các chế độ sau khi bạn mở lại thuộc tính tác vụ.
- 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 lệnh gỡ bỏ Kaspersky Endpoint Security, hãy bắt đầu khôi phục ứng dụng sau khi khởi động lại máy tính.

- 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.

- Bạn phải khởi động lại hệ thống khi cài đặt Kaspersky Endpoint Security cho Windows trên máy chủ được cài đặt ứng dụng Kaspersky Security for Windows Server (KSWS) và Windows Defender. Khởi động lại hệ thống là điều cần thiết ngay cả khi bạn đã bật cài đặt ứng dụng mà không cần khởi động lại hệ thống. Windows Defender cho Windows Server nằm trong danh sách phần mềm không tương thích với Kaspersky Endpoint Security cho Windows. Trước khi cài đặt ứng dụng, trình cài đặt sẽ gỡ bỏ Windows Defender cho Windows Server. Việc gỡ bỏ phần mềm không tương thích cần khởi động lại hệ thống.

- Bạn phải tắt Bảo vệ bằng mật khẩu KSWS trước khi cài đặt Kaspersky Endpoint Security cho Windows (KES) trên máy chủ được cài đặt Kaspersky Security for Windows Server (KSWS). Sau khi chuyển từ KSWS sang KES, hãy bật Bảo vệ bằng mật khẩu trong thiết lập ứng dụng.

- 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.

- Chuyển từ Kaspersky Small Office Security (KSOS) sang Kaspersky Endpoint Security (KES) có tính năng Bảo vệ bằng mật khẩu đã được bật kể từ KSOS bản dựng 21.16.*.*. Để chuyển các phiên bản KSOS cũ hơn, bạn phải tắt Bảo vệ bằng mật khẩu hoặc gỡ bỏ KSOS theo cách thủ công. Chuyển từ KSOS sang KES với tính năng Bảo vệ bằng mật khẩu bị tắt sẽ được thực hiện bình thường.

- Bạn không thể cài đặt Kaspersky Endpoint Security trên ổ đĩa di động khởi động. Khi cài đặt, Kaspersky Endpoint Security sẽ hiển thị một thông báo lỗi: *Bạn đã chọn thư mục hoặc ổ đĩa không hợp lệ. Ứng dụng phải cài đặt trên ổ đĩa cứng*. Nếu bạn cố cài đặt ứng dụng trên ổ đĩa di động bằng công cụ của bên thứ ba, hệ điều hành có thể bị sập (BSOD) trong quá trình khởi động. Điều này có nghĩa là Kaspersky Endpoint Security không hỗ trợ Windows To Go và các giải pháp tương tự. Để quét máy tính từ ổ đĩa di động, bạn có thể sử dụng ứng dụng Kaspersky Rescue Disk miễn phí.

- Cài đặt Kaspersky Endpoint Security với các thành phần mạng trên máy chủ đầu cuối có phiên RDP nhiều người dùng liên quan đến một số điều đặc biệt cần phải cân nhắc. Hệ điều hành buộc tất cả phiên làm việc của người dùng phải kết thúc sau khi phiên làm việc của Quản trị viên kết thúc. Để kết nối với máy chủ đầu cuối, bạn phải khởi động lại máy chủ hoặc đăng nhập vào hệ thống cục bộ. Hành vi như vậy được quyết định bởi đặc thù hoạt động của hệ điều hành Windows.

- Nếu các tiện ích web Kaspersky Endpoint Security cho Windows (phiên bản 12.11.0.2004) và Kaspersky Endpoint Security cho Linux (phiên bản 12.4.0.1354) được cài đặt trong Kaspersky Security Center 16.0 hoặc Kaspersky Security Center 16.1, việc cập nhật tiện ích web Kaspersky Endpoint Security cho Windows lên phiên bản 12.11.0.6004 có thể dẫn đến sự cố trong các chính sách của Kaspersky Endpoint Security cho Linux.

  Giải pháp khả dĩ: vào cửa sổ **Settings** → **Web plug-ins** và gỡ bỏ tiện ích bổ sung web Kaspersky Endpoint Security cho Windows, tiện ích bổ sung web Kaspersky Endpoint Security cho Linux và Unified Protection and Management Plug-in từ danh sách. Sau đó, hãy cài đặt tiện ích web Kaspersky Endpoint Security cho Linux trước, rồi cài đặt tiện ích web Kaspersky Endpoint Security cho Windows.

- Trong giao diện web, danh sách các thành phần hiển thị không chính xác trong thuộc tính gói cài đặt của Kaspersky Endpoint Security 12.11 cho Windows. Thành phần riêng biệt Anti-Cryptor không có sẵn trong phiên bản này của ứng dụng. Khả năng bảo vệ thư mục chia sẻ trước mã hóa bên ngoài được tích hợp trong thành phần Phát hiện hành vi. Trong Kaspersky Endpoint Security 12.12 cho Windows, chức năng này là một thành phần riêng biệt. Đồng thời, trong Bảng điều khiển quản trị (MMC), danh sách các thành phần được hiển thị đúng.

- Khi sử dụng phiên bản tiện ích web 7.0 trở lên, danh sách các thành phần được chọn để cài đặt theo mặc định được hiển thị không đúng trong thuộc tính gói cài đặt đối với Kaspersky Endpoint Security 14.1 trở về trước. Nếu danh sách này không được sửa đổi khi tạo gói cài đặt, ứng dụng sẽ được cài đặt bằng bộ thành phần mặc định được chỉ định cho phiên bản ứng dụng tương ứng.

Nâng cấp ứng dụng

- Kể từ phiên bản 11.0.0 của ứng dụng, bạn có thể cài đặt tiện ích MMC cho Kaspersky Endpoint Security cho Windows đè 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, the thiết lập lịch tác vụ cục bộ cho các tác vụ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng*, *Quét khu vực quan trọng*, *Quét tùy chỉnh* và *Kiểm tra tính toàn vẹn của ứng dụng* 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.

- 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 *Critical* 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 nâng cấp Kaspersky Endpoint Security lên phiên bản 11.10.0 trở lên mà không cần khởi động lại, máy tính sẽ được cài đặt hai ứng dụng Kaspersky Endpoint Security. Không gỡ bỏ phiên bản trước của ứng dụng theo cách thủ công. Phiên bản trước đó sẽ tự động được gỡ bỏ khi máy tính được khởi động lại.

- Sau khi nâng cấp Kaspersky Endpoint Security trên máy tính chạy Microsoft Windows 11, menu ngữ cảnh tập tin có thể hiển thị các mục cho cả phiên bản ứng dụng trước đó và phiên bản mới. Khởi động lại máy tính của bạn hai lần để đảm bảo menu ngữ cảnh tập tin hoạt động đúng.

- Nếu tính năng Tự bảo vệ của ứng dụng bị tắt và tất cả các bộ điều hợp mạng đều bị dừng thì các thành phần mạng của ứng dụng sẽ không hoạt động tính từ lúc kết thúc quá trình nâng cấp ứng dụng cho đến khi khởi động lại máy tính. Các thành phần mạng của ứng dụng bao gồm Bảo vệ mối đe dọa web, Bảo vệ mối đe dọa thư điện tử, Bảo vệ mối đe dọa mạng, Tường lửa, Phòng chống xâm nhập máy chủ và Kiểm soát web. Hãy khởi động lại máy tính để ứng dụng hoạt động đúng.

- Thành phần Phòng chống Tấn công BadUSB không hoạt động kể từ lúc kết thúc nâng cấp ứng dụng cho đến khi khởi động lại máy tính. Hãy khởi động lại máy tính để ứng dụng hoạt động đúng.

- Không thể nâng cấp ứng dụng nếu quá trình nâng cấp trước đó chưa hoàn tất. Hãy khởi động lại máy tính để ứng dụng hoạt động đúng.

- 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.

- Nếu bạn quản lý Kaspersky Endpoint Security bằng Kaspersky Security Center Cloud Console thì không được phép cập nhật ứng dụng theo cách cục bộ. Khi cập nhật ứng dụng theo cách cục bộ, không thể chấp nhận Thỏa thuận xử lý dữ liệu cho Kaspersky Security Center Cloud Console.

Hỗ trợ kiến trúc Arm

- Cài đặt Kaspersky Endpoint Security ở chế độ Light Agent trên máy ảo dựa trên kiến trúc Arm hiện không được hỗ trợ.

- Kaspersky Disk Encryption không được hỗ trợ trên các máy tính chạy trên kiến trúc Arm.

- Mã hóa tập tin không được hỗ trợ trên các máy tính chạy trên kiến trúc Arm.

- Tính năng mã hóa ổ đĩa di động không được hỗ trợ trên máy tính chạy trên kiến trúc Arm.

- Trên máy tính chạy Windows 11 cho Arm64, EDR Agent không tương thích với Bitdefender Endpoint Security Tools.

- Chức năng bảo vệ tín hiệu âm thanh và chức năng bảo vệ truy cập webcam không được hỗ trợ trên các máy tính chạy trên kiến trúc Arm.

- Trên máy tính có kiến trúc Arm, phần mở rộng Mail Threat Protection hỗ trợ các phiên bản 32 bit và 64 bit của Outlook 2016, Outlook 2021, Outlook 2024 và Outlook 365 dành cho Arm64.

- Kaspersky Endpoint Security không gửi các đối tượng dành cho kiến trúc Arm đến Kaspersky Sandbox.

- Kiểm soát in không được hỗ trợ trên các máy tính chạy trên kiến trúc Arm.

- Trên máy tính chạy kiến trúc Arm, tác vụ *IOC Scan* chỉ hỗ trợ các tập tin email từ các ứng dụng thư sau: phiên bản 32 bit và 64 bit của Outlook 2016 và Outlook 2021, 2024 và 365 dành cho Arm64.

- Trên máy tính chạy Windows 11 cho Arm64, xác thực dựa trên token có thể không khả dụng vì hệ điều hành không thể phát hiện chứng chỉ hợp lệ trên token. Hiện tượng này là do cách hệ điều hành tương tác với phần mềm token. Ví dụ: hệ điều hành có thể không có các trình điều khiển cần thiết để thiết bị hoạt động. Trong trường hợp này, Kaspersky Endpoint Security cũng không hỗ trợ xác thực dựa trên token (Bảo vệ bằng mật khẩu). Bạn có thể sử dụng các phương thức xác thực khác, chẳng hạn như thông tin đăng nhập của người dùng.

Hỗ trợ các nền tảng máy chủ

- Trên các máy chủ có *loại bỏ dữ liệu trùng lặp* được bật, bạn cần thêm tập tin fsdmhost.exe vào danh sách các ứng dụng được tin tưởng. Điều này giúp tối ưu hóa hiệu năng của ứng dụng và ngăn tình trạng quá tải cho CPU.

- 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 phần mềm độc hại hoạt động đúng.

  - Sau khi tác vụ *Quét phần mềm độc hại* được khởi chạy, các loại trừ quét được thêm vào bằng iChecker sẽ được đặt lại khi máy khủ 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.

- Kaspersky Endpoint Security được cài đặt trên máy chủ được triển khai Microsoft Data Protection Manager (DPM) có thể khiến DPM hoạt động sai. Vấn đề này liên quan đến các hạn chế trong hoạt động của DPM. Để loại bỏ các sự cố, bạn nên thêm ổ đĩa máy chủ cục bộ vào loại trừ cho thành phần Bảo vệ mối đe dọa tập tin và các tác vụ *Quét phần mềm độc hại*.

- Chế độ Server 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.
- Hệ điều hành Windows 10 Enterprise đa phiên và Windows 11 Enterprise đa phiên được hỗ trợ, nhưng có một số 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 khả năng 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 Lab\**\*"
  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.

- Kaspersky Endpoint Security tương thích với hypervisor VMware ESXi kèm theo những hạn chế sau:

  - Kaspersky Endpoint Security có thể không tương thích với trình điều khiển Guest Introspection (vnetWFP.sys, vnetFLT.sys và các trình điều khiển khác). Để giải quyết vấn đề không tương thích, hãy cập nhật trình điều khiển lên phiên bản mới nhất hoặc gỡ bỏ trình điều khiển.

  - Trong một số trường hợp, nỗ lực ngắt kết nối ổ đĩa di động trên máy ảo một cách an toàn có thể không thành công. Cố gắng ngắt kết nối an toàn thiết bị một lần nữa.

- Cài đặt Kaspersky Endpoint Security trên máy ảo có tác nhân Citrix VDA có thể dẫn đến lỗi tương thích. Đây là do Citrix Provisioning Services có khả năng tương thích hạn chế với các giải pháp chống virus. Để biết các phương pháp hay nhất khi sử dụng các giải pháp chống virus với Citrix Provisioning Services, hãy tham khảo trang web hỗ trợ của Citrix.

- Kaspersky Endpoint Security sẽ bỏ qua tác vụ quét ổ đĩa di động nếu ổ đĩa đó được kết nối với máy ảo trên hypervisor Citrix (tác vụ *Quét ổ đĩa di động*). Trên các thiết bị như vậy, hệ điều hành sẽ nhận diện ổ đĩa di động được kết nối như một ổ đĩa mạng. Trong những trường hợp như vậy, bạn có thể sử dụng tác vụ *Quét tùy chỉnh*. Ứng dụng hoạt động giống nhau ở chế độ tiêu chuẩn và chế độ Light Agent.

- Nếu Kaspersky Endpoint Security được cài đặt trên máy ảo trong cơ sở hạ tầng sử dụng công nghệ Citrix App Layering thì các tập tin được ứng dụng phát hiện là bị nhiễm mã độc với trạng thái *Đối tượng sẽ bị xóa khi khởi động lại* sẽ không tự động bị xóa khi máy ảo khởi động lại.

  Để xóa các tập tin đó, bạn phải gắn tập tin VHDX chứa User Layer lên máy tính của quản trị viên Citrix App Layering và chạy Quét phần mềm độc hại trên ổ đĩa đã được gắn.

- Trước khi tạo bản chụp nhanh Golden Image của máy ảo được cài đặt Kaspersky Endpoint Security, bạn nên tắt máy ảo và tạo bản chụp nhanh "cold". Nếu bạn tạo bản chụp nhanh trong khi máy ảo đang chạy (bản chụp nhanh "hot"), thì hoạt động chính xác của ứng dụng không được đảm bảo.

Khả năng tương thích với Kaspersky Security Center

- Trong Bảng điều khiển Kaspersky Security Center Web phiên bản 14.1 trở về trước, tên của các khu vực chức năng cho các thành phần Kiểm tra nhật ký và Giám sát tính toàn vẹn tập tin không được hiển thị chính xác trong phần cài đặt quyền truy cập người dùng của thuộc tính Máy chủ quản trị.

- Sau khi sửa chữa ứng dụng, chức năng bảo vệ kết nối của máy tính với Máy chủ quản trị bị tắt. Sau khi sửa chữa ứng dụng, hãy chạy lại tác vụ *Bảo vệ kết nối Máy chủ quản trị*.

- Trong Bảng điều khiển quản trị Kaspersky Security Center, cửa sổ **Lựa chọn một người dùng hoặc một nhóm người dùng** chỉ hiển thị 50.000 người dùng đầu tiên từ danh sách người dùng của Kaspersky Security Center. Hãy xem Trợ giúp của Kaspersky Security Center để biết thêm chi tiết.

- Khi tìm kiếm các thiết bị được quản lý trong Bảng điều khiển quản trị Kaspersky Security Center, thẻ **Application components** có thể hiển thị đồng thời nhiều biến thể tên của cùng một thành phần ứng dụng, bao gồm cả các tên tương ứng với các phiên bản cũ hơn của Kaspersky Endpoint Security. Tên của một số thành phần cũng có thể bị trùng lặp.

  Để tìm kiếm theo thành phần, bạn chỉ cần chọn một trong các biến thể được hiển thị. Để biết thêm chi tiết về việc phát hiện thiết bị, hãy tham khảo Trợ giúp Kaspersky Security Center.

- Trong Bảng điều khiển web Kaspersky Security Center 15.1 Bản cập nhật 2 có Tiện ích web Kaspersky Endpoint Security cho Windows phiên bản 12.11 trở lên và Tiện ích Unified Protection and Management đã được cài đặt thì các điều kiện kích hoạt hồ sơ cho chính sách sẽ không hoạt động. Kaspersky Security Center không tự động thêm các thiết bị mới đáp ứng điều kiện kích hoạt hồ sơ vào bảng điều khiển.

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.

- 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. Nguyên nhân là trong quá trình cài đặt, ứng dụng sẽ kích hoạt giấy phép dùng thử nhúng trước. Cần phải có kết nối internet.

- 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. Nguyên nhân là trong quá trình cài đặt bản cập nhật, ứng dụng sẽ kích hoạt giấy phép dùng thử nhúng trước. Cần phải có kết nối internet.

- 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 14.2, 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.

Bảo vệ mối đe dọa thư điện tử

- Khi quét email bằng Phần mở rộng Bảo vệ mối đe dọa thư điện tử cho Microsoft Outlook, bạn nên sử dụng Chế độ bộ nhớ đệm máy chủ Exchange (Use Cached Exchange Mode).

- Kaspersky Endpoint Security không hỗ trợ phiên bản 64 bit của ứng dụng thư Microsoft Outlook. Điều này có nghĩa là Kaspersky Endpoint Security sẽ không quét các tập tin Microsoft Outlook (tập tin PST và OST) nếu phiên bản 64 bit của Microsoft Outlook được cài đặt trên máy tính, ngay cả khi bạn thêm thư vào trong phạm vi quét.

- Kaspersky Endpoint Security không hỗ trợ ứng dụng thư Microsoft Outlook New.

- Nếu bạn đã tắt tính năng khử mã độc các mối đe dọa được phát hiện bởi Bảo vệ mối đe dọa thư điện tử và nhận được một email bị nhiễm mã độc trong hộp thư Outlook thì Bảoo vệ mối đe dọa web có thể chặn liên lạc với máy chủ Exchange qua MAPI. Khi đó, thành phần Bảo vệ mối đe dọa web sẽ tạo ra một sự kiện phát hiện mối đe dọa và gửi đến Kaspersky Security Center. Để khôi phục kết nối giữa máy tính và máy chủ Exchange, bạn phải xóa email bị nhiễm mã độc khỏi hộp thư Outlook theo cách thủ công.

  Khi cập nhật phiên bản ứng dụng mà không cần khởi động lại máy tính cấp độ bảo vệ của thành phần Bảo vệ mối đe dọa thư điện tử sẽ tạm thời bị giảm (tối đa một phút). Nếu bạn nhận được email bị nhiễm mã độc trong hộp thư Outlook trong khi cập nhật ứng dụng thì thành phần Bảo vệ mối đe dọa web cũng sẽ chặn kết nối đến máy chủ Exchange qua MAPI. Để khôi phục kết nối, hãy xóa email bị nhiễm mã độc khỏi hộp thư Outlook.

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 khôi phục các tập tin có dung lượng lên đến 100 MB.
- 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, xlsm, 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.

Tường lửa

- Nếu quy tắc gói tin mạng hoặc quy tắc mạng ứng dụng chỉ định tên DNS, Kaspersky Endpoint Security có thể gửi yêu cầu đến máy chủ DNS để xác định địa chỉ IP của các tài nguyên này. Tường lửa sử dụng địa chỉ IP để giám sát hoạt động mạng. Do đó, ứng dụng sẽ phân giải tên DNS thành địa chỉ IP. Bạn chỉ nên sử dụng tên DNS trong các quy tắc cho các máy tính mạng LAN hoặc các dịch vụ nội bộ.
- Để chỉ định quy tắc cho tất cả các địa chỉ IPv6, hãy thêm dải địa chỉ ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff. Tường lửa không hỗ trợ tên đại diện ::/0.
- 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.

- 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 *Giới hạn mức 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.

- Nếu bạn cấm mọi hoạt động mạng bằng Tường lửa, thành phần Bảo vệ mối đe dọa mạng có thể phát hiện ra cuộc tấn công kiểu Quét cổng. Điều này có thể xảy ra vì ứng dụng khởi động Bảo vệ mối đe dọa mạng trước Tường lửa để phát hiện hoạt động đáng ngờ trong mạng.

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.

Kaspersky Security Network

- Kaspersky Endpoint Security không hỗ trợ giao thức HTTPS khi kết nối với Proxy KSN (hộp kiểm **Use HTTPS** được chọn trong thiết lập kết nối Proxy KSN) nếu địa chỉ của máy chủ chứa các chữ cái không phải tiếng La-tinh (ký tự không thuộc bảng ASCII).

- Trong Kaspersky Security Center, khi chuyển từ sử dụng Kaspersky Security Network Toàn cầu sang sử dụng một Kaspersky Security Network Riêng (KPSN) 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.

- Kể từ Kaspersky Endpoint Security 12.9 cho Windows, khi chuyển từ KPSN sang KSN toàn cầu, bạn cần xác nhận lại sự đồng ý của mình với Tuyên bố Kaspersky Security Network. Để thực hiện, bạn cần bật sử dụng Kaspersky Security Network trong thuộc tính chính sách hoặc trong giao diện ứng dụng và xác nhận sự đồng ý của mình với Tuyên bố Kaspersky Security Network. Nếu bạn đã sử dụng KSN toàn cầu, trước tiên bạn phải tắt Sử dụng KSN, sau đó bật lại và xác nhận sự đồng ý của mình với Tuyên bố Kaspersky Security Network. Nếu bạn không đồng ý với Tuyên bố Kaspersky Security Network, ứng dụng sẽ không thể truy cập dữ liệu của Kaspersky Security Network.

- Kaspersky Endpoint Security không gửi các tập tin văn bản (như tập tin TXT, CSV, LOG và DOCX không chứa macro) đến Kaspersky Security Network để quét. Ứng dụng gửi các tập tin có thể gây nguy hiểm đến KSN để quét. Các tập tin này bao gồm các tập tin thực thi hoặc các tập tin có thể chứa mã thực thi (chẳng hạn như macro trong các tập tin DOCX). Các thành phần khác của ứng dụng chịu trách nhiệm quét các tập tin văn bản. Bạn cũng có thể kiểm tra theo cách thủ công danh tiếng của tập tin văn bản từ menu ngữ cảnh của tập tin. Nếu tập tin văn bản có danh tiếng *Không tin tưởng (Kaspersky Security Network)* thì ứng dụng sẽ bỏ qua hành động được xác định cho các mối đe dọa được phát hiện.

Kiểm soát ứng dụng

- Khi làm việc với các Quy tắc kiểm soát ứng dụng, không nên thêm hơn 100.000 điều kiện bao gồm và loại trừ cho các ứng dụng trên các danh mục khác nhau, với điều kiện là Kaspersky Endpoint Security đang chạy trên máy tính đáp ứng yêu cầu phần cứng tối thiểu và hoạt động trên Microsoft Windows 10.

- Chỉ các tập tin nén ở định dạng ZIP mới được hỗ trợ khi làm việc với các Quy tắc kiểm soát ứng dụng trong Bảng điều khiển web của 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 với các quy tắc Kiểm soát ứng dụng trong Bảng điều khiển web của Kaspersky Security Center, kích thước tối đa được hỗ trợ của tập tin được tải lên là 104 MB. 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.

- Nếu đã thêm mới *Quy tắc kiểm soát ứng dụng định sẵn* khi nâng cấp Kaspersky Endpoint Security thì bạn không thể áp dụng các quy tắc này cho các phiên bản trước của ứng dụng.

- Khi các ứng dụng web lũy 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.

- Khi chuyển chính sách KSWS sang hồ sơ chính sách KES, Trình hướng dẫn chuyển đổi hàng loạt Chính sách và tác vụ (Trình hướng dẫn chuyển đổi) sẽ đổi tên các danh mục ứng dụng nếu tên danh mục chứa các ký tự bị cấm: `'` `*` `<` `>` `?` `\` `:` `|`. Trình hướng dẫn chuyển đổi sẽ thay thế các ký tự này bằng ký tự `_`. Ví dụ: danh mục ứng dụng `KSWS::\Everyone:[C61F-3B7C-4D89-96A1]` sẽ được đổi tên thành `KSWS_Everyone_[C61F-3B7C-4D89-96A1]`.

Kiểm soát Thiết bị

- Kaspersky Endpoint Security có thể ghi lại các sự kiện kết nối và ngắt kết nối thiết bị bên ngoài. Các dịch vụ Windows sử dụng tài khoản người dùng hệ thống để kết nối hoặc ngắt kết nối thiết bị. Điều này khiến chúng ta không thể biết được người dùng nào đang kết nối hoặc ngắt kết nối thiết bị. Kaspersky Endpoint Security sẽ chỉ định tài khoản người dùng SYSTEM trong sự kiện.

- 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.

- Khi ứng dụng được nâng cấp mà không khởi động lại máy tính, thành phần Kiểm soát thiết bị sẽ không áp dụng quy tắc truy cập cho các thiết bị được kết nối lại. Tuy nhiên, nếu thiết bị được kết nối trước khi nâng cấp thì thành phần Kiểm soát thiết bị sẽ áp dụng đúng các quy tắc. Khởi động lại máy tính để ứng dụng hoạt động đúng với các thiết bị được kết nối lại.

- Trên máy tính đã cài đặt Kaspersky Endpoint Security phiên bản 12.0, chế độ truy cập máy in **Cho phép và không ghi** cho loại thiết bị **Máy in qua mạng** được gọi là **Tùy thuộc vào bus kết nối**, nếu chính sách Kaspersky Endpoint Security phiên bản 12.1 được áp dụng trên máy tính. Trong các chế độ này, ứng dụng sẽ thực hiện các hành động tương tự. Trong Kaspersky Endpoint Security phiên bản 12.1, chế độ truy cập dành cho máy in qua mạng được đặt tên đúng là **Cho phép và không ghi**.

- Kể từ Kaspersky Endpoint Security 12.0 cho Windows, ứng dụng cho phép cấu hình quy tắc in cho máy in (kiểm soát in). Sau khi cài đặt ứng dụng có kiểm soát in hoặc nâng cấp ứng dụng lên phiên bản có kiểm soát in, bạn phải khởi động lại máy tính. Cho đến khi máy tính được khởi động lại, Kaspersky Endpoint Security sẽ không áp dụng các quy tắc in và chỉ có thể kiểm soát quyền truy cập máy in. Nếu việc khởi động lại máy tính ảnh hưởng bất lợi đến quy trình công việc trong tổ chức thì bạn chỉ cần khởi động lại dịch vụ spoolsv (Print Spooler). Kiểm soát in không được hỗ trợ trên các máy tính chạy trên kiến trúc Arm.

- Kể từ với Kaspersky Endpoint Security 12.0 cho Windows, giao thức WPA3 được ứng dụng hỗ trợ cho các thiết bị kiểu **Wi-Fi**. Nếu một chính sách của Kaspersky Endpoint Security phiên bản 12.2 được áp dụng trên một máy tính thì giao thức WPA2 sẽ được chọn trên các máy tính có Kaspersky Endpoint Security phiên bản 11.11.0 trở về trước; WPA2/WPA3 được chọn cho các phiên bản 12.0 đến 12.1; WPA3 được chọn cho các phiên bản 12.2 trở lên.

- Các thiết bị của Apple được phân loại thành thiết bị di động (MTP) và thiết bị iTunes. Hệ điều hành có thể nhận diện sai kết nối của thiết bị Apple và không xác định thiết bị Apple đó là một thiết bị di động (MTP). Do đó, thiết bị Apple đó sẽ không khả dụng trong trình quản lý tập tin nhưng có thể truy cập được trong ứng dụng iTunes. Kết quả là Kaspersky Endpoint Security sẽ chỉ kiểm soát quyền truy cập thiết bị Apple đó trong ứng dụng iTunes. Để truy cập thiết bị Apple của bạn dưới dạng thiết bị di động (MTP) thì bạn cần truy cập Trình quản lý thiết bị và xóa Trình điều khiển USB thiết bị di động Apple ra khỏi danh sách Trình điều khiển USB. Sau khi máy tính khởi động lại, hệ điều hành sẽ nhận diện thiết bị Apple đó là thiết bị di động (MTP) và thiết bị iTunes. Kaspersky Endpoint Security sẽ kiểm soát quyền truy cập thiết bị cả trong ứng dụng iTunes và trong Trình quản lý tập tin.

- Trong Kaspersky Endpoint Security 12.3 cho Windows, thiết lập truy cập sẽ khác đối với loại thiết bị **Bluetooth**. Nếu bạn chỉ định **Tùy thuộc vào bus kết nối** trong phiên bản trước của ứng dụng thì sau khi nâng cấp ứng dụng lên phiên bản 12.3, giá trị được cấu hình sẽ thay đổi thành **Cho phép và không ghi**. Điều này không làm thay đổi hoạt động của thiết bị.

- Kiểm soát thiết bị chỉ hỗ trợ các thiết bị Bluetooth thông qua ngăn xếp Bluetooth của Microsoft Windows. Kiểm soát thiết bị có thể hoạt động không chính đúng với ngăn xếp Bluetooth của bên thứ ba.

- Nếu thiết bị Bluetooth ẩn hoặc giả mạo Lớp thiết bị (COD) thì Kiểm soát thiết bị có thể hoạt động không đúng.

- Trên máy tính Windows 7 hoặc Windows 8 có trình điều khiển dongle Bluetooth Realtek nhất định, tính năng chỉ cho phép kết nối các thiết bị Bluetooth làm thiết bị đầu vào (lớp HID) có thể không khả dụng. Có nghĩa là, nếu bạn cấm truy cập thiết bị Bluetooth trong thiết lập ứng dụng và thêm thiết bị đầu vào vào danh sách loại trừ thì Kiểm soát thiết bị có thể ngăn truy cập tất cả các thiết bị Bluetooth.

Kiểm soát Web

- Các định dạng OGV và WEBM không được hỗ trợ.

- Giao thức RTMP không được hỗ trợ.

- Kiểmm soát web chỉ hỗ trợ WSL1. Ứng dụng không kiểm soát lưu lượng WSL2.

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 được **Báo cáo về các quy tắc Kiểm soát thích ứng sự cố được kích hoạt** 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.

- Kaspersky Security Center 15.1 không thể tạo báo cáo **Báo cáo về trạng thái các quy tắc Kiểm soát thích ứng sự cố** chi tiết cho một quy tắc cụ thể.

- Các quy tắc Kiểm soát thích ứng sự cố chỉ khả dụng ở ngôn ngữ trùng khớp với ngôn ngữ cài đặt tiện ích web. Nếu bạn thay đổi ngôn ngữ giao diện, Bảng điều khiển web sẽ hiển thị danh sách quy tắc trống. Để truy cập các quy tắc, hãy thay đổi ngôn ngữ giao diện trở lại ngôn ngữ cài đặt tiện ích web.

Mã hóa ổ đĩa (FDE)

- Kaspersky Disk Encryption không được hỗ trợ trên các máy tính chạy trên kiến trúc Arm.

- Tính năng BitLocker Drive Encryption không được hỗ trợ trên các máy tính chạy hệ điều hành Windows Home.

- Với mã hóa ổ đĩa BitLocker, người dùng có thể tự thay đổi mật khẩu xác thực bằng API của Windows. Trong những trường hợp như vậy, BitLocker sẽ bỏ qua các yêu cầu về mật khẩu được thiết lập trong chính sách Kaspersky Endpoint Security. Nói cách khác, người dùng có thể đặt bất kỳ mật khẩu nào.

- 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.

- Nhiều tác nhân tải xuống không thể cùng tồn tại trên một máy tính được mã hóa.

- Khi cố gắng khôi phục ảnh của ổ đĩa GPT khởi động ở trạng thái không được mã hóa, hệ điều hành có thể khiến hệ điều hành không hoạt động được. Để tránh điều này, hãy làm theo các khuyến nghị sau:

  - Giải mã hoàn toàn ổ đĩa trước khi khôi phục ảnh từ bản sao lưu.

  - Sử dụng sao chép lần lượt từng sector khi tạo ảnh.

  - Xóa dữ liệu khỏi các sector đầu tiên của ổ đĩa được mã hóa trước khi khôi phục ảnh và khởi tạo lại đĩa.

- 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 `<domain>/<Windows account name>`, 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 không được hỗ trợ trên các máy tính chạy trên kiến trúc Arm.
- Hệ điều hành Microsoft Windows Embedded không hỗ trợ mã hóa tập tin và thư mục.
- 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.
- Ứng dụng chỉ hỗ trợ mã hóa tập tin trên các thiết bị có hệ thống tập tin NTFS và FAT32. Nếu tập tin mã hóa được chuyển sang một thiết bị có hệ thống tập tin không được hỗ trợ (ví dụ: exFAT), thì tập tin trên thiết bị đó sẽ không được mã hóa và sẽ có thể bị sửa đổi.
- 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 Encrypting File System 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.
- Ví dụ: khi sao chép tập tin đã giải mã sang thiết bị lưu trữ di động, tập tin đó có thể vẫn được mã hóa. Điều này có thể xảy ra vì khi trình quản lý tập tin (ví dụ: explorer.exe) cố gắng truy cập tập tin được mã hóa, nó sẽ lưu giá trị băm của tập tin vào danh sách đặc biệt của tiến trình. Sau khi giải mã tập tin, khi trình quản lý tập tin cố gắng truy cập tập tin, tiến trình sẽ tìm kiếm giá trị hash của tập tin trong danh sách. Nếu tìm thấy giá trị hash, Kaspersky Endpoint Security sẽ mã hóa tập tin đó. Để tránh điều này, bạn cần xóa danh sách của tiến trình. Hệ điều hành sẽ tự động xóa danh sách của tiến trình khi danh sách đầy. Bạn cũng có thể xóa danh sách theo cách thủ công. Để thực hiện, bạn có thể khởi động lại máy tính, khởi động lại tiến trình đang sử dụng để truy cập tập tin (ví dụ: explorer.exe) hoặc có thể sử dụng trình quản lý tập tin khác mà bạn chưa sử dụng để truy cập tập tin được mã hóa.
- 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). Mã hóa các tập tin ngoại tuyến hoặc công nghệ Branch Caching qua SMB cho máy chủ cũng không được hỗ trợ. Chúng tôi khuyến nghị cấm quản lý ngoại tuyến các tài nguyên được chia sẻ ở cấp chính sách nhóm. Có thể chỉnh sửa sác 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.
- 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 (Windows Subsystem for Linux).

- Khi thành phần Mã hóa mức độ tập tin được cài đặt, POSIX (Portable Operating System Interface) 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.

Detection and Response (EDR, NDR, MDR, XDR, Sandbox)

- Bạn không thể quét một đối tượng bị cách ly do kết quả của tác vụ *Move file to Quarantine*.

- Không thể cách ly một Luồng dữ liệu thay thế (Alternate Data Stream, 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.

- Kaspersky Endpoint Security không chạy các tác vụ *IOC Scan* 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 *IOC Scan* trên ổ đĩa mạng. Ví dụ: `\\server\shared_folder`.

- Để đảm bảo tác vụ *IOC Scan* sử dụng các từ EmailItem hoạt động đúng, tiện ích web Kaspersky Endpoint Security phải được cập nhật lên phiên bản mới nhất.

- Trên máy tính chạy kiến trúc Arm, tác vụ *IOC Scan* chỉ hỗ trợ các tập tin email từ các ứng dụng thư sau: phiên bản 32 bit và 64 bit của Outlook 2016 và Outlook 2021, 2024 và 365 dành cho Arm64.

- 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 nhập chính sách từ tập tin KLP, giá trị tham số xác định việc chấp nhận các điều khoản và điều kiện của Thỏa thuận Kaspersky Detection and Response Expert sẽ không được áp dụng. Do đó, sau khi chính sách được nhập, Kaspersky Endpoint Security không thực hiện chức năng của EDR Agent. Để EDR Agent hoạt động, hãy mở chính sách, thay đổi bất kỳ tham số nào và lưu thiết lập chính sách.

- Khi phát hiện một dấu hiệu về sự xâm nhập trong khi chạy tác vụ *IOC Scan*, ứng dụng chỉ cách ly một tập tin cho từ FileItem. Không hỗ trợ cách ly một tập tin cho các từ khác.

- 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.

- 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.

- Cấu hình [KES+KEA+tác nhân tích hợp] không được hỗ trợ. Cấu hình đó sẽ làm gián đoạn tương tác giữa các ứng dụng và giải pháp Detection and Response được triển khai trong tổ chức của bạn. Ngoài ra, sử dụng Kaspersky Endpoint Agent và tác nhân tích hợp sẵn trên cùng một máy tính có thể dẫn đến trùng lặp đo từ xa và tăng tải cho máy tính và mạng. Sau khi chuyển sang cấu hình [KES + tác nhân tích hợp], hãy đảm bảo rằng Kaspersky Endpoint Agent đã được gỡ bỏ khỏi máy tính. Nếu Kaspersky Endpoint Agent tiếp tục hoạt động sau khi chuyển, hãy gỡ bỏ ứng dụng theo cách thủ công (ví dụ: sử dụng tác vụ *Uninstall application remotely*).

  Bộ cài đặt cho phép bạn triển khai Kaspersky Endpoint Agent trên một máy tính được cài đặt Kaspersky Endpoint Security và tác nhân tích hợp. Kaspersky Endpoint Agent và tác nhân tích hợp cũng có thể được cài đặt trên một máy tính do kết quả của tác vụ *Thay đổi thành phần ứng dụng*. Hành vi này phụ thuộc vào các phiên bản của Kaspersky Endpoint Security và Kaspersky Endpoint Agent.

- Khi tạo thông tin chi tiết về cảnh báo, ứng dụng sẽ cung cấp thông tin về mối đe dọa được phát hiện, bao gồm cả hash của các tập tin đã sửa đổi. Kaspersky Endpoint Security tính toán hash của tập tin trong khi tạo thông tin chi tiết về cảnh báo. Lưu ý rằng giá trị hash gốc của tập tin khi sự kiện sửa đổi tập tin được tạo có thể không giống với giá trị hash được tính toán khi chi tiết cảnh báo được tạo.

- Tác nhân tích hợp, EDR (KATA), tiếp tục cách ly mạng của máy tính sau khi máy tính khởi động lại, ngay cả khi thời gian cách ly đã hết. Để ngăn việc cách ly máy tính lặp lại, bạn cần tắt cách ly mạng trong bảng điều khiển Kaspersky Anti Targeted Attack Platform.

- Bạn nên nâng cấp ứng dụng sau khi kết thúc Cách ly mạng. Sau khi nâng cấp Kaspersky Endpoint Security, bạn có thể dừng Cách ly mạng.

- Các tác nhân tích hợp cho EDR (KATA), EDR Optimum và EDR Expert không tương thích với nhau. Do đó, bạn có thể bỏ qua việc kích hoạt tác nhân tích hợp EDR với giấy phép Tiện ích bổ trợ Kaspersky Endpoint Detection and Response độc lập nếu đã kích hoạt Kaspersky Endpoint Security với chức năng EDR khác. Ví dụ: kích hoạt tác nhân tích hợp EDR (KATA) bằng giấy phép độc lập sẽ được bỏ qua nếu bạn đã kích hoạt Kaspersky Endpoint Security bằng giấy phép [KES EDR Optimum].

- Trong Kaspersky Endpoint Security phiên bản 12.1, tác nhân EDR (KATA) tích hợp không hỗ trợ các tập tin siêu dữ liệu sau cho tác vụ *Nhận tập tin siêu dữ liệu NTFS*: $Secure:$SDH:$INDEX_ROOT; $Secure:$SDH:$INDEX_ALLOCATION; $Secure:$SDH:$BITMAP; $Secure:$SII:$INDEX_ROOT; $Secure:$SII:$INDEX_ALLOCATION; $Secure:$SII:$BITMAP; $Extend\$UsnJrnl:$J:$DATA; $Extend\$UsnJrnl:$Max:$DATA. Đã thêm hỗ trợ cho các tập tin siêu dữ liệu này vào phiên bản Kaspersky Endpoint Security 12.2.

- Bạn có thể gặp lỗi khi kết nối máy tính với máy chủ Central Node khi chuyển từ Kaspersky Endpoint Agent sang Kaspersky Endpoint Security cho giải pháp Kaspersky Anti Targeted Attack Platform (EDR). Lý do là trình hướng dẫn chuyển đổi trong Bảng điều khiển web sẽ bỏ qua các thiết lập chính sách sau và không chuyển chúng:

  - Cấm sửa đổi thiết lập **Connection settings** ("khóa").

    Theo mặc định, bạn có thể sửa đổi thiết lập ("khóa" đang mở). Do đó, thiết lập không được áp dụng trên máy tính đó. Bạn phải cấm sửa đổi thiết lập và đóng "khóa".

  - Bộ chứa mã hóa.

    Nếu đang sử dụng xác thực hai chiều để kết nối với máy chủ Central Node thì bạn phải thêm lại bộ chứa mã hóa. Trình hướng dẫn chuyển đổi sẽ chuyển chính xác chứng chỉ TLS của máy chủ.

  Trình hướng dẫn chuyển đổi chính sách và tác vụ trong Bảng điều khiển quản trị (MMC) sẽ chuyển tất cả các thiết lập cho giải pháp Kaspersky Anti Targeted Attack Platform (EDR).

- Trạng thái kích hoạt ứng dụng bị hiển thị sai khi ứng dụng được cài đặt ở chế độ Endpoint Detection and Response Agent để hỗ trợ giải pháp Kaspersky Managed Detection and Response không có kết nối với Kaspersky Security Center. Sau tải về tập tin BLOB, khu vực thông báo trên thanh tác vụ Windows hiển thị sai trạng thái: *Ứng dụng chưa được kích hoạt*. Tuy nhiên, giao diện ứng dụng lại hiển thị đúng trạng thái kích hoạt. Hãy khởi động lại máy tính để ứng dụng hoạt động đúng.

- Kaspersky Endpoint Security cho phép tích hợp với giải pháp Kaspersky Anti Targeted Attack Platform bằng cách sử dụng thành phần EDR (KATA) hoặc Endpoint Sensor (không được hỗ trợ). Lưu ý rằng bạn chỉ có thể sử dụng một trong các thành phần để tương tác với Kaspersky Anti Targeted Attack Platform. Để xem trạng thái của thành phần này, hãy mở thuộc tính máy tính trong Bảng điều khiển quản trị (MMC), trong phần **Applications**, hãy mở thuộc tính của Kaspersky Endpoint Security cho Windows và vào phần **Components**. Những cân nhắc đặc biệt sau đây áp dụng để hiển thị trạng thái thành phần tương tác với Kaspersky Anti Targeted Attack Platform:

  - Đối với tiện ích quản lý 12.0 và các phiên bản cũ hơn, ứng dụng sẽ hiển thị trạng thái hiện tại của **Endpoint Sensor**. Trong Kaspersky Endpoint Security 12.0 trở về trước, thành phần EDR (KATA) không khả dụng. Thành phần EDR (KATA) đã được ra mắt trong phiên bản 12.1.

  - Đối với tiện ích quản lý 12.1 và các phiên bản mới hơn, ứng dụng sẽ hiển thị trạng thái chung của **Endpoint Detection and Response (KATA)**, có thể có nghĩa là trạng thái Endpoint Sensor hoặc trạng thái thành phần EDR (KATA). Điều này tùy thuộc vào phiên bản ứng dụng được cài đặt trên máy tính của người dùng và các thành phần khả dụng mà bạn có thể sử dụng để tương tác với Kaspersky Anti Targeted Attack Platform.

- Kể từ Kaspersky Endpoint Security phiên bản 12.6 trở lên, Bảng điều khiển web Kaspersky Security Center phiên bản 14.2 trở xuống không hiển thị đúng tên của thành phần **Endpoint Detection and Response (KATA)** trong thuộc tính của máy tính. Thay vì thành phần **Endpoint Detection and Response (KATA)**, ứng dụng sẽ hiển thị tên của thành phần **Endpoint Detection and Response Expert (KATA EDR)**. Để xem danh sách các thành phần, hãy mở thuộc tính máy tính trong Bảng điều khiển web, trong phần **Applications**, mở thuộc tính của Kaspersky Endpoint Security cho Windows và vào phần **Components**. Kể từ Bảng điều khiển web Kaspersky Security Center phiên bản 15.1 trở lên, ứng dụng sẽ hiển thị đúng tên thành phần.

- Khi cập nhật tiện ích quản lý Kaspersky Endpoint Detection and Response lên phiên bản 15.3 được cài đặt trong Bảng điều khiển web phiên bản 14.0–14.2, chi tiết cảnh báo được hiển thị không chính xác. Để thông tin cảnh báo hoạt động chính xác, hãy khởi động lại Máy chủ quản trị Kaspersky Security Center.

- Tiện ích quản lý Kaspersky Endpoint Detection and Response phiên bản 15.4 trở lên không hỗ trợ Kaspersky Security Center phiên bản 14.0. Sau khi cập nhật tiện ích quản lý, thông tin chi tiết cảnh báo được hiển thị không chính xác.

- Các giải pháp Kaspersky Extended Detection and Response (XDR) phiên bản 1.4 không hỗ trợ tiện ích web Kaspersky Endpoint Security cho Windows phiên bản 12.12 trở lên. Bạn có thể giữ nguyên phiên bản tiện ích web hiện tại hoặc cập nhật giải pháp XDR lên phiên bản 2.0 trở lên.

- Kaspersky Endpoint Security không gửi các đối tượng dành cho kiến trúc Arm đến Kaspersky Sandbox.

- Kaspersky Endpoint Security hỗ trợ tối đa tổng cộng 10.000 quy tắc lọc sự kiện bao gồm và loại trừ của EDR Expert (on-premises).

- Các quy tắc lọc sự kiện EDR Expert (on-premises) sẽ không được chuyển từ chính sách xuống các thiết bị được quản lý đang chạy Kaspersky Endpoint Security phiên bản 14.0 trở xuống nếu vượt quá giới hạn hỗ trợ về số lượng quy tắc lọc được lưu trữ. Ứng dụng sẽ hiển thị cảnh báo tương ứng.

- Kaspersky Endpoint Security cho Windows phiên bản 12.11–14.1 không hỗ trợ các tính năng sau: Sự kiện đo từ xa của EDR Expert (on-premises):

  - LDAP Attribute Change
  - GPO Change
  - SCCM Local Config Mismatch
  - SCCM Config Change
  - SCCM Deployment Task
  - Smb Connection Open

  Kể từ phiên bản 14.2, Kaspersky Endpoint Security hỗ trợ tất cả các sự kiện đo từ xa của EDR Expert (on-premises) ngoại trừ LDAP Attribute Change.

Các hạn chế khác

- Hệ điều hành Windows, bắt đầu từ phiên bản 11 24H2, hỗ trợ công nghệ UDP Receive Segment Coalescing Offload (URO). Công nghệ này được bật theo mặc định nếu máy tính có card mạng và trình điều khiển tương thích. Tắt URO trên máy tính của người dùng có thể làm giảm đáng kể hiệu năng của ứng dụng.

- Kaspersky Endpoint Security hỗ trợ hệ thống con WSL (Windows Subsystem for Linux) với những hạn chế:

  - WSL 1. Ứng dụng giám sát lưu lượng mạng và phát hiện các mối đe dọa thông qua HTTP / HTTPS. Do Kaspersky Endpoint Security sử dụng chứng chỉ riêng để quét các kết nối HTTPS bảo mật nên hoạt động của một số ứng dụng của bên thứ ba có thể bị gián đoạn.
  - WSL 2. Ứng dụng không hỗ trợ WSL 2.

- 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 một 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 vè 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.

- Các lỗi kết nối TLS có thể xảy ra khi phần mềm của bên thứ ba hoạt động với thư viện Libcurl. Điều này có thể liên quan đến chứng chỉ Kaspersky mà Kaspersky Endpoint Security sử dụng để quét các kết nối được mã hóa. Để tiếp tục làm việc, bạn có thể tắt xác thực chứng chỉ cho phần mềm bên thứ ba (không khuyến nghị) hoặc thêm phần thân chứng chỉ Kaspersky vào bộ lưu trữ chứng chỉ cURL. Để biết thông tin chi tiết, hãy tham khảo Cơ sở tri thức của Kaspersky.

- 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.

- 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.

- 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 của Windows.

- 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.

- Tắt tùy chọn **Vô hiệu hóa quản lý bên ngoài các dịch vụ hệ thống** 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\`.

- Nếu bạn đang sử dụng các chính sách (Software Restriction Policies, SRP) thì máy tính có thể không nạp thành công (màn hình đen). Để ngăn các sự cố, bạn cần cho phép sử dụng các thư viện ứng dụng trong thuộc tính SRP. Trong thuộc tính SRP, hãy thêm quy tắc có mức độ bảo mật **Không hạn chế** cho tập tin khkum.dll (mục menu **Quy tắc hash mới**). Tập tin này nằm trong thư mục `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.14.2\klhk\klhk_x64\`. Nếu bạn đã chọn phương thức này, bạn cần xóa thêm hộp kiểm **Tải xuống các bản cập nhật của mô-đun ứng dụng** trong thiết lập tác vụ *Cập nhật* cho Kaspersky Endpoint Security. Để biết chi tiết về việc sử dụng SRP, hãy tham khảo tài liệu của Microsoft.

  Bạn cũng có thể tắt SRP và sử dụng thành phần Kiểm soát ứng dụng của Kaspersky Endpoint Security để kiểm soát việc sử dụng ứng dụng.

- Nếu máy tính thuộc một miền trong Windows Group Policy Object (Group Policy Object, GPO) với tham số DriverLoadPolicy được đặt thành 8 (Good only), 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 (Good and unknown). Thiết lập ELAM nằm trong chính sách bên dưới: **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.

- 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).

- Nếu Kaspersky Endpoint Security được cài đặt trên máy chủ của SQL Server DBMS, ứng dụng sẽ gửi yêu cầu đến phiên bản của máy chủ. Đây là điều cần thiết để quét các tác vụ của Tác nhân SQL Server và ngăn các tác vụ độc hại chạy. Kaspersky Endpoint Security sử dụng tài khoản SQL Server người dùng để quét các tác vụ. Ứng dụng gửi yêu cầu đến máy chủ khi quét bộ nhớ hệ thống và sau khi cập nhật cơ sở dữ liệu chống virus.

- 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.

  - Ứng dụng Kaspersky Endpoint Security không tương thích với thành phần Bảo vệ ổ đĩa và mã hóa dữ liệu của phần mềm Secret Net Studio.

    Không thể cài đặt ứng dụng trên máy tính có triển khai Secret Net Studio với thành phần Bảo vệ ổ đĩa và mã hóa dữ liệu. Để tạo khả năng tương tác, bạn phải gỡ bỏ thành phần Bảo vệ ổ đĩa và mã hóa dữ liệu 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.

- Khi nhập quy tắc Giám sát tính toàn vẹn hệ thống, ứng dụng sẽ kiểm tra ID và tên của quy tắc. Nếu các ID quy tắc giống nhau, Kaspersky Endpoint Security sẽ thay thế các quy tắc hiện có bằng quy tắc mới. Khi xuất quy tắc, ứng dụng sẽ tự động gán ID. Ví dụ: quy tắc có ID giống hệt nhau có thể tồn tại nếu bạn chỉnh sửa thủ công các tập tin XML quy tắc đã xuất. Nếu ID quy tắc là duy nhất nhưng tên quy tắc giống nhau thì Kaspersky Endpoint Security sẽ thêm `(1)`, v.v. vào tên của quy tắc.

- Kể từ phiên bản 12.11 của Kaspersky Endpoint Security cho Windows, bạn sẽ không thể xem thiết lập của chính sách chính cha đang được mở trong nhóm con trong Bảng điều khiển web. Bảng điều khiển web cũng hiển thị cảnh báo: *This policy is inherited. You can edit the policy settings only in the administration group in which it was created*.

- Thông báo bật lên có độ dài hơn 256 ký tự sẽ không được hiển thị trong Bảng điều khiển quản trị (MMC).

- Tên các thành phần trong chính sách và trong gói cài đặt có thể khác nhau. Ví dụ: Endpoint Detection and Response Expert (on-premises) có thể được đặt tên là Endpoint Detection and Response (KATA), Endpoint Detection and Response Expert (on-premises), Kaspersky Anti Targeted Attack Platform Integration. Tên các thành phần cũng có thể khác nhau tùy thuộc vào phiên bản của 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.

Cloud Discovery

Cloud Discovery quản lý quyền truy cập của người dùng vào các dịch vụ đám mây. Các ví dụ về dịch vụ đám mây bao gồm Microsoft Teams, Salesforce và Microsoft Office 365. Các dịch vụ đám mây được nhóm thành các danh mục, ví dụ: *Chia sẻ tập tin*, *Trình nhắn tin*, *Email*.

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 các thư mục con bên trong `Folder`, ngoại trừ chính `Folder`. Một đại diện phải có ít nhất một cấp 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. Một tập hợp dữ liệu về một đối tượng độc hại hoặc hoạt động độc hại.

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.

Light Agent

Thành phần Kaspersky Endpoint Security for Virtualization Light Agent. Nó được cài đặt trên mỗi máy ảo cần được bảo vệ.

Máy chủ tích hợp

Thành phần Kaspersky Endpoint Security for Virtualization Light Agent. Tương tác giữa các thành phần của Kaspersky Endpoint Security và cơ sở hạ tầng ảo.

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.

SVM

Máy ảo bảo mật – một máy ảo đặc biệt được cài đặt dịch vụ scanserver (Máy chủ bảo vệ, một thành phần của Kaspersky Endpoint Security for Virtualization Light Agent).

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.

Xác thực Kerberos

Cơ chế xác thực lẫn nhau giữa máy khách và máy chủ trước khi thiết lập kết nối giữa chúng, cho phép giao tiếp qua các mạng không bảo mật. Cơ chế này dựa trên một loại vé mà người dùng nhận được từ một trung tâm xác thực được tin tưởng.

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 mối đe dọa tập tin

Thành phần Bảo vệ mối đe dọa tập tin cho phép bạn ngăn chặn sự lây nhiễm vào hệ thống tập tin máy tính. Theo mặc định, thành phần Bảo vệ mối đe dọa tập tin sẽ nằm vĩnh viễn trong RAM của máy tính và quét tất cả các tập tin đã mở, đã lưu và đã chạy theo thời gian thực. Thành phần này sẽ quét các tập tin trên tất cả các ổ đĩa máy tính, bao gồm cả 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 ở trong lưu trữ đám mây OneDrive, Kaspersky Endpoint Security sẽ tải về và quét nội dung tập tin.

Cấu hình thành phần Bảo vệ mối đe dọa tập tin

Tham số	Mô tả
Mức độ bảo mật *(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)*	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 được gọi là *mức độ bảo mật*: • **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. • **Khuyên dùng**. Mức độ bảo mật tập tin này được khuyến nghị bởi các chuyên gia của Kaspersky Lab. Thành phần Bảo vệ mối 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 mối 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 mối 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 mối đe dọa tập tin sẽ không quét các tập tin hỗn hợp.
Loại tập tin *(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)*	**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, ứng dụng 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, ứng dụng 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.

Tham số	Mô tả
Phạm vi quét	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. 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 chỉ có thể loại trừ một đối tượng (như các ổ đĩa di động) ra khỏi phạm vi quét.
Công nghệ máy học và phân tích dấu hiệu *(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)*	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. Dựa trên khuyến nghị của các chuyên gia Kaspersky, máy học và phân tích dấu hiệu luôn được bật.
Phân tích hành vi *(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)*	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.
Hành động khi phát hiện mối đe dọa	**Khử mã độc, xóa nếu không thể khử mã độc**. Nếu chọn tùy chọn này, ứng dụng sẽ tự động cố gắng khử mã độc tập tin bị nhiễm được phát hiện. Nếu không thể khử mã độc, ứng dụng sẽ xóa tập tin đó. **Khử mã độc, chặn nếu không thể khử mã độc**. Nếu chọn tùy chọn này, ứng dụng sẽ tự động cố gắng khử mã độc tập tin bị nhiễm được phát hiện. Nếu việc khử mã độc không thành công, ứng dụng sẽ chặn tập tin này. **Chặn**. Nếu tùy chọn này được chọn, ứng dụng sẽ tự động chặn tập tin bị nhiễm mà không cố gắng khử mã độc hoặc xóa tập tin. Trước khi cố gắng khử mã độc hoặc xóa một tập tin bị nhiễm, ứng dụng 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.
Chỉ quét các tập tin mới và bị chỉnh sửa	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. Ứng dụng 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	Quét các gói phân phối của ứng dụng 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. Ứng dụng sẽ quét các tập tin định dạng văn phòng nhỏ hơn 1 MB, bất kể hộp kiểm này có được chọn hay không.
Quét các tập tin có định dạng email	Quét các tập tin định dạng email. Ứng dụng sẽ quét các tập tin MSG và EML. Các tập tin định dạng email cũng bao gồm các đối tượng OLE và tập tin MHT. Kaspersky Endpoint Security sẽ quét các tập tin định dạng email nhỏ hơn 1 MB, bất kể hộp kiểm này có được chọn hay không.
Không giải nén các tập tin hỗn hợp lớn	Nếu hộp kiểm này được chọn, ứng dụng sẽ không quét các tập tin hỗn hợp nếu dung lượng của chúng vượt quá giá trị ấn định. Nếu bỏ chọn hộp kiểm này, ứng dụng sẽ quét các tập tin tổ hợp thuộc mọi kích thước. Ứng dụng sẽ quét các tập tin lớn được trích xuất từ tập tin nén, bất kể hộp kiểm này có được chọn hay không.

Tham số	Mô tả
Giải nén các tập tin hỗn hợp trong nền	Nếu hộp kiểm được chọn, ứng dụng sẽ cấp quyền truy cập các tập tin hỗn hợp lớn hơn giá trị được chỉ định trước khi các tập tin này được quét. Trong trường hợp này, Kaspersky Endpoint Security sẽ giải nén và quét các tập tin tổng hợp trong nền. Ứng dụng sẽ cung cấp quyền truy cập vào các tập tin phức hợp nhỏ hơn giá trị này chỉ sau khi giải nén và quét các tập tin này. Nếu hộp kiểm này không được chọn, ứng dụng sẽ chỉ cấp quyền truy cập vào các tập tin hỗn hợp sau khi giải nén và quét các tập tin thuộc mọi kích thước.
Chế độ quét *(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)*	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. **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.
Sử dụng công nghệ iSwift *(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)*	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 tác vụ 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 iSwift được cải tiến từ công nghệ iChecker cho hệ thống tập tin NTFS.
Sử dụng công nghệ iChecker *(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)*	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 tác vụ 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).
Tạm dừng Bảo vệ mối đe dọa tập tin *(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)*	Điều này sẽ tạm thời và tự động tạm dừng hoạt động của Bảo vệ mối đe dọa tập tin tại thời điểm được chỉ định hoặc khi làm việc với các ứng dụng được chỉ định.
Thao tác quét tập tin được thực thi trong container Windows	Nếu phát hiện mối đe dọa bên trong container, ứng dụng sẽ áp dụng hành động được chọn cho thành phần Bảo vệ mối đe dọa tập tin. **Dừng container nếu khử mã độc không thành công**. Ứng dụng có thể không có đủ quyền đọc và ghi cho đối tượng được phát hiện. Trong trường hợp đó, khử mã độc hoặc xóa đối tượng được phát hiện là việc không thể. Nếu cho hộp kiểm này, ứng dụng sẽ chặn đối tượng được phát hiện và dừng container. Nếu bỏ chọn hộp kiểm này, ứng dụng chỉ chặn đối tượng được phát hiện. **Không quét các thao tác tập tin được thực thi trong container Windows**. Nếu chọn hộp kiểm, ứng dụng sẽ chỉ quét container khi container đó được khởi động. Nếu bỏ chọn hộp kiểm, ứng dụng sẽ quét container liên tục theo thời gian thực.

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 kết nối đến 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.

Để sử dụng Bảo vệ mối đe dọa web, bạn phải hoàn thành cấu hình ban đầu của ứng dụng:

- Để giám sát lưu lượng HTTPS, hãy bật kết nối được mã hóa quét (được bật theo mặc định).
- Chọn các cổng mà Kaspersky Endpoint Security phải giám sát (theo mặc định, ứng dụng sẽ giám sát tất cả các cổng).
- Chọn các ứng dụng có lưu lượng mà bạn muốn Kaspersky Endpoint Security giám sát. Hầu hết các trình duyệt đã có trong danh sách ứng dụng đều được Kaspersky khuyên dùng. Hãy thêm theo cách thủ công nếu trình duyệt của bạn không có trong danh sách.
- Bạn nên chèn một tập lệnh tương tác trang web vào lưu lượng truy cập web (chèn tập lệnh bị tắt theo mặc định). Tập lệnh này cho phép đăng ký các sự kiện Bảo vệ mối đe dọa web cho nhật ký sự kiện ứng dụng, nhật ký sự kiện HĐH và báo cáo.

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

Cấu hình thành phần Bảo vệ mối đe dọa web

Tham số	Mô tả
Mức độ bảo mật *(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)*	Đối với thành phần Bảo vệ mối đe dọa web, ứng dụng có thể áp dụng các nhóm thiết lập khác nhau. Các nhóm thiết lập được lưu trữ trong ứng dụng được gọi là *mức độ bảo mật*: • **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 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 ứng dụng 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 nhanh.
Hành động khi phát hiện mối đe dọa	**Chặn**. 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.
Kiểm tra địa chỉ web bằng cách đối chiếu với cơ sở dữ liệu địa chỉ web độc hại *(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)*	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.

Tham số	Mô tả
Sử dụng phân tích hành vi *(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)*	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.
Kiểm tra địa chỉ web bằng cách đối chiếu với cơ sở dữ liệu địa chỉ web lừa đảo *(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)*	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.
Không quét lưu lượng web từ các địa chỉ web được tin tưởng	Nếu chọn tùy chọn này, 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. 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 mối đe dọa web, Bảo vệ mối đe dọa thư điện tử và Kiểm soát web đang hoạt động.

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
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Để quét lưu lượng truy cập trong ứng dụng thư Mozilla Thunderbird, MyOffice Mail và R7-Office Organizer, bạn cần phải thêm chứng chỉ Kaspersky vào kho chứng chỉ và chọn kho chứng chỉ riêng.

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 Mail Threat Protection hỗ trợ các phiên bản 32 bit và 64 bit của Outlook 2010, 2013, 2016, 2019, 2021, 2024 và 365. Trên máy tính có kiến trúc Arm, phần mở rộng Mail Threat Protection hỗ trợ các phiên bản 32 bit và 64 bit của Outlook 2016, Outlook 2021, Outlook 2024 và Outlook 365 dành cho Arm64.

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 phần đính kèm, Kaspersky Endpoint Security sẽ thêm thông tin về hành động đã thực hiện vào chủ đề thư, ví dụ: *[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 *(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)*	Đối với thành phần Bảo vệ mối đe dọa thư điện tử, ứng dụng có thể áp dụng các nhóm thiết lập khác nhau. Các nhóm thiết lập được lưu trữ trong ứng dụng được gọi là *mức độ bảo mật*: • **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. • **Khuyên dùng**. Mức độ bảo mật email mang đến sự cân bằng tối ưu giữa hiệu năng của ứng dụng 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 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.
Hành động khi phát hiện mối đe dọa	**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, ứng dụng 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, ứng dụng sẽ xóa đối tượng bị nhiễm. Ứng dụng sẽ thêm thông tin về hành động được thực hiện vào chủ đề thư, ví dụ: *[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, ứng dụng 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, ứng dụng sẽ thêm cảnh báo vào chủ đề thư điện tử. 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, ứng dụng sẽ cố gắng khử mã độc đối tượng được phát hiện. Nếu không thể khử mã độc đối tượng, ứng dụng 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, ứng dụng sẽ thêm cảnh báo vào 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, ứng dụng sẽ chặn gửi thư và ứng dụng thư điện tử sẽ hiển thị lỗi.
Phạm vi bảo vệ *(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)*	*Phạm vi bảo vệ* 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.
Quét lưu lượng POP3, SMTP, NNTP, và IMAP	Thành phần Bảo vệ mối đe dọa thư điện tử sẽ 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.
Kết nối phần mở rộng Microsoft Outlook	Nếu hộp kiểm này được chọn, tính năng quét các email được truyền tải qua giao thứcPOP3, 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 Cached Exchange Mode. 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.

Tham số	Mô tả
Phân tích hành vi *(chỉ khả dụng trong Bảng điều khiển quản trị (MMC) và trong giao diện Kaspersky Endpoint Security)*	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.
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. Ứng dụng 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). Nếu trong quá trình quét, ứng dụng 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. Các tập tin có tiền tố PR.
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. Ứng dụng sẽ quét các tập tin định dạng văn phòng nhỏ hơn 1 MB, bất kể hộp kiểm này có được chọn hay không.
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 nén 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 nén 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 nén đính kèm email sẽ bị hạn chế trong khoảng thời gian được quy định.
Bộ lọc tập tin đính kèm	Chức năng bộ lọc tập tin đính kèm không được áp dụng cho các email gửi đi. **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: tattachment.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. 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 mối đe dọa mạng

Thành phần *Bảo vệ mối đe dọa mạng* (còn được gọi là Intrusion Detection System, IDS) sẽ giám sát lưu lượng truy cập mạng đến để biết hoạt động đặc trưng của các cuộc tấn công mạng. Khi ứng dụng 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 ứng dụng. 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.

Tham số	Mô tả
Coi hoạt động quét cổng và làm nghẽn mạng là các cuộc tấn công	*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. 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 mối đe dọa. 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.
Chặn các thiết bị tấn công cho N phút	Nếu tùy chọn này được bật, thành phần Bảo vệ mối đe dọa mạng sẽ thêm máy tính tấn công vào danh sách chặn. Điều này có nghĩa là thành phần Bảo vệ mối 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 999 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 mối đe dọa mạng bị thay đổi.
Loại trừ	Danh sách này chứa các địa chỉ IP mà Bảo vệ mối đe dọa mạng sẽ không chặn các cuộc tấn công mạng từ đó. Bạn có thể thêm một địa chỉ IP có cổng và giao thức được chỉ định. Ứng dụng không ghi lại thông tin về các cuộc tấn công mạng từ địa chỉ IP nằm trong danh sách loại trừ.
Bảo vệ chống giả mạo MAC	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.

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

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

Các kiểu kết nối mạng

Tường lửa cho phép bạn kiểm soát hoạt động mạng tùy thuộc vào kiểu của kết nối mạng. Kaspersky Endpoint Security sẽ nhận kiểu kết nối mạng từ hệ điều hành của máy tính. Kiểu của kết nối mạng trong hệ điều hành được người dùng đặt khi thiết lập kết nối. Bạn có thể thay đổi kiểu của kết nối mạng trong mục thiết lập của Kaspersky Endpoint Security. Tường lửa sẽ giám sát hoạt động mạng tùy thuộc vào kiểu mạng được chỉ định trong mục thiết lập của Kaspersky Endpoint Security chứ không phải trong hệ điều hành.

Có các kiểu kết nối mạng sau đây:

- **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 kiểu *Mạng công cộng* cho Internet theo mặc định. Bạn không thể thay đổi kiểu 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.

Tham số	Mô tả
Quy tắc gói tin	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. 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. 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. Các quy tắc gói tin mạng có ưu tiên cao hơn so với các quy tắc mạng cho ứng dụng.
Các mạng khả dụng	Bảng này chứa thông tin về các kết nối mạng được Tường lửa phát hiện trên máy tính. Trạng thái *Mạng công cộng* được gán cho internet ở chế độ mặc định. Bạn không thể thay đổi trạng thái của internet.
Quy tắc cho các ứng dụng	**Ứng dụng**. 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. 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. **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 khỏi kết nối đến máy tính.

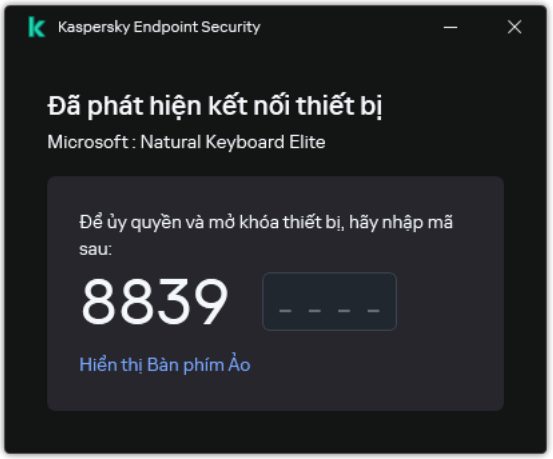
Khi một thiết bị USB được kết nối với máy tính và hệ điều hành xác định đó là một bàn phím thì ứng dụng sẽ nhắc người dùng nhập một mã số do ứng dụng tạo ra từ bàn phím này hoặc sử dụng Bàn phím ảo nếu có (xem hình bên dưới). Thủ tục này được gọi là xác thực bàn phím.

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.



Chứng thực bàn phím

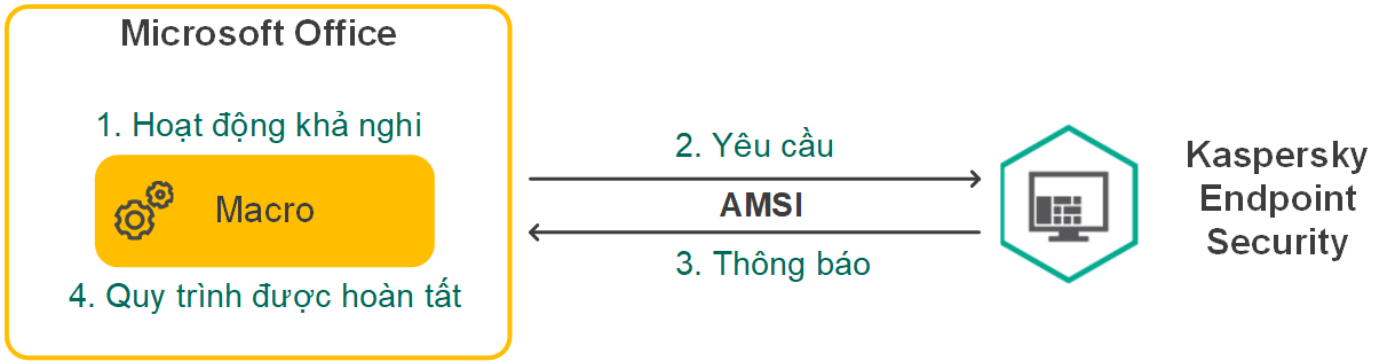
Cấu hình thành phần Phòng chống Tấn công BadUSB

Tham số	Mô tả
Nghiêm cấm việc sử dụng Bàn phím Ảo để xác thực các thiết bị USB	Nếu nút bật/tắt được chuyển thành bật, 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.
Nghiêm cấm việc sử dụng mã vạch để ủy quyền cho các thiết bị USB	Nếu bật công tắc bật/tắt này, ứng dụng sẽ không hiển thị mã vạch trong thông báo xác thực máy quét mã vạch.
Số lượng lần thử ủy quyền cho 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 năm lần nhập mã cho phép thì ứng dụng sẽ chặn thiết bị USB sau lần thử 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 sẽ lại có năm lần thử nhập mã cho phép.
Kết thúc thời gian chờ khi đạt số lượng lần thử tối đa	Thời gian khóa thiết bị USB sau số lần nhập mã xác thực 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 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 / Enterprise multi-session
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-session
- Windows Server 2016 Essentials / Standard / Datacenter (bao gồm chế độ Server Core);
- Windows Server 2019 Essentials / Standard / Datacenter (bao gồm chế độ Server Core);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (bao gồm chế độ Core Server);
- Windows Server 2025 Standard / Datacenter.

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. Ứng dụng 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	Quét các gói phân phối của ứng dụng 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. Ứng dụng sẽ quét các tập tin định dạng văn phòng nhỏ hơn 1 MB, bất kể hộp kiểm này có được chọn hay không.
Không giải nén các tập tin hỗn hợp lớn	Nếu hộp kiểm này được chọn, ứng dụng sẽ không quét các tập tin hỗn hợp nếu dung lượng của chúng vượt quá giá trị ấn định. Nếu bỏ chọn hộp kiểm này, ứng dụng sẽ quét các tập tin tổ hợp thuộc mọi kích thước. Ứng dụng 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.

Thành phần Phòng chống khai thác còn giám sát các cổng mạng để tìm các tiến trình của ứng dụng có thể đe dọa đến tính bảo mật của máy tính. Ứng dụng sẽ lấy thông tin về những tiến trình như vậy thông qua cơ sở dữ liệu chống virus.

Cấu hình thành phần Phòng chống khai thác

Tham số	Mô tả
Khi phát hiện khai thác	**Chặn**. 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.
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 và cung cấp chức năng bảo vệ chủ động cho máy tính.

Thành phần Phát hiện hành vi còn giám sát các cổng mạng để tìm các tiến trình của ứng dụng có thể đe dọa đến tính bảo mật của máy tính. Ứng dụng sẽ lấy thông tin về những tiến trình như vậy thông qua cơ sở dữ liệu chống virus.

Cấu hình thành phần Phát hiện hành vi

Tham số	Mô tả
Hành động khi phát hiện hoạt động của phần mềm độc hại	**Xóa**. 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. **Chặn**. 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.

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 dữ liệu cá nhân (ví dụ: các tập tin và ứng dụng)

Hoạt động mạng của các ứng dụng được kiểm soát bởi thành phần 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 sử dụng 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. Đặt 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	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. 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. Quyền truy cập của ứng dụng được trình bày trong các bảng sau: • **Tập tin và registry hệ thống**. Bảng quyền truy cập tài nguyên hệ điều hành và dữ liệu cá nhân cho các ứng dụng thuộc nhóm tin tưởng. • **Quyền**. Bảng quyền truy cập cho các tiến trình và tài nguyên của hệ điều hành đối với các ứng dụng thuộc nhóm tin tưởng. • **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.
Bảo vệ tài nguyên	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. Một tài nguyên có thể là một danh mục registry, tập tin hoặc thư mục, hoặc khóa registry.
Nhóm tin tưởng cho các ứng dụng được khởi chạy trước khi Kaspersky Endpoint Security	Một nhóm tin tưởng trong đó Kaspersky Endpoint Security sẽ đặt các ứng dụng được khởi chạy trước Kaspersky Endpoint Security.
Cập nhật quy tắc cho các ứng dụng trước đó chưa biết từ KSN	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.
Tin tưởng các ứng dụng được ký số	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*. *Nhà cung cấp được tin tưởng* 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. 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.
Xóa quy tắc cho các ứng dụng không được khởi động nhiều hơn N số ngày (từ 1 đến 90)	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: • Bạn đặt ứng dụng vào nhóm tin tưởng hoặc cấu hình quyền truy cập của ứng dụng một cách thủ công. • Ứng dụng chưa khởi chạy trong khoảng thời gian xác định. 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. 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.
Nhóm tin tưởng cho các ứng dụng không có trong các nhóm khác	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. Bạn có thể chọn một trong các tùy chọn sau: • **Giới hạn mức Thấp**. • **Giới hạn mức Cao**. • **Không tin tưởng**.

Công cụ khắc phục

Thành phần 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 phần mềm độc hại.

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.

Chức năng KSN có thể không khả dụng trong ứng dụng ở Hoa Kỳ.

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 tiếng của các địa chỉ web được quét, cũng như thông tin về danh mục và danh tiếng của các tập tin được quét. Để biết thêm chi tiết về cách cấu hình quyền truy cập vào KSN, hãy tham khảo Trợ giúp Kaspersky Security Center.

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.

Cơ sở hạ tầng cơ sở dữ liệu danh tiếng của Kaspersky

Kaspersky Endpoint Security hỗ trợ các giải pháp cơ sở hạ tầng sau để làm việc với cơ sở dữ liệu danh tiếng của Kaspersky:

- *Kaspersky Security Network (KSN)* là giải pháp được hầu hết các ứng dụng Kaspersky sử dụng. Người tham gia vào KSN sẽ nhận thông tin từ Kaspersky 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.

- *Kaspersky Private Security Network (KPSN)* 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 và truy cập các dữ liệu thống kê khác mà không cần gửi dữ liệu cho Kaspersky từ máy tính của riêng họ. KPSN được thiết kế dành cho khách hàng doanh nghiệp, là những khách hàng 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.

Tham số	Mô tả
Bật 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. 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	*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. 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 Máy chủ quản trị làm máy chủ 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 các máy chủ Kaspersky Security Network nếu máy chủ proxy KSN không khả dụng *(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 và trên một bên thứ ba (khi Kaspersky Private Security Network được sử dụng).

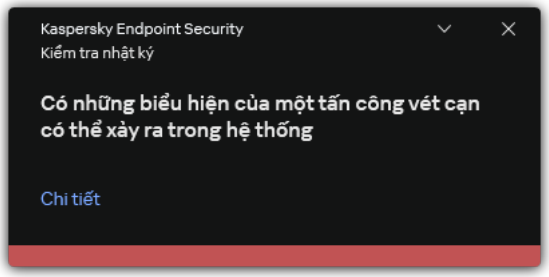
Kiểm tra nhật ký

Thành phần này khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows cho máy chủ. Thành phần này không khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows dành cho máy trạm.

Kiểm tra nhật ký sẽ giám sát tính toàn vẹn của môi trường được bảo vệ dựa trên phân tích nhật ký sự kiện của Windows. Khi ứng dụng phát hiện các dấu hiệu của hành vi bất thường trong hệ thống, ứng dụng sẽ thông báo cho quản trị viên, vì hành vi này có thể chỉ báo một nỗ lực tấn công mạng.

Kaspersky Endpoint Security sẽ phân tích nhật ký sự kiện của Windows và phát hiện vi phạm theo các quy tắc. Thành phần này bao gồm quy tắc định trước. Các quy tắc định trước được cung cấp bởi phân tích hành vi. Bạn cũng có thể thêm các quy tắc của riêng của mình (quy tắc tùy chỉnh). Khi một quy tắc kích hoạt, ứng dụng sẽ tạo một sự kiện có trạng thái *Critical* (xem hình bên dưới).

Nếu bạn muốn sử dụng Kiểm tra nhật ký, hãy đảm bảo rằng thiết lập bảo mật chính sách kiểm tra được cấu hình và hệ thống đang ghi nhật ký các sự kiện liên quan (để biết chi tiết, hãy xem Website hỗ trợ kỹ thuật của Microsoft.).



Thông báo Kiểm tra nhật ký

Thiết lập Kiểm tra nhật ký

Tham số	Mô tả
Các quy tắc định trước	Danh sách các quy tắc Kiểm tra nhật ký. Các quy tắc định trước bao gồm các mẫu hoạt động bất thường trên máy tính được bảo vệ. Hoạt động bất thường có thể báo hiệu một cuộc tấn công có chủ đích.
Quy tắc tùy chỉnh	Danh sách các quy tắc Kiểm tra nhật ký được thêm bởi người dùng. Bạn có thể đặt tiêu chí kích hoạt quy tắc Kiểm tra nhật ký của riêng mình. Để thực hiện, bạn phải nhập ID sự kiện và chọn nguồn sự kiện. Bạn có thể chọn một nguồn sự kiện trong số các nhật ký tiêu chuẩn: *Application*, *Security* hoặc *System*. Bạn cũng có thể chỉ định nhật ký của ứng dụng bên thứ ba.

Anti-Cryptor

Thành phần Anti-Cryptor sẽ 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.

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.

Tham số	Mô tả
Loại trừ theo tên hoặc địa chỉ IP	**Loại trừ theo tên hoặc địa chỉ IP**. Danh sách các máy tính sẽ không bị giám sát khi thực hiện mã hóa thư mục được chia sẻ. 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. **Loại trừ theo tên đại diện**. Loại trừ phạm vi bảo vệ. Việc loại trừ một thư mục khỏi phạm vi bảo vệ 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. 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 cấp 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.
Hành động khi phát hiện mối đe dọa	• **Thông báo**. Nếu tùy chọn 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 này vào danh sách các mối đe dọa đang hoạt động, hãy thêm một mục vào báo cáo giao diện ứng dụng cục bộ và gửi thông tin về hoạt động độc hại được phát hiện tới Kaspersky Security Center. • **Chặn kết nối trong (phút) 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 quyền truy cập sửa đổi tập tin cho phiên đã khởi tạo hoạt động độc hại và sẽ tạo các bản sao lưu của tập tin bị sửa đổi. Nếu thành phần Công cụ khắc phục được bật và tùy chọn **Chặn kết nối trong (phút) N phút** được chọn thì các tập tin bị sửa đổi sẽ được khôi phục từ bản sao lưu.
Phạm vi bảo vệ	*Phạm vi bảo vệ* là danh sách các đường dẫn đến các thư mục chia sẻ mà Kaspersky Endpoint Security theo dõi hoạt động đối với tập tin. Kaspersky Endpoint Security hỗ trợ các biến môi trường và ký tự `*` cùng `?` khi nhập tên đại diện. Theo mặc định, ứng dụng sẽ tự động xác định các thư mục được chia sẻ và theo dõi hoạt động đối với tập tin trong tất cả các thư mục.

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).

Để sử dụng Kiểm soát web, bạn phải hoàn tất cấu hình ban đầu của ứng dụng:

- Để giám sát lưu lượng HTTPS, hãy bật kết nối được mã hóa quét (được bật theo mặc định).
- Chọn các cổng mà Kaspersky Endpoint Security phải giám sát (theo mặc định, ứng dụng sẽ giám sát tất cả các cổng).

- Chọn các ứng dụng có lưu lượng mà bạn muốn Kaspersky Endpoint Security giám sát. Hầu hết các trình duyệt đã có trong danh sách ứng dụng đều được Kaspersky khuyên dùng. Hãy thêm theo cách thủ công nếu trình duyệt của bạn không có trong danh sách.

- Bạn nên chèn một tập lệnh tương tác trang web vào lưu lượng truy cập web (chèn tập lệnh bị tắt theo mặc định). 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.

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 ẩn các ảnh. 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 *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 *Các tập tin ứng dụng văn phòng* chỉ với danh mục website *Email 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.

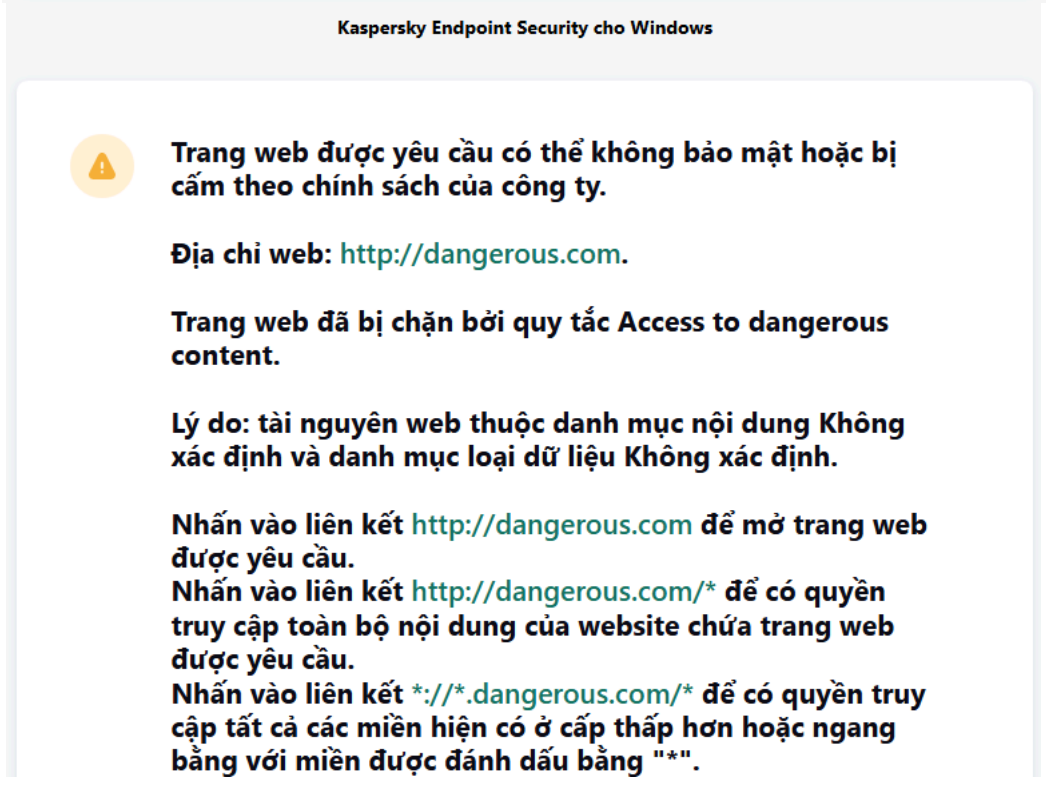
- Lịch quy tắc.

  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.





Thông báo của 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 mặc định	*Quy tắc mặc định* 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: • **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.
Chấm dứt các phiên trình duyệt của người dùng đang hoạt động sau khi áp dụng quy tắc	Nếu hộp kiểm được chọn, Kiểm soát web sẽ chấm dứt kết nối tới các tài nguyên web bị chặn ngay sau khi áp dụng chính sách. Trình duyệt sẽ ngay lập tức dừng tải dữ liệu từ trang web. Khi bạn làm mới trang web hoặc truy cập trang web bị cấm khác, ứng dụng sẽ hiển thị cảnh báo. Kiểm soát web chỉ cho phép ngắt kết nối ngay lập tức các tài nguyên web trong trình duyệt web. Đối với các ứng dụng khác, Kiểm soát web chỉ hạn chế các kết nối mới. Nếu bỏ chọn hộp kiểm này, Kiểm soát web sẽ chỉ hạn chế các kết nối mới tới các tài nguyên web bị cấm. Kiểm soát web không chấm dứt các kết nối đang hoạt động.
Mẫu	**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. Các biến đặc biệt được cung cấp để quản lý mẫu tin nhắn (ví dụ: `%USER_NAME%`). Biến cho phép sử dụng một mẫu tin nhắn duy nhất cho nhiều máy tính khác nhau.
Ghi lại việc mở ra các trang được cho phép	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. 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. 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.

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 mất hoặc rò rỉ dữ liệu.

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 **Advanced → Repositories → Hardware**.

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 – .
  - Bởi quy tắc (chỉ dành cho máy in và thiết bị di động) – .
  - Tùy thuộc vào bus kết nối (ngoại trừ Wi-Fi) – .
  - Chặn với ngoại lệ (Chỉ 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). Nếu như chế độ **Tùy thuộc vào bus kết nối** được chọn cho loại thiết bị, ứng dụng sẽ cho phép hoặc từ chối truy cập thiết bị, tùy thuộc vào giao diện kết nối (ví dụ: 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 (Hardware ID hay HWID). Bạn có thể xem ID trong thuộc tính thiết bị bằng cách sử dụng công cụ hệ điều hành. Ví dụ về ID thiết bị: `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 Vendor ID (VID) và một Product ID (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.

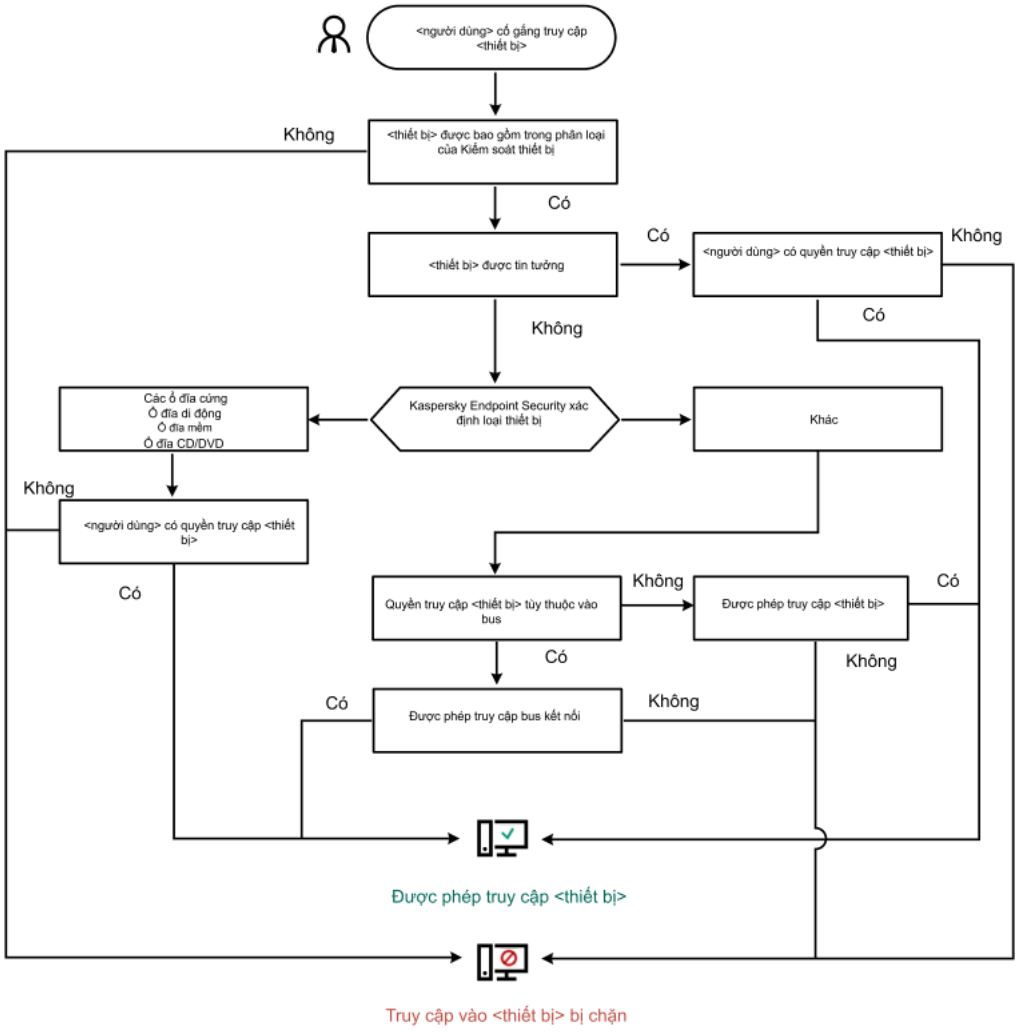
Khi một thiết bị bị chặn bởi Kiểm soát thiết bị được kết nối đến máy tính, Kaspersky Endpoint Security sẽ chặn quyền truy cập và hiển thị một thông báo (xem hình dưới đây).



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).



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.

Tham số	Mô tả
Cho phép các yêu cầu truy cập tạm thời *(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)*	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. Khi dùng 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. Kaspersky Endpoint Security cho phép hoặc từ chối truy cập các thiết bị, tùy thuộc vào kiểu bus kết nối nếu chọn chế độ **Tùy thuộc vào bus kết nối**.
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.
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 thiết bị 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 thiết bị 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 thiết bị 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. Chức năng này cũng cho phép gộp danh sách trong hồ sơ chính sách. Để gộp danh sách, trong hồ sơ có mức độ ưu tiên cao nhất, hãy bật tính năng kế thừa thiết lập từ cấu hình có mức độ ưu tiên thấp hơn. Để biết thêm chi tiết về mức độ ưu tiên của hồ sơ chính sách, vui lòng tham khảo Trợ giúp của Kaspersky Security Center.
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 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. Nếu một kết nối đang hoạt động và một kết nối mới đều 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. 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. Anti-Bridging hỗ trợ hoạt động với các loại thiết bị sau: bộ điều hợp mạng, Wi-Fi và modem.
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* hoặc danh mục khác), 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. Quản trị viên có thể tạo nhiều quy tắc. Một ứng dụng có thể khớp tiêu chí của nhiều quy tắc. Một quy tắc chặn được ưu tiên hơn một quy tắc cho phép. Kaspersky Endpoint Security sẽ kiểm tra xem ứng dụng có khớp với quy tắc nào không mỗi khi khởi động. Kaspersky Endpoint Security sẽ so sánh tuần tự ứng dụng với tất cả các quy tắc Kiểm soát ứng dụng.

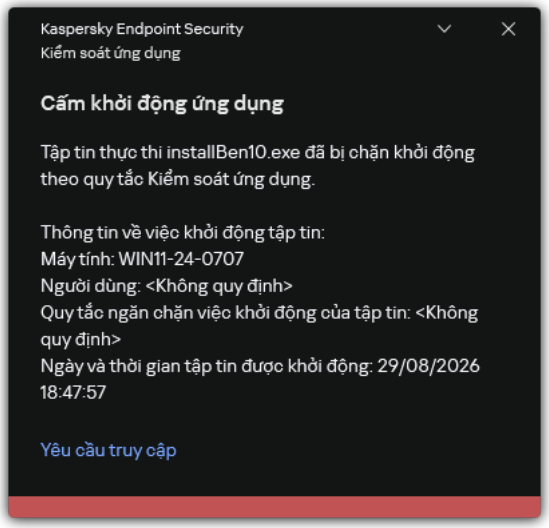
3. Chọn chế độ Kiểm soát ứng dụng.

   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.

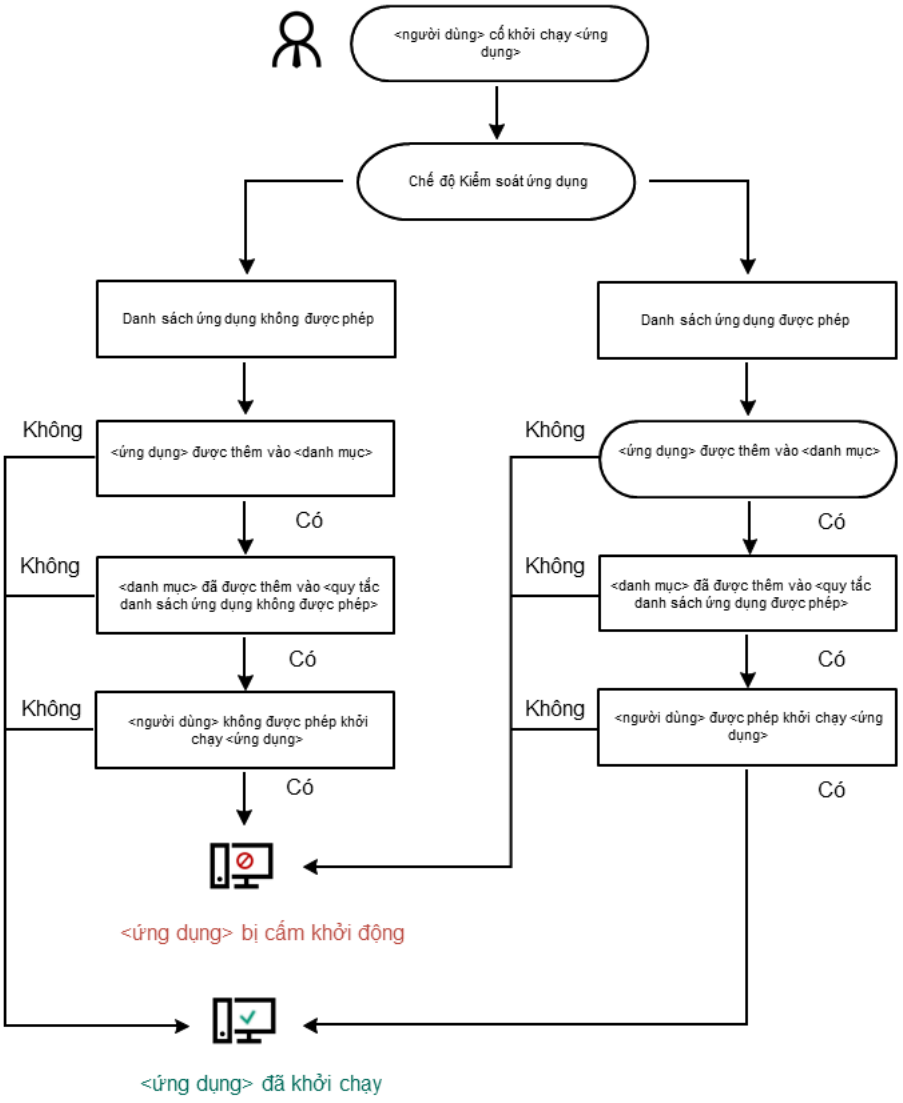
  Quy tắc kiểm soát ứng dụng được tạo trong Bảng điều khiển quản trị Kaspersky Security Center dựa trên các danh mục ứng dụng tùy chỉnh của bạn chứ không dựa trên các điều kiện bao gồm và loại trừ như trong trường hợp trong giao diện cục bộ của Kaspersky Endpoint Security.

- 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

Tham số	Mô tả
Hành động khi khởi động các ứng dụng bị chặn theo quy tắc	**Áp dụng quy tắc**. Kaspersky Endpoint Security sẽ quản lý việc khởi động các ứng dụng theo chế độ đã chọn. **Kiểm tra quy tắc**. 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 ứng dụng trong báo cáo.
Chế độ Kiểm soát khởi động ứng dụng	Bạn có thể 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. Khi chế độ **Danh sách được phép** được chọn, hai quy tắc Kiểm soát ứng dụng sẽ tự động được tạo: • **Tập tin ảnh hoàn hảo**. • **Trình cập nhật được tin tưởng**. 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.
Giám sát việc tải các mô-đun DLL	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. 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 "**Tập tin ảnh hoàn hảo\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. 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.
Sử dụng xác minh chữ ký số nghiêm ngặt	Bạn có thể chọn chứng chỉ làm điều kiện kích hoạt cho một quy tắc Kiểm soát ứng dụng. Nếu chọn hộp kiểm này, Kaspersky Endpoint Security sẽ chỉ áp dụng các quy tắc cho các ứng dụng được ký bằng chứng chỉ từ kho chứng chỉ hệ thống được tin tưởng. Các ứng dụng được ký bằng chứng chỉ như vậy cũng được coi là được tin tưởng bởi các thành phần bảo vệ, ví dụ như tác vụ *Quét phần mềm độc hại*. Tuy nhiên, nếu bạn chỉ định chứng chỉ từ một kho khác trong quy tắc Kiểm soát ứng dụng thì Kaspersky Endpoint Security sẽ không áp dụng quy tắc đó. Nếu bỏ chọn hộp kiểm này, Kaspersky Endpoint Security sẽ áp dụng các quy tắc cho các ứng dụng được ký bằng chứng chỉ từ Kho chứng chỉ gốc được tin tưởng của Windows. Những ứng dụng như vậy không thuộc vùng tin tưởng. Các thành phần bảo vệ sẽ giám sát hoạt động của các ứng dụng đó.
Mẫu tin nhắn về việc chặn 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 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.

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 không điển hình (ví dụ, quy tắc *Khởi chạy Microsoft PowerShell từ ứng dụng office*). 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

Việc 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 huấn luyện, Kaspersky Endpoint Security sẽ ghi lại sự kiện này trong báo cáo kích hoạt quy tắc và kho lưu trữ **Rule triggers in Smart Training state**.

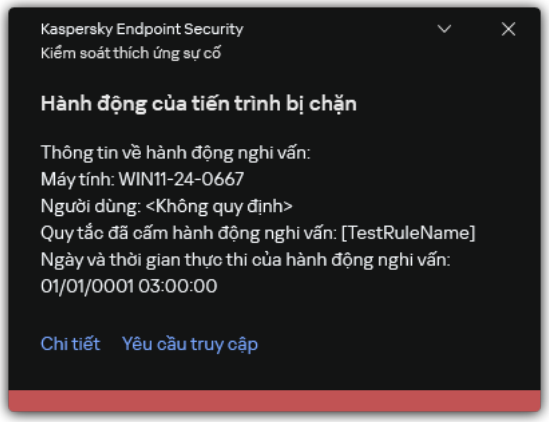
2. Phân tích báo cáo kích hoạt quy tắc.

   Quản trị viên sẽ phân tích báo cáo kích hoạt quy tắc hoặc nội dung của kho lưu trữ **Rule triggers 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 theo thời gian thực 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 **Rule triggers in Smart Training state**. Bạn nên kiểm tra báo cáo về việc kích hoạt các quy tắc và nội dung của kho lưu trữ **Rule triggers in Smart Training state**.

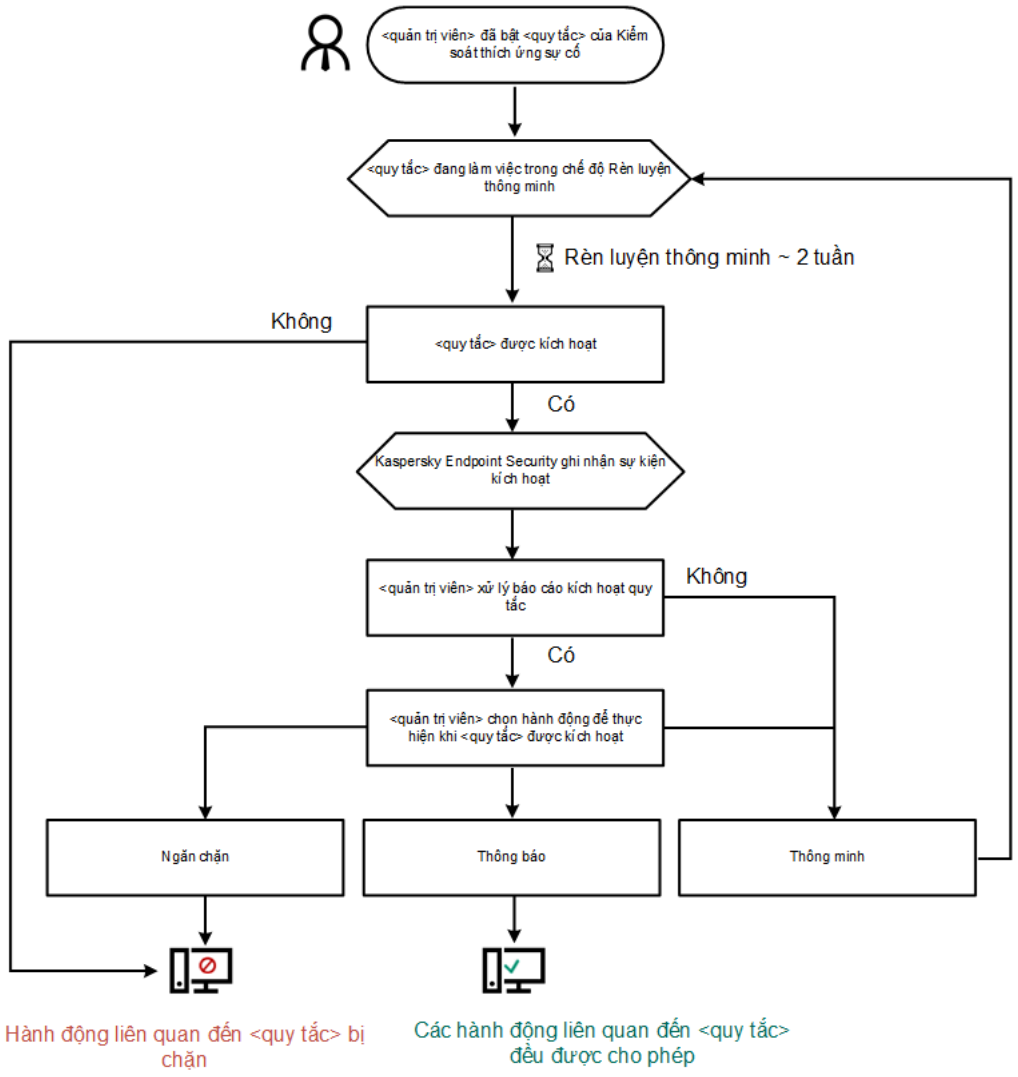
Khi một ứng dụng độc hại cố gắng thực hiện một hành động, Kaspersky Endpoint Security sẽ chặn hành động đó và hiển thị một thông báo (xem hình dưới đây).



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
Báo cáo về trạng thái các quy tắc Kiểm soát thích ứng sự cố *(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)*	Báo cáo này chứa thông tin về trạng thái của quy tắc phát hiện Kiểm soát thích ứng sự cố (ví dụ, *Đã tắt* hoặc *Chặn*). Báo cáo này được tạo cho tất cả các nhóm quản trị.
Báo cáo về các quy tắc Kiểm soát thích ứng sự cố được kích hoạt *(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)*	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.

Tham số	Mô tả
Quy tắc	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 thông thường.
Mẫu	**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.

Giám sát tính toàn vẹn của hệ thống

Thành phần này khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows cho máy chủ. Thành phần này không khả dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Windows dành cho máy trạm.

Kể từ phiên bản 12.6, Kaspersky Endpoint Security cho Windows đã bao gồm thành phần Giám sát toàn vẹn của hệ thống thay vì thành phần Giám sát tính toàn vẹn của tập tin. Thành phần Giám sát tính toàn vẹn của hệ thống bao gồm tất cả chức năng của Giám sát tính toàn vẹn của tập tin và ngoài ra còn cho phép giám sát các thay đổi của registry và kết nối của các thiết bị bên ngoài.

Thành phần Giám sát tính toàn vẹn của hệ thống sẽ giám sát những thay đổi trong hệ điều hành, có thể cho biết các hành vi xâm nhập bảo mật máy tính. Khi phát hiện những thay đổi như vậy, Kaspersky Endpoint Security sẽ tạo ra các sự kiện tương ứng và cảnh báo cho quản trị viên. Giám sát tính toàn vẹn hệ thống có thể hoạt động ở chế độ thời gian thực và cũng có thể thực hiện kiểm tra tính toàn vẹn hệ thống theo yêu cầu.

Giám sát tính toàn vẹn của hệ thống theo thời gian thực

Ở chế độ thời gian thực, Giám sát tính toàn vẹn của hệ thống theo dõi các thay đổi trong các đối tượng mà bạn đã đưa vào phạm vi của thành phần (*phạm vi giám sát*). Giám sát tính toàn vẹn hệ thống cũng cho phép chặn truy cập trái phép vào các đối tượng đó trong thời gian thực.

Kiểm tra tính toàn vẹn của hệ thống theo yêu cầu

Kiểm tra tính toàn vẹn của hệ thống theo yêu cầu là một tác vụ mà bạn có thể chạy thủ công hoặc theo lịch. Để chạy tác vụ *Kiểm tra tính toàn vẹn của hệ thống*, bạn phải cấu hình phạm vi của thành phần (*phạm vi giám sát*) và tạo đường cơ sở. *Đường cơ sở* là trạng thái được ghi lại của các đối tượng trong hệ thống, được ứng dụng sử dụng làm tham chiếu khi so sánh với trạng thái hiện tại.

Tham số	Mô tả
Chế độ hoạt động để chặn quy tắc	• **Chặn**. Ở chế độ này, Giám sát tính toàn vẹn hệ thống sẽ chặn các hành động với tập tin và khóa registry khỏi phạm vi giám sát và tạo ra một sự kiện tương ứng. • **Thông báo**. Ở chế độ này, Giám sát tính toàn vẹn hệ thống cho phép thực hiện các hành động với tập tin và khóa registry từ phạm vi giám sát và tạo ra một sự kiện tương ứng.
Giám sát tính toàn vẹn của hệ thống theo thời gian thực	Ở chế độ thời gian thực, Giám sát tính toàn vẹn của hệ thống theo dõi các thay đổi trong các đối tượng mà bạn đã đưa vào phạm vi của thành phần (*phạm vi giám sát*). Giám sát tính toàn vẹn hệ thống cũng cho phép chặn truy cập trái phép vào các đối tượng đó trong thời gian thực.
Giám sát thiết bị	Giám sát tính toàn vẹn hệ thống sẽ giám sát kết nối và ngắt kết nối của các thiết bị bên ngoài.
Giám sát tập tin và registry	Giám sát tính toàn vẹn hệ thống sẽ giám sát các thay đổi đối với tập tin, thư mục và registry.
Kiểm tra tính toàn vẹn của hệ thống	Kiểm tra tính toàn vẹn của hệ thống theo yêu cầu là một tác vụ mà bạn có thể chạy thủ công hoặc theo lịch. Để chạy tác vụ *Kiểm tra tính toàn vẹn của hệ thống*, bạn phải cấu hình phạm vi của thành phần (*phạm vi giám sát*) và tạo đường cơ sở. *Đường cơ sở* là trạng thái được ghi lại của các đối tượng trong hệ thống, được ứng dụng sử dụng làm tham chiếu khi so sánh với trạng thái hiện tại.

Endpoint Sensor

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 ba đơn vị chức năng:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Bạn có thể mua tất cả các đơn vị chức năng hoặc mua riêng từng đơn vị chức năng. 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.

Sandbox

Kaspersky Endpoint Security for Windows bao gồm một tác nhân tích hợp sẵn để tích hợp với giải pháp Kaspersky Sandbox. Thành phần *Sandbox* phát hiện và tự động chặn các mối đe dọa nâng cao trên máy tính. 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. 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 (các máy chủ Sandbox). Để biết chi tiết về giải pháp này, vui lòng tham khảo Trợ giúp của Kaspersky Sandbox và Trợ giúp của Kaspersky Anti Targeted Attack Platform.

Kể từ phiên bản 12.7, Kaspersky Endpoint Security cho Windows hỗ trợ thành phần Sandbox, là một phần của giải pháp Kaspersky Anti Targeted Attack Platform. Ngược lại với giải pháp Kaspersky Sandbox, thành phần KATA Sandbox cho phép quét tập tin không chỉ theo cách tự động mà còn cho phép theo cách thủ công từ menu ngữ cảnh của tập tin.

KATA Sandbox cần có Kaspersky Anti Targeted Attack Platform 7.0 trở lên được triển khai.

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 Sandbox

Tham số	Mô tả
Integration mode	**Kaspersky Sandbox**. Tích hợp với giải pháp Kaspersky Sandbox. Ứng dụng chỉ gửi các tập tin để quét trong Kaspersky Sandbox ở chế độ tự động. **KATA Sandbox**. Tích hợp với thành phần Sandbox của giải pháp Kaspersky Anti Targeted Attack Platform. Bạn có thể chọn chế độ gửi tập tin để quét: • **Manually**. Người dùng gửi tập tin theo cách thủ công để quét từ menu ngữ cảnh (**Gửi đến Sandbox**). • **Automatically**. Ứng dụng tự động phát hiện các đối tượng và gửi chúng đến Sandbox để quét. • **Combined**.
Server connection settings	**Timeout (msec)**. Thời gian chờ kết nối cho máy chủ Sandbox (đối với Kaspersky Sandbox) hoặc máy chủ Central Node (đối với KATA). 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 máy chủ 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. **Request queue**. Kích thước của thư mục hàng chờ yêu cầu. Khi gửi nhiều đối tượng để quét trong Sandbox, 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, 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. **Server TLS certificate**. Để cấu hình kết nối được tin tưởng với máy chủ Sandbox (đối với Kaspersky Sandbox) hoặc máy chủ Central Node (đối với KATA), bạn phải chuẩn bị chứng chỉ TLS. Sau đó, bạn phải thêm chứng chỉ vào máy tính bằng chính sách. Bạn cũng cần thêm chứng chỉ vào máy chủ Sandbox (đối với Kaspersky Sandbox) hoặc máy chủ Central Node (đối với KATA). **Use two-way authentication** (chỉ dành cho KATA Sandbox). Xác thực hai chiều khi thiết lập kết nối bảo mật giữa Kaspersky Endpoint Security và máy chủ Central Node. Để sử dụng xác thực hai chiều, bạn cần bật xác thực hai chiều trong cài đặt máy chủ Central Node, sau đó lấy bộ chứa mã hóa và đặt mật khẩu để bảo vệ bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể nhận một bộ chứa mã hóa trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform). Sau khi cấu hình thiết lập Central Node, bạn cũng cần bật xác thực hai chiều trong thiết lập của Kaspersky Endpoint Security và tải bộ chứa mã hóa được bảo vệ bằng mật khẩu.
Connection to Sandbox servers	**Kaspersky Sandbox**. Thiết lập kết nối máy chủ 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. **KATA Sandbox**. Thiết lập kết nối máy chủ Central Node. Central Node sẽ chọn cài đặt tối ưu để quét và cân bằng tải giữa các máy chủ Sandbox.
Action on threat detection	**Move copy to Quarantine, delete object**. 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. **Run Critical Areas Scan**. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ chạy tác vụ *Critical Areas Scan*. Theo mặc định, Kaspersky Endpoint Security sẽ quét nhân kernel, các tiến trình đang chạy, và phân vùng khởi động ổ đĩa. **Create IOC Scan task**. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ tự động tạo tác vụ *IOC Scan (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 (*Move copy to Quarantine, delete object* hoặc *Run Critical Areas Scan*). Để sửa đổi các thiết lập khác của tác vụ *IOC Scan*, hãy vào mục thiết lập tác vụ.
IOC Scan scope	**Critical file areas**. 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. **File areas on system drive of the computer**. Nếu tùy chọn này được chọn, Kaspersky Endpoint Security sẽ thực hiện quét IOC trên ổ đĩa hệ thống của máy tính.
Run IOC Scan task	**Manually**. Chế độ chạy trong đó bạn có thể tiến hành tác vụ *IOC Scan* theo cách thủ công tại một thời điểm thuận tiện cho bạn. **Automatically**. Chế độ chạy trong đó Kaspersky Endpoint Security sẽ chạy tác vụ *IOC Scan* tự động sau khi phát hiện một mối đe dọa. **Run only when the computer is idle**. Chế độ chạy trong đó Kaspersky Endpoint Security sẽ chạy *Quét IOC* 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.

Managed Detection and Response

Kaspersky Endpoint Security cho Windows hỗ trợ tích hợp với giải pháp Managed Detection and Response được quản lý. 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.

Thiết lập Managed Detection and Response

Tham số	Mô tả
Tập tin cấu hình MDR	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.

Endpoint Detection and Response

Kaspersky Endpoint Security for Windows bao gồm một tác nhân tích hợp cho giải pháp Kaspersky Endpoint Detection and Response Optimum (sau đây gọi là "EDR Optimum"). Kể từ phiên bản 11.8.0, Kaspersky Endpoint Security cho Windows 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. *Báo động* là một sự kiện trong cơ sở hạ tầng CNTT của công ty mà ứng dụng đã xác định là bất thường hoặc đáng ngờ và có thể gây ra mối đe dọa bảo mật cho cơ sở hạ tầng CNTT của công ty. *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 Endpoint Detection and Response Optimum trong Bảng điều khiển web và Bảng điều khiển đám mây. Cài đặt của thành phần Endpoint Detection and Response Expert (cloud) chỉ khả dụng trong Bảng điều khiển đám mây.

Tham số	Mô tả
Enable advanced system activity logging	Việc mở rộng đo từ xa giúp cải thiện độ chính xác của việc phát hiện IOC, nhưng lại tiêu tốn nhiều tài nguyên máy tính hơn. Bạn nên bật tính năng đo từ xa mở rộng trên máy tính để quét IOC hồi cứu. *Quét IOC hồi cứu* là một chế độ của tác vụ *IOC Scan*, trong đó Kaspersky Endpoint Security sẽ quét để tìm dấu hiệu về sự xâm nhập bằng cách sử dụng dữ liệu trong một khoảng thời gian nhất định. Chế độ này được thiết kế để tìm kiếm các dấu hiệu xâm nhập thông qua dữ liệu đo từ xa của máy tính được bảo vệ, chẳng hạn như hoạt động mạng, các tiến trình, tập tin và các dữ liệu đo từ xa khác. Nếu tính đo từ xa mở rộng bị vô hiệu hóa, Kaspersky Endpoint Security có thể sẽ thay đổi thông tin về các dấu hiệu xâm nhập đã phát hiện.
Network Isolation	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: • 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.
Automatically unlock isolated device in (hours)	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	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. 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. 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.
Execution Prevention	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. Để sử dụng thành phần Phòng chống thực thi, bạn cần thêm 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.
Action on execution or opening of forbidden object	**Block and add to event log**. 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. **Add to event log**. 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.
Execution prevention rules	*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.

Tham số	Mô tả
Cloud Sandbox	*Cloud Sandbox* là công nghệ cho phép bạn phát hiện các mối đe dọa nâng cao trên máy tính. Kaspersky Endpoint Security sẽ tự động chuyển tiếp các tập tin được phát hiện tới Cloud Sandbox để phân tích. Cloud Sandbox sẽ chạy các tập tin này trong một môi trường cách ly để xác định hoạt động độc hại và quyết định danh tiếng của chúng. Sau đó, dữ liệu về các tập tin này sẽ được gửi đến Kaspersky Security Network. Do đó, nếu Cloud Sandbox đã phát hiện ra tập tin độc hại thì Kaspersky Endpoint Security sẽ thực hiện hành động thích hợp để loại bỏ mối đe dọa này trên tất cả các máy tính nơi tập tin này được phát hiện. Công nghệ Cloud Sandbox được bật vĩnh viễn và khả dụng cho tất cả người dùng Kaspersky Security Network bất kể họ đang sử dụng loại giấy phép nào. Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ bật bộ đếm các mối đe dọa được phát hiện bằng Cloud Sandbox trong cửa sổ chính của ứng dụng trong **Công nghệ phát hiện mối đe dọa**. Kaspersky Endpoint Security cũng sẽ chỉ báo công nghệ phát hiện mối đe dọa Cloud Sandbox trong các sự kiện ứng dụng và trong *Report on threats* trong bảng điều khiển Kaspersky Security Center.

Endpoint Detection and Response Expert (on-premises)

Endpoint Detection and Response Expert (on-premises)

Kaspersky Endpoint Security cho Windows hỗ trợ tích hợp với giải pháp Kaspersky Endpoint Detection and Response Expert (on-premises). *Kaspersky Endpoint Detection and Response Expert (on-premises)* là giải pháp bảo mật mạng doanh nghiệp bao gồm các ứng dụng Kaspersky cho phép tổ chức phòng vệ trước hầu hết các loại rủi ro mạng và xử lý các tình huống phát tán mối đe dọa quan trọng nhất. Các thành phần của EDR Expert (on-premises) được triển khai trên Open Single Management Platform (OSMP). Nền tảng này chạy các kịch bản đa nền tảng trong một giao diện duy nhất và cho phép tích hợp các ứng dụng Kaspersky với ứng dụng của bên thứ ba thành một hệ thống bảo mật toàn diện.

Một trong những yếu tố cốt lõi của giải pháp là *SIEM*. SIEM theo dõi các sự kiện đến từ tất cả các thành phần và liên kết các sự kiện này với nhau bằng cách sử dụng các quy tắc do nhà cung cấp và người dùng định nghĩa. EDR Expert (on-premises) xem xét nhật ký và dữ liệu đo từ xa nhận được từ cơ sở hạ tầng của doanh nghiệp để tự động phát hiện các cuộc tấn công và cho phép điều tra sự cố bằng cách sử dụng biểu đồ điều tra thống nhất, kết hợp tất cả các sự kiện được thu thập trong EDR Expert (on-premises), bao gồm các sự kiện từ các ứng dụng Kaspersky và các sản phẩm bảo mật thông tin của bên thứ ba.

Để ứng phó với các sự cố phức tạp, EDR Expert (on-premises) sử dụng các kịch bản được thiết lập sẵn và do người dùng định nghĩa. Bạn cũng có thể sử dụng hành động phản hồi từ ứng dụng của bên thứ ba và kịch bản phản hồi liên quan đến nhiều ứng dụng.

Endpoint Detection and Response (KATA)

Kaspersky Endpoint Security for Windows hỗ trợ làm việc với thành phần Kaspersky Endpoint Detection and Response, thuộc giải pháp Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *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 ba đơn vị chức năng:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Bạn có thể mua tất cả các đơn vị chức năng hoặc mua riêng từng đơn vị chức năng. Để biết chi tiết về giải pháp này, vui lòng tham khảo Trợ giúp của Kaspersky Anti Targeted Attack Platform.

Kaspersky Endpoint Security 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 (dữ liệu đo từ xa) được gửi đến máy chủ của Kaspersky Anti Targeted Attack Platform. Trong trường hợp này, Kaspersky Endpoint Security cũng gửi thông tin đến máy chủ của Kaspersky Anti Targeted Attack Platform về các mối đe dọa được phát hiện bởi ứng dụng, bao gồm cả thông tin về kết quả xử lý các mối đe dọa này.

Việc tích hợp EDR (KATA) và NDR (KATA) được cấu hình trong bảng điều khiển Kaspersky Security Center. Tác nhân tích hợp sau đó được quản lý bằng bảng điều khiển Kaspersky Anti Targeted Attack Platform, bao gồm hoạt động chạy các tác vụ, quản lý các đối tượng được cách ly, xem báo cáo và các hành động khác.

Thiết lập Endpoint Detection and Response Expert (on-premises)

Tham số	Mô tả
Connection to telemetry collection servers	*Máy chủ thu thập đo từ xa* là một máy chủ thuộc giải pháp SIEM, có chức năng thu thập, chuẩn hóa, tương quan, phân tích và lưu trữ thông tin về các sự kiện xảy ra trên máy tính. Cấu hình như sau để kết nối với máy chủ thu thập dữ liệu đo từ xa (KUMA): • **Timeout (sec)**. Thời gian chờ phản hồi tối đa của máy chủ. Khi hết thời gian chờ, Kaspersky Endpoint Security sẽ cố gắng kết nối với một máy chủ khác. • **Server certificate**. Chứng chỉ TLS để thiết lập kết nối được tin tưởng với máy chủ. Bạn có thể lấy chứng chỉ TLS trên Open Single Management Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Use two-way authentication**. Xác thực hai chiều khi thiết lập kết nối bảo mật giữa Kaspersky Endpoint Security và máy chủ. Để sử dụng xác thực hai chiều, bạn cần bật xác thực hai chiều trong thiết lập máy chủ, sau đó lấy bộ chứa mã hóa và đặt mật khẩu để bảo vệ bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể lấy container mã hóa trên Open Single Management Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises)). Sau khi cấu hình thiết lập máy chủ, bạn cũng cần bật xác thực hai chiều trong thiết lập của Kaspersky Endpoint Security và tải bộ chứa mã hóa được bảo vệ bằng mật khẩu. Bộ chứa mã hóa phải được bảo vệ bằng mật khẩu. Không thể thêm bộ chứa mã hóa có mật khẩu trống.
Address và **Port** (máy chủ thu thập dữ liệu đo từ xa)	Thiết lập để kết nối với máy chủ thu thập dữ liệu đo từ xa. Bạn có thể nhập địa chỉ IP (IPv4 hoặc IPv6). Bạn có thể thêm nhiều địa chỉ máy chủ thu thập đo từ xa. Kaspersky Endpoint Security sẽ cố gắng kết nối với máy chủ bằng địa chỉ IP đầu tiên. Nếu không thể thiết lập kết nối, Kaspersky Endpoint Security sẽ cố gắng kết nối bằng địa chỉ IP thứ hai trong danh sách, v.v.
Send telemetry to telemetry collection servers	Chức năng này cho phép bạn tắt hoàn toàn việc gửi đo lường từ xa đến máy chủ KATA. Ví dụ: nếu bạn đang sử dụng Kaspersky Anti Targeted Attack Platform cùng với một giải pháp khác cũng sử dụng phép đo lường từ xa, bạn có thể tắt gửi đo lường từ xa cho KATA (EDR). Điều này cho phép bạn tối ưu hóa mức tải máy chủ cho các giải pháp này. Nếu bạn đã triển khai giải pháp Managed Detection and Response và KATA (EDR) thì bạn có thể sử dụng đo lường từ xa MDR và tạo các tác vụ Phản hồi về mối đe dọa trong KATA (EDR). • **Send telemetry with IOA only**. Điều này cho phép tối ưu hóa dữ liệu đo từ xa và chỉ gửi dữ liệu đo từ xa có IOA. *Dấu hiệu tấn công (IOA)* là một quy tắc chứa mô tả về hành vi đáng ngờ trong hệ thống có thể cho biết một cuộc tấn công có chủ đích. Ứng dụng so sánh hành vi đang diễn ra trong hệ thống với các quy tắc này và ghi lại các sự kiện cho thấy có cuộc tấn công có chủ đích. Ứng dụng sử dụng công nghệ *quét luồng* cho phép theo dõi các sự kiện như vậy theo thời gian thực. • **Maximum event transmission delay (sec)**. Ứng dụng sẽ đồng bộ với máy chủ để gửi các sự kiện sau khi hết khoảng thời gian đồng bộ. Thiết lập mặc định là 30 giây. • **Limit the number of event packets per transmission**. Ứng dụng sẽ đồng bộ với máy chủ khi bộ đệm được lấp đầy bằng các sự kiện. Thiết lập mặc định là 1024 sự kiện. Chức năng này cho phép vô hiệu hóa lưu trữ tạm thời các sự kiện trước khi đồng bộ hóa với máy chủ.
Enable request throttling	Tính năng này giúp tối ưu hóa mức tải trên máy chủ. Nếu chức năng này được kích hoạt, ứng dụng sẽ hạn chế việc truyền sự kiện. Nếu số lượng sự kiện vượt quá giới hạn được cấu hình thì Kaspersky Endpoint Security sẽ ngừng gửi sự kiện. Cấu hình thiết lập đo từ xa: • **Maximum number of events per hour**. Ứng dụng sẽ phân tích luồng dữ liệu đo từ xa và hạn chế gửi sự kiện nếu luồng sự kiện vượt quá giới hạn số sự kiện mỗi giờ đã được cấu hình. Kaspersky Endpoint Security sẽ tiếp tục gửi sự kiện sau một giờ. Thiết lập mặc định là 3000 sự kiện mỗi giờ. Nếu ứng dụng được cài đặt trên máy chủ, luồng dữ liệu đo từ xa sẽ cao hơn. Đối với máy chủ, bạn nên tăng giá trị lên 60.000 sự kiện mỗi giờ. • **Percentage of event limit excess**. Ứng dụng sẽ sắp xếp sự kiện theo loại (ví dụ: sự kiện "thay đổi trong registry") và hạn chế truyền gửi sự kiện nếu tỷ lệ sự kiện cùng loại trên tổng số sự kiện vượt quá hạn mức được cấu hình theo tỷ lệ. Kaspersky Endpoint Security sẽ tiếp tục gửi sự kiện khi tỷ lệ của các sự kiện khác trên tổng số sự kiện trở lại đủ lớn. Thiết lập mặc định là 15%.
Send sync request to server every (min)	Tần suất yêu cầu đồng bộ được gửi đến máy chủ. Trong quá trình đồng bộ, Kaspersky Endpoint Security sẽ gửi thông tin về các thiết lập và tác vụ ứng dụng được sửa đổi.

Tham số	Mô tả
Connection to response servers	*Máy chủ phản hồi* là một máy chủ dùng để tiếp nhận và quét dữ liệu, nghiên cứu hành vi của các đối tượng và công bố kết quả của các nghiên cứu đó. Cấu hình như sau để kết nối máy chủ phản hồi: • **Timeout (sec)**. Thời gian chờ phản hồi tối đa của máy chủ. Khi hết thời gian chờ, Kaspersky Endpoint Security sẽ cố gắng kết nối với một máy chủ khác. • **Server certificate**. Chứng chỉ TLS để thiết lập kết nối được tin tưởng với máy chủ. Bạn có thể lấy chứng chỉ TLS trên Open Single Management Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Use two-way authentication**. Xác thực hai chiều khi thiết lập kết nối bảo mật giữa Kaspersky Endpoint Security và máy chủ. Để sử dụng xác thực hai chiều, bạn cần bật xác thực hai chiều trong thiết lập máy chủ, sau đó lấy bộ chứa mã hóa và đặt mật khẩu để bảo vệ bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể lấy container mã hóa trên Open Single Management Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises)). Sau khi cấu hình thiết lập máy chủ, bạn cũng cần bật xác thực hai chiều trong thiết lập của Kaspersky Endpoint Security và tải bộ chứa mã hóa được bảo vệ bằng mật khẩu.
Address và **Port** (máy chủ phản hồi)	Thiết lập để kết nối với máy chủ phản hồi. Bạn có thể nhập địa chỉ IP (IPv4 hoặc IPv6). Bạn có thể thêm nhiều địa chỉ máy chủ thu thập đo từ xa. Kaspersky Endpoint Security sẽ cố gắng kết nối với máy chủ bằng địa chỉ IP đầu tiên. Nếu không thể thiết lập kết nối, Kaspersky Endpoint Security sẽ cố gắng kết nối bằng địa chỉ IP thứ hai trong danh sách, v.v.

Thiết lập Endpoint Detection and Response (KATA)

Tham số	Mô tả
Send sync request to server every (min)	Tần suất yêu cầu đồng bộ được gửi đến máy chủ. Trong quá trình đồng bộ, Kaspersky Endpoint Security sẽ gửi thông tin về các thiết lập và tác vụ ứng dụng được sửa đổi.
Connection to KATA servers	Cấu hình như sau để kết nối máy chủ Central Node: • **Timeout (sec)**. Thời gian chờ phản hồi tối đa của máy chủ Central Node. Khi hết thời gian chờ, Kaspersky Endpoint Security sẽ cố gắng kết nối với một máy chủ Central Node khác. • **Server certificate**. Chứng chỉ TLS để thiết lập kết nối được tin tưởng với máy chủ Central Node. Bạn có thể lấy chứng chỉ TLS trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform). • **Use two-way authentication**. Xác thực hai chiều khi thiết lập kết nối bảo mật giữa Kaspersky Endpoint Security và máy chủ Central Node. Để sử dụng xác thực hai chiều, bạn cần bật xác thực hai chiều trong cài đặt máy chủ Central Node, sau đó lấy bộ chứa mã hóa và đặt mật khẩu để bảo vệ bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể nhận một bộ chứa mã hóa trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform). Sau khi cấu hình thiết lập Central Node, bạn cũng cần bật xác thực hai chiều trong thiết lập của Kaspersky Endpoint Security và tải bộ chứa mã hóa được bảo vệ bằng mật khẩu. Bộ chứa mã hóa phải được bảo vệ bằng mật khẩu. Không thể thêm bộ chứa mã hóa có mật khẩu trống.
Address và **Port** (máy chủ KATA)	Thiết lập kết nối với máy chủ Kaspersky Anti Targeted Attack Platform. Nhập địa chỉ IP (IPv4 hoặc IPv6) và cổng của máy chủ Central Node để kết nối. Bạn có thể thêm nhiều địa chỉ máy chủ Central Node. Kaspersky Endpoint Security sẽ cố gắng kết nối với máy chủ bằng địa chỉ IP đầu tiên. Nếu không thể thiết lập kết nối, Kaspersky Endpoint Security sẽ cố gắng kết nối bằng địa chỉ IP thứ hai trong danh sách, v.v.
Send telemetry to KATA	Chức năng này cho phép bạn tắt hoàn toàn việc gửi đo lường từ xa đến máy chủ KATA. Ví dụ: nếu bạn đang sử dụng Kaspersky Anti Targeted Attack Platform cùng với một giải pháp khác cũng sử dụng phép đo lường từ xa, bạn có thể tắt gửi đo lường từ xa cho KATA (EDR). Điều này cho phép bạn tối ưu hóa mức tải máy chủ cho các giải pháp này. Nếu bạn đã triển khai giải pháp Managed Detection and Response và KATA (EDR) thì bạn có thể sử dụng đo lường từ xa MDR và tạo các tác vụ Phản hồi về mối đe dọa trong KATA (EDR). Cấu hình thiết lập đo từ xa: • **Maximum event transmission delay (sec)**. Ứng dụng sẽ đồng bộ với máy chủ để gửi các sự kiện sau khi hết khoảng thời gian đồng bộ. Thiết lập mặc định là 30 giây. • **Maximum number of event packages**. Ứng dụng sẽ đồng bộ với máy chủ khi bộ đệm được lấp đầy bằng các sự kiện. Thiết lập mặc định là 1024 sự kiện.

Tham số	Mô tả
Enable request throttling	Tính năng này giúp tối ưu hóa mức tải trên máy chủ. Nếu chức năng này được kích hoạt, ứng dụng sẽ hạn chế việc truyền sự kiện. Nếu số lượng sự kiện vượt quá giới hạn được cấu hình thì Kaspersky Endpoint Security sẽ ngừng gửi sự kiện. Cấu hình thiết lập đo từ xa: • **Maximum number of events per hour**. Ứng dụng sẽ phân tích luồng dữ liệu đo từ xa và hạn chế gửi sự kiện nếu luồng sự kiện vượt quá giới hạn số sự kiện mỗi giờ đã được cấu hình. Kaspersky Endpoint Security sẽ tiếp tục gửi sự kiện sau một giờ. Thiết lập mặc định là 3000 sự kiện mỗi giờ. Nếu ứng dụng được cài đặt trên máy chủ, luồng dữ liệu đo từ xa sẽ cao hơn. Đối với máy chủ, bạn nên tăng giá trị lên 60.000 sự kiện mỗi giờ. • **Percentage of event limit excess**. Ứng dụng sẽ sắp xếp sự kiện theo loại (ví dụ: sự kiện "thay đổi trong registry") và hạn chế truyền gửi sự kiện nếu tỷ lệ sự kiện cùng loại trên tổng số sự kiện vượt quá hạn mức được cấu hình theo tỷ lệ. Kaspersky Endpoint Security sẽ tiếp tục gửi sự kiện khi tỷ lệ của các sự kiện khác trên tổng số sự kiện trở lại đủ lớn. Thiết lập mặc định là 15%.

Network Detection and Response (KATA)

Kaspersky Endpoint Security for Windows hỗ trợ làm việc với thành phần Kaspersky Network Detection and Response, thuộc giải pháp Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *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 ba đơn vị chức năng:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Bạn có thể mua tất cả các đơn vị chức năng hoặc mua riêng từng đơn vị chức năng. Để biết chi tiết về giải pháp này, vui lòng tham khảo Trợ giúp của Kaspersky Anti Targeted Attack Platform.

Kaspersky Endpoint Security 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 (dữ liệu đo từ xa) được gửi đến máy chủ của Kaspersky Anti Targeted Attack Platform. Trong trường hợp này, Kaspersky Endpoint Security cũng gửi thông tin đến máy chủ của Kaspersky Anti Targeted Attack Platform về các mối đe dọa được phát hiện bởi ứng dụng, bao gồm cả thông tin về kết quả xử lý các mối đe dọa này.

Việc tích hợp EDR (KATA) và NDR (KATA) được cấu hình trong bảng điều khiển Kaspersky Security Center. Tác nhân tích hợp sau đó được quản lý bằng bảng điều khiển Kaspersky Anti Targeted Attack Platform, bao gồm hoạt động chạy các tác vụ, quản lý các đối tượng được cách ly, xem báo cáo và các hành động khác.

Tham số	Mô tả
Thiết lập kết nối máy chủ	**Thời gian chờ (giây)**. Thời gian chờ phản hồi tối đa của máy chủ Central Node. Khi hết thời gian chờ, Kaspersky Endpoint Security sẽ cố gắng kết nối với một máy chủ Central Node khác. **Chứng chỉ TLS máy chủ**. Chứng chỉ TLS để thiết lập kết nối được tin tưởng với máy chủ Central Node. Bạn có thể lấy chứng chỉ TLS trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform). **Sử dụng xác thực hai chiều**. Xác thực hai chiều khi thiết lập kết nối bảo mật giữa Kaspersky Endpoint Security và máy chủ Central Node. Để sử dụng xác thực hai chiều, bạn cần bật xác thực hai chiều trong cài đặt máy chủ Central Node, sau đó lấy bộ chứa mã hóa và đặt mật khẩu để bảo vệ bộ chứa mã hóa. Một *bộ chứa mã hóa* là kho lưu trữ PFX có chứng chỉ và khóa riêng. Bạn có thể nhận một bộ chứa mã hóa trong bảng điều khiển Kaspersky Anti Targeted Attack Platform (xem hướng dẫn trong Trợ giúp của Kaspersky Anti Targeted Attack Platform). Sau khi cấu hình thiết lập Central Node, bạn cũng cần bật xác thực hai chiều trong thiết lập của Kaspersky Endpoint Security và tải bộ chứa mã hóa được bảo vệ bằng mật khẩu. Bộ chứa mã hóa phải được bảo vệ bằng mật khẩu. Không thể thêm bộ chứa mã hóa có mật khẩu trống.
Địa chỉ và **Cổng**	Thiết lập kết nối với máy chủ Kaspersky Anti Targeted Attack Platform. Nhập địa chỉ IP (IPv4 hoặc IPv6) và cổng của máy chủ Central Node để kết nối. Bạn có thể thêm nhiều địa chỉ máy chủ Central Node. Kaspersky Endpoint Security sẽ cố gắng kết nối với máy chủ bằng địa chỉ IP đầu tiên. Nếu không thể thiết lập kết nối, Kaspersky Endpoint Security sẽ cố gắng kết nối bằng địa chỉ IP thứ hai trong danh sách, v.v.
Gửi yêu cầu đồng bộ đến máy chủ NDR sau mỗi (phút)	Tần suất yêu cầu đồng bộ được gửi đến máy chủ. Trong quá trình đồng bộ, Kaspersky Endpoint Security sẽ gửi thông tin về các thiết lập và tác vụ ứng dụng được sửa đổi.
Độ trễ truyền gửi sự kiện tối đa (giây)	Ứng dụng sẽ đồng bộ với máy chủ để gửi các sự kiện sau khi hết khoảng thời gian đồng bộ. Thiết lập mặc định là 30 giây.
Cho phép làm nghẽn yêu cầu	Tính năng này giúp tối ưu hóa mức tải trên máy chủ. Nếu chức năng này được kích hoạt, ứng dụng sẽ hạn chế việc truyền sự kiện. Nếu số lượng sự kiện vượt quá giới hạn được cấu hình thì Kaspersky Endpoint Security sẽ ngừng gửi sự kiện.
Số lượng sự kiện tối đa mỗi giờ	Ứng dụng sẽ phân tích luồng dữ liệu đo từ xa và hạn chế gửi sự kiện nếu luồng sự kiện vượt quá giới hạn số sự kiện mỗi giờ đã được cấu hình. Kaspersky Endpoint Security sẽ tiếp tục gửi sự kiện sau một giờ. Thiết lập mặc định là 3000 sự kiện mỗi giờ. Nếu ứng dụng được cài đặt trên máy chủ, luồng dữ liệu đo từ xa sẽ cao hơn. Đối với máy chủ, bạn nên tăng giá trị lên 60.000 sự kiện mỗi giờ.
Tỷ lệ vượt quá hạn mức sự kiện	Ứng dụng sẽ sắp xếp sự kiện theo loại (ví dụ: sự kiện "thay đổi trong registry") và hạn chế truyền gửi sự kiện nếu tỷ lệ sự kiện cùng loại trên tổng số sự kiện vượt quá hạn mức được cấu hình theo tỷ lệ. Kaspersky Endpoint Security sẽ tiếp tục gửi sự kiện khi tỷ lệ của các sự kiện khác trên tổng số sự kiện trở lại đủ lớn. Thiết lập mặc định là 15%.

Tích hợp KUMA

Kaspersky Endpoint Security cho Windows hỗ trợ giải pháp Kaspersky Unified Monitoring and Analysis Platform. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* là giải pháp quản lý sự kiện và thông tin bảo mật (SIEM) dành cho hạ tầng CNTT của các tổ chức. KUMA cho phép phát hiện, phân tích và giảm thiểu các mối đe dọa bảo mật trước khi chúng có thể gây hại.

Tham số	Mô tả
Maximum delay when sending events (sec)	Ứng dụng sẽ đồng bộ với máy chủ để gửi các sự kiện sau khi hết khoảng thời gian đồng bộ. Thiết lập mặc định là 30 giây.
Connection to KUMA servers	**Timeout (sec)**. Thời gian tối đa để chờ phản hồi từ máy chủ KUMA (mặc định là 5 giây). Khi hết thời gian chờ, Kaspersky Endpoint Security sẽ cố gắng kết nối với một máy chủ KUMA khác. **Server certificate**. Chứng chỉ TLS để thiết lập kết nối được tin tưởng với máy chủ KUMA. Bạn có thể lấy chứng chỉ TLS trong bảng điều khiển Kaspersky Unified Monitoring and Analysis Platform (xem hướng dẫn trong phần Trợ giúp của Kaspersky Unified Monitoring and Analysis Platform). Để thiết lập kết nối được tin tưởng, trong bảng điều khiển KUMA, trong thiết lập bộ nối tcp, bạn phải chọn chế độ TLS **With verification** (xem thiết lập cho bộ nối loại tcp trong Trợ giúp của Kaspersky Unified Monitoring and Analysis Platform). **Use two-way authentication**. Xác thực hai chiều khi thiết lập kết nối bảo mật giữa KES và KUMA. Để sử dụng xác thực hai chiều, trong bảng điều khiển KUMA, trong thiết lập bộ nối, bạn phải chọn chế độ TLS **Custom PFX with client authentication** (xem thiết lập cho bộ nối trong phần Trợ giúp của Kaspersky Unified Monitoring and Analysis Platform). Sau đó, bạn phải tải xuống một chứng chỉ máy chủ và đặt mật khẩu để bảo vệ container mật mã. Bộ chứa mã hóa phải được bảo vệ bằng mật khẩu. Không thể thêm bộ chứa mã hóa có mật khẩu trống.
Máy chủ KUMA	Kết nối với thiết lập máy chủ Kaspersky Unified Monitoring and Analysis Platform. Bạn có thể nhập địa chỉ IP (IPv4 hoặc IPv6). Bạn có thể thêm nhiều địa chỉ máy chủ KUMA. Kaspersky Endpoint Security sẽ cố gắng kết nối với máy chủ bằng địa chỉ IP đầu tiên. Nếu không thể thiết lập kết nối, Kaspersky Endpoint Security sẽ cố gắng kết nối bằng địa chỉ IP thứ hai trong danh sách, v.v.

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

Kaspersky Disk Encryption không được hỗ trợ trên các máy tính chạy trên kiến trúc Arm.

Sau khi ổ cứng hệ thống đã được mã hóa, vào lần khởi động tiếp theo, người dùng sẽ phải hoàn tất xác thực sử dụng Authentication Agent trước khi ổ cứng có thể được truy cập và hệ điều hành có thể được nạp. Điều này đòi hỏi bạn nhập vào mật khẩu của token hoặc thẻ thông minh được kết nối đến máy tính, hoặc tên người dùng và mật khẩu của tài khoản Authentication Agent được tạo bởi quản trị viên mạng máy tính cục bộ sử dụng tác vụ *Quản lý tài khoản Authentication Agent*. Những tài khoản này đều dựa trên các tài khoản Microsoft Windows được người dùng sử dụng để đăng nhập vào hệ điều hành. Bạn 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 cơ sở hạ tầng của Kaspersky Next. 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.

Khi mã hóa ổ đĩa, BitLocker sẽ đặt bộ tải khởi động và các tập tin phụ khác vào system partition. Phân vùng này không được mã hóa. Hệ điều hành sẽ tự động tạo phân vùng hệ thống trong quá trình cài đặt Windows. Nếu ổ đĩa được phân vùng đầy đủ trước khi cài đặt Windows, hệ điều hành không thể tạo phân vùng hệ thống. Trong trường hợp này, khi bạn tiến hành mã hóa đĩa BitLocker, hệ điều hành sẽ nhắc bạn phân vùng lại đĩa và tạo một phân vùng hệ thống. Sau khi tạo phân vùng hệ thống, hệ điều hành sẽ tiến hành mã hóa BitLocker.

BitLocker cung cấp ổ lưu trữ an toàn các khóa truy cập bằng mô-đun nền tảng được tin tưởng. *Trusted Platform Module* (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 cứng hệ thống, người dùng cần thực hiện xác thực BitLocker để khởi động hệ điều hành. Sau khi xác thực, BitLocker sẽ cho phép người dùng đăng nhập. BitLocker không hỗ trợ công nghệ đăng nhập một lần (SSO).

Sau khi mã hóa ổ đĩa, BitLocker sẽ tạo khóa khôi phục. Kaspersky Endpoint Security sẽ gửi khóa khôi phục 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 khóa khôi phục và thông tin về mã hóa ổ đĩa đến Kaspersky Security Center.

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	**Mã hóa tất cả ổ đĩa cứng**. Nếu chọn tùy chọn này, ứng dụng sẽ mã hóa tất cả các ổ cứng khi chính sách được áp dụng. 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. **Giải mã tất cả đĩa cứng**. Nếu chọn tùy chọn này, ứng dụng sẽ giải mã tất cả các ổ cứng đã được mã hóa từ trước khi chính sách được áp dụng. **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.
Tự động tạo các tài khoản Authentication Agent cho người dùng Windows 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.
Thiết lập tạo tài khoản Authentication Agent	**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.
Tự động tạo các tài khoản Authentication Agent cho mọi người dùng của máy tính này sau khi đăng nhập	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 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 *Quản lý tài khoản Authentication Agent* cho máy tính có ổ đĩa đã được mã hóa.
Lưu tên người dùng đã nhập vào Authentication Agent	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.

Tham số	Mô tả
Chỉ mã hóa dung lượng ổ đĩa được sử dụng (giảm thời gian mã hóa)	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. Việc bật hoặc tắt tính năng **Chỉ mã hóa dung lượng ổ đĩa được sử dụng (giảm thời gian mã hóa)** 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. Theo mặc định, hộp kiểm này bị xóa.
Sử dụng Hỗ trợ USB chuẩn cũ (không khuyên dùng)	Hộp kiểm này bật hoặc tắt chức năng Legacy USB Support. *Hỗ trợ USB chuẩn cũ* **là** 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). Legacy USB Support không ảnh hưởng đến hỗ trợ cho các thiết bị USB sau khi hệ điều hành đã được khởi động. 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. Khi chức năng Legacy USB Support 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.
Thiết lập mật khẩu	Thiết lập độ mạnh của mật khẩu tài khoản 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.
Sử dụng công nghệ Single Sign-On (SSO)	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. 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. 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.
Chồng lên các nhà cung cấp dịch vụ thông tin xác thực bên thứ ba	Kaspersky Endpoint Security hỗ trợ nhà cung cấp thông tin xác thực bên thứ ba ADSelfService Plus. Khi làm việc với các nhà cung cấp dịch vụ thông tin xác thực bên thứ ba, Authentication Agent sẽ chặn mật khẩu trước khi hệ điều hành được nạp. Điều này có nghĩa là người dùng chỉ cần nhập mật khẩu một lần khi đăng nhập vào Windows. Sau khi đăng nhập vào Windows, người dùng có thể sử dụng các khả năng của nhà cung cấp dịch vụ thông tin xác thực bên thứ ba, ví dụ như để xác thực trong các dịch vụ của công ty. Các nhà cung cấp dịch vụ thông tin xác thực bên thứ ba cũng cho phép người dùng đặt lại mật khẩu của riêng họ một cách độc lập. Trong trường hợp này, Kaspersky Endpoint Security sẽ tự động cập nhật mật khẩu cho Authentication Agent. Nếu đang sử dụng nhà cung cấp dịch vụ thông tin xác thực bên thứ ba không được ứng dụng hỗ trợ, bạn có thể gặp một số hạn chế trong hoạt động công nghệ Đăng nhập một lần.
Trợ giúp	**Chứng thực**. Văn bản trợ giúp xuất hiện trong cửa sổ Authentication Agent khi nhập thông tin đăng nhập tài khoản. **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. **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.

Tham số	Mô tả
Chế độ mã hóa	**Mã hóa tất cả ổ đĩa cứng**. Nếu chọn tùy chọn này, ứng dụng sẽ mã hóa tất cả các ổ cứng khi chính sách được áp dụng. 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. **Giải mã tất cả đĩa cứng**. Nếu chọn tùy chọn này, ứng dụng sẽ giải mã tất cả các ổ cứng đã được mã hóa từ trước khi chính sách được áp dụng. **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.
Cần nhập liệu bàn phím trong quá trình tiền khởi động để bật xác thực BitLocker trên máy tính bảng	Sử dụng 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). 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. 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. Nếu hộp kiểm bị xóa thì BitLocker Drive Encryption không khả dụng trên máy tính bảng.
Sử dụng mã hóa phần cứng (Windows 8 và các phiên bản mới hơn)	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.
Chỉ mã hóa dung lượng ổ đĩa được sử dụng (Windows 8 và các phiên bản mới hơn)	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. Việc bật hoặc tắt tính năng **Chỉ mã hóa dung lượng ổ đĩa được sử dụng (giảm thời gian mã hóa)** 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. Theo mặc định, hộp kiểm này bị xóa.

Tham số	Mô tả
Phương thức xác thực	**Chỉ 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. **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). *Trusted Platform Module* (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: • **Sử dụng mã PIN cho TPM**. Nếu hộp kiểm này được chọn, người dùng có thể sử dụng 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. • **Mô-đun nền tảng tin tưởng (TPM), hoặc mật khẩu nếu TPM không khả dụng**. Nếu chọn tùy chọn này, 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. Phương thức xác thực đã chọn phải được cấu hình bằng cách chỉ định các yêu cầu về mật khẩu hoặc mã PIN: • **Độ dài tối thiểu của mã PIN (ký tự)** (giá trị mặc định là 6). • **Độ dài mật khẩu tối thiểu (ký tự)** (giá trị mặc định là 8). • **Số lượng tối đa mật khẩu / mã PIN được lưu trữ** (giá trị mặc định là 5). • **Giới hạn thời gian hiệu lực của mật khẩu/mã PIN cho TPM (ngày)** (bị tắt theo mặc định). • **Sử dụng mã PIN tăng cường (chứa chữ và số)**. *Mã PIN cải tiến* cho phép sử dụng các ký tự khác ngoài ký tự số: chữ cái La-tinh viết hoa và viết thường, ký tự đặc biệt và dấu cách. Bị tắt theo mặc định.
Tự động tạo lại khóa khôi phục (ngày)	Tự động cập nhật mật khẩu thành khôi phục quyền truy cập ổ đĩa được bảo vệ bằng BitLocker. Nếu hộp kiểm được chọn, hãy chỉ định khoảng thời gian hiệu lực của mật khẩu khóa khôi phục. Điều này giúp ngăn sử dụng lại mật khẩu khóa khôi phục.

Mã hóa mức độ tập tin

Mã hóa tập tin không được hỗ trợ trên các máy tính chạy trên kiến trúc Arm.

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.

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 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.

Thiết lập thành phần Mã hóa mức độ tập tin

Tham số	Mô tả
Chế độ mã hóa	**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. **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. **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.
Mã hóa	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: • **Các thư mục được xác định trước**. Kaspersky Endpoint Security cho phép bạn thêm các khu vực sau: **Tài liệu**. 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). • **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: 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 *Tập tin nén*. Bạn cũng có thể thêm phần mở rộng tập tin một cách thủ công.

Tham số	Mô tả
Giải mã	Thẻ này hiển thị quy tắc giải mã cho các tập tin được lưu trữ trên ổ đĩa nội bộ.
Quy tắc cho các ứng dụng	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.
Gói mã hóa	Yêu cầu đối với độ mạnh của mật khẩu cần được đáp ứng khi tạo các gói mã hóa.

Mã hóa ổ đĩa di động

Tính năng mã hóa ổ đĩa di động không được hỗ trợ trên máy tính chạy trên kiến trúc Arm.

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:

- Full Disk Encryption (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).

- File Level Encryption (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

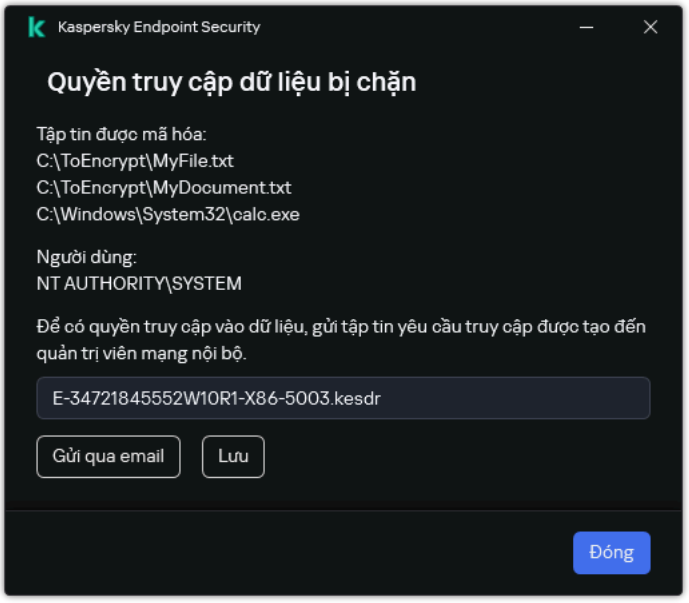
Tham số	Mô tả
Chế độ mã hóa	**Mã hóa toàn bộ ổ đĩa di động**. Nếu mục này được chọn, khi áp dụng chính sách với thiết lập mã hóa được chỉ định cho các ổ đĩa di động, Kaspersky Endpoint Security sẽ mã hóa ổ đĩa di động theo từng sector, bao gồm cả hệ thống tập tin của chúng. **Mã hóa tất cả các tập tin**. 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. **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. **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. **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.
Chế độ di động	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. 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. Chế độ di động khả dụng với chế độ **Mã hóa tất cả các tập tin** hoặc **Chỉ mã hóa các tập tin mới**.
Chỉ mã hóa dung lượng ổ đĩa được sử dụng	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. 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. 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. 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**. 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.

Quy tắc tùy chỉnh	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:
	• 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:
	  • Theo ID thiết bị (Hardware ID hay HWID)
	  • Theo kiểu thiết bị: Vendor ID (VID) và Product ID (PID)

Tham số	Mô tả
Cho phép mã hóa ổ đĩa di động ở chế độ ngoại tuyến	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. 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.
Thiết lập mật khẩu mã hóa / Trình quản lý tập tin 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:

- **Đến**. 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.
- **Thông điệp của người dùng**. 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.

Kể từ Kaspersky Endpoint Security 12.5 cho Windows, bạn có thể thêm đo lường từ xa EDR vào vùng tin tưởng. Điều này cho phép tối ưu hóa dữ liệu mà ứng dụng gửi đến máy chủ Đo lường từ xa cho giải pháp Kaspersky Anti Targeted Attack Platform (EDR).

Kể từ Kaspersky Endpoint Security 12.6 cho Windows, loại trừ quét và ứng dụng được tin tưởng được thêm vào khu vực tin tưởng. Các ứng dụng được tin tưởng và loại trừ quét được xác định trước giúp nhanh chóng cấu hình Kaspersky Endpoint Security trên máy chủ SQL, máy chủ Microsoft Exchange và System Center Configuration Manager. Điều này có nghĩa là bạn không cần thiết lập khu vực tin tưởng theo cách thủ công cho ứng dụng trên máy chủ.

Kể từ Kaspersky Endpoint Security 12.8 cho Windows, bạn có thể cài đặt ứng dụng ở chế độ Light Agent để bảo vệ môi trường ảo. Các loại trừ quét được định sẵn và các ứng dụng được tin tưởng có thể giúp bạn nhanh chóng cấu hình Kaspersky Endpoint Security trong các môi trường máy ảo Citrix và VMware.

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 pháp. Đây là các phần mềm có thể bị khai thác bởi bọn tội phạm để làm hỏng máy tính hoặc dữ liệu người dùng. Những ứng dụng như vậy không nhất thiết có mục đích xấu, nhưng có thể bị tin tặc lợi dụng. Để biết thông tin chi tiết về các ứng dụng hợp pháp mà kẻ xâm nhập có thể lợi dụng để xâm nhập máy tính hoặc dữ liệu người dùng, vui lòng truy cập trang web Bách khoa toàn thư của Kaspersky.

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 phần mềm độc hại*

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 giám sát 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. Sau khi một ứng dụng được thêm vào danh sách các ứng dụng được tin tưởng, Kaspersky Endpoint Security sẽ ngừng giám sát hoạt động của ứng dụng đó.

Sự khác nhau giữa loại trừ quét và ứng dụng được tin tưởng là đối với loại trừ, Kaspersky Endpoint Security sẽ không quét các tập tin, trong khi đối với ứng dụng được tin tưởng thì ứng dụng không kiểm soát các tiến trình được khởi chạy. Nếu một ứng dụng được tin tưởng tạo một tập tin độc hại trong thư mục không có trong loại trừ quét thì Kaspersky Endpoint Security sẽ phát hiện tập tin đó và loại bỏ mối đe dọa. Nếu thư mục đó được thêm vào loại trừ thì Kaspersky Endpoint Security sẽ bỏ qua tập tin này.

Ví dụ: nếu bạn coi các đối tượng được sử dụng bởi ứng dụng Microsoft Windows Notepad là các đối tượng an toàn, có nghĩa là bạn tin tưởng ứng dụng này thì bạn có thể thêm Microsoft Windows Notepad vào danh sách các ứng dụng được tin tưởng để các đối tượng được sử dụng bởi ứng dụng này sẽ không bị giám sát. Làm vậy sẽ tăng hiệu năng máy tính, điều này đặc biệt quan trọng khi sử dụng các ứng dụng máy chủ.

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.

Các ứng dụng được tin tưởng sẽ giúp tránh các sự cố tương thích giữa Kaspersky Endpoint Security và các ứng dụng khác (ví dụ: sự cố quét hai lần lưu lượng mạng của một máy tính bên thứ ba bởi Kaspersky Endpoint Security và bởi một ứng dụng chống virus khác).

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

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 cho máy tính.

- **Virus và sâu**

  Danh mục con: Virus và sâu (Viruses_and_Worms)

  Cấp độ nguy hiểm: 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 kịch bản* và *virus macro*.

  Virus có thể lây nhiễm cho các tập tin sử dụng nhiều kỹ thuật khác nhau. *Overwriting* 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. *Parasitic* virus sẽ sửa nội dung tập tin, để chúng vận hành toàn bộ hoặc một phần chức năng. *Companion* 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 Link*, *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	Name	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 tin nhanh	Chúng được phát tán qua các ứng dụng nhắn 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 Internet Relay Chats, 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 gẫu 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: • 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

  Cấp độ nguy hiểm: 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	Name	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: • **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 bảng 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: • 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	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. 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).
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 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). 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. 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.
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	Name	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	*Mã khai thác* 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". 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. 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.
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 Tán gẫu 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.
Spoofer	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 Spoofer 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

  Cấp độ nguy hiểm: 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 kẻ xâm nhập để gây tổn hại cho 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	Name	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 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 ngầm 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 ngầm 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 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.

- **Phần mềm hợp pháp có thể bị kẻ xâm nhập sử dụng làm hư hại máy tính của bạn hoặc dữ liệu cá nhân**

  Danh mục con: Các phần mềm hợp pháp có thể được sử dụng bởi kẻ xâm nhập để gây tổn hại cho 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	Name	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 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 ngầm 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 ngầm 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 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**

  Danh mục con: Các tập tin được đóng gói có thể gây hại.

  Cấp độ nguy hiểm: Trung bình.

  Tập tin được đóng gói bằng một trình đóng gói đặc biệt, dùng để đóng gói phần mềm độc hại: virus, sâu, Trojan. Kaspersky Endpoint Security sẽ quét mô-đun giải nén trong các tập nén SFX (tự động giải nén).

  Để ẩn phần mềm độc hại khỏi sự phát hiện của phần mềm diệt virus, tin tặc đóng gói phần mềm đó bằng các trình đóng gói đặc biệt. Chuyên gia của Kaspersky đã xác định các trình nén phổ biến nhất trong giới tin tặc.

- **Các đối tượng được đóng gói nhiều lớp**

  Danh mục con: Các tập tin được đóng gói có thể gây hại.

  Cấp độ nguy hiểm: Trung bình.

  Tập tin được đóng gói bằng một trình đóng gói đặc biệt, dùng để đóng gói phần mềm độc hại: virus, sâu, Trojan. Kaspersky Endpoint Security sẽ quét mô-đun giải nén trong các tập nén SFX (tự động giải nén).

  Để ẩn phần mềm độc hại khỏi sự phát hiện của phần mềm diệt virus, tin tặc đóng gói phần mềm đó bằng các trình đóng gói đặc biệt. Chuyên gia của Kaspersky đã xác định các trình nén phổ biến nhất trong giới tin tặc.

Loại trừ

Bảng này chứa thông tin về các mục loại trừ quét.

Bạn nên chỉ định đường dẫn tương đối thay vì đường dẫn tuyệt đối. Làm vậy cho phép loại trừ không chỉ các đối tượng hệ thống tập tin mà còn cả các đối tượng không có tập tin. Ví dụ: `*\Program Files (x86)\Folder\Subfolder.`

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 các thư mục con bên trong `Folder`, ngoại trừ chính `Folder`. Một đại diện phải có ít nhất một cấp 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 sử dụng mặt nạ ở bất kỳ đâu trong đường dẫn tập tin hoặc thư mục. Ví dụ: nếu bạn muốn phạm vi quét bao gồm thư mục Downloads cho tất cả tài khoản người dùng trên máy tính, hãy nhập tên đại diện `C:\Users\*\Downloads\`.

    Kaspersky Endpoint Security hỗ trợ các biến môi trường

    > Kaspersky Endpoint Security không hỗ trợ biến môi trường `%userprofile%` khi tạo một danh sách các loại trừ bằng 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.

- 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*`, ứng dụng sẽ loại trừ các đối tượng `Client-IRC`, `Client-P2P` và `Client-SMTP` khỏi quá trình quét.

> Kaspersky Endpoint Security ẩn danh sách loại trừ quét trong giao diện người dùng của ứng dụng nếu cấu hình loại trừ quét bị quản trị viên chặn trong bảng điều khiển (biểu tượng "ổ khóa đóng") và loại trừ quét cục bộ bị cấm (hộp kiểm **Cho phép sử dụng các loại trừ cục bộ** bị xóa).

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.

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 trong 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.

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.

> Kaspersky Endpoint Security ẩn danh sách tổng hợp các ứng dụng được tin tưởng trong giao diện người dùng của ứng dụng nếu cấu hình của các ứng dụng được tin tưởng bị quản trị viên chặn trong bảng điều khiển (biểu tượng "ổ khóa đóng") và các ứng dụng được tin tưởng cục bộ bị cấm (hộp kiểm **Cho phép sử dụng các ứng dụng được tin tưởng cục bộ** bị xóa).

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. Chức năng này cũng cho phép gộp danh sách trong hồ sơ chính sách. Để gộp danh sách, trong hồ sơ có mức độ ưu tiên cao nhất, hãy bật tính năng kế thừa thiết lập từ cấu hình có mức độ ưu tiên thấp hơn. Để biết thêm chi tiết về mức độ ưu tiên của hồ sơ chính sách, vui lòng tham khảo Trợ giúp của Kaspersky Security Center.
Cho phép sử dụng các loại trừ cục bộ / Cho phép sử dụng các ứng dụng được tin tưởng cục bộ *(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)*	*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. 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. 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.
Đo lường từ xa EDR (KATA) / NDR (KATA) *(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)*	Bảng này chứa thông tin về các loại trừ đo lường từ xa EDR.
Đo lường từ xa KUMA *(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)*	Danh sách các sự kiện sẽ được gửi đến Kaspersky Unified Monitoring and Analysis Platform (KUMA). Kaspersky Endpoint Security hoạt động ở các chế độ sau: • **Gửi tất cả các sự kiện**. Ở chế độ này, ứng dụng sẽ gửi tất cả các sự kiện từ nhật ký Windows, ngoại trừ các sự kiện được thêm vào quy tắc loại trừ. • **Chỉ gửi các sự kiện được chọn**. Ở chế độ này, ứng dụng chỉ gửi các sự kiện được thêm vào các quy tắc bao gồm.
Kho chứng chỉ hệ thống tin tưởng	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 **Tin tưởng**. 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.

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

Tham số	Mô tả
Khởi chạy ứng dụng khi máy tính khởi động (khuyên dùng)	Khi chọn tùy chọn này, Kaspersky Endpoint Security sẽ được khởi chạy sau khi hệ điều hành được nạp, để bảo vệ máy tính trong toàn phiên sử dụng. Khi xóa tùy chọn này, 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.
Sử dụng công nghệ Khử mã độc nâng cao (cần tài nguyên máy tính đáng kể)	Thông thường, Kaspersky Endpoint Security sẽ chấm dứt các phần mềm độc hại được phát hiện trước khi máy tính bị nhiễm. Công nghệ khử mã độc tiên tiến sẽ bảo vệ máy tính trước phần mềm độc hại đang hoạt động (đang bị nhiễm mã độc), do đó giảm thiểu nguy cơ mất dữ liệu và lây lan của mối đe dọa. Nếu công nghệ này được kích hoạt, khi phát hiện hoạt động độc hại, Kaspersky Endpoint Security sẽ hiển thị thông báo ở dạng cửa sổ bật lên. Trong thông báo này, Kaspersky Endpoint Security sẽ đề xuất người dùng tùy chọn thực hiện Khử mã độc nâng cao cho máy tính. Sau khi người dùng chấp thuận quy trình này, Kaspersky Endpoint Security sẽ vô hiệu hóa mối đe dọa rồi 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. 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. 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, bạn 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 phần mềm độc hại*. Sau đó bạn cần khởi chạy tác vụ *Quét phần mềm độc hại*.
Sử dụng Kaspersky Security Center như máy chủ proxy để kích hoạt *(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)*	Nếu chọn hộp kiểm này, ứng dụng sẽ sử dụng Máy chủ quản trị Kaspersky Security Center làm máy chủ proxy để kết nối với máy chủ kích hoạt. Đây là điều cần thiết khi bạn đang sử dụng mã kích hoạt để kích hoạt ứng dụng trong một phần mạng bị cô lập không có quyền truy cập internet. Nếu đang kích hoạt ứng dụng bằng tập tin khóa, thì bạn không cần truy cập internet.
Bật Tự bảo vệ	Nếu chức năng này được bật, 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.
Chặn quản lý các dịch vụ ứng dụng từ bên ngoài	Nếu chức năng này được bật, Kaspersky Endpoint Security sẽ không cho phép quản lý các dịch vụ của ứng dụng bằng các ứng dụng của bên thứ ba (chẳng hạn như CMD). Khi một nỗ lực quản lý các dịch vụ của ứng dụng được thực hiện bằng ứng dụng của bên thứ ba, 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). Bạn chỉ có thể cho phép quản lý từ bên ngoài các dịch vụ của ứng dụng trên các máy tính không hỗ trợ công nghệ AM-PPL hoặc trên các máy tính có công nghệ này bị tắt.

Tham số	Mô tả
Hoãn các tác vụ theo lịch trong khi đang sử dụng nguồn pin	Nếu chọn hộp kiểm này, chế độ tiết kiệm điện sẽ được kích hoạt khi máy tính hoạt động bằng pin. Kaspersky Endpoint Security sẽ tạm hoãn các tác vụ theo lịch. Bạn có thể bắt đầu các tác vụ quét và cập nhật một cách thủ công, nếu cần thiết. Khi chế độ tiết kiệm điện 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: • *Quét toàn bộ*. • *Quét khu vực quan trọng*. • *Quét tùy chỉnh*. • *Kiểm tra tính toàn vẹn của ứng dụng*. • *Quét IOC*. • *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* (chỉ áp dụng cho các bản vá) Ứng dụng chỉ bỏ qua các bản cập nhật cơ sở dữ liệu theo lịch khi máy tính xách tay đang chạy bằng pin và mức pin dưới 30% (giá trị mặc định). Bạn có thể thay đổi mức sạc pin tối thiểu bằng cách chỉnh sửa registry. Tại mức tối thiểu đó, ứng dụng bắt đầu bỏ qua các bản cập nhật cơ sở dữ liệu chống virus đã lên lịch. Trong tất cả các trường hợp khác, Kaspersky Endpoint Security sẽ cập nhật cơ sở dữ liệu theo lịch, bất kể máy tính xách tay đang cắm nguồn hay chạy bằng pin, hoặc ứng dụng có đang ở chế độ tiết kiệm pin hay không.
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 cấu hình để nhường tài nguyên cho các ứng dụng khác.
Hạn chế mức sử dụng CPU cho các tác vụ quét	Để tối ưu hóa hiệu năng của Kaspersky Endpoint Security, bạn có thể giới hạn mức sử dụng CPU thông qua tác vụ *Quét phần mềm độc hại*. Nếu chọn hộp kiểm này, mức tải trung bình trên tất cả các lõi CPU từ tác vụ *Quét phần mềm độc hại* đạt tới giá trị đã chỉ định. Theo mặc định, hộp kiểm này bị xóa.
Cho phép ghi tập tin kết xuất	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 *(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)*	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. Các trạng thái sau khả dụng *OK*, *Cảnh báo* và *Nghiêm trọng*.
Cài đặt các bản cập nhật nhưng không khởi động lại máy tính	Nâng cấp ứng dụng mà không cần khởi động lại máy tính cho phép bạn đảm bảo hoạt động của các máy chủ không bị gián đoạn. Bạn có thể nâng cấp ứng dụng mà không cần khởi động lại kể từ phiên bản 11.10.0. Bạn phải khởi động lại máy tính để nâng cấp phiên bản cũ hơn của ứng dụng. Kể từ phiên bản 11.11.0, bạn có thể thực hiện các tác vụ sau mà không cần khởi động lại máy tính: • cài đặt các bản vá lỗi • thay đổi nhóm thành phần ứng dụng • cài đặt Kaspersky Endpoint Security qua Máy chủ Kaspersky Security cho Windows Giá trị mặc định của tham số thay đổi tùy thuộc vào loại hệ điều hành. Nếu ứng dụng được cài đặt trên máy trạm, việc nâng cấp ứng dụng mà không có tùy chọn khởi động lại sẽ bị vô hiệu. Nếu ứng dụng được cài đặt trên máy chủ thì việc nâng cấp ứng dụng không có tùy chọn khởi động lại sẽ được bật.

Tham số	Mô tả
Khả năng tương thích với phần mềm quản trị từ xa *(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)*	Nếu việc sử dụng Kaspersky Endpoint Security cùng với Remote Administration Tools (RAT) gây ra sự cố, bạn có thể bật chế độ tương thích. Sự cố có thể liên quan đến khả năng không tương thích của RAT với chức năng Secure Desktop của ứng dụng. Mục đích của chức năng này là để xác nhận các hành động có khả năng làm giảm mức độ bảo mật của máy tính. Chức năng này cho phép ứng dụng hiển thị hộp thoại xác nhận riêng rẽ với các tiến trình khác. Chức năng này sử dụng các quyền nâng cao để bảo mật yêu cầu. Nhờ vậy, chỉ người dùng mới có thể xác nhận hành động chứ không phải phần mềm độc hại. Nếu chọn tùy chọn này, chế độ tương thích với RAT sẽ được bật. Ứng dụng sẽ hiển thị hộp thoại xác nhận không có chức năng này. Điều này có thể giảm mức độ bảo mật của máy tính. Bạn không nên bật chế độ tương thích nếu Kaspersky Endpoint Security không gây ra sự cố với RAT. Nếu xóa tùy chọn này, chế độ tương thích với RAT sẽ bị tắt. Theo mặc định, hộp kiểm này bị xóa. Ví dụ: Khi sử dụng trình duyệt ở chế độ RemoteApp, Kaspersky Endpoint Security có thể không hiển thị cửa sổ xác nhận khi truy cập một website có chứng chỉ không được tin tưởng vì RemoteApp không hỗ trợ chức năng Secure Desktop của ứng dụng. Điều này có thể khiến trình duyệt gặp tình trạng không phản hồi. Để trình duyệt hoạt động chính bình thường ở chế độ RemoteApp, bạn phải bật chế độ tương thích. Bạn cũng có thể thử bật chế độ tương thích nếu gặp sự cố với chức năng Secure Desktop khi sử dụng phần mềm bên thứ ba khác.

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.14.2\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 của các tập tin được lưu trữ trong thư mục `C:\ProgramData\Kaspersky Lab\KES.14.2\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 được tích hợp với các giải pháp của Kaspersky 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, Trợ giúp của Kaspersky Endpoint Detection and Response Expert, Trợ giúp của Kaspersky Anti Targeted Attack Platform và Trợ giúp của Kaspersky Endpoint Detection and Response Expert (on-premises).

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
Delete reports after (days)	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.
Limit the size of report file to (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.
Delete objects after (days)	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.
Limit the size of Backup to (MB)	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 1024 MB. Để tránh vượt quá kích thước lưu trữ 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.
Limit the size of Quarantine	Nếu hộp kiểm được chọn, kích thước tối đa của Khu vực cách ly sẽ bị giới hạn theo giá trị mặc định. Theo mặc định, kích cỡ tối đa là 1024 MB. Khi Khu vực cách ly đạt dung lượng tối đa, Kaspersky Endpoint Security sẽ gửi sự kiện *Không đủ không gian trống trong ổ lưu trữ của Khu vực cách ly* đến Kaspersky Security Center và phát 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.
Notify when the Quarantine storage reaches (%)	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.

Tham số	Mô tả
Truyền dữ liệu đến Máy chủ quản trị *(chỉ khả dụng trong Kaspersky Security Center)*	Các danh mục sự kiện trên các máy khách có thông tin phải được gửi đến Máy chủ quản trị. Bạn có thể tắt truyền một số dữ liệu để tối ưu hóa dung lượng đĩa trên Máy chủ quản trị. Ứng dụng sẽ gửi các sự kiện thuộc các danh mục sau: • **About Quarantine files**. Bạn có thể xem danh sách các tập tin được cách ly trong bảng điều khiển Kaspersky Security Center, trong thư mục **Advanced** → **Repositories** → **Quarantine**. Kaspersky Endpoint Security chỉ sử dụng Khu vực cách ly khi được tích hợp với các giải pháp của Kaspersky Detection and Response. • **About files in Backup**. Bạn có thể xem danh sách các tập tin trong Sao lưu trong bảng điều khiển Kaspersky Security Center, trong thư mục **Advanced** → **Repositories** → **Backup**. • **About unprocessed files**. Bạn có thể xem danh sách các tập tin chưa được xử lý trong Kaspersky Security Center, trong thư mục **Advanced** → **Repositories** → **Active threats**. • **About installed devices**. Bạn có thể xem danh sách các thiết bị được kết nối trong bảng điều khiển Kaspersky Security Center, trong thư mục **Advanced** → **Repositories** → **Hardware**. Danh sách các thiết bị cũng có trong thuộc tính máy tính và trong chính sách Kaspersky Endpoint Security cho Windows (phần **Kiểm soát thiết bị**). • **About started applications**. Bạn có thể xem danh sách các tập tin thực thi trong bảng điều khiển Kaspersky Security Center, trong thư mục **Advanced** → **Application management** → **Executable files**. Danh sách các tập tin thực thi cũng có trong phần thuộc tính máy tính. • **About file encryption errors**. Bạn có thể xem danh sách các tập tin trong Sao lưu trong bảng điều khiển Kaspersky Security Center, trong thư mục **Advanced** → **Data encryption and protection** → **Encryption events**. Danh sách lỗi cũng có trong phần thuộc tính máy tính. • **Report on Adaptive Anomaly Control rules state**. Bạn có thể xem báo cáo trong bảng điều khiển Kaspersky Security Center, trong nút **Administration Server** trên thẻ **Reports**. Báo cáo này cũng có trong thuộc tính chính sách Kaspersky Endpoint Security cho Windows (phần **Kiểm soát thích ứng sự cố**). • **Report on triggered Adaptive Anomaly Control rules**. Bạn có thể xem báo cáo trong bảng điều khiển Kaspersky Security Center, trong nút **Administration Server** trên thẻ **Reports**. Báo cáo này cũng có trong thuộc tính chính sách Kaspersky Endpoint Security cho Windows (phần **Kiểm soát thích ứng sự cố**). • **About a threat development chain**. Bạn có thể xem chi tiết phát hiện trong Bảng điều khiển web Kaspersky Security Center, trong phần **Monitoring** → **Alerts**. Thông tin về chuỗi phát triển mối đe dọa được sử dụng bởi các giải pháp của Kaspersky Endpoint Detection and Response.

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 cổng mạng và thiết lập quét kết nối được mã hóa.

Các tùy chọn mạng

Tham số	Mô tả
Hạn chế lưu lượng trên các kết nối tính phí lưu lượng	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. 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	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. 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.
Thiết lập Máy chủ Proxy	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. 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, ứng dụng sẽ sử dụng địa chỉ máy chủ proxy được đặt trong thiết lập của trình duyệt Microsoft Internet Explorer.
Bỏ qua máy chủ proxy đối với các địa chỉ cục bộ	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.

Tham số	Mô tả
Thiết lập xác thực máy chủ proxy	Để xác thực ứng dụng trên máy chủ proxy để truy cập internet, bạn phải nhập thông tin đăng nhập của người dùng. Kaspersky Endpoint Security hỗ trợ xác thực tự động trên máy chủ proxy. Nếu xác thực tự động không thành công, ứng dụng sẽ nhắc bạn nhập thông tin đăng nhập. **Không sử dụng xác thực**. **Xác thực NTLM**. Xác thực NTLM bằng tài khoản người dùng hiện tại (mặc định). **Xác thực NTLM bằng tên người dùng và mật khẩu**. Xác thực NTLM bằng thông tin đăng nhập được điền thủ công. **Tên người dùng và mật khẩu**. Xác thực bằng thông tin đăng nhập được điền thủ công. **Xác thực tự động**. **Xác thực Kerberos**. Xác thực Kerberos bằng tài khoản người dùng hiện tại. Để đảm bảo xác thực Kerberos hoạt động đúng khi sử dụng bản ghi CNAME cho địa chỉ máy chủ proxy, bạn phải đăng ký Tên chủ thể dịch vụ (SPN) cho mỗi bản ghi CNAME. **Xác thực Kerberos bằng tên người dùng và mật khẩu**. Xác thực Kerberos bằng thông tin đăng nhập được điền thủ công. Nếu chọn xác thực Kerberos, Kaspersky Endpoint Security có thể, tùy thuộc vào thiết lập máy chủ proxy, thực hiện xác thực bằng giao thức Kerberos hoặc NTLM.
Giám sát các cổng	**Giám sát tất cả các cổng mạng**. Trong chế độ giám sát cổng mạng này, các thành phần bảo vệ (Bảo vệ mối đe dọa tập tin, Bảo vệ mối đe dọa web và Bảo vệ mối đe dọa thư điện tử) sẽ giám sát dòng dữ liệu được truyền qua bất kỳ cổng mạng mở nào trên máy tính. **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. **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. **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.
Quét kết nối được mã hóa	Kaspersky Endpoint Security sẽ quét lưu lượng mạng mã hóa được truyền qua các giao thức sau: • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Kaspersky Endpoint Security hỗ trợ các chế độ quét kết nối được mã hóa sau: • **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 mối đe dọa web, 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. 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.

Tham số	Mô tả
Chứng chỉ gốc được tin tưởng	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.
Truy cập một tên miền bằng chứng chỉ không được tin tưởng	• **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 *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. • **Chặn**. 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.
Truy cập một miền có lỗi quét kết nối được mã hóa	• **Chặn**. Nếu một lỗi quét kết nối được mã hóa xảy ra, Kaspersky Endpoint Security sẽ chặn kết nối mạng. • **Cho phép và thêm miền vào loại trừ**. Nếu một lỗi quét kết nối được mã hóa xảy ra, 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**. 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	Nếu hộp kiểm này được chọn, ứng dụng sẽ giám sát và chặn các kết nối mạng được thiết lập qua giao thức SSL 2.0. Nếu hộp kiểm này bị xóa, ứng dụng sẽ không chặn các kết nối mạng được thiết lập qua giao thức SSL 2.0. Tuy nhiên, ứng dụng không giám sát lưu lượng mạng qua giao thức này.
Chặn các kết nối SSL 3.0	Nếu hộp kiểm này được chọn, ứng dụng sẽ chặn các kết nối mạng được thiết lập qua giao thức SSL 3.0. Nếu hộp kiểm này bị xóa, ứng dụng sẽ không chặn các kết nối mạng được thiết lập qua giao thức SSL 3.0. Ứng dụng sẽ giám sát lưu lượng mạng qua giao thức này. Mọi thành phần của ứng dụng đều hoạt động mà không có hạn chế.
Chặn các kết nối TLS 1.0	Nếu hộp kiểm này được chọn, ứng dụng sẽ chặn các kết nối mạng được thiết lập qua giao thức TLS 1.0. Nếu hộp kiểm này bị xóa, ứng dụng sẽ không chặn các kết nối mạng được thiết lập qua giao thức TLS 1.0. Ứng dụng sẽ giám sát lưu lượng mạng qua giao thức này. Mọi thành phần của ứng dụng đều hoạt động mà không có hạn chế.
Giải mã kết nối mã hóa với các website sử dụng chứng chỉ EV	Các chứng chỉ EV (Extended Validation Certificate) sẽ xác nhận tính xác thực của các trang web 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. Nếu hộp kiểm được chọn, ứng dụng sẽ giải mã và giám sát các kết nối được mã hóa với các website sử dụng chứng chỉ EV. Nếu hộp kiểm này không được chọn, ứng dụng 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.

Tham số	Mô tả
Cấu hình địa chỉ được tin tưởng	Tính năng này sử dụng danh sách địa chỉ web mà Kaspersky Endpoint Security không quét kết nối mạng. 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 mối đe dọa web, Bảo vệ mối đe dọa thư điện tử và Kiểm soát web đang hoạt động. 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. Kaspersky Endpoint Security không hỗ trợ biểu tượng `*` cho các địa chỉ IP. Bạn có thể chọn một dải địa chỉ IP bằng cách sử dụng mặt nạ mạng con (ví dụ: 198.51.100.0/24). Ví dụ: • `domain.com` – 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`). • `subdomain.domain.com` –bản ghi này bao gồm các địa chỉ sau: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Bản ghi không bao gồm tên miền `domain.com`. • `*.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`.
Cấu hình ứng dụng được tin tưởng	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 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.
Để quét kết nối được mã hóa trong các ứng dụng có kho chứng chỉ riêng, hãy sử dụng *(chỉ khả dụng trong giao diện Kaspersky Endpoint Security)*	Nếu hộp kiểm này được chọn, ứng dụng 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. 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, ứng dụng sẽ không quét lưu lượng được mã hóa trong trình duyệt Mozilla Firefox và ứng dụng thư điện tử Thunderbird. Ứng dụng sẽ 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. • **Kho chứng chỉ Windows (khuyên dùng)**. Chứng chỉ gốc của Kaspersky được thêm vào kho này trong quá trình cài đặt Kaspersky Endpoint Security. • **Kho chứng chỉ riêng**. 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
Tương tác với người dùng *(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)*	**Hiển thị giao diện giản lược**. 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 chỉ hiển thị các thông báo yêu cầu người dùng thao tác phía trên biểu tượng ứng dụng. **Hiển thị giao diện người dùng**. 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. **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. *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. **Không hiển thị giao diện người dùng**. 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.

Tham số	Mô tả
Access to local tasks	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. Nếu bỏ chọn hộp kiểm này, các tác vụ cục bộ sẽ bị ẩn trong giao diện ứng dụng. 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. 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.
View group tasks	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. Khi hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ hiển thị một danh sách tác vụ trống.
Manage group tasks	Nếu hộp kiểm được chọn, người dùng có thể khởi chạy và dừng các tác vụ nhóm được chỉ định trong bảng điều khiển 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 giản lược. 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 bảng điều khiển Kaspersky Security Center.
Cấu hình thông báo	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 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.
Cấu hình thông báo qua 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. Theo mặc định, Kaspersky Endpoint Security sẽ sử dụng thiết lập thông báo email từ Kaspersky Security Center. Để biết thêm chi tiết về thiết lập thông báo email, hãy tham khảo Trợ giúp Kaspersky Security Center. Nếu cần cấu hình thông báo email riêng lẻ, bạn có thể chỉnh sửa các thiết lập sau: • **Địa chỉ người gửi**. Địa chỉ email của người gửi. Bạn không nên sử dụng một địa chỉ không tồn tại. • **Máy chủ SMTP**. Một hoặc nhiều địa chỉ máy chủ email của tổ chức của bạn (ví dụ: `mail.company.com`). Bạn có thể nhập địa chỉ IP (IPv4 hoặc IPv6). Để xác thực người dùng trên máy chủ SMTP, hãy nhập thông tin đăng nhập của người gửi vào các trường tương ứng. Để kiểm tra thông báo qua email, bạn có thể gửi một thư kiểm tra. • **Địa chỉ người nhận**. Địa chỉ email của người nhận mà ứng dụng sẽ gửi thông báo. • **Chế độ gửi**. Chế độ gửi của thông báo email. Kaspersky Endpoint Security có thể gửi thư ngay lập tức khi một sự kiện xảy ra; cách khác, nó có thể tuân theo một lịch trình được cấu hình sẵn.
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 chống phần mềm độc hại 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	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. Sau khi bật Bảo vệ bằng mật khẩu, Kaspersky Endpoint Security sẽ nhắc bạn đặt một mật khẩu cho tài khoản KLAdmin.
Hỗ trợ người dùng / **Liên kết đến tài nguyên web** *(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)*	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.
Hỗ trợ người dùng / **Mô tả** *(chỉ khả dụng trong Bảng điều khiển Kaspersky Security Center)*	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 thiết lập ứng dụng theo khuyến nghị của Kaspersky bất kỳ lúc nào. Khi thiết lập được khôi phục, mức độ bảo mật **Khuyên 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.

Cập nhật chức năng (bao gồm việc cung cấp các bản cập nhật dấu hiệu diệt virus và bản cập nhật bộ mã) có thể không khả dụng trong ứng dụng ở Hoa Kỳ.

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.

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 lỗ hổng bảo mật trong Kaspersky Endpoint Security, bổ sung các chức năng mới, hoặc tăng cường các chức năng sẵn có.

Trong khi cập nhật, các mô-đun ứng dụng và cơ sở dữ liệu trên máy tính của bạn sẽ được so sánh với các phiên bản đã cập nhật tại nguồn cập nhật. Nếu cơ sở dữ liệu và các mô-đun ứng dụng hiện tại của bạn khác với các phiên bản cập nhật tương ứng, phần còn thiếu của bản cập nhật sẽ được cài đặt trên máy tính của bạn.

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.

Nếu ứng dụng đang hoạt động trong Chế độ Light Agent, cần có những cân nhắc đặc biệt đối với việc cập nhật cơ sở dữ liệu và mô-đun ứng dụng.

Thiết lập cập nhật mô-đun ứng dụng và cơ sở dữ liệu

Tham số	Mô tả
Lịch cập nhật cơ sở dữ liệu	**Tự động**. Trong chế độ này, ứng dụng 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. **Manually**. Chế độ chạy tác vụ cập nhật này cho phép bạn khởi chạy thủ công tác vụ cập nhật. **By schedule**. 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.
Run missed tasks	Nếu hộp kiểm này được chọn, Kaspersky Endpoint Security sẽ bắt đầu lại tác vụ bị bỏ qua ngay khi có thể. Có thể bỏ qua tác vụ, ví dụ như nếu máy tính bị tắt vào thời điểm bắt đầu tác vụ được lên lịch. Khi ứng dụng có cơ hội thực thi các tác vụ bị bỏ lỡ, ứng dụng sẽ chạy các tác vụ một cách ngẫu nhiên trong một khoảng thời gian nhất định để phân phối tải trên máy tính. Khi hộp kiểm này bị xóa, Kaspersky Endpoint Security sẽ không chạy các tác vụ bị bỏ qua. Thay vào đó, ứng dụng sẽ chạy tác vụ kế tiếp dựa theo lịch hiện tại.

Tham số	Mô tả
Nguồn cập nhật	*Nguồn cập nhật* là một tài nguyên chứa các bản cập nhật cơ sở dữ liệu và mô-đun ứng dụng của Kaspersky Endpoint Security. Nguồn cập nhật bao gồm máy chủ Kaspersky Security Center và Kaspersky, máyy chủ cập nhật của Kaspersky và các thư mục cục bộ hoặc thư mục mạng. Nếu máy chủ cập nhật của Kaspersky không khả dụng, Kaspersky Endpoint Security có thể sử dụng các tên miền thay thế để cập nhật cơ sở dữ liệu và các mô-đun phần mềm ứng dụng. Để biết thông tin chi tiết, hãy tham khảo Cơ sở tri thức Hỗ trợ kỹ thuật. 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 hồi gói cập nhật từ nguồn khả dụng đầu tiên. Theo mặc định, Kaspersky Endpoint Security sử dụng máy chủ Kaspersky Security Center làm nguồn cập nhật đầu tiên. Điều này giúp tiết kiệm lưu lượng khi cập nhật. Nếu một chính sách không được áp dụng cho máy tính, các máy chủ của Kaspersky sẽ được chọn làm nguồn cập nhật đầu tiên trong thiết lập của tác vụ cục bộ *Cập nhật cơ sở dữ liệu và mô-đun ứng dụng* vì ứng dụng có thể không có quyền truy cập vào máy chủ Kaspersky Security Center. Nếu ứng dụng đang chạy trong Chế độ Light Agent thì một thư mục trên SVM sẽ được chọn làm nguồn cập nhật.
Chạy cập nhật cơ sở dữ liệu với quyền	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 thiết lập ứng dụng, bạn có thể chỉ định một người dùng có các quyền đó và khởi chạy tác vụ cập nhật Kaspersky Endpoint Security theo tài khoản người dùng đó.
Tải xuống các bản cập nhật của mô-đun ứng dụng	Tải xuống các bản cập nhật mô-đun ứng dụng cùng các bản cập nhật cơ sở dữ liệu ứng dụng. 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: • **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. 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. 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. Hộp kiểm được chọn theo mặc định.
Sao chép các bản cập nhật vào thư mục	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.14.2\Update distribution\`.

Tham số	Mô tả
Máy chủ proxy cho các bản cập nhật *(chỉ khả dụng trong giao diện Kaspersky Endpoint Security)*	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. Để cấu hình tự động máy chủ proxy, Kaspersky Endpoint Security sử dụng giao thức WPAD (Web Proxy Auto-Discovery Protocol). 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.
Bỏ qua máy chủ proxy đối với các địa chỉ cục bộ *(chỉ khả dụng trong giao diện Kaspersky Endpoint Security)*	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.

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 nhóm *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 nhóm *Giới hạn mức 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 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 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 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

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, xlsm cho mẫu Microsoft Office Excel 2007 với hỗ trợ macro, và xlam cho tiện ích Microsoft Office Excel 2007 với hỗ trợ macro

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

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

sldx – một trang Microsoft PowerPoint 2007

sldm – một trang Microsoft PowerPoint 2007 với hỗ trợ macro

thmx – một chủ đề Microsoft Office 2007

Phụ lục 4. Các loại tập tin cho bộ lọc đính kèm Bảo vệ mối 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 tập tin đính kèm email, thành phần Bảo vệ mối 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

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, xlsm cho mẫu Microsoft Office Excel 2007 với hỗ trợ macro, và xlam cho tiện ích Microsoft Office Excel 2007 với hỗ trợ macro

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

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

sldx – một trang Microsoft PowerPoint 2007

sldm – một trang Microsoft PowerPoint 2007 với hỗ trợ macro

thmx – một chủ đề Microsoft Office 2007

Phụ lục 5. Thiết lập mạng 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 thiết lập mạng sau để tương tác với các dịch vụ bên ngoài.

Địa chỉ	Mô tả
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Giao thức: `HTTPS` Cổng: `443`	Kích hoạt ứng dụng.

Địa chỉ	Mô tả

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`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`
	Cập nhật cơ sở dữ liệu và các mô-đun phần mềm ứng dụng.

`downloads.upd.kaspersky.com` Giao thức: `HTTPS` Cổng: `443`	• Cập nhật cơ sở dữ liệu và các mô-đun phần mềm ứng dụng. • Xác minh quyền truy cập vào máy chủ Kaspersky. 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). 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.
`touch.kaspersky.com` Giao thức: `HTTP`	• Nhận thời gian được tin tưởng để kiểm tra thời hạn hiệu lực của chứng chỉ (kết nối TLS). • Cảnh báo về từ chối quyền truy cập vào tài nguyên web trong trình duyệt khi tính năng Bảo vệ mối đe dọa web đang chạy.

Địa chỉ	Mô tả

`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`
`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`
	Cập nhật cơ sở dữ liệu và các mô-đun phần mềm ứng dụng.

`ds.kaspersky.com`
`dc1.ksn.kaspersky-labs.com`
`dc1-file.ksn.kaspersky-labs.com`
`dc1-pp.ksn.kaspersky-labs.com`
`dc1-st.ksn.kaspersky-labs.com`
Giao thức: `HTTPS`
Cổng: `443`
	Sử dụng Kaspersky Security Network.

`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: `KSN`
Cổng: `443`, `1443`
	Sử dụng Kaspersky Security Network.

`click.kaspersky.com`
 	
`redirect.kaspersky.com`
Giao thức: `HTTPS`
Cổng: `443`
	Theo các liên kết trong giao diện.

Thiết lập, được sử dụng để mã hóa

Địa chỉ	Mô tả

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Giao thức: `HTTP`
Cổng: `80`
	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 phần mềm độc hại, 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` – *Info*, `2` – *Warning*, `3` – *Functional failure*, `4` – *Critical*.
- `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 for 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 được lưu trữ trên máy chủ trong bao lâu

Nghiêm trọng

Giấy phép đã hết hạn

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 cực kỳ lỗi thời

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)	✓

Chức năng tự động chạy 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 không 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)	✓

Ứng dụng đã thiết lập kết nối đến một website 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 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)	✓

Malicious object detected (local bases)

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 Chống công cụ mã hóa Phòng chống khai thác Quét phần mềm độc hại
ID sự kiện Windows	`302`
ID sự kiện Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND`
Tham số sự kiện	• `GNRL_EA_PARAM_1` là hash của đối tượng (SHA256). • `GNRL_EA_PARAM_2` là tên của đối tượng. Khi phát hiện mã hóa bên ngoài của các thư mục được chia sẻ, ứng dụng sẽ hiển thị đường dẫn đến tập tin đích. • `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 (`typei`). • `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 Kaspersky Private Security Network (`blacklist`): `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)	✓

Malicious object detected (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 Chống công cụ mã hóa Phòng chống khai thác Quét phần mềm độc hại
ID sự kiện Windows	`302`
ID sự kiện Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND_BY_KSN`
Tham số sự kiện	• `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 (`typei`). • `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 Kaspersky Private Security Network (`blacklist`): `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 Phát hiện hành vi Chống công cụ mã hóa Quét phần mềm độc hại
ID sự kiện Windows	`312`
ID sự kiện Kaspersky Security Center	`GNRL_EV_OBJECT_NOTCURED`
Tham số sự kiện	• `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 (`typei`). • `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 Kaspersky Private Security Network (`blacklist`): `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)	✓

Cannot be deleted

Trạng thái	ⓘ
Thành phần	Bảo vệ mối đe dọa tập tin Phòng chống xâm nhập máy chủ Phát hiện hành vi Chống công cụ mã hóa Quét phần mềm độc hại
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)	✓

Processing error

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 phần mềm độc hại
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)	✓

Process terminated

Trạng thái	ⓘ
Thành phần	Bảo vệ mối đe dọa tập tin Phòng chống xâm nhập máy chủ Phát hiện hành vi Quét phần mềm độc hại
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)	✓

Unable to terminate process

Trạng thái	ⓘ
Thành phần	Bảo vệ mối đe dọa tập tin Phòng chống xâm nhập máy chủ Phát hiện hành vi Quét phần mềm độc hại
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)	–

Dangerous link blocked

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	• 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 (typei). • 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 (blacklist): true hoặc false.
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Dangerous link opened

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	• 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 (typei). • 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 (blacklist): true hoặc false.
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Previously opened dangerous link detected

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	• 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 (typei). • 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 (blacklist): true hoặc false.

Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Process action blocked

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	• `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 tổng kiểm 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)	✓

AMSI request was blocked

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)	✓

Network activity blocked

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	• `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: `12B012B012B012B012B012B012B012B0`. • `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	• `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)	✓

Prohibited process was started before Kaspersky Endpoint Security startup

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)	✓

Access denied (local bases)

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	• 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)	✓

Access denied (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	• 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)	✓

Operation with the device prohibited

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	• 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)	✓

Network connection blocked

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)	✓

Thao tác với thiết bị sẽ bị cấm cho đến khi Kaspersky Endpoint Security được khởi động

Trạng thái	!
Thành phần	Kiểm soát thiết bị
ID sự kiện Windows	816
ID sự kiện Kaspersky Security Center	00000330
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Kết nối thiết bị sẽ bị cấm cho đến khi Kaspersky Endpoint Security được khởi động

Trạng thái	!
Thành phần	Kiểm soát thiết bị
ID sự kiện Windows	817
ID sự kiện Kaspersky Security Center	00000331
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Error updating component

Trạng thái	!
Thành phần	Cập nhật
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)	✓

Error distributing component updates

Trạng thái	!
Thành phần	Cập nhật
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)	–

Local update error

Trạng thái	!
Thành phần	Cập nhật
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)	–

Network update error

Trạng thái	!
Thành phần	Cập nhật
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)	–

Cannot start two tasks at the same time

Trạng thái	!
Thành phần	Cập nhật
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 minh cơ sở dữ liệu và mô-đun ứng dụng

Trạng thái	!
Thành phần	Cập nhật
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
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
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)	✓

Update completed successfully, update distribution failed

Trạng thái	!
Thành phần	Cập nhật
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)	–

Internal task error

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)	–

Patch installation failed

Trạng thái	!
Thành phần	Cập nhật
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)	✓

Patch rollback failed

Trạng thái	!
Thành phần	Cập nhật
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)	✓

Error applying file encryption / decryption rules

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)	✓

File encryption / decryption error

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	• 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)	✓

File access blocked

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	• 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 cho phép 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)	✓

Error disabling portable mode

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)	✓

Error creating encrypted package

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)	✓

Error encrypting / decrypting device

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)	✓

Could not load encryption module

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)	✓

The task for managing Authentication Agent accounts ended with an error

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)	✓

Policy cannot be applied

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)	✓

FDE upgrade failed

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)	✓

FDE upgrade rollback failed (for more information, please refer to the Kaspersky Endpoint Security for Windows Online Help)

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)	✓

Kaspersky Anti Targeted Attack Platform server unavailable

Trạng thái	⚠
Thành phần	Endpoint Sensor
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)	✓

Failed to delete object

Trạng thái	⚠
Thành phần	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)	✓

Object not quarantined (Sandbox)

Trạng thái	⚠
Thành phần	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)	✓

An internal error occurred

Trạng thái	⚠
Thành phần	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)	✓

Invalid Sandbox server certificate

Trạng thái	ⓘ
Thành phần	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)	✓

The Sandbox node is unavailable

Trạng thái	ⓘ
Thành phần	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)	✓

Failed to process the object in Sandbox

Trạng thái	ⓘ
Thành phần	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)	✓

Maximum load to Sandbox is exceeded

Trạng thái	ⓘ
Thành phần	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)	–

IOC found

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)	✓

Sandbox license verification failed

Trạng thái	!
Thành phần	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)	✓

Không thể gửi tác vụ quét đến Sandbox bởi người dùng

Trạng thái	!
Thành phần	Sandbox
ID sự kiện Windows	2623
ID sự kiện Kaspersky Security Center	00000a3e
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Lỗi khi tạo tác vụ Sandbox

Trạng thái	!
Thành phần	Sandbox
ID sự kiện Windows	2621
ID sự kiện Kaspersky Security Center	00000a3d
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Object startup blocked

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)	✓

Process startup blocked

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)	✓

Script execution blocked

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)	✓

Object not quarantined (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)	✓

Process startup is not blocked

Trạng thái	!
Thành phần	Endpoint Detection and Response
ID sự kiện Windows	2561
ID sự kiện Kaspersky Security Center	00000a01
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Object is not blocked

Trạng thái	!
Thành phần	Endpoint Detection and Response
ID sự kiện Windows	2562
ID sự kiện Kaspersky Security Center	00000a02
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Script execution is not blocked

Trạng thái	!
Thành phần	Endpoint Detection and Response

ID sự kiện Windows	2563
ID sự kiện Kaspersky Security Center	00000a03
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Error changing application components

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)	✓

There are patterns of a possible brute-force attack in the system

Trạng thái	ⓘ
Thành phần	Kiểm tra nhật ký
ID sự kiện Windows	2800
ID sự kiện Kaspersky Security Center	00000af0
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

There are patterns of a possible Windows Event Log abuse

Trạng thái	ⓘ
Thành phần	Kiểm tra nhật ký
ID sự kiện Windows	2801
ID sự kiện Kaspersky Security Center	00000af1
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Atypical actions detected on behalf of a new service installed

Trạng thái	ⓘ
Thành phần	Kiểm tra nhật ký
ID sự kiện Windows	2802
ID sự kiện Kaspersky Security Center	00000af2
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Atypical logon that uses explicit credentials detected

Trạng thái	ⓘ
Thành phần	Kiểm tra nhật ký

ID sự kiện Windows	2803
ID sự kiện Kaspersky Security Center	00000af3
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

There are patterns of a possible Kerberos forged PAC (MS14-068) attack in the system

Trạng thái	ⓘ
Thành phần	Kiểm tra nhật ký
ID sự kiện Windows	2804
ID sự kiện Kaspersky Security Center	00000af4
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Suspicious changes detected in the privileged built-in Administrators group

Trạng thái	ⓘ
Thành phần	Kiểm tra nhật ký
ID sự kiện Windows	2805
ID sự kiện Kaspersky Security Center	00000af5
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

There is an atypical activity detected during a network logon session

Trạng thái	ⓘ
Thành phần	Kiểm tra nhật ký
ID sự kiện Windows	2806
ID sự kiện Kaspersky Security Center	00000af6
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Log Inspection rule triggered

Trạng thái	ⓘ
Thành phần	Kiểm tra nhật ký
ID sự kiện Windows	2807
ID sự kiện Kaspersky Security Center	00000af7
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Atypical event occurs too often. Event aggregation started

Trạng thái	ⓘ
Thành phần	Kiểm tra nhật ký

ID sự kiện Windows	2808
ID sự kiện Kaspersky Security Center	00000af8
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Report on an atypical event for the aggregation period

Trạng thái	!
Thành phần	Kiểm tra nhật ký
ID sự kiện Windows	2809
ID sự kiện Kaspersky Security Center	00000af9
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Error connecting to the EDR Expert server

Trạng thái	!
Thành phần	Endpoint Detection and Response Expert (on-premises)
ID sự kiện Windows	2850
ID sự kiện Kaspersky Security Center	00000b22
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Invalid certificate of the EDR Expert server

Trạng thái	!
Thành phần	Endpoint Detection and Response Expert (on-premises)
ID sự kiện Windows	2851
ID sự kiện Kaspersky Security Center	00000b23
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Invalid certificate of the agent on the EDR Expert server

Trạng thái	!
Thành phần	Endpoint Detection and Response Expert (on-premises)
ID sự kiện Windows	2852
ID sự kiện Kaspersky Security Center	00000b24
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Lỗi kết nối với máy chủ phản hồi EDR Expert

Trạng thái	!
Thành phần	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)

ID sự kiện Windows	2858
ID sự kiện Kaspersky Security Center	00000b22
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Chứng chỉ không hợp lệ của máy chủ phản hồi EDR Expert

Trạng thái	ⓘ
Thành phần	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID sự kiện Windows	2859
ID sự kiện Kaspersky Security Center	00000b23
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Chứng chỉ không hợp lệ của tác nhân trên máy chủ phản hồi EDR Expert

Trạng thái	ⓘ
Thành phần	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID sự kiện Windows	2860
ID sự kiện Kaspersky Security Center	00000b24
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Lỗi kết nối máy chủ thu thập đo lường từ xa EDR Expert

Trạng thái	ⓘ
Thành phần	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID sự kiện Windows	2854
ID sự kiện Kaspersky Security Center	00000b22
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Chứng chỉ không hợp lệ của máy chủ thu thập đo lường từ xa EDR Expert

Trạng thái	ⓘ
Thành phần	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID sự kiện Windows	2855
ID sự kiện Kaspersky Security Center	00000b23
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Chứng chỉ không hợp lệ của tác nhân trên máy chủ thu thập đo lường từ xa EDR Expert

Trạng thái	⚠
Thành phần	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID sự kiện Windows	2856
ID sự kiện Kaspersky Security Center	00000b24
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Lỗi kết nối với máy chủ NDR

Trạng thái	⚠
Thành phần	Network Detection and Response (KATA)
ID sự kiện Windows	3080
ID sự kiện Kaspersky Security Center	00000c08
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Chứng chỉ không hợp lệ của máy chủ NDR

Trạng thái	⚠
Thành phần	Network Detection and Response (KATA)
ID sự kiện Windows	3081
ID sự kiện Kaspersky Security Center	00000c09
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Chứng chỉ không hợp lệ của tác nhân trên máy chủ NDR

Trạng thái	⚠
Thành phần	Network Detection and Response (KATA)
ID sự kiện Windows	3082
ID sự kiện Kaspersky Security Center	00000c0a
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Thiết bị của bạn được kết nối với Máy chủ quản trị không được tin tưởng. Hãy liên hệ với quản trị viên

Trạng thái	⚠
Thành phần	Bảo vệ kết nối Máy chủ quản trị
ID sự kiện Windows	3301
ID sự kiện Kaspersky Security Center	00000ce5
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

File or folder change was detected

Trạng thái	ⓘ / ⚠ / ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2950
ID sự kiện Kaspersky Security Center	00000b86
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Để cấu hình thời gian lưu giữ cho sự kiện này, hãy vào phần **Event configuration** của chính sách và đặt thời gian lưu giữ cho sự kiện Giám sát toàn vẹn hệ thống chung – *File or folder change was detected*.

Object changes too often. Event aggregation started

Trạng thái	ⓘ / ⚠ / ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2955
ID sự kiện Kaspersky Security Center	00000b8b
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Report on object modification for the aggregation period

Trạng thái	ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2953
ID sự kiện Kaspersky Security Center	00000b89
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Trạng thái	ⓘ / ⚠ / ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2956
ID sự kiện Kaspersky Security Center	00000b8c
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Để cấu hình thời gian lưu giữ cho sự kiện này, hãy vào phần **Event configuration** của chính sách và đặt thời gian lưu giữ cho sự kiện Giám sát toàn vẹn hệ thống chung – *File or folder change was detected*.

Registry change was detected

Trạng thái	ⓘ / ⚠ / ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2951
ID sự kiện Kaspersky Security Center	00000b87
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Để cấu hình thời gian lưu giữ cho sự kiện này, hãy vào phần **Event configuration** của chính sách và đặt thời gian lưu giữ cho sự kiện Giám sát toàn vẹn hệ thống chung – *File or folder change was detected*.

Device connection / disconnection is detected

Trạng thái	ⓘ / ⚠ / ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2952
ID sự kiện Kaspersky Security Center	00000b88
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Để cấu hình thời gian lưu giữ cho sự kiện này, hãy vào phần **Event configuration** của chính sách và đặt thời gian lưu giữ cho sự kiện Giám sát toàn vẹn hệ thống chung – *File or folder change was detected*.

Phạm vi giám sát bao gồm các đối tượng không đúng

Trạng thái	ⓘ / ⚠ / ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2903
ID sự kiện Kaspersky Security Center	00000b89
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Để cấu hình thời gian lưu giữ cho sự kiện này, hãy vào phần **Event configuration** của chính sách và đặt thời gian lưu giữ cho sự kiện Giám sát toàn vẹn hệ thống chung – *File or folder change was detected*.

Attempts to perform the restricted operations with the object is too many. Event aggregation started

Trạng thái	ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2963
ID sự kiện Kaspersky Security Center	00000b93
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

An operation with the files of the monitoring scope was blocked

Trạng thái	ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2959
ID sự kiện Kaspersky Security Center	00000b8f
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Để cấu hình thời gian lưu giữ cho sự kiện này, hãy vào phần **Event configuration** của chính sách và đặt thời gian lưu giữ cho sự kiện Giám sát toàn vẹn hệ thống chung – *File or folder change was detected*.

Registry modification blocked

Trạng thái	ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2960
ID sự kiện Kaspersky Security Center	00000b90
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Để cấu hình thời gian lưu giữ cho sự kiện này, hãy vào phần **Event configuration** của chính sách và đặt thời gian lưu giữ cho sự kiện Giám sát toàn vẹn hệ thống chung – *File or folder change was detected*.

Processing error

Trạng thái	ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2954
ID sự kiện Kaspersky Security Center	00000b8a
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

System Integrity Monitoring: rule triggering disabled for user accounts without matching security identifier (SID)

Trạng thái	ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2964
ID sự kiện Kaspersky Security Center	00000b94
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Application Control: rule triggering disabled for user accounts without matching security identifier (SID)

Trạng thái	!
Thành phần	Kiểm soát ứng dụng
ID sự kiện Windows	711
ID sự kiện Kaspersky Security Center	000002c7
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Device Control: rule triggering disabled for user accounts without matching security identifier (SID)

Trạng thái	!
Thành phần	Kiểm soát thiết bị
ID sự kiện Windows	810
ID sự kiện Kaspersky Security Center	0000032a
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Web Control: rule triggering disabled for user accounts without matching security identifier (SID)

Trạng thái	!
Thành phần	Kiểm soát Web
ID sự kiện Windows	757
ID sự kiện Kaspersky Security Center	000002f5
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Adaptive Anomaly Control: rule triggering disabled for user accounts without matching security identifier (SID)

Trạng thái	!
Thành phần	Kiểm soát thích ứng sự cố
ID sự kiện Windows	504
ID sự kiện Kaspersky Security Center	000001f8
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Log Inspection: rule triggering disabled for user accounts without matching security identifier (SID)

Trạng thái	!
Thành phần	Kiểm tra nhật ký
ID sự kiện Windows	2810
ID sự kiện Kaspersky Security Center	00000afa
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

SVM is unavailable

Trạng thái	!
Thành phần	Light Agent
ID sự kiện Windows	3151
ID sự kiện Kaspersky Security Center	00000c4f
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Malicious object detected. Advanced Disinfection should be started on a virtual machine template

Trạng thái	!
Thành phần	Light Agent
ID sự kiện Windows	3182
ID sự kiện Kaspersky Security Center	00000c6e
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Đã chặn kết nối mạng được thiết lập qua giao thức không còn được sử dụng nữa

Trạng thái	!
Thành phần	Bảo vệ
ID sự kiện Windows	75
ID sự kiện Kaspersky Security Center	0000004b
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Lỗi kết nối máy chủ KUMA

Trạng thái	!
Thành phần	Tích hợp KUMA
ID sự kiện Windows	2854
ID sự kiện Kaspersky Security Center	00000b26
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Chứng chỉ không hợp lệ của máy chủ KUMA

Trạng thái	!
Thành phần	Tích hợp KUMA
ID sự kiện Windows	2855
ID sự kiện Kaspersky Security Center	00000b27
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Chứng chỉ không hợp lệ của tác nhân trên máy chủ KUMA

Trạng thái	!
Thành phần	Tích hợp KUMA
ID sự kiện Windows	2856
ID sự kiện Kaspersky Security Center	00000b28
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

SIEM server connection error

Trạng thái	!
Thành phần	Tích hợp KUMA
ID sự kiện Windows	3250
ID sự kiện Kaspersky Security Center	00000cb2
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Invalid certificate of the SIEM server

Trạng thái	!
Thành phần	Tích hợp KUMA
ID sự kiện Windows	3251
ID sự kiện Kaspersky Security Center	00000cb3
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Invalid certificate of the agent on the SIEM server

Trạng thái	!
Thành phần	Tích hợp KUMA
ID sự kiện Windows	3252
ID sự kiện Kaspersky Security Center	00000cb4
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Lỗi chức năng

Task cannot be performed

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)	✓

Invalid task settings. Settings not applied

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

Application crashed during previous session

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)	–

License expires soon

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)	✓

Databases are out of date

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)	✓

Automatic updates are disabled

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)	✓

Self-Defense is disabled

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)	✓

Protection components are disabled

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)	✓

Computer is running in safe mode

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)	–

There are unprocessed files

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)	✓

Group policy applied

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)	✓

Task stopped

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)	✓

Quit and reopen the application to complete updating

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)	✓

Computer restart required

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)	✓

The license allows the use of components that have not been installed

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)	✓

Advanced Disinfection started

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)	✓

Advanced Disinfection completed

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)	✓

Incorrect reserve key

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)	✓

Subscription expires soon

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 Chống công cụ mã hóa Phòng chống khai thác Bảo vệ mối đe dọa web
ID sự kiện Windows	331

ID sự kiện Kaspersky Security Center	`GNRL_EV_OBJECT_BLOCKED`
Tham số sự kiện	• `GNRL_EA_PARAM_1` là hash của đối tượng (SHA256). • `GNRL_EA_PARAM_2` là tên của đối tượng. Khi phát hiện mã hóa bên ngoài của các thư mục được chia sẻ, ứng dụng sẽ hiển thị đường dẫn đến tập tin đích. • `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 (`type`). • `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 Kaspersky Private Security Network (`blacklist`): `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)	–

The operating system settings do not allow to control access to Wi-Fi networks

Trạng thái	⚠
Thành phần	Kiểm soát thiết bị
ID sự kiện Windows	249
ID sự kiện Kaspersky Security Center	000000f9
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	–

Object not restored from Backup

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)	–

Suspicious network activity detected

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)	✓

Encrypted connection terminated

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)	✓

Participation in KSN disabled

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)	✓

Processing of some OS functions is disabled

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)	✓

Quarantine storage is almost out of space

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)	✓

Network connection blocked

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)	✓

Cannot create a backup copy

Trạng thái	⚠
Thành phần	Bảo vệ mối đe dọa tập tin Phát hiện hành vi Chống công cụ mã hóa Phòng chống xâm nhập máy chủ Quét phần mềm độc hại
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)	✓

Object not processed

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 phần mềm độc hại
ID sự kiện Windows	`314`
ID sự kiện Kaspersky Security Center	`0000013a`
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Object encrypted

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)	–

Object corrupted

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 phần mềm độc hại
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)	–

Legitimate software that can be used by intruders to damage your computer or personal data was detected (local bases)

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 Chống công cụ mã hóa Chống công cụ mã hóa Quét phần mềm độc hại
ID sự kiện Windows	`303`
ID sự kiện Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND`
Tham số sự kiện	• `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 (`type`).
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Legitimate software that can be used by intruders to damage your computer or personal data was detected (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 Chống công cụ mã hóa Chống công cụ mã hóa Quét phần mềm độc hại
ID sự kiện Windows	`303`
ID sự kiện Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND_BY_KSN`
Tham số sự kiện	• `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 (`type`).
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Object deleted

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 Chống công cụ mã hóa Quét phần mềm độc hại

ID sự kiện Windows	307
ID sự kiện Kaspersky Security Center	GNRL_EV_OBJECT_DELETED
Tham số sự kiện	• 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 (type). • 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 Kaspersky Private Security Network (blacklist): 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)	✓

Object disinfected

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 phần mềm độc hại
ID sự kiện Windows	306
ID sự kiện Kaspersky Security Center	GNRL_EV_OBJECT_CURED
Tham số sự kiện	• 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 (type). • 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 Kaspersky Private Security Network (blacklist): 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)	✓

Object will be disinfected on restart

Trạng thái	⚠
Thành phần	Phòng chống xâm nhập máy chủ Bảo vệ mối đe dọa tập tin Quét phần mềm độc hại
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)	–

Object will be deleted on restart

Trạng thái	⚠
Thành phần	Phát hiện hành vi Chống công cụ mã hóa Phòng chống khai thác Phòng chống xâm nhập máy chủ Bảo vệ mối đe dọa tập tin Quét phần mềm độc hại
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)	–

Object deleted according to settings

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)	–

Rollback completed

Trạng thái	⚠
Thành phần	Bảo vệ mối đe dọa tập tin Phát hiện hành vi Chống công cụ mã hóa Phòng chống khai thác Quét phần mềm độc hại
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)	✓

Error removing the previous version of the application

Trạng thái	⚠
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	246
ID sự kiện Kaspersky Security Center	000000f6
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Object download was blocked

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	• 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 (type). • 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 Kaspersky Private Security Network (blacklist): 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)	✓

Keyboard authorization error

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)	✓

The object scan result has been sent to a third-party application

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	• 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 (type). • 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 Kaspersky Private Security Network (blacklist): 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)	✓

Task settings applied successfully

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)	✓

Warning about undesirable content (local bases)

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	• 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)	✓

Warning about undesirable content (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	• 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)	✓

Undesirable content was accessed after a warning

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)	–

Temporary access to the device activated

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)	–

Operation canceled by the user

Trạng thái	⚠
Thành phần	Cập nhật
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)	✓

User has opted out of the encryption policy

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)	✓

Interrupted applying file encryption / decryption rules

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)	–

File encryption / decryption interrupted

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)	–

Device encryption / decryption interrupted

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)	–

Failed to install or upgrade Kaspersky Disk Encryption drivers in the WinRE image

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)	✓

Module signature check failed

Trạng thái	⚠
Thành phần	Kiểm tra tính toàn vẹn của hệ thống
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)	✓

Application startup was blocked

Trạng thái	⚠
Thành phần	Endpoint Sensor
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)	✓

Document opening was blocked

Trạng thái	⚠
Thành phần	Endpoint Sensor
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)	✓

Process was terminated by the Kaspersky Anti Targeted Attack Platform server administrator

Trạng thái	⚠
Thành phần	Endpoint Sensor
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)	✓

The application was terminated by the Kaspersky Anti Targeted Attack Platform server administrator

Trạng thái	⚠
Thành phần	Endpoint Sensor
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)	✓

File or stream was deleted by the Kaspersky Anti Targeted Attack Platform server administrator

Trạng thái	⚠
Thành phần	Endpoint Sensor
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)	✓

File was restored from quarantine on the Kaspersky Anti Targeted Attack Platform server by the administrator

Trạng thái	⚠
Thành phần	Endpoint Sensor
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)	✓

File was quarantined on the Kaspersky Anti Targeted Attack Platform server by the administrator

Trạng thái	⚠
Thành phần	Endpoint Sensor
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)	✓

Network activity of all third-party applications is blocked

Trạng thái	⚠
Thành phần	Endpoint Sensor
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)	✓

Network activity of all third-party applications is unblocked

Trạng thái	⚠
Thành phần	Endpoint Sensor
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)	✓

Object will be deleted after restart (Sandbox)

Trạng thái	⚠
Thành phần	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)	✓

Total size of scan tasks exceeded the limit

Trạng thái	⚠
Thành phần	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)	✓

Object startup allowed, event logged

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)	✓

Process startup allowed, event logged

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)	✓

Object will be deleted after restart (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)	✓

Network isolation

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)	✓

Termination of network isolation

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)	✓

Restart required to complete the task

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)	✓

Connection to a website with an untrusted certificate is established by user decision

Trạng thái	⚠
Thành phần	Network Detection and Response (KATA)
ID sự kiện Windows	70

ID sự kiện Kaspersky Security Center	00000046
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	–

Application startup blockage message to administrator

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	• 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)	✓

Device access blockage message to administrator

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	• 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)	✓

Web page access blockage message to administrator

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	• 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)	✓

Device connection blocked

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	• 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)	✓

Application activity blockage message to administrator

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	• 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)	✓

Starting the cloud service client application is blocked

Trạng thái	⚠
Thành phần	Cloud Discovery
ID sự kiện Windows	2212
ID sự kiện Kaspersky Security Center	000008a4
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Access to the cloud service is blocked

Trạng thái	⚠
Thành phần	Cloud Discovery
ID sự kiện Windows	2213
ID sự kiện Kaspersky Security Center	000008a5
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

File or folder change was detected

Trạng thái	ⓘ / ⚠ / ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2950
ID sự kiện Kaspersky Security Center	00000b86
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Để cấu hình thời gian lưu giữ cho sự kiện này, hãy vào phần **Event configuration** của chính sách và đặt thời gian lưu giữ cho sự kiện Giám sát toàn vẹn hệ thống chung – *File or folder change was detected*.

Object changes too often. Event aggregation started

Trạng thái	ⓘ / ⚠ / ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2955
ID sự kiện Kaspersky Security Center	00000b8b
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Report on object modification for the aggregation period

Trạng thái	ⓘ / ⚠ / ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2956
ID sự kiện Kaspersky Security Center	00000b8c
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Để cấu hình thời gian lưu giữ cho sự kiện này, hãy vào phần **Event configuration** của chính sách và đặt thời gian lưu giữ cho sự kiện Giám sát toàn vẹn hệ thống chung – *File or folder change was detected*.

Registry change was detected

Trạng thái	ⓘ / ⚠ / ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2951
ID sự kiện Kaspersky Security Center	00000b87
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Để cấu hình thời gian lưu giữ cho sự kiện này, hãy vào phần **Event configuration** của chính sách và đặt thời gian lưu giữ cho sự kiện Giám sát toàn vẹn hệ thống chung – *File or folder change was detected*.

Device connection / disconnection is detected

Trạng thái	ⓘ / ⚠ / ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2952
ID sự kiện Kaspersky Security Center	00000b88
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Để cấu hình thời gian lưu giữ cho sự kiện này, hãy vào phần **Event configuration** của chính sách và đặt thời gian lưu giữ cho sự kiện Giám sát toàn vẹn hệ thống chung – *File or folder change was detected*.

Phạm vi giám sát bao gồm các đối tượng không đúng

Trạng thái	ⓘ / ⚠ / ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2903
ID sự kiện Kaspersky Security Center	00000b89
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Để cấu hình thời gian lưu giữ cho sự kiện này, hãy vào phần **Event configuration** của chính sách và đặt thời gian lưu giữ cho sự kiện Giám sát toàn vẹn hệ thống chung – *File or folder change was detected*.

The prohibited operation was allowed in test mode

Trạng thái	⚠
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2961
ID sự kiện Kaspersky Security Center	00000b91
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Không thể kết nối với Máy chủ tích hợp lâu hơn 30 phút. Hãy kiểm tra trạng thái Máy chủ tích hợp và thiết lập mạng

Trạng thái	⚠
Thành phần	Light Agent
ID sự kiện Windows	3102
ID sự kiện Kaspersky Security Center	00000c1e
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Unable to connect to the Integration Server for more than 6 hours. Check Integration Server status and network settings

Trạng thái	⚠
Thành phần	Light Agent
ID sự kiện Windows	3103
ID sự kiện Kaspersky Security Center	00000c1f
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Không thể kết nối với Máy chủ tích hợp. Hãy kiểm tra trạng thái Máy chủ tích hợp và thiết lập mạng

Trạng thái	⚠
Thành phần	Light Agent
ID sự kiện Windows	3101
ID sự kiện Kaspersky Security Center	00000c1d
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Cần cập nhật mẫu máy ảo

Trạng thái	⚠
Thành phần	Light Agent
ID sự kiện Windows	3181
ID sự kiện Kaspersky Security Center	00000c6d
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

The Standard license is terminated. The application is running under the Enterprise license

Trạng thái	⚠
Thành phần	Light Agent
ID sự kiện Windows	3171
ID sự kiện Kaspersky Security Center	00000c64
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Trạng thái	⚠
Thành phần	Giám sát tính toàn vẹn của tập tin
ID sự kiện Windows	2901
ID sự kiện Kaspersky Security Center	00000b55
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Trạng thái	⚠
Thành phần	Giám sát tính toàn vẹn của tập tin

ID sự kiện Windows	2900
ID sự kiện Kaspersky Security Center	00000b54
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Thông báo thông tin

Application started

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)	–

Application stopped

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)	–

Self-Defense restricted access to the protected resource

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)	✓

Report cleared

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)	✓

Group policy disabled

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)	–

Application settings changed

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)	–

Task started

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)	✓

Task completed

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)	✓

All application components that are defined by the license have been installed and run in normal mode

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)	–

Subscription settings have changed

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)	✓

Subscription has been renewed

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)	✓

Object restored from Backup

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)	✓

User name and password input

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)	–

Participation in KSN enabled

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)	✓

KSN servers available

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)	✓

The application works and processes data under relevant laws and uses the appropriate infrastructure

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)	✓

Object restored from Quarantine

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)	✓

Object deleted from Quarantine

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)	✓

A backup copy of the object was created

Trạng thái	ⓘ
Thành phần	Bảo vệ mối đe dọa tập tin Bảo vệ mối đe dọa thư điện tử Phát hiện hành vi Chống công cụ mã hóa Phòng chống xâm nhập máy chủ Sandbox Quét phần mềm độc hại
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)	✓

Overwritten by a copy that was disinfected earlier

Trạng thái	ⓘ
Thành phần	Bảo vệ mối đe dọa tập tin Phòng chống xâm nhập máy chủ Quét phần mềm độc hại
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)	–

Password-protected archive detected

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 phần mềm độc hại
ID sự kiện Windows	`322`
ID sự kiện Kaspersky Security Center	`GNRL_EV_PASSWD_ARCHIVE_FOUND`
Tham số sự kiện	• `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)	✓

Information about detected object

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 phần mềm độc hại
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)	✓

The object is in the Kaspersky Private Security Network allowlist

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 phần mềm độc hại
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)	✓

Object renamed

Trạng thái	ⓘ
Thành phần	Bảo vệ mối đe dọa thư điện tử Phòng chống khai thác Phát hiện hành vi Chống công cụ mã hóa Quét phần mềm độc hại
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)	✓

Object processed

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 phần mềm độc hại
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)	–

Object skipped

Trạng thái	ⓘ
Thành phần	Phòng chống xâm nhập máy chủ Bảo vệ mối đe dọa tập tin Bảo vệ AMSI Quét phần mềm độc hại
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)	–

Archive detected

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 phần mềm độc hại
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)	–

Packed object detected

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 phần mềm độc hại
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)	–

Link processed

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)	–

Application startup allowed

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)	–

Update source is selected

Trạng thái	ⓘ
Thành phần	Cập nhật
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
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)	–

The link is in the Kaspersky Private Security Network allowlist

Trạng thái	ⓘ
Thành phần	Bảo vệ mối 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)	✓

Application placed in the trusted group

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)	✓

Application placed in restricted group

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)	✓

Host Intrusion Prevention was triggered

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)	✓

File restored

Trạng thái	ⓘ
Thành phần	Phát hiện hành vi Chống công cụ mã hóa 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)	✓

Registry value restored

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)	–

Registry value deleted

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)	–

Process action skipped

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	• 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)	✓

Keyboard authorized

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)	✓

Network activity allowed

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)	–

Application startup prohibited in test mode

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	• 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)	✓

Application startup allowed in test mode

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	• 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)	–

A page that is allowed was opened

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)	–

Operation with the device allowed

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)	–

File operation performed

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	• 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)	–

No available updates

Trạng thái	ⓘ
Thành phần	Cập nhật
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)	–

Update distribution completed successfully

Trạng thái	ⓘ
Thành phần	Cập nhật
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)	–

Downloading files

Trạng thái	ⓘ
Thành phần	Cập nhật
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)	–

File downloaded

Trạng thái	ⓘ
Thành phần	Cập nhật
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)	–

File installed

Trạng thái	ⓘ
Thành phần	Cập nhật
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)	–

File updated

Trạng thái	ⓘ
Thành phần	Cập nhật
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)	–

File rolled back due to update error

Trạng thái	ⓘ
Thành phần	Cập nhật
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)	–

Updating files

Trạng thái	ⓘ
Thành phần	Cập nhật
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)	–

Distributing updates

Trạng thái	ⓘ
Thành phần	Cập nhật
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)	–

Rolling back files

Trạng thái	ⓘ
Thành phần	Cập nhật
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)	–

Creating the list of files to download

Trạng thái	ⓘ
Thành phần	Cập nhật
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)	–

Downloading patches

Trạng thái	ⓘ
Thành phần	Cập nhật
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)	–

Installing patch

Trạng thái	ⓘ
Thành phần	Cập nhật
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)	–

Patch installed

Trạng thái	ⓘ
Thành phần	Cập nhật
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)	–

Rolling back patch

Trạng thái	ⓘ
Thành phần	Cập nhật
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)	–

Patch rolled back

Trạng thái	ⓘ
Thành phần	Cập nhật
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)	–

Started applying file encryption / decryption rules

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)	✓

Finished applying file encryption / decryption rules

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)	✓

Resumed applying file encryption / decryption rules

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)	–

File encryption / decryption started

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)	–

File encryption / decryption completed

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)	–

File has not been encrypted because it is an exclusion

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)	–

Portable mode enabled

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)	–

Portable mode disabled

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)	–

Device encryption / decryption started

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)	–

Device encryption / decryption completed

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)	–

Device encryption / decryption resumed

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)	–

Device is not encrypted

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)	–

Device encryption / decryption process has been switched to active mode

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)	–

Device encryption / decryption process has been switched to passive mode

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)	–

Encryption module loaded

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)	–

New Authentication Agent account created

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)	–

Authentication Agent account deleted

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)	–

Authentication Agent account password changed

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)	–

Successful Authentication Agent login

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)	–

Failed Authentication Agent login attempt

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)	–

Hard drive accessed using the procedure of requesting access to encrypted devices

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)	–

Failed attempt to access the hard drive using the procedure of requesting access to encrypted devices

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)	–

Account was not added. This account already exists

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)	–

Account was not modified. This account does not exist

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)	–

Account was not deleted. This account does not exist

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)	–

FDE upgrade successful

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)	✓

FDE upgrade rollback successful

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)	✓

Failed to uninstall Kaspersky Disk Encryption drivers from the WinRE image

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)	✓

BitLocker recovery key was changed

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)	✓

BitLocker password / PIN was changed

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)	✓

BitLocker recovery key was saved to a removable drive

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)	✓

Processing of tasks from the Kaspersky Anti Targeted Attack Platform server is inactive

Trạng thái	ⓘ
Thành phần	Endpoint Sensor
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 connected to server

Trạng thái	ⓘ
Thành phần	Endpoint Sensor
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)	✓

Connection to the Kaspersky Anti Targeted Attack Platform server restored

Trạng thái	ⓘ
Thành phần	Endpoint Sensor
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)	✓

Tasks from the Kaspersky Anti Targeted Attack Platform server are being processed

Trạng thái	ⓘ
Thành phần	Endpoint Sensor
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)	✓

Object deleted

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)	–

Wipe task statistics

Trạng thái	ⓘ
Thành phần	Endpoint Detection and Response Expert (on-premises)
ID sự kiện Windows	2853
ID sự kiện Kaspersky Security Center	00000b25
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

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)	✓

Object quarantined (Sandbox)

Trạng thái	ⓘ
Thành phần	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)	✓

Object deleted (Sandbox)

Trạng thái	ⓘ
Thành phần	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)	–

IOC Scan started

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)	✓

IOC Scan completed

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)	✓

Object quarantined (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)	✓

Object deleted (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)	✓

Application components successfully changed

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	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	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	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	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)	–

Máy chủ quản trị mà thiết bị của bạn kết nối với được đặt là được tin tưởng

Trạng thái	ⓘ
Thành phần	Bảo vệ kết nối Máy chủ quản trị
ID sự kiện Windows	3300
ID sự kiện Kaspersky Security Center	00000ce4

Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Thiết bị của bạn được kết nối với Máy chủ quản trị được tin tưởng mới

Trạng thái	ⓘ
Thành phần	Bảo vệ kết nối Máy chủ quản trị
ID sự kiện Windows	3302
ID sự kiện Kaspersky Security Center	00000ce6
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Máy chủ quản trị mà thiết bị của bạn kết nối với không còn được đặt là được tin tưởng

Trạng thái	ⓘ
Thành phần	Bảo vệ kết nối Máy chủ quản trị
ID sự kiện Windows	3303
ID sự kiện Kaspersky Security Center	00000ce7
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Asynchronous Sandbox detection

Trạng thái	ⓘ
Thành phần	Sandbox
ID sự kiện Windows	2619
ID sự kiện Kaspersky Security Center	GNRL_EV_APP_INCIDENT_OCCURED
Tham số sự kiện	• GNRL_EA_PARAM_1 là tham số của các thành phần 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)	✓

The scan task has been successfully sent to Sandbox by a user

Trạng thái	ⓘ
Thành phần	Sandbox
ID sự kiện Windows	2622
ID sự kiện Kaspersky Security Center	00000a3e
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Device is connected

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	• 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)	✓

Device is disconnected

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	• 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)	✓

Successful connection to the EDR Expert server

Trạng thái	ⓘ
Thành phần	Endpoint Detection and Response Expert (on-premises)
ID sự kiện Windows	2853
ID sự kiện Kaspersky Security Center	00000b25
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Kết nối thành công với máy chủ phản hồi EDR Expert

Trạng thái	ⓘ
Thành phần	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID sự kiện Windows	2853
ID sự kiện Kaspersky Security Center	00000b25
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Kết nối thành công với máy chủ đo lường từ xa EDR Expert

Trạng thái	ⓘ
Thành phần	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID sự kiện Windows	2857
ID sự kiện Kaspersky Security Center	00000b26
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Kết nối thành công với máy chủ NDR

Trạng thái	ⓘ
Thành phần	Network Detection and Response (KATA)
ID sự kiện Windows	3083
ID sự kiện Kaspersky Security Center	00000c0b
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Starting the cloud service client application is allowed

Trạng thái	ⓘ
Thành phần	Cloud Discovery
ID sự kiện Windows	2210
ID sự kiện Kaspersky Security Center	000008a2
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Access to the cloud service is allowed

Trạng thái	ⓘ
Thành phần	Cloud Discovery
ID sự kiện Windows	2211
ID sự kiện Kaspersky Security Center	000008a3
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Truy cận khu vực được bảo vệ

Trạng thái	ⓘ
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	2004
ID sự kiện Kaspersky Security Center	000007d4
Nhật ký sự kiện của Windows (mặc định)	✓
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

File or folder change was detected

Trạng thái	ⓘ / ⚠ / ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2950
ID sự kiện Kaspersky Security Center	00000b86
Nhật ký sự kiện của Windows (mặc định)	–

Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Để cấu hình thời gian lưu giữ cho sự kiện này, hãy vào phần **Event configuration** của chính sách và đặt thời gian lưu giữ cho sự kiện Giám sát toàn vẹn hệ thống chung – *File or folder change was detected*.

Object changes too often. Event aggregation started

Trạng thái	ⓘ / ⚠ / ⓔ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2955
ID sự kiện Kaspersky Security Center	00000b8b
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Report on object modification for the aggregation period

Trạng thái	ⓘ / ⚠ / ⓔ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2956
ID sự kiện Kaspersky Security Center	00000b8c
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Để cấu hình thời gian lưu giữ cho sự kiện này, hãy vào phần **Event configuration** của chính sách và đặt thời gian lưu giữ cho sự kiện Giám sát toàn vẹn hệ thống chung – *File or folder change was detected*.

Registry change was detected

Trạng thái	ⓘ / ⚠ / ⓔ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2951
ID sự kiện Kaspersky Security Center	00000b87
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Để cấu hình thời gian lưu giữ cho sự kiện này, hãy vào phần **Event configuration** của chính sách và đặt thời gian lưu giữ cho sự kiện Giám sát toàn vẹn hệ thống chung – *File or folder change was detected*.

Device connection / disconnection is detected

Trạng thái	ⓘ / ⚠ / ⓔ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2952
ID sự kiện Kaspersky Security Center	00000b88

Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Để cấu hình thời gian lưu giữ cho sự kiện này, hãy vào phần **Event configuration** của chính sách và đặt thời gian lưu giữ cho sự kiện Giám sát toàn vẹn hệ thống chung – *File or folder change was detected*.

Phạm vi giám sát bao gồm các đối tượng không đúng

Trạng thái	ⓘ / ⚠ / ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2903
ID sự kiện Kaspersky Security Center	00000b89
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Để cấu hình thời gian lưu giữ cho sự kiện này, hãy vào phần **Event configuration** của chính sách và đặt thời gian lưu giữ cho sự kiện Giám sát toàn vẹn hệ thống chung – *File or folder change was detected*.

Baseline created

Trạng thái	ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2957
ID sự kiện Kaspersky Security Center	00000b8d
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Baseline updated

Trạng thái	ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2958
ID sự kiện Kaspersky Security Center	00000b8e
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

An operation is performed by the trusted user

Trạng thái	ⓘ
Thành phần	Giám sát tính toàn vẹn của hệ thống
ID sự kiện Windows	2962
ID sự kiện Kaspersky Security Center	00000b92
Nhật ký sự kiện của Windows (mặc định)	–

Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Để cấu hình thời gian lưu giữ cho sự kiện này, hãy vào phần **Event configuration** của chính sách và đặt thời gian lưu giữ cho sự kiện Giám sát toàn vẹn hệ thống chung – *File or folder change was detected*.

Connected to SVM

Trạng thái	ⓘ
Thành phần	Light Agent
ID sự kiện Windows	3152
ID sự kiện Kaspersky Security Center	00000c50
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

A new temporary password was created

Trạng thái	ⓘ
Thành phần	Kiểm toán hệ thống
ID sự kiện Windows	265
ID sự kiện Kaspersky Security Center	00000109
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Connected to the Integration Server

Trạng thái	ⓘ
Thành phần	Light Agent
ID sự kiện Windows	3105
ID sự kiện Kaspersky Security Center	00000c21
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Restoring connection to the Integration Server

Trạng thái	ⓘ
Thành phần	Light Agent
ID sự kiện Windows	3104
ID sự kiện Kaspersky Security Center	00000c20
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Kết nối thành công với máy chủ KUMA

Trạng thái	ⓘ
Thành phần	Tích hợp KUMA

ID sự kiện Windows	2857
ID sự kiện Kaspersky Security Center	00000b29
Nhật ký sự kiện của Windows (mặc định)	–
Nhật ký sự kiện của Kaspersky Security Center (mặc định)	✓

Phụ lục 7. 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

Tên ứng dụng	Tập tin thực thi	Phần mở rộng tập tin
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 8. Trình thông dịch tập lệnh được hỗ trợ để Phòng chống thực thi

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
- msiexec.exe
- perl.exe

- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.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 9. Phạm vi quét IOC trong registry (RegistryItem)

Khi bạn thêm loại **Windows registry - RegistryItem** vào phạm vi quét IOC, Kaspersky Endpoint Security sẽ quét các khóa registry sau theo mặc định:

```
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\Aedebug

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

Phụ lục 10. 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.
- Sau khi tải lên các tập tin IOC, bạn có thể chỉnh sửa thủ công các tập tin đó trong trình chỉnh sửa tích hợp trực tiếp trong thuộc tính tác vụ. Kaspersky Endpoint Security hỗ trợ chỉnh sửa các tập tin IOC tuân thủ tiêu chuẩn OpenIOC 1.1. Không thể chỉnh sửa nội dung của các tập tin IOC tuân thủ phiên bản OpenIOC 1.0.
- Nếu khi tạo một tác vụ *IOC Scan* 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 *IOC Scan* 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 *IOC Scan*.

- Bạn nên tạo một tập tin IOC cho mỗi mối đe dọa. Điều này giúp cho việc phân tích kết quả của tác vụ *IOC Scan* 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`
	
	Đối với các thuật ngữ Email/*, chỉ có điều kiện `contains` và `is` được hỗ trợ. Để tác vụ Quét IOC hồi cứu hoạt động đúng, khi sử dụng điều kiện `is`, địa chỉ email trong các tập tin IOC phải được chỉ định theo định dạng sau: `"name@example.org" <SMTP:name@example.org>`. Khi chạy tác vụ *Quét IOC* thông thường, chỉ cần ghi rõ địa chỉ email theo định dạng sau là đủ: `name@example.org`.

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"`: xâu 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 xâu 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 chỉ báo được thiết lập theo định dạng `ISO 8601, Zulu time zone, UTC`.

Phụ lục 11. API cho EDR Threat Response

Kaspersky Endpoint Security 12.9 cho Windows ra mắt hỗ trợ cho các hành động EDR Threat Response (EDR responses) bằng cách sử dụng Kaspersky Security Center OpenAPI. Tức là bạn có thể gọi các phương thức của OpenAPI để tự động phản hồi mối đe dọa EDR bằng Python. Bạn có thể gọi những phương thức này khi tích hợp với các giải pháp SIEM. *Kaspersky Unified Monitoring and Analysis Platform*, giải pháp Kaspersky SIEM, hỗ trợ OpenAPI của EDR Threat Response kể từ phiên bản 3.4.1. Để biết ví dụ về tập lệnh, vui lòng tham khảo tài liệu KUMA.

Để thực hiện các hành động EDR Threat Response, bạn cần tạo một yêu cầu và gửi bằng cách sử dụng KSC Open API (`AddIncident`). Sau khi yêu cầu được xử lý, một tác vụ đặc biệt sẽ được tạo trong bảng điều khiển Kaspersky Security Center.

Để tạo tác vụ khi ứng phó với các mối đe dọa EDR, bạn phải thiết lập kết nối nền giữa Máy chủ quản trị và Bảng điều khiển web Kaspersky Security Center. Dịch vụ kết nối nền có sẵn trong Kaspersky Security Center Windows 14.2 trở lên và trong Kaspersky Security Center Linux 15.2 trở lên. Các bảng điều khiển khác, bao gồm bảng điều khiển của giải pháp Kaspersky Detection and Response, đều không được hỗ trợ.

Đối với EDR Threat Response, bạn cần chỉ định các tham số yêu cầu cơ bản, ví dụ như ở định dạng JSON:

- `task` là loại tác vụ (xem bên dưới).
- `targetHost` là ID của máy tính mà tập lệnh phải được chạy. Đối số bắt buộc. Tập lệnh lấy tham số này từ sự kiện.
- `responseEventIncidentArea` là tên của ứng dụng đã chạy tập lệnh (ví dụ: `KUMA`). Tham số này được thêm vào tên của tác vụ đã tạo.

Để cấu hình EDR Threat Response, bạn cần chỉ định thiết lập tác vụ ở định dạng JSON trong tham số `"KLINCDT_BODY": json.dumps(data)`. Kết quả là, ứng dụng sẽ tạo ra `[Response][KUMA] <task type> - <Date> <Time> - <ID>` trong bảng điều khiển Kaspersky Security Center.

Kết nối với Kaspersky Security Center OpenAPI

Là một phần của EDR Threat Response, ứng dụng này sẽ tạo ra các tác vụ đặc biệt trong bảng điều khiển Kaspersky Security Center. Để tạo các tác vụ này, cần phải thiết lập kết nối giữa máy tính và Kaspersky Security Center. Để đạt được điều này, phải chỉ định các tham số kết nối Kaspersky Security Center trong yêu cầu.

> Trong Kaspersky XDR phiên bản 2.1, phương thức xác thực yêu cầu đã thay đổi. Kaspersky XDR sử dụng mã thông báo PAT thay vì xác thực bằng tên người dùng và mật khẩu. Do đó, không thể chạy tập lệnh trong Kaspersky XDR. Để biết thêm thông tin về việc xác thực yêu cầu, vui lòng tham khảo Trợ giúp của Kaspersky XDR.

Các tham số kết nối Kaspersky Security Center

Tham số	Loại	Mô tả
`kscHost`	`string`	Địa chỉ máy chủ quản trị của Kaspersky Security Center. Tham số bắt buộc.
`kscPort`	`int`	Cổng kết nối máy chủ quản trị. Tham số bắt buộc.
`kscCert`	`string`	Đường dẫn đến tập tin chứng chỉ để kết nối với Máy chủ quản trị Kaspersky Security Center. Theo mặc định, tham số được đặt thành `False`.
`kscUser`	`string`	Tên tài khoản người dùng. Tham số bắt buộc.
`kscPassword`	`string`	Mật khẩu tài khoản người dùng. Tham số bắt buộc.

Ví dụ

```
# KSC connection info
# reads Environment variables by default, change with corresponding values
# KSC host, string, required
kscHost = "kscHost"
# KSC port, required, default is "13299"
kscPort = "13299"
# KSC certificate file path, default is False
kscCert = False
# KSC user, string, required
kscUser = "kscUser"
# KSC password, string, required
kscPassword = "kscPassword"

server_url = 'https://' + kscHost + ':' + str(kscPort)
    server = KlAkAdmServer.Create(
        server_url, kscUser, kscPassword, verify=kscCert)

    params = validate(args)

    data = {"targetHost": <MyHost>,
            "task": task,
            "params": params,
            "responseEventIncident": True,
            "responseEventIncidentArea":"Kuma"}

    oHostGroup = KlAkHostGroup(server)

    incdnt = oHostGroup.AddIncident({"KLINCDT_SEVERITY": 2,
                                     "KLINCDT_ADDED": paramDateTime(datetime.datetime.now()),
                                     "KLINCDT_BODY": json.dumps(data),
                                     "KLHST_WKS_HOSTNAME":  args.targetHost}).RetVal()

    oHostGroup.UpdateIncident(incdnt, {"KLINCDT_IS_HANDLED": False,
                                       "KLHST_WKS_HOSTNAME":  args.targetHost})
```

Dữ liệu tài khoản người dùng không được bảo vệ, do đó bạn cần phải dành riêng một người dùng để thực hiện những hành động này.

Lấy tập tin – getFile

Thiết lập tác vụ Lấy tập tin

Tham số	Loại	Mô tả
md5hash	string	Giá trị hash MD5 của tập tin bạn muốn lấy.
sha256hash	string	Giá trị hash SHA256 của tập tin bạn muốn lấy.
path	string	Đường dẫn đến tập tin bạn muốn lấy.

Ví dụ

```
type getFile = {
  task: 'getFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

Xóa tập tin – deleteFile

Thiết lập tác vụ Xóa tập tin

Tham số	Loại	Mô tả
md5hash	string	Giá trị hash MD5 của tập tin bạn muốn xóa.
sha256hash	string	Giá trị hash SHA256 của tập tin bạn muốn xóa.
path	string	Đường dẫn đến tập tin bạn muốn xóa.
searchInSubfolders?	boolean	Tìm kiếm tập tin mà bạn muốn xóa trong các thư mục con.

Ví dụ

```
type deleteFile = {
  task: 'deleteFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // recursive search for a file (subfolder), optional
    searchInSubfolders?: boolean;
  };
  responseEventIncidentArea: string;
};
```

Di chuyển tập tin đến Khu vực cách ly – quarantineFile

Thiết lập tác vụ Di chuyển tập tin đến Khu vực cách ly

Tham số	Loại	Mô tả
`md5hash`	`string`	Giá trị hash MD5 của tập tin bạn muốn cách ly.
`sha256hash`	`string`	Giá trị hash SHA256 của tập tin bạn muốn cách ly.
`path`	`string`	Đường dẫn đến tập tin bạn muốn cách ly.

Ví dụ

```
type quarantineFile = {
  task: 'quarantineFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

Quét IOC – iocScan

Thiết lập tác vụ Quét IOC

Tham số	Loại	Mô tả
`ioc`	`string`	Đường dẫn đến tập tin nén ZIP chứa tập tin IOC mà bạn muốn sử dụng để quét.
`isolateHost`	`boolean`	Cô lập máy tính khỏi mạng khi phát hiện dấu hiệu xâm nhập để ngăn chặn mối đe dọa lây lan.
`scanCriticalAreas`	`boolean`	Chạy tác vụ *Quét khu vực quan trọng* khi phát hiện dấu hiệu xâm nhập.
`quarantineObject`	`boolean`	Xóa đối tượng độc hại khi phát hiện dấu hiệu xâm nhập. 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.

Ví dụ

```
type iocScan = {
  task: 'iocScan';
  targetHost: string;
  params: {
    // the path to the zip archive with ioc files in base64 encoding
    ioc: string;
    // isolation of the computer from the network
    isolateHost: boolean;
    // critical areas scan
    scanCriticalAreas: boolean;
    // quarantine the file
    quarantineObject: boolean;
  };
  responseEventIncidentArea: string;
};
```

Bắt đầu tiến trình – startProcess

Thiết lập tác vụ Bắt đầu tiến trình

Tham số	Loại	Mô tả
executablePath	string	Đường dẫn đến tập tin thực thi được sử dụng để khởi chạy tiến trình.
arguments?	string	Đối số dòng lệnh bổ sung để khởi chạy tiến trình.
workingFolder?	string	Đường dẫn đến thư mục làm việc của tiến trình.

Ví dụ

```
type startProcess = {
  task: 'startProcess';
  targetHost: string;
  params: {
    // the path to the file
    executablePath: string;
    // command line arguments, optional
    arguments?: string;
    // a working folder, optional
    workingFolder?: string;
  };
  responseEventIncidentArea: string;
};
```

Chấm dứt tiến trình – terminateProcess

Thiết lập tác vụ Chấm dứt tiến trình

Tham số	Loại	Mô tả
md5hash	string	Giá trị hash MD5 của tập tin mà bạn muốn chấm dứt tiến trình.
sha256hash	string	Giá trị hash SHA256 của tập tin mà bạn muốn chấm dứt tiến trình.
path	string	Đường dẫn đến tập tin bạn muốn xóa.
caseSensitive	boolean	Phân biệt chữ hoa chữ thường khi tìm kiếm tập tin.

Ví dụ

```
type terminateProcess = {
  task: 'terminateProcess';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Cách ly mạng máy tính – isolateHost

Thiết lập cách ly mạng máy tính

Tham số	Loại	Mô tả
`action`	`string`	Chế độ hoạt động của Cách ly mạng.

Ví dụ

```
type isolateHost = {
  task: 'isolateHost';
  targetHost: string;
  params: {
    // 0 - turning off network isolation, 1 - turning on network isolation
    action: number;
  };
  responseEventIncidentArea: string;
};
```

Phòng chống thực thi – preventExecution

Thiết lập Phòng chống thực thi

Tham số	Loại	Mô tả
`hash`	`string`	Giá trị hash MD5 của tập tin mà bạn muốn ngăn không cho chạy.
`path`	`string`	Đường dẫn đến tập tin mà bạn muốn ngăn không cho chạy.
`caseSensitive`	`boolean`	Phân biệt chữ hoa chữ thường khi tìm kiếm tập tin.

Ví dụ

```
type preventExecution = {
  task: 'preventExecution';
  targetHost: string;
  params: {
    // a valid md5 hash of the file
    hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Quét phần mềm độc hại – onDemandScan

Thiết lập tác vụ Quét phần mềm độc hại

Tham số	Loại	Mô tả
`path`	`string`	Danh sách các tập tin và thư mục được phân cách bằng dấu cách để Quét tùy chỉnh.
`recursive`	`boolean`	Chế độ quét đệ quy.

Tham số	Loại	Mô tả
type	`number`	Phạm vi quét.

```
ScanObjectType = Enum("ScanObjectType",
                      [
                          ("SystemMemory", 14),
                          ("StartupObjectsAndRunningProcesses", 15),
                          ("DiskBootSectors", 16),
                          ("SystemBackupStorage", 17),
                          ("Email", 18),
                          ("Folder", 22),
                          ("AllRemovableDrives", 23),
                          ("AllNetworkDrives", 24),
                          ("AllFixedDrives", 25)])
```

Ví dụ

```
type onDemandScan = {
  task: 'onDemandScan';
  targetHost: string;
  // please note, this is an array
  // array of scan object
  params: [{
    // enabling the scan object
    enabled: boolean;
    // an empty string or the path to the folder to scan
    path: string;
    // recursive scan mode
    recursive: boolean;
    // ID scan object
    type: number;
  }];
  responseEventIncidentArea: string;
};
```

Phụ lục 12. Tài khoản người dùng trong quy tắc thành phần ứng dụng

Để cấu hình một số thành phần ứng dụng, bạn phải thêm các quy tắc đặc biệt. Ví dụ: đối với Kiểm soát web, bạn phải thêm quy tắc có danh sách địa chỉ web mà bạn muốn ứng dụng chặn. Trong quy tắc thành phần ứng dụng, bạn cũng có thể cấu hình lịch cho thành phần đó hoặc chọn người dùng mà ứng dụng phải áp dụng quy tắc.

Các quy tắc phải được thêm vào để cấu hình các thành phần ứng dụng sau:

- Kiểm soát ứng dụng.
- Kiểm soát web.
- Kiểm soát thiết bị.
- Kiểm tra nhật ký.
- Kiểm soát thích ứng sự cố.
- Giám sát tính toàn vẹn của hệ thống.

Kể từ Kaspersky Endpoint Security cho Windows 12.5, bạn có thể chọn người dùng không chỉ từ Active Directory mà còn từ danh sách người dùng trong Kaspersky Security Center. Bạn cũng có thể nhập dữ liệu tài khoản người dùng cục bộ theo cách thủ công. Điều này có nghĩa là bạn có thể thêm người dùng theo những cách sau:

- Active Directory (khuyên dùng)
- Danh sách người dùng trong Kaspersky Security Center
- Tài khoản người dùng cục bộ

Để sử dụng đúng tất cả các phương pháp chọn người dùng, bạn cần cập nhật ứng dụng và tiện ích quản lý Kaspersky Endpoint Security lên phiên bản 12.5 trở lên.

Kaspersky khuyến nghị chỉ sử dụng tài khoản người dùng cục bộ trong những trường hợp đặc biệt khi không thể sử dụng tài khoản người dùng miền. Để biết chi tiết về các rủi ro bảo mật khi sử dụng tài khoản cục bộ, hãy xem Cơ sở tri thức của Microsoft. Bạn chịu hoàn toàn trách nhiệm về tính bảo mật của máy tính nếu tài khoản người dùng cục bộ được sử dụng; đặc biệt điều này bao gồm trách nhiệm kiểm soát và hạn chế quyền truy cập vào thiết lập của Kaspersky Endpoint Security.

Ứng dụng sử dụng SID (Định danh bảo mật) của người dùng để nhận dạng người dùng. Khi sử dụng tài khoản người dùng từ Active Directory hoặc từ danh sách người dùng Kaspersky Security Center, ứng dụng sẽ xác định SID trên Máy chủ quản trị. Điều này có nghĩa là ứng dụng sẽ không áp thêm mức tải lên máy tính để nhận dạng người dùng. Nếu bạn đã thêm hơn 1000 tài khoản người dùng cục bộ vào quy tắc ứng dụng, ứng dụng sẽ liên hệ với bộ điều khiển miền để xác định người dùng. Điều này có nghĩa là mức tải trên máy tính sẽ tăng lên. Để tối ưu hóa tác động đến hiệu năng trên máy tính, chúng tôi khuyên bạn nên sử dụng tài khoản người dùng từ Active Directory hoặc danh sách người dùng Kaspersky Security Center.

Ứng dụng sử dụng tên NetBIOS để xác định các tài khoản người dùng được thêm thủ công theo định dạng `<username>` và `<hostname>\<username>`. Tên NetBIOS có thể dài tới 16 byte (15 ký tự). Nếu tên máy tính dài hơn 15 ký tự, ứng dụng không thể xác định được người dùng. Sau đó, ứng dụng vô hiệu hóa quy tắc và tạo một lỗi, ví dụ: *Web Control: rule triggering disabled for user accounts without matching security identifier (SID)*. Để quy tắc này hoạt động, bạn phải rút ngắn tên máy tính theo cách thủ công. Bạn có thể thêm tài khoản người dùng từ Active Directory hoặc Kaspersky Security Center. Trong trường hợp này, ứng dụng sẽ tự động rút ngắn tên máy tính.

Kaspersky Endpoint Security cũng hỗ trợ người dùng và nhóm tích hợp (như nhóm "Tất cả") trong các quy tắc. Do cách xác định SID của người dùng nên ứng dụng chỉ cho phép sử dụng các tài khoản người dùng tích hợp được thêm từ Active Directory hoặc danh sách người dùng trong Kaspersky Security Center. Các quy tắc trong đó tài khoản người dùng tích hợp được thêm cục bộ sẽ không có hiệu lực.

Thông tin pháp lý

Cung cấp dữ liệu

Phần này chứa thông tin về dữ liệu mà ứng dụng Kaspersky Endpoint Security có thể lưu trữ trên thiết bị và tự động truyền tới Kaspersky trong quá trình hoạt động.

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.

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 yêu cầu duy nhất đến các dịch vụ của Đơn vị sở hữu bản quyền;
- 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 tại;
  - Khóa hiện hoạt;
  - Thời hạn giấy phép Kaspersky Endpoint Security;
  - Tình trạng hiện tại của giấy phép;
  - loại giấy phép hiện tại;
  - 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 tri 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 bổ 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 quãng, 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 dời, 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, Kaspersky Sandbox và Kaspersky Anti Targeted Attack Platform 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.

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 IOC Scan (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 truy vấn 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 IOC Scan (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 truy vấn HTTP

Kaspersky Endpoint Detection and Response Expert (on-premises)

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

Tác nhân tích hợp của Kaspersky Endpoint Security sẽ lưu trữ các dữ liệu sau cục bộ:

- Dữ liệu cần thiết để tích hợp với thành phần EDR Expert (on-premises):
  - Địa chỉ và cổng để kết nối với máy chủ KATA Central Node
  - Địa chỉ và cổng để kết nối với máy chủ truyền dữ liệu đo từ xa
  - Địa chỉ và cổng để kết nối với máy chủ phản hồi
  - Thông tin về các chứng chỉ được sử dụng để tích hợp với KATA Central Node
  - Thông tin về các chứng chỉ được sử dụng để tích hợp với máy chủ truyền dữ liệu đo từ xa
  - Thông tin về các chứng chỉ được sử dụng để tích hợp với máy chủ phản hồi
- Các tập tin được cách ly

Dữ liệu từ các sự kiện đo từ xa đã truyền gửi

- **Dữ liệu đo từ xa**
  - Dữ liệu trên các tập tin:
    - Định danh duy nhất của tập tin
    - Loại tập tin
    - Đường dẫn đến tập tin
    - Kích thước tập tin
    - Thuộc tính tập tin
    - Định danh vùng
    - Ngày và giờ tạo tập tin
    - Ngày và giờ sửa đổi tập tin lần cuối
    - Tên tập tin gốc
    - Tên ứng dụng
    - Phiên bản ứng dụng.
    - Nhà cung cấp ứng dụng
    - Mô tả tập tin
    - Phiên bản tập tin.
    - Giá trị băm MD5 và SHA256 của đối tượng
    - Kết quả xác minh mã nhận diện tập tin
    - Tên tổ chức cấp chứng chỉ
    - Tên người sở hữu chứng chỉ
    - Số sê-ri chứng chỉ
  - Thông tin về kết quả quét AMSI:
    - Định danh duy nhất của tiến trình đã khởi tạo hoạt động
    - Loại nội dung của đối tượng được truyền đến AMSI
    - Nội dung của đối tượng được truyền đến AMSI

    - Tên đối tượng
    - Giá trị băm MD5 và SHA256 của đối tượng
- Dữ liệu về việc chặn ứng dụng:
    - Định danh duy nhất của tiến trình đã khởi tạo chặn ứng dụng
    - Định danh duy nhất của tiến trình gốc
    - Định danh hệ thống duy nhất của tiến trình
    - Lệnh dùng để khởi chạy một tiến trình
    - ID phiên đăng nhập
    - Mức độ toàn vẹn của tiến trình
    - Trạng thái tiến trình
    - Định danh duy nhất của tập tin tiến trình
    - Xử lý dòng lệnh
    - Danh sách định danh duy nhất của các tập tin đã được thông dịch
- Dữ liệu về các lần mở tập tin bị chặn:
    - Định danh duy nhất của tiến trình đã khởi tạo mở tập tin
    - Định danh duy nhất của tập tin
- Dữ liệu về quá trình tải trình điều khiển:
    - Mã định danh duy nhất của trình điều khiển đã được tải
- Dữ liệu về các sự kiện:
    - Định danh duy nhất của sự kiện
    - Ngày và giờ của sự kiện
- Dữ liệu về việc sửa đổi tập tin:
    - Định danh duy nhất của tiến trình đã khởi tạo việc sửa đổi
    - Định danh duy nhất của tập tin
    - Loại thao tác sửa đổi
    - Cờ chỉ báo rằng tập tin sẽ bị xóa sau khi máy tính khởi động lại
    - Định danh duy nhất của tập tin được sửa đổi
    - Định danh duy nhất của tâp tin trước khi sửa đổi

    - Tập hợp các cờ bit xác định cách thức mở tập tin
    - Dữ liệu về các thao tác trên danh sách kiểm soát truy cập
    - Dữ liệu về những thay đổi về quyền sở hữu hoặc nhóm cha của tập tin
- Dữ liệu về phiên đăng nhập:
    - ID phiên đăng nhập
    - Tên của người dùng đã đăng nhập
    - Loại tài khoản người dùng
    - Loại phiên
- Dữ liệu về kết nối mạng:
    - Định danh duy nhất của tiến trình đã khởi tạo kết nối
    - Địa chỉ IP cục bộ được sử dụng để khởi tạo kết nối
    - Địa chỉ IP từ xa của điểm cuối kết nối
    - Hướng kết nối
    - Giao thức truyền dữ liệu
    - Phương thức HTTP
    - Đường dẫn không có tên máy chủ
    - Tên máy chủ
    - Trạng thái động của tiến trình tại thời điểm kết nối
    - Cờ chỉ báo rằng kết nối đang mở ở cấp độ socket thô
    - Phiên bản TLS được sử dụng trong phiên kết nối
    - Tên của máy chủ TLS
    - Giá trị hash MD5 và SHA1 của chứng chỉ máy chủ TLS
    - Danh sách các tên thay thế môn học (SAN) của chứng chỉ
    - Tên tổ chức cấp chứng chỉ TLS
    - Số sê-ri chứng chỉ
    - Thuật toán mã hóa được sử dụng
    - Ngày bắt đầu và ngày kết thúc của chứng chỉ

    - Dấu vân tay JA3 của trình khách TLS
    - Dấu vân tay JA3S của máy chủ
- Dữ liệu được thu thập trong khi nghe trên một cổng mạng:
    - Định danh duy nhất của tiến trình đã khởi tạo kết nối
- Dữ liệu đầu vào dòng lệnh:
    - Định danh duy nhất của tiến trình đã khởi tạo đầu vào bảng điều khiển
    - Loại đầu vào bảng điều khiển
    - Văn bản do người dùng hoặc tiến trình nhập vào
- Dữ liệu về việc tạo tiến trình:
    - Định danh duy nhất của tiến trình
    - Định danh duy nhất của tiến trình gốc
    - Định danh hệ thống duy nhất của tiến trình
    - Lệnh dùng để khởi chạy một tiến trình
    - ID phiên đăng nhập
    - Mức độ toàn vẹn của tiến trình
    - Định danh duy nhất của tập tin tiến trình
    - Danh sách định danh duy nhất của các tập tin đã được thông dịch
    - Loại tiến trình
- Dữ liệu về mô-đun được tiến trình nạp:
    - Định danh duy nhất của tiến trình đã khởi tạo tải xuống
    - Đường dẫn đầy đủ đến tập tin đã được tải lên tiến trình
    - Định danh duy nhất của tập tin mô-đun
    - Tên đầy đủ của tập tin assembly .NET, liệu tập tin được tải có phải là một mô-đun .NET
    - Các cờ của tập tin assembly .NET được định nghĩa trong tệp kê khai
- Dữ liệu về việc kết thúc tiến trình:
    - Định danh duy nhất của tiến trình bị chấm dứt

- Dữ liệu về việc sửa đổi registry:
  - Định danh duy nhất của tiến trình đã khởi tạo sửa đổi registry
  - Loại thao tác với registry
  - Đường dẫn đầy đủ đến khóa registry
  - Tên của giá trị bên trong khóa registry
  - Loại dữ liệu được lưu trữ trong giá trị khóa registry
  - Dữ liệu được chỉ định trong giá trị khóa registry
  - Tên của khóa trước khi đổi tên
  - Thông tin liên quan đến sự thay đổi quyền sở hữu của nhóm khóa hoặc khóa chính
  - Danh sách các thay đổi đối với danh sách kiểm soát truy cập (ACL) của khóa
- Dữ liệu về mối đe dọa được phát hiện và quá trình xử lý:
  - Cờ chỉ báo việc phát hiện mối đe dọa đã chạy trong nền
  - Phán quyết mối đe dọa
  - Tên phán quyết
  - Định danh duy nhất của bản ghi cơ sở dữ liệu
  - Thời điểm bản ghi mối đe dọa được lưu vào cơ sở dữ liệu
  - Chế độ xử lý mối đe dọa
  - Loại đối tượng bị lây nhiễm
  - Tên đối tượng bị lây nhiễm
  - Giá trị băm MD5 và SHA256 của đối tượng
  - Định danh duy nhất của đối tượng bị nhiễm
  - Định danh duy nhất của tiến trình đã tải xuống đối tượng bị nhiễm từ internet
  - URL tải xuống đối tượng bị nhiễm
  - Địa chỉ email người gửi đã gửi đối tượng bị lây nhiễm
  - Giao thức mạng nhận đối tượng bị nhiễm
  - Địa chỉ cục bộ nơi nhận đối tượng bị lây nhiễm
  - Địa chỉ bên ngoài nhận đối tượng bị lây nhiễm

    - Loại nội dung của đối tượng
    - Nội dung của đối tượng
- Dữ liệu về quyền truy cập vào các tiến trình:
    - Định danh duy nhất của tiến trình đã nỗ lực truy cập
    - Định danh duy nhất của tiến trình mục tiêu đã được truy cập
    - Tập hợp các quyền được yêu cầu từ tiến trình đích
    - Loại thao tác
    - Tập hợp các lệnh gọi tại thời điểm truy cập vào một tiến trình
    - Bộ mô tả tiến trình nguồn
    - Bộ mô tả tiến trình đích
- Dữ liệu về DNS:
    - Định danh duy nhất của tiến trình đã khởi tạo truy vấn DNS
    - Địa chỉ IP của máy chủ DNS
    - Các cờ quản lý hành vi của truy vấn DNS
    - Trạng thái hoàn thành yêu cầu
    - Tên miền đủ được chỉ định trong truy vấn DNS
    - Kiểu dữ liệu trong truy vấn DNS
    - Phản hồi từ máy chủ DNS
- Dữ liệu về việc chèn mã:
    - Định danh duy nhất của tiến trình đã cố gắng chèn mã
    - Phương thức truy cập đã sử dụng
    - Tập hợp các lệnh gọi tại thời điểm phát hiện mã được chèn
    - Định danh duy nhất của tiến trình đích có mã đã được tải lên
    - Dữ liệu về những thay đổi trong chuỗi lệnh của tiến trình đích
    - Địa chỉ tiến trình đích
    - Tên của thư viện DLL đã được tải lên tiến trình đích
    - Đường dẫn đầy đủ đến tập tin DDL

- Dữ liệu về các thao tác với các kênh được đặt tên:
  - Định danh duy nhất của tiến trình đã tạo hoặc kết nối với kênh
  - Tên đầy đủ của kênh được đặt tên
  - Loại thao tác (tạo hoặc kết nối)
- Dữ liệu về các truy vấn WMI:
  - Định danh duy nhất của tiến trình đã khởi tạo thao tác WMI
  - Loại thao tác WMI
  - Tên của thiết bị đích cho truy vấn WMI
  - Tài khoản người dùng đã khởi tạo truy vấn WMI
  - Nội dung của truy vấn WMI
  - Không gian tên nơi thực hiện truy vấn WMI
  - Tên bộ lọc WMI
  - Tên của đối tượng sử dụng
  - Văn bản mô tả hành động của đối tượng sử dụng
- Dữ liệu về các truy vấn LDAP:
  - Định danh duy nhất của tiến trình đã thực hiện truy vấn LDAP
  - Phạm vi tìm kiếm của các truy vấn LDAP
  - Bộ lọc LDAP
  - Tham số chỉ định phân vùng Active Directory mà truy vấn hướng đến
  - Thuộc tính tìm kiếm LDAP
- Dữ liệu về các thiết bị USB được kết nối:
  - Loại thao tác với thiết bị USB
  - Loại thiết bị USB
  - Định danh của thiết bị USB
  - Tên thiết bị USB
  - Đường dẫn đến thiết bị USB
  - Cờ chỉ báo thiết bị USB là ổ đĩa hệ thống
- Dữ liệu về việc tạo, xóa và sửa đổi tác vụ đã lên lịch

- Dữ liệu về việc tạo, xóa và sửa đổi dịch vụ
- Dữ liệu về việc gắn/tháo hệ thống tập tin
- Dữ liệu về hoạt động của thành phần EDR Expert on-premise:
  - Thông tin về việc khởi động/dừng tác nhân
  - Thông tin về việc cài đặt/gỡ cài đặt tác nhân
  - Định danh duy nhất cho khởi động tác nhân
  - Định danh hệ thống của tiến trình tác nhân
  - Định danh duy nhất của tiến trình tác nhân
  - Lý do chấm dứt tác nhân
  - Mã chấm dứt tiến trình tác nhân
- Thiết lập lọc sự kiện:
  - Các tên mô-đun
  - Đường dẫn đầy đủ đến các đối tượng
  - Giá trị băm MD5 và SHA256 của các đối tượng
  - Định danh của các mục trong nhật ký sự kiện Windows
  - Thiết lập chứng chỉ số
  - Hướng lưu lượng, địa chỉ IP, cổng, giao thức, đường dẫn đầy đủ đến tập tin thực thi
  - Các tên người dùng
  - Các kiểu đăng nhập người dùng
  - Các loại sự kiện đo lường từ xa được áp dụng bộ lọc

Dữ liệu từ các yêu cầu của thành phần EDR Expert tới tác nhân tích hợp của Kaspersky Endpoint Security

- Thiết lập tác vụ chung:
  - Loại tác vụ
  - Thiết lập lịch tác vụ
  - Tên và mật khẩu của các tài khoản thông qua đó các tác vụ có thể được chạy
  - Các phiên bản thiết lập

    - Định danh đối tượng được cách ly
    - Đường dẫn đến các đối tượng
    - Giá trị băm MD5 và SHA256 của các đối tượng
    - Dòng lệnh để khởi chạy tiến trình kèm các đối số
    - Các cờ của các hành động bổ sung được thực hiện sau khi hoàn thành tác vụ
    - Định danh tập tin IOC cần được truy xuất từ máy chủ
    - IOC files
    - Tên dịch vụ
    - Kiểu khởi chạy dịch vụ
    - Các thư mục phải nhận được các kết quả của tác vụ *Nhận pháp lý*
    - Tên đại diện của đối tượng và phần mở rộng cho tác vụ *Nhận pháp lý*
- Thiết lập cách ly mạng:
    - Các loại thiết lập
    - Các phiên bản thiết lập
    - Danh sách loại trừ cách ly mạng và thiết lập loại trừ: hướng lưu lượng, địa chỉ IP, cổng, giao thức và đường dẫn đầy đủ đến các tập tin thực thi
    - cờ của những hành động bổ sung
    - Thời gian vô hiệu cách ly tự động
- Thiết lập Phòng chống thực thi:
    - Các loại thiết lập
    - Các phiên bản thiết lập
    - Danh sách các quy tắc phòng chống thực thi và thiết lập quy tắc: đường dẫn đến đối tượng, loại đối tượng, giá trị băm MD5 và SHA256 của đối tượng
    - cờ của những hành động bổ sung

Dữ liệu từ các yêu cầu được Kaspersky Endpoint Security gửi đến thành phần EDR Expert

Khi tích hợp với giải pháp EDR Expert (on-premises), các dữ liệu sau được lưu trữ cục bộ trên máy tính.

- Trong các yêu cầu đồng bộ hóa:
  - ID duy nhất
  - Phần cơ bản của địa chỉ web máy chủ
  - Tên máy tính
  - Địa chỉ IP của máy tính
  - Địa chỉ MAC của máy tính
  - Giờ địa phương trên máy tính
  - Trạng thái tự bảo vệ của Kaspersky Endpoint Security
  - Tên và phiên bản của hệ điều hành được cài đặt trên máy tính
  - Phiên bản của Kaspersky Endpoint Security
  - Các phiên bản thiết lập ứng dụng và cài đặt tác vụ
  - Trạng thái tác vụ: định danh tác vụ, trạng thái thực thi, mã lỗi
- Trong các yêu cầu lấy tập tin từ máy chủ:
  - Định danh duy nhất của tập tin
  - Định danh duy nhất của Kaspersky Endpoint Security
  - Định danh duy nhất của chứng chỉ
  - Phần cơ bản của địa chỉ web của máy chủ có thành phần Central Node được cài đặt
  - Địa chỉ IP của máy chủ
- Trong các báo cáo kết quả thực thi tác vụ:
  - Địa chỉ IP của máy chủ
  - Thông tin về các đối tượng được phát hiện trong quá trình quét IOC hoặc quét YARA
  - Các cờ của các hành động bổ sung được thực hiện sau khi hoàn thành tác vụ
  - Lỗi thực thi tác vụ và mã trả về
  - Trạng thái hoàn thành tác vụ
  - Thời gian hoàn thành tác vụ

    - Các phiên bản của thiết lập được sử dụng để thực hiện các tác vụ
    - Thông tin về các đối tượng được gửi tới máy chủ, các đối tượng được cách ly và các đối tượng được khôi phục từ khu vực cách ly: đường dẫn đến các đối tượng, giá trị băm MD5 và SHA256, định danh của các đối tượng được cách ly
    - Thông tin về các tiến trình được khởi chạy hoặc bị dừng trên máy tính theo yêu cầu của máy chủ: PID và UniquePID, mã lỗi, giá trị băm MD5 và SHA256 của các đối tượng
    - Thông tin về các dịch vụ đã khởi tạo hoặc dừng trên máy tính theo yêu cầu của máy chủ: tên dịch vụ, loại khởi chạy, mã lỗi, giá trị băm MD5 và SHA256 của ảnh tập tin của dịch vụ
    - Thông tin về các đối tượng được thực hiện kết xuất bộ nhớ để quét YARA (đường dẫn, định danh tập tin kết xuất)
    - Các tập tin được yêu cầu bởi máy chủ
- Dữ liệu về các tiến trình đang chạy:
    - Tên tập tin thực thi, bao gồm đường dẫn đầy đủ và phần mở rộng
    - Tham số autorun của tiến trình
    - ID tiến trình
    - ID phiên đăng nhập
    - Tên phiên đăng nhập
    - Ngày và thời gian khởi tạo tiến trình
    - Giá trị băm MD5 và SHA256 của đối tượng
- Dữ liệu trên các tập tin:
    - Đường dẫn đến tập tin
    - Tên tập tin.
    - Kích thước tập tin
    - Thuộc tính tập tin
    - Ngày và giờ tạo tập tin
    - Ngày và giờ sửa đổi tập tin lần cuối
    - Mô tả tập tin
    - Tên công ty
    - Giá trị băm MD5 và SHA256 của đối tượng
    - Khóa registry (đối với các mục tự động chạy)

- Dữ liệu về các lỗi xảy ra khi thông tin về các đối tượng được truy xuất:
  - Tên đầy đủ của đối tượng đã được xử lý khi xảy ra lỗi
  - Mã lỗi
- Dữ liệu trong kết quả quét YARA:

  Tác nhân tích hợp của Kaspersky Endpoint Security sẽ tự động chuyển kết quả quét YARA tới Kaspersky Anti Targeted Attack Platform để xây dựng một chuỗi phát triển mối đe dọa.

  Dữ liệu tạm thời được lưu trữ cục bộ trong hàng chờ để gửi kết quả thực hiện tác vụ đến máy chủ Kaspersky Anti Targeted Attack Platform. Dữ liệu sẽ bị xóa khỏi bộ lưu trữ tạm thời sau khi đã được gửi.
  - Giá trị băm MD5 và SHA256 của tập tin
  - Tên đầy đủ của tập tin
  - Đường dẫn đến tập tin
  - Kích thước tập tin
  - 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
- Dữ liệu trong kết quả quét IOC:
  - Địa chỉ IP từ bảng ARP
  - Địa chỉ vật lý từ bảng ARP
  - Tên bản ghi DNS
  - Loại bản ghi DNS
  - Tên máy chủ
  - Địa chỉ IP
  - ID sự kiện trong nhật ký
  - Tên nguồn dữ liệu trong nhật ký
  - Tên nhật ký

- Tên người dùng
- Ngày và giờ tạo sự kiện, theo định dạng ISO
- Giá trị băm MD5 và SHA256 của tập tin
- Tên đầy đủ của tập tin
- Kích thước tập tin
- Địa chỉ IP từ xa và cổng có kết nối được thiết lập trong quá trình quét
- Địa chỉ IP và cổng của bộ tiếp hợp cục bộ
- Giao thức
- 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
- Đường dẫn đến khóa registry
- Tên khóa registry
- Giá trị văn bản của khóa registry
- Tên dịch vụ
- Mô tả về dịch vụ
- Đường dẫn và tên của dịch vụ DLL
- Đường dẫn và tên của tập tin thực thi dịch vụ
- Định danh Windows (PID) của dịch vụ
- Loại dịch vụ
- Trạng thái dịch vụ
- Chế độ khởi chạy dịch vụ
- Tên hệ điều hành
- Phiên bản hệ điều hành

- Tên mạng máy tính không chứa tên miền
- Tên miền hoặc nhóm làm việc
- Tên người dùng
- Tên phân vùng
- Chữ cái phân vùng
- Loại phân vùng

Kaspersky Network Detection and Response (KATA)

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 đo từ xa

- **Dữ liệu về các tập tin**
  - Định danh duy nhất của tập tin
  - Loại tập tin
  - Đường dẫn đến tập tin
  - Kích thước tập tin
  - Thuộc tính tập tin
  - Định danh vùng
  - Ngày và giờ tạo tập tin
  - Ngày và giờ sửa đổi tập tin lần cuối
  - Tên tập tin gốc
  - Tên ứng dụng
  - Phiên bản ứng dụng.
  - Nhà cung cấp ứng dụng
  - Mô tả tập tin
  - Phiên bản tập tin.

- Giá trị băm MD5 và SHA256 của đối tượng
- Kết quả xác minh mã nhận diện tập tin
- Ngày và giờ tạo mã nhận diện tập tin
- Chuỗi chứng chỉ được sử dụng trong tập tin mã nhận diện
- Loại chuỗi chứng chỉ
- Các chứng chỉ trong chuỗi
- Tên tổ chức cấp chứng chỉ
- Tên người sở hữu chứng chỉ
- Số sê-ri chứng chỉ
- Thuật toán dấu vân tay chứng chỉ
- Dấu vân tay chứng chỉ
- Thời hạn hiệu lực của chứng chỉ

- **Dữ liệu về phiên đăng nhập**
  - ID phiên đăng nhập
  - Tên tài khoản của người dùng đã đăng nhập
  - Loại tài khoản người dùng
  - Loại phiên
  - Địa chỉ IP của máy tính đã thực hiện nỗ lực đăng nhập
  - Địa chỉ IP của máy tính cục bộ có nỗ lực đăng nhập được thực hiện
  - Cờ chỉ báo phiên làm việc được thể hiện bởi sự kiện này có đặc quyền nâng cao và quyền quản trị
  - Tham số cho biết liệu các phiên đăng nhập khác có được liên kết với phiên đăng nhập này hay không
  - Giao thức được sử dụng cho phiên dòng lệnh
  - Giao thức IPv4 được sử dụng cho phiên dòng lệnh
- **Dữ liệu về giao tiếp mạng**
  - Thời điểm bắt đầu và kết thúc của khoảng thời gian thu thập dữ liệu
  - Danh sách kết nối
  - Địa chỉ IP cục bộ của máy tính

- Địa chỉ MAC cục bộ của máy tính
- Địa chỉ IP từ xa của máy tính
- Địa chỉ MAC từ xa của máy tính
- Địa chỉ IP của cổng
- Số lượng gói dữ liệu được truyền
- Số lượng gói dữ liệu được nhận
- Tổng số byte đã truyền
- Giao thức truyền dữ liệu
- Trường EtherType của khung Ethernet
- Tiền tố dữ liệu của gói tin đầu tiên trong khoảng thời gian đó
- Địa chỉ IPv4 của giao diện mạng mà qua đó quá trình giao tiếp được ghi lại

- **Thông tin về kết nối mạng**
  - Định danh duy nhất của tiến trình đã khởi tạo kết nối
  - Giao thức truyền dữ liệu
  - Địa chỉ IP cục bộ được sử dụng để khởi tạo kết nối
  - Địa chỉ IP từ xa của điểm cuối kết nối
  - Phương thức HTTP
  - Đường dẫn không có tên máy chủ
  - Tên máy chủ
  - Trạng thái động của tiến trình tại thời điểm kết nối
  - Hướng kết nối
  - Trạng thái tiến trình động
  - Trường EtherType của khung Ethernet
- **Dữ liệu được thu thập trong khi nghe trên một cổng mạng**
  - Định danh duy nhất của tiến trình đã khởi tạo kết nối
  - Giao thức truyền dữ liệu
  - Địa chỉ cục bộ
  - Trạng thái động của tiến trình tại thời điểm kết nối

- **Kết quả xác minh kết nối**
  - Thiết lập mạng của máy chủ
  - Mô tả giao diện mạng
  - Tên miền DNS
  - Địa chỉ MAC cục bộ của máy tính
  - Số liệu đo lường kết nối IP
  - Danh sách địa chỉ IP
  - Địa chỉ IP
  - Mặt nạ mạng
  - Địa chỉ IP của cổng
  - Địa chỉ MAC của cổng
  - Danh sách các bản vá đã cài đặt
  - Số hiệu bản vá
  - Ngày cài đặt bản vá
  - Kiểu thiết bị
  - Nhà cung cấp thiết bị
  - ID máy chủ trong Kaspersky Security Center
  - Mô tả phần mềm diệt virus Kaspersky đã được cài đặt
  - Tên thành phần của phần mềm diệt virus Kaspersky đã được cài đặt
  - Phiên bản thành phần của phần mềm diệt virus Kaspersky đã được cài đặt
  - Phiên bản cơ sở dữ liệu của thành phần diệt virus Kaspersky đã được cài đặt
  - Ngày cập nhật cơ sở dữ liệu lần cuối của thành phần diệt virus Kaspersky đã được cài đặt
  - Trạng thái thành phần của phần mềm diệt virus Kaspersky đã được cài đặt
  - Danh sách khóa giấy phép
  - Số sê-ri của khóa
  - Loại khóa

- Ngày hết hạn khóa
- Trạng thái khóa

- **Dữ liệu về việc tạo tiến trình trên máy chủ**
  - Định danh duy nhất của tiến trình
  - Định danh duy nhất của tiến trình gốc
  - Định danh hệ thống duy nhất của tiến trình
  - Lệnh dùng để khởi chạy một tiến trình
  - ID phiên đăng nhập
  - ID phiên dòng lệnh
  - Định danh duy nhất của tập tin tiến trình
  - Mức độ toàn vẹn của tiến trình
  - Danh sách token quyền của tiến trình
  - Các quyền thuộc tính
  - Danh sách định danh duy nhất của các tập tin đã được thông dịch
  - Trạng thái tiến trình
  - Lệnh dùng để khởi chạy một tiến trình
- **Dữ liệu về việc kết thúc tiến trình**
  - Định danh duy nhất của tiến trình
- **Dữ liệu về mối đe dọa được phát hiện**
  - Thông tin về mối đe dọa
  - Phán quyết mối đe dọa
  - Số bản ghi AMR
  - Phiên bản cơ sở dữ liệu diệt virus
  - Chế độ phát hiện mối đe dọa
  - Định danh duy nhất của mối đe dọa
  - Công nghệ bảo vệ
  - Thông tin về vật thể bị lây nhiễm
  - Loại đối tượng bị lây nhiễm

- Tên đối tượng bị lây nhiễm
- Giá trị băm MD5 và SHA256 của đối tượng
- Định danh duy nhất của tiến trình bị lây nhiễm
- Định danh duy nhất của đối tượng bị nhiễm
- Định danh duy nhất của tiến trình đã tải xuống đối tượng bị nhiễm từ internet
- URL tải xuống đối tượng bị nhiễm
- Địa chỉ email người gửi đã gửi đối tượng bị lây nhiễm
- Giao thức mạng nhận đối tượng bị nhiễm
- Địa chỉ cục bộ nơi nhận đối tượng bị lây nhiễm
- Địa chỉ bên ngoài nhận đối tượng bị lây nhiễm
- Loại nội dung của đối tượng
- Bối cảnh của mối đe dọa được phát hiện
- Nội dung của đối tượng
- Cờ chỉ báo việc phát hiện mối đe dọa đã chạy trong nền

- **Dữ liệu về quá trình xử lý mối đe dọa**
  - Thông tin về mối đe dọa
  - Phán quyết mối đe dọa
  - Số bản ghi AMR
  - Phiên bản cơ sở dữ liệu diệt virus
  - Chế độ phát hiện mối đe dọa
  - Tên đối tượng bị lây nhiễm
  - Giá trị băm MD5 và SHA256 của đối tượng
  - Định danh duy nhất của tiến trình bị lây nhiễm
  - Định danh duy nhất của đối tượng bị nhiễm
  - Giao thức mạng nhận đối tượng bị nhiễm
  - Địa chỉ cục bộ nơi nhận đối tượng bị lây nhiễm
  - Địa chỉ bên ngoài nhận đối tượng bị lây nhiễm
  - Trạng thái xử lý mối đe dọa

- Lý do không thể khắc phục mối đe dọa
- Địa chỉ vật lý cục bộ

- **Dữ liệu về người dùng**
  - SID người dùng
  - ID người dùng
  - Tên người dùng
  - Tên đầy đủ của người dùng
  - Mô tả người dùng
  - Liệu tài khoản đang hoạt động hay bị chặn
  - Liệu mật khẩu đã hết hạn hay chưa
  - Liệu có cần thay đổi mật khẩu hay không
  - Liệu có cho phép thay đổi mật khẩu hay không
  - Loại tài khoản người dùng
  - Liệu tính năng đăng nhập tự động có được bật cho tài khoản này hay không
  - Danh sách các nhóm có người dùng

Tích hợp với Kaspersky Unified Monitoring and Analysis Platform (KUMA)

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.

Khi tích hợp với Kaspersky Unified Monitoring and Analysis Platform (KUMA), dữ liệu thiết lập kết nối sẽ được truyền gửi, cũng như tất cả các sự kiện được ghi lại trong Nhật ký Windows.

Các nhật ký sự kiện chính của Windows bao gồm System, Security, Application, ForwardedEvents và HardwareEvents. Người dùng cũng có thể tạo và làm việc với nhật ký tùy chỉnh để đáp ứng các yêu cầu cụ thể của họ.

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.

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 thì hãy sử dụng Kaspersky Private Security Network (KPSN) hoặc tắt sử dụng KSN. Để biết thêm chi tiết về KPSN, 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.

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 tại Hoa Kỳ và/hoặc các quốc gia khác.

Amazon, Amazon Web Services, AWS là các thương hiệu của Amazon.com, Inc. hoặc các chi nhánh của hãng.

Apple, FireWire, iTunes, Mac và Safari là các thương hiệu của Apple Inc.

Arm là thương hiệu đã được đăng ký của Arm Limited (hoặc các công ty con của hãng) tại Hoa Kỳ và/hoặc 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.

Cisco, Cisco AnyConnect, IOS là các thương hiệu đã đăng ký hoặc thương hiệu của Cisco Systems, Inc. và/hoặc các công ty liên kết của công ty tại Hoa Kỳ và một số quốc gia khác.

Citrix, Citrix Provisioning, Citrix Provisioning Services, Citrix Virtual Apps and Desktop, XenDesktop và XenServer là các thương hiệu đã đăng ký hoặc thương hiệu của Cloud Software Group, Inc. và/hoặc các công ty con tại Hoa Kỳ và/hoặc các quốc gia khác.

Cloudflare, Cloudflare Workers và logo Cloudflare là các thương hiệu và/hoặc thương hiệu đã đăng ký của Cloudflare, Inc. tại Hoa Kỳ và các khu vực tài phán khác.

Core là thương hiệu của Intel Corporation hoặc các công ty con của hãng.

dBase là một thương hiệu của dataBased Intelligence, Inc.

Dell Technologies, Dell, EMC và các thương hiệu khác là thương hiệu của Dell Inc. hoặc các công ty con của hãng.

Docker và logo Docker là các thương hiệu hoặc thương hiệu đã đăng ký của Docker, Inc. tại Hoa Kỳ và/hoặc các quốc gia khác. Docker, Inc. và các bên khác cũng có thể có quyền thương hiệu trong các điều khoản khác được sử dụng ở đây.

ESET là thương hiệu hoặc thương hiệu đã đăng ký của ESET spol. s r.o. hoặc của thực thể ESET tương ứng.

Foxit là thương hiệu đã đăng ký của Foxit Corporation.

Radmin là một thương hiệu được đăng ký của Famatech.

Google, Android, Google Public DNS, Google Chrome, Chrome là các thương hiệu của Google LLC.

HUAWEI, FusionCompute và FusionSphere là các thương hiệu của Huawei Technologies Co., Ltd.

ICQ là thương hiệu và/hoặc nhãn hiệu Dịch vụ của ICQ LLC.

Intel là thương hiệu của Intel Corporation hoặc các công ty con của hãng.

IBM là một thương hiệu của International Business Machines Corporation, được đăng ký ở nhiều khu vực tài phán trên thế giới.

Lenovo và Lenovo 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 của Mail.ru LLC.

McAfee là thương hiệu hoặc thương hiệu đã đăng ký của McAfee LLC hoặc các công ty con của hãng tại Hoa Kỳ và/hoặc các quốc gia khác.

Microsoft, Access, Active Directory, ActiveSync, Bing, BitLocker, Excel, Hyper-V, Internet Explorer, JScript, LifeCam Cinema, Microsoft Edge, MSDN, MS-DOS, MultiPoint, Office 365, Outlook, PowerPoint, PowerShell, Skype, SQL Server, Surface, Visual Basic, Visual FoxPro, Windows, Windows Live, Windows PowerShell, Windows Server và Windows Store là các thương hiệu của tập đoàn Microsoft.

Mozilla, Firefox và Thunderbird là thương hiệu của Mozilla Foundation tại Hoa Kỳ và các quốc gia khác.

NetApp là một thương hiệu hoặc thương hiệu đã đăng ký của NetApp, Inc. tại Hoa Kỳ và/hoặc các quốc gia khác.

OpenSSL là thương hiệu thuộc sở hữu của OpenSSL Software Foundation.

OpenStack là thương hiệu của OpenStack Foundation tại Hoa Kỳ và các quốc gia khác.

Oracle, Java và JavaScript là các thương hiệu đã đăng ký của Oracle và/hoặc công ty chi nhánh của hãng.

Python là thương hiệu hoặc thương hiệu đã đăng ký của Python Software Foundation.

Realtek là một thương hiệu của Realtek Semiconductor Corporation.

SAMSUNG là thương hiệu của SAMSUNG tại Hoa Kỳ hoặc các quốc gia khác.

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.

Trend Micro là thương hiệu hoặc thương hiệu đã đăng ký của Trend Micro Incorporated.

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 ESXi, VMware Horizon, VMware Workstation, VMware Tools, VMware vSphere là các thương hiệu đã đăng ký và/hoặc thương hiệu của VMware, Inc. tại Hoa Kỳ và các quốc gia khác.

Thông tin về mã của bên thứ ba

Thông tin về mã của bên thứ ba có trong tập tin legal_notices.txt, trong thư mục cài đặt của ứng dụng.