**HƯỚNG DẪN CẤU HÌNH PHÒNG CHỐNG MÃ ĐỘC TỐNG TIỀN WANNACRY**

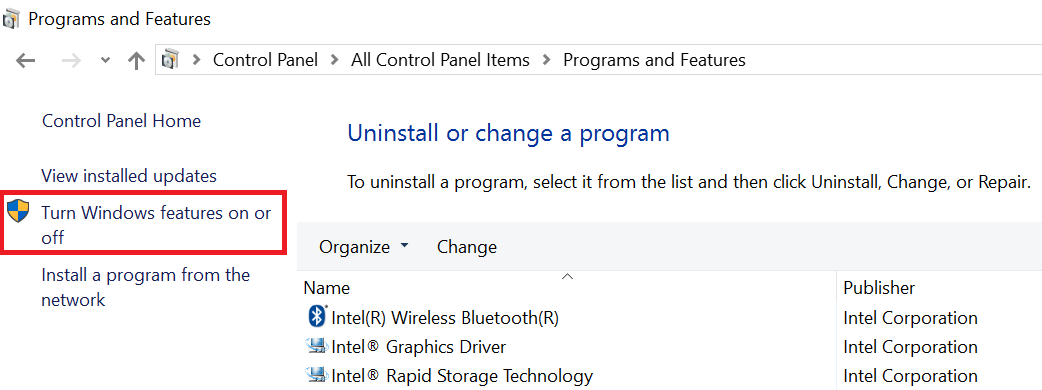
Để tránh bị mã độc mã hóa dữ liệu (mã độc tống tiền) WannaCry, người dùng không click vào các đường link hoặc các file đính kèm trong email, trong các tin nhắn trừ khi xác nhận được những file đính kèm và đường link này là an toàn.

Đồng thời, người dùng cần sao lưu tất cả các dữ liệu quan trọng sang những thiết bị lưu trữ hoặc lưu trữ trên Cloud.

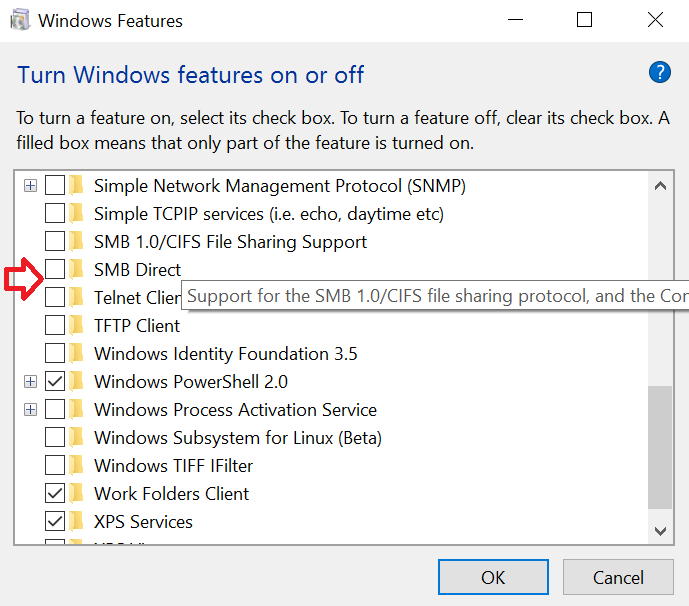
**Hướng dẫn cho khách hàng cá nhân:**

1. Kiểm tra và tắt SMB trên máy tính, Laptop

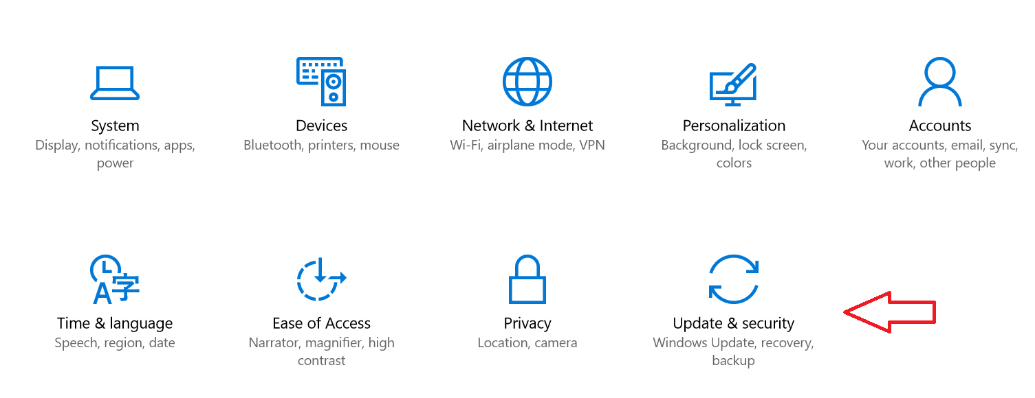
Mở **Control Panel** và Click **Turn Windows features on or off**



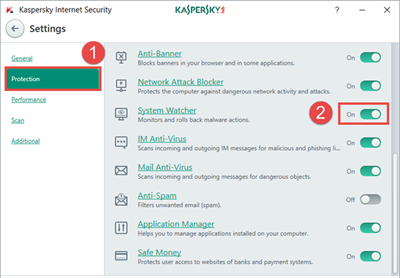
Bỏ chọn tại các dòng SMB



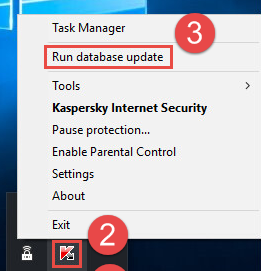
1. Chạy Windows Updates



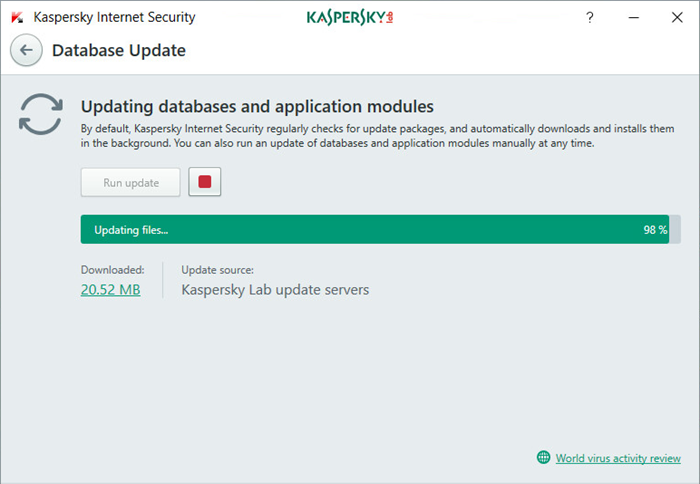
1. Cài đặt Phần mềm Antivirus có bản quyền của Kaspersky và bật các tính năng System Watcher, IM Anti-Virus, Mail Anti-Virus



1. Đảm bảo rằng Database đã được update. Nếu không, click chuột phải vào biểu tượng của Kaspersky trên thanh Task bar và chọn **Run database Update**



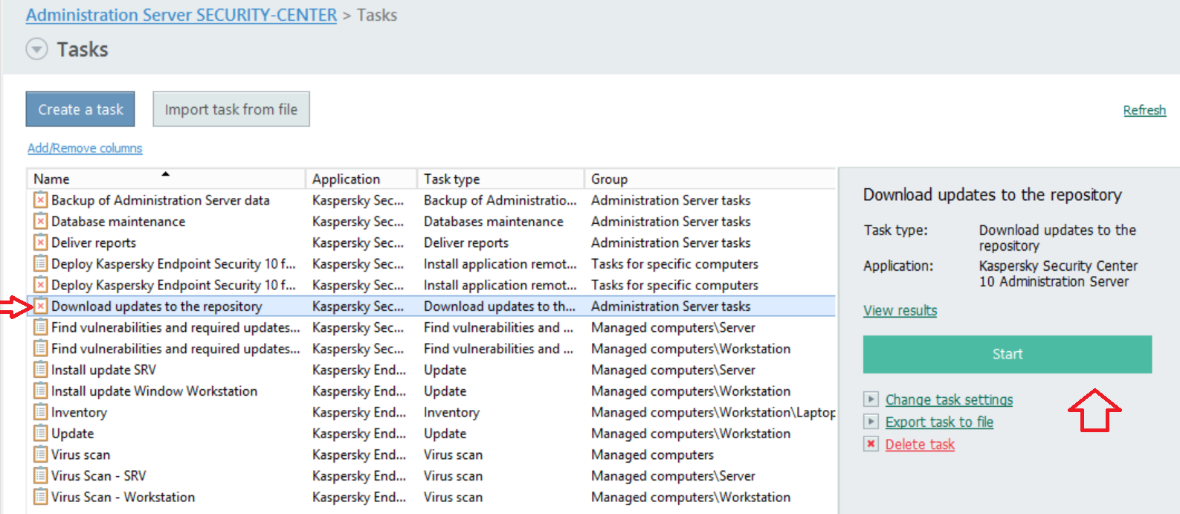
Và chạy Update



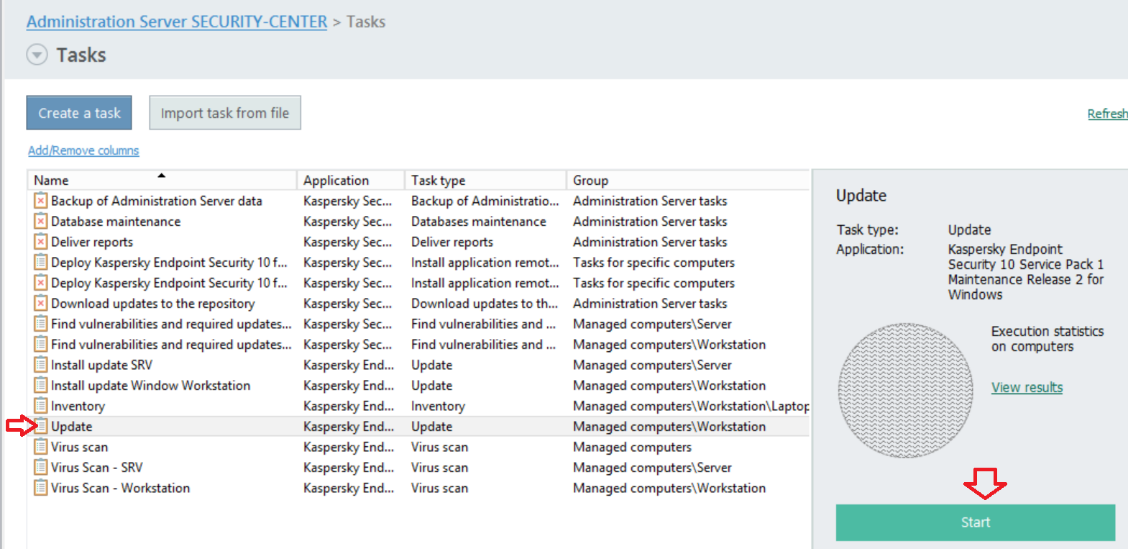
1. Thực hiện dò quét virus trên máy tính. Khởi động lại máy tính nếu phát hiện các mã độc.
2. Nếu phát hiện có tấn công từ phần mềm độc hại như tên gọi MEM: Trojan.Win64.EquationDrug.gen thì cần reboot lại hệ thống.

**Hướng dẫn cho khách hàng doanh nghiệp – tổ chức:**

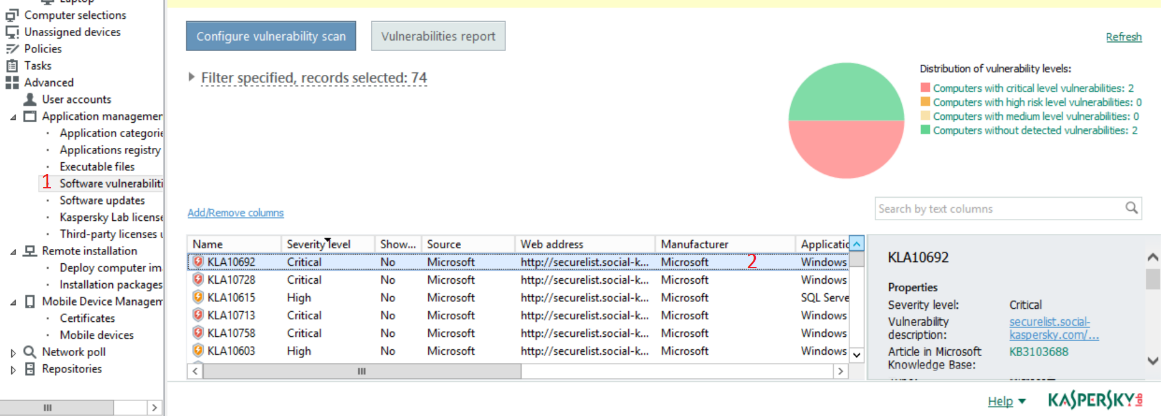
1. Quản trị viên cần gửi cảnh báo cho tất cả người dùng trong hệ thống về mã mã độc tống tiền WannaCry và yêu cầu người dùng không click vào các đường link cũng như file đính kèm mà không thể kiểm chứng độ an toàn cũng như không như truy cập vào các Website có nội dung không tốt.
2. Sao lưu toàn bộ các dữ liệu quan trọng sang các thiết bị lưu trữ, lưu trữ trên Cloud.
3. Trên Kaspersky Security Center, quản trị viên thực hiện chạy cập nhật.



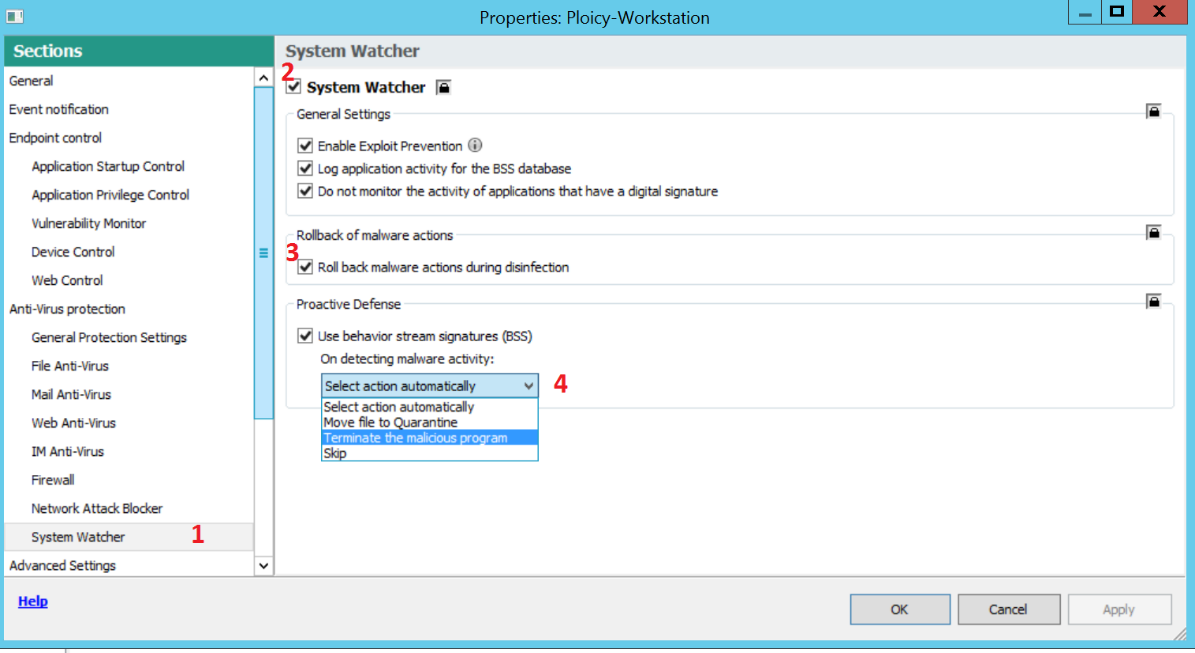
Và lên lịch update cho các máy chủ, máy trạm.



1. Hãy sử dụng tính năng Vulnerabitliy, Patch Management trong KESB để phát hiện toàn bộ các lỗ hổng trong hệ thống. Đặc biệt, đối với các thiết bị có chứa lỗ hổng MS17-010 cần cách ly và thực hiện chạy Update.

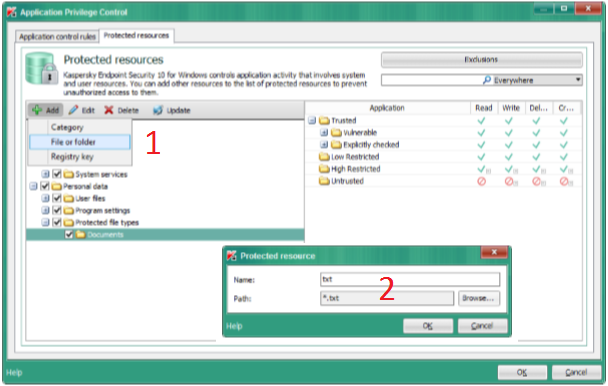


1. Bật tính năng **System Watcher** và chọn **Roll back malware actions during disinfection**

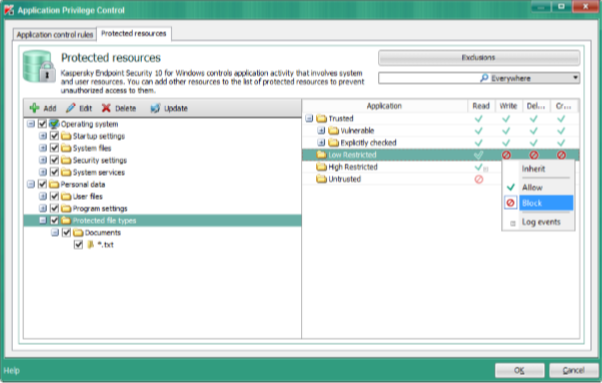


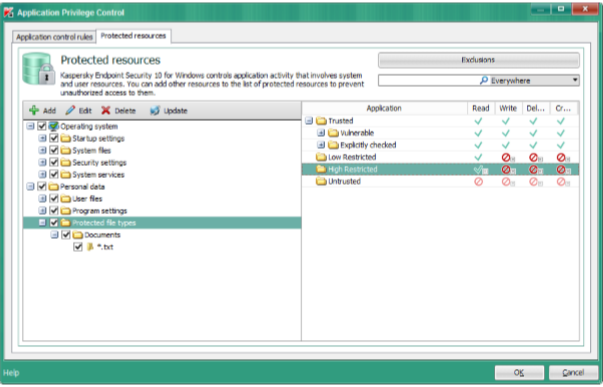
1. Cấu hình **Application Privilege Control** để ngăn chặn mã độc tống tiền xóa file gốc sau khi mã hóa.

Thêm các extension để thiết lập quyền cho các ứng dụng này như *.txt, .docx, .pptx…*

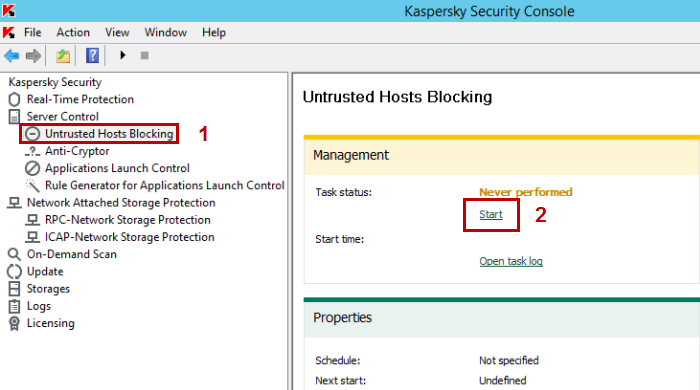


Chọn **Block** trên các hành động **Write, Delete** và **Creat** với cả **Low Resticted** và **High Restricted**

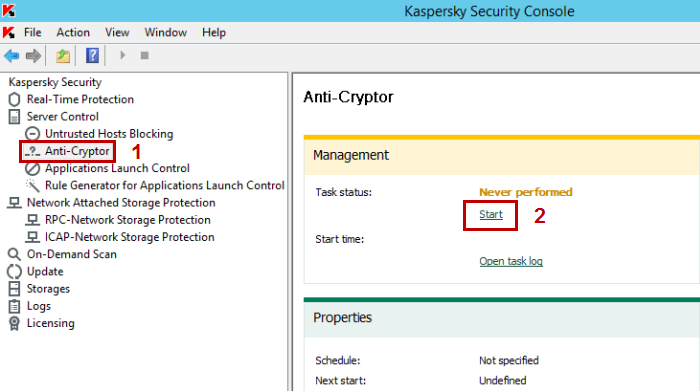




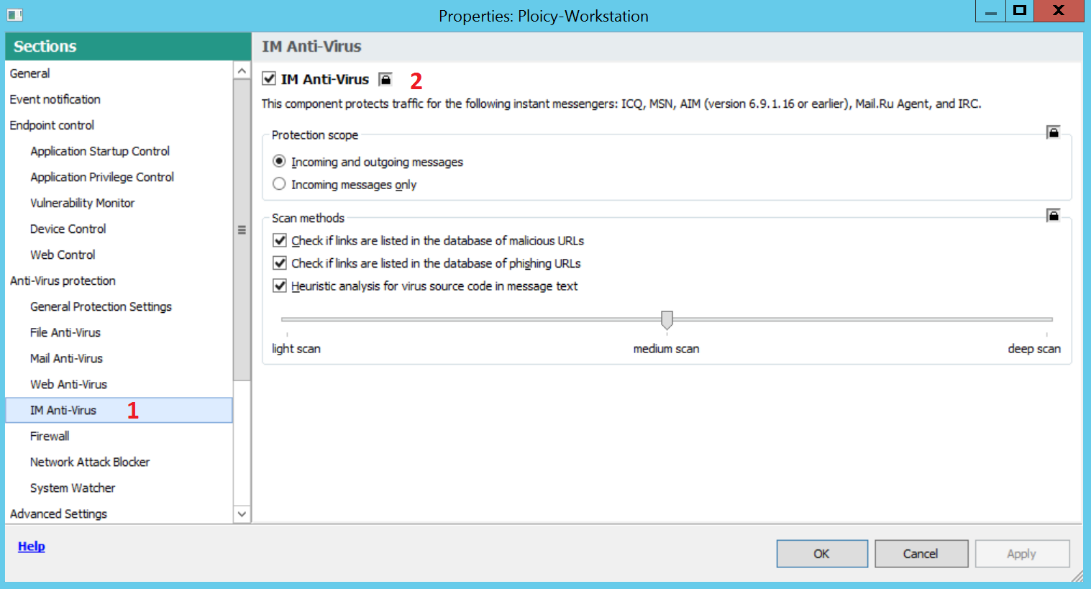
1. Bật tính năng Anti-Cryptor for Windows Server.



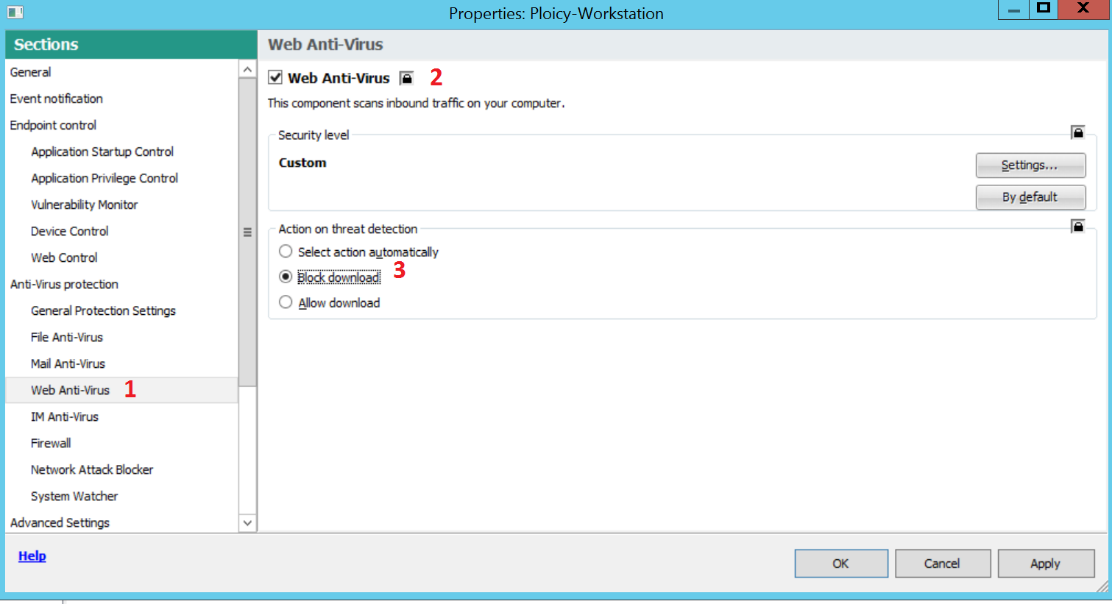
Và cấu hình trong Anti-Cryptor



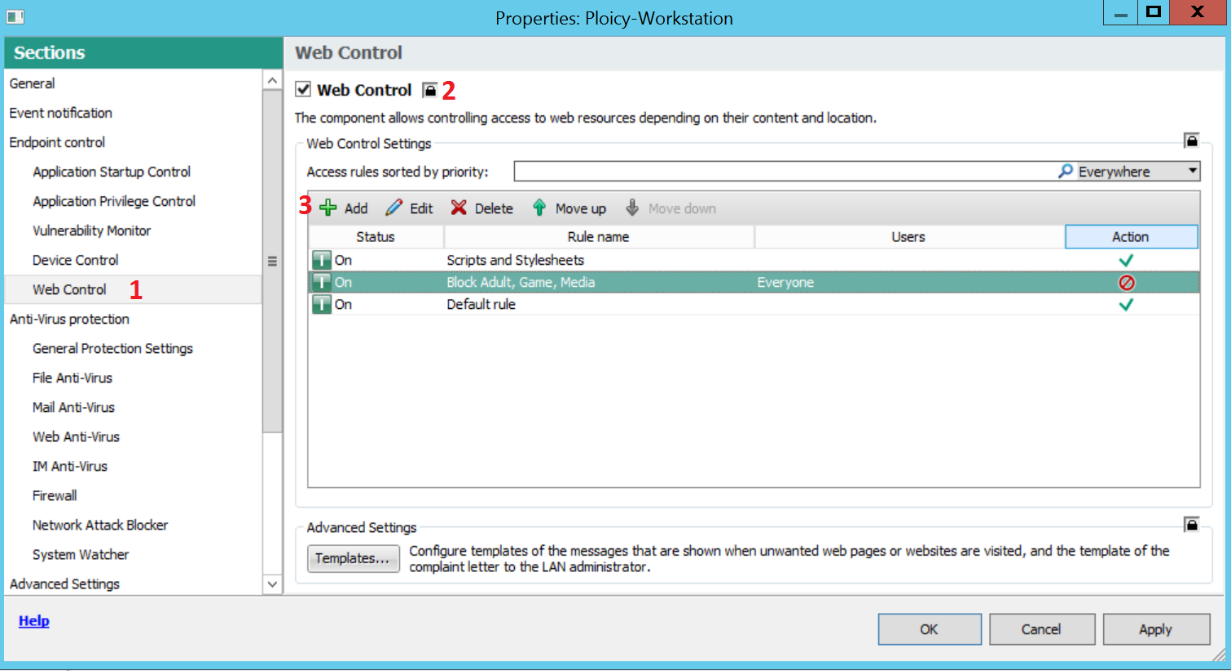
1. Để ngăn chặn lây nhiễm mã độc mã hóa tống tiến từ các nguồn online, bật tính năng IM Anti-virus



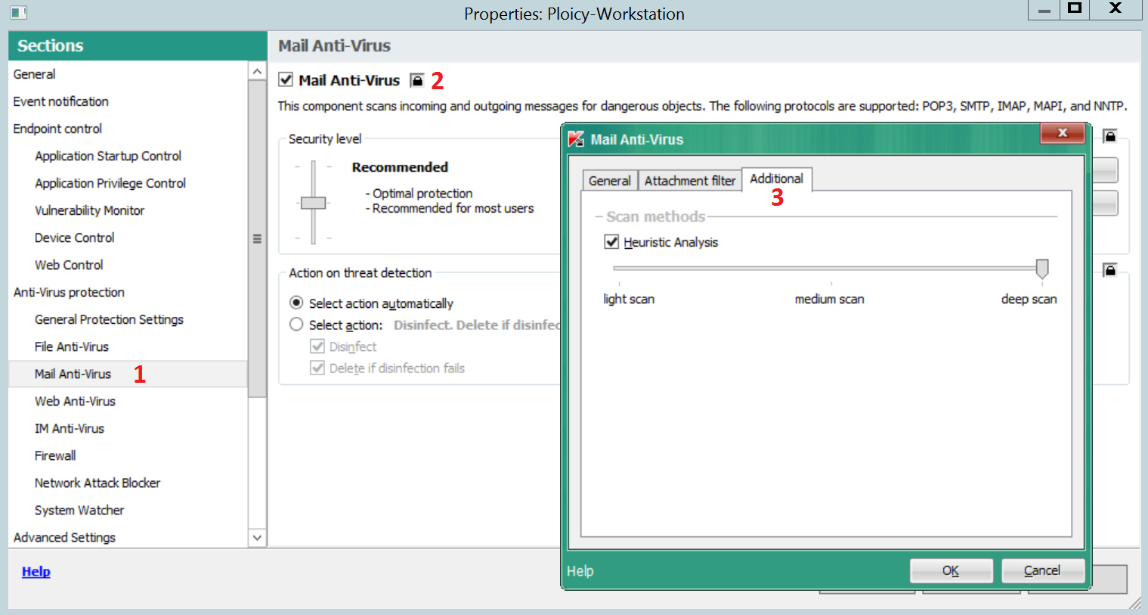
Bật tính năng Web Anti-Virus và chọn Block Download



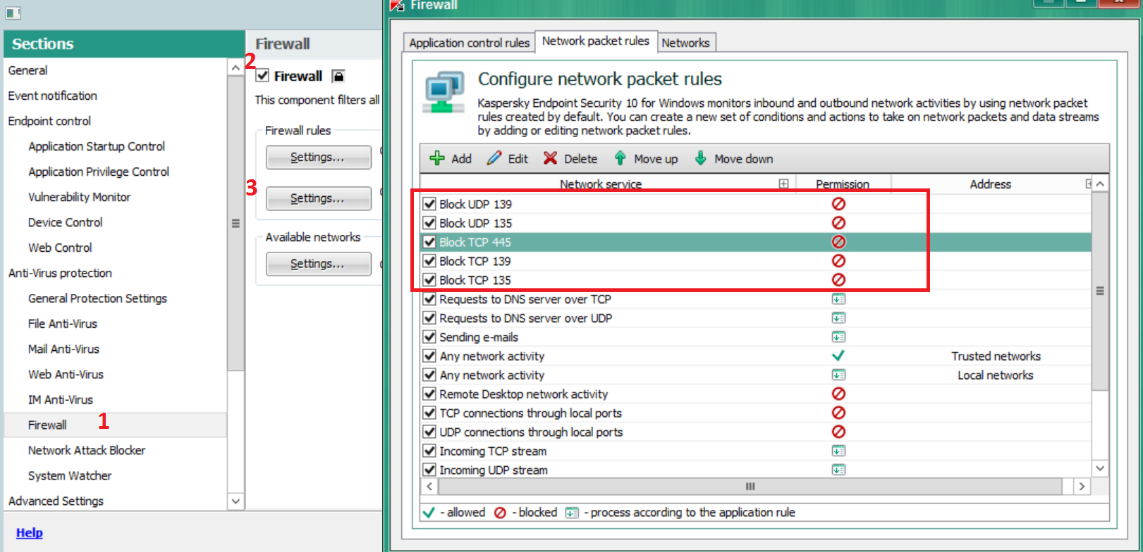
Bật Web Control và cấm người dùng truy cập các website không phù hợp.



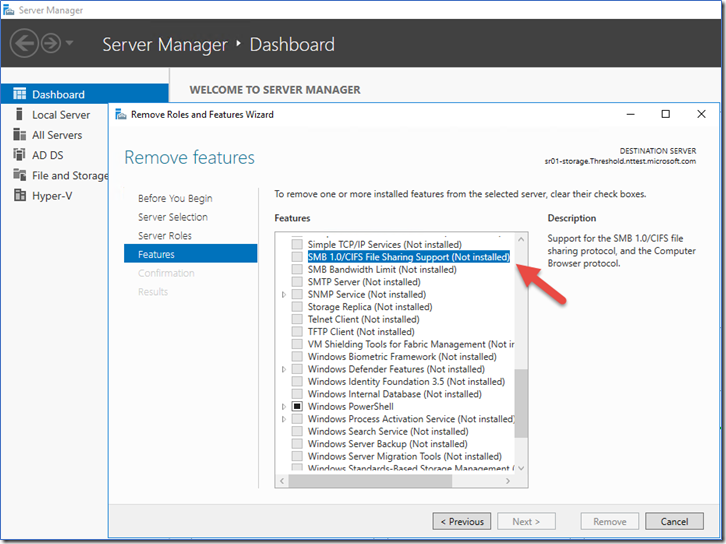
Bật tính năng Mail Anti-Virus



1. Trên KSC, cấu hình cấm inbound/outbound trên các port TCP/UDP 135, 139 và TCP 445.



1. Nếu có thể, tắt SMB



1. Chạy Virus Scan task

