

KS. LÊ NGỌC CƯỜNG

Hướng dẫn sử dụng

Norton AntiVirus

2001
&

McAfee VirusScan



NHÀ XUẤT BẢN THỐNG KÊ

K.S LÊ NGỌC CƯỜNG

Hướng Dẫn Sử Dụng

Norton AntiVirus 2001 & McAfee VirusScan

NHÀ XUẤT BẢN THỐNG KÊ

Hướng Dẫn Sử Dụng

Norton AntiVirus 2001

Và

McAfee VirusScan

Lời nói đầu

Nhà ngày nay, phần lớn những người sử dụng máy tính thường xuyên gửi thông tin, chia sẻ dữ liệu và truyền các file cho nhau. Dù được thực hiện bằng cách nào, qua modem, đĩa mềm, các mạng hay qua Internet thì điều này hẳn đã tạo điều kiện thuận lợi cho virus phát triển và lây lan nhanh hơn bao giờ hết.

Nhằm giúp các bạn tự bảo vệ mình trong môi trường này đồng thời biết cách xử lý khi phát hiện một virus, chúng tôi biên soạn cuốn **“Hướng dẫn sử dụng Norton AntiVirus 2001 và McAfee VirusScan”**.

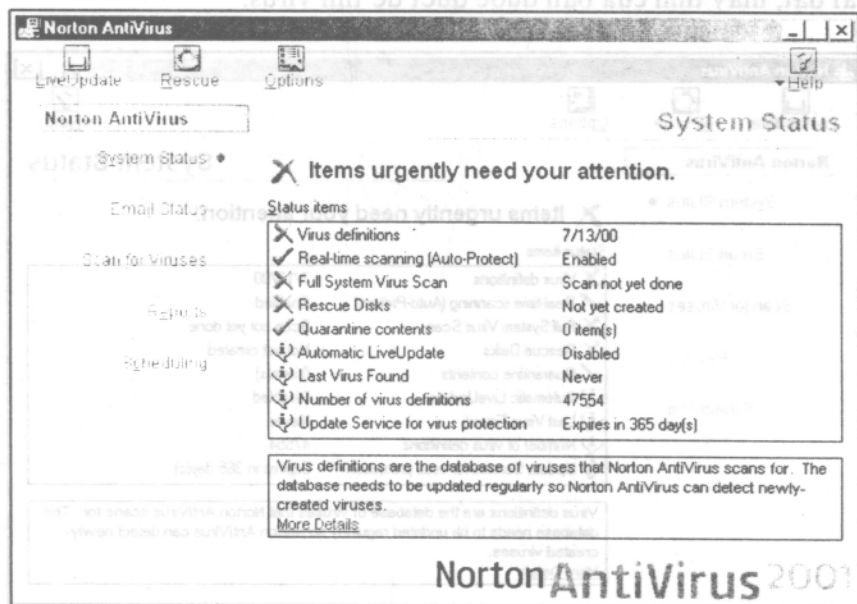
Sách gồm hai phần và 1 phụ lục : Phần 1 giới thiệu về Norton AntiVirus 2001, cách hoạt động của nó cũng như cách quét, xử lý và loại bỏ những vùng bị nhiễm virus. Phần 2 hướng dẫn các bạn tìm hiểu phần mềm chống virus VirusScan, cách sử dụng VShield scanner, VirusScan Console và các trình tiện ích, cách cấu hình cũng như giải thích khi nào và tại sao phải sử dụng chúng. Phụ lục hướng dẫn sử dụng bàn phím với phần mềm NEWTOUCH.

Với nội dung nêu trên cộng với cách bố cục theo từng đề mục, hình ảnh minh họa rõ ràng, chúng tôi hy vọng cuốn sách này sẽ giúp ích nhiều cho các bạn trong việc phòng chống và loại bỏ virus.

Chúc các bạn thành công.

Tác giả

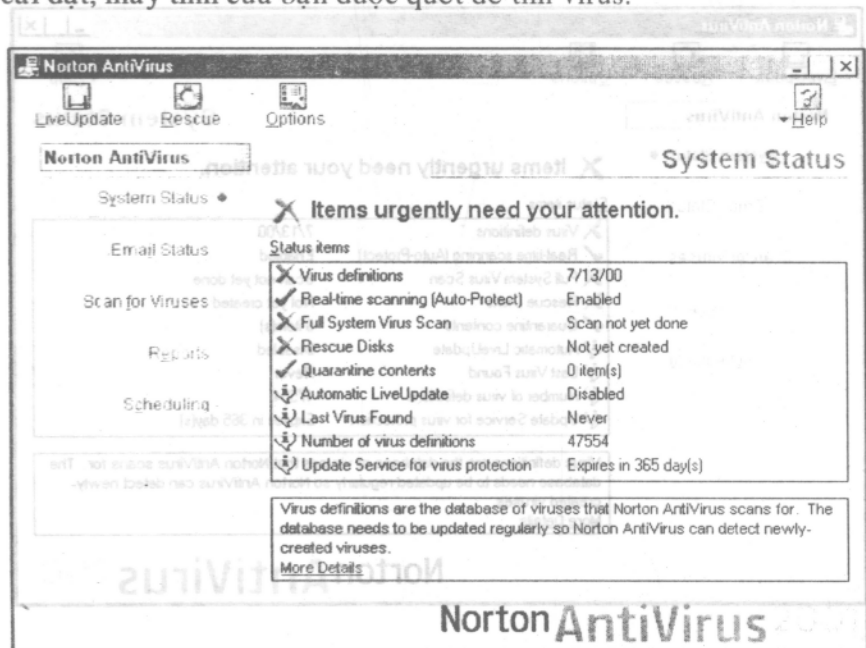
PHẦN 1

Norton
AntiVirus 2001

Bài 1

GIỚI THIỆU VỀ NORTON ANTIVIRUS 2001

Khi bạn cài đặt Norton AntiVirus và chấp nhận các tùy chọn đã xác lập sẵn, máy tính của bạn đã an toàn, là một phần của tiến trình cài đặt, máy tính của bạn được quét để tìm virus.



Norton AntiVirus tự động kiểm tra các record khởi động để tìm virus vào lúc khởi động hệ thống, kiểm tra virus cho các chương trình mà bạn sử dụng, quét tất cả các ổ đĩa cục bộ mỗi tuần một lần, và

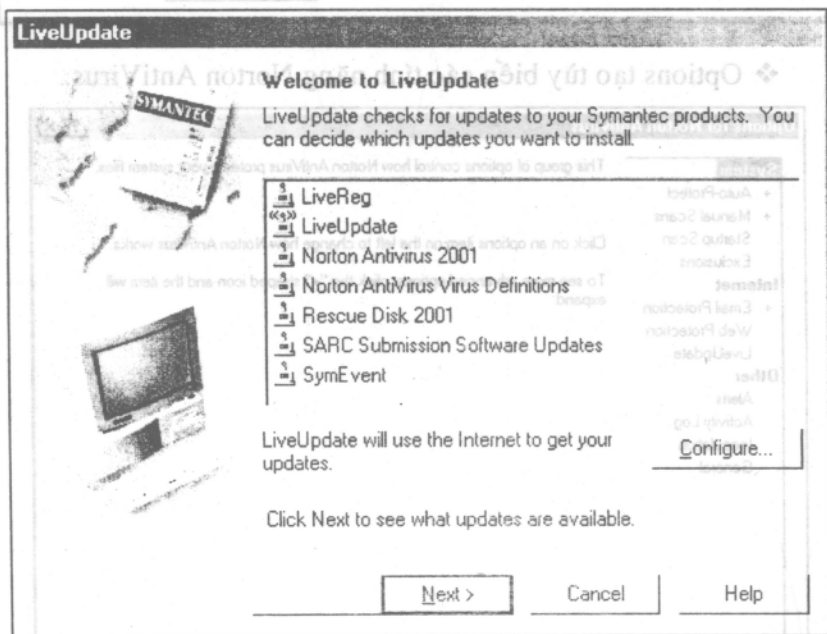
giám sát bất kỳ máy tính nào cho thấy có sự hoạt động của virus. Nó cũng quét các file mà bạn tải xuống từ Internet và kiểm tra các đĩa mềm để tìm các virus khởi động khi bạn sử dụng chúng.

Với Norton AntiVirus, bạn có thể quét các file, các folder, hay toàn bộ các ổ đĩa để tìm virus, và cách ly các file bị nhiễm để gửi chúng đến Symantec AntiVirus Research Center (SARC). Các file được gửi đến SARC được phân tích và các kết quả được báo cáo tự động trong vòng bảy ngày.

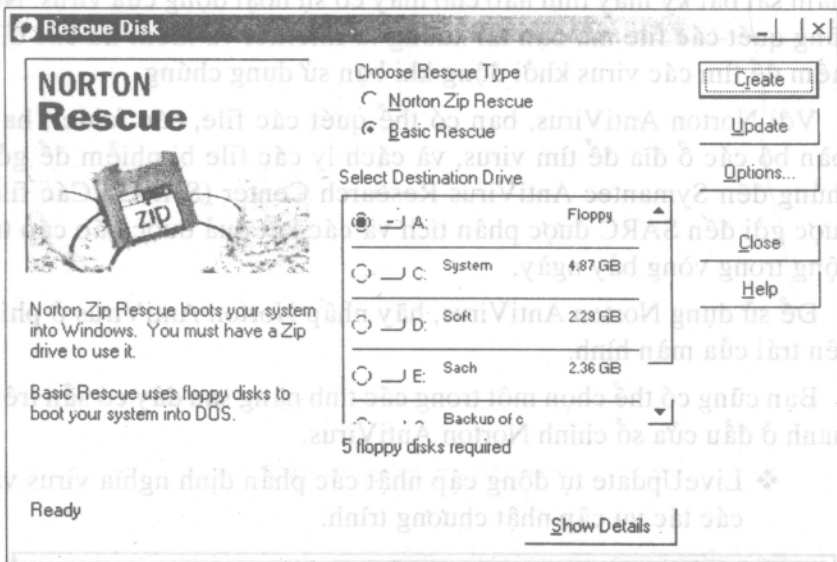
Để sử dụng Norton AntiVirus, hãy nhấp Norton AntiVirus ở phía bên trái của màn hình.

Bạn cũng có thể chọn một trong các tính năng sau đây có sẵn trên thanh ở đầu cửa sổ chính Norton AntiVirus.

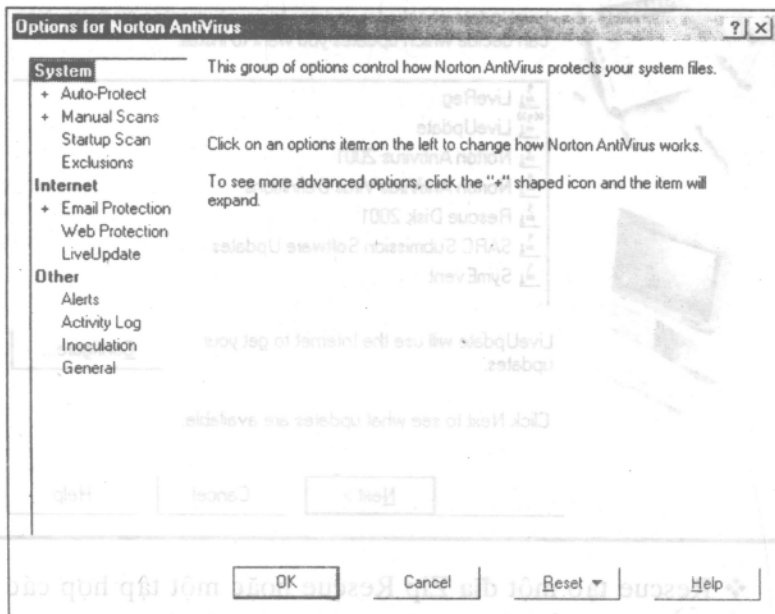
- ❖ LiveUpdate tự động cập nhật các phần định nghĩa virus và các tác vụ cập nhật chương trình.



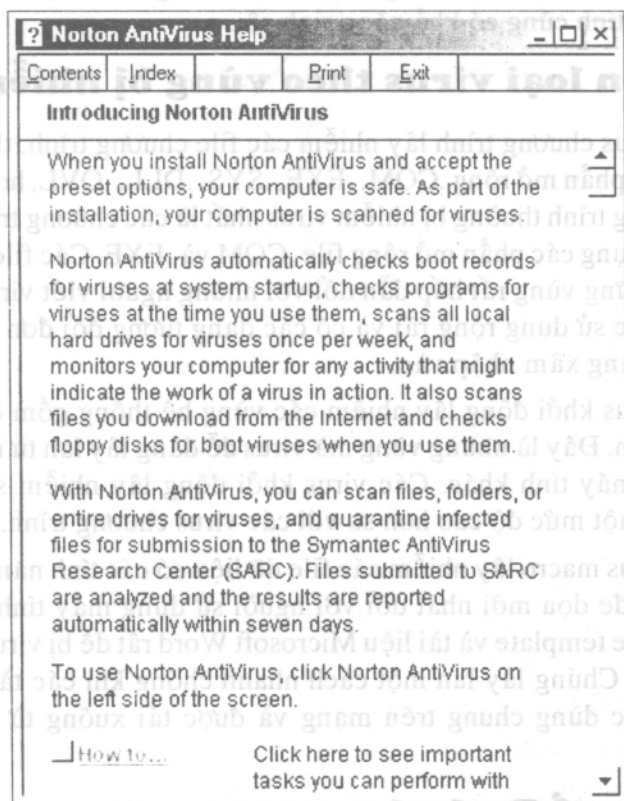
- ❖ Rescue tạo một đĩa Zip Rescue hoặc một tập hợp các đĩa mềm truy cứu.



❖ Options tạo tùy biến các tính năng Norton AntiVirus.



❖ Help trình bày thêm thông tin về cửa sổ mà bạn đang xem.



I. Thế nào là một virus máy tính?

Virus máy tính là các chương trình máy tính khả thi. Giống như virus sinh học, chúng tìm và xâm nhập vào một máy tính. Cũng như một virus cúm cúm, vốn tìm và xâm nhập vào cơ thể người, virus máy tính xâm nhập vào một hạng mục, chẳng hạn như một vùng khởi động máy tính (record khởi động) hay một file khả thi.

Phần lớn virus vẫn hoạt động trong bộ nhớ cho đến khi bạn tắt máy tính. Khi bạn tắt máy tính, virus bị loại ra khỏi bộ nhớ, nhưng không ra khỏi file, các file, hay đĩa bị nhiễm. Vì vậy, vào lần kế tiếp bạn sử dụng máy tính, chương trình virus được kích hoạt trở lại và

xâm nhập vào nhiều chương trình hơn. Giống như virus sinh học, virus máy tính cũng có khả năng sinh sôi.

II. Phân loại virus theo vùng bị nhiễm:

Các virus chương trình lây nhiễm các file chương trình, thường là các file có phần mở rộng .COM, .EXE, .SYS, .DLL, .OVL, hoặc SCR. Các chương trình thường bị nhiễm virus nhất là các chương trình DOS chuẩn sử dụng các phần mở rộng file .COM và .EXE. Các file chương trình là những vùng rất hấp dẫn đối với những người viết virus bởi vì chúng được sử dụng rộng rãi và có các dạng tương đối đơn giản mà virus dễ dàng xâm nhập vào.

Các virus khởi động lây nhiễm các vùng hệ thống gồm đĩa cứng và đĩa mềm. Đây là những vùng mà virus dễ dàng lây lan từ máy tính này sang máy tính khác. Các virus khởi động lây nhiễm sang các vùng với một mức độ cao hơn so với các virus chương trình.

Các virus macro lây nhiễm các file dữ liệu có các tính năng macro và là mối đe dọa mới nhất đối với người sử dụng máy tính. Chẳng hạn, các file template và tài liệu Microsoft Word rất dễ bị virus macro xâm nhập. Chúng lây lan một cách nhanh chóng khi các tài liệu bị nhiễm được dùng chung trên mạng và được tải xuống từ các site Internet.

III. Bàn về Exclusions

Norton AntiVirus sử dụng các hạng mục trong Exclusions List vào tất cả các hoạt động Wb mà nó thực hiện. Một exclusions là một điều kiện thường sẽ được tìm thấy, nhưng bạn đã yêu cầu Norton AntiVirus đừng kiểm tra đối với một file cụ thể.

Ghi chú

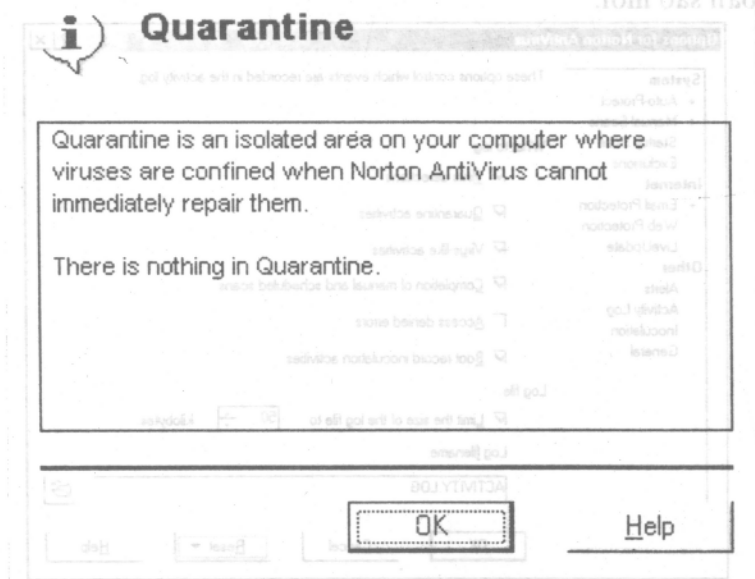
Nếu bạn di chuyển hay đặt lại tên một file, bạn đang tự động làm mất hiệu lực các phân loại bỏ của nó. Một trường hợp ngoại lệ là Include subfolders được chọn và file được di chuyển mà không đặt lại tên.

IV. Bàn về Norton AntiVirus Quarantine

Đôi khi Norton AntiVirus tìm thấy một loại virus chưa được biết đến và không thể loại bỏ bằng các virus hiện hành. Hoặc bạn có một file mà bạn nghĩ là nó bị nhiễm virus và chưa được tìm thấy. Bạn có thể chứa các file trong một vùng đặc biệt có tên là Quarantine. Các file trong Quarantine không thể tương tác với phần còn lại của hệ thống, vì vậy nếu chúng bị nhiễm, virus sẽ không lây lan. Từ Norton AntiVirus Quarantine, một file có thể được gửi trực tiếp qua Internet đến Symantec AntiVirus Research Center (SARC) để phân tích. SARC xác định file có bị nhiễm hay không. Nếu bị nhiễm, SARC báo cáo cho bạn biết kết quả. Nếu một virus mới được tìm thấy trong file mà bạn gửi đi, SARC sẽ tạo và gửi cho bạn các định nghĩa virus cập nhật để dò tìm và loại bỏ virus mới trên máy tính của bạn.

Bạn phải có một nối kết Internet để gửi một mẫu và một địa chỉ e-mail để nhận thông tin trả lời. Bạn được thông báo bằng e-mail về kết quả phân tích trong vòng bảy ngày.

System Status Details

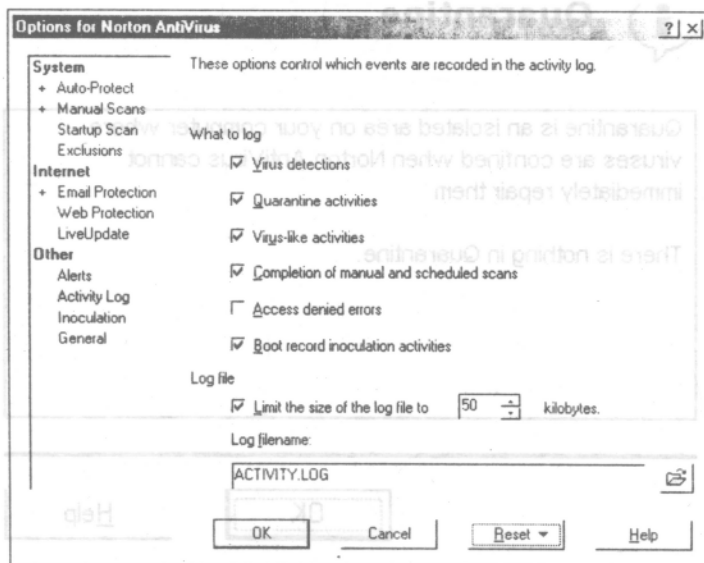


Ngoài các file trong Quarantine, Quarantine còn chứa hai nhóm hạng mục khác:

- ❖ Các hạng mục sao lưu dự phòng: Để bảo đảm an toàn dữ liệu, Norton AntiVirus được xác lập sẵn để tạo một bản sao lưu dự phòng của một file trước khi cố thực hiện việc sửa chữa. Các bản sao lưu dự phòng này cũng được chứa trong Quarantine. Sau khi file sửa chữa đã được xác nhận, bạn có thể xóa hạng mục bị nhiễm ra khỏi Quarantine.
- ❖ Các hạng mục đã được gửi đến SARC: Các file được gửi đến SARC để phân tích sẽ được cô lập. Sau khi nhận kết quả phân tích, bạn có thể xác định cần thực hiện điều gì với hạng mục.

V. Bàn về Activity Log

File Activity Log chứa các chi tiết về các hoạt động Norton AntiVirus, chẳng hạn như các sự cố được tìm thấy khi nào và các xử lý ra sao. Bạn có thể sử dụng Activity Log sau khi quét để tìm các file trên đĩa vẫn còn bị nhiễm và có thể cần được dò tìm và thay thế bằng các bản sao mới.



Từ hộp thoại Activity Log, bạn có thể:

- ❖ Nhấp Print để in Activity Log ra một máy in hay một file.
- ❖ Nhấp Filter để hiển thị các event nhất định, chẳng hạn như tất cả các phần dò tìm virus.

Ghi chú

Chỉ các hạng mục đang được hiển thị trong hộp danh sách mới được in. Nếu bạn đã lọc Activity Log thì chỉ các hạng mục được lọc mới được in.

- ❖ Nhấp Clear để xóa tất cả các hạng mục trong Activity Log.

Từ trang Activity Log trong hộp thoại Options, bạn có thể giới hạn hoặc tăng kích cỡ của Activity Log. Khi log đạt đến kích cỡ tối đa, nó bắt đầu ghi đè lên các hạng mục cũ nhất.

VI. Bàn về Repair Wizard

Norton AntiVirus có một Repair Wizard hướng dẫn bạn về các bước loại bỏ bất kỳ virus nào được tìm thấy trên máy tính trong suốt quá trình quét mà bạn khởi tạo hay lập thời biểu. Khi một virus được tìm thấy trong quá trình quét, Repair Wizard xuất hiện để nghị bạn chọn:

- ❖ Xử lý ngay tất cả virus.
- ❖ Xem các virus nào đã lây nhiễm máy tính của bạn và yêu cầu bạn xử lý hay loại bỏ các virus, mỗi lần một loại virus.
- ❖ Cách li các file bị nhiễm để gửi đến Symantec AntiVirus Research Center (SARC) để phân tích thêm.

Ngay sau khi Wizard đã thực hiện xong phần việc của nó, bạn nên luôn quét lại máy tính để bảo đảm tất cả virus đã được loại bỏ

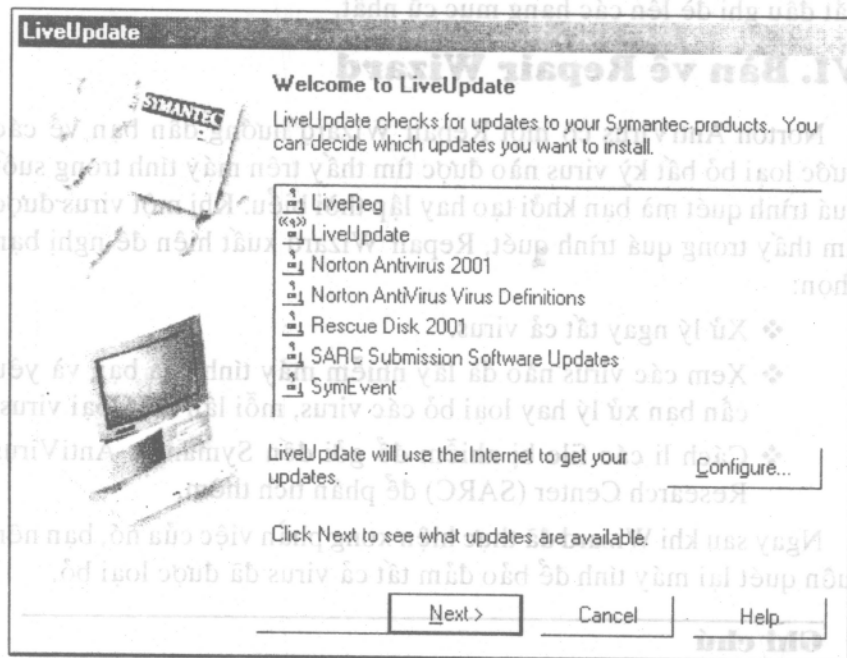
Ghi chú

Nếu bạn đã chọn để xóa các file mà chúng không thể được xử lý hay không có bản sao không bị nhiễm của file chương trình, bạn có thể nhận một bản sao thay thế từ nhà sản xuất. Nếu bạn không có bản sao không bị nhiễm của một file Microsoft .doc, .dot, hoặc .xls (vốn

có thể bị nhiễm bởi Macro Virus mới), bạn vẫn cần xóa file ra khỏi đĩa để tránh lây lan sang các file khác. Bạn nên tập thói quen cách giữ các đĩa gốc ở một nơi an toàn và thực hiện sao lưu dự phòng các file.

VII. Bàn về việc cập nhật các phần định nghĩa virus với LiveUpdate

Để ngăn chặn các virus mới xâm nhập vào máy tính, bạn phải thường xuyên cập nhật các file định nghĩa virus. Nếu máy tính của bạn được nối kết với Internet, và bạn đã chấp nhận các tùy chọn xác lập sẵn khi bạn cài đặt Norton AntiVirus, LiveUpdate tự động cập nhật đều đặn các file định nghĩa virus. Bạn cũng có thể lập thời biểu cho LiveUpdate để nó xảy ra vào bất kỳ thời điểm nào mà bạn chọn:



Ghi chú

Bạn cũng có thể tìm các file định nghĩa virus đã cập nhật trên nhiều hệ thống trực tuyến khác (nhấp More Info và chọn Sources For Updating Virus Definitions.) hay yêu cầu chúng bằng thư hoặc e-mail.

VIII. Những vùng mà virus lây nhiễm và không lây nhiễm

Một số virus máy tính làm hỏng dữ liệu trên các đĩa bằng cách phá hỏng các chương trình, xóa các file, hoặc thậm chí định dạng lại toàn bộ đĩa cứng. Tuy nhiên, phần lớn virus không gây hư hại gì cả; chúng chỉ sao chép hay hiển thị các thông báo.

Những vùng mà virus lây nhiễm:

- ❖ Các file chương trình khả thi, chẳng hạn như các chương trình xử lý văn bản, các chương trình trang bảng tính, hay các chương trình hệ điều hành.
- ❖ Các đĩa bằng cách xâm nhập vào các chương trình đặc biệt ở những vùng đĩa được gọi là record khởi động và record khởi động chính. Đây là các chương trình mà máy tính của bạn sử dụng để khởi động.
- ❖ Một file trước khi nó được gửi kèm với một thông báo e-mail, các đĩa dữ liệu và các đĩa được sử dụng để chuyển gửi các chương trình.

Những vùng mà virus không lây nhiễm:

- ❖ Phần cứng, chẳng hạn như bàn phím hay monitor. Mặc dù bạn có thể gặp những sự cố lạ chẳng hạn như sự biến dạng màn hình hay các ký tự không xuất hiện khi được gõ nhập, một virus chỉ lây nhiễm các chương trình điều khiển sự hiển thị hay bàn phím. Không phải các đĩa bị hư mà chỉ dữ liệu được lưu trữ trên chúng là bị phá hỏng. Các virus chỉ có thể lây nhiễm các file và làm hỏng dữ liệu.
- ❖ Các đĩa được bảo vệ ghi hay các thông báo e-mail dựa vào text.

Ghi chú

Norton AntiVirus cũng quét các tài liệu Microsoft Word và Excel khi quét các file chương trình. Mặc dù đây không phải là các file chương trình nhưng chúng có chứa mã và có thể bị nhiễm Macro Virus.

IX. Bàn về Virus List

Bạn có thể biết Norton AntiVirus đã tìm thấy các virus nào bằng cách xem danh sách các tên virus. Bạn cũng có thể xem các phần mô tả về các virus cụ thể, bao gồm các triệu chứng và các bí danh của chúng.

Để ngăn chặn các virus vừa mới phát hiện xâm nhập vào máy tính, bạn nên cập nhật đều đặn các file định nghĩa virus. Norton AntiVirus sử dụng thông tin trong các file định nghĩa virus để dò tìm virus trong quá trình quét. Các file định nghĩa virus đã cập nhật thường có sẵn qua LiveUpdate. Bạn có thể lập thời biểu cập nhật tự động vào bất kỳ lúc nào bạn muốn. Ngay sau khi các file định nghĩa virus đã cập nhật được cài đặt, bạn sẽ nhìn thấy các tên virus mới trong Virus List.

Bài 2

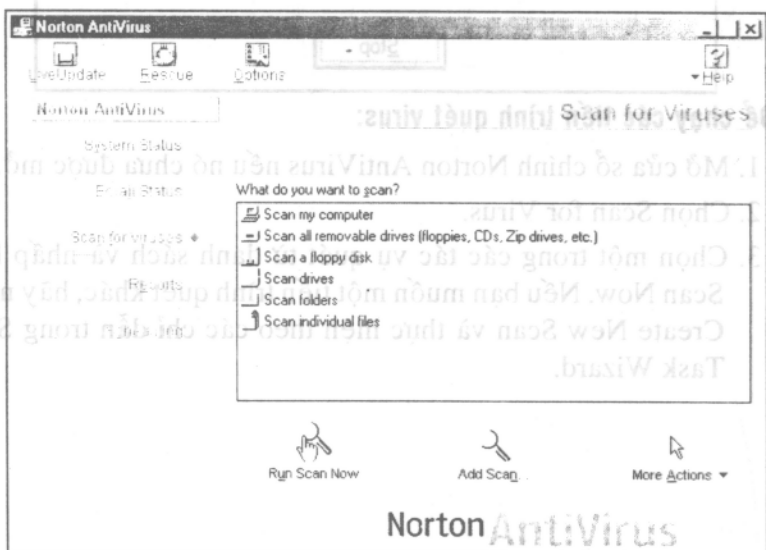
CÁC TÁC VỤ QUAN TRỌNG TRONG NORTON ANTIVIRUS

Trong bài này, chúng ta sẽ học các tác vụ quan trọng nhất mà Norton AntiVirus giúp bạn thực hiện.

I. Quét để tìm virus trên máy tính

Để tìm virus trên máy tính của bạn, hãy thực hiện một trong các thao tác sau đây:

- ❖ Khởi chạy tiến trình quét virus bằng cách mở cửa sổ chính Norton AntiVirus, chọn Scan for Viruses, chọn một tác vụ quét từ danh sách, và nhấp Run Scan Now.

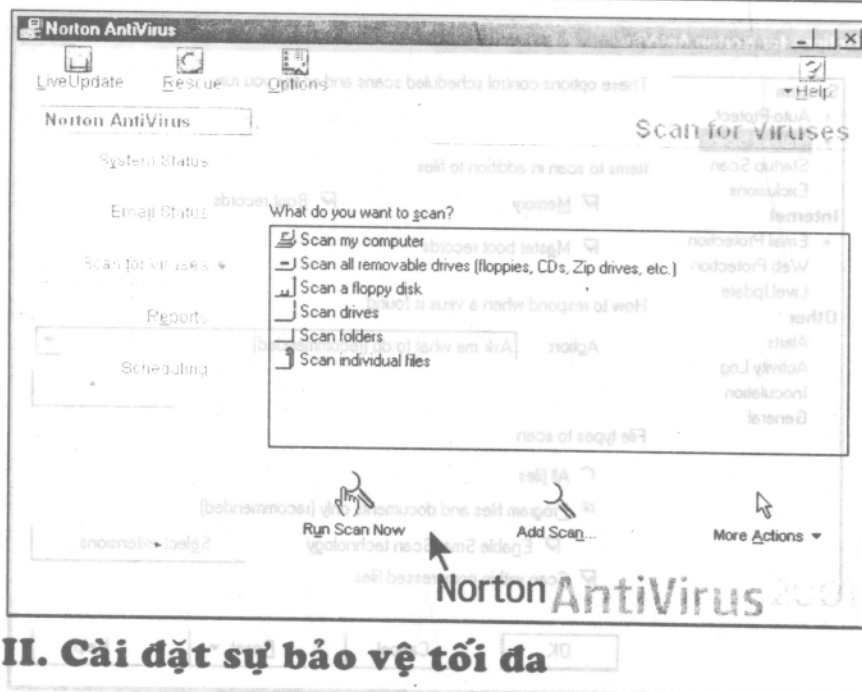


- ❖ Tạo một tác vụ quét mới bằng cách mở cửa sổ chính Norton AntiVirus, chọn Scan for Viruses, và nhấn Create New Scan. Sau đó thực hiện theo các chỉ dẫn trong Scan Task Wizard.



Để chạy các tiến trình quét virus:

1. Mở cửa sổ chính Norton AntiVirus nếu nó chưa được mở.
2. Chọn Scan for Virus.
3. Chọn một trong các tác vụ quét từ danh sách và nhấn Run Scan Now. Nếu bạn muốn một tiến trình quét khác, hãy nhấn Create New Scan và thực hiện theo các chỉ dẫn trong Scan Task Wizard.



II. Cài đặt sự bảo vệ tối đa

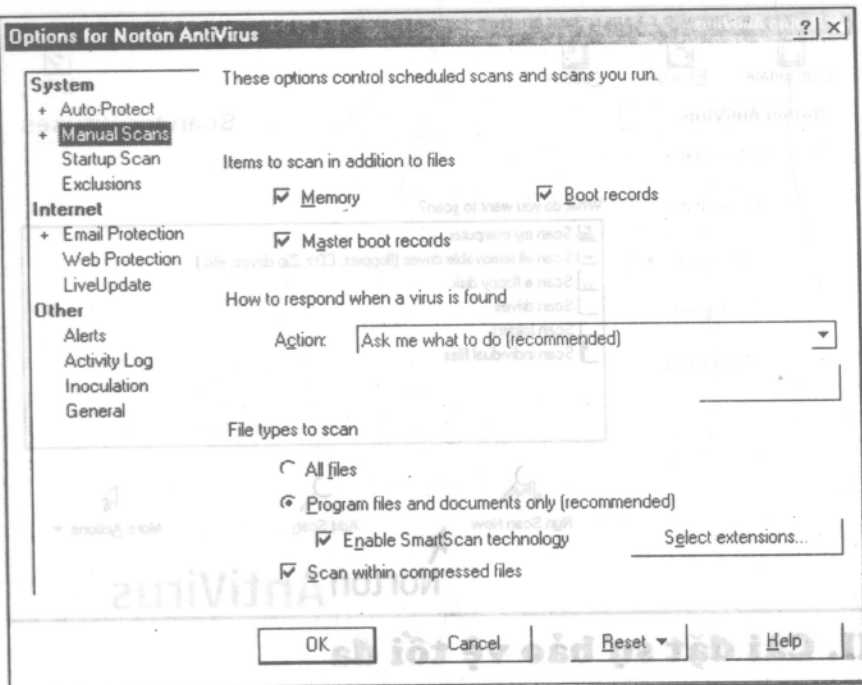
Khi bạn cài đặt Norton AntiVirus với các tùy chọn đã được xác lập sẵn, máy tính của bạn được bảo vệ tự động để tránh các virus đã biết và chưa biết, cảnh báo bạn bất kỳ khi nào một virus được tìm thấy. Tuy nhiên, bạn có thể tăng sự bảo vệ bằng cách thực hiện các thao tác sau đây:

- ❖ Tạo tùy biến các xác lập để bảo vệ tối đa
- ❖ Lập thời biểu quét virus
- ❖ Lập thời biểu LiveUpdate

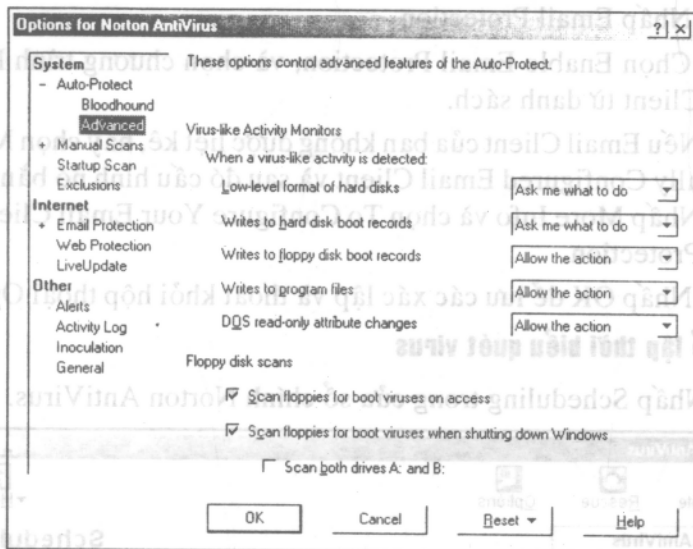
Nếu bạn có một nối kết Internet và đã chấp nhận các tùy chọn xác lập sẵn khi bạn cài đặt, bạn sẽ nhận đều đặn các trình cập nhật file mà Norton AntiVirus cần bảo vệ thường xuyên để tránh virus.

1. Để tạo tùy biến các xác lập cho việc bảo vệ tối đa

1. Nhấp Options trên cửa sổ Norton AntiVirus.
2. Nhấp Manual Scans nếu nó chưa được chọn.

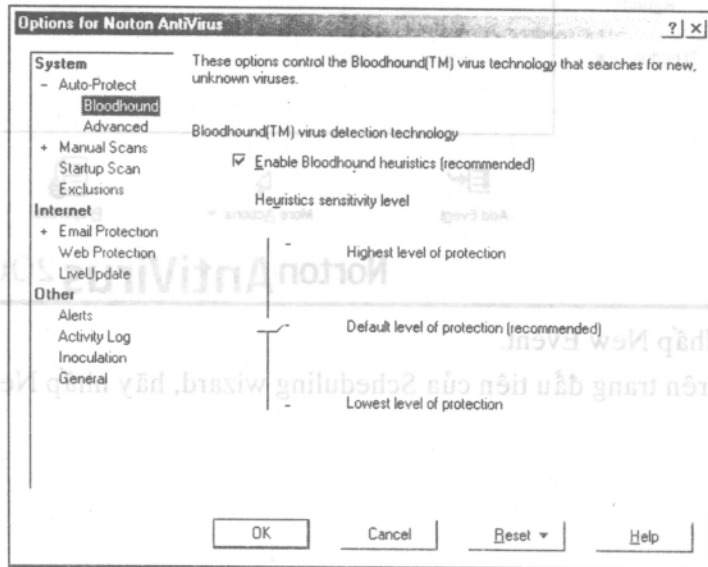


3. Bảo đảm All Files được chọn dưới File Types To Scan.
4. Bảo đảm Ask Me What To Do được chọn trong hộp danh sách How To Respond When A Virus Is Found.
5. Nhấp Auto-Protect.
6. Kiểm tra tất cả các tùy chọn dưới Scan Files When They Are (chúng được bật theo mặc định).
7. Nhấp vào dấu cộng ở kế bên Auto-Protect.
8. Nhấp Advanced.
9. Nhấp Ask Me What To Do trong mỗi hộp danh sách xổ xuống Virus-Like Activity Monitors.



10. Kiểm tra tất cả các tùy chọn dưới Floppy Disk Scans.

11. Nhấp Bloodhound, và sau đó di chuyển thanh slider lên phía trên để tăng cấp độ dò tìm đối với các virus chưa được biết đến.



12. Nhấp Email Protection.

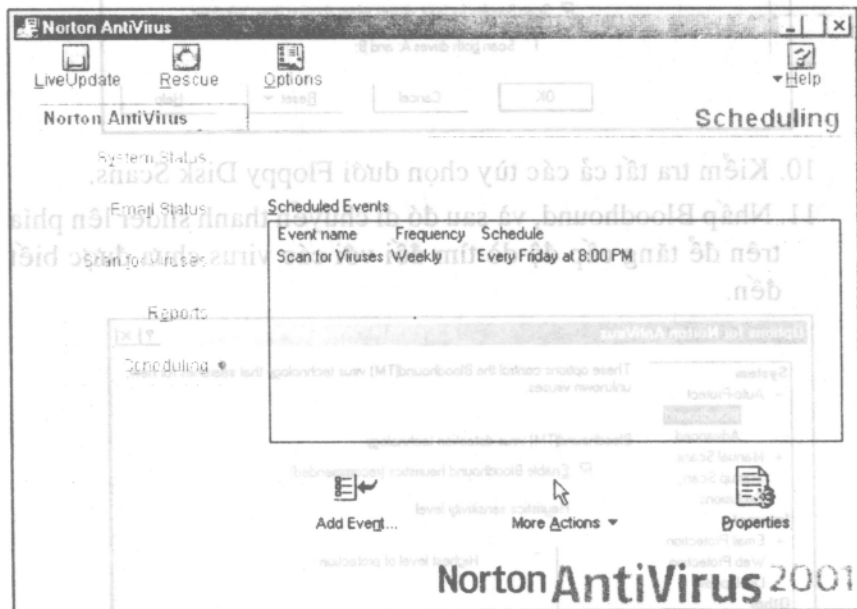
13. Chọn Enable Email Protection, và chọn chương trình Email Client từ danh sách.

Nếu Email Client của bạn không được liệt kê, hãy chọn Manually Configured Email Client và sau đó cấu hình nó bằng tay. Nhấp More Info và chọn To Configure Your Email Client for Protection.

14. Nhấp OK để lưu các xác lập và thoát khỏi hộp thoại Option.

2. Để lập thời biểu quét virus

1. Nhấp Scheduling trong cửa sổ chính Norton AntiVirus.



2. Nhấp New Event.

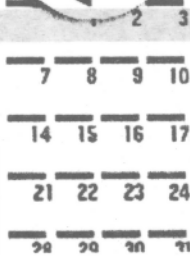
3. Trên trang đầu tiên của Scheduling wizard, hãy nhấp Next.

Norton AntiVirus Scheduling Wizard



Welcome to the Norton AntiVirus Scheduling Wizard. This wizard will help you to schedule virus scans and virus protection updates.

To begin scheduling an event, click Next.



Next >

Cancel

4. Chọn Schedule A Virus Scan.

Norton AntiVirus Scheduling Wizard



Select the type of event you would like to schedule, and then click Next.

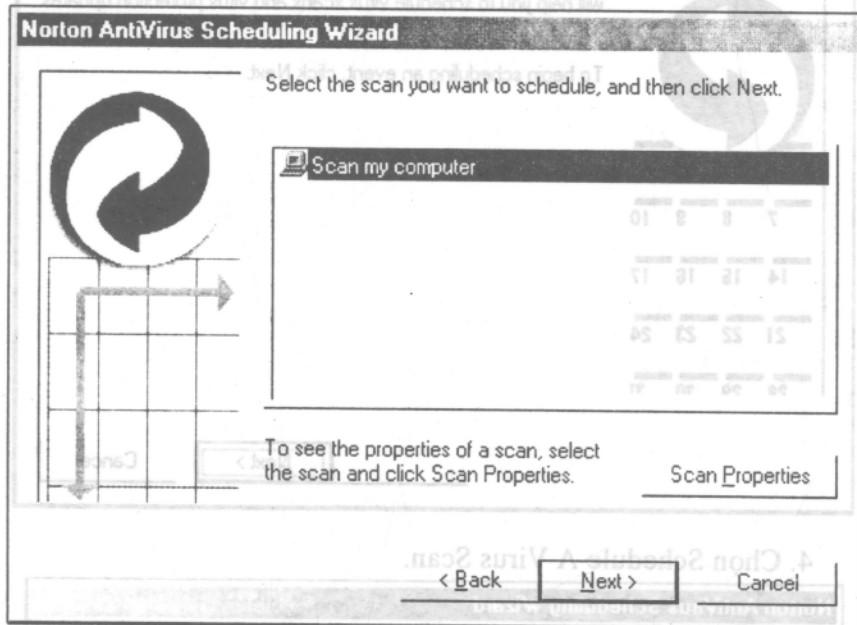
- ☒ Schedule a virus scan
- ☐ Schedule LiveUpdate to update your virus protection
- ☐ Schedule another program to run
- ☐ Schedule a message to be displayed

< Back

Next >

Cancel

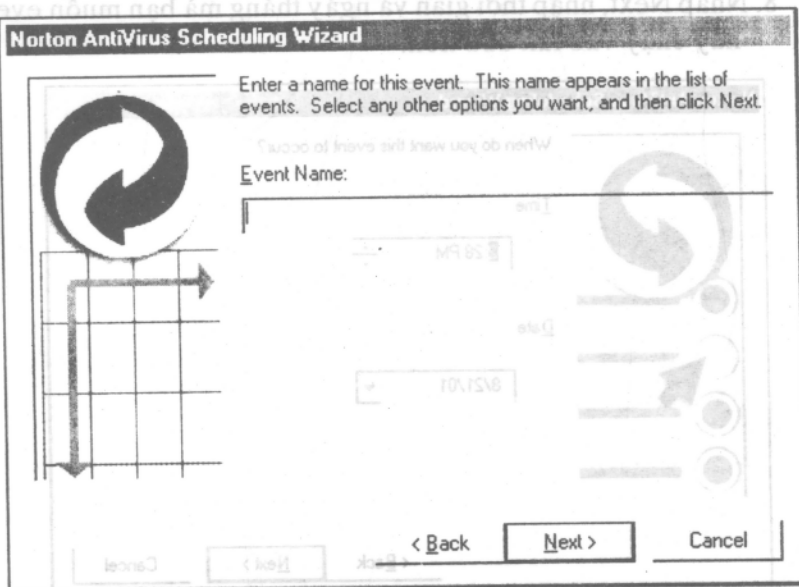
5. Nhấp Next và chọn tác vụ quét mà bạn muốn từ danh sách. Nếu bạn không nhìn thấy tác vụ quét mà bạn muốn lập thời biểu, bạn sẽ cần xác định một tác vụ mới.



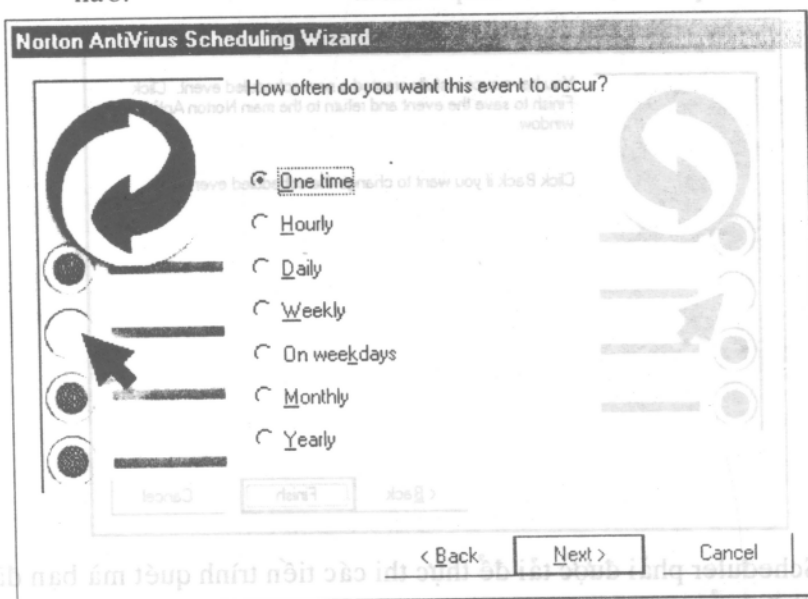
6. Nhấp Next và nhập một nội dung mô tả ngắn gọn vào hộp text Description.

Nội dung này sẽ xuất hiện trong hộp danh sách Event trong cửa sổ chính Scheduler.

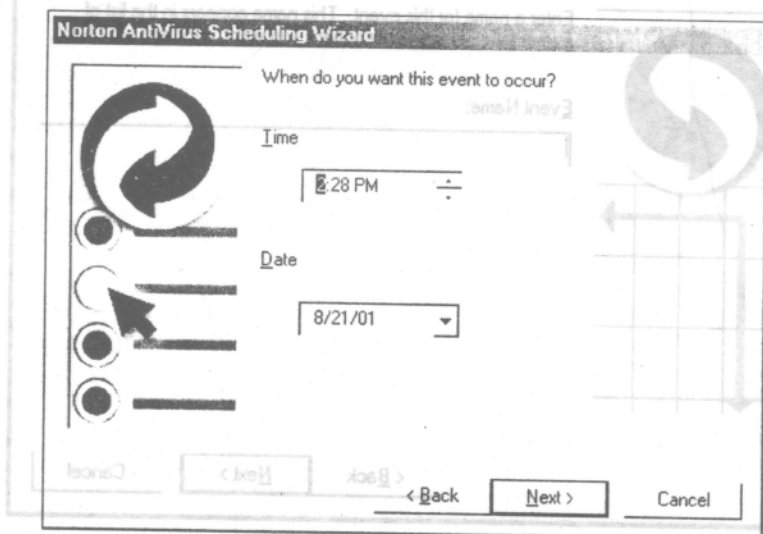




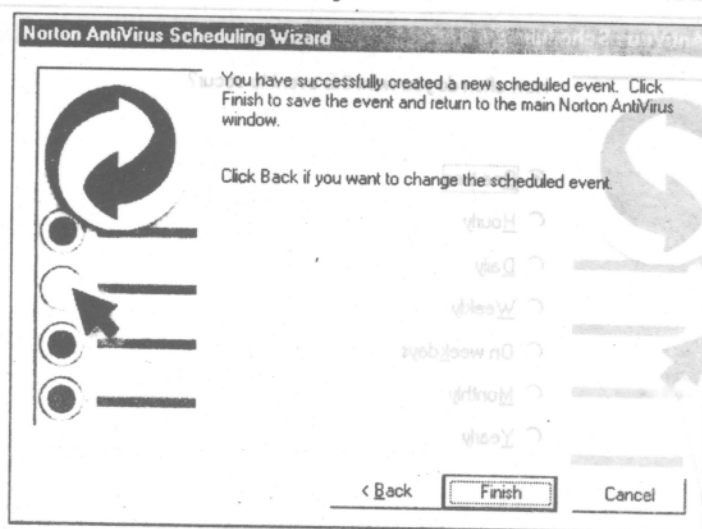
7. Nhấp Next và chọn bạn muốn quét thường xuyên như thế nào.



8. Nhấp Next, nhập thời gian và ngày tháng mà bạn muốn event này chạy vào lần đầu tiên.



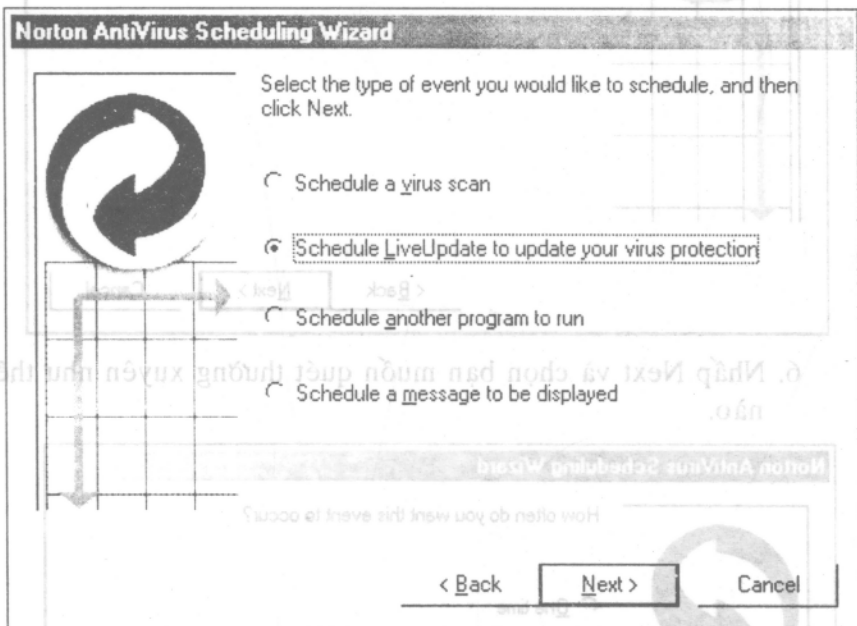
9. Nhấp Next, sau đó nhấp Finish.



Scheduler phải được tải để thực thi các tiến trình quét mà bạn đã lập thời biểu.

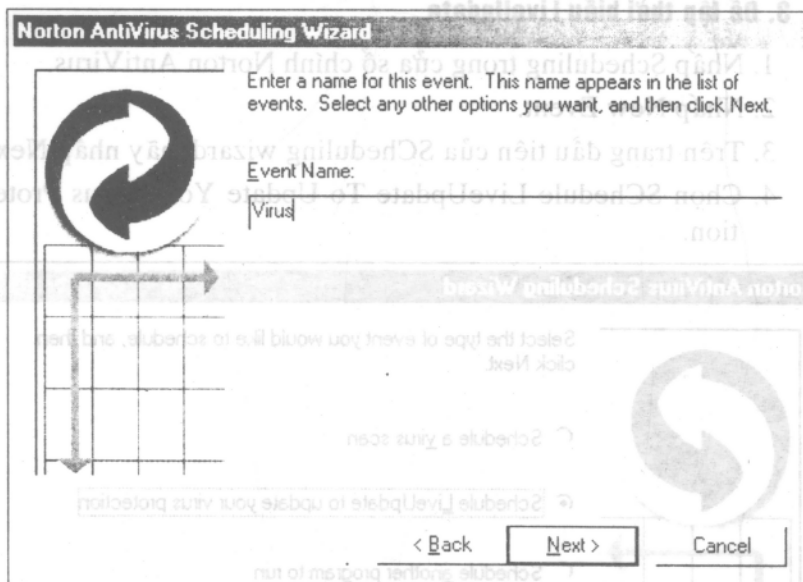
3. Để lập thời biểu LiveUpdate

1. Nhấp Scheduling trong cửa sổ chính Norton AntiVirus.
2. Nhấp New Event.
3. Trên trang đầu tiên của Scheduling wizard, hãy nhấp Next.
4. Chọn Schedule LiveUpdate To Update Your Virus Protection.

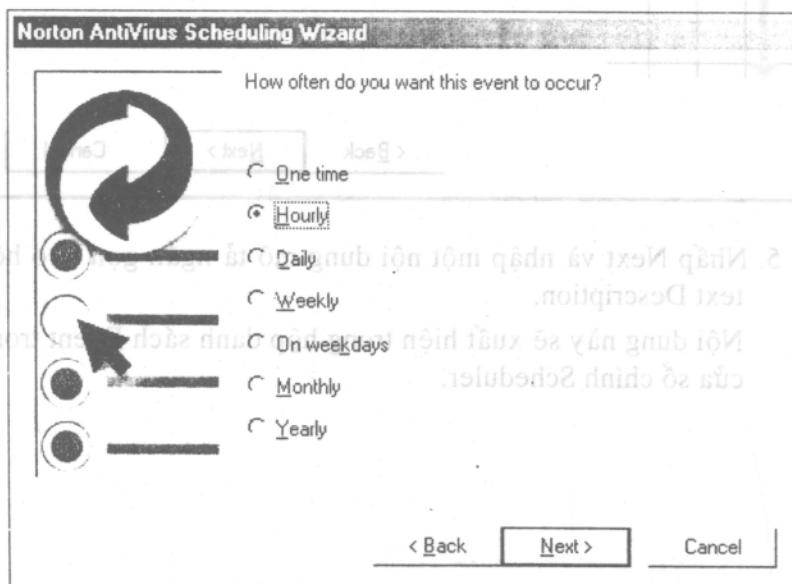


5. Nhấp Next và nhập một nội dung mô tả ngắn gọn vào hộp text Description.

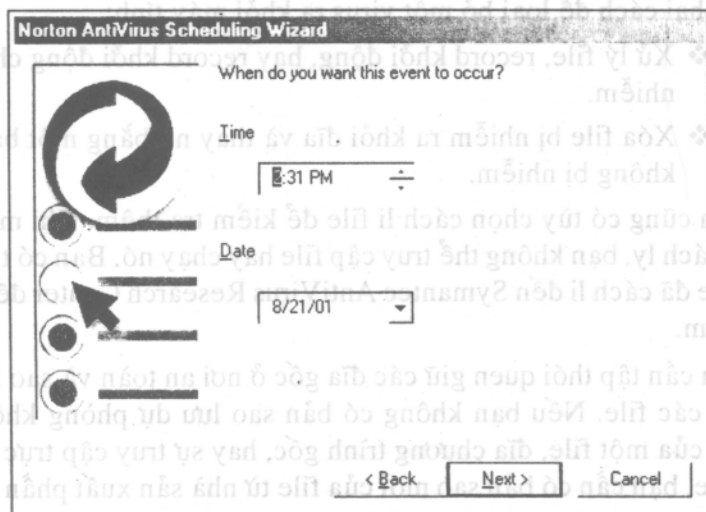
Nội dung này sẽ xuất hiện trong hộp danh sách Event trong cửa sổ chính Scheduler.



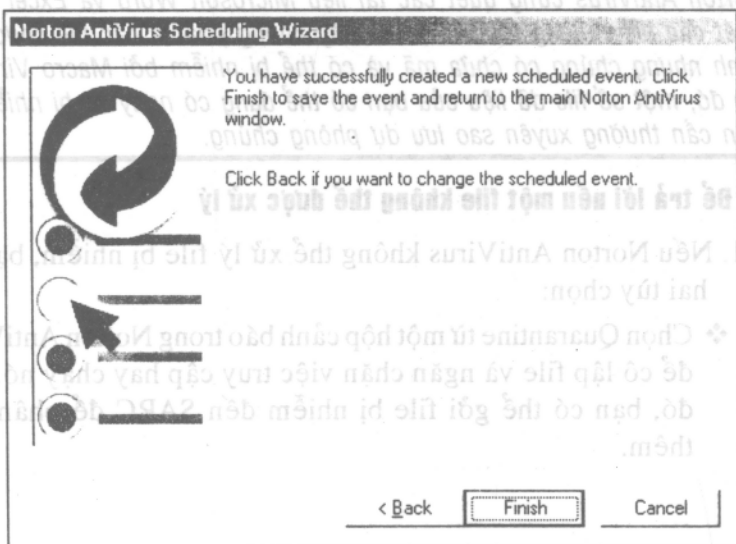
6. Nhấp Next và chọn bạn muốn quét thường xuyên như thế nào.



7. Nhấp Next, nhập thời gian và ngày tháng mà bạn muốn Event này chạy vào lần đầu tiên.



8. Nhấp Next, sau đó nhấp Finish



Scheduler phải đang chạy để thực thi các tiến trình Web mà bạn đã lập thời biểu.

III. Loại bỏ virus ra khỏi máy tính

Có hai cách để loại bỏ một virus ra khỏi máy tính:

- ❖ Xử lý file, record khởi động, hay record khởi động chính bị nhiễm.
- ❖ Xóa file bị nhiễm ra khỏi đĩa và thay nó bằng một bản sao không bị nhiễm.

Bạn cũng có tùy chọn cách li file để kiểm tra thêm. Khi một file được cách ly, bạn không thể truy cập file hay chạy nó. Bạn có thể gửi các file đã cách li đến Symantec AntiVirus Research Center để kiểm tra thêm.

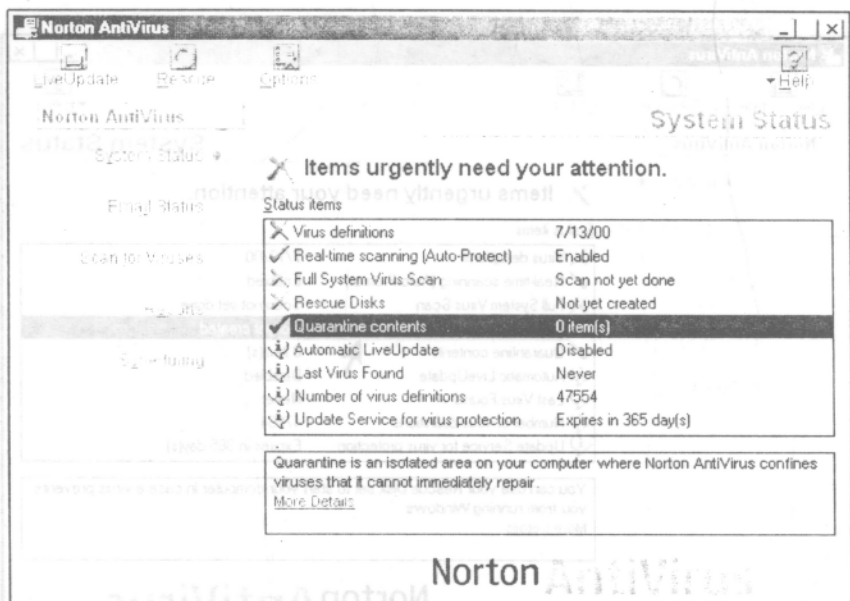
Bạn cần tập thói quen giữ các đĩa gốc ở nơi an toàn và sao lưu dự phòng các file. Nếu bạn không có bản sao lưu dự phòng không bị nhiễm của một file, đĩa chương trình gốc, hay sự truy cập trực tuyến vào file, bạn cần có bản sao mới của file từ nhà sản xuất phần mềm.

Ghi chú

Norton AntiVirus cũng quét các tài liệu Microsoft Word và Excel khi quét các file chương trình. Mặc dù đây không phải là các file chương trình nhưng chúng có chứa mã và có thể bị nhiễm bởi Macro Virus. Do đó, một số file dữ liệu của bạn có thể đang có nguy cơ bị nhiễm. Bạn cần thường xuyên sao lưu dự phòng chúng.

1. Để trả lời nếu một file không thể được xử lý

1. Nếu Norton AntiVirus không thể xử lý file bị nhiễm, bạn có hai tùy chọn:
 - ❖ Chọn Quarantine từ một hộp cảnh báo trong Norton AntiVirus để cô lập file và ngăn chặn việc truy cập hay chạy nó. Sau đó, bạn có thể gửi file bị nhiễm đến SARC để phân tích thêm.

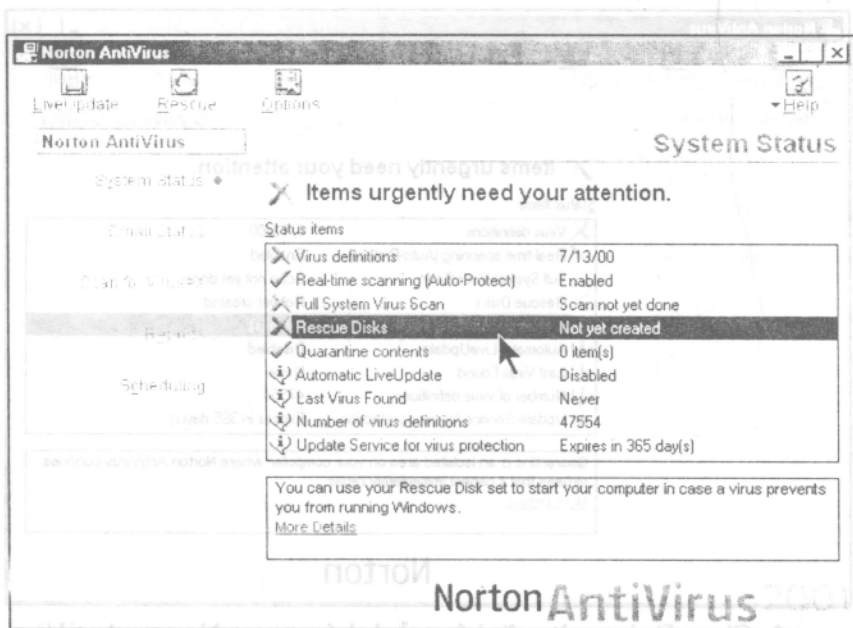


❖ Chọn Delete từ một hộp cảnh báo trong Norton AntiVirus hoặc xóa file bằng tay tra khỏi đĩa cứng hay đĩa mềm từ trong Windows hoặc DOS.

2. Thay file bằng một bản sao không bị nhiễm, hãy sao chép hoặc cài đặt lại file từ các đĩa của nhà sản xuất ban đầu.

2. Để trả lời nếu Norton AntiVirus không thể xử lý thành công record khởi động chính hay một record khởi động trên đĩa cứng của bạn:

Sử dụng Rescue Boot Disk đã được ghi bảo vệ để phục hồi các record khởi động trở lại trạng thái không bị nhiễm.



Nếu Norton AntiVirus không thể xử lý thành công một record khởi động trên một đĩa mềm:

- ❖ Hãy sao chép bất kỳ file quan trọng nào từ đĩa mềm sang một đĩa khác. Đĩa mềm vẫn bị nhiễm và bạn không thể khởi động từ đĩa đó.

3. Để trả lời nếu Norton AntiVirus không thể xử lý thành công một hệ thống file:

1. Khởi động lại máy tính bằng cách sử dụng đĩa khởi động Windows 95/98 mà bạn đã tạo khi cài đặt Windows 95/98.
2. Từ dòng nhắc A, hãy gõ nhập Sys C: và nhấn Enter.
 Thao tác này sẽ ghi đè lên record khởi động trên ổ đĩa C và các file hệ thống.
3. Khi dòng nhắc A hiển thị, hãy lấy đĩa ra và khởi động máy tính với lệnh Ctrl+Alt+Del hoặc tắt máy và sau đó bật nó trở lại.

Ghi chú

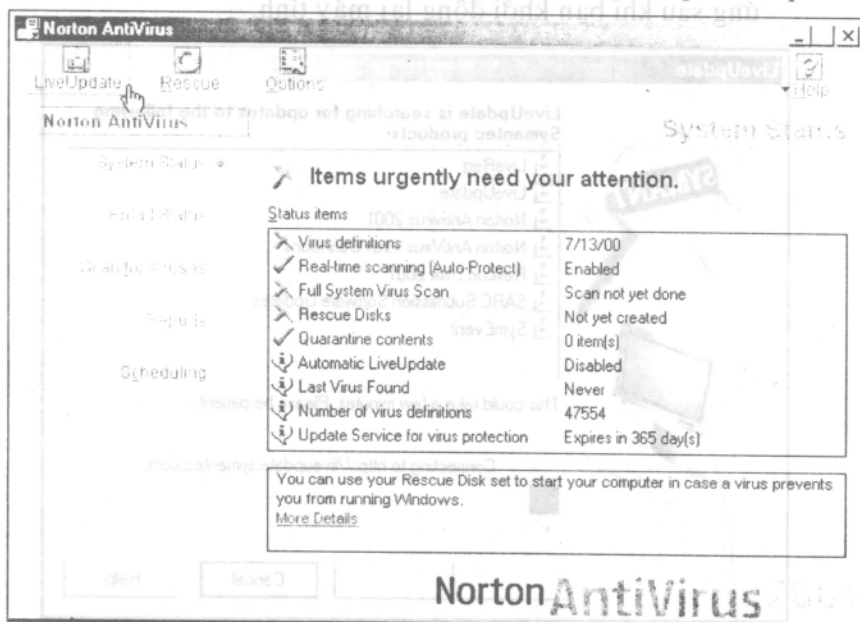
Nếu Win.com bị nhiễm, bạn có thể phải sao chép file bằng tay từ đĩa sang folder thích hợp trên ổ đĩa cứng.

4. Để trả lời một cảnh báo Norton AntiVirus

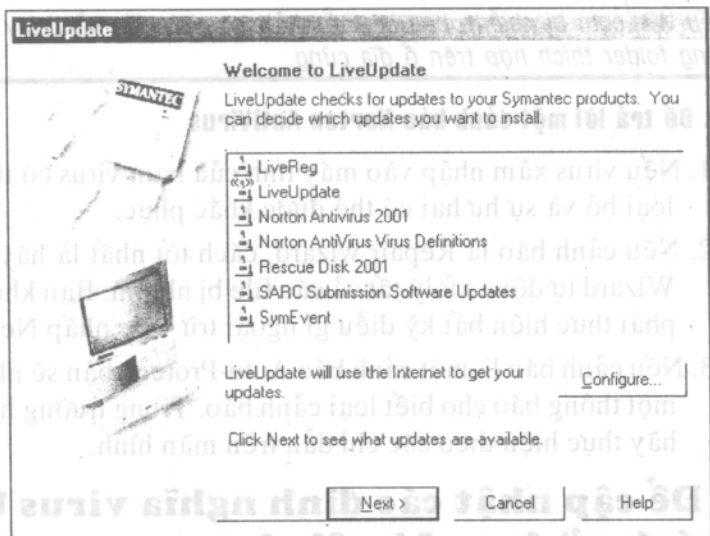
1. Nếu virus xâm nhập vào máy tính của bạn, virus có thể được loại bỏ và sự hư hại có thể được khắc phục.
2. Nếu cảnh báo là Repair wizard, cách tốt nhất là hãy để cho Wizard tự động xử lý tất cả các file bị nhiễm. Bạn không cần phải thực hiện bất kỳ điều gì ngoại trừ việc nhấp Next.
3. Nếu cảnh báo là một cảnh báo Auto-Protect, bạn sẽ nhìn thấy một thông báo cho biết loại cảnh báo. Trong trường hợp này, hãy thực hiện theo các chỉ dẫn trên màn hình.

IV. Để cập nhật các định nghĩa virus bằng cách sử dụng LiveUpdate

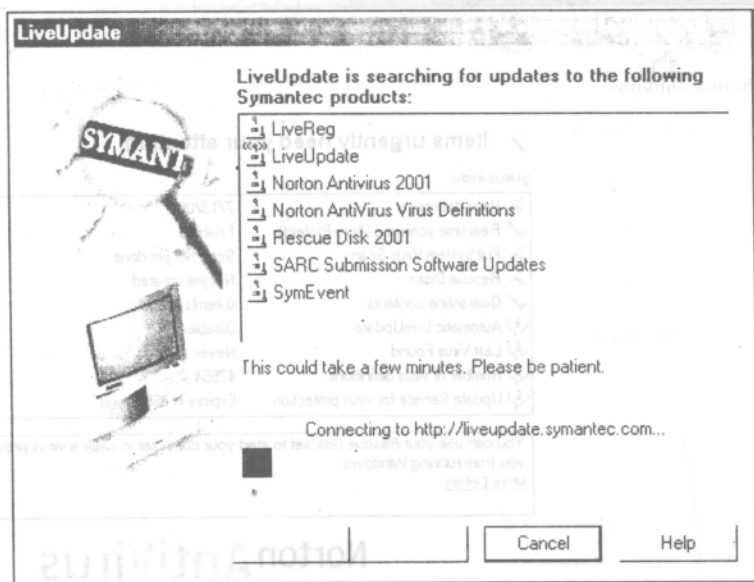
1. Trong cửa sổ chính Norton AntiVirus, hãy nhấp LiveUpdate.



2. Nhấp Next và thực hiện theo các chỉ dẫn trên màn hình.



Các file định nghĩa virus mới được cài đặt tự động và đạt hiệu ứng sau khi bạn khởi động lại máy tính.



Ghi chú

Nếu bạn không có sự truy cập vào Internet, bạn có thể đặt các đĩa cập nhật định nghĩa virus của symantec bằng email.

1. Bể cập nhật virus mới:

Ghi chú

Nếu không cập nhật thường xuyên, máy tính của bạn không được bảo vệ hoàn toàn. Nếu máy tính của bạn được nối kết với Internet, và nếu bạn đã chấp nhận tùy chọn xác lập sẵn khi bạn cài đặt Norton AntiVirus, bạn sẽ tự động nhận các LiveUpdate đã lập thời biểu sẵn.

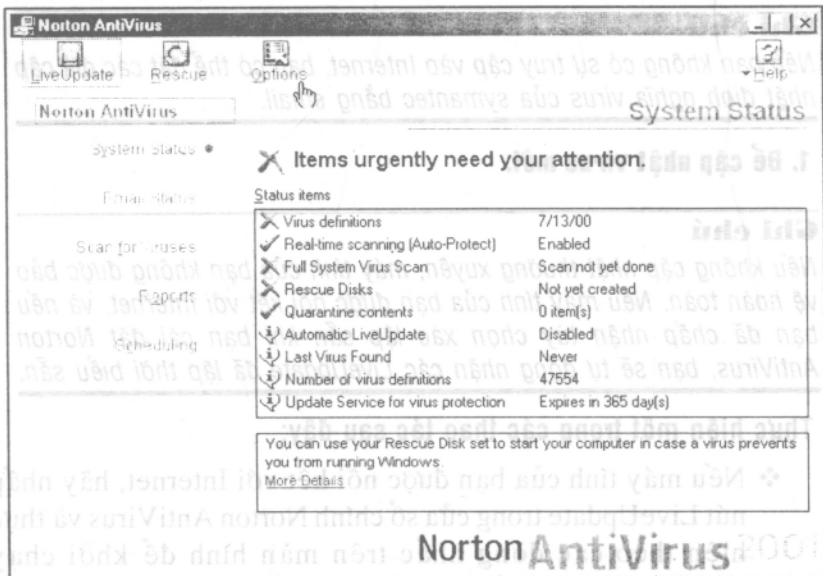
Thực hiện một trong các thao tác sau đây:

- ❖ Nếu máy tính của bạn được nối kết với Internet, hãy nhấp nút LiveUpdate trong cửa sổ chính Norton AntiVirus và thực hiện theo các dòng nhắc trên màn hình để khởi chạy LiveUpdate vào bất kỳ lúc nào mà bạn chọn.
- ❖ Nếu máy tính của bạn được nối kết Internet, hãy giữ cho các LiveUpdate tự động được bật.
- ❖ Nếu bạn không có một modem hay nối kết Internet, hãy đặt các đĩa cập nhật đĩa virus của Symantec qua thư.

Thực hiện theo các chỉ dẫn về cập nhật mà bạn nhận được.

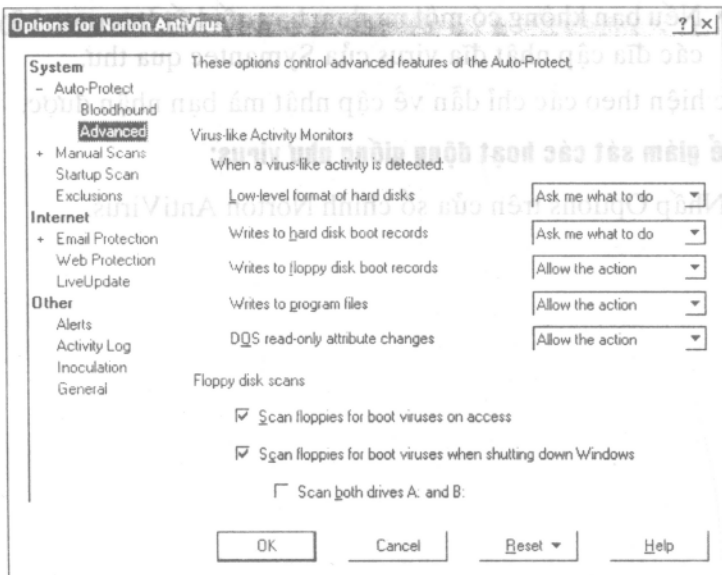
2. Bể giám sát các hoạt động giống như virus:

1. Nhấp Options trên cửa sổ chính Norton AntiVirus.



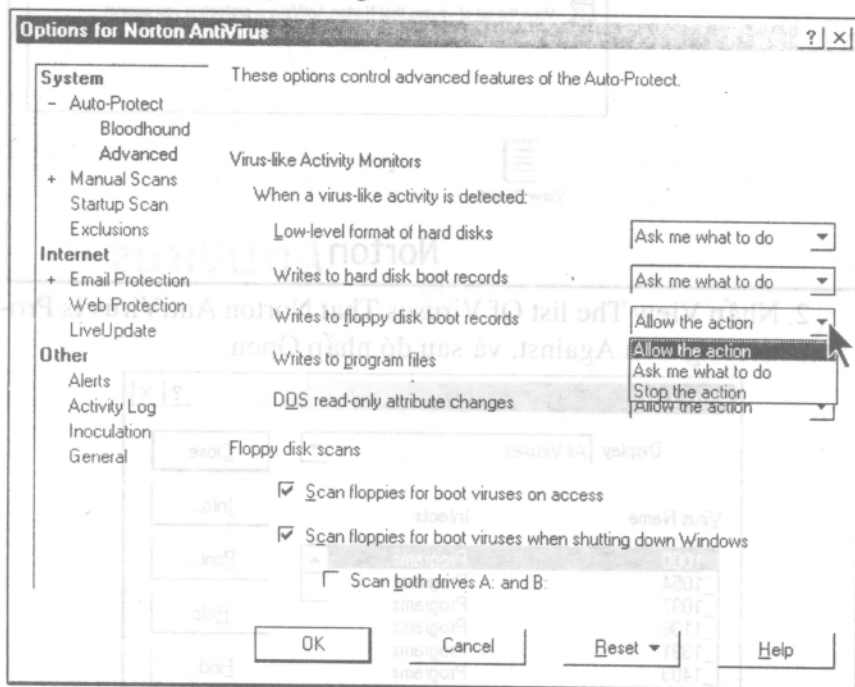
2. Nhấp vào dấu cộng ở kế bên Auto-Protect.

3. Nhấp Advanced.



4. Nhấp vào một tùy chọn trong mỗi hộp danh sách xổ xuống để chỉ định Norton AntiVirus nên thực hiện điều gì khi nó tìm thấy hoạt động giống như virus.

Tùy chọn đã xác lập sẵn cho một số hoạt động là Allow The Action. Để xác lập một mức độ bảo vệ cao hơn, hãy nhấp Ask Me What To Do. Tùy chọn này cung cấp cho bạn các tùy chọn Continue, Stop, hoặc Exclude mỗi khi hoạt động xảy ra. Nói cách khác, bạn có thể xác định việc có nên chấp nhận hoạt động hay không.

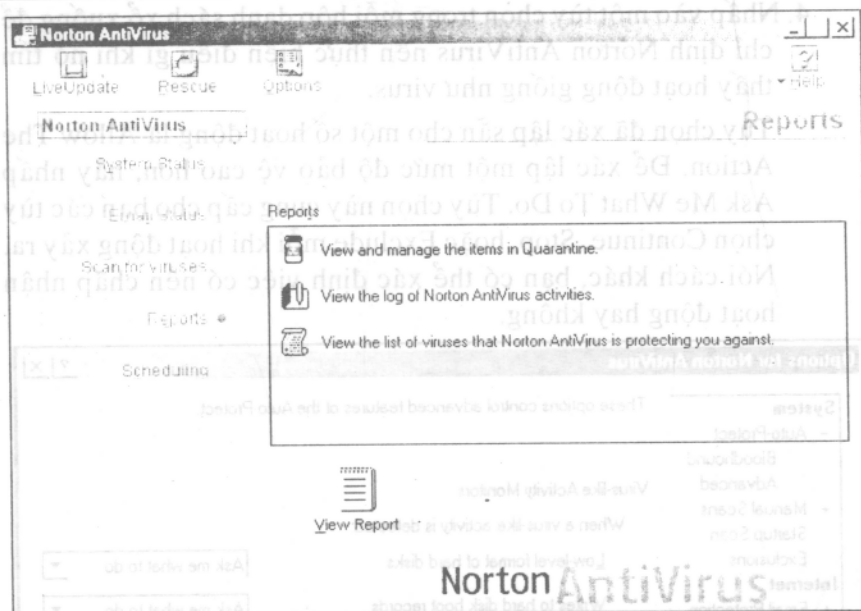


5. Nhấp OK để lưu các xác lập và đóng hộp thoại Options.

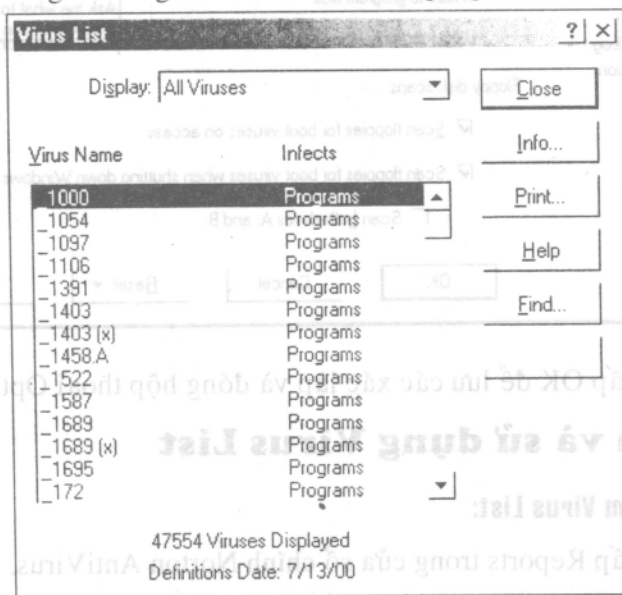
V. Tìm và sử dụng Virus List

1. Để tìm Virus List:

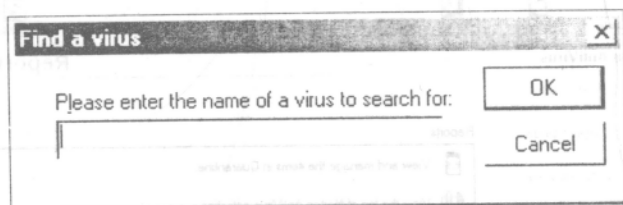
1. Nhấp Reports trong cửa sổ chính Norton AntiVirus.



2. Nhấp View The list Of Viruses That Norton AntiVirus Is Protecting You Against, và sau đó nhấp Open.



3. Nhấp Find. Hộp thoại Find A Virus được mở.



4. Bắt đầu nhập tên hay một phần của tên virus mà bạn muốn tìm, và sau đó nhấp OK.

Virus đầu tiên trong danh sách phù hợp với tiêu chuẩn tìm kiếm của bạn sẽ được chọn trong danh sách.

5. Nhấp Find Next để tìm hạng mục kế tiếp trong danh sách phù hợp với tiêu chuẩn tìm của bạn.

Ghi chú

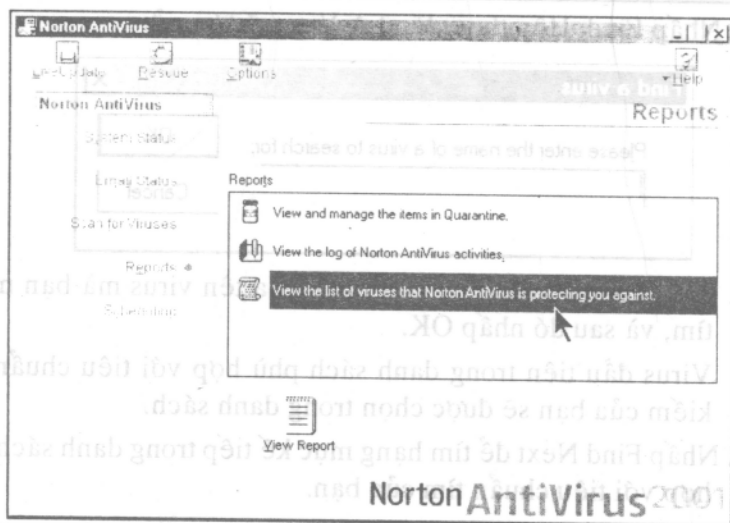
Để giảm số lượng virus mà bạn phải tìm, hãy chọn một loại virus từ hộp danh sách Display. Chẳng hạn, bạn có thể muốn lập virus list để hiển thị chỉ các virus khởi động hay các virus macro.

Nếu một virus không được tìm thấy trên danh sách, tên virus có thể khác với tên mà bạn nghĩ. Chẳng hạn, virus thường được gọi là Michelangelo được gọi là Stoned. Michelangelo.D.

2. Để sử dụng Virus List

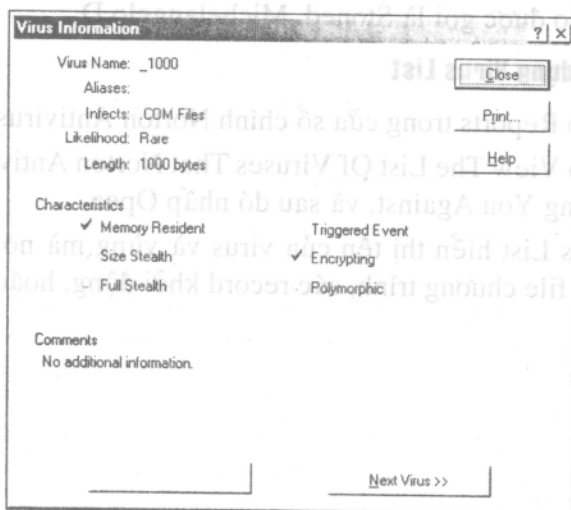
1. Nhấp Reports trong cửa sổ chính Norton Antivirus.
2. Nhấp View The List Of Viruses That Norton Antivirus Is Protecting You Against, và sau đó nhấp Open.

Virus List hiển thị tên của virus và vùng mà nó lây nhiễm (các file chương trình, các record khởi động, hoặc cả hai).

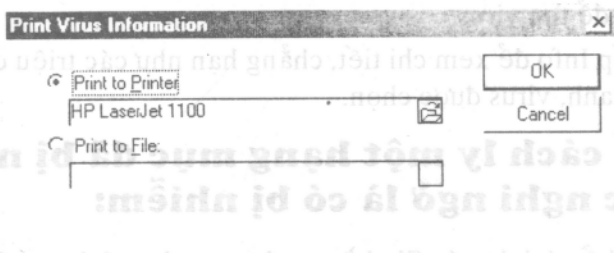


3. Sử dụng bất kỳ một trong các tùy chọn sau đây để quản lý Virus List:

- ❖ Chọn một hạng mục từ hộp danh sách sổ xuống Display để xem các loại virus khác nhau.
- ❖ Nhấp Info để xem các chi tiết, chẳng hạn như các triệu chứng và bí danh, về một loại virus cụ thể.



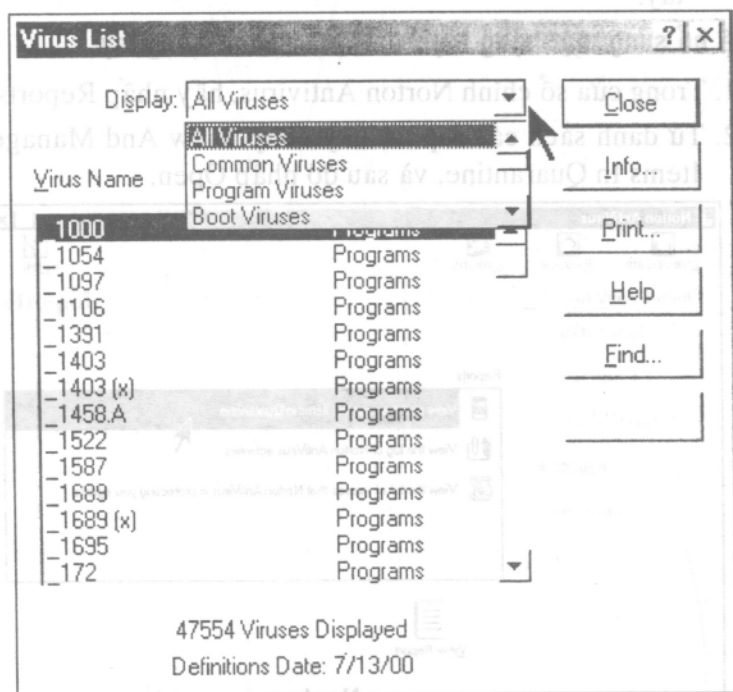
- ❖ Nhấp Print để in Virus List ra một máy in hoặc ra một file.



VI. Hiện thị thông tin về một virus

1. Nhấp Report trong cửa sổ chính Norton Antivirus.
2. Nhấp View The List Of Viruses That Norton Antivirus Is Protecting You Against, và sau đó nhấp Open.

Virus List hiển thị tên của virus và vùng mà nó lây nhiễm (các file chương trình, các record khởi động, hoặc cả hai).



3. Chọn virus mà bạn quan tâm trên danh sách, hoặc sử dụng file để tìm virus.
4. Nhấp Info để xem chi tiết, chẳng hạn như các triệu chứng và bí danh, virus được chọn.

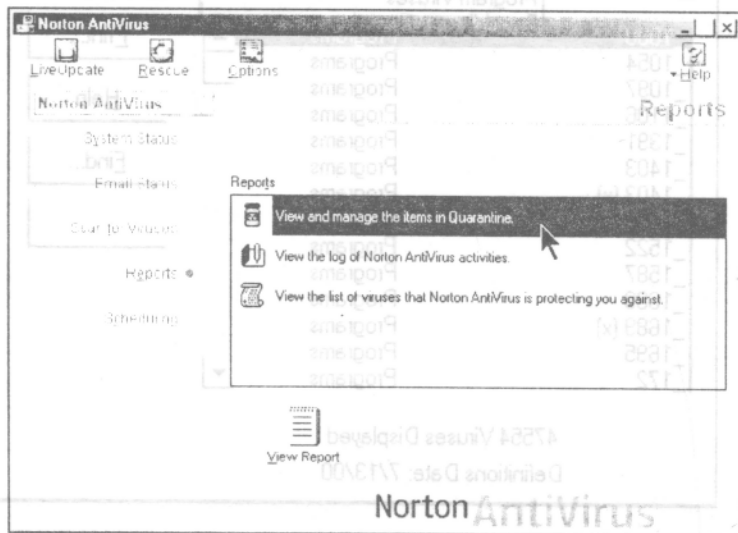
VII. Để cách ly một hạng mục đã bị nhiễm hoặc nghi ngờ là có bị nhiễm:

Bạn có thể cách ly các file bằng một trong ba cách sau đây:

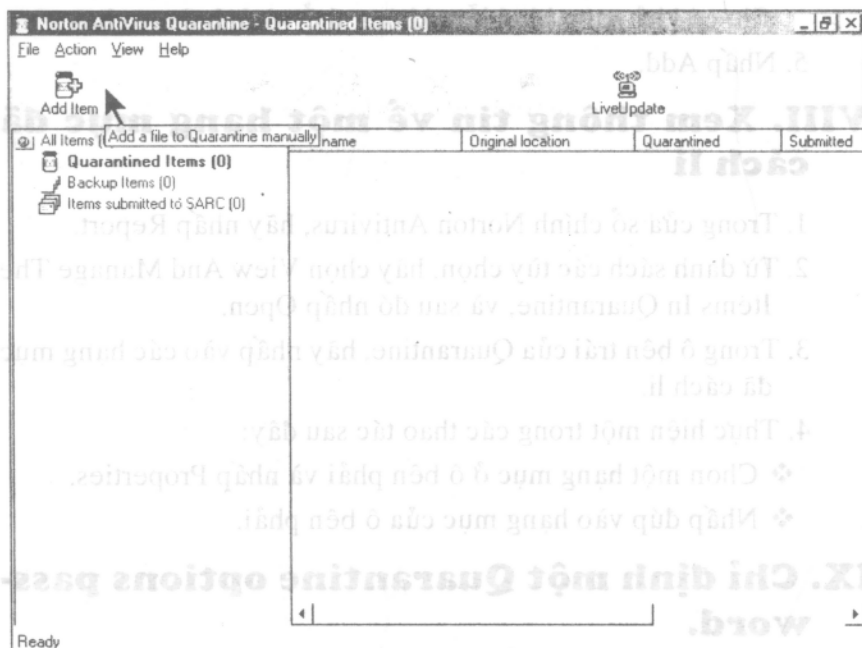
- ❖ Chọn Quarantine sau khi nhận một cảnh báo Norton Antivirus.
- ❖ Cấu hình Norton Antivirus để cách ly các hạng mục thay vì xử lý chúng hoặc cách ly chúng nếu chúng không thể được xử lý.
- ❖ Bổ sung một file nghi ngờ có bị nhiễm vào Quarantine bằng tay.

Để bổ sung một hạng mục vào Quarantine bằng tay:

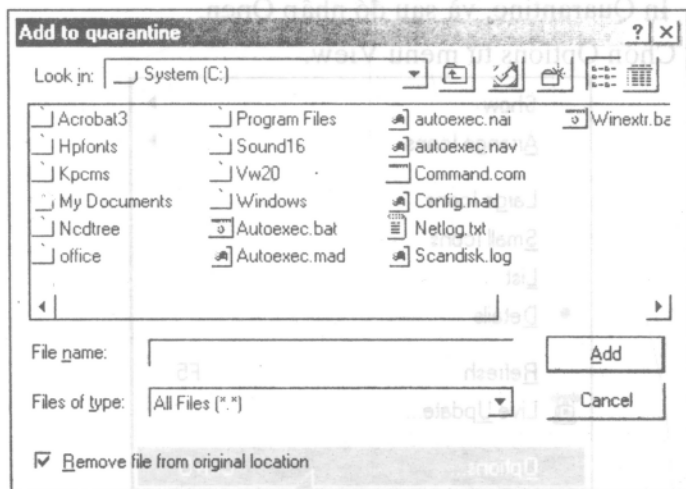
1. Trong cửa sổ chính Norton Antivirus, hãy nhấp Reports.
2. Từ danh sách các report, hãy nhấp View And Manage The Items In Quarantine, và sau đó nhấp Open.



3. Nhấp Add Item



4. Trong hộp thoại Add To Quarantine, hãy xác định file mà bạn muốn bổ sung vào.



Nếu tùy chọn Remove File From Original Location được chọn, file có khả năng bị nhiễm không thể vô tình được chạy.

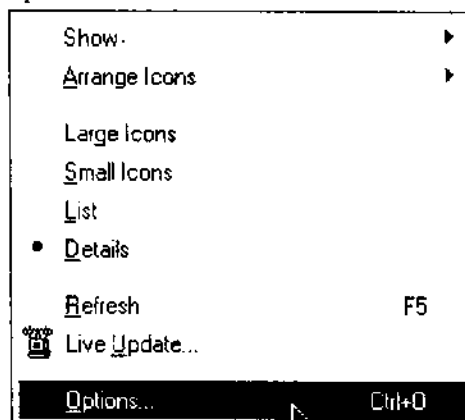
5. Nhấp Add.

VIII. Xem thông tin về một hạng mục đã cách li

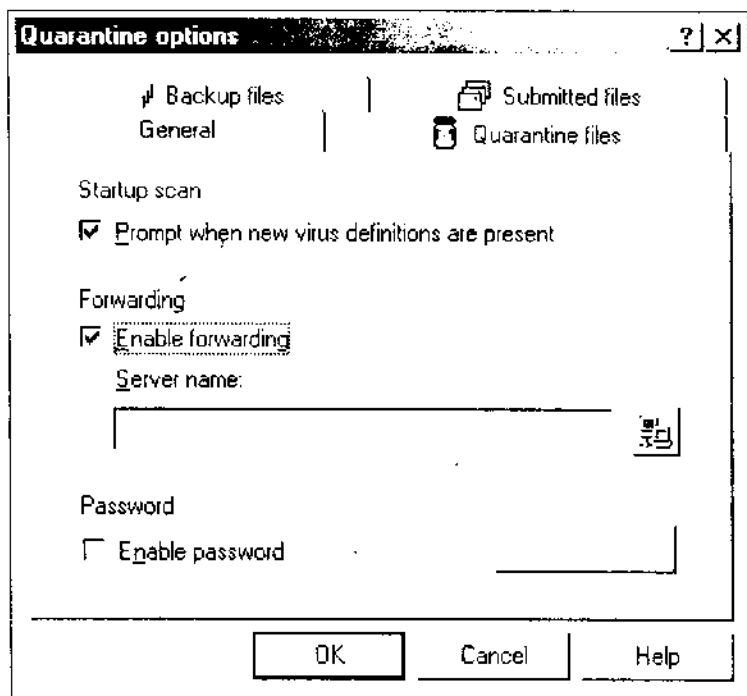
1. Trong cửa sổ chính Norton Antivirus, hãy nhấp Report.
2. Từ danh sách các tùy chọn, hãy chọn View And Manage The Items In Quarantine, và sau đó nhấp Open.
3. Trong ô bên trái của Quarantine, hãy nhấp vào các hạng mục đã cách li.
4. Thực hiện một trong các thao tác sau đây:
 - ❖ Chọn một hạng mục ở ô bên phải và nhấp Properties.
 - ❖ Nhấp đúp vào hạng mục của ô bên phải.

IX. Chỉ định một Quarantine options password.

1. Trong cửa sổ chính Norton Antivirus, hãy nhấp Report.
2. Từ danh sách các tùy chọn, chọn View And Manage The Items In Quarantine, và sau đó nhấp Open.
3. Chọn Options từ menu View.



4. Nhấp nhữn General.
5. Chon Enable Password và nhấp Set Password.



Nhập một password gồm 1 đếnn 16 ký tự. Các password không nhập với kiểu chữ.

6. Nhập lại password vào hợp Confirm New Password.
7. Nhấp OK để đóng hợp change Password.

X. Chỉ định các hành động Quarantine có thể chấp nhận được

1. Trong cửa sổ chính Norton Antivirus, hãy nhấp Report.
2. Từ danh sách các tùy chon, hãy chon View And Manege The Items In Quarantine, và sau đó nhấp Open.
3. Chon Options từ menu View.

4. Nhấp vào các nhãn Quarantine Files, Submitted, hoặc Backup Files và kiểm tra các hành động nào mà bạn muốn chấp nhận đối với mỗi kiểu file.

Nếu bạn không muốn người sử dụng có thể thay đổi các tùy chọn Quarantine, bạn có thể xác lập một password để ngăn chặn cách thay đổi không mong muốn đối với các tùy chọn Quarantine từ nhãn General.

XI. Để gửi một file đã cách li với SARC

Quarantine có Scan and Deliver Wizard nhấp đơn giản hóa việc gửi một hạng mục đến SARC để phân tích. Khi bạn nhấp Submit Item, Wizard phân tích file và có thể đề nghị một hành động thay vì gửi nó đến SARC. Chẳng hạn, virus có thể là loại có thể đã được loại bỏ bằng cách định nghĩa virus hiện hành. Tuy nhiên, bạn có thể bỏ qua đề nghị này và gửi nó.

1. Trong cửa sổ chính Norton Antivirus, hãy nhấp Report.
2. Từ danh sách các tùy chọn, hãy chọn View And Manage The Items In Quarantine, và sau đó nhấp Open
3. Ở ô bên trái của Quarantine, hãy nhấp các hạng mục đã cách li.
4. Chọn một file trong danh sách các hạng mục đã cách li và nhấp Submit Item.
5. Thực hiện theo các chỉ dẫn trong Scan and Deliver Wizard nhằm thu thập thông tin và gửi file đến SARC để phân tích.

 Bài 3

CÁCH HOẠT ĐỘNG CỦA NORTON ANTIVIRUS

I. Cách hoạt động của Norton Antivirus

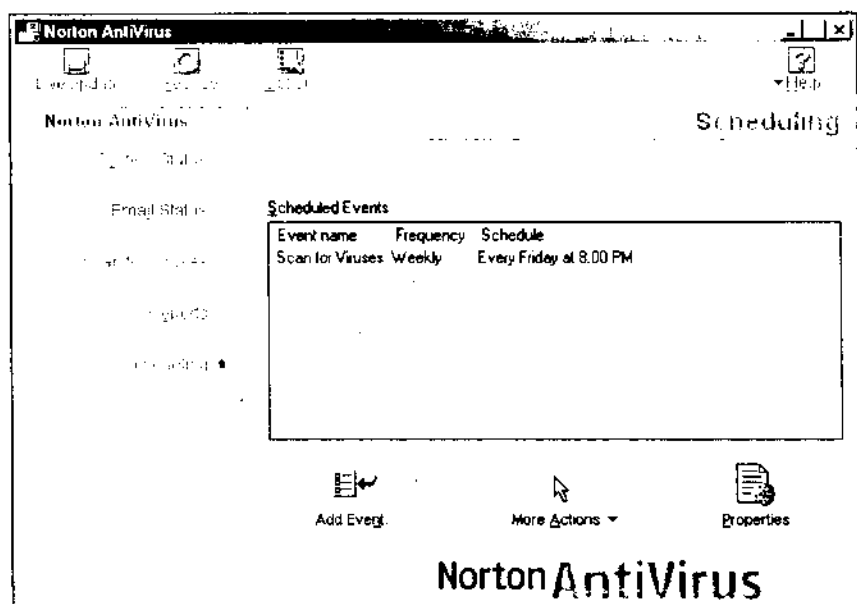
Chương trình quét kiểm tra các file chương trình để tìm các virus đã được nhận biết. Nó là phần chính của sự bảo vệ Norton Antivirus. Nó tìm các virus đã biết khi bạn khởi tạo các tiến trình quét bằng tay, khi bạn lập thời biểu để quét virus vào những thời điểm nhất định, trong suốt các tiến trình quét được chạy tự động mỗi khi bạn khởi động máy tính, và dựa vào tính năng Auto-Protect của một file được sử dụng. Chương trình quét cũng xác nhận các record khởi động đã được bảo vệ không bị thay đổi.

1. Các tiến trình quét bằng tay

Sử dụng nút Scan Now trong cửa sổ chính Norton Antivirus để khởi tạo các tiến trình quét bằng tay. Các tiến trình quét này dò tìm các virut đã biết trong các file, các folder, hay các ổ đĩa cụ thể trên máy tính của bạn.

2. Các tiến trình quét theo thời biểu

Các tiến trình quét theo thời biểu là các tiến trình quét bằng tay được chạy tự động vào các thời điểm đã xác định trước. Các tiến trình quét này bổ sung vào các tính năng bảo vệ tự động khác để bảo đảm máy tính của bạn không bị nhiễm virus. Là một phần của tiến trình cài đặt Norton Antivirus, một tiến trình quét virus máy tính được lập thời biểu để chạy tự động mỗi tuần một lần.

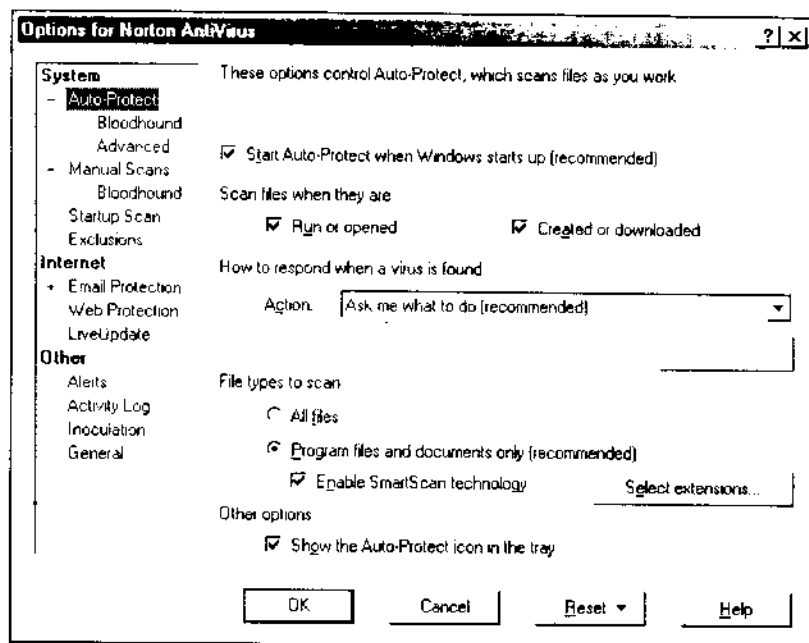


3. Các tiến trình quét vào lúc khởi động

Tiến trình bảo vệ đầu tiên nhằm chống lại sự xâm nhập của virus là các tiến trình quét đặc biệt xảy ra tự động mỗi khi máy tính của bạn khởi động. Các tiến trình này quét tất cả các virus lây nhiễm các file và các record khởi động mà máy tính của bạn sử dụng để chuẩn bị làm việc. Các tiến trình quét vào lúc khởi động là một phần quan trọng trong việc bảo vệ virus bởi vì chúng bảo đảm máy tính của bạn hoàn toàn không bị nhiễm virus mỗi khi bạn khởi động nó.

4. Auto-Protect

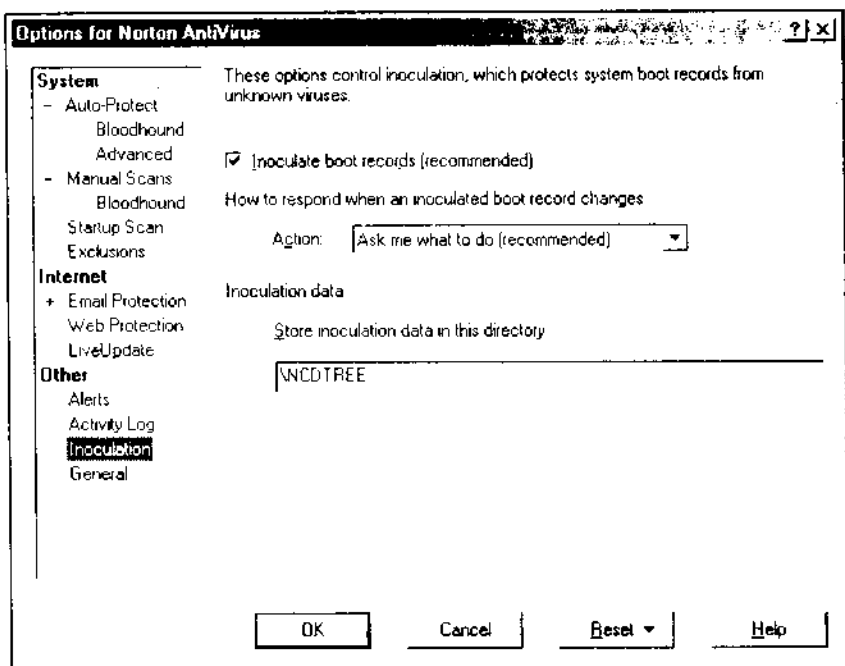
Auto-Protect, một tính năng bảo vệ tự động của Norton Antivirus, quét các file chương trình, các tài liệu, và các file template tài liệu để tìm các virus bất kỳ khi nào chúng được sử dụng.



Ngoài việc kiểm tra các file để tìm các virus đã biết, Auto-Protect còn sử dụng công nghệ Bloodhound và giám sát các hoạt động giống như virus để bảo đảm các virus chưa được biết đến không lây nhiễm máy tính của bạn cũng như không làm hỏng dữ liệu trong suốt quá trình hoạt động bình thường. Auto-Protect được bật sau khi cài đặt, trừ phi bạn tắt nó.

5. Phòng ngừa virus

Ngay sau khi các đĩa đã được quét để xác nhận rằng chúng hoàn toàn không bị nhiễm virus, Norton Antivirus phòng ngừa các record khởi động để bảo đảm chúng không bị nhiễm. Khi một record khởi động đã được phòng ngừa, Norton Antivirus ghi lại các thông tin quan trọng vì nó (tương tự như việc lấy dấu tay) trong một file đặc biệt được thiết kế để chứa dữ liệu phòng ngừa này. Vào những lần quét sau đó, Norton Antivirus so sánh dấu tay hiện tại với dấu tay đã lưu. Bạn sẽ nhận được một cảnh báo nếu có bất kỳ sự thay đổi nào cho thấy có sự tồn tại của virus. Các record khởi động được phòng ngừa tự động trong tiến trình cài đặt Norton Antivirus.



6. Các file định nghĩa virus

Các file định nghĩa virus chứa thông tin mà Norton Antivirus sử dụng trong suốt các tiến trình quét để dò tìm các virus đã biết. Norton Antivirus phụ thuộc vào thông tin cập nhật. Mỗi khi một virus mới được phát hiện, phần ký hiệu của virus đó phải được thêm vào file định nghĩa virus. Bạn nên cập nhật các file định nghĩa virus ít nhất mỗi tháng một lần để Norton Antivirus có thông tin cần thiết để tìm tất cả các virus đã biết. Các file định nghĩa virus mới có sẵn đều đặn trong Symantec. Nếu bạn có một modem hay một nối kết Internet, Norton Antivirus có thể cập nhật các file định nghĩa virus cho bạn một cách tự động.

7. Tất cả virus máy tính được phân thành hai nhóm

- ❖ **Nhóm virus đã biết:** Một virus đã biết là một virus đã được xác định. Các kỹ sư Symantec thường xuyên theo dõi sự

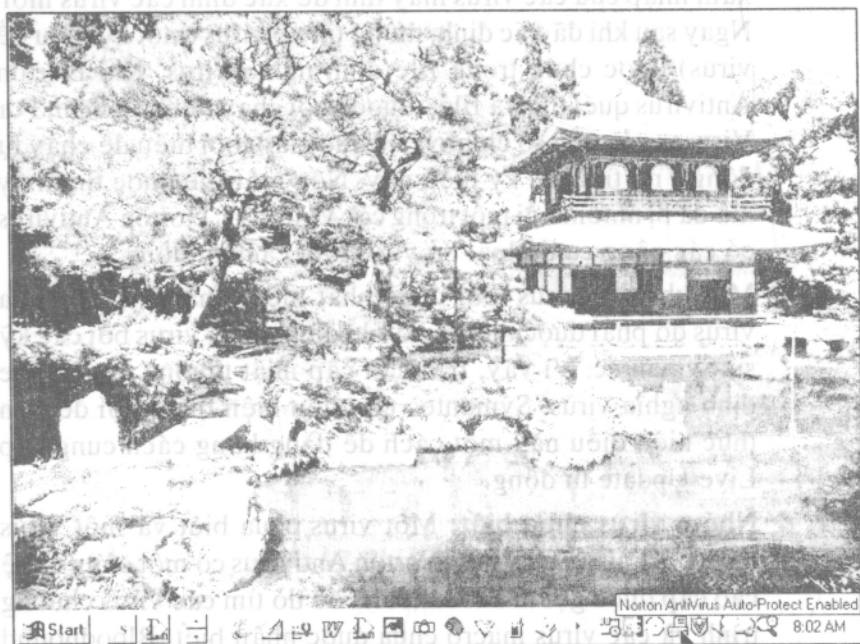
xâm nhập của các virus máy tính để xác định các virus mới. Ngay sau khi đã xác định, thông tin về virus (một ký hiệu về virus) được chứa trong file định nghĩa virus. Khi Norton Antivirus quét đĩa và file - được khởi chạy từ trang Scan For Viruses của cửa sổ chính hoặc được lập thời biểu để chạy tự động - nó tìm các ký hiệu này. Nếu một file được tìm thấy mà đã bị nhiễm bởi một trong các virus này, Norton Antivirus có các công cụ để loại bỏ virus một cách tự động.

Mỗi khi một virus mới được phát hiện, phần ký hiệu của virus đó phải được thêm vào file định nghĩa virus bởi các kỹ sư Symantec. Vì vậy, bạn cần cập nhật thường xuyên file định nghĩa virus. Symantec tạo điều kiện thuận lợi để bạn thực hiện điều này một cách dễ dàng bằng cách cung cấp Live Update tự động.

- ❖ **Nhóm virus chưa biết:** Một virus chưa biết và một virus chưa có định nghĩa virus. Norton Antivirus có một công nghệ cao cấp được gọi là Bloodhound để dò tìm các virus chương trình và các virus macro chưa được nhận biết. Bloodhound cô lập và xác định nhiều vùng logic của một file và sau đó phân tích sự logic của chương trình để tìm hoạt động giống như virus. Bloodhound dò tìm các virus chưa biết với một tỷ lệ rất cao. Ngoài ra, Norton Antivirus dò tìm các virus chưa biết bằng cách giám sát sự hoạt động trên máy tính của bạn khi Norton Antivirus tìm thấy một hoạt động bị nghi là có những virus, nó ngăn chặn ngay hoạt động này.

II. Sử dụng Norton Antivirus

1. Nhấp đúp vào biểu Norton Antivirus trên thanh tác vụ Windows ở góc phía dưới bên phải của nền màn hình để mở Norton Antivirus.



2. Từ cửa sổ chính Norton Antivirus, bạn có thể xem tình trạng hiện hành của hệ thống; khởi chạy các tiến trình quét bằng tay cho các file, các folder, hay các ổ đĩa được chọn; chạy chương trình Norton Antivirus Quarantine; và lập thời biểu cho các tiến trình quét virus đều đặn.

III. Bàn về Norton Antivirus Auto-Protect

Auto-Protect làm việc trong nền để bảo vệ bạn theo nhiều cách:

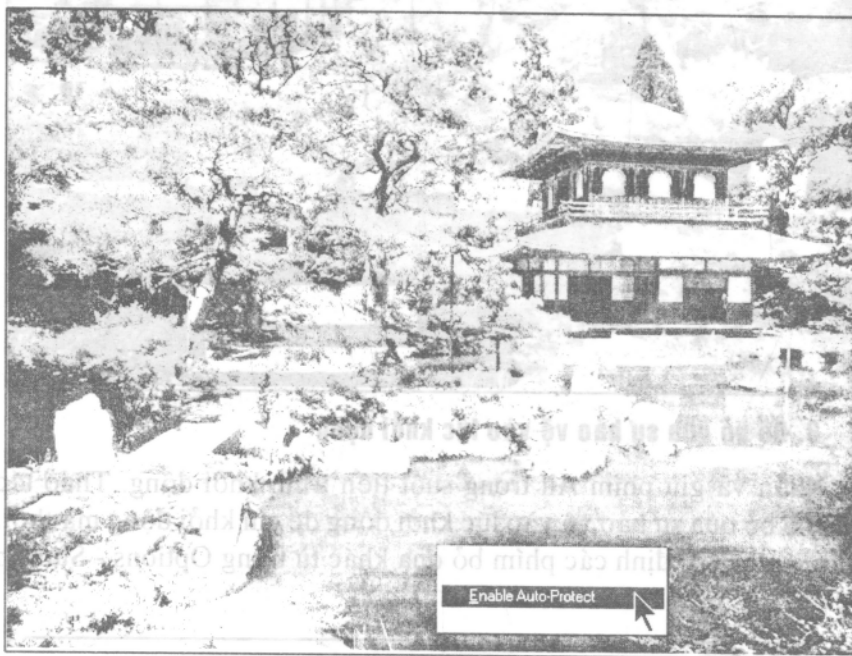
- ❖ Dò tìm các virus có thể đã có và loại bỏ chúng.
- ❖ Ngăn chặn virus lây nhiễm máy tính của bạn.
- ❖ Giám sát các hoạt động có thể có sự tồn tại của một virus chưa biết.

Ngoài các tiến trình quét mà Auto-Protect thực hiện trong nền, bạn cũng có thể khởi chạy các tiến trình quét vào bất kỳ lúc nào và

lập thời biểu để chạy các tiến trình quét vào các thời điểm đã xác định trước.

1. Để bật Auto-Protect:

1. Nhấp phải vào biểu tượng Norton Antivirus ở góc phía dưới bên phải của thanh tác vụ trên nền màn hình Windows.
2. Nhấp Enable Auto-Protect.

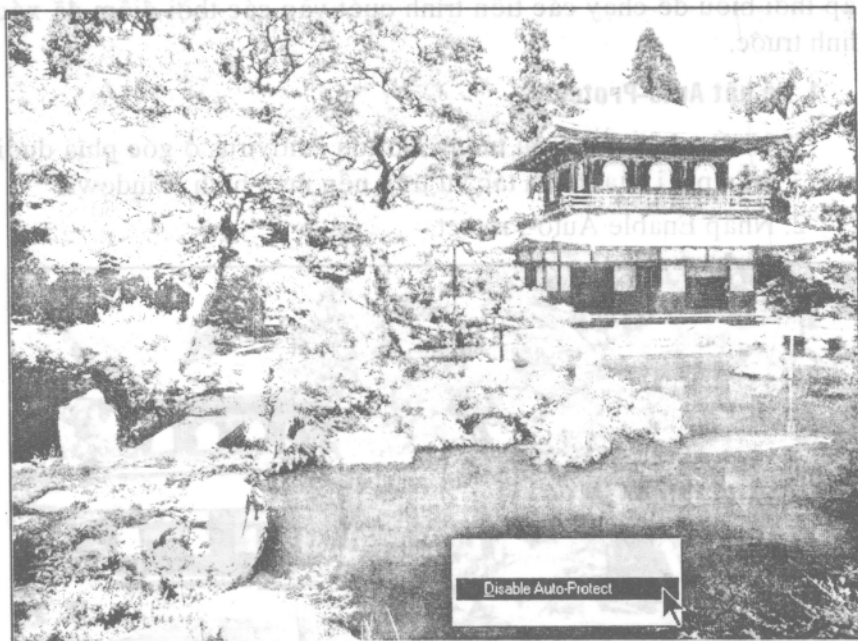


Ghi chú

Norton Antivirus được xác lập sẵn để bật Auto-Protect vào bất kỳ khi nào bạn khởi động máy tính.

2. Để tắt tạm thời Auto-Protect

1. Nhấp phải vào biểu tượng Norton Antivirus ở góc phía dưới bên phải của thanh tác vụ trên nền màn hình Windows.
2. Nhấp Disable Auto-Protect.



3. Để bỏ qua sự bảo vệ vào lúc khởi động

Nhấn và giữ phím Alt trong suốt tiến trình khởi động. Thao tác này sẽ bỏ qua sự bảo vệ vào lúc khởi động để chỉ khởi động mà thôi. Bạn có thể chỉ định các phím bỏ qua khác từ trang Options - Startup Scan.

Ghi chú

Việc bỏ qua sự bảo vệ vào lúc khởi động sẽ giảm bớt mức độ bảo vệ.

IV. Các lệnh chuyển đổi dòng lệnh

NAVW32.EXE là giao diện Windows và chương trình quét. Nó có thể được chạy với các lệnh chuyển đổi dòng lệnh, thường là từ lệnh Run trong menu Start, để thay thế các xác lập cấu hình.

NAVW32 [[pathname] options]

pathname

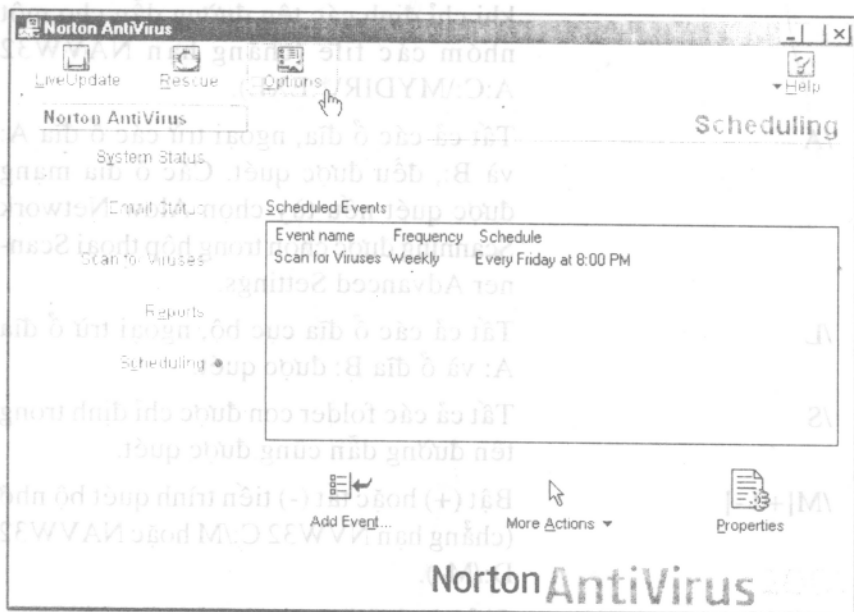
Mọi ổ đĩa, folder, file, hay sự kết hợp giữa

chúng đều được quét. Nếu bạn muốn quét một tổ hợp các hạng mục, hãy sử dụng một khoảng trống để tách các hạng mục. Bạn có thể sử dụng các ký tự thay thế khi chỉ định các tên đường dẫn cho một nhóm các file (chẳng hạn NAVW32 A:C:\MYDIR*.EXE).

- /A Tất cả các ổ đĩa, ngoại trừ các ổ đĩa A: và B:, đều được quét. Các ổ đĩa mạng được quét nếu tùy chọn Allow Network Scanning được chọn trong hộp thoại Scanner Advanced Settings.
- /L Tất cả các ổ đĩa cục bộ, ngoại trừ ổ đĩa A: và ổ đĩa B: được quét.
- /S Tất cả các folder con được chỉ định trong tên đường dẫn cũng được quét.
- /M[+ | -] Bật (+) hoặc tắt (-) tiến trình quét bộ nhớ (chẳng hạn NAVW32 C:/M hoặc NAVW32 D:/M-).
- /MEM Chỉ bộ nhớ được quét.
- /B[+ | -] Bật (+) hoặc tắt (-) tiến trình quét các record khởi động (chẳng hạn NAVW32 A:/B+ hoặc NAVW32 B:/B-).
- /BOOT Chỉ các record khởi động của các ổ đĩa được chỉ định mới được quét.
- /NORESULTS Không có kết quả quét nào được báo cáo trên màn hình.
- /DEFAULT Đưa các xác lập trở lại tình trạng mặc định khi bạn nhận Norton Antivirus.
- /HEUR:[0|1|2|3] Xác lập độ nhạy của Bloodhound (tm).

V. Xác định cách hoạt động của chế độ bảo vệ vào lúc khởi động.

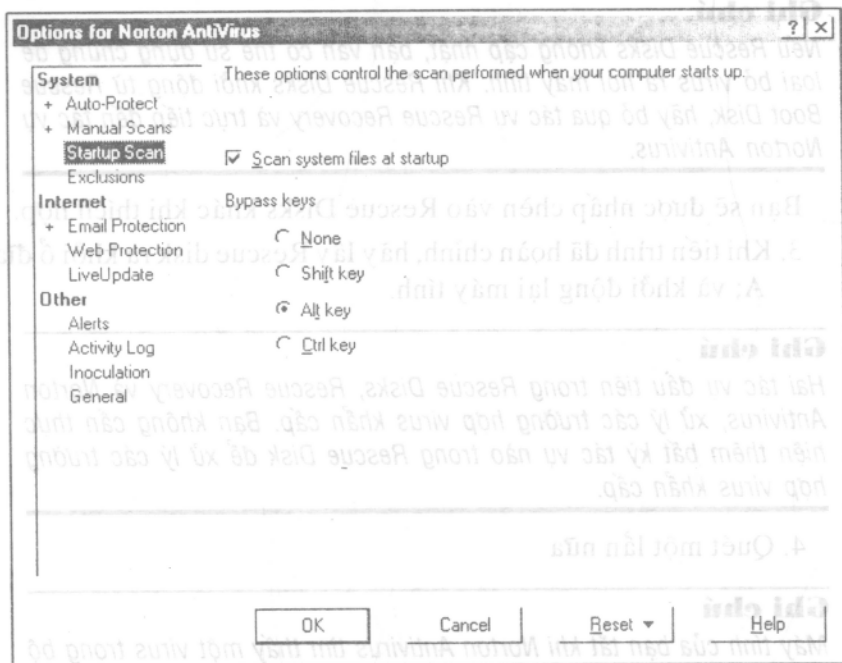
1. Nhấp Options trên cửa sổ chính Norton Antivirus.



2. Nhấp Startup nếu nó chưa được chọn.

3. Chỉ định các vùng mà bạn muốn Norton Antivirus quét mỗi khi bạn khởi động máy tính trong hộp nhóm Items To Scan.

Bạn nên giữ nguyên các tùy chọn đã xác lập sẵn (mọi thứ đều được chọn).



4. Chọn phím bỏ qua (phím Alt là tùy chọn đã xác lập sẵn).

Nếu bạn làm việc trong một môi trường có độ rủi ro cao, hoặc nếu nhiều người khác đang sử dụng máy tính của bạn, bạn nên chọn None.

5. Nhấp OK để lưu các xác lập và thoát khỏi hộp thoại Options.

VI. Khởi động lại máy tính đã tắt

1. Khởi động lại máy tính bằng cách đặt Rescue Boot Disk vào ổ đĩa A: và bật máy tính.

Ghi chú

Nếu bạn chưa tạo Rescue Disks, hãy sử dụng Emergency Disks mà bạn tạo từ CD sản phẩm.

2. Thực hiện theo các chỉ dẫn trên màn hình.

Ghi chú

Nếu Rescue Disks không cập nhật, bạn vẫn có thể sử dụng chúng để loại bỏ virus ra khỏi máy tính. Khi Rescue Disks khởi động từ Rescue Boot Disk, hãy bỏ qua tác vụ Rescue Recovery và trực tiếp đến tác vụ Norton Antivirus.

Bạn sẽ được nhấp chèn vào Rescue Disks khác khi thích hợp.

3. Khi tiến trình đã hoàn chỉnh, hãy lấy Rescue disk ra khỏi ổ đĩa A; và khởi động lại máy tính.

Ghi chú

Hai tác vụ đầu tiên trong Rescue Disks, Rescue Recovery và Norton Antivirus, xử lý các trường hợp virus khẩn cấp. Bạn không cần thực hiện thêm bất kỳ tác vụ nào trong Rescue Disk để xử lý các trường hợp virus khẩn cấp.

4. Quét một lần nữa

Ghi chú

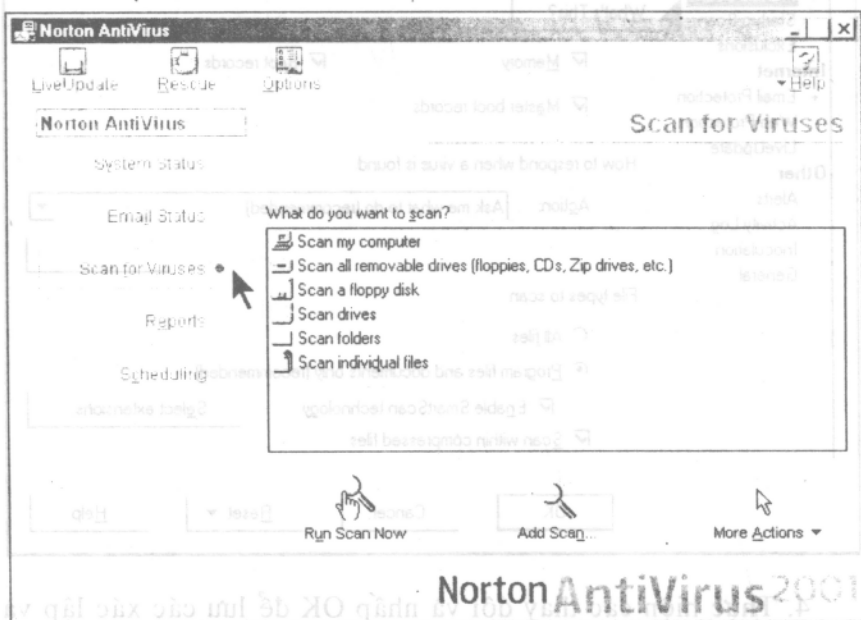
Máy tính của bạn tắt khi Norton Antivirus tìm thấy một virus trong bộ nhớ nếu bạn chọn Shutdown Computer trong Auto-Protect trong hộp thoại Options.

Bài 4

QUÉT CÁC Ổ ĐĨA, CÁC FILE VÀ CÁC FOLDER

I. Quét các ổ đĩa

1. Mở cửa sổ chính Norton Antivirus nếu nó chưa được mở.
2. Chọn Scan for Viruses.

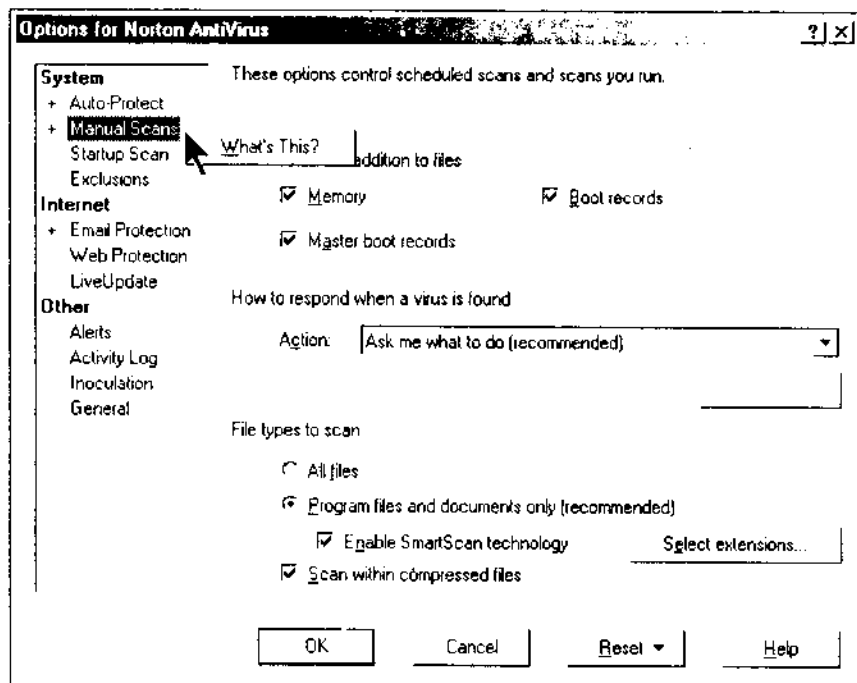


3. Chọn Scan All Hard Disks For Viruses từ danh sách và nhấn Run Scan Now. Bạn có cũng có thể xác định một tác vụ quét

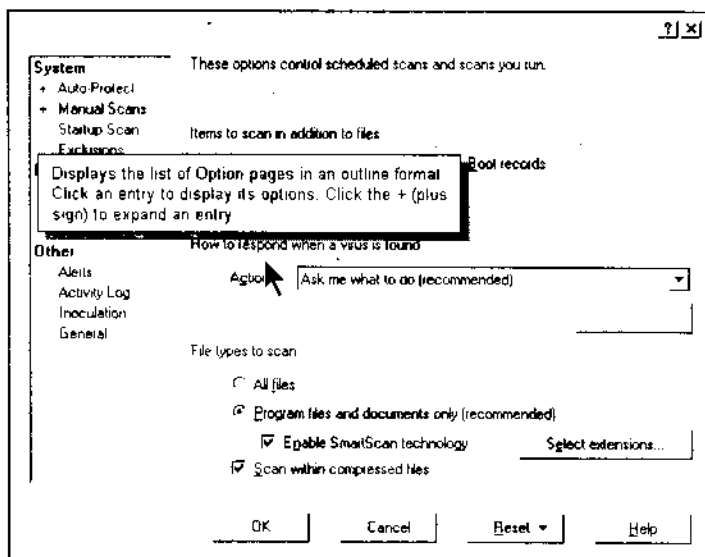
mới để quét chỉ các ổ đĩa cứng được chọn bằng cách nhấp Create New Scan và thực hiện theo các chỉ dẫn trong Scan Task wizard.

II. Thay đổi các tùy chọn quét đôi với các tiến trình quét mà bạn khởi chạy hay lập thời biểu

1. Nhấp Options trên cửa sổ chính Norton Antivirus.
2. Nhấp Manual Scans nếu nó chưa được chọn.
3. Nhấp phải vào một tùy chọn bất kỳ và nhấp What's This? để tìm hiểu thêm thông tin về tùy chọn đó.

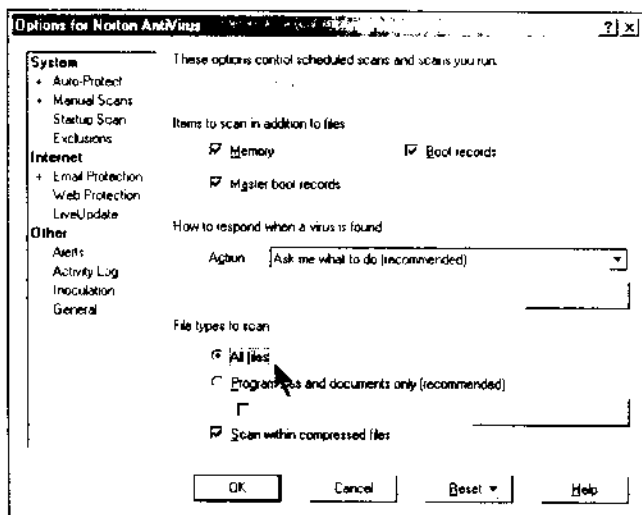


4. Thực hiện các thay đổi và nhấp OK để lưu các xác lập và thoát.

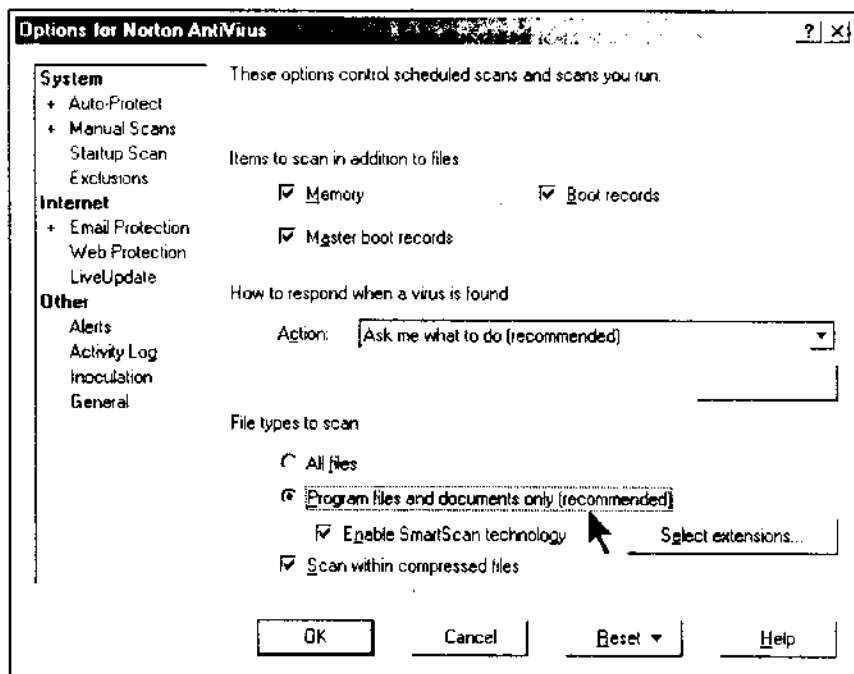


III. Chọn các phần mở rộng file mà Norton Antivirus quét

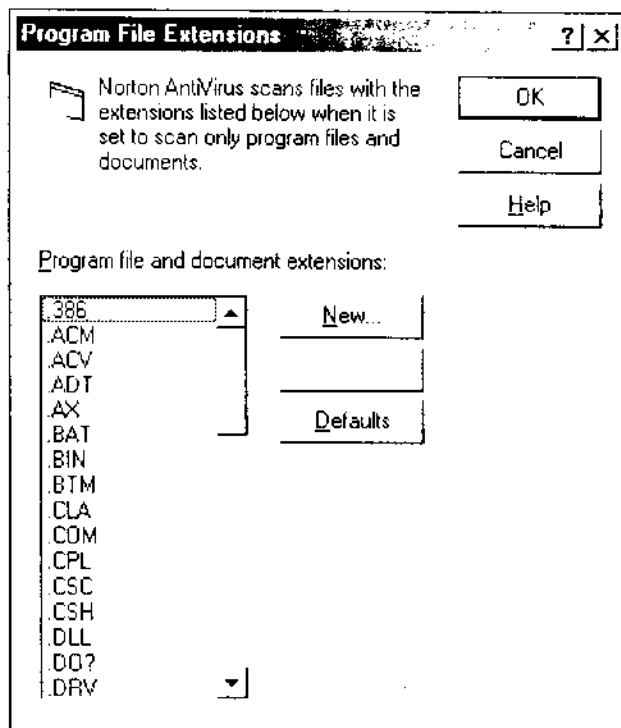
1. Trong các xác lập Manual Scan, hãy nhấp vào kiểu file cần quét: All Files hoặc Program Files And Documents Only.



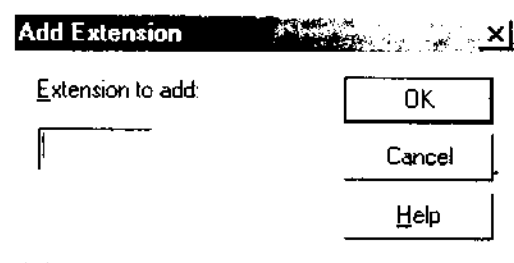
2. Nếu bạn đã chọn Program Files And Document Only, hãy nhấp Select Extension để hiển thị hộp thoại Program File Extensions.



3. Nhấp New để hiển thị hộp thoại Add Extension.
4. Nhập bất kỳ phần mở rộng file nào không theo tiêu chuẩn mà bạn sử dụng để đặt tên cho các file khả thi.



5. Nhấp OK để lưu các xác lập và thoát khỏi hộp thoại New Program File Extensions.



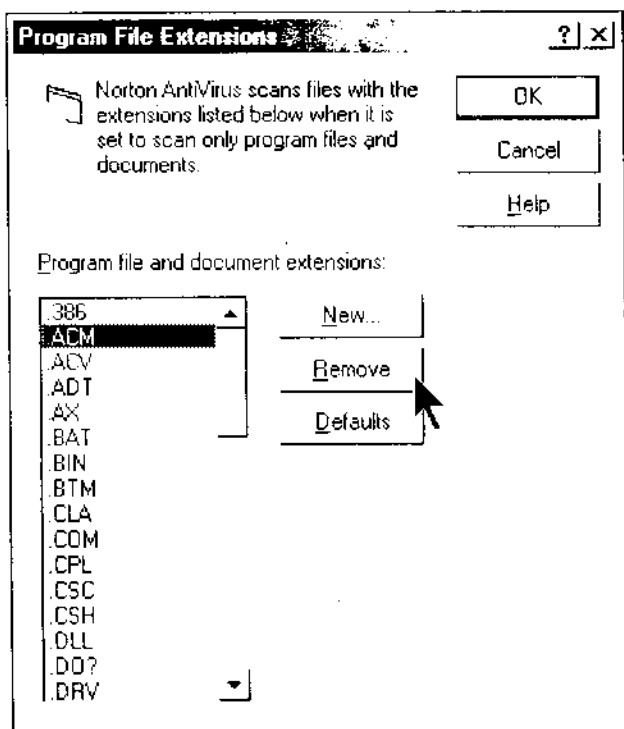
Hộp thoại Program File Extensions lại xuất hiện.

6. Nhấp OK để lưu các xác lập và thoát khỏi hộp thoại Program File Extensions.
Hộp thoại Options xuất hiện.

7. Nhấp OK để lưu các xác lập và thoát khỏi hộp thoại Options.

Để loại bỏ một phần mở rộng file ra khỏi tiến trình quét:

1. Trong bước 3 ở trên, hãy chọn phần mở rộng từ danh sách và nhấp Remove.

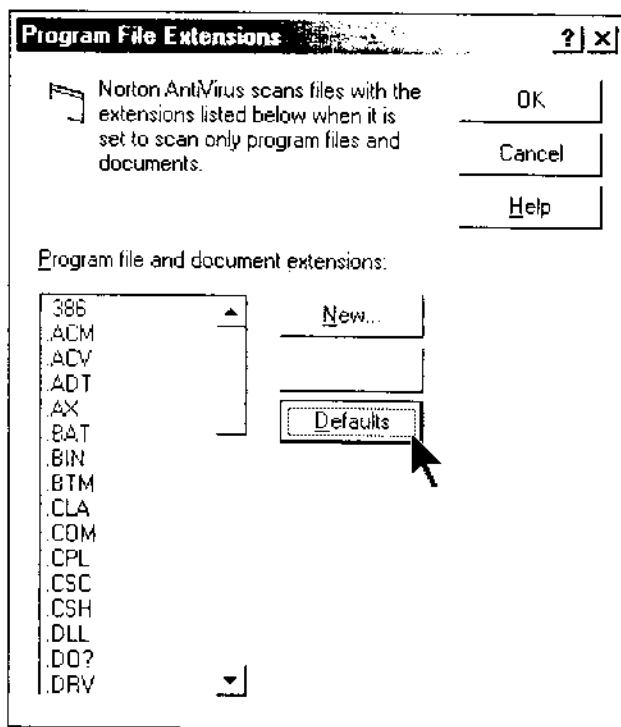


2. Tiếp tục với bước sáu ở trên.

Để làm cho danh sách phần mở rộng file trở lại các xác lập mặc định:

1. Trong bước 3 ở trên, hãy nhấp Defaults.

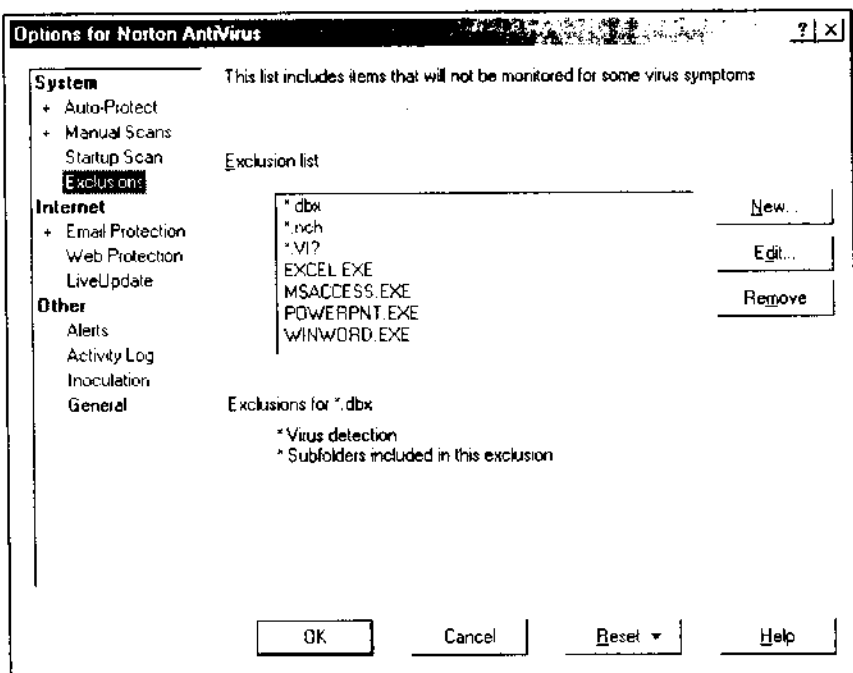
2. Tiếp tục với bước 6 ở trên.



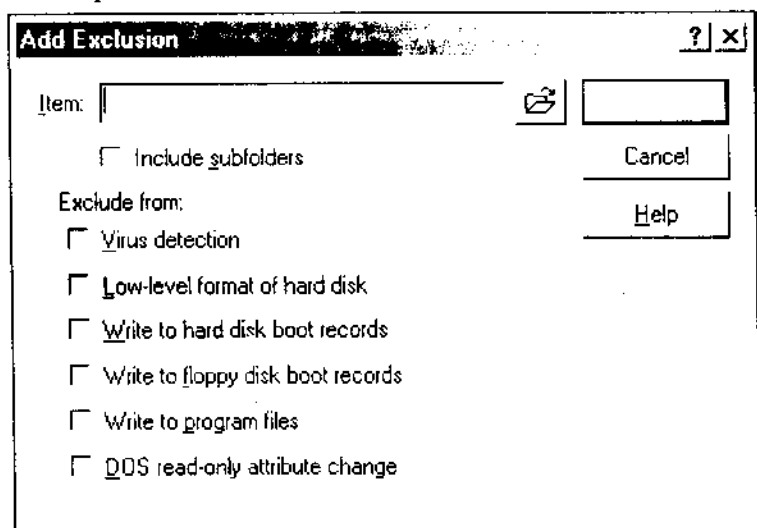
Norton Antivirus cũng quét các tài liệu Microsoft Word và Excel khi quét các file chương trình. Mặc dù đây không phải là các file chương trình nhưng chúng có chứa mã và có thể bị nhiễm các virus macro.

IV. Loại bỏ các file ra khỏi tiến trình quét virus

1. Nhấp Options trên cửa sổ chính Norton Antivirus.
2. Nhấp nhấn Exclusions nếu nó chưa được chọn.

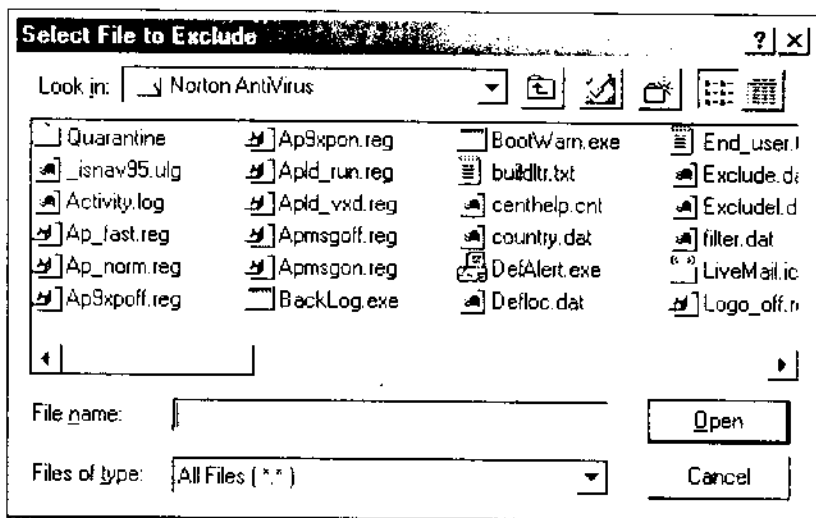


3. Nhấp New.



4. Thực hiện một trong các thao tác sau đây:

- ❖ Sử dụng nút browse để hiển thị hộp thoại Select File To Exclude mà từ đó bạn có thể chọn một file để hiển thị trong hộp text Item.



- ❖ Nhập một tên file vào hộp text Item. Bạn có thể sử dụng các ký tự thay thế chẳng hạn như c:/*.*.COM. Bạn nên chọn Include Subfolders nếu bạn muốn bảo đảm rằng tất cả các file có phần mở rộng đó đều được loại bỏ.

Hãy thận trọng vì việc loại bỏ các file sẽ giảm bớt mức độ bảo vệ.

V. Lưu ý về việc quét các ổ đĩa mạng

Bởi vì không phải lúc nào bạn cũng có các đặc quyền truy cập vào một ổ đĩa mạng giống như với ổ đĩa cục bộ, nên có một số điểm hạn chế khi quét các ổ đĩa mạng với Norton Antivirus. Việc quét các ổ đĩa mạng mất nhiều thời gian hơn việc quét các ổ đĩa cục bộ. Những người khác có thể thực hiện việc tạo, xóa, hay di chuyển các file trên một ổ đĩa trong khi Norton Antivirus đang quét.

Các đặc quyền truy cập ổ đĩa Các hoạt động mà bạn có thể thực hiện

None

Không có

Read-Only

Quét, nhưng không xử lý hay xóa các file bị nhiễm, hoặc phòng ngừa.

Read-Write

Quét, xử lý, xóa, và phòng ngừa.

VI. Quét một file riêng lẻ

1. Mở cửa sổ chính Norton Antivirus nếu nó chưa được mở.
2. Chọn Scan for Viruses.
3. Chọn Scan One or More Files For Viruses từ danh sách và chạy Run Scan Now. Chọn các file mà bạn muốn quét từ hộp thoại.
4. Nhấp Open.



VII. Quét một folder

1. Mở cửa sổ chính Norton Antivirus nếu nó chưa được mở.
2. Chọn Scan for Viruses.
3. Chọn Scan One or More Folders For Viruses từ danh sách và chạy Run Scan Now. Chọn folder mà bạn muốn quét từ cây thư mục.
4. Nhấp Scan.

VIII. Quét một đường dẫn

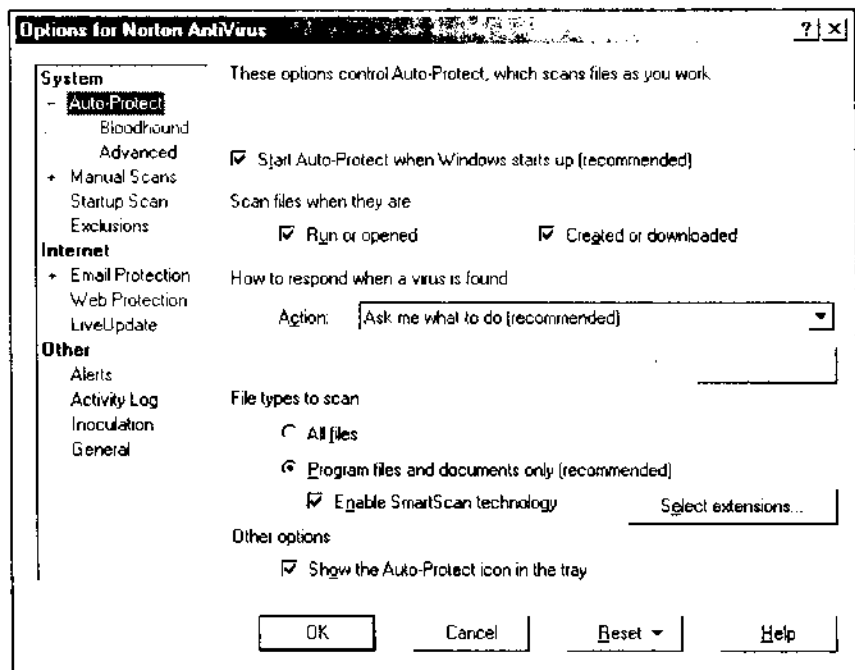
1. Mở cửa sổ chính Norton Antivirus nếu nó chưa được mở.
2. Chọn Scan for Viruses.
3. Chọn Scan One or More Folders For Viruses từ danh sách và chạy Run Scan Now. Chọn folder ở cấp độ cao nhất trong đường dẫn mà bạn muốn quét từ cây thư mục.
4. Nhấp Scan.

IX. Chọn khi nào các file được quét bởi Auto-Protect

1. Nhấp Options trên cửa sổ chính Norton Antivirus.
2. Chọn Auto-Protect nếu nó chưa được chọn.
3. Chọn khi nào Norton Antivirus sẽ tự động quét một file.

Ghi chú

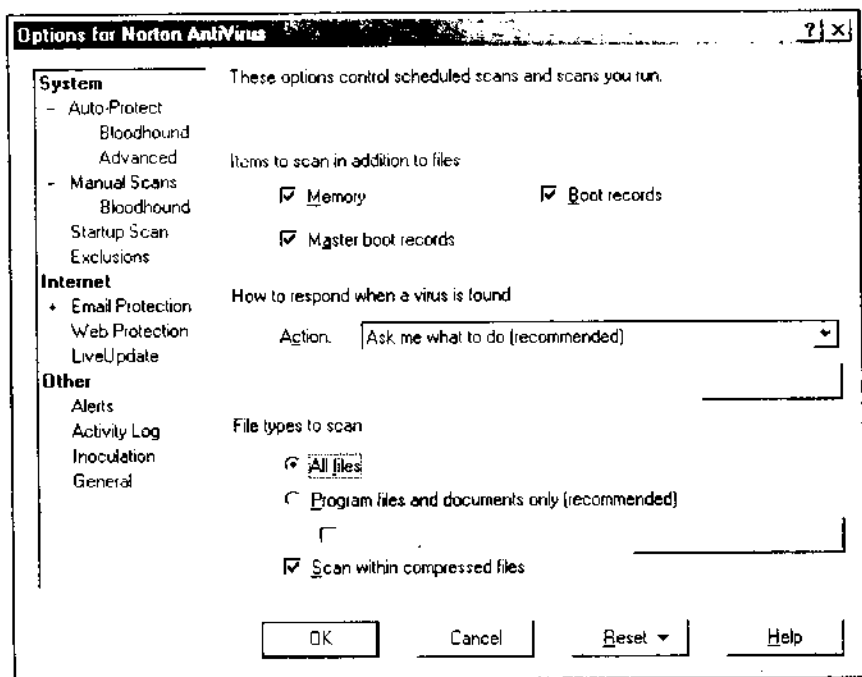
Chọn tất cả các tùy chọn để bảo đảm bảo vệ đến mức tối đa.



4. Nhấp OK để lưu các xác lập và đóng hộp thoại.

X. Chọn các file nào cần quét khi bạn khởi chạy một tiến trình quét bằng tay hay quét theo thời biểu.

1. Nhấp Options trong cửa sổ chính Norton Antivirus.
2. Nhấp Manual Scans nếu nó chưa được chọn.
3. Chọn các vùng mà máy tính sẽ quét trước khi các file chương trình được quét.



Ghi chú

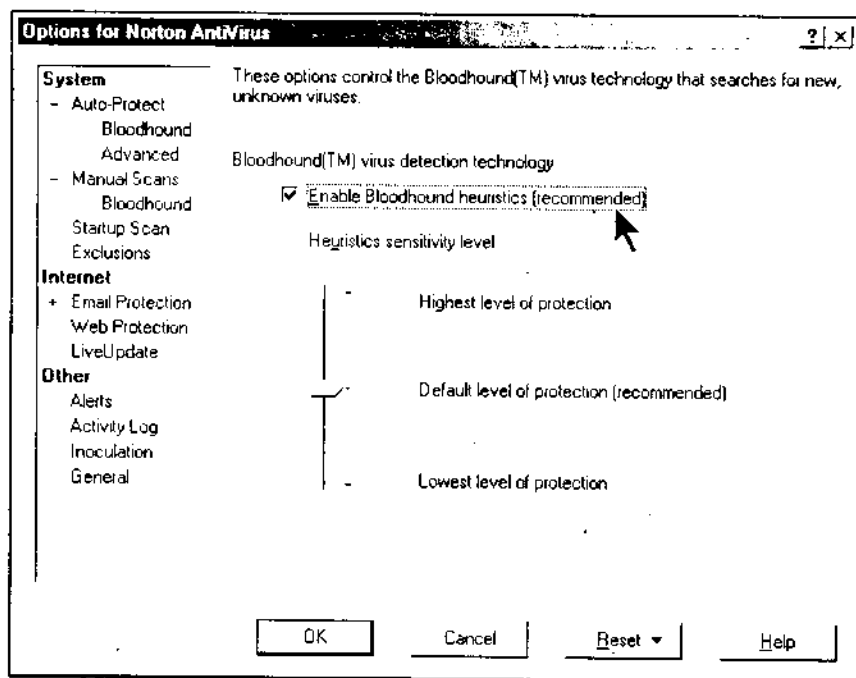
Theo mặc định, tất cả các tùy chọn đều được chọn nếu bạn đã thực hiện cài đặt hoàn chỉnh Norton Antivirus.

4. Nhấp Program Files để quét chỉ các file nghi ngờ là có nhiễm virus. Tuy nhiên, nếu bạn làm việc trong một môi trường mà bạn có thể gặp các file chương trình không có các phần mở rộng file chuẩn, hãy nhấp All Files.
5. Nhấp Select Extensions để hiển thị hộp thoại Program File Extensions, hộp thoại này liệt kê các phần mở rộng file mà Norton Antivirus quét.

XI. Xác lập các tùy chọn quét

1. Nhấp vào dấu + ở kế bên Manual Scans hoặc Auto-Protect.
2. Nhấp Bloodhound.

3. Bảo đảm Enable Bloodhound Heuristics được chọn.



Bạn có thể rê pointer để tăng sự bảo vệ virus đối với các virus khó dò tìm và chưa được nhận biết. Tiến trình quét này có thể mất nhiều thời gian hơn.

4. Nhấp OK để lưu các xác lập và thoát khỏi hộp thoại.

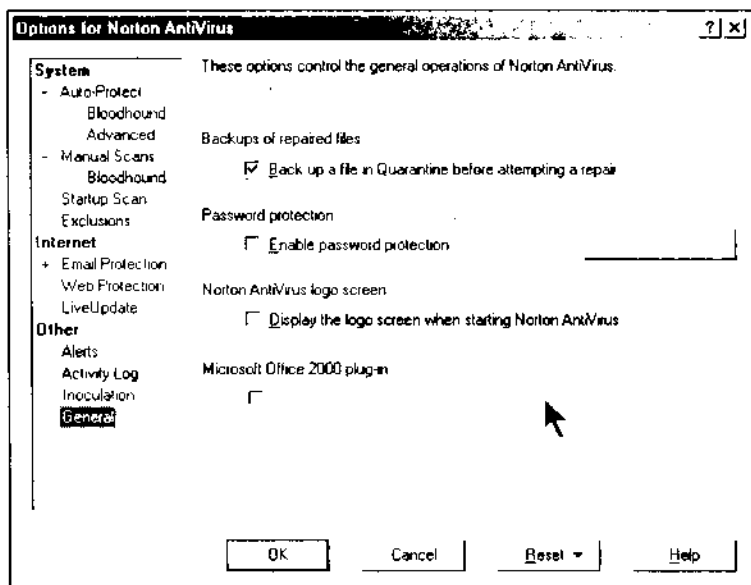
XII. Xác lập các tùy chọn quét chung

1. Nhấp Options trên cửa sổ chính Norton Antivirus.

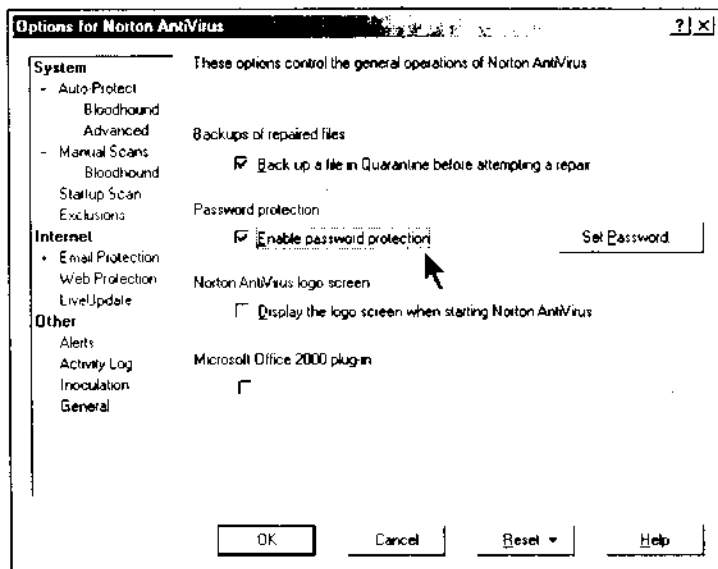
2. Nhấp General.

3. Xác lập các tùy chọn sau đây một cách thích hợp:

- ❖ Chọn Back Up A File in Quarantine Before Attempting A Repair để nhờ Norton Antivirus tạo một bản sao của file bị nhiễm trước khi xử lý nó.



❖ Chọn Chế độ bảo vệ Enable Password để các xác lập tùy chọn không bị thay đổi do vô ý.



- ❖ Chọn Display The Logo Screen When Starting Norton Antivirus để hiển thị màn hình splash bất kỳ khi nào bạn khởi động Norton Antivirus.
 - ❖ Chọn plug-in Microsoft Office 2000 để bật chế độ bảo vệ khi bạn mở các file trong Microsoft Office 2000.
4. Nhấp OK để lưu các xác lập và thoát khỏi hộp thoại Options.

Làm việc với các kết quả quét :

Thực hiện một trong các thao tác sau đây:

- ❖ Nhấp Print để in các kết quả quét ra một máy in hay một file.
- ❖ Nhấp Details để xem các chi tiết về tiến trình quét, chẳng hạn như các file nào bị sự cố và mỗi sự cố đã được xử lý như thế nào. Nếu không có sự cố nào được tìm thấy, nút Details sẽ ở dạng chìm mờ.

Ghi chú

Hộp thoại Scan Results xuất hiện vào cuối tiến trình quét, sau khi bạn đã phản hồi đối với bất kỳ sự cố nào và tóm tắt những điều đã xảy ra trong suốt tiến trình quét.



XỬ LÝ VÀ LOẠI BỎ CÁC FILE BỊ NHIỄM VIRUS

I. Xử lý file hay record khởi động đã bị nhiễm virus

1. Chọn Repair.

Nếu nút lệnh Repair ở dạng chìm mờ, thì Norton AntiVirus đã được cấu hình để không bật nó hoặc hạng mục không thể được xử lý.

2. Sau khi xử lý các file hay các record khởi động đã bị nhiễm, hãy quét lại các ổ đĩa và các đĩa mềm để xác nhận không có file hay record khởi động nào khác bị nhiễm virus.

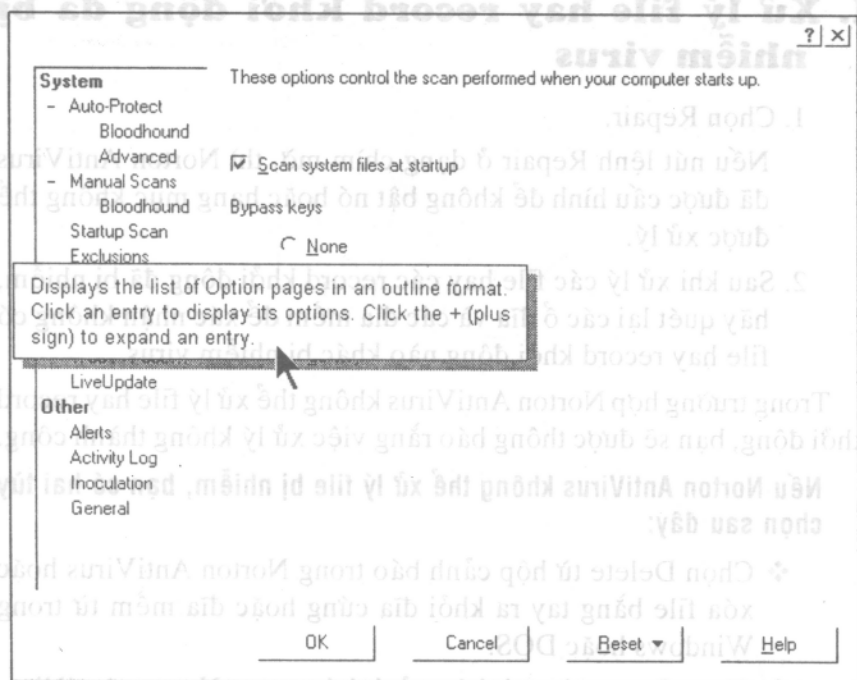
Trong trường hợp Norton AntiVirus không thể xử lý file hay record khởi động, bạn sẽ được thông báo rằng việc xử lý không thành công.

Nếu Norton AntiVirus không thể xử lý file bị nhiễm, bạn có hai tùy chọn sau đây:

- ❖ Chọn Delete từ hộp cảnh báo trong Norton AntiVirus hoặc xóa file bằng tay ra khỏi đĩa cứng hoặc đĩa mềm từ trong Windows hoặc DOS.
- ❖ Chọn Quarantine từ hộp cảnh báo trong Norton AntiVirus để cô lập file và ngăn chặn sự truy cập hay chạy nó. Sau đó bạn có thể gỡ file bị nhiễm đến SARC để phân tích thêm.

II. Thay đổi cách hoạt động của Norton AntiVirus

1. Nhấp Options trên cửa sổ chính Norton AntiVirus.
2. Nhấp vào một hạng mục trong Options outline ở phía bên trái của hộp thoại Options.
Một nội dung mô tả ngắn gọn về hạng mục xuất hiện ở đầu cửa sổ.
3. Nhấp phải vào một tùy chọn bất kỳ và nhấp What's This? để tìm hiểu thông tin về tùy chọn đó.
4. Thay đổi bất kỳ xác lập nào mà bạn muốn.

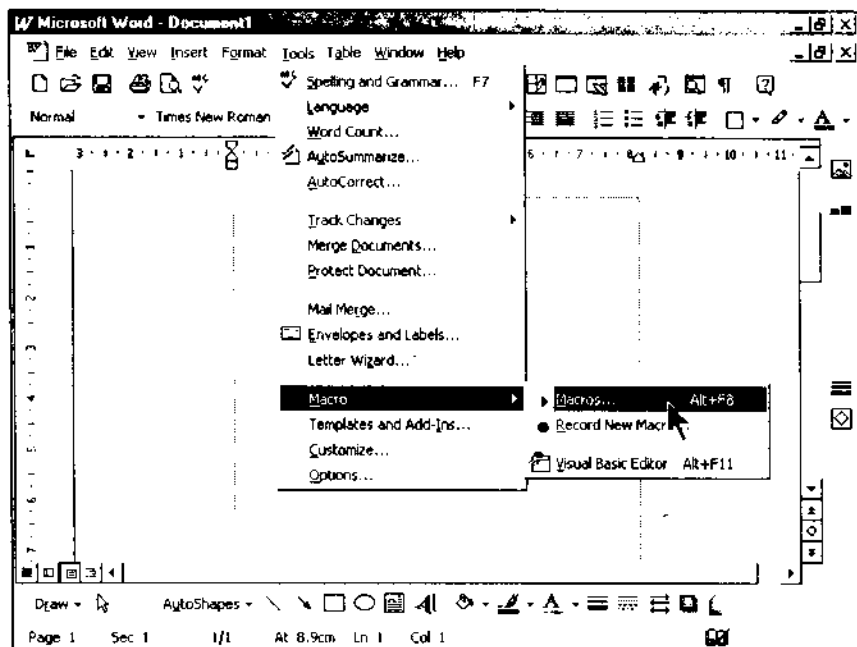


5. Nhấp OK để đóng và thoát khỏi màn hình. (Nếu bạn không nhấp OK, bạn sẽ mất tất cả những thay đổi mà bạn đã thực hiện).

Bây giờ các xác lập này có thứ tự ưu tiên cao hơn so với các tùy chọn đã xác lập sẵn. Bạn không cần khởi động lại máy tính.

III. Loại bỏ một virus macro Microsoft Word

1. Đóng Word và đặt lại tên cho file Normal.dot là Name.dot.
2. Mở Word và xác nhận rằng Macro và Customize đang nằm trên menu Tools.

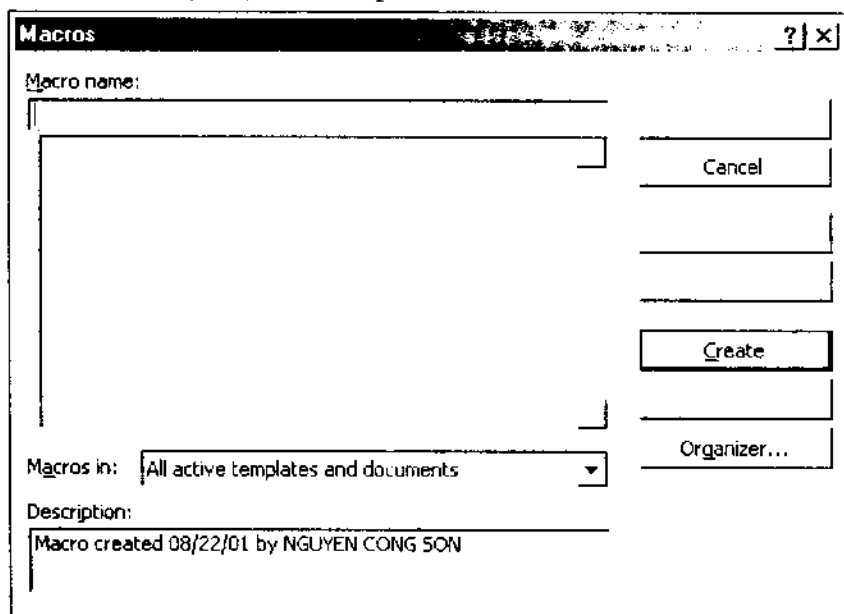


3. Mở một tài liệu mới và trên menu Insert, hãy nhấp File.
4. Định hướng đến folder có chứa file bị nhiễm.
5. Nhấp để chọn file bị nhiễm.
6. Nhấn giữ phím SHIFT và nhấp OK.
7. Tiếp tục giữ phím SHIFT cho đến khi file bị nhiễm được mở trong Word.

Ghi chú

Việc nhấn giữ phím SHIFT trong khi mở một file sẽ giữ không cho bất kỳ macro tự động nào của Word chạy.

- Để xem có bất kỳ macro nào trong tài liệu mới hay không, hãy trở đến Macro trên menu Tools, và sau đó nhấp Macro. Trong danh sách Macro In, hãy nhấp "All active templates and document". Dưới Macro Name, sẽ không có bất kỳ macro nào được liệt kê. Nhấp Cancel.

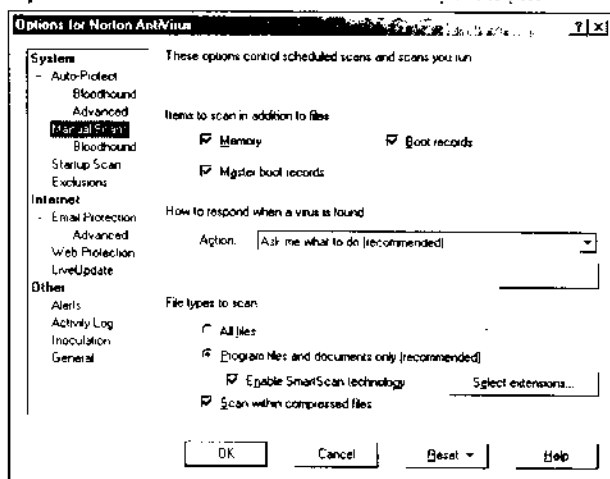


- Lưu file với một tên khác.
- Xóa file bị nhiễm.

IV. Chọn hành động mà Norton AntiVirus sẽ thực hiện khi một virus được tìm thấy trong suốt tiến trình quét bằng tay hay quét theo thời biểu:

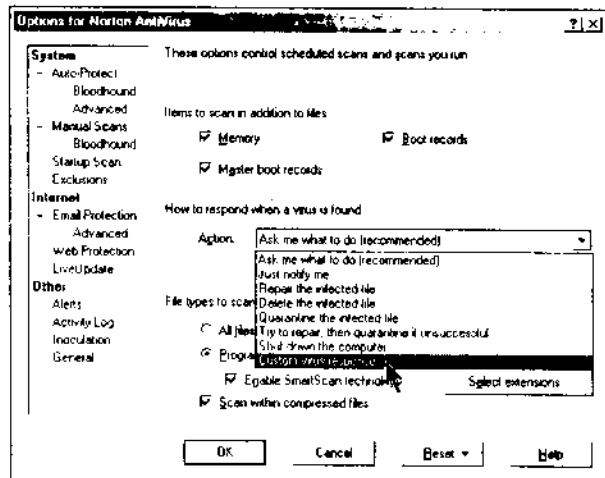
- Nhấp Options trên cửa sổ chính Norton AntiVirus.

2. Nhấp Manual Scans nếu nó chưa được chọn.

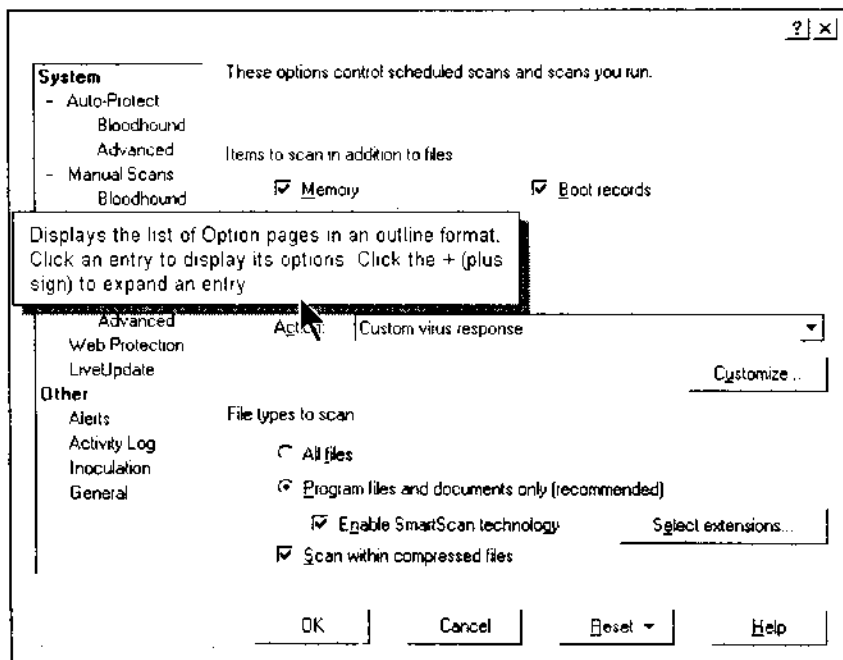


3. Chọn một tùy chọn bất kỳ trong hộp danh sách xổ xuống How To Respond.

Nếu bạn chọn Custom Virus Response, hãy nhấp nút Customize để hiển thị một hộp thoại mà trong đó bạn có thể chỉ định các tùy chọn nào mà bạn muốn Norton AntiVirus tạo sẵn cho ba loại virus lây nhiễm: các virus file, các virus record khởi động, và các virus macro.



4. Nhấp phải vào một tùy chọn bất kỳ và nhấp What's This? để tìm hiểu thêm thông tin về tùy chọn đó.



5. Nhấp OK để lưu các xác lập và thoát khỏi hộp thoại.

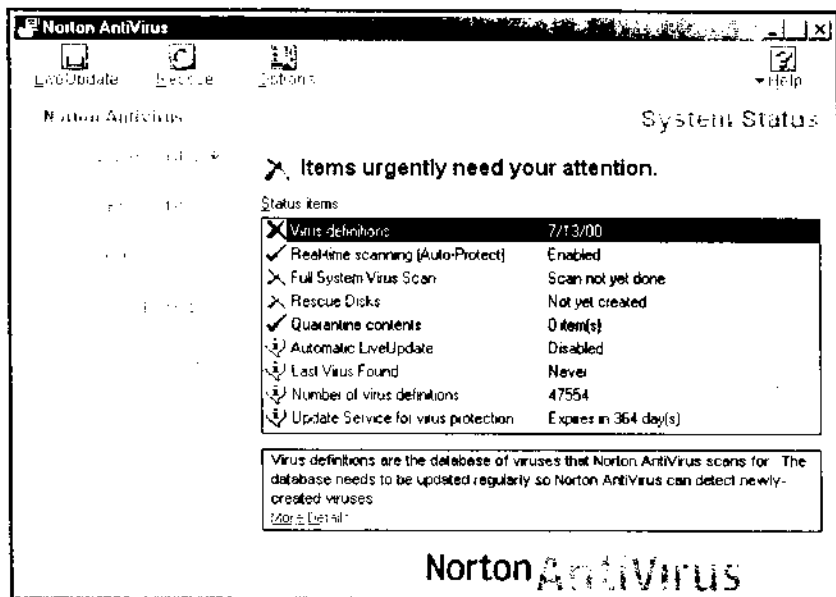
V. Loại bỏ một file bị nhiễm

1. Nhấp Delete trong hộp cảnh báo trong hộp Norton AntiVirus, sau đó thực hiện theo các dòng nhắc trên màn hình.
Nếu nút Delete ở dạng chìm mờ, Norton AntiVirus đã không được cấu hình để bật nó hoặc hạng mục không thể được xóa.
2. Sau khi xóa các file bị nhiễm, hãy quét tất cả các ổ đĩa và các đĩa mềm bằng Norton AntiVirus để xác nhận không có file nào khác bị nhiễm virus.
3. Ngay sau khi bạn đã chắc chắn rằng hệ thống của mình không bị nhiễm virus, hãy thay các file mà bạn đã xóa bằng các bản

sao không bị nhiễm. (Bảo đảm bạn đã quét các file thay thế trước khi sao chép chúng sang đĩa cứng).

Nếu bạn không nhớ file nào cần được thay thế, hãy xem Activity Log để tìm tên file.

Bạn không thể phục hồi các file đã được xóa bởi Norton AntiVirus ngay cả với các tiện ích phục hồi phải đặc biệt, chẳng hạn như Norton Utilities. Bảo đảm bạn có một bản sao không bị nhiễm của file trước khi xóa nó. Tuy nhiên, ngay cả khi bạn không có một bản sao sạch (không bị nhiễm) của file, bạn vẫn cần xóa file bị nhiễm. Bạn không nên giữ lại file đã bị nhiễm virus trên đĩa của bạn. Bạn có thể nhận một bản sao mới của file từ nhà sản xuất.



VI. Sử dụng Help

1. Tìm sự trợ giúp:

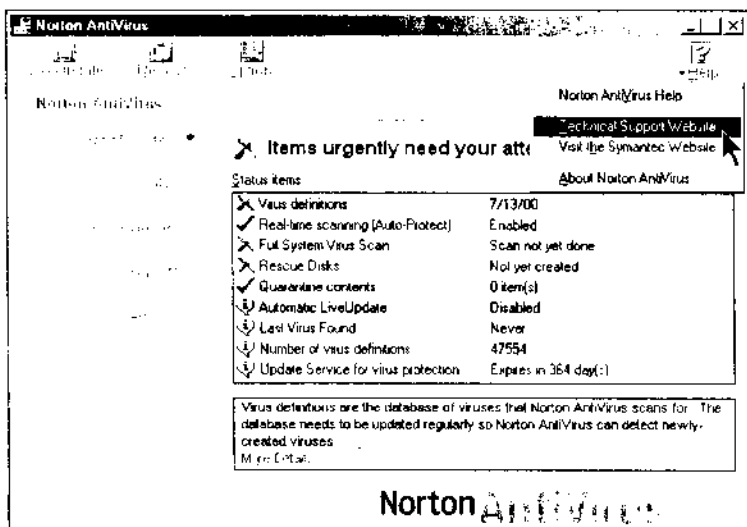
Thực hiện một trong các thao tác sau đây:

- ❖ Chọn Norton AntiVirus từ menu Help.
- ❖ Từ hộp thoại Norton AntiVirus:

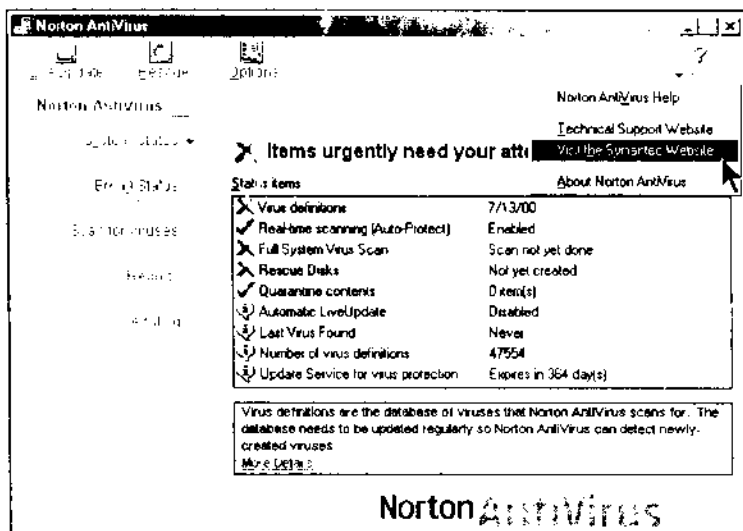
Nhấp nút Help.

Nhấp phải vào một tùy chọn bất kỳ trên màn hình Norton AntiVirus và chọn What's This? để xem phần định nghĩa ngắn gọn về tùy chọn.

❖ Chọn Technical Support Website từ menu Help.



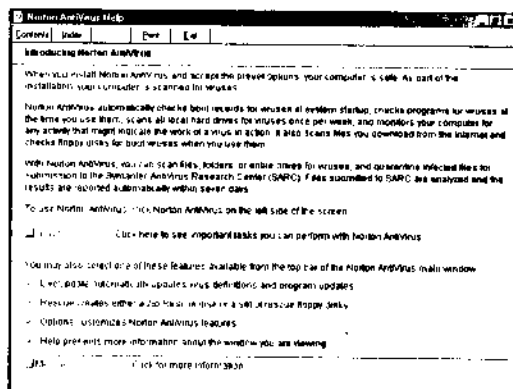
❖ Chọn Visit The Symantec Website từ menu Help.



Bạn có thể để mở cửa sổ Help trên màn hình bằng cách thu nhỏ tối đa cửa sổ Help hoặc bằng cách nhấp nhiều lần vào giữa cửa sổ Help và sản phẩm.

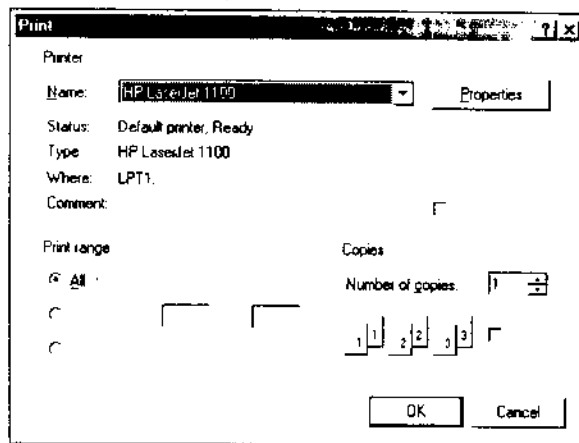
2. Các menu Help

Các menu sau đây có sẵn từ các cửa sổ chính về chủ điểm trợ giúp:



File

- ❖ Nhấp Open để chọn từ một danh sách các file trợ giúp có sẵn khác.
- ❖ Nhấp Print Topic để hiển thị một hộp thoại print mà bạn có thể in chủ điểm hiện hành từ đó.



❖ Nhấp Exit để đóng hộp thoại trợ giúp.

Edit

Chọn nội dung trợ giúp để sao chép sang một file khác hoặc nhấp Annotate để tạo ký hiệu trợ giúp riêng của bạn. Sau đó, để xem ký hiệu này, hãy nhấp vào biểu tượng kẹp giấy ở kế bên phần nội dung trợ giúp.

Bookmark

Nhấp Define và đặt tên cho bookmark để bạn có thể sử dụng nó vào việc tìm lại chủ điểm, và sau đó nhấp OK để lưu các xác lập và thoát khỏi hộp thoại.

Để trở lại chủ điểm này, hãy nhấp bookmark, và sau đó nhấp vào tên chủ điểm.

Options

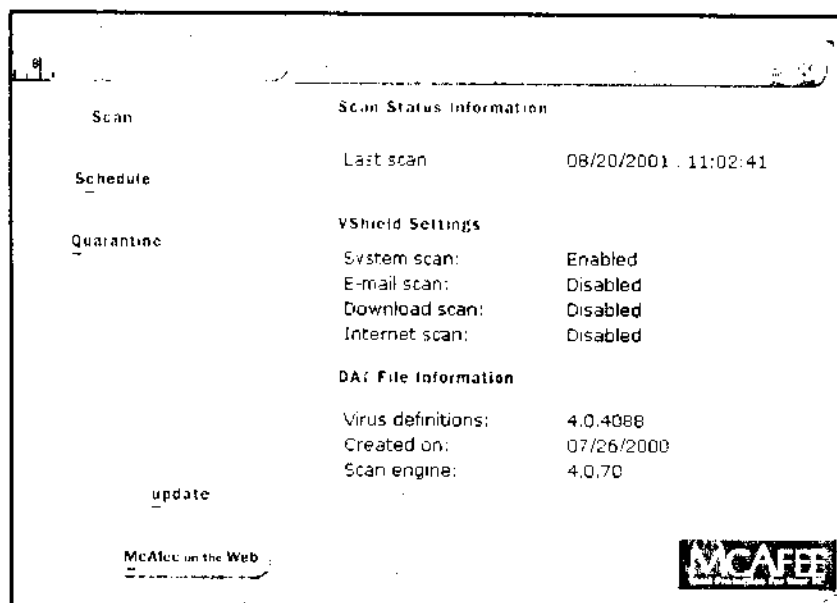
Xác lập nhiều tùy chọn về cách hiển thị nội dung trợ giúp bao gồm cả cách hiển thị của các menu Help. Bạn có tùy chọn để xem thanh nút chuẩn, vốn hiển thị các tùy chọn, chẳng hạn như Contents, Index, và v.v...

3. Xem trình trợ giáo trực tuyến

1. Nhấp <http://www.symantec.com/techsupp/tutorial/nav2001/> để đến Web site của Symantec.
2. Nhấp vào nút thích hợp ở kế bên trình trợ giáo mà bạn muốn xem.

PHẦN 2

McAfee VirusScan



Bài 6

TÌM HIỂU TRÌNH ỨNG DỤNG VIRUSSCAN

Các sản phẩm desktop anti-virus của McAfee sử dụng hai phương pháp chung để bảo vệ hệ thống. Phương pháp thứ nhất là quét nền. Phương pháp này hoạt động liên tục theo dõi các virus khi bạn sử dụng máy tính cho các công việc hàng ngày. Trong sản phẩm VirusScan, VShield scanner thực hiện chức năng này.

Phương pháp thứ hai là trách nhiệm của bạn. Bạn quyết định khi nào và nơi nào phần mềm sẽ tìm virus, sau đó bạn chỉnh sửa và chạy các hoạt động phù hợp với nhu cầu của mình. Bạn có thể chạy các hoạt động đồng thời hoặc liên tiếp nhau, tạo các xác lập khác nhau, chỉ định các mục đích quét khác nhau cho các hoạt động, và lưu các xác lập trong các file có thể xuất để sử dụng sau này.

Trình ứng dụng này hoạt động trong hai chế độ:

- ❖ Chế độ VirusScan "Classic". Giao diện này chạy rất nhanh với các tùy chọn cấu hình tối thiểu, nhưng có đầy đủ tính năng của công cụ quét McAfee anti-virus. Để xem diện mạo của giao diện này, hãy nhấp [here](#):
- ❖ Chế độ VirusScan Advanced. Giao diện này làm tăng thêm tính linh hoạt cho các tùy chọn cấu hình của chương trình, bao gồm khả năng chạy đồng thời nhiều hoạt động quét. Để xem diện mạo của giao diện này, hãy nhấp [here](#).

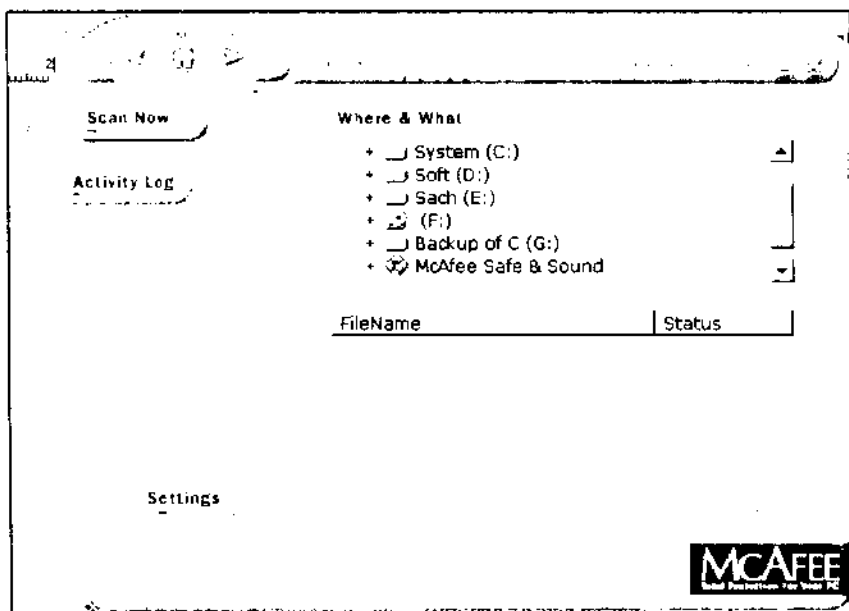
Để xem phần so sánh tính năng giữa hai chế độ, hãy nhấp [here](#):

Ngoài ra, bất kỳ tác vụ quét nào mà bạn tạo và cấu hình trong VirusScan sẽ khởi động trình ứng dụng VirusScan khi chúng chạy.

Các tùy chọn cấu hình đối với tác vụ này sẽ hơi khác với các tùy chọn cấu hình có sẵn trong cửa sổ trình ứng dụng, nhưng cùng một trình ứng dụng chạy trong cả hai trường hợp.

I. Khi nào và tại sao cần sử dụng trình ứng dụng VirusScan

Việc duy trì một môi trường tính toán an toàn có nghĩa là phải quét virus đều đặn. Phụ thuộc vào mức độ hoán đổi các đĩa mềm với những người sử dụng, sự chia sẻ các file trên mạng cục bộ, hoặc sự tương tác với các máy tính khác của Internet, việc quét “đều đặn” có thể là quét ít nhất mỗi tháng một lần, hoặc một ngày nhiều lần. Tốt nhất là nên quét ngay trước khi bạn sao lưu dữ phòng dữ liệu, quét trước khi bạn cài đặt phần mềm mới hay phần mềm nâng cấp, đặc biệt là phần mềm mà bạn tải từ các máy tính khác, và quét khi bạn khởi động hay tắt máy tính của mình mỗi ngày.



Chúng ta phải quét virus đều đặn cho hệ thống bởi vì:

- ❖ Sự quét nền sẽ kiểm tra các file khi chúng thực thi. VShield

scanner tìm mã virus khi các file khả thi chạy hoặc khi bạn đọc một đĩa mềm, nhưng trình ứng dụng VirusScan có thể kiểm tra các ký hiệu mã trong các file được chứa theo đĩa cứng của bạn. Nếu bạn ít khi chạy một file bị nhiễm, VShield scanner không thể tìm thấy virus cho đến khi nó hủy việc tải. Tuy nhiên, trình ứng dụng VirusScan có thể dò tìm một virus mà nó đang chờ cơ hội để chạy.

- ❖ Các virus luôn có tính xâm nhập. Nếu bạn vô tình để một đĩa mềm trong ổ đĩa khi khởi động máy tính, một virus có thể xâm nhập vào bộ nhớ trước khi VShield scanner đặc biệt là khi bạn chưa cấu hình scanner để quét các đĩa mềm. Nhưng sau khi xâm nhập vào bộ nhớ, virus có thể lây nhiễm bất kỳ chương trình nào bao gồm cả VShield scanner.
- ❖ VShield scanner đòi hỏi phải có thời gian và các nguồn tài nguyên. Việc quét virus khi bạn chạy, sao chép hay lưu các file có thể bị trì hoãn, mặc dù sự khởi động phần mềm và các tác vụ khác chỉ mất một khoảng thời gian rất nhỏ.
- ❖ Trong hệ thống mạng phần lớn là những người sử dụng máy tính ngày nay làm việc trên đó, việc tải một virus từ một nguồn mà bạn chưa hề biết có thể chỉ mất một vài giây. Nếu sự xung đột phần mềm làm tắt sự quét nền trong khoảng thời gian đó, hoặc nếu bạn chưa cấu hình sự quét nền để theo dõi một điểm truy cập nào đó, bạn có thể gặp virus. Các hoạt động quét đều đặn thường giúp tránh sự lây lan virus hay bất kỳ hư hại nào.

Nếu bạn thường xuyên nối kết Internet hoặc tải xuống các file, bạn có thể cần lập thời biểu quét virus đều đặn cho hệ thống vào những thời khoảng nhất định, để bạn không phải ghi nhớ việc khởi động trình ứng dụng VirusScan. VirusScan Console cung cấp các tùy chọn rất linh hoạt cho mục đích này.

II. Xác định trình ứng dụng VirusScan

Trình ứng dụng VirusScan có nhiều file liên quan được chứa trong hai vị trí chung trên đĩa cứng. Phần lớn các file mà trình ứng dụng cần

cho các chức năng quét nhất định, cập nhật các file để diệt virus, và gởi các thông tin cảnh báo nằm trong các folder con trong folder McAfee VirusScan Common Files. Nếu bạn đã cài đặt phần mềm theo vị trí mặc định của nó, bạn sẽ tìm thấy folder này trong vị trí sau đây:

C:\Program Files\Common Files\McAfee VirusScan

SCAN32.EXE, file khả thi trình ứng dụng, cũng nằm trong folder Common Files, như trong folder con của riêng nó. Trong các tiến trình cài đặt mặc định, bạn sẽ tìm thấy nó trong vị trí sau đây:

C:\Program Files\Common Files\McAfee VirusScan\On Demand Scanner\Scan32\SCAN32.EXE

Bạn có thể chạy SCAN32.EXE từ một dòng lệnh Windows để khởi động trình ứng dụng. Để tìm hiểu thêm, hãy nhấp [here](#):

Nhiều file thư viện khác mà trình ứng dụng cần cũng nằm trong thư mục chương trình VirusScan, bạn sẽ tìm thấy nó trong vị trí sau đây:

III. Các file phụ thuộc và liên quan đối với trình ứng dụng VirusScan

Trình ứng dụng VirusScan chạy ở dạng một file khả thi riêng biệt mà bạn có thể tự mình khởi động nó, hoặc VirusScan Consol có thể khởi động theo thời biểu mà bạn đã lập. Trình ứng dụng này cần nhiều file hỗ trợ để thực hiện chức năng, bao gồm một số file liên quan đến công cụ quét McAfee. Bảng sau đây liệt kê trình ứng dụng VirusScan và các file liên quan:

Các file chương trình

Các file này chạy trực tiếp ở dạng các file trình ứng dụng VirusScan hoặc ở dạng các file hỗ trợ hay thư viện trình ứng dụng VirusScan riêng biệt.

File	Chức năng	Vị trí
SCAN32.EXE	File khả thi trình ứng dụng VirusScan. Chạy trong tất cả môi trường Windows 32-bit	C:\Program Files\McAfee VirusScan\VirusScan
ADVGUI.DLL	File thư viện trình ứng dụng VirusScan. Cung cấp các thành phần giao diện người dùng cho giao diện VirusScan Advanced	C:\Program Files\McAfee VirusScan\VirusScan

Các file phụ thuộc

Trình ứng dụng VirusScan cần các file này để chạy vào các thời điểm khác nhau trong suốt quá trình hoạt động của nó, nhưng đây không phải là các file chương trình ứng dụng VirusScan, hoặc không dành riêng cho sự hỗ trợ trình ứng dụng VirusScan.

File	Chức năng	Vị trí
AVSYNMGR.EXE	Dịch vụ quản lý VirusScan. Khởi tạo, khởi động và ngưng tất cả các dịch vụ VirusScan và các thành phần. Phải chạy để bật tất cả các thành phần VirusScan.	C:\Program Files\McAfee VirusScan\VirusScan
AVSYNCH.DLL	Điều khiển sự giao tiếp giữa các thành phần thông qua bộ nhớ dùng chung	C:\Program Files\McAfee VirusScan\VirusScan
SYNCUTIL.DLL	Chứa dữ liệu dùng chung giữa các thành phần	C:\Program Files\McAfee VirusScan\VirusScan

VSUTIL.DLL	Cung cấp các tiện ích chung cho các thành phần	C:\Program Files\ McAfee VirusScan\ VirusScan
AVSMCPA.CPL	VirusScan control panel applet	C:\Windows\System or C:\Winnt\System 32
RESDLL.DLL	File nguồn tài nguyên dành cho tất cả thành phần VirusScan	C:\Program Files\ Common Files\ McAfee VirusScan\ McPal
MCSCAN32.DLL	File công cụ McAfee Scan	C : \ P r o g r a m Files\Common Files\McAfee Virus Scan\ VirusScan Engine\ 4.0.xx
RWABS16.DLL	File hỗ trợ đối với công cụ quét	C:\Program Files\ Common Files\ McAfee VirusScan\ VirusScan Engine\ 4.0.xx
RWABS32.DLL	File hỗ trợ đối với công cụ quét	C:\Program Files\ Common Files\ McAfee VirusScan\ VirusScan Engine\ 4.0.xx
MESSAGES.DAT	File hỗ trợ đối với công cụ quét. Cung cấp các thông báo dò tìm virus cho công cụ	C:\Program Files\ Common Files\ McAfee VirusScan\ VirusScan Engine\ 4.0.xx
S95EXT.DLL	File phần mở rộng Shell. Cho phép bạn nhấp phải vào các file xác lập VSC mà bạn ghi và khởi động	C:\Program Files\ McAfee VirusScan\ VirusScan

các hoạt động quét hoặc
xem các đặc tính của tác
vụ quét.

Các file tạm thời

Trình ứng dụng VirusScan và các file liên quan của nó sử dụng các file này là “các bản đồ bộ nhớ” để chứa các tùy chọn cấu hình đã sao chép từ phần đăng ký Windows khi chương trình chạy. Các file này bắt đầu với một kích cỡ file chuẩn và dữ liệu tối thiểu, mở rộng hoặc thu nhỏ khi cần thiết để chứa dữ liệu cấu hình.

File	Chức năng	Vị trí
SYNC_MAP. MMF	File bản đồ bộ nhớ dành cho AVSYNCH.DLL	C:\Program Files\ McAfee VirusScan\
AVCONSOLE .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
DAV_CONS .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
DAV_EXCL .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
DAV_SCAN .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
DSCANDEF .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
DSCANDEF .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan

DVS_EXCL .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
VSCANGEN .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
VSCANODS .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan

IV. Khởi động trình ứng dụng VirusScan

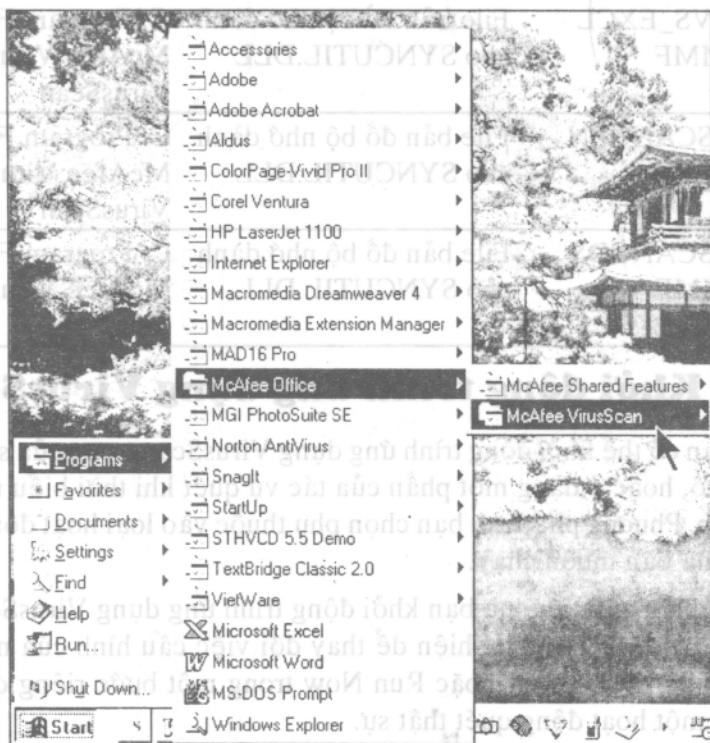
Bạn có thể khởi động trình ứng dụng VirusScan trong cửa sổ riêng của nó, hoặc ở dạng một phần của tác vụ quét khi thời biểu mà bạn đã lập. Phương pháp mà bạn chọn phụ thuộc vào loại hoạt động quét nào mà bạn muốn chạy.

Khi lần đầu tiên mà bạn khởi động trình ứng dụng VirusScan, nó mở để bạn có thể thực hiện để thay đổi việc cấu hình của nó. Bạn phải nhấp Scan Now hoặc Run Now trong một bước riêng để khởi động một hoạt động quét thật sự.

Nhấp các nút ở kế bên mỗi hạng mục được liệt kê để tìm hiểu thêm về các phương pháp khác nhau mà bạn có thể sử dụng để khởi động trình ứng dụng:

Phương pháp 1: Hiển thị của sổ chính trình ứng dụng VirusScan

Nhấp Start trong thanh tác vụ Windows, trở đến Program, sau đó trở đến McAfee VirusScan. Kế tiếp, hãy chọn McAfee VirusScan.



Cửa sổ chính VirusScan Classic xuất hiện. Từ đây, bạn có thể:

- ❖ Bắt đầu quét ngay lập tức. Nhấp Scan Now để trình ứng dụng quét hệ thống với các tùy chọn cấu hình mà bạn đã xác lập sau cùng, hoặc với các tùy chọn mặc định.
- ❖ Chuyển đổi giữa các giao diện Classic và Advanced. Sử dụng giao diện Classic cho các hoạt động quét nhanh và đơn giản vốn sử dụng các xác lập mặc định. Để chuyển sang giao diện Advanced từ đó, hãy chọn Advanced từ menu Tools.
- ❖ Sử dụng giao diện Advanced để điều khiển hầu hết mọi khía cạnh của hoạt động quét. Để trở lại giao diện Classic từ điểm đó, hãy chọn Classic từ menu Tools.
- ❖ Cấu hình các tùy chọn quét mới. Chỉ định các file nào cần quét, sau đó chọn các tùy chọn trả lời, báo cáo, cảnh báo và

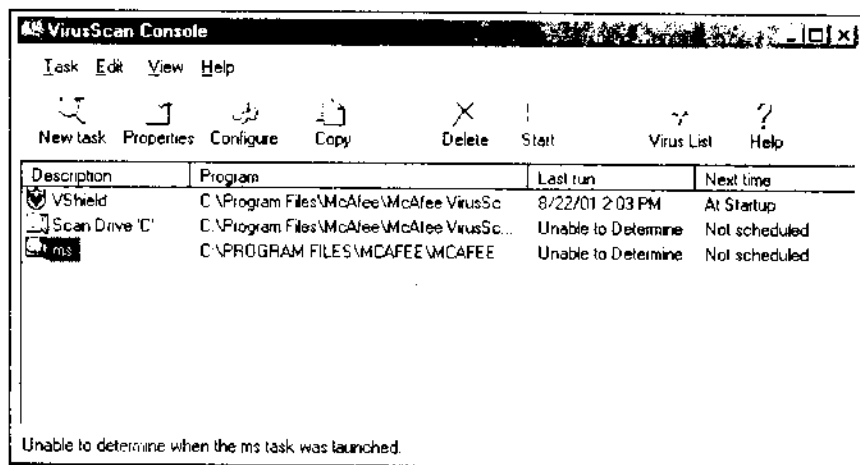
loại bỏ trong mỗi trang đặc tính. Để tìm hiểu thêm về các tùy chọn, hãy nhấp [here](#):

Kế tiếp, hãy nhấp nút New Scan ở bên phải của cửa sổ - hoặc chọn Save As Default từ menu File - để lưu các tùy chọn mà bạn đã chọn ở dạng các tùy chọn mặc định. Các tùy chọn này sẽ điều khiển mỗi hoạt động rất mới mà bạn chạy từ điểm đó. Bạn có thể thay đổi các tùy chọn thường xuyên, sau đó lưu chúng trở lại theo cùng cách để thay đổi các tùy chọn cũ bằng các tùy chọn mới. Chọn Save Settings từ menu File để lưu các tùy chọn của bạn vào một file xác lập. Bạn có thể sử dụng file này để chạy các hoạt động quét sau này hoặc gửi nó đến các máy tính khác để điều khiển các hoạt động quét của các máy tính đó.

- ❖ Xem activity log dành cho trình ứng dụng VirusScan. Chọn View Activity Log từ menu File để mở file VSCLOG.TXT trong cửa sổ Notepad.
- ❖ Bảo vệ các xác lập của bạn bằng một password. Chọn password Protect từ menu Tools để mở một hộp thoại bạn có thể sử dụng hộp thoại này để khóa bất kỳ trang đặc tính nào của trình ứng dụng VirusScan. Chọn mỗi trang đặc tính mà bạn muốn bảo vệ, sau đó nhấp nút Password ở bên phải để gán một password.

Phương pháp 2: Khởi động một tác vụ quét từ VirusScan Console

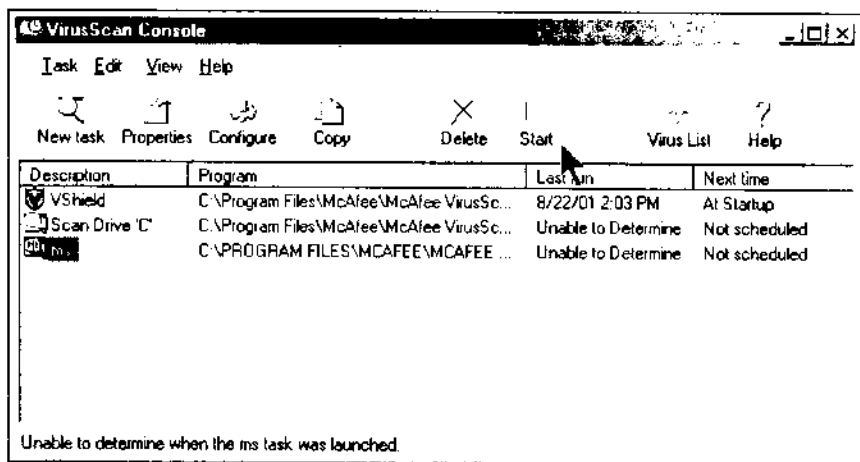
Nhấp đúp vào biểu tượng VirusScan Console () trong hệ thống Windows để hiển thị cửa sổ Console.



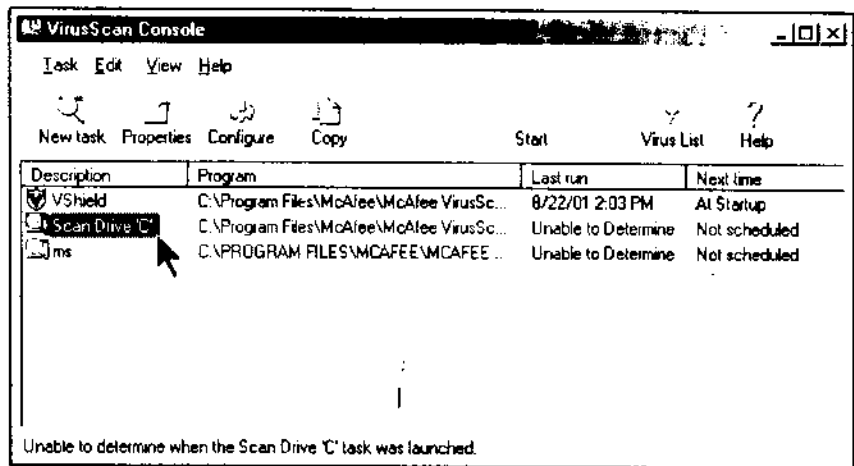
Nếu biểu tượng này không xuất hiện trong hệ thống, hãy nhấp Start trong thanh tác vụ Windows, trở đến Programs, sau đó trở đến McAfee VirusScan. Kế tiếp, hãy chọn VirusScan Console.

Console có hai tác vụ đã được xác lập sẵn, các tác vụ này sử dụng trình ứng dụng VirusScan để chạy - Scan My Computer và Scan Drive "C". Bạn có thể :

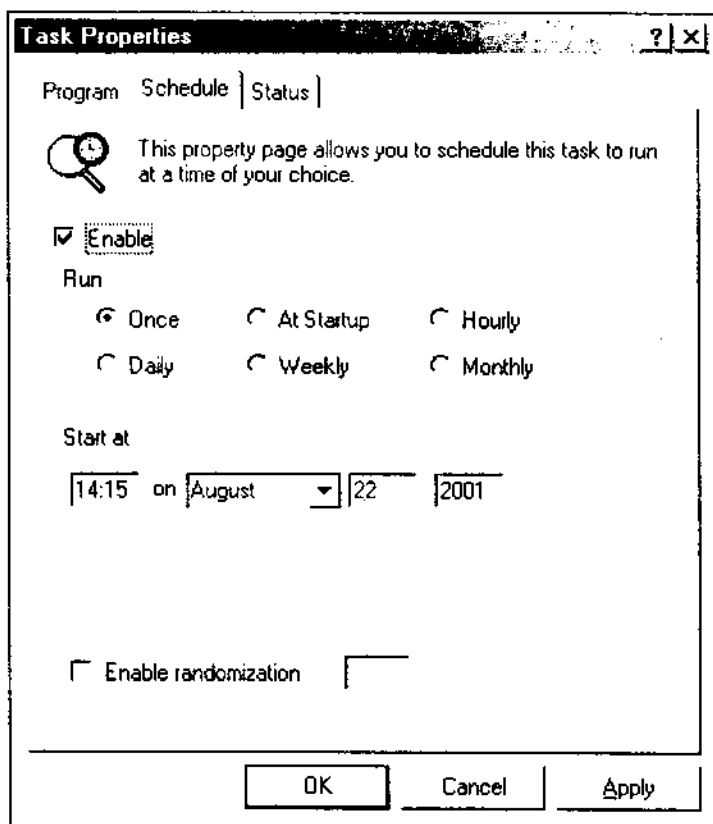
- ❖ Khởi động một trong các tác vụ đã xác lập sẵn trong cấu hình mặc định của nó. Chọn một tác vụ trong danh sách tác vụ, sau đó nhấp trong thanh công cụ Console (). Nếu tác vụ quét được xác lập để khởi động tự động, cửa sổ trình ứng dụng VirusScan sẽ mở và tác vụ sẽ chạy ngay lập tức. Nếu tác vụ không được xác lập để khởi động tự động, cửa sổ sẽ mở, nhưng bạn phải nhấp Scan Now để khởi động.



- ❖ Tạo và lập thời biểu cho một tác vụ mới của riêng bạn. Nhấp () trong thanh công cụ Console để mở hộp thoại Task Properties. Đặt tên cho tác vụ, chọn các tùy chọn bảo đảm an toàn cho nó, hãy chỉ định cách mà bạn muốn nó xuất hiện khi nó chạy và bạn muốn nó thực hiện điều gì khi nó hoàn tất. Để xác lập các tùy chọn cấu hình cho tác vụ, hãy nhấp nút Configure ở cuối trang đặc tính. Để tìm hiểu về các tùy chọn.



Kế tiếp, hãy nhấp nhấn Schedule để chỉ định khi nào tác vụ sẽ chạy. Chọn hộp kiểm Enable task để chuẩn bị chạy nó theo thời gian đã định. Để tìm hiểu về cách lập thời biểu cho tác vụ.



Phương pháp 3: Khởi động một tác vụ quét từ một file xác lập

Bạn có thể sử dụng bất kỳ file xác lập nào mà bạn đã lưu với các tùy chọn cấu hình riêng của bạn để khởi động trình ứng dụng VirusScan.

Xác định và nhấp đúp vào một file xác lập mà bạn đã lưu từ cửa sổ trình ứng dụng VirusScan.

Thao tác này sẽ mở cửa sổ trình ứng dụng VirusScan và tải các

tùy chọn cấu hình mà bạn đã lưu. Bạn cũng có thể mở cửa sổ này và tải các xác lập bằng cách nhấp phải vào các file, sau đó chọn Start từ menu tắt.

Thông thường, bạn sẽ tìm các file xác lập trong thư mục chương trình VirusScan, nhưng bạn có thể lưu các file xác lập ở bất kỳ nơi nào trên đĩa cứng. Các file xác lập VirusScan có phần mở rộng .VSC.

• Khi cửa sổ VirusScan xuất hiện, hãy nhấp Scan Now để bắt đầu hoạt động quét với các xác lập mà bạn đã chỉ định.

Bạn cũng có thể thay đổi các xác lập trước khi chạy tác vụ quét. Để thực hiện điều này, hãy thực hiện một trong các thao tác sau đây:

- ❖ Mở cửa sổ trình ứng dụng VirusScan theo các bước đã mô tả ở trên, sau đó thay đổi các tùy chọn cấu hình trong mỗi trang đặc tính.
- ❖ Nhấp phải vào file xác lập .VSC, sau đó chọn Properties từ menu tắt.

Thao tác này sẽ mở hộp thoại Properties với các nhãn cấu hình tương tự như các nhãn có sẵn khi bạn cấu hình trình ứng dụng VirusScan từ VirusScan Console. Để xem diện mạo của hộp thoại Properties này, hãy nhấp [here](#):

Để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính này.

Phương pháp 4: Khởi động trình ứng dụng từ dòng lệnh

Nhấp Start trong thanh tác vụ Windows, trở đến Programs, sau đó chọn MS-DOS Prompt nếu máy tính của bạn chạy Windows 95 hoặc Windows 98. Nếu máy tính của bạn chạy Windows NT Workstation v4.0 hoặc Windows 2000 Professional, hãy chọn Command Prompt.

Windows hiển thị một cửa sổ nhắc lệnh. Nếu bạn đã cài đặt phần mềm VirusScan theo vị trí mặc định của nó, hãy thay đổi xem thư mục sau:

C:\Program Files\Common Files\McAfee VirusScan\On Demand Scanner\Scan32

Kế tiếp, hãy gõ nhập dòng sau đây vào dòng nhắc lệnh:

```
scan32.exe <scan target> /<configuration options>
```

Ở đây, <scan target> có nghĩa là bất kỳ ổ đĩa, đường dẫn thư mục hay tên file nào mà bạn muốn trình ứng dụng kiểm tra. Chỉ định các ổ đĩa có các tên theo kiểu DOS - chẳng hạn C hoặc D: - và cung cấp các tên đường dẫn đầy đủ cho các thư mục theo các quy ước dành sẵn cho hệ điều hành của bạn. Bạn có thể sử dụng các tên dài trên các hệ thống Windows NT Workstation v4.0 và Windows 2000 Professional, nhưng bạn phải sử dụng các tên bị cắt ngắn trên các hệ thống Windows 95 và Windows 98.

Sau scan target là tập hợp các tùy chọn cấu hình, nếu có, mà bạn muốn hoạt động quét này sử dụng khi nó chạy.

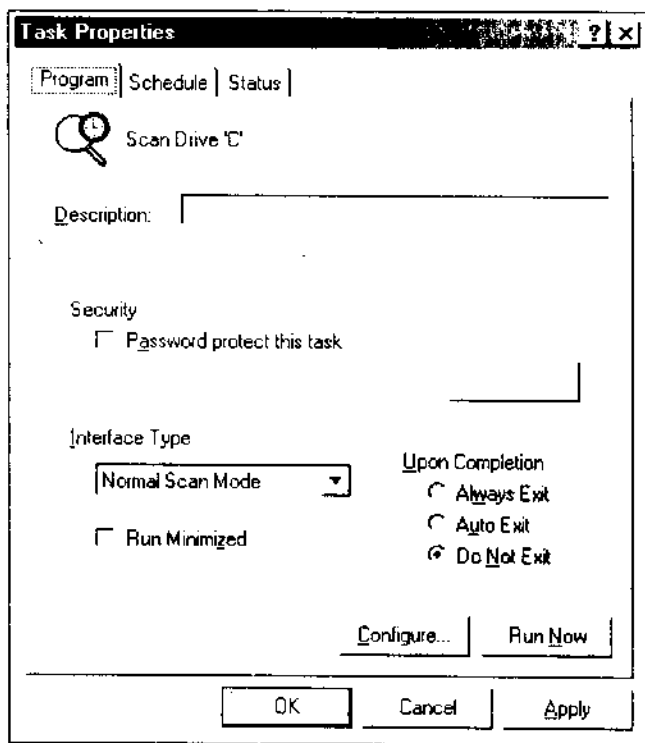
Đặt trước mỗi tùy chọn một dấu /. Mặc dù trình ứng dụng sẽ cho phép bạn chỉ định một số tùy chọn không có dấu /, nhưng việc chỉ định các dấu khác sẽ cho ra một lỗi. Bạn có thể chỉ định bất kỳ tham số cần thiết nào cho các tùy chọn không có ký hiệu đặc biệt.

Phụ thuộc vào các tùy chọn dòng lệnh mà bạn chọn, việc khởi động trình ứng dụng bằng cách này có thể chạy một hoạt động quét hoặc hiển thị cửa sổ trình ứng dụng VirusScan, trong cửa sổ này bạn có thể chọn các tùy chọn cấu hình cho hoạt động quét.

V. Ngưng trình ứng dụng VirusScan

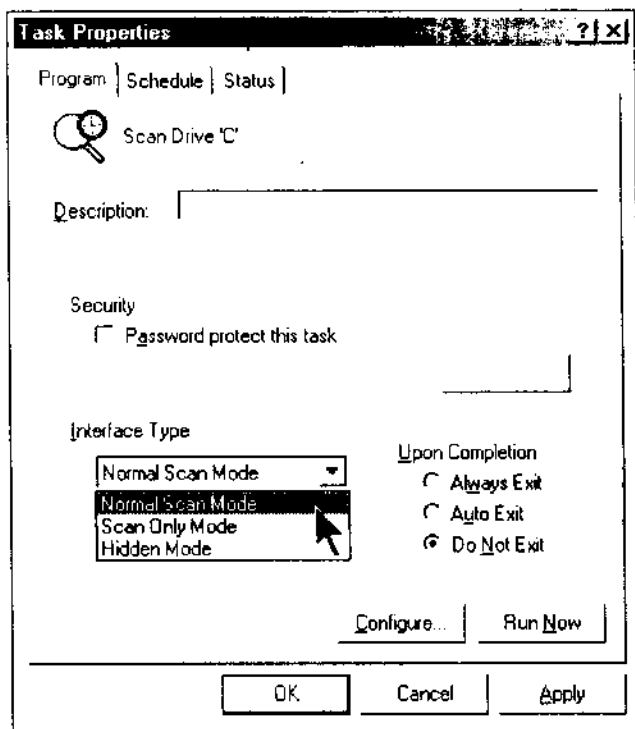
Trình ứng dụng VirusScan có hai trạng thái hoạt động phân biệt:

- ❖ Chạy một hoạt động quét. Trong trạng thái này, VirusScan đã thật sự bắt đầu vào một hoạt động quét và đang tìm virus trong các đích quét mà bạn chỉ định.
- ❖ Mở và kích khởi cấu hình. Trong trạng thái này, cửa sổ trình ứng dụng VirusScan - hoặc hộp thoại Task Properties dành cho một tác vụ cụ thể - được mở. Bạn có thể sử dụng cửa sổ hoặc hộp thoại này để cấu hình và lưu các xác lập quét, như trình ứng dụng sẽ không bắt đầu chạy cho đến khi bạn nhấp các nút Scan Now hoặc Run Now, hoặc cho đến khi bắt đầu một tác vụ quét theo thời biểu.



Để ngưng một hoạt động quét đang diễn ra, bạn có thể:

- ❖ Nhấp Stop trong cửa sổ trình ứng dụng VirusScan. Bạn có thể sử dụng tùy chọn này nếu bạn đã bắt đầu hoạt động quét từ chính cửa sổ trình ứng dụng, hoặc nếu bạn đã bắt đầu một tác vụ quét theo thời biểu với loại giao diện Normal Scan Mode. Tùy chọn này vẫn để mở cửa sổ trình ứng dụng hoặc hộp thoại Task Properties.



Nhấp **■** để ngưng một tác vụ quét đang chạy với loại giao diện Scan Only. Để xem diện mạo của trình ứng dụng khi nó sử dụng giao diện này.

Việc ngưng một hoạt động quét bằng cách này sẽ đóng ngay hộp thoại Scan Only **u**. Để hộp thoại này vẫn mở, hãy nhấp để tạm ngưng hoạt động quét, sau đó nhấp để bắt đầu lại nó **►**.

Nhấp Stop khi tùy chọn đó xuất hiện trong một thông tin cảnh báo đã tìm thấy virus. Tùy chọn này xuất hiện chỉ khi bạn yêu cầu trình ứng dụng hiển thị nó.

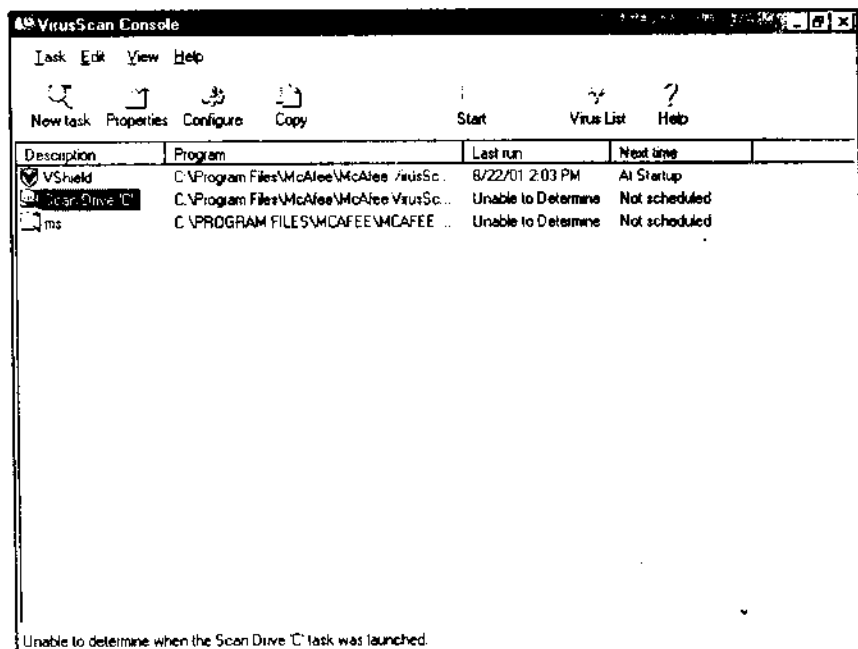
Nhấp Stop trong trang đặc tính VirusScan control panel Service. Thao tác này sẽ ngưng tất cả các thành phần VirusScan ngay lập tức, loại bỏ VShield scanner và VirusScan Console ra khỏi bộ nhớ. Nó cũng đóng tất cả các cửa sổ vào hộp thoại của thành phần VirusScan.

ngoại trừ chính VirusScan control.

Nếu bạn nhấp Start để tải lại các thành phần VirusScan, VShield scanner và VirusScan Console sẽ lại khởi động, nhưng trình ứng dụng VirusScan thì không, nó cũng sẽ không khởi động lại hoạt động quét trước đó. Để khởi động lại hoạt động quét, bạn phải mở cửa sổ trình ứng dụng và nhấp Scan Now, hoặc lập lại thời biểu cho tác vụ quét.

Để đóng các cửa sổ trình ứng dụng VirusScan hoặc các hộp thoại, bạn có thể:

- ❖ Chọn Close từ menu File trong cửa sổ trình ứng dụng VirusScan, hoặc nhấp vào hộp đóng chuẩn.
- ❖ Nhấp OK hoặc Cancel trong hộp Task Properties để trở lại cửa sổ VirusScan Console.



VI. Cấu hình các xác lập trình ứng dụng VirusScan

Bạn có thể chạy trình ứng dụng VirusScan để điều khiển các hoạt động quét chuyên biệt vào bất kỳ lúc nào, hoặc bạn có thể cài đặt một tác vụ quét vốn chạy trình ứng dụng vào các thời khoảng đã xác lập trước. Mặc dù mỗi phương pháp khởi động và sử dụng trình ứng dụng như nhau, nhưng cách mà bạn cấu hình các xác lập cho tác vụ quét và cách mà bạn sử dụng trình ứng dụng để quét hệ thống thì khác nhau.

Phần mềm VirusScan phản ánh điểm khác biệt đó trong hai phương pháp mà nó cung cấp cho bạn để cấu hình trình ứng dụng.

- ❖ Mở cửa sổ chính dành cho trình ứng dụng VirusScan - hoặc trong một giao diện Classic hoặc trong giao diện Advanced - để xác lập các tùy chọn cho các hoạt động quét mà bạn dự định chạy “theo yêu cầu” hoặc nói cách khác là bất kỳ khi nào cần thiết.
- ❖ Khởi động VirusScan Console để xác lập các tùy chọn cho một tác vụ quét mà bạn dự định chạy đều đặn và tự động. Bạn có thể chỉnh sửa một tác vụ quét hiện có hoặc tạo và cấu hình một tác vụ mới.

Nhấp vào các nút ở kế bên mỗi phương pháp được liệt kê để tìm hiểu các tùy chọn cấu hình:

Using the VirusScan Classic interface

Using the VirusScan Advanced interface

Scheduling VirusScan tasks

VII. Cấu hình giao diện VirusScan Classic

Để trình ứng dụng VirusScan bảo vệ hệ thống của bạn, bạn phải cho nó biết:

- ❖ Bạn muốn nó quét vùng nào
- ❖ Bạn muốn nó thực hiện điều gì nếu nó tìm thấy một virus

- ❖ Nó sẽ báo cho bạn biết bằng cách nào khi tìm thấy virus
- ❖ Bạn có muốn nó theo dõi các hành động của nó hay không

Một loạt các trang đặc tính trong cửa sổ VirusScan điều khiển các tùy chọn dành cho mỗi tác vụ - nhấp vào mỗi nhãn để cài đặt trình ứng dụng dành cho tác vụ của bạn. Để tìm hiểu thêm nhiều thông tin về các tùy chọn cấu hình, hãy chuyển sang giao diện VirusScan Advanced. Chọn Advanced từ menu Tools trong cửa sổ VirusScan Classic.

Bạn có thể bắt đầu một hoạt động quét với các tùy chọn mà bạn đã chọn vào bất kỳ lúc nào - chỉ cần nhấp Scan Now. Để lưu các thay đổi ở dạng các tùy chọn quét mặc định, hãy chọn Save As Default từ menu File hoặc nhấp New Scan. Để lưu các xác lập trong một file mới, hãy chọn Save Settings từ menu File, đặt tên cho file trong hộp thoại vừa xuất hiện, sau đó nhấp Save.

File xác lập mà bạn lưu sẽ có tên file với phần mở rộng .VCS.

Nhấp vào các nút ở kế bên mỗi tên nhãn để tìm hiểu cách chọn các tùy chọn dành cho các nút đó.

1. Chọn các tùy chọn Where & What

Khi lần đầu tiên bạn khởi động nó, trình ứng dụng VirusScan nghĩ rằng bạn muốn quét ổ đĩa C: và tất cả các folder con của nó, và muốn kiểm tra chỉ các file dễ bị nhiễm virus.

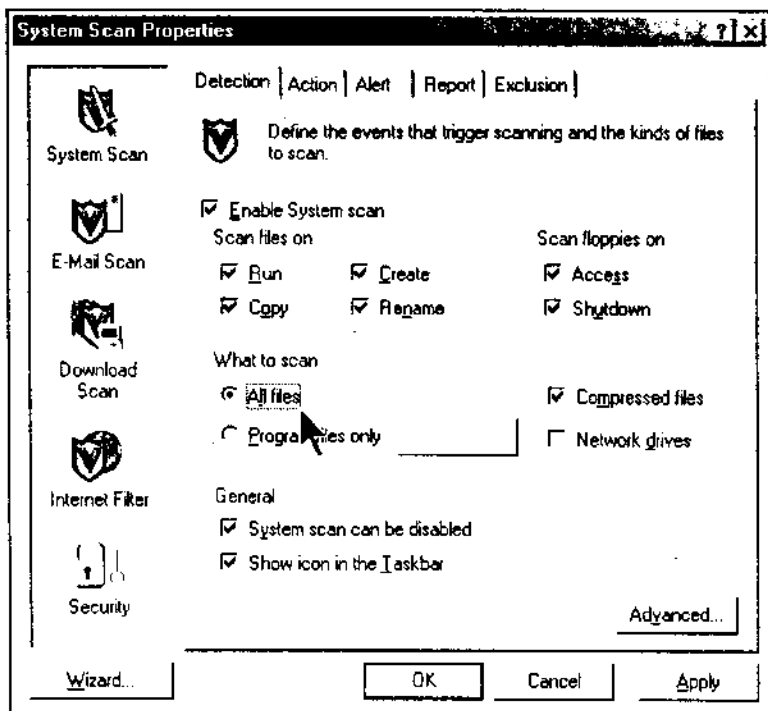
Để xác lập hay thay đổi các tùy chọn, hãy thực hiện các bước sau đây:

1. Chọn một ổ đĩa hay folder trên hệ thống hoặc trên mạng mà bạn muốn trình ứng dụng kiểm tra để tìm virus.
Gõ nhập một đường dẫn cho volume hay folder đích trong hộp text được cung cấp, hoặc nhấp Browse để xác định mục đích quét phù hợp.
2. Chọn hộp kiểm Include subfolders để nhờ trình ứng dụng tìm virus trong bất kỳ folder nào nằm trong đích quét.

Ghi chú

Việc chọn Include subfolders sẽ làm cho trình ứng dụng quét chỉ các file được chứa ở cấp độ gốc của folder mà bạn chỉ định. Để quét các file đó, hãy xóa chọn hộp kiểm Include subfolders.

- Chỉ định các kiểu file nào mà bạn muốn trình ứng dụng xem xét. Bạn có thể
 - ❖ Quét các file đã nén. Chọn hộp kiểm Compressed files để nhờ trình ứng dụng tìm virus trong các file và các file archive đã nén. Mặc dù điều này cung cấp cho bạn sự bảo vệ tốt hơn, nhưng việc quét các file và các file archive đã nén có thể kéo dài hoạt động quét.
 - ❖ Quét tất cả các file. Chọn hộp kiểm All Files để nhờ trình ứng dụng quét tất cả các file trên đích mà bạn đã chỉ định, cho dù chúng có phần mở rộng nào.

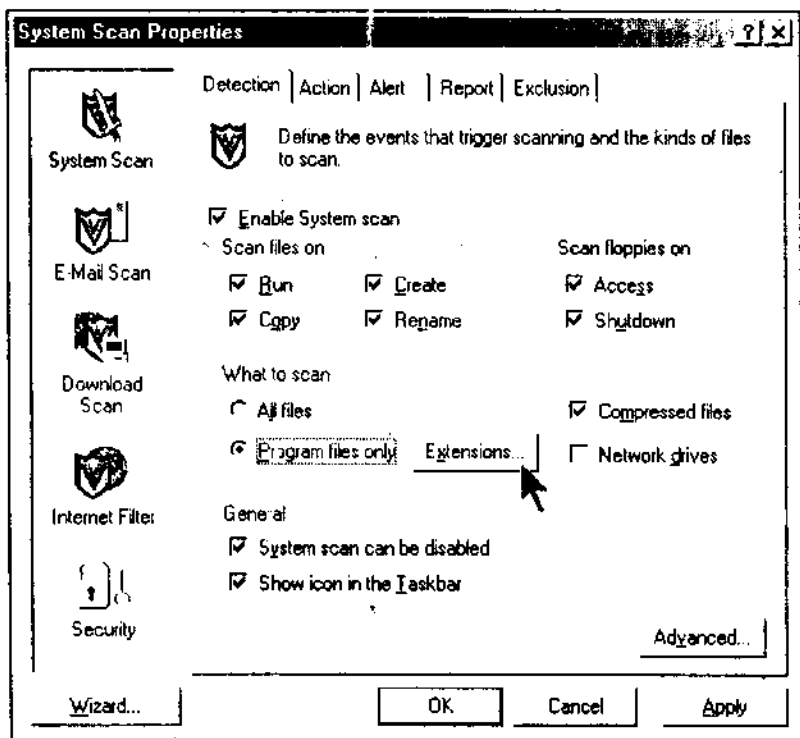


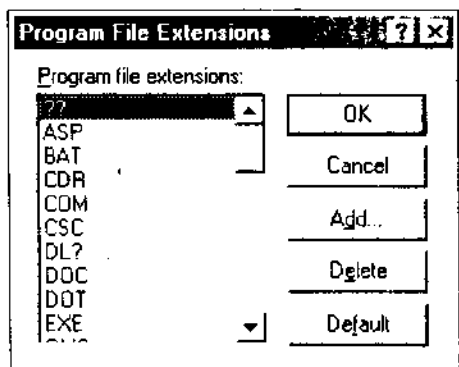
Ghi chú

McAfee đề nghị bạn chọn tùy chọn này cho hoạt động quét đầu tiên, hoặc định kỳ, để bảo đảm hệ thống của bạn hoàn toàn không bị nhiễm virus. Sau đó bạn có thể giới hạn phạm vi của các hoạt động quét sau này.

- ❖ Chọn các kiểu file. Các virus không thể lây nhiễm các file không có chứa mã khả thi, dù đó là mã script, macro, hay nhị phân. Do đó bạn có thể thu hẹp phạm vi của các hoạt động quét đối với các file dễ bị nhiễm virus nhất. Để thực hiện điều này, hãy nhấp vào nút Program files only.

Để xem hay chỉ định các phần mở rộng tên file mà trình ứng dụng kiểm tra, hãy nhấp Extensions. Thao tác này sẽ mở hộp thoại Program File Extensions. Để tìm hiểu về cách thay đổi các file được liệt kê ở đây, hãy nhấp here.





4. Tiếp theo, bạn có thể:

- ❖ Nhấp Scan Now để bắt đầu một hoạt động quét với các tùy chọn này.

Chọn các tùy chọn cấu hình khác. Nhấp vào mỗi nút để tìm hiểu các tùy chọn trong các trang đặc tính còn lại:

Action options

Report options

- ❖ Nhấp nút New Scan hoặc chọn Save As Default từ menu File để lưu các xác lập cho các hoạt động quét sau này sử dụng chúng.
- ❖ Chọn Save Settings từ menu File để lưu các xác lập trong một file mới mà bạn có thể sử dụng để chạy các hoạt động quét sau này, hoặc gửi đến các máy tính khác để sử dụng chúng. Kế tiếp, hãy đặt tên cho file trong hộp thoại vừa xuất hiện, sau đó nhấp Save.

2. Chọn các tùy chọn Action dành cho giao diện VirusScan Classic

Khi trình ứng dụng VirusScan tìm thấy một virus, nó hỏi bạn muốn nó thực hiện điều gì với file bị nhiễm. Bạn cũng có thể nhờ nó tự động thực hiện một hành động mà bạn xác định trước.

Để xác lập hoặc thay đổi các tùy chọn này:

1. Chọn một phần phản hồi từ danh sách When a virus is found. Vùng ở ngay phía dưới danh sách sẽ thay đổi để hiển thị các

tùy chọn bổ sung cho mỗi phần phản hồi. Các tùy chọn như sau:

- ❖ **Prompt user for action.** Chọn phần phản hồi này nếu bạn đang ở tại máy tính khi ở trình ứng dụng quét đĩa. Trình ứng dụng sẽ hiển thị một thông tin cảnh báo khi nó tìm thấy một virus và cung cấp cho bạn đầy đủ các tùy chọn phản hồi có sẵn.
- ❖ **Move infected files automatically.** Chọn phần phản hồi này để nhờ trình ứng dụng di chuyển các file bị nhiễm đến một folder cách li ngay sau khi nó tìm thấy chúng.

Theo mặc định, trình ứng dụng di chuyển các file này đến một folder có tên là `\Infected` trong thư mục chương trình VirusScan. Bạn có thể nhập một tên khác hoặc hộp text được cho, hoặc nhấp **Browse** để xác định một folder thích hợp trên đĩa cứng.

- ❖ **Clean infected files automatically.** Chọn phần phản hồi này để yêu cầu trình ứng dụng loại bỏ mã virus ra khỏi file bị nhiễm ngay sau khi tìm thấy nó. Nếu trình ứng dụng không thể loại bỏ virus, nó sẽ ghi chú sự cố này vào file log của nó.
- ❖ **Delete infected files automatically.** Chọn tùy chọn này để nhờ trình ứng dụng xóa ngay mỗi file bị nhiễm mà nó tìm thấy. Nhớ bật tính năng báo cáo để bạn có một bản ghi về các file mà trình ứng dụng đã xóa. Bạn sẽ cần phục hồi các file đã xóa từ các bản sao lưu dự phòng. Nếu trình ứng dụng không thể xóa một file bị nhiễm, nó sẽ ghi sự cố này trong log file của nó.
- ❖ **Continue scanning.** Sử dụng tùy chọn này chỉ khi bạn dự định để máy tính hoạt động trong khi trình ứng dụng kiểm tra virus. Nếu bạn cũng kích hoạt tính năng báo cáo, trình ứng dụng sẽ báo cáo các tên của bất kỳ virus nào mà nó tìm thấy và tên của các file bị nhiễm để bạn có thể xóa chúng ngay khi có thể.

2. Tiếp theo, bạn có thể:

- ❖ Nhấp Scan Now để bắt đầu một hoạt động quét với các tùy chọn này.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào mỗi nút để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại:

Where & What options

Report options

- ❖ Nhấp nút Scan Now hoặc chọn Save As Default từ menu File để lưu các xác lập cho các hoạt động quét sau này sử dụng chúng.
- ❖ Chọn Save Settings từ menu File để lưu các xác lập trong một file mới mà bạn có thể sử dụng để chạy các hoạt động quét sau này, hoặc gửi đến các máy tính khác để sử dụng chúng. Kế tiếp, hãy đặt tên cho file trong hộp thoại vừa xuất hiện, sau đó nhấp Save.

3. Chọn các tùy chọn Report dành cho giao diện VirusScan

Theo mặc định, trình ứng dụng phát ra tiếng bíp khi nó tìm thấy một virus. Bạn có thể bật hoặc tắt thông tin cảnh báo này, hoặc bổ sung một thông tin cảnh báo vào hộp thoại Virus Found vốn xuất hiện khi phần mềm VirusScan tìm thấy một file bị nhiễm. Thông tin cảnh báo của bạn có thể chứa bất kỳ thông tin nào, từ một cảnh báo đơn giản đến các lệnh chỉ dẫn cách báo cáo sự cố cho một người điều hành mạng.

Bạn cũng có thể xác lập kích cỡ và vị trí của log file VirusScan ở đây. Theo mặc định, trình ứng dụng liệt kê các xác lập hiện hành của nó và tóm tắt tất cả các hành động mà nó thực hiện trong suốt các hoạt động quét trong một log file được gọi là VSCLOG.TXT. Bạn có thể giữ file này ở dạng log file, hoặc bạn có thể chỉ định một file text hiện có khác để trình ứng dụng sử dụng. Trình ứng dụng sẽ không tự tạo một file text mới.

Để xác lập hoặc thay đổi các tùy chọn ở đây, hãy thực hiện các bước sau đây:

1. Chọn các phương pháp cảnh báo mà bạn muốn trình ứng dụng sử dụng khi nó tìm thấy một virus. Bạn có thể nhờ nó:

- ❖ Hiển thị một thông báo tùy ý. Chọn hộp kiểm Display message, sau đó nhập thông báo mà bạn muốn nó xuất hiện trong hộp text được chọn. Bạn có thể nhập một thông báo dài đến 225 ký tự. Để hiển thị thông báo, bạn phải đã chọn tùy chọn Prompt user for action trong trang Action.
- ❖ Phát ra tiếp bíp. Chọn hộp kiểm Sound alert.

2. Chọn hộp kiểm log to file.

Để chỉ định một log file khác với VSCLOG.TXT, hãy nhập một tên file và đường dẫn vào hộp text được cho, hoặc nhấp Browse để xác định một file thích hợp ở nơi khác trên đĩa cứng hay trên mạng.

3. Để giảm thiểu kích cỡ của log file, hãy chọn hộp kiểm Limit size of log file to, sau đó nhập một giá trị dành cho kích cỡ file, theo đơn vị kilobyte, vào hộp text được cho.

Nhập một giá trị giữa 10KB và 999KB. Theo mặc định, trình ứng dụng giới hạn kích cỡ file là 100KB. Nếu dữ liệu trong log vượt quá kích cỡ file mà bạn đã xác lập, trình ứng dụng sẽ xóa log hiện có và bắt đầu lại từ điểm mà nó đã rời khỏi.

4. Kế tiếp, bạn có thể:

- ❖ Nhấp Scan Now để bắt đầu một hoạt động quét với các tùy chọn này.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào mỗi nút để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại:

Where & What options

Action options

- ❖ Nhấp nút New Scan hoặc chọn Save As Default từ menu File để lưu các xác lập cho các hoạt động quét sau này sử dụng chúng.
- ❖ Chọn Save Settings từ menu File để lưu các xác lập trong

một file mới mà bạn có thể sử dụng để chạy các hoạt động quét sau này, hoặc gởi đến các máy tính khác để sử dụng chúng. Kế tiếp, hãy đặt tên cho file trong hộp thoại vừa xuất hiện, sau đó nhấp Save.

VIII. Cấu hình giao diện VirusScan Advanced

Để trình ứng dụng VirusScan bảo vệ hệ thống của bạn, bạn phải cho nó biết:

- ❖ Bạn muốn nó quét vùng nội dung nào
- ❖ Bạn muốn nó thực hiện điều gì nếu nó tìm thấy virus
- ❖ Nó sẽ cho bạn biết bằng cách nào khi tìm thấy một virus
- ❖ Bạn có muốn theo dõi hành động của nó hay không
- ❖ Bạn không muốn nó quét virus cho các hạng mục nào

Nhấp vào các nút ở kế bên mỗi tên nhãn để tìm hiểu cách chọn các tùy chọn dành cho các nút đó.

1. Chọn các tùy chọn Detection dành cho giao diện VirusScan Advanced

Để xác lập hay thay đổi các tùy chọn này, hãy thực hiện các bước sau đây:

1. Chọn những phần nào của hệ thống hay mạng mà bạn muốn phần mềm VirusScan kiểm tra để tìm virus. Bạn có thể:
 - ❖ Bổ sung các đích quét. Nhấp Add để mở hộp thoại Add Scan item.
 - ❖ Thay đổi các đích quét. Chọn một trong các đích quét được liệt kê, sau đó nhấp Edit để mở hộp thoại Edit Item to Scan. Hộp thoại này xuất hiện cùng với đích quét đang được chỉ định. Chọn hoặc nhập vào một đích quét mới, sau đó nhấp OK để đóng hộp thoại.
 - ❖ Loại bỏ các đích quét. Chọn một trong các đích quét được liệt kê, sau đó nhấp Remove để xóa nó.

2. Chỉ định các kiểu file mà bạn muốn trình ứng dụng kiểm tra.

3. Kế tiếp, bạn có thể:

- ❖ Nhấp Scan Now để bắt đầu một hoạt động quét với các tùy chọn này.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút này để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại:

Action options

Alert options

Report options

Exclusion options

- ❖ Nhấp nút New Scan hoặc chọn Save As Default từ menu File để lưu các xác lập cho các hoạt động quét sau này sử dụng chúng.
- ❖ Chọn Save Settings từ menu File để lưu các xác lập trong một file mới mà bạn có thể sử dụng để chạy các hoạt động quét sau này, hoặc gởi đến các máy tính khác để sử dụng chúng. Kế tiếp, hãy đặt tên cho file trong hộp thoại vừa xuất hiện, sau đó nhấp Save.

2. Chọn các tùy chọn Action hành cho giao diện VirusScan Advanced

Để xác lập hay thay đổi các tùy chọn này:

1. Chọn một trong các tùy chọn phản hồi sau đây từ danh sách When a virus is found.

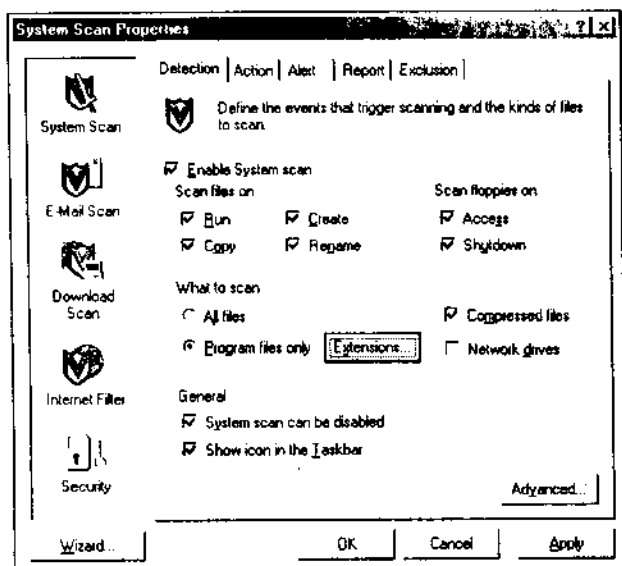
- ❖ Prompt user for action
- ❖ Move infected files automatically
- ❖ Clean infected files automatically
- ❖ Delete infected files automatically
- ❖ Continue scanning

2. Kế tiếp, bạn có thể:

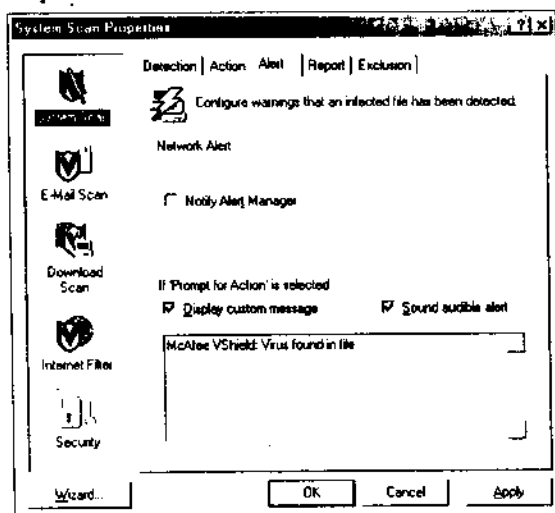
- ❖ Nhấp Scan Now để bắt đầu một hoạt động quét với các tùy chọn này.

- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào mỗi nút để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại:

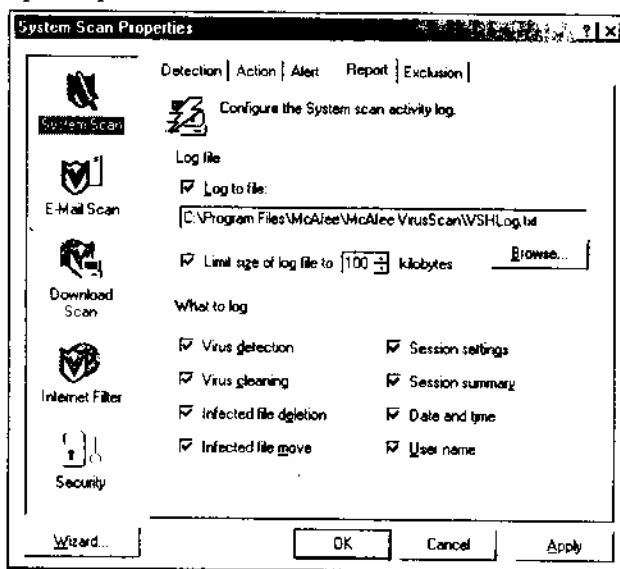
Detection optionss



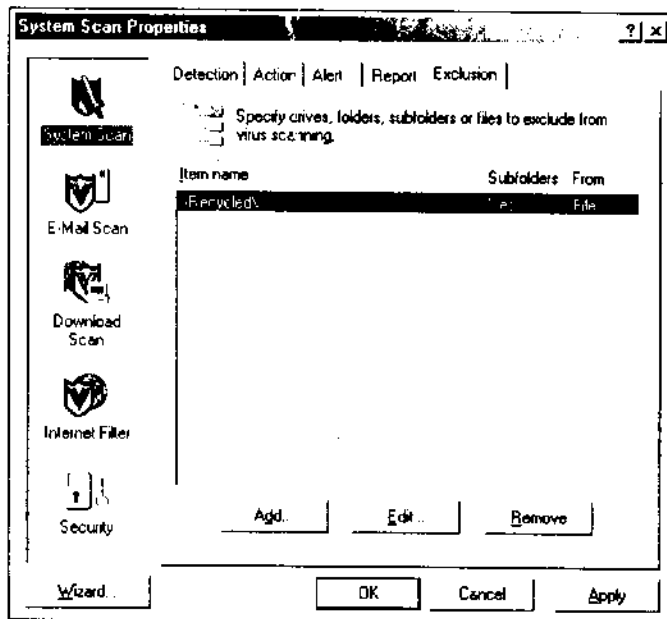
Alert options



Report options



Exclusion options

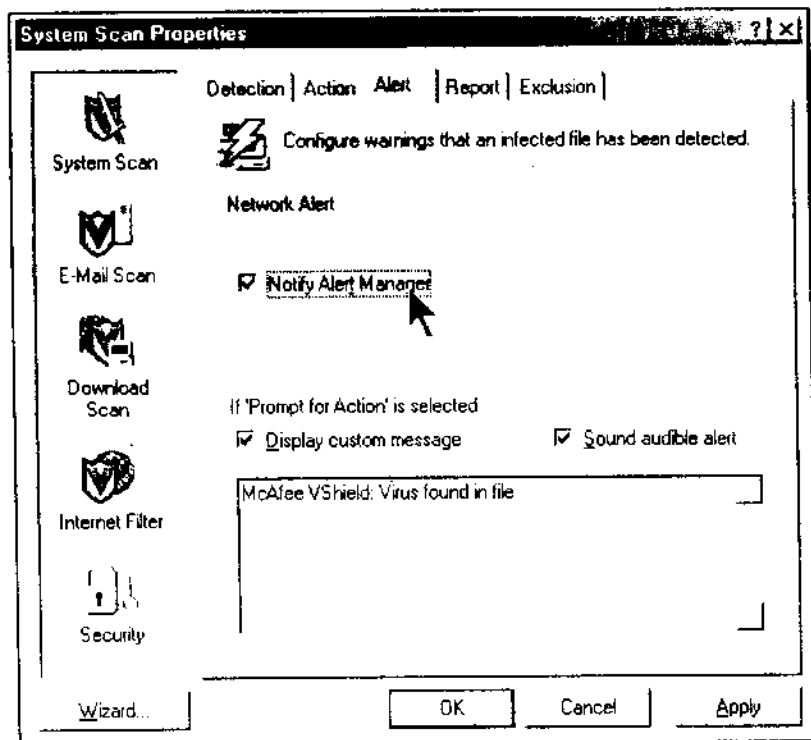


- ❖ Nhấp nút New Scan hoặc chọn Save As Default từ menu File để lưu các xác lập cho các hoạt động quét sau này sử dụng chúng.
- ❖ Chọn Save Settings từ menu File để lưu các xác lập trong một file mới mà bạn có thể sử dụng để chạy các hoạt động quét sau này, hoặc gửi đến các máy tính khác để sử dụng chúng. Kế tiếp, hãy đặt tên cho file trong hộp thoại vừa xuất hiện, sau đó nhấp Save.

3. Chọn các tùy chọn Alert dành cho giao diện VirusScan Advanced

Thực hiện các bước sau đây:

1. Chọn hộp kiểm Notify Alert Manager để nhờ trình ứng dụng gửi các thông tin cảnh báo đến Alert Manager để phân phối.

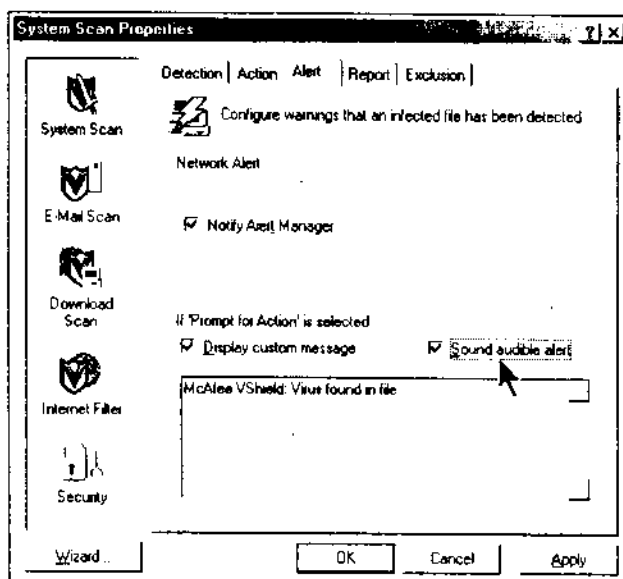


Alert Manager là một thành phần phần mềm McAfee riêng biệt vốn thu thập các thông tin cảnh alert và sử dụng nhiều phương pháp để gửi chúng đến những người mà bạn chỉ định. Để nhờ trình ứng dụng VirusScan gửi các thông tin cảnh báo này một cách thành công, bạn phải chọn hộp kiểm Notify Alert Manager ở đây và phải cài đặt tiện ích Alert Manager Client Configuration. Bạn có thể gửi các thông tin cảnh báo trực tiếp đến một server Alert Manager, hoặc bạn có thể gửi các thông tin cảnh báo ở dạng các file text (.ALR) đến một thư mục Centralized Alerting mà server Alert Manager kiểm tra theo định kỳ. Để tìm hiểu thêm, hãy nhấp [here](#).

Ghi chú

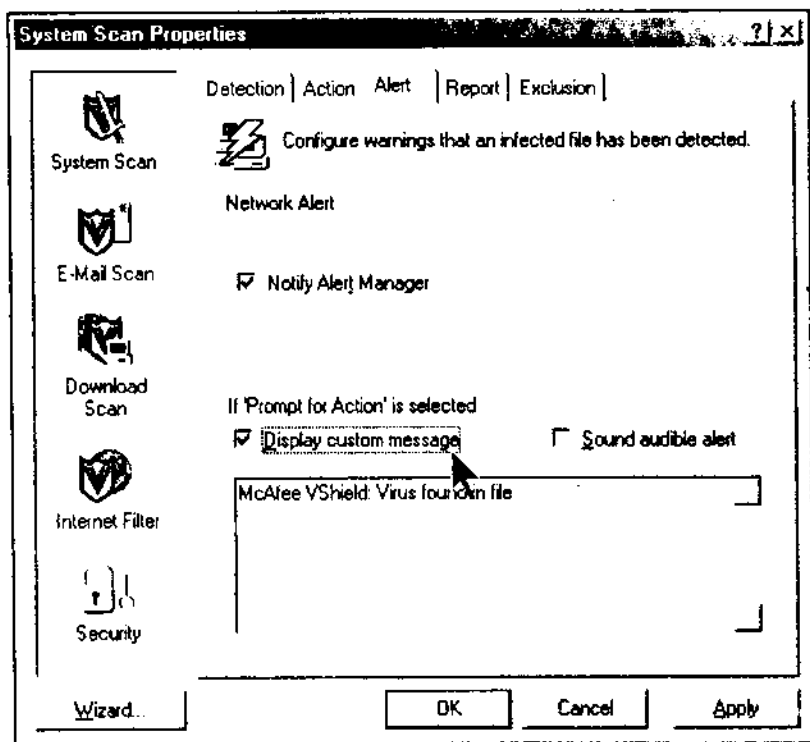
Việc xóa chọn hộp kiểm này có nghĩa là bạn yêu cầu trình ứng dụng VirusScan dừng gửi thông tin cảnh báo qua Alert Manager, nhưng nó không ảnh hưởng đến các thông tin cảnh báo khác mà bạn cấu hình trong trang đặc tính này.

2. Chọn hộp kiểm Sound audible alert để nhờ trình ứng dụng phát ra tiếng bíp khi nó tìm thấy một file bị nhiễm.



Bạn có thể thay đổi xác lập dành cho tùy chọn này chỉ khi bạn chọn Prompt for user action trong trang đặc tính Action. Nếu không, hộp kiểm sẽ hiển thị và sử dụng xác lập mà nó đã có khi bạn chọn hạng mục Prompt for user action vào lần sau cùng. Trình ứng dụng sẽ phát ra tiếng bíp cảnh báo hoặc mở file .WAV mà bạn đã nhờ máy tính xác lập.

3. Chọn hộp kiểm Display custom message để nhờ trình ứng dụng bổ sung một thông báo tùy biến vào hộp alert mà nó hiển thị khi nó tìm thấy một file bị nhiễm.



Bạn có thể thay đổi xác lập dành cho tùy chọn này chỉ khi bạn chọn Prompt for user action trong trang đặc tính Action. Nếu không, hộp kiểm sẽ hiển thị xác lập mà nó đã có khi bạn chọn Prompt for user action vào lần cuối cùng. Nếu bạn không chọn hạng mục đó trong trang Action, không có hộp alert nào

xuất hiện và bạn sẽ không nhìn thấy từ một thông tin tùy biến nào ngay cả khi bạn chọn hộp kiểm này.

4. Nhập thông báo mà bạn muốn module hiển thị trong hộp text được cho. Bạn có thể nhập tối đa đến 250 ký tự.

5. Kế tiếp, bạn có thể:

- ❖ Nhấp Scan Now để bắt đầu một hoạt động quét với các tùy chọn này.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào mỗi nút để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại:

Detection options

Action options

Report options

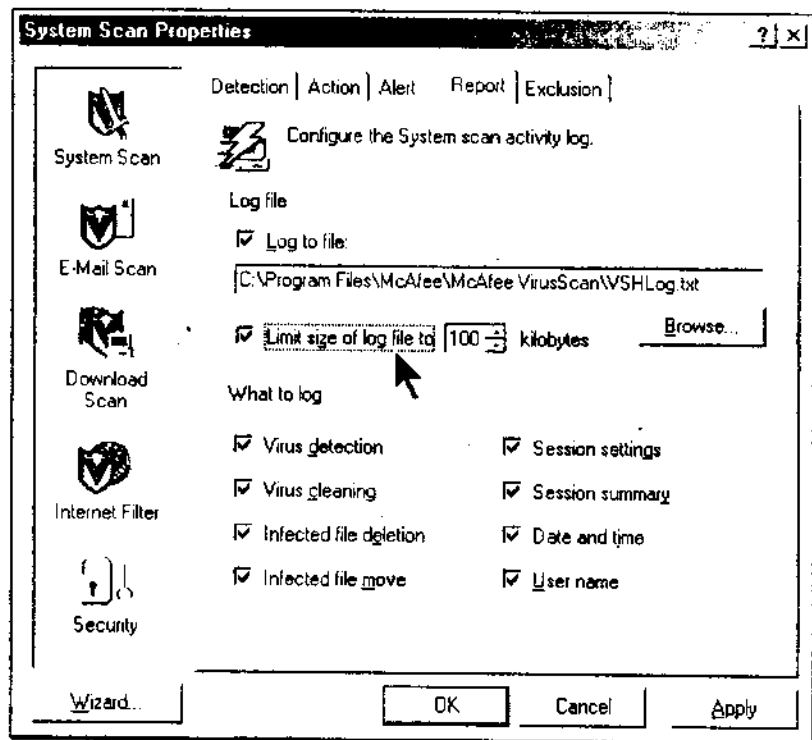
Exclusion options

- ❖ Nhấp nút New Scan hoặc chọn Save As Default từ menu File để lưu các xác lập cho các hoạt động quét sau này sử dụng chúng.
- ❖ Chọn Save Settings từ menu File để lưu các xác lập trong một file mới mà bạn có thể sử dụng để chạy các hoạt động quét sau này, hoặc gởi đến các máy tính khác để sử dụng chúng. Kế tiếp, hãy đặt tên cho file trong hộp thoại vừa xuất hiện, sau đó nhấp Save.

4. Chọn các tùy chọn Report dành cho giao diện VirusScan Advanced

Để quyết định trình ứng dụng sẽ ghi lại dữ liệu nào và kích cỡ của log file là bao nhiêu:

1. Chọn hộp kiểm Log to file.
2. Chọn hộp kiểm Limit size of log file to để giảm thiểu kích cỡ của log file. Nếu bạn không chọn hộp kiểm này, log file có thể tăng đến kích cỡ mà khoảng trống đĩa của bạn cho phép.



3. Nhập một giá trị dành cho kích cỡ file, khi đơn vị kilobyte, và hộp text được cho.

Để xem các nội dung của log file, hãy chọn View Activity Log từ menu File trong cửa sổ trình ứng dụng VirusScan.

4. Chọn các hộp kiểm phù hợp với thông tin mà bạn muốn trình ứng dụng ghi lại.

5. Kế tiếp, bạn có thể:

- ❖ Nhấp Scan Now để bắt đầu một hoạt động quét với các tùy chọn này.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào mỗi nút để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại:

Detection options

Action options

Alert options

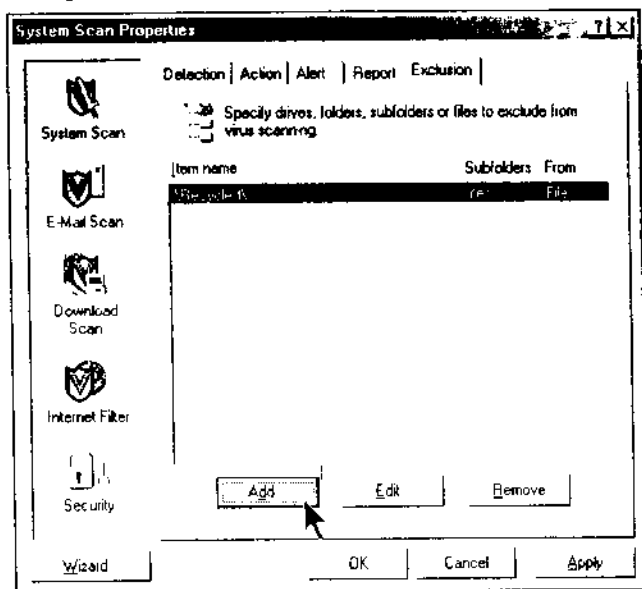
Exclusion options

- ❖ Nhấp nút New Scan hoặc chọn Save As Default từ menu File để lưu các xác lập cho các hoạt động quét sau này sử dụng chúng.
- ❖ Chọn Save Settings từ menu File để lưu các xác lập trong một file mới mà bạn có thể sử dụng để chạy các hoạt động quét sau này, hoặc gởi đến các máy tính khác để sử dụng chúng. Kế tiếp, hãy đặt tên cho file trong hộp thoại vừa xuất hiện, sau đó nhấp Save.

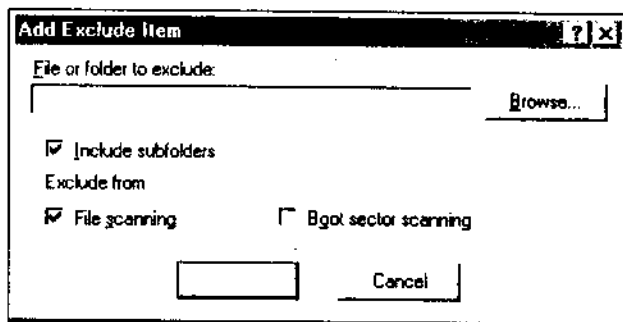
5. Chọn các tùy chọn Exclusion dành cho giao diện VirusScan Advanced

Để chỉ định các hạng mục nào mà trình ứng dụng VirusScan sẽ bỏ qua trong suốt các hoạt động quét của nó, hãy thực hiện các bước sau đây:

1. Nhấp Add để loại bỏ một hạng mục mới.



Thao tác này sẽ mở hộp thoại Add Exclude Item. Để tìm hiểu cách chỉ định các hạng mục mà bạn muốn loại ra khỏi một hoạt động quét, hãy nhấp [here](#).



Theo mặc định, bạn có thể loại ra đến 100 đích quét duy nhất. Để thay đổi con số này, hãy mở VirusScan control panel, nhấp nhấn Components, sau đó nhập một con số mới vào hộp text Maximum number of exclude items.

2. Chọn một trong các hạng mục hiển thị, sau đó nhấp Edit để thay đổi định nghĩa hạng mục.

Thao tác này sẽ mở hộp thoại Edit Exclude Item. Thực hiện các thay đổi mà bạn cần, sau đó nhấp OK để đóng hộp thoại.

3. Chọn một trong các hạng mục hiển thị, sau đó nhấp Remove để xóa một hạng mục ra khỏi danh sách. Điều này có nghĩa là trình ứng dụng VirusScan sẽ quét hạng mục trong suốt hoạt động kế tiếp của nó.

4. Kế tiếp, bạn có thể:

- ❖ Nhấp Scan Now để bắt đầu một hoạt động quét với các tùy chọn này.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào mỗi nút để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại:

Detection options

Action options

Alert options

Report options

- ❖ Nhấp nút New Scan hoặc chọn Save As Default từ menu File để lưu các xác lập cho các hoạt động quét sau này sử dụng chúng.
- ❖ Chọn Save Settings từ menu File để lưu các xác lập trong một file mới mà bạn có thể sử dụng để chạy các hoạt động quét sau này, hoặc gửi đến các máy tính khác để sử dụng chúng. Kế tiếp, hãy đặt tên cho file trong hộp thoại vừa xuất hiện, sau đó nhấp Save.

6. Bảo vệ các xác lập VirusScan để tránh sự thay đổi khi không được quét

Trình ứng dụng VirusScan cho phép bạn xác lập một password để bảo vệ các xác lập mà bạn chọn trong mỗi trang đặc tính nhằm tránh sự thay đổi khi không được phép. Tính năng này đặc biệt hữu ích cho những người quản lý hệ thống cần ngăn chặn những người sử dụng gây cản trở cho họ trong việc phòng chống virus.

Để khóa các xác lập mà bạn chọn cho tác vụ này, hãy thực hiện các bước sau đây:

1. Chọn các xác lập mà bạn muốn bảo vệ trong danh sách các hạng mục hiển thị trong trang đặc tính này.

Mỗi hạng mục được liệt kê tiêu biểu cho toàn bộ trang đặc tính và tất cả các xác lập chứa trong đó. Bạn có thể bảo vệ một hoặc tất cả các trang dành cho các tác vụ này. Các trang đặc tính đã được bảo vệ hiển thị một biểu tượng ổ khóa đã được khóa. Để loại bỏ sự bảo vệ ra khỏi một trang đặc tính, hãy nhấp vào biểu tượng này để khóa nó.

2. Nhấp password để mở hộp thoại Specify Password.

Nhập một password vào hộp text đầu tiên, sau đó nhập lại password này vào hộp text ở phía dưới để xác nhận sự chọn lựa của bạn. Kế tiếp, hãy nhấp OK để đóng hộp thoại Specify Password.

3. Nhấp OK để lưu các tùy chọn cấu hình và trở lại cửa sổ VirusScan.

IX. Cấu hình các tác vụ VirusScan theo thời biểu

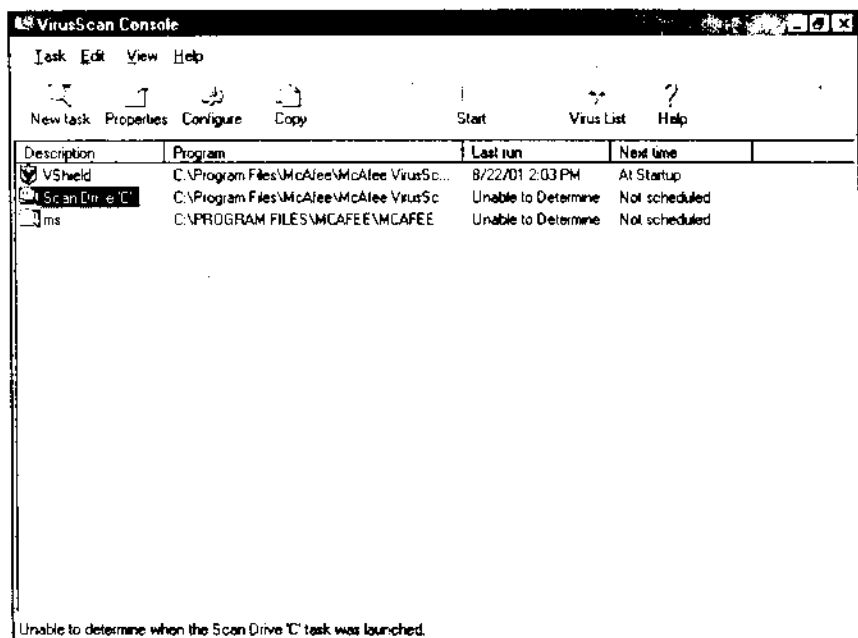
Để cấu hình một tác vụ VirusScan mà nó sẽ chạy theo thời biểu mà bạn chỉ định, bạn phải cho trình ứng dụng biết:

- ❖ Bạn muốn nó chạy khi nào
- ❖ Bạn muốn nó quét vùng nội dung nào
- ❖ Bạn muốn nó thực hiện điều gì nếu nó tìm thấy một virus
- ❖ Nó nên cho bạn biết bằng cách nào khi tìm thấy một virus
- ❖ Bạn có muốn theo dõi các hành động của nó hay không
- ❖ Bạn không muốn nó quét virus cho các hạng mục nào
- ❖ Bạn có muốn bảo vệ các xác lập mà bạn đã chọn để tránh sự thay đổi khi không được phép hay không

VirusScan Console cung cấp nhiều trang đặc tính mà bạn có thể sử dụng để xác định tác vụ. Các trang đặc tính này có nhiều tùy chọn tương tự các tùy chọn trong cửa sổ chính dành cho trình ứng dụng VirusScan. Ngoài ra chúng còn có thêm các tùy chọn khác nhằm giúp bạn xác định một tác vụ mà bạn muốn chạy đều đặn.

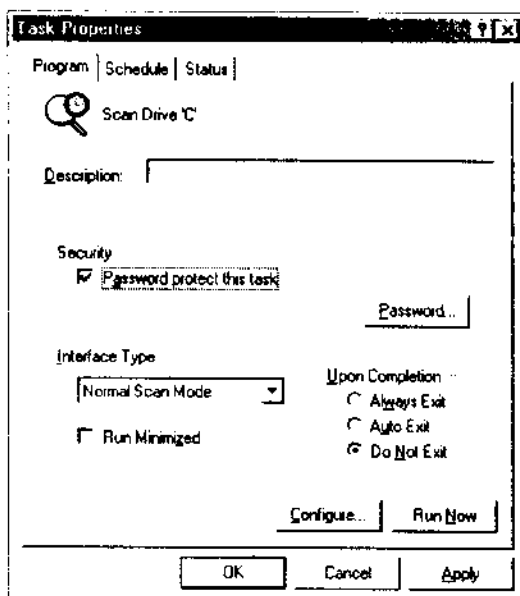
Để bắt đầu, hãy thực hiện các bước sau đây:

1. Nhấp đúp vào biểu tượng VirusScan Console  trong thanh tác vụ Windows để hiển thị nó.
Thao tác này sẽ mở cửa sổ Console.
2. Nhấp trong thanh công cụ Console  để mở hộp thoại Task Properties.

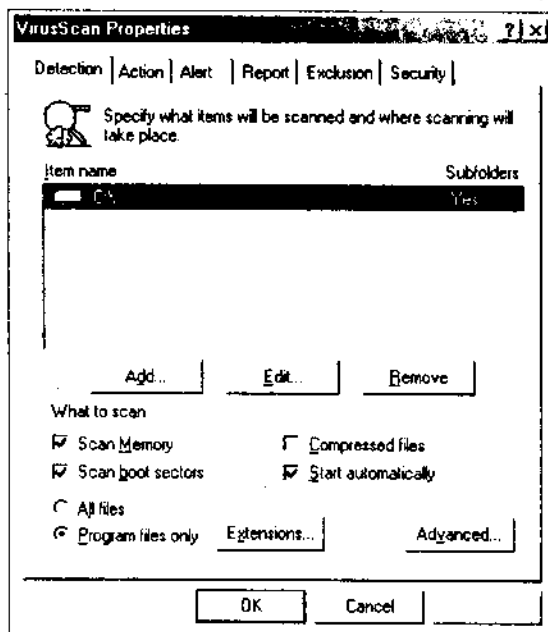


Trong hộp thoại này, bạn có thể đặt tên cho các tác vụ bảo vệ nó bằng một password, chỉ định cách mà nó sẽ xuất hiện khi chạy, và cho nó biết cần thực hiện điều gì khi đã thực hiện xong tác vụ.

Bạn có thể bắt đầu một hoạt động quét với các tùy chọn mà bạn đã chọn cho tác vụ vào bất kỳ lúc nào - chỉ cần nhấp Run Now. Để lưu các tùy chọn cấu hình cho tác vụ này, hãy nhấp OK hoặc Apply. Để đóng hộp thoại Task Properties mà không lưu các thay đổi, hãy nhấp Cancel.



3. Nhấp Configure để mở hộp thoại VirusScan Properties.



Hộp thoại này cung cấp cho bạn các tùy chọn cần thiết để biến đổi tác vụ sao cho phù hợp với các nhu cầu của bạn. Nhấp vào các nút được liệt kê ở phía dưới để tìm hiểu cách chọn các tùy chọn cho mỗi trang đặc tính.

1. Chọn các tùy chọn Detection dành cho các tác vụ VirusScan theo thời biểu

Để xác lập hay thay đổi các tùy chọn này, hãy thực hiện các bước sau đây:

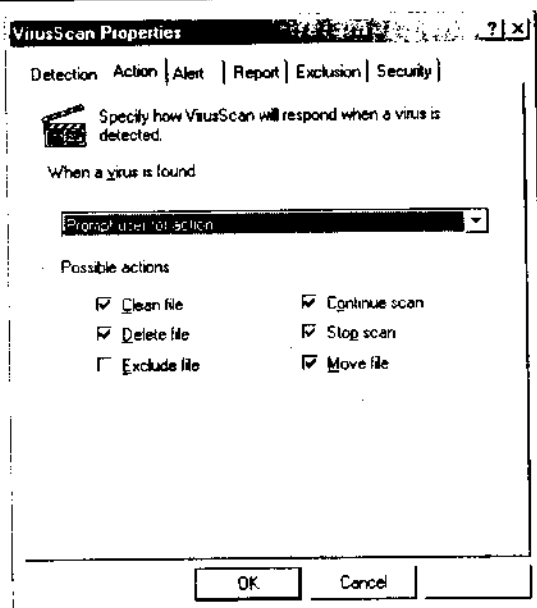
1. Chọn những phần nào của hệ thống hay mạng mà bạn muốn phần mềm VirusScan kiểm tra để tìm virus.
2. Chọn các tùy chọn quét đặc biệt.
3. Chỉ định các kiểu file nào mà bạn muốn trình ứng dụng kiểm tra.
4. Nếu bạn muốn các tác vụ này chạy khi bạn vắng mặt, hãy chọn Start automatically để yêu cầu trình ứng dụng VirusScan bắt đầu quét ngay sau khi nó khởi động.

Nếu bạn không chọn hộp kiểm này, Console sẽ khởi động trình ứng dụng VirusScan, nhưng trình ứng dụng sẽ chờ bạn nhấp vào Scan Now để bắt đầu tác vụ. Việc không chọn hộp kiểm này sẽ cung cấp cho bạn một cơ hội để hủy hoạt động quét nếu nó gây cản trở cho công việc của bạn.

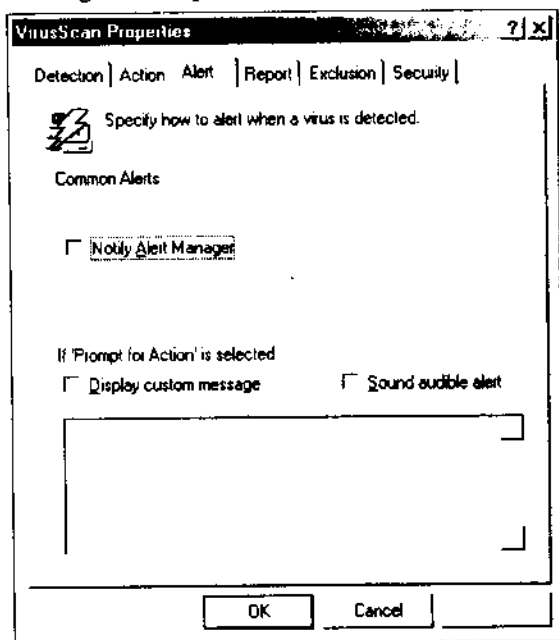
5. Kế tiếp, bạn có thể:

- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại VirusScan Properties.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút sau đây để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại.

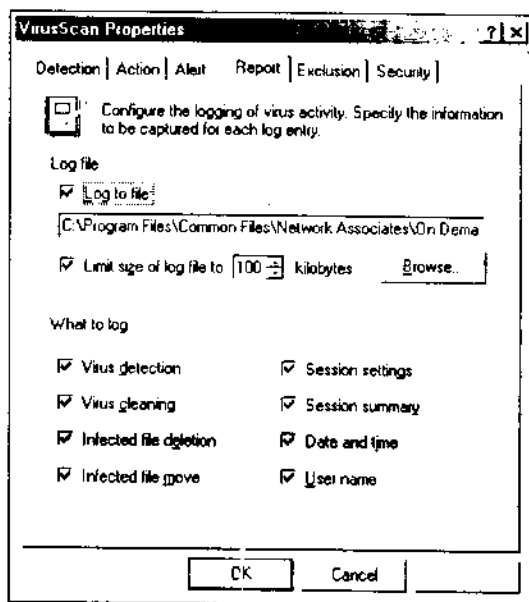
Choosing Action optionss



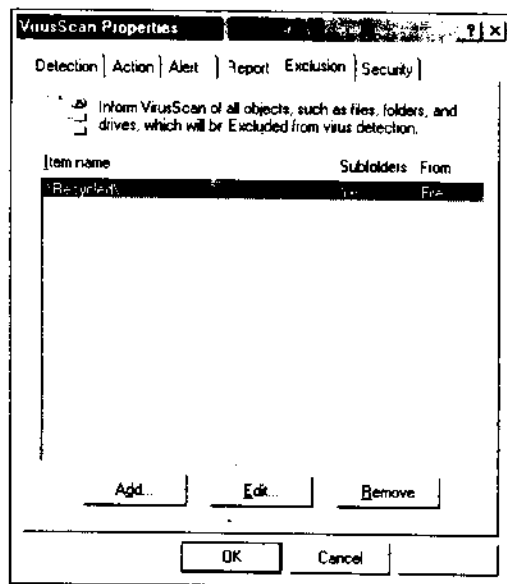
Choosing Alert options



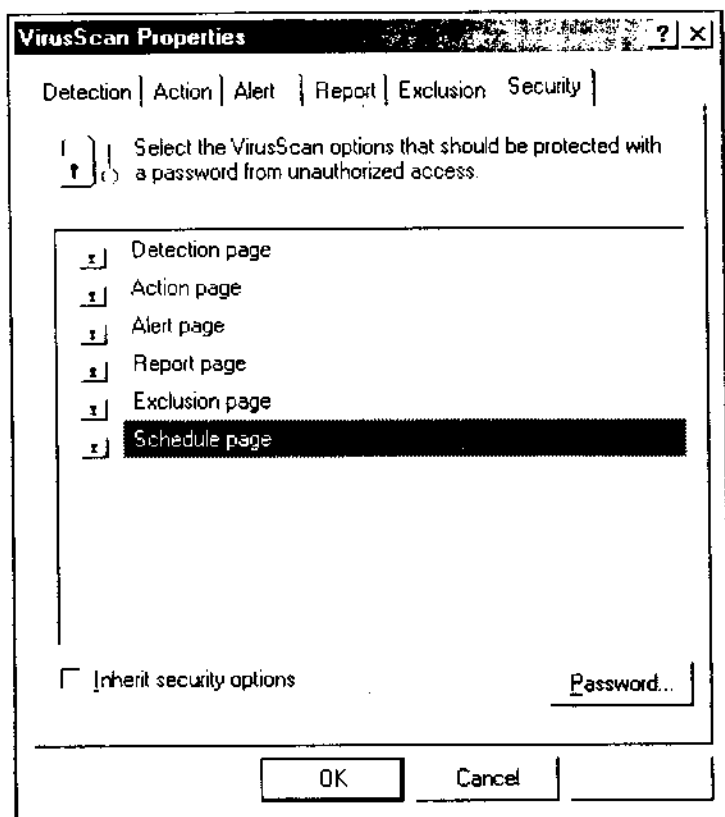
Choosing Report options



Choosing Exclusion options



Choosing Security options

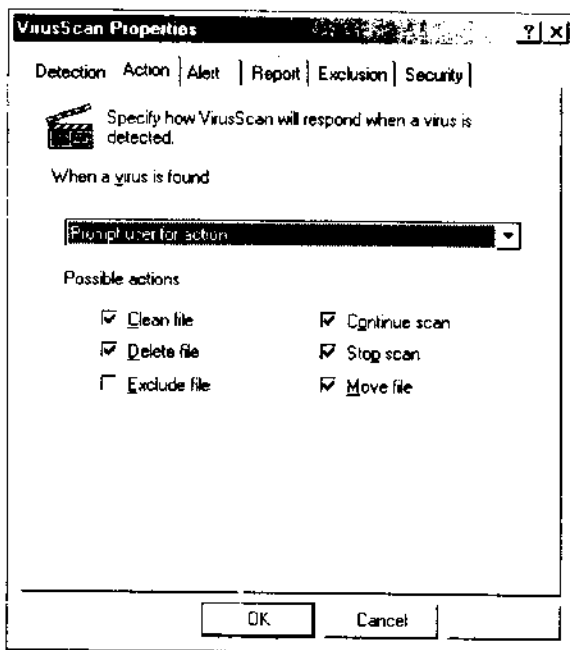


- ❖ Nhấp OK để lưu các tùy chọn cấu hình và trở lại hộp thoại Task Properties. Trong hộp thoại này, bạn có thể nhấp Run Now để bắt đầu một hoạt động quét với các tùy chọn mà bạn đã chọn.

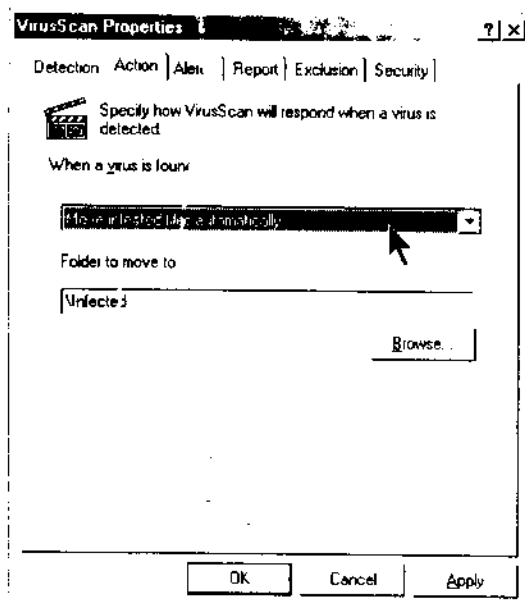
2. Chọn các tùy chọn Action dành cho các tác vụ VirusScan theo thời điểm

Để xác lập hay thay đổi các tùy chọn dành cho tác vụ này:

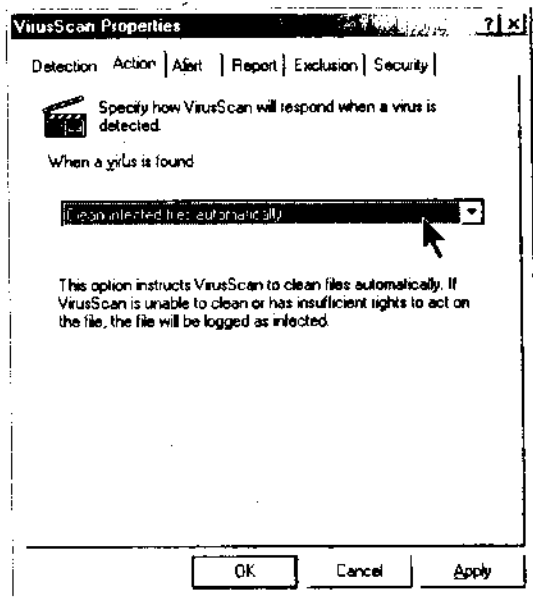
1. Chọn một trong các tùy chọn phản hồi sau đây từ danh sách When a virus is found.
 - ❖ Prompt user for action



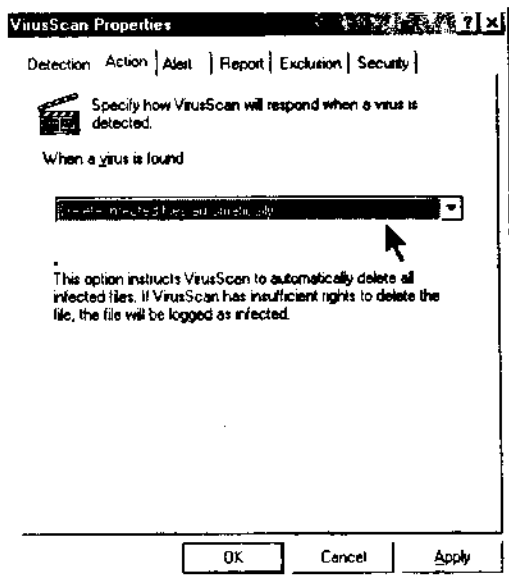
❖ Move infected files automatically



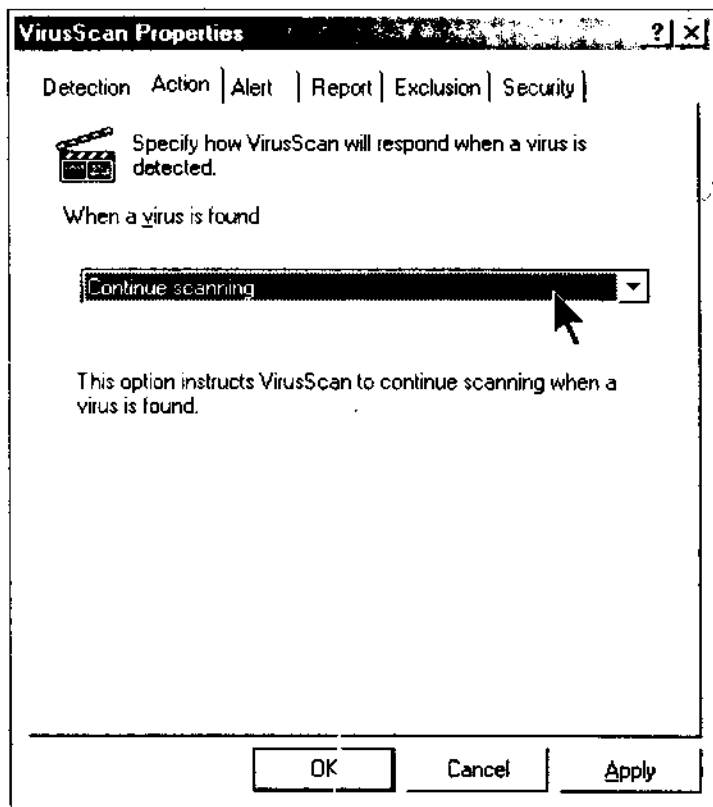
❖ Clean infected files automatically



❖ Delete infected files automatically



❖ Continue scanning



2. Kế tiếp, bạn có thể:

- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại VirusScan Properties.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút sau đây để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại.

Choosing Detection options

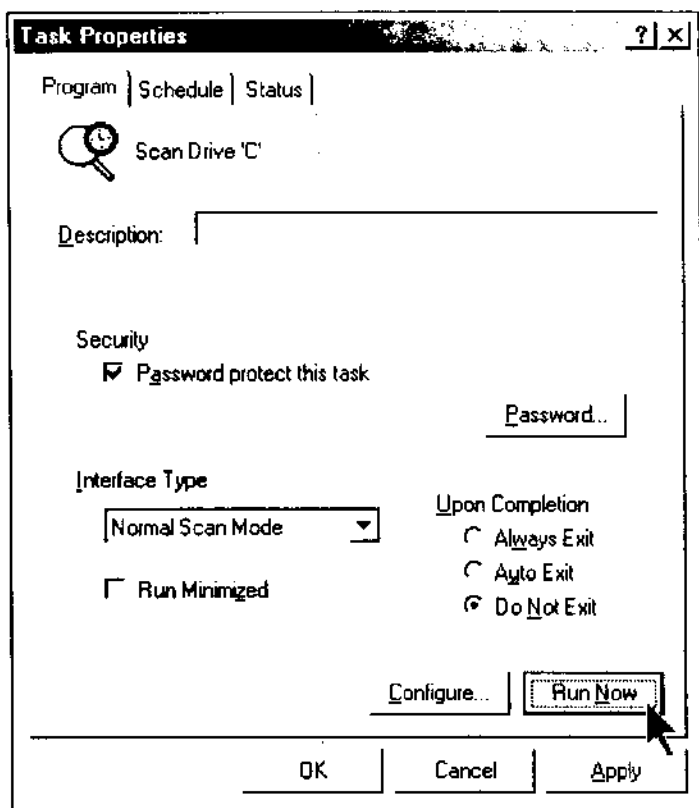
Choosing Alert options

Choosing Report options

Choosing Exclusion options

Choosing Security options

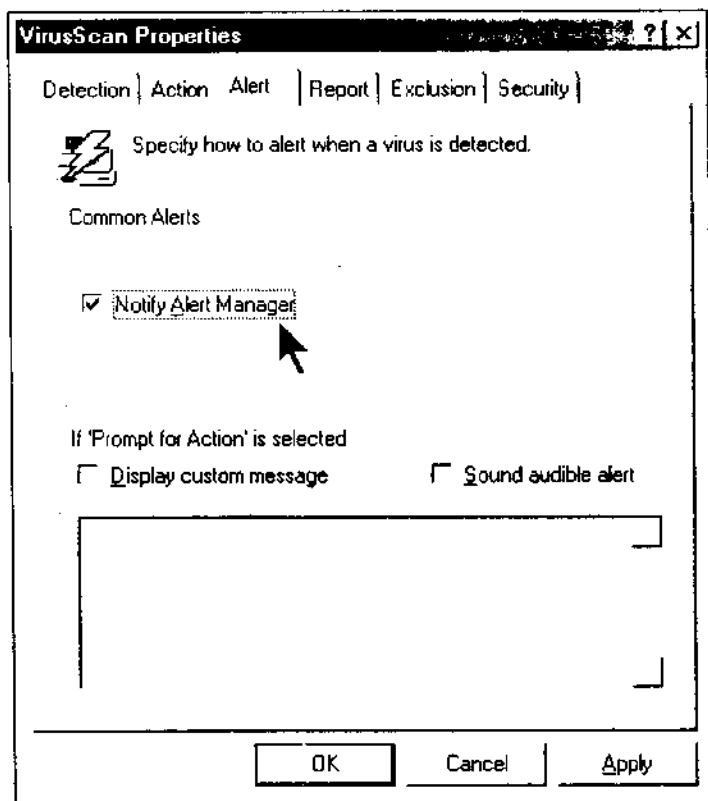
- ❖ Nhấp OK để lưu các tùy chọn cấu hình và trở lại hộp thoại Task Properties. Trong hộp thoại này, bạn có thể nhấp Run Now để bắt đầu một hoạt động quét với các tùy chọn mà bạn đã chọn.



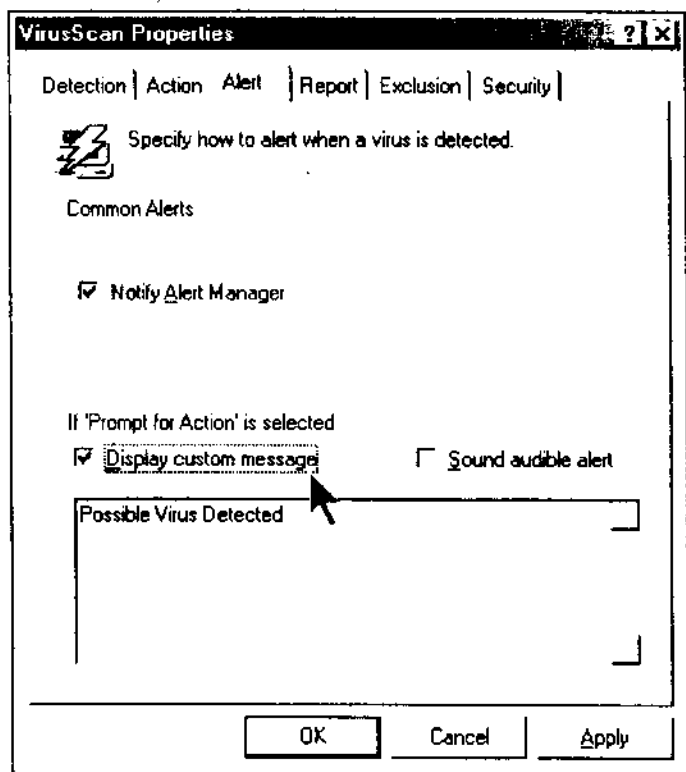
3. Chọn các tùy chọn Alert dành cho các tác vụ VirusScan theo thời điểm

Thực hiện các bước sau đây;

1. Chọn hộp kiểm Notify Alert Manager để nhờ trình ứng dụng gửi các thông tin cảnh báo đến Alert Manager để phân phối.



2. Chọn hộp kiểm Sound audible alert để nhờ trình ứng dụng phát ra tiếng bíp khi nó tìm thấy một file bị nhiễm.
3. Chọn hộp kiểm Display custom message để nhờ trình ứng dụng bổ sung một thông báo tùy biến vào hộp alert mà nó hiển thị khi tìm thấy một file bị nhiễm virus.



4. Nhập thông báo mà bạn muốn module hiển thị trong hộp text được cho. Bạn có thể nhập tối đa đến 250 ký tự.

5. Kế tiếp, bạn có thể:

- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại VirusScan Properties.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút sau đây để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại.

Choosing Detection optionss

Choosing Alert options

Choosing Report options

Choosing Exclusion options

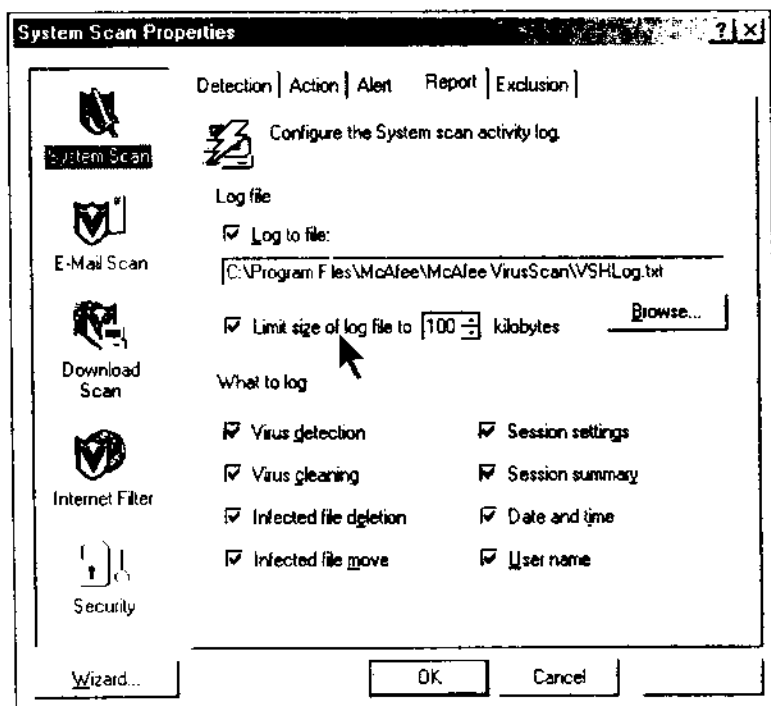
Choosing Security options

- ❖ Nhấp OK để lưu các tùy chọn cấu hình và trở lại hộp thoại Task Properties. Trong hộp thoại này, bạn có thể nhấp Run Now để bắt đầu một hoạt động quét với các tùy chọn mà bạn đã chọn.

4. Chọn các tùy chọn Report dành cho các tác vụ VirusScan theo thời biểu

Để quyết định trình ứng dụng sẽ ghi lại dữ liệu nào và kích cỡ của log file là bao nhiêu, hãy thực hiện các bước sau đây:

1. Chọn hộp kiểm log to file.
2. Chọn hộp kiểm Limit size of log file to để giảm thiểu log file. Nếu bạn không chọn hộp kiểm này, log file có thể tăng đến kích cỡ mà khoảng trống đĩa của bạn cho phép.



3. Nhập một giá trị dành cho kích cỡ file, theo đơn vị kilobyte, vào hộp text được cho.

Để xem các nội dung của log file, hãy mở cửa sổ trình ứng dụng VirusScan, sau đó chọn View Activity Log từ menu File.

4. Chọn các hộp kiểm phù hợp với thông tin mà bạn muốn trình ứng dụng ghi lại.

5. Kế tiếp, bạn có thể:

- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại VirusScan Properties.

- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút sau đây để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại.

Choosing Detection options

Choosing Alert options

Choosing Report options

Choosing Exclusion options

Choosing Security options

- ❖ Nhấp OK để lưu các tùy chọn cấu hình và trở lại hộp thoại Task Properties. Trong hộp thoại này, bạn có thể nhấp Run Now để bắt đầu một hoạt động quét với các tùy chọn mà bạn đã chọn.

5. Chọn các tùy chọn Exclusion dành cho các tác vụ VirusScan theo thời biểu

Để chỉ định các hạng mục nào mà trình ứng dụng VirusScan sẽ bỏ qua khi tác vụ quét này chạy, hãy thực hiện các bước sau đây:

1. Nhấp Add để loại ra một hạng mục mới.

2. Chọn một trong các hạng mục hiển thị, sau đó nhấp Edit để thay đổi định nghĩa hạng mục.

Thao tác này sẽ mở hộp thoại Edit Exclude Item. Thực hiện các thay đổi cần thiết, sau đó nhấp OK để đóng hộp thoại.

3. Chọn một trong các hạng mục hiển thị, sau đó nhấp Remove

để xóa một hạng mục ra khỏi danh sách. Điều này có nghĩa là trình ứng dụng VirusScan sẽ quét hạng mục trong suốt hoạt động kế tiếp của nó.

4. Kế tiếp, bạn có thể:

- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại VirusScan Properties.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút sau đây để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại.

Choosing Detection options

Choosing Alert options

Choosing Report options

Choosing Exclusion options

Choosing Security options

- ❖ Nhấp OK để lưu các tùy chọn cấu hình và trở lại hộp thoại Task Properties. Trong hộp thoại này, bạn có thể nhấp Run Now để bắt đầu một hoạt động quét với các tùy chọn mà bạn đã chọn.

8. Chọn các tùy chọn Security dành cho các tác vụ VirusScan theo thời biểu

Để khóa các xác lập mà bạn đã chọn cho tác vụ này, hãy thực hiện các bước sau đây:

1. Chọn các xác lập mà bạn muốn bảo vệ trong danh sách các hạng mục ở giữa trang đặc tính.
2. Nhấp Password để mở hộp thoại Specify Password.

Nhập một password vào hộp text đầu tiên, sau đó nhập lại password này vào hộp text ở phía dưới để xác nhận sự chọn lựa của bạn. Kế tiếp, hãy nhấp OK để đóng hộp thoại Specify Password.

3. Chọn hộp kiểm Inherit security options ở cuối trang để bảo đảm các xác lập bảo vệ an toàn của bạn sẽ xuất hiện theo

mặc định trong bất kỳ tác vụ nào mà bạn tạo bằng cách sao chép tác vụ này.

4. Kế tiếp, bạn có thể:

- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại VirusScan Properties.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút sau đây để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại.

Choosing Detection options

Choosing Alert options

Choosing Report options

Choosing Exclusion options

Choosing Security options

- ❖ Nhấp OK để lưu các tùy chọn cấu hình và trở lại hộp thoại Task Properties. Trong hộp thoại này, bạn có thể nhấp Run Now để bắt đầu một hoạt động quét với các tùy chọn mà bạn đã chọn.

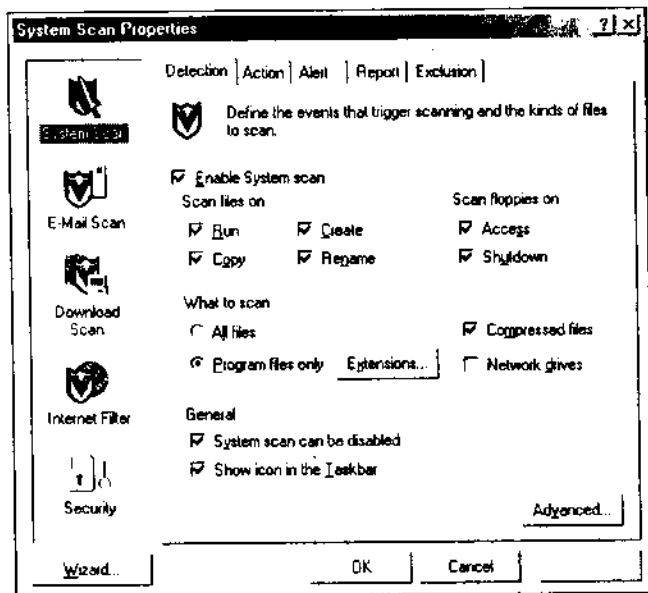
Bài 7

TÌM HIỂU VSHIELD SCANNER

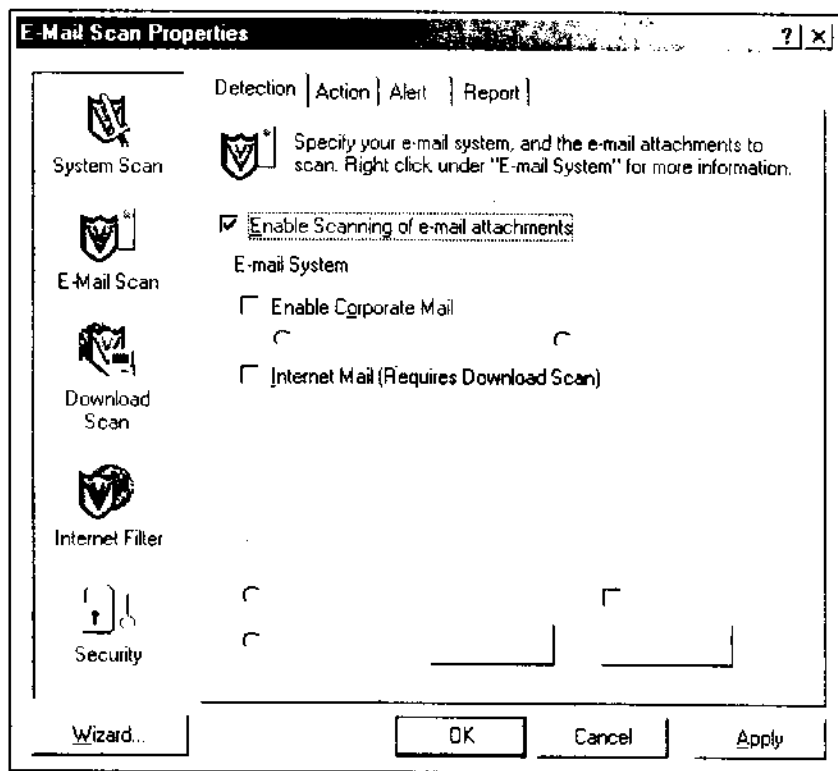
VShield scanner có năm module liên quan, mỗi module có một chức năng riêng biệt. Bạn có thể cấu hình các xác lập cho tất cả các module này trong hộp thoại VShield Properties.

Các module VShield bao gồm:

- ❖ **System Scan.** Module này tìm các virus trên đĩa cứng khi bạn làm việc với máy tính. Nó thay đổi các file khi hệ thống của bạn hay các máy tính khác đọc các file từ đĩa cứng hay ghi các file vào nó. Nó cũng có thể quét từ các đĩa mềm và các ổ đĩa mạng được ánh xạ sang hệ thống của bạn.

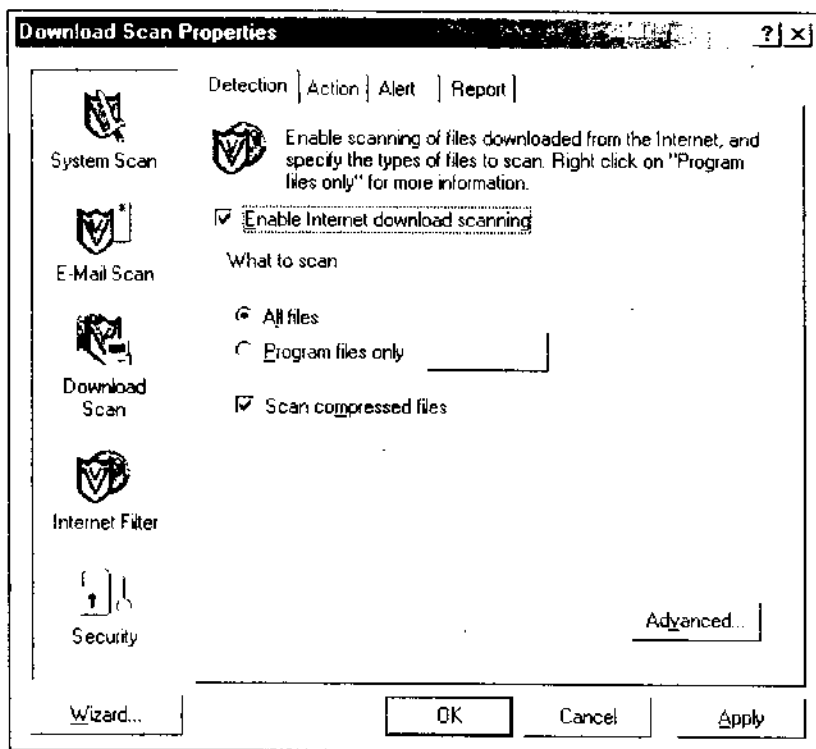


- ❖ **E-mail Scan.** Module này quét các thông báo e-mail và các file đính kèm thông báo mà bạn nhận được thông qua các hệ thống e-mail nội bộ và Internet. Nó quét hộp thư Microsoft Exchange hoặc Outlook và các hệ thống e-mail cc:Mail cũ hơn. Nó hoạt động kết hợp với module Download Scan để quét thư Internet đến thông qua các nguồn Simple Mail Transfer Protocol (SMTP) hoặc Post Office Protocol (POP-3). Để sử dụng module này, bạn phải cài đặt nó từ tùy chọn Custom trong Setup.

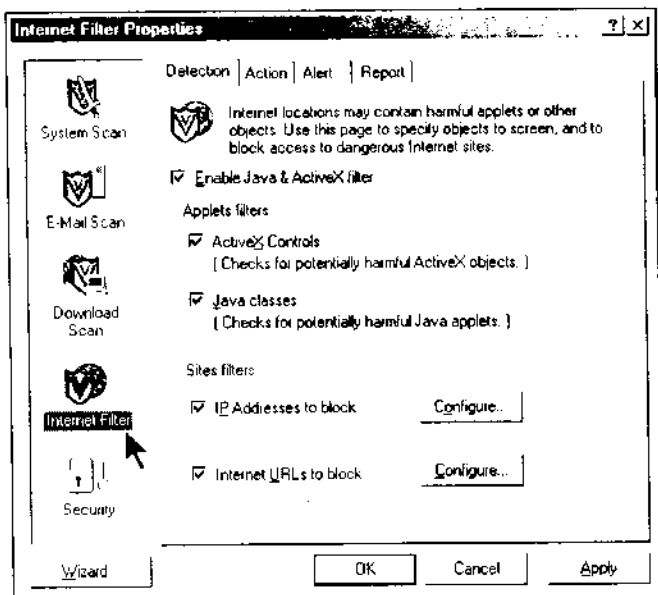


- ❖ **Download Scan.** Module này quét các file mà bạn tải xuống hệ thống từ Internet. Nếu bạn đã bật tùy chọn Internet mail trong module E-Mail Scan, nó sẽ chứa e-mail và các file đính kèm vốn thông qua các hệ thống e-mail SMTP hoặc

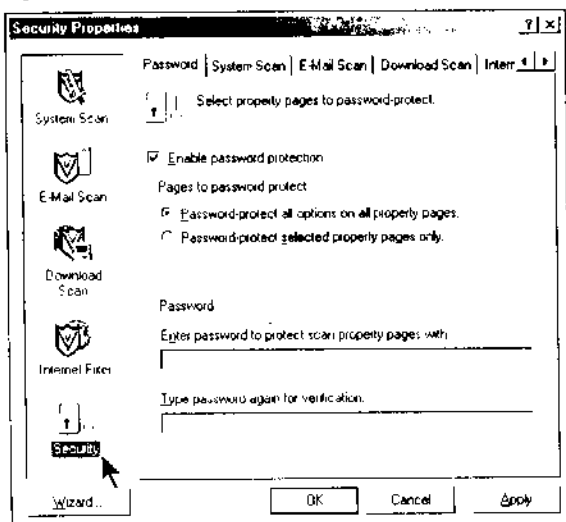
POP-3, bao gồm cả những chương trình e-mail client chẳng hạn như Eudora Pro, Microsoft Outlook Express, NetScape mail, và America Online mail. Để sử dụng module này, bạn phải cài đặt nó từ tùy chọn Custom trong Setup.



- ❖ **Internet Filter.** Module này tìm và ngăn chặn việc tải và thực thi các lớp Java và ActiveX control từ hệ thống khi bạn vào các site Internet. Nó cũng ngăn chặn việc bộ trình duyệt nối kết với các site Internet nguy hiểm. Để sử dụng module này, bạn phải cài đặt nó từ tùy chọn Custom trong Setup.



- ❖ **Security.** Module này cung cấp sự bảo vệ bằng password cho các module VShield còn lại. Bạn có thể bảo vệ một hoặc tất cả các trang đặc tính module riêng lẻ và xác lập một password để ngăn chặn sự thay đổi khi không được phép.



Ghi chú

Bởi vì VShield scanner chạy liên tục nên bạn không được cài đặt hay chạy trên một VShield scanner trên cùng một workstation. Điều này có thể làm cho scanner gây cản trở đến các hoạt động khác.

I. Các bộ trình duyệt web và các e-mail client tương thích

VShield scanner làm việc liên tục với nhiều bộ trình duyệt web phổ biến nhất và phần mềm e-mail client có sẵn dành cho nền Windows. Để làm việc với bộ trình duyệt, bạn đừng cài đặt scanner vượt quá những gì mà bạn đã thực hiện để nối kết máy tính với Internet. Tuy nhiên, bạn phải cấu hình scanner để nó hoạt động chính xác với phần mềm e-mail client của bạn.

McAfee đã thử nghiệm các bộ trình duyệt web sau đây và xác nhận rằng chúng hoạt động chính xác với VShield scanner:

- ❖ Netscape Navigator v3.x
- ❖ Netscape Navigator v4.0.x
- ❖ Microsoft Internet Explorer v3.x
- ❖ Microsoft Internet Explorer v4.x

McAfee cũng đã thử nghiệm các e-mail client và xác nhận rằng chúng hoạt động với module VShield Download Scan:

- ❖ Microsoft Outlook Express
- ❖ Qualcomm Eudora v3.x và v4.x
- ❖ Netscape Mail (đi kèm với phần lớn của phiên bản Netscape Navigator và Netscape Communicator)
- ❖ America Online mail v3.0 và v4.0

Để làm việc với module VShield E-mail Scan, bạn phải sử dụng các phiên bản đặc biệt của Lotus cc:Mail, hoặc phần mềm e-mail client của bạn phải hỗ trợ tiêu chuẩn MAPI của Microsoft. McAfee đã thử nghiệm các client sau đây và xác nhận rằng chúng hoạt động chính xác với module E-mail scan:

- ❖ Microsoft Exchange v4.0, v5.0 và v5.5
- ❖ Microsoft Outlook 97, Outlook 98 và Outlook 2000
- ❖ Lotus cc:Mail v6.x, v7.x và v8.x (không tương thích MAPI)

McAfee không chứng nhận tính tương thích của VShield scanner với các phần mềm client không được liệt kê ở trên.

II. Tại sao bạn nên sử dụng VShield scanner

VShield scanner có các tính năng tương thích duy nhất làm cho nó trở thành một phần hợp nhất của bộ phần mềm chống virus toàn diện VirusScan. Các tính năng này bao gồm:

- ❖ Quét vào lúc truy cập. Điều này có nghĩa là scanner tìm virus trong các file mà bạn mở, sao chép, lưu, hoặc chỉnh sửa và các file mà bạn đọc hoặc ghi vào đĩa mềm và các ổ đĩa mạng. Do đó nó có thể dò tìm và ngăn chặn virus ngay sau khi chúng xuất hiện trên hệ thống, bao gồm kể cả virus xâm nhập qua e-mail hoặc qua Internet.
- ❖ Dò tìm và ngăn chặn các đối tượng nguy hiểm. VShield scanner có thể ngăn chặn các đối tượng ActiveX và Java nguy hiểm đạt được sự truy cập vào hệ thống của bạn. Scanner thực hiện điều này bằng cách quét hàng trăm đối tượng mà bạn tải xuống khi bạn nối kết với web hoặc các file Internet khác, và các file đính kèm mà bạn nhận được cùng với e-mail. Nó so sánh các hạng mục này dựa vào danh sách các đối tượng nguy hiểm hiện tại mà nó lưu giữ và ngăn chặn chúng gây ra bất kỳ sự cố nào.
- ❖ Lọc site Internet. VShield scanner có kèm theo một danh sách các site web hay Internet nguy hiểm có thể gây nguy hại cho hệ thống của bạn, thường ở dạng phần mềm có thể tải xuống. Bạn có thể bổ sung bất kỳ site khác mà bạn không muốn phần mềm bộ trình duyệt của bạn nối kết với nó, bằng cách liệt kê địa chỉ Internet Protocol (IP) hoặc tên domain của nó.

- ❖ Hoạt động tự động. VShield scanner hợp nhất với một dãy bộ phần mềm trình duyệt và các trình ứng dụng e-mail client. Điều này cho phép scanner nối kết và quét các file đính kèm e-mail để tìm virus trước khi chúng xâm nhập vào máy tính của bạn.

Nếu bạn nối kết với Internet hoặc làm việc trên một mạng, việc ngưng để chạy thành phần này có thể nâng cao rất nhiều khả năng dò tìm và loại bỏ phần mềm nguy hiểm trước khi nó có cơ hội phá hỏng hệ thống của bạn.

III. Xác định VShield scanner trên hệ thống

VShield scanner có nhiều file dịch vụ Windows và trình điều khiển thiết bị liên quan, các file thư viện và các file hỗ trợ, không có file nào có giao diện người dùng. Các file này tương tác với hệ điều hành và các phần khác của phần mềm VirusScan khi thực hiện chức năng. Bạn sẽ tìm thấy phần lớn các file này trong vị trí sau đây, nếu bạn đã cài đặt phần mềm VirusScan với các tùy chọn mặc định của nó:

C:\Program Files\Common Files\McAfee VirusScan\McShield

Thành phần giao diện người dùng chính dành cho VShield scanner là tiện ích cấu hình của nó, VSCONFIG.EXE. File này nằm trong chương trình thư mục VirusScan, bạn sẽ tìm thấy thư mục này trong vị trí sau đây:

C:\Program Files\McAfee VirusScan\VirusScan

Bạn có thể nhấp đúp vào file này để chạy nó, nhưng McAfee đề nghị bạn khởi động chương trình cấu hình VShield từ một nơi khác trong giao diện VirusScan.

Để tìm hiểu thêm về các file mà VShield scanner cần hoạt động, hãy nhấp [here](#):

IV. Khởi động VShield scanner

Vào cuối tiến trình cài đặt VirusScan, Setup sẽ hỏi bạn có muốn bật VShield scanner vào lúc này hay không. Nếu bạn muốn VShield scanner tải vào bộ nhớ ngay lập tức và bắt đầu làm việc với các tùy

chọn mặc định vốn cung cấp cho bạn một chế độ phòng chống cơ bản. Nếu bạn không muốn, VShield scanner sẽ tải tự động vào lần kế tiếp bạn khởi động lại máy tính của mình.

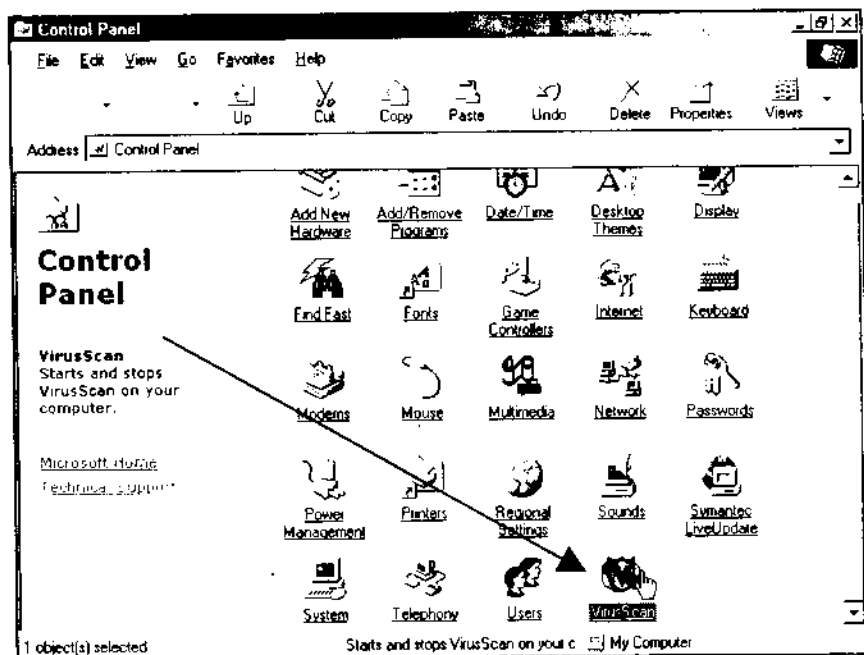
Khi VShield scanner khởi động lần đầu tiên, nó hiển thị một đối tượng trong file hệ thống Windows nhằm cho biết module nào trong số các module của nó đang hoạt động.

Khởi động VShield scanner tự động

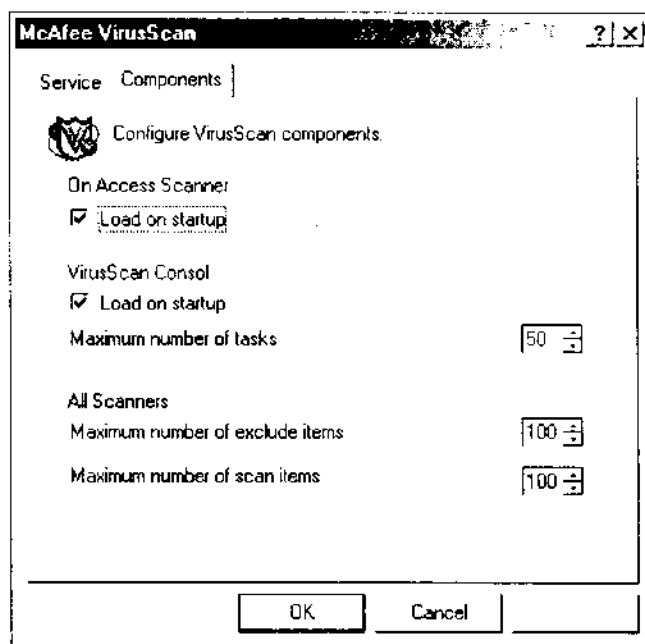
Nếu VShield scanner không khởi động tự động, bạn có thể xác lập nó để thực hiện điều này trong VirusScan control panel.

Thực hiện các bước sau đây:

1. Nhấp Start trong thanh tác vụ Windows, trở đến Settings, rồi sau đó chọn Control panel.



2. Xác định và nhấp đúp vào VirusScan control panel để mở nó.
3. Nhấp nhấn Components.



4. Chọn hộp kiểm Load VShield on startup ở đầu trang đặc tính Component.

5. Nhấp OK để đóng control panel.

VShield scanner sẽ khởi động khi bạn khởi động máy tính vào lần kế tiếp.

Bật VShield scanner và các module của nó

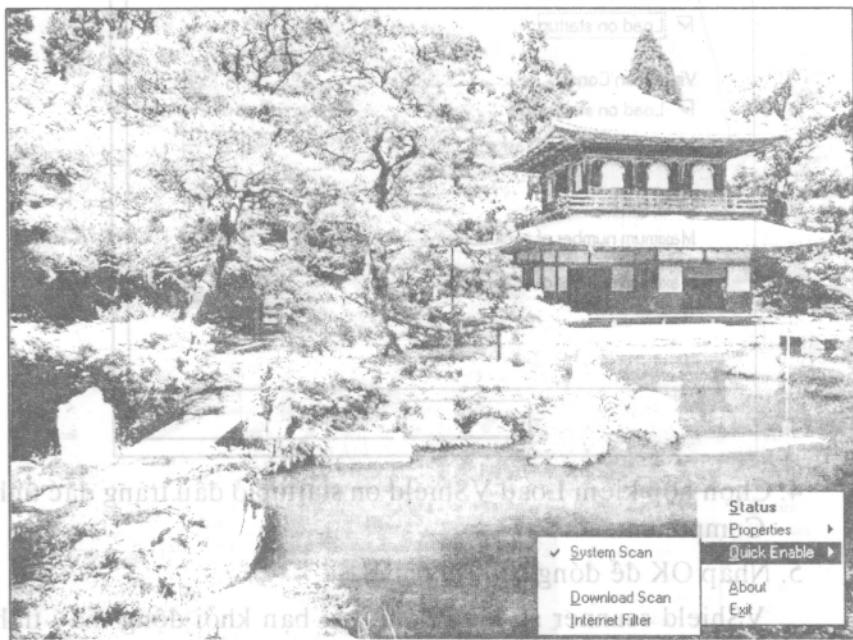
Ngay sau khi bạn đã cài đặt tất cả các thành phần VShield, bạn có thể sử dụng bất kỳ một trong bốn phương pháp sau đây để bật chúng.

Ghi chú

Việc bật một module có nghĩa là kích hoạt nó và tải nó vào bộ nhớ của máy tính để sử dụng. VShield scanner có thể khởi động và vẫn hoạt động cho bộ nhớ ngay cả khi không có module nào của nó được bật.

Sử dụng menu tắt VShield. Thực hiện các bước sau đây:

1. Nhấp phải vào biểu tượng VShield (🛡️) trong khay hệ thống Windows để hiển thị menu tắt của nó.
2. Trở vào Quick Enable.



3. Chọn một trong các tên module không có dấu kiểm. Các tên module có dấu kiểm ở kế bên chúng cho biết các module đó đang hoạt động. Các module không có dấu kiểm là các module không hoạt động.

Phụ thuộc vào tổ hợp module nào mà bạn bật, biểu tượng VShield sẽ hiển thị một trạng thái khác.

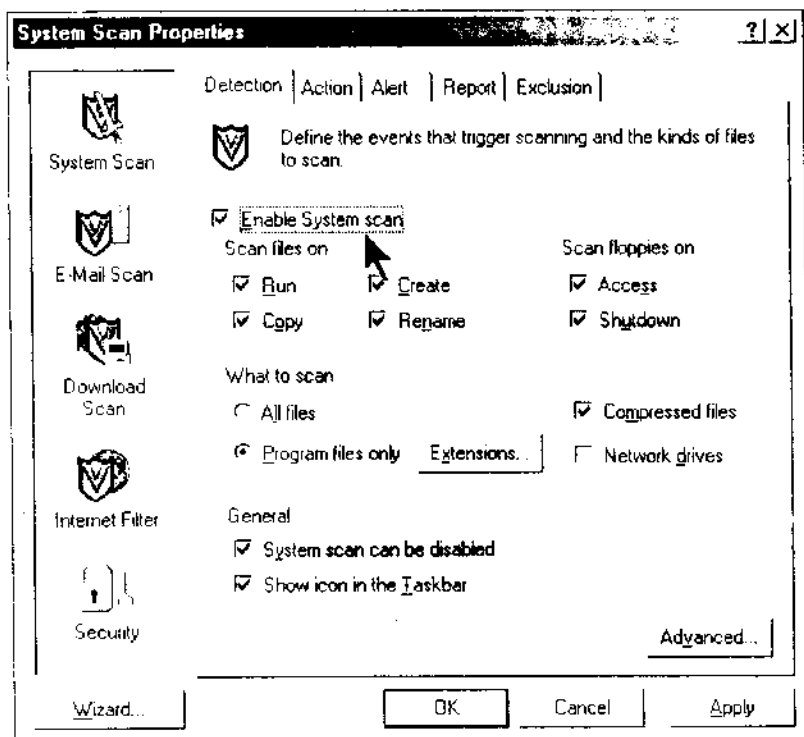
Sử dụng hộp thoại System Scan Status. Thực hiện các bước sau đây:

1. Nhấp đúp vào biểu tượng VShield (🛡️) trong khay hệ thống Windows để mở hộp thoại System Scan Status.

- Đối với mỗi module mà bạn muốn bật, hãy nhấp vào nút tương ứng, sau đó nhấp Enable. Nút tương tự trong trang đặc tính dành cho các module hoạt động sẽ có tên là Disable.
- Nhấp Close để đóng hộp thoại.

Sử dụng hộp thoại VShield Properties. Thực hiện các bước sau đây:

- Nhấp đúp vào biểu tượng VShield () trong khay hệ thống Windows để mở hộp thoại System Scan Status.
- Nhấp Properties để mở hộp thoại VShield Properties.
- Đối với mỗi module mà bạn muốn bật, hãy nhấp vào biểu tượng tương ứng dọc theo phía bên trái của hộp thoại, sau đó nhấp vào Detection.
- Chọn hộp kiểm Enable ở đầu mỗi trang.



Khi bạn thực hiện điều này, scanner sẽ bật module đó. Phụ thuộc vào tổ hợp module nào mà bạn bật, biểu tượng VShield sẽ hiển thị một trạng thái khác. Nếu bạn bật tất cả các module của nó, scanner sẽ hiển thị () trong khay hệ thống Windows, trừ khi bạn xóa chọn hộp kiểm Show icon in the taskbar trong trang đặc tính System Scan Detection.

Sử dụng VirusScan Console. Thực hiện các bước sau đây:

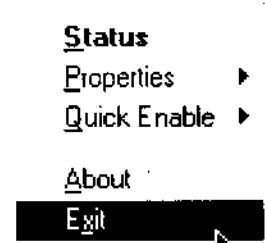
1. Nhấp đúp vào biểu tượng VirusScan Console () trong khay hệ thống Windows để hiển thị cửa sổ Console .
2. Chọn VShield trong danh sách tác vụ, và sau đó chọn Enable từ menu Task.

Console sẽ bật module System Scan và bất kỳ module nào khác mà bạn đã bật trước đó. Bạn không thể sử dụng phương pháp này để bật các module riêng lẻ khác với module System Scan.

Nhấp vào nút minimize hoặc close ở góc phía trên bên phải cửa sổ Console để thu nhỏ cửa sổ Console trở lại biểu tượng khay hệ thống.

Ghi chú

Đừng chọn Exit từ menu Task. Thao tác này sẽ tắt Console và hủy tải nó từ bộ nhớ. Để chạy bất kỳ tác vụ nào mà bạn đã lập thời biểu, Console phải hoạt động.



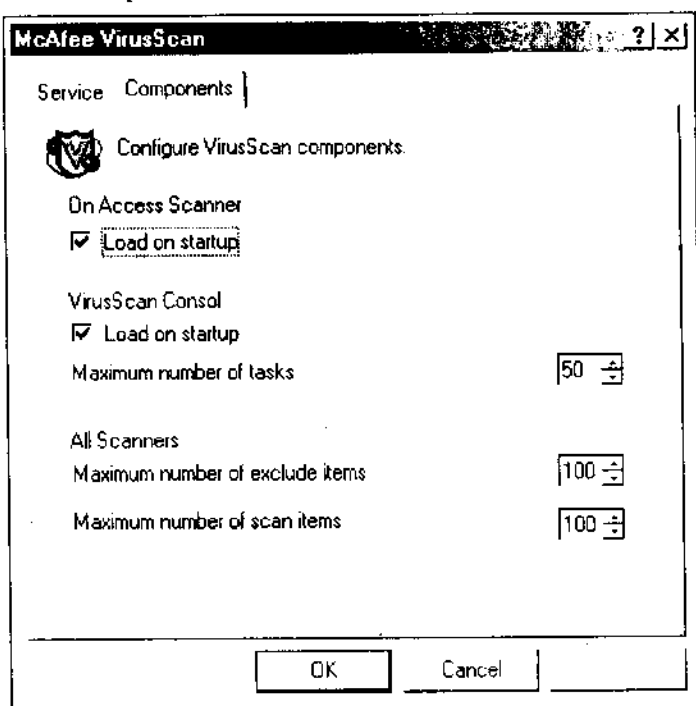
V. Ngưng hoặc tắt VShield scanner

Ngăn chặn scanner tự động khởi động

Nếu bạn không muốn VShield scanner khởi động tự động, bạn có thể sử dụng VirusScan control panel để ngăn chặn nó thực hiện điều này.

Thực hiện các bước sau đây:

1. Nhấp Start trong thanh tác vụ Windows, trở đến Settings, rồi sau đó chọn Control panel.
2. Xác định và nhấp đúp vào VirusScan control panel để mở nó.
3. Nhấp nhấn Components.
4. Xóa chọn hộp kiểm Load VShield on startup ở đầu trang đặc tính Component.



5. Nhấp OK để đóng control panel.

VShield sẽ không ngưng hay hủy tải vào lúc này, nhưng nó sẽ không khởi động khi bạn khởi động máy tính của mình vào lần kế tiếp.

Ngưng hoàn toàn VShield scanner

Bạn có thể ngưng VShield scanner bằng một trong ba cách sau đây.

Ghi chú

Việc ngưng hoàn toàn scanner có nghĩa là hủy kích hoạt tất cả các module VShield và loại bỏ các scanner ra khỏi bộ nhớ. Biểu tượng VShield sẽ biến mất khỏi khay hệ thống. Vào lúc này, bạn có thể khởi động lại scanner chỉ từ VirusScan control panel, từ VirusScan Console, hoặc bằng cách khởi động lại máy tính nếu bạn đã xác lập VShield để nó tải lúc khởi động.

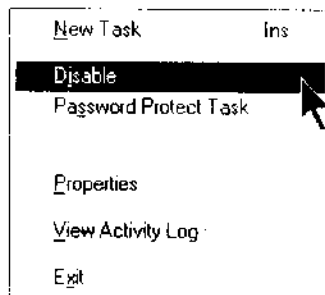
Sử dụng menu tắt VShield. Thực hiện các bước sau đây:

1. Nhấp phải vào biểu tượng VShield () trong khay hệ thống Windows để hiển thị menu tắt của nó.
2. Chọn Exit.

VShield scanner sẽ ngưng và hủy tải nó từ bộ nhớ. VShield sẽ biến mất khỏi thanh tác vụ Windows.

Sử dụng VirusScan Console. Thực hiện các bước sau đây:

1. Nhấp đúp vào biểu tượng VirusScan Console () trong khay hệ thống Windows để hiển thị cửa sổ Console.
2. Chọn VShield trong thanh tác vụ, sau đó chọn Disable từ menu Task.

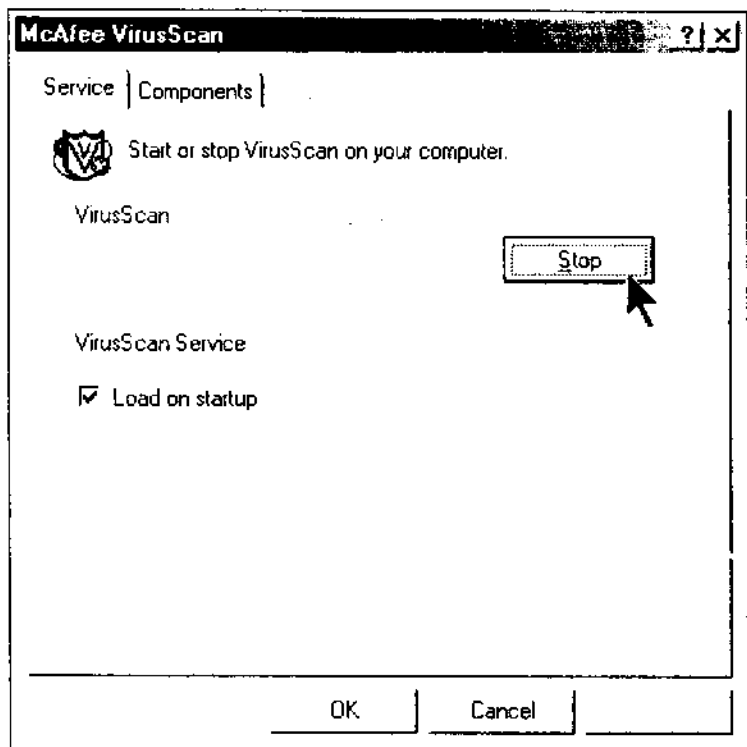


Console sẽ ngưng VShield scanner và tắt cả các module của nó, hủy tải chúng từ bộ nhớ. Biểu tượng VShield sẽ biến mất khỏi thanh tác vụ Windows.

3. Nhấp vào nút minimize hoặc close ở góc phía trên bên phải của cửa sổ Console để thu nhỏ nó trở lại biểu tượng khay hệ thống.

Sử dụng VirusScan control panel. Thực hiện các bước sau đây:

1. Nhấp Start trong khay hệ thống Windows, trở đến Settings, rồi sau đó chọn Control Panel.
2. Xác định và nhấp đúp vào VirusScan control panel để mở nó.
3. Nhấp nhãn Service.
4. Nhấp Stop.



Tất cả các thành phần VirusScan đang hoạt động sẽ ngưng, đóng tất cả các cửa sổ hay các hộp thoại đang mở, loại bỏ các biểu tượng của chúng ra khỏi khay hệ thống Windows và hủy tải từ bộ nhớ.

5. Nhấp Ok để đóng control panel.

Tắt VShield scanner và các module của nó

Bạn có thể sử dụng bất kỳ một trong ba phương pháp sau đây để tắt bất kỳ các module của VShield.

Ghi chú

Việc tắt một module có nghĩa là hủy kích hoạt nó và ngăn chặn việc chạy nó trong suốt một tác vụ quét. Nó không có nghĩa là ngưng scanner và hủy tải nó từ bộ nhớ của máy tính. VShield scanner có thể vẫn hoạt động trong bộ nhớ ngay cả khi không có module nào của nó được bật. Scanner để lại một biểu tượng trong khay hệ thống Windows mà bạn có thể sử dụng để bật nó trở lại.

Sử dụng menu tắt VShield. Thực hiện các bước sau đây:

1. Nhấp phải biểu tượng VShield () trong khay hệ thống Windows để hiển thị menu tắt của nó.
2. Trỏ đến Quick Enable.
3. Chọn một trong các tên module có một dấu kiểm ở kế bên nó để hủy kích hoạt nó. Các tên module có một dấu kiểm ở kế bên chúng là các module đang hoạt động. Các tên module không có dấu kiểm ở kế bên là các module không đang hoạt động.

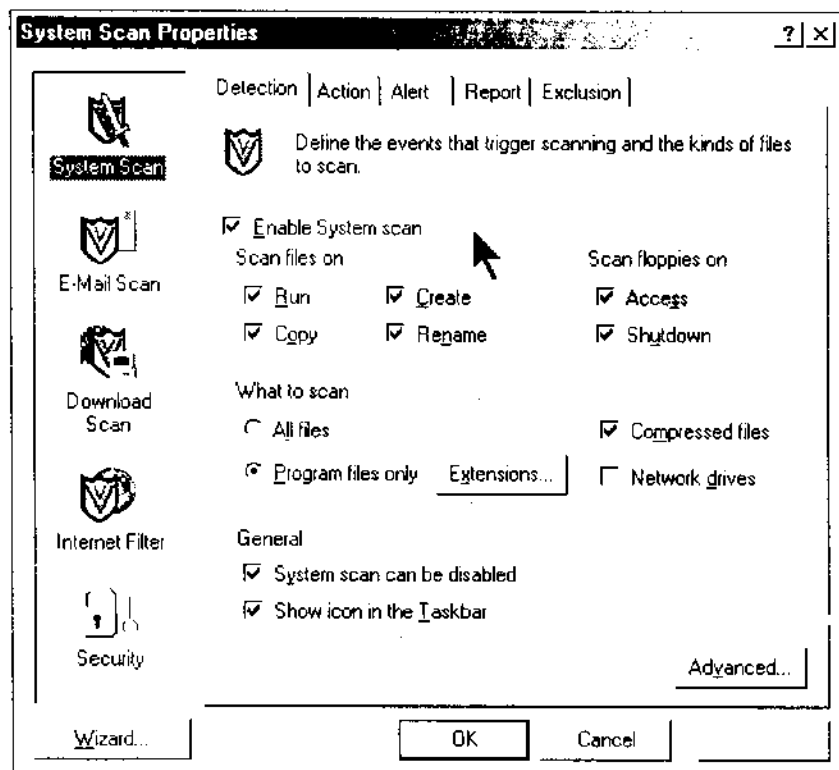
Sử dụng hộp thoại System Scan Statup. Thực hiện các bước sau đây:

1. Nhấp đúp vào biểu tượng VShield () trong khay hệ thống Windows để mở hộp thoại System Scan Status.
2. Đối với mỗi module mà bạn muốn tắt, hãy nhấp vào nhãn tương ứng, sau đó nhấp Disable. Nút tương tự trong trang đặc tính dành cho các module không hoạt động sẽ có tên là Enable.

3. Nhấp Close để đóng hộp thoại.

Sử dụng hộp thoại VShield Properties. Thực hiện các bước sau đây:

1. Nhấp đúp biểu tượng VShield () trong khay hệ thống Windows để mở hộp thoại System Scan Status.
2. Nhấp vào Properties để mở hộp thoại VShield Properties.
3. Đối với mỗi module mà bạn muốn tắt, hãy nhấp vào biểu tượng tương ứng dọc theo phía bên trái của hộp thoại, sau đó nhấp nhấn Detection.
4. Xóa chọn hộp kiểm Enable tại đầu mỗi trang.



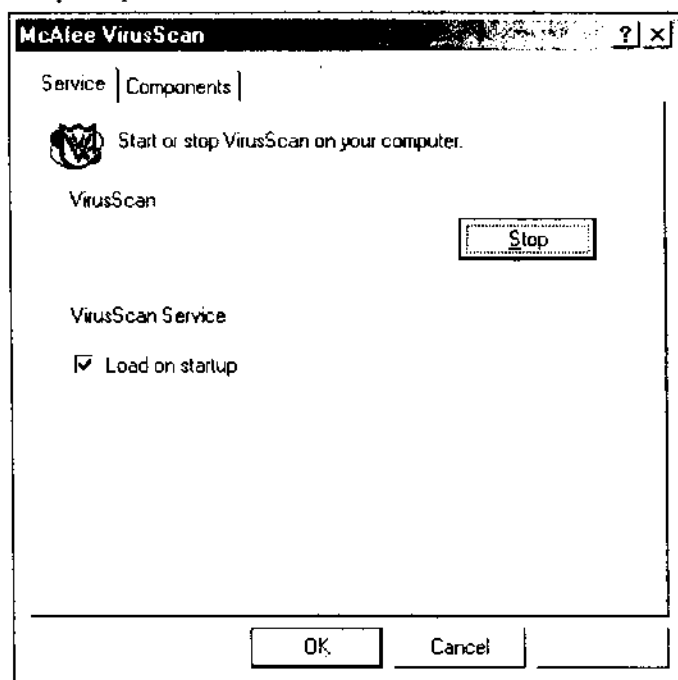
Khi bạn thực hiện điều này, scanner sẽ tắt module đó và làm cho tất cả các tùy chọn cấu hình trong trang đó trở nên không có sẵn. Phụ

thuộc vào các module nào mà bạn đã tắt, Biểu tượng VShield sẽ hiển thị một trạng thái khác. Nếu bạn tắt tất cả các module của nó, scanner sẽ hiển thị trong khay hệ thống Windows, trừ khi bạn xóa chọn hộp kiểm Show icon in the taskbar trong trang đặc tính System Scan Detection. Trong trường hợp đó, VShield sẽ không hiển thị một biểu tượng trong khay hệ thống.

VI. Khởi động lại tại VShield scanner và Console từ control panel

Thực hiện các bước sau đây:

1. Nhấp Start trong thanh tác vụ Windows, trở đến Settings, rồi sau đó chọn Control Panel.
2. Xác định và nhấp đúp VirusScan control panel để mở nó.
3. Nhấp nhấn Service.
4. Nhấp Stop



Tất cả các thành phần VirusScan hoạt động sẽ ngưng, đóng tất cả các cửa sổ hoặc hộp thoại đang mở, loại bỏ các biểu tượng của nó ra khỏi khay hệ thống Windows, và hủy tải từ bộ nhớ.

5. Nhấp Start trong cùng trang đặc tính.
6. VShield scanner và VirusScan Console sẽ khởi động lại và hiển thị các biểu tượng của chúng trong khay hệ thống Windows.
7. Nhấp OK để đóng control panel

VII. Các file phụ thuộc và liên quan dành cho VShield scanner

VShield scanner chạy ở dạng một dịch vụ Windows NT trên các hệ thống Windows NT Workstation v4.0 và Windows 2000 Professional, và ở dạng một trình điều khiển thiết bị ảo trên các hệ thống Windows 95 và Windows 98. Nó cần nhiều file hỗ trợ để thực hiện chức năng, bao gồm cả một số file vận hành các module khác nhau của nó. Bảng sau đây liệt kê VShield và các file liên quan:

Các file chương trình

Các file sau đây chạy trực tiếp ở dạng thành phần VShield hoặc ở dạng các file hỗ trợ hay thư viện VShield chuyên biệt.

File	Chức năng	Vị trí
VSTAT.EXE	Điều khiển sự giao tiếp giữa các chương trình trong các thành phần VShield, hiển thị biểu tượng VShield	C:\Program Files\McAfee VirusScan\
VSCONFIG.EXE	Cấu hình các xác lập VShield, hiển thị hộp thoại VShield Properties	C:\Program Files\McAfee VirusScan\
MFLDR.DLL	File thư viện dùng để sử dụng với các hệ thống	C:\Program Files\McAfee VirusScan\

	e-mail MAPI; điều khiển sự truy cập và các chức năng xuất	VirusScan
CONFWIZ.EXE	File wizard cấu hình VShield	C:\Program Files\McAfee VirusScan\VirusScan
VSHWIN32.EXE	Giao tiếp giữa VSSTAT .EXE và module VShield System Scan	C:\Program Files\McAfee VirusScan\VirusScan
MCSHIELD.EXE	Module System Scan. Chạy ở dạng một dịch vụ Windows NT trên các hệ thống Windows NT Workstation v4.0 và Windows 2000 Professional	C:\Program Files\Common Files\McAfee VirusScan\VirusScan\McShield
NAIEVENT.DLL	Nguồn logging event. Chỉ chạy trên các hệ thống Windows NT Workstation v 4.0 và Windows 2000 Professional	C:\Program Files\Common Files\McAfee VirusScan\VirusScan\McShield
MCSHIELD.DLL	File nguồn tài nguyên dành cho module System Scan. Chỉ chạy trên Windows NT Workstation v4.0 và Windows 2000 Professional	C:\Program Files\Common Files\McAfee VirusScan\VirusScan\McShield\Res09
NAIANN.DLL	File hỗ trợ dành cho module System Scan. Các hệ thống Windows NT Workstation v4.0 và Windows 2000 Professional	C:\Program Files\Common Files\McAfee VirusScan\McShield

NAIFILTR.SYS	Trình điều khiển lọc dành cho module System Scan. Chỉ chạy trên các hệ thống Windows NT và Windows 2000 Professional	C:\Program Files\Common Filies\McAfee VirusScan\McShield
NAIFSREC.SYS	Bộ chỉ dẫn lại hệ thống file dành cho module System Scan. Chỉ chạy trên các hệ thống Windows NT Workstation v4.0 và Windows 2000 Professional	C:\Winnt\System32\drivers
NTCLIENT.DLL	File hỗ trợ đối với module System Scan. Chỉ chạy trên hệ thống Windows NT Workstation v4.0 và Windows 2000 Professional	C:\Program Files\McAfee VirusScan\VirusScan
SCANSERV.DLL	File hỗ trợ dành cho module System Scan. Chỉ chạy trên hệ thống Windows NT Workstation v4.0 và Windows 2000 Professional	C:\Program Files\McAfee VirusScan\VirusScan\McShield
VSHIELD.VXD	Module VShield System Scan. Chạy ở dạng một trình điều khiển thiết bị ảo Windows trên các hệ thống Windows 95 và Windows 98.	C:\Windows\System
VSHINT.VXD	File hỗ trợ VShield. Khởi tạo các dịch vụ dành cho giao diện chế độ bảo vệ DOS. Chỉ chạy trên các hệ thống Windows 95 và Windows 98	C:\Windows\System

MCSCAN32.VXD	Công cụ quét McAfee. Chỉ chạy trên các hệ thống Windows 95 và Windows 98	C:\Windows\System
MCUTIL.VXD	File hỗ trợ dành cho module System Scan. Chỉ chạy trên các hệ thống Windows 95 và Windows 98	C:\Windows\System
MCKRNL.VXD	File hỗ trợ dành cho module System Scan. Chỉ chạy trên các hệ thống Windows 95 và Windows 98	C:\Windows\System
SCANEMAL.DLL	Quét e-mail mà bạn nhận được từ Internet hai từ mạng của bạn thông qua các hệ thống e-mail MAPI	C:\Program Files\ McAfee VirusScan\ VirusScan
CCM_SCAN.EXE	Quét e-mail mà bạn nhận được thông qua các hệ thống Lotus cc:Mail v7.x và các hệ thống cc: Mail trước đây	C:\Program Files\ McAfee VirusScan\ VirusScan
WEBSCANX.EXE	Cung cấp tính năng cho các module VShield Download Scan và Internet Filter. Khởi tạo WBHOOK32.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
WBHOOK32.DLL	Cung cấp tính năng cho các module VShield Download Scan, và Internet Filter. Ngăn chặn các file được tải xuống thông qua các bộ trình duyet Web để công cụ quét kiểm tra	C:\Program Files\ McAfee VirusScan\ VirusScan

Các file phụ thuộc

VShield cần các file này để chạy, nhưng đây không phải là các file chương trình VShield, hoặc không dành riêng cho sự hỗ trợ VShield.

File	Chức năng	Vị trí
AVSYNMGREXEXE	Dịch vụ quản lý VirusScan. Khởi tạo, khởi động và ngưng tất cả các thành phần của dịch vụ VirusScan. Phải chạy để bật tất cả các thành phần VirusScan	C:\Program Files\ McAfee VirusScan\ VirusScan
AVSYNCH.DLL	Điều khiển sự giao tiếp giữa các thành phần thông qua bộ nhớ dùng chung	C:\Program Files\ McAfee VirusScan\ VirusScan
SYNCUTIL.DLL	Chứa các dữ liệu dùng chung giữa các thành phần	C:\Program Files\ McAfee VirusScan\ VirusScan
VSUTIL.DLL	Cung cấp các tiện ích chung cho các thành phần	C:\Program Files\ McAfee VirusScan\ VirusScan
AVSMCPA.CPL	VirusScan control panel applet	C:\Windows\System or C:\WinNT\ Sys- tem 32
RESDDL.DLL	File nguồn tài nguyên dành cho tất cả các thành phần	C:\Program Files\ Common Files\ McAfee VirusScan\ McPal
MCSCAN32.DLL	File công cụ McAfee Scan	C:\Program Files\Common Files\McAfee VirusScan\VirusScan Engine4.0.xx

RWABS16.DLL	File hỗ trợ dành cho công cụ quét	C:\Program Files\Common Files\McAfee VirusScan\VirusScan Engine\4.0.xx
RWABS32.DLL	File hỗ trợ dành cho công cụ quét	C:\Program Files\Common Files\McAfee VirusScan\VirusScan Engine\4.0.xx
MESSAGES.DAT	File hỗ trợ dành cho công cụ quét. Cung cấp các thông báo dò tìm virus cho công cụ	C:\Program Files\Common Files\McAfee VirusScan\VirusScan Engine\4.0.xx

Các file tạm thời

VShield scanner và các file liên quan của nó sử dụng các file này làm “các bản đồ bộ nhớ” để chứa các tùy chọn cấu hình được sao chép từ phần đăng ký Windows khi chương trình chạy. Các file này bắt đầu với một kích cỡ file chuẩn và dữ liệu tối thiểu, mở rộng hay thu nhỏ khi cần thiết để chứa dữ liệu cấu hình.

File	Chức năng	Vị trí
SYNC+MAP.MMF	File bản đồ bộ nhớ dành cho AVSYNCH.DDL	C:\Program Files\McAfee VirusScan\VirusScan
AVCONSOLE.MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\McAfee VirusScan\VirusScan
DAV_CONS.MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\McAfee VirusScan\VirusScan

DAV_EXCL .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
DAV_SCAN .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
DEXCLDEF .MFF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
DSCANDEF .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
DVS_EXCL .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
VSCANGEN .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
VSCANOAS .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
VSCANODS .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan

VIII. Xem các số liệu thống kê VShield scanner

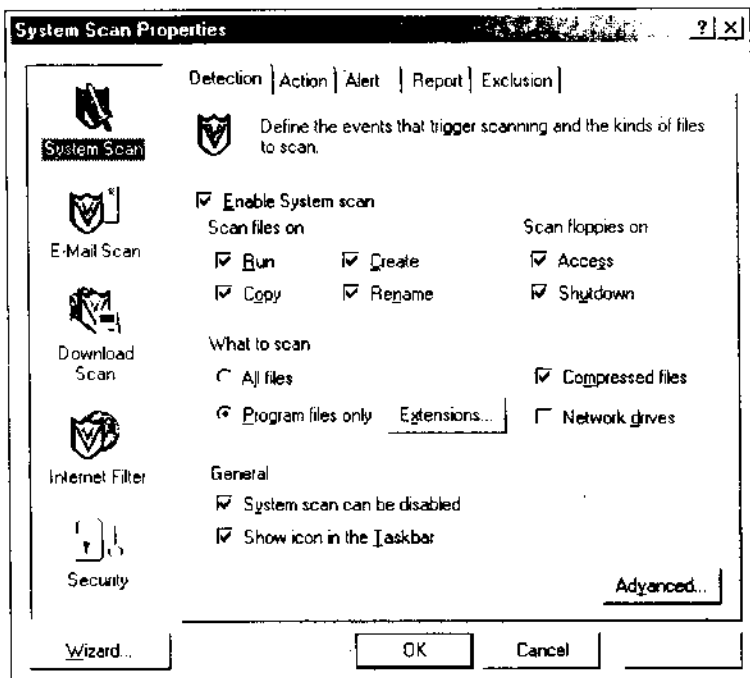
Ngay sau khi bạn kích hoạt và cấu hình VShield scanner, nó hoạt động liên tục trong nền, theo dõi và sau đó quét e-mail mà bạn nhận được, các file mà bạn chạy hoặc tải xuống, hoặc các đối tượng Java và ActiveX mà bạn gặp.

Để xem một bản tóm tắt thời gian thực tế về tiến độ của nó:

1. Nhấp đúp vào biểu tượng file hệ thống VShield () để mở hộp thoại Status.
2. Nhấp nhấn tương ứng với module chương trình mà bạn muốn theo dõi tiến độ của nó.

Thông tin mà mỗi module sẽ báo cáo là:

- ❖ System Scan. Module này báo cáo số lượng file mà nó đã quét, số lượng các file bị nhiễm mà nó đã tìm thấy, và số mà nó đã xử lý, di chuyển hay xóa bỏ.
- ❖ E-mail Scan. Module báo cáo số lượng file mà nó đã quét, số lượng file bị nhiễm mà nó đã tìm thấy, và số mà nó đã di chuyển hay đã xóa.
- ❖ Download Scan. Module báo cáo số lượng file mà nó đã quét, số lượng file bị nhiễm mà nó đã tìm thấy, và số mà nó đã di chuyển hay đã xóa.
- ❖ Internet Filter. Module báo cáo số lượng đối tượng Java và ActiveX hoặc site Internet mà nó đã quét và số mà nó đã “ngăn cấm”, hay tránh không cho bạn gặp phải.



Để xem một phần mô tả ngắn gọn của mỗi hạng mục xuất hiện trong trang này, hãy nhấp phải vào một hình hay nhãn, sau đó chọn What's This? từ menu tắt, hoặc nhấp vào nút dấu chấm hỏi ở góc phía trên bên phải của hộp thoại, sau đó nhấp vào hạng mục mà bạn muốn xem phần mô tả của nó.

Nếu bạn đã kích hoạt tính năng báo cáo, VShield Scanner cũng ghi thông tin tương tự trong các file cho mỗi module. Bạn cũng có thể xem thông tin này trong hộp thoại Task Properties dành cho mỗi module VShield. Để tìm hiểu cách hiển thị thông tin này, hãy nhấp here.

Các chức năng khác có sẵn trong hộp thoại này là:

- ❖ **Bật hay tắt các module.** Nhấp vào nhãn tương ứng với thành phần chương trình mà bạn muốn bật hay tắt, sau đó nhấp Enable để khởi động thành phần chương trình. Nhấp Disable để tách nó.

- ❖ Mở hộp thoại VShield Properties. Nhấp vào nhãn tương ứng với thành phần chương trình mà bạn muốn cấu hình, sau đó nhấp Properties để mở hộp thoại VShield Properties dành cho module đó. Để tìm hiểu cách chọn các cấu hình dành cho scanner, hãy nhấp [here](#).

IX. Cấu hình VShield scanner

Để cấu hình VShield scanner sao cho nó bảo vệ hệ thống của bạn, bạn phải cho nó biết:

- ❖ Bạn muốn nó quét vùng nội dung nào, và trong một số trường hợp bạn muốn nó quét một hạng mục vào lúc nào.
- ❖ Bạn muốn nó thực hiện điều gì nếu nó tìm thấy một virus
- ❖ Nó nên cho bạn biết bằng cách nào khi nó tìm thấy một virus
- ❖ Bạn có muốn nó theo dõi các hành động của nó hay không
- ❖ Bạn không muốn nó quét virus cho các hạng mục nào
- ❖ Bạn có muốn bảo vệ các xác lập mà bạn đã chọn để tránh sự thay đổi khi không được phép hay không

VShield scanner cung cấp nhiều trang đặc tính mà bạn có thể sử dụng để cho nó biết cách hoạt động. Bạn có thể bật và cấu hình một hoặc tất cả các module VShield scanner trong một tổ hợp bất kỳ phù hợp với nhu cầu của bạn.

Ghi chú

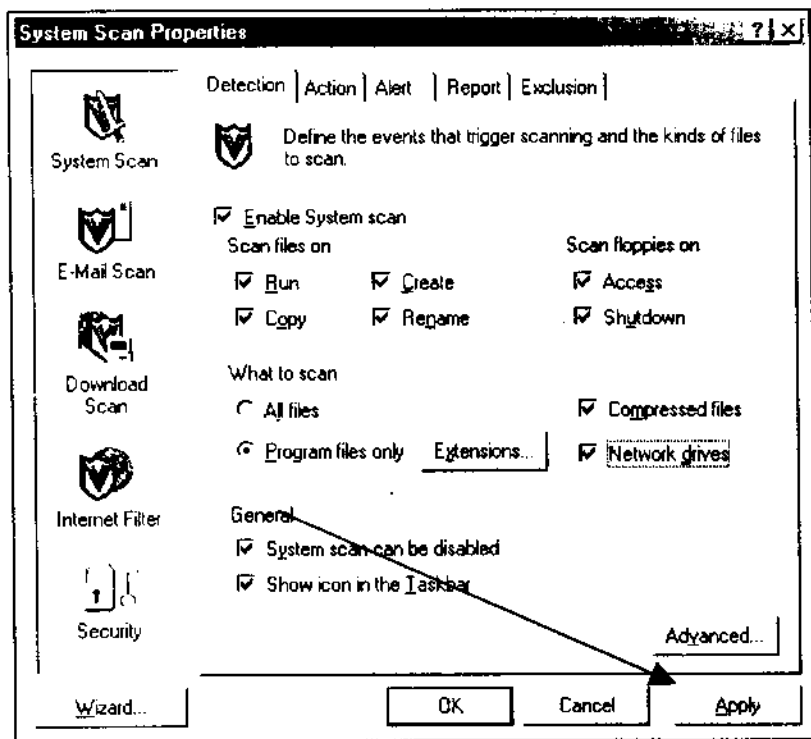
Để xem và cấu hình tất cả các VShield, bạn phải chạy Setup với các tùy chọn cài đặt Custom. Một tiến trình cài đặt tiêu biểu không cài đặt các module E-mail Scan, Download Scan, hay Internet Filter. Theo mặc định, VShield scanner chỉ khởi động khi module System Scan được bật.

Để bắt đầu, hãy thực hiện các bước sau đây:

1. Nhấp phải vào biểu tượng VShield trong thanh tác vụ Windows, trở đến Properties trong menu tắt, sau đó chọn System Scan.

Thao tác này sẽ mở hộp thoại VShield Properties. Trong hộp thoại này, thanh tiêu đề sẽ tương ứng với biểu tượng module đang được chọn. Ở đây, thanh tiêu đề sẽ có tên là System Scan Properties.

2. Nhấp vào bất kỳ một trong các biểu tượng module dọc theo phía bên trái của hộp thoại để hiển thị các trang đặc tính dành cho module đó.



Bạn có thể chỉ định các tùy chọn cấu hình VShield vào bất kỳ lúc nào - chỉ cần nhấp OK hoặc Apply ở cuối hộp thoại. Để đóng hộp thoại VShield Properties mà không lưu các thay đổi, hãy nhấp Cancel.

Hộp thoại VShield Properties cung cấp cho bạn các tùy chọn cần thiết để cấu hình mỗi module phù hợp với nhu cầu của bạn. Nhấp vào các nút được liệt kê ở phía dưới để tìm hiểu cách chọn các tùy

chọn dành cho mỗi module;

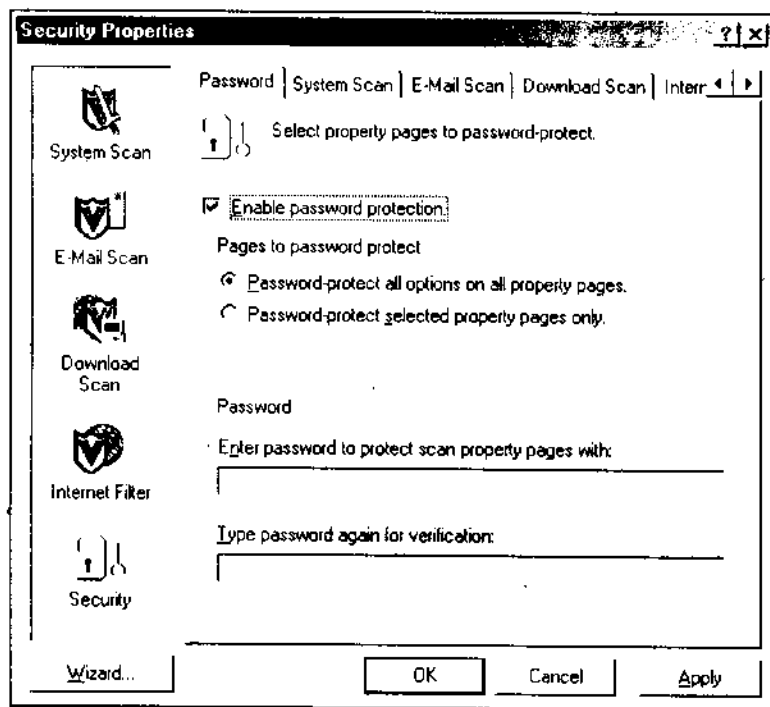
System scan module

E-mail Scan module

Download Scan module

Internet Filter module

Security



X. Cấu hình System Scan

Module VShield System Scan nằm trong phần chính của VShield scanner. Nó quét các file đến từ bất kỳ nguồn nào, bao gồm cả các file mà các module VShield khác gửi nó từ Internet và các thông báo e-mail. Module có thể kiểm tra hệ thống để tìm virus mỗi khi bạn mở, chạy, sao chép, lưu, đặt lại tên hay chỉnh sửa các file trên đĩa cứng của bạn trên bất kỳ phương tiện có thể tháo rời nào được gắn

với máy tính, hoặc trên các ổ đĩa mạng được ánh xạ sang hệ thống. Nó cũng có thể dò tìm các virus mỗi khi bạn đọc hoặc ghi vào một đĩa mềm. Là một tùy chọn cao cấp, bạn có thể kích hoạt tiến trình quét, cung cấp cho scanner tính năng dò tìm các virus chưa được nhận biết hay chưa được phân loại.

Module có thể thực hiện nhiều hành động tự động để phản hồi bất kỳ virus nào mà nó tìm thấy, và có thể báo cáo những gì nó đã thực hiện bằng một thông tin cảnh báo khi nó thực hiện hành động hay đưa vào log file để bạn có thể xem xét khi bạn có thời gian rảnh. Bạn cũng có thể xác lập để nó hỏi bạn cần thực hiện điều gì khi nó tìm thấy một virus.

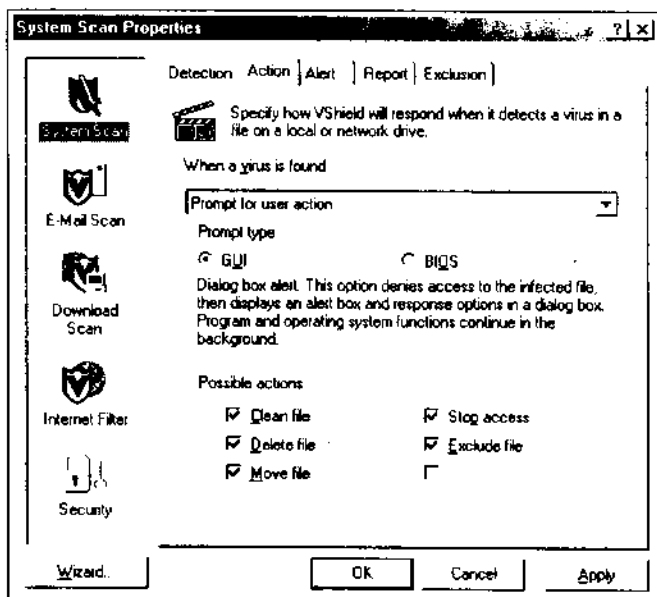
Ở nơi khác trong module này, bạn có thể chọn các tùy chọn yêu cầu VShield scanner hiển thị một biểu tượng trạng thái trong thanh tác vụ Windows để bạn có thể xem lướt qua các module VShield nào đang hoạt động, nếu có. Một tùy chọn khác cho phép bạn tách module System Scan. Tùy chọn này không thể có sẵn nếu bạn chạy phần mềm VirusScan trong chế độ an toàn.

Để chọn các tùy chọn, hãy nhấp vào biểu tượng System Scan ở phía bên trái của hộp thoại System Scan Properties để hiển thị các trang đặc tính dành cho module này.

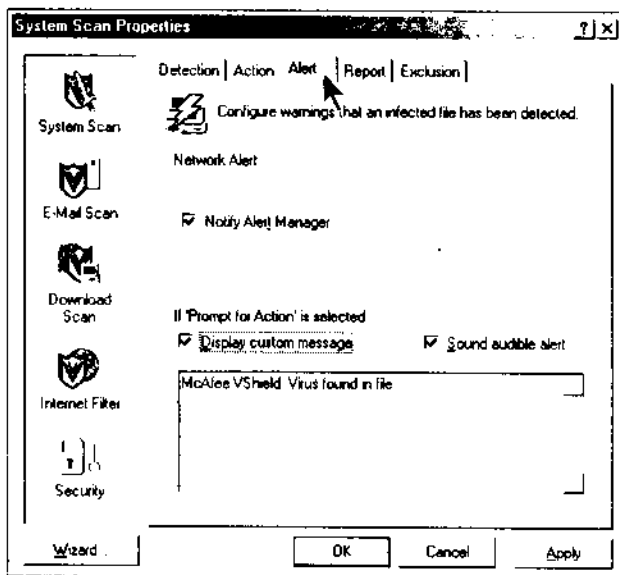
Kế tiếp, hãy nhấp vào các nút được liệt kê ở phía dưới để tìm hiểu các tùy chọn dành cho mỗi trang đặc tính:

Detection options

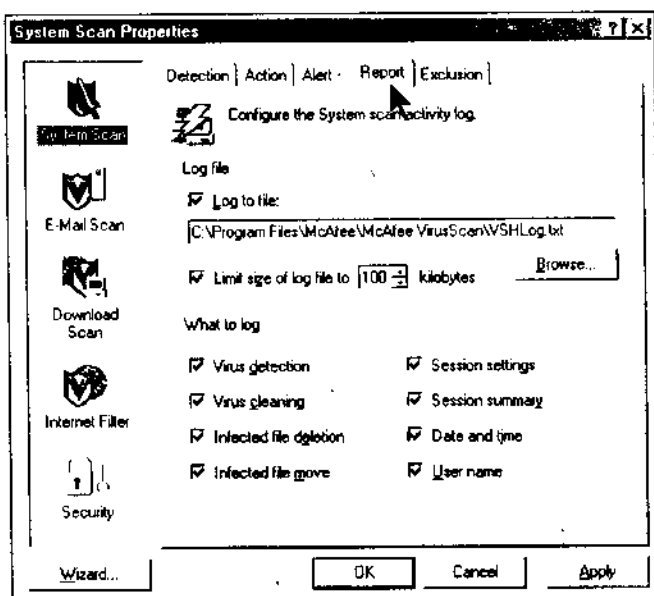
Action options



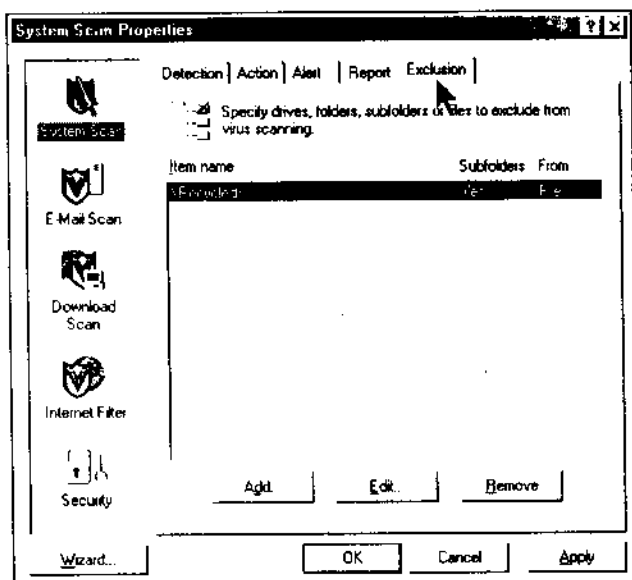
Alert options



Report



Exclusion



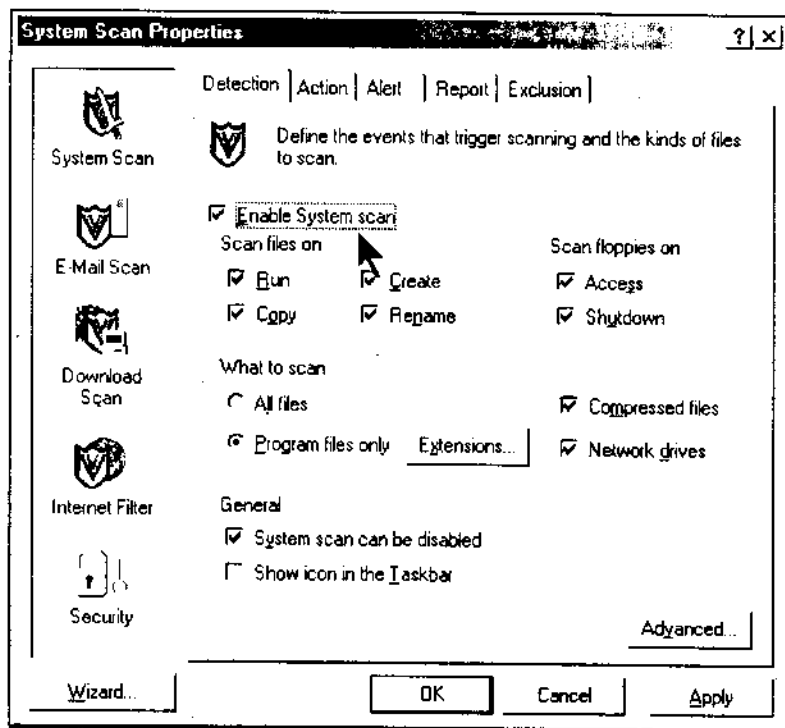
1. Chọn các tùy chọn Detection dành cho module System Scan

Khi bạn kích hoạt nó lần đầu tiên, module system Scan cho rằng bạn muốn nó quét virus mỗi khi bạn làm việc với bất kỳ file nào dễ bị nhiễm virus, dù trên đĩa cứng hay đĩa mềm, và dù bạn đọc file hay ghi file vào đĩa cứng. Module cũng sẽ kiểm tra các file nén theo mặc định, nhưng sẽ không sử dụng tiến trình quét dò tìm trừ khi bạn kích hoạt nó.

Để thay đổi các tùy chọn cấu hình, hãy thực hiện các bước sau đây:

1. Xác nhận hộp kiểm Enable System Scan được chọn.

Việc chọn hộp kiểm này sẽ kích hoạt các tùy chọn còn lại trong trang đặc tính này. Hãy xóa chọn hộp kiểm này để tắt tất cả các tùy chọn cấu hình trong trang này và ngăn chặn module System Scan quét hệ thống của bạn.



2. Hãy cho module biết bạn muốn nó tìm virus vào lúc nào và ở đâu. Bạn có thể nhờ nó:

- ❖ Quét các file khi bạn làm việc với chúng, mỗi khi bạn mở, chạy, sao chép, rê, đặt lại tên, hay sử dụng các file trên đĩa cứng, mã virus có thể thực thi và lây lan sang các file khác. Để ngăn chặn điều này trên các máy tính đang chạy Windows NT Workstation v4.0 hoặc Windows 2000 Professional, hãy chọn cả hai hộp kiểm Inbound files và Outbound files. Trên các máy tính đang chạy Windows 95 hay Windows 98, hãy chọn mỗi hộp kiểm Run, Copy, Creat và Rename.

Ghi chú

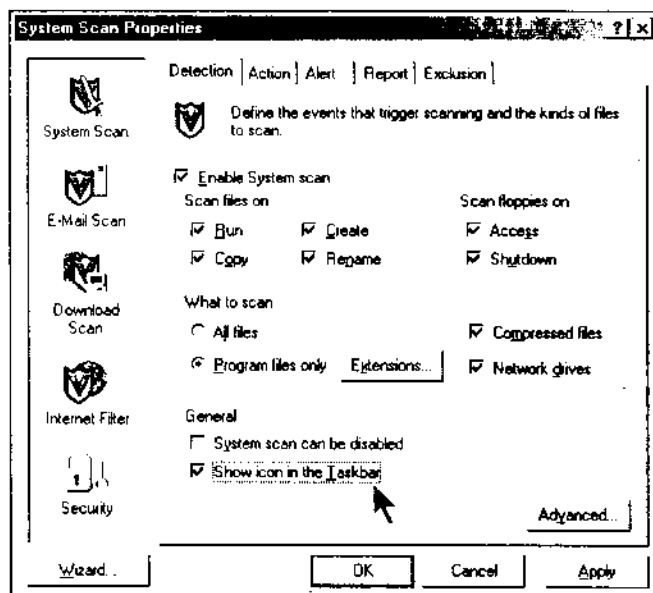
Nếu bạn có các ổ đĩa mạng được ánh xạ sang máy tính mà bạn sao chép các file từ đó, hoặc nếu những người sử dụng mạng khác sao chép các file từ máy tính của bạn, McAfee đề nghị bạn nên cài đặt VShield scanner trên cả máy tính của bạn và trên máy tính có ổ đĩa mạng. Bạn cũng nên chọn tất cả các hộp kiểm trong vùng Scan trong trang Detection, và hộp kiểm Network drives trong vùng What to Scan.

Sau đó, bản sao của module System Scan sẽ kiểm tra các file khi máy tính đọc chúng từ đĩa cứng, kiểm tra lại khi nó ghi chúng vào đĩa cứng của máy tính đích. Nếu máy tính đích có bản sao riêng của nó vì module System Scan đang hoạt động, nó cũng sẽ quét file khi bạn ghi nó vào ổ đĩa mạng nếu module System Scan đó có hộp kiểm Inbound files được chọn.

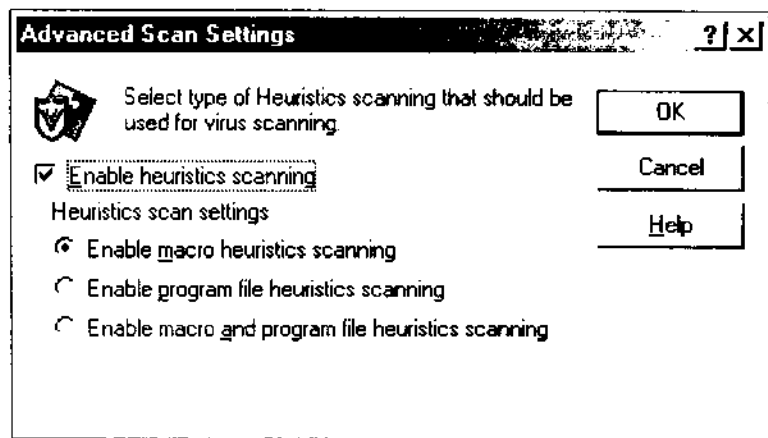
Nếu bạn dự định sao chép các file từ một server vốn không sao chép các file từ máy tính, và nếu những người sử dụng mạng khác cũng thực hiện điều này, bạn có thể cấu hình các máy tính để chúng quét chỉ các file mà chúng ghi vào các đĩa cứng - hoặc chỉ các file mà chúng đọc từ các đĩa cứng - để ngăn chặn việc hai máy tính quét cùng file. Tuy nhiên, nếu bạn thực hiện điều này, bạn nên cấu hình mỗi máy tính như nhau. Nếu không, một máy tính vốn chỉ quét các file đi có thể sao chép một file bị nhiễm từ một server vốn chỉ quét các file quét đến.

Quét các file trên các đĩa mềm. Các virus sector khởi động có thể ẩn trong các khối khởi động của bất kỳ đĩa mềm nào đã định dạng, sau đó xâm nhập vào bộ nhớ ngay khi máy tính của bạn đọc ổ đĩa mềm. Chọn hộp kiểm Access để nhờ module System Scan kiểm tra các đĩa mềm mỗi khi máy tính đọc hay ghi vào chúng. Chọn hộp kiểm Shutdown để nhờ module ghép bất kỳ đĩa mềm nào mà bạn để lại trong ổ đĩa khi bạn tắt máy tính. Điều này bảo đảm virus này có thể xâm nhập vào khi máy tính đọc ổ đĩa mềm vào lúc khởi động.

3. Chỉ định các kiểu file nào mà bạn muốn module System Scan kiểm tra
4. Chọn các tùy chọn quản lý VShield scanner. Các tùy chọn này cho phép bạn điều khiển sự tương tác với VShield scanner. Bạn có thể:
 - ❖ Tắt module System Scan vào bất kỳ lúc nào. Chọn hộp kiểm System Scan can be disabled để nhờ tùy chọn này tắt module. McAfee đề nghị bạn để mở module System Scan để đạt được sự bảo vệ tối đa. Việc xóa chọn hộp kiểm này sẽ xóa các hạng mục Exit và System Scan ra khỏi menu tắt VShield và nút Disable ra khỏi hộp thoại VShield Status.
 - ❖ Hiện thị biểu tượng VShield trong khay hệ thống Windows. Chọn hộp kiểm Show icon in the Taskbar để nhờ VShield scanner hiện thị biểu tượng này trong khay hệ thống. Việc nhấp đúp vào biểu tượng sẽ mở hộp thoại VShield Status. Việc nhấp phải vào biểu tượng sẽ hiện thị một menu tắt.



5. Bật tiến trình quét dò tìm. Nhấp Advanced để mở hộp thoại Advanced Scan Settings. Để tìm hiểu tiến trình quét dò tìm và cách kích hoạt nó.



6. Kế tiếp, bạn có thể:

- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại System Scan Properties.

- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút này để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại:

Action options

Alert options

Report

Exclusion

- ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại System Scan Properties.
- ❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.

Ghi chú

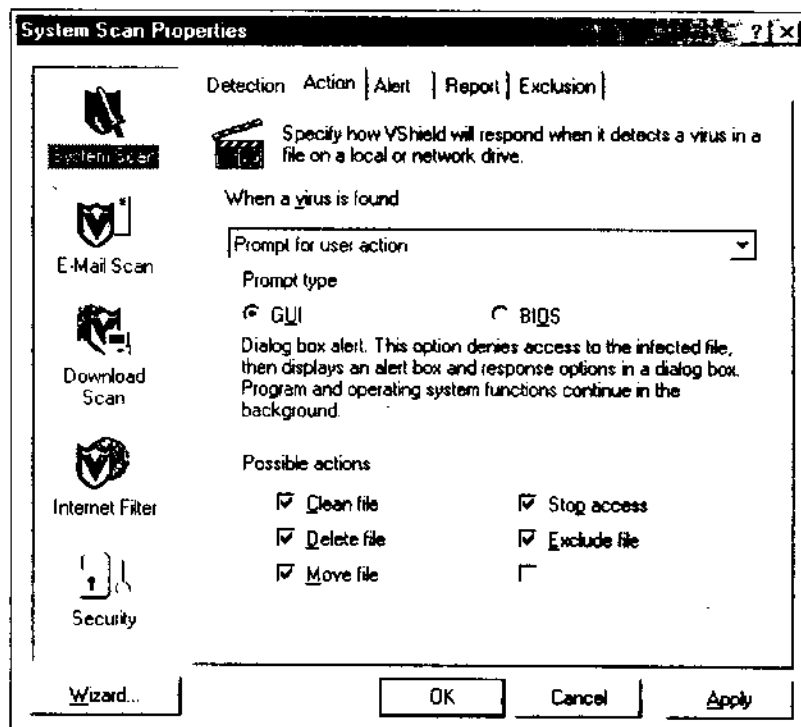
Việc nhấp Cancel sẽ không Undo bất kỳ thay đổi nào mà bạn đã lưu bằng cách nhấp Apply.

2. Chọn các tùy chọn Action dành cho module System Scan

Khi module System Scan dò tìm virus, nó có thể phản hồi bằng cách hỏi bạn nó cần thực hiện điều gì với file bị nhiễm, hoặc bằng cách tự động thực hiện hành động mà bạn đã xác định trước. Sử dụng trên đặc tính Action để chỉ định các tùy chọn phản hồi nào mà bạn muốn module cung cấp cho bạn khi nó tìm thấy một virus, hoặc cách hành động nào mà bạn muốn nó thực hiện.

Để thay đổi các tùy chọn cấu hình, hãy thực hiện các bước sau đây:

1. Chọn một trong các tùy chọn phản hồi sau đây từ danh sách When a virus is found.
 - ❖ Prompt for user action.
 - ❖ Move infected files automatically.
 - ❖ Clean infected files automatically.
 - ❖ Delete infected files automatically.
 - ❖ Deny access to infected files and continue.



2. Chọn một chế độ nhắc. Tùy chọn này chỉ có sẵn trên hệ thống đang chạy Windows 95 hay Windows 98. Với tùy chọn này, bạn có thể chỉ định loại thông tin cảnh báo mà bạn muốn module System Scan hiển thị khi nó tìm thấy một virus. Các tùy chọn của bạn là:

- ❖ BIOS. Nhấp vào nút này để xem một thông tin cảnh báo ở chế độ text chiếm toàn màn hình vốn cung cấp cho bạn một dãy các tùy chọn phản hồi, bao gồm cả tùy chọn để tiếp tục mà không thực hiện bất kỳ hành động nào để xử lý virus. Chế độ này cũng tạm ngưng hệ thống của bạn cho đến khi bạn chọn một tùy chọn phản hồi.
- ❖ GUI. Nhấp vào nút này để xem một thông tin cảnh báo chuẩn bằng đồ họa vốn cung cấp một dãy các tùy chọn phản hồi. dãy này sẽ không bao gồm Continue access. Khi dòng nhắc

nhắc bạn chọn, hệ thống vẫn tiếp tục với các hoạt động bình thường trong nền.

3. Kế tiếp, bạn có thể:

- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại System Scan Properties.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút này để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại:

Detection options

Alert options

Report

Exclusion

- ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại System Scan Properties.
- ❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.

Ghi chú

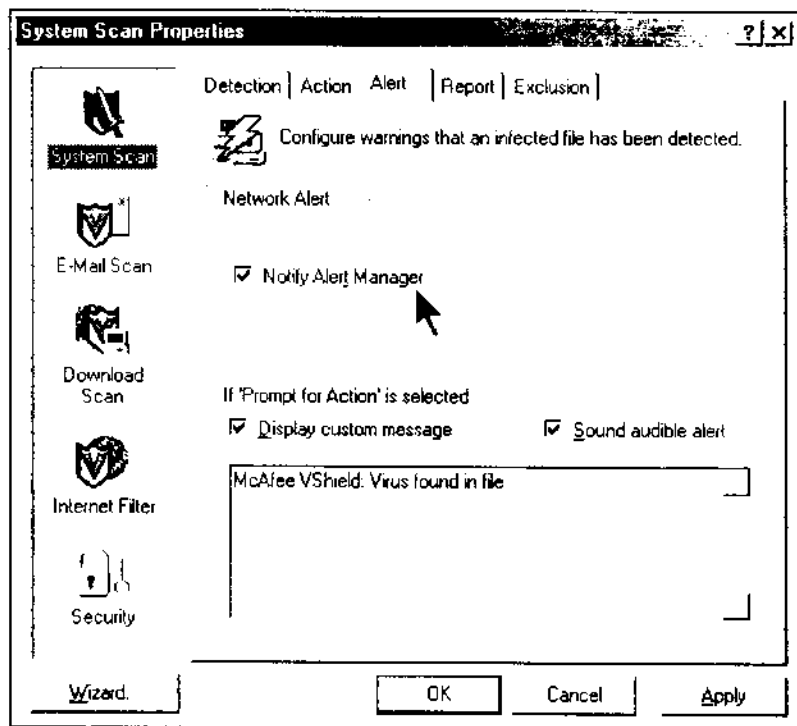
Việc nhấp Cancel sẽ không Undo bất kỳ thay đổi nào mà bạn đã lưu bằng cách nhấp Apply.

3. Chọn các tùy chọn Alert dành cho module System Scan

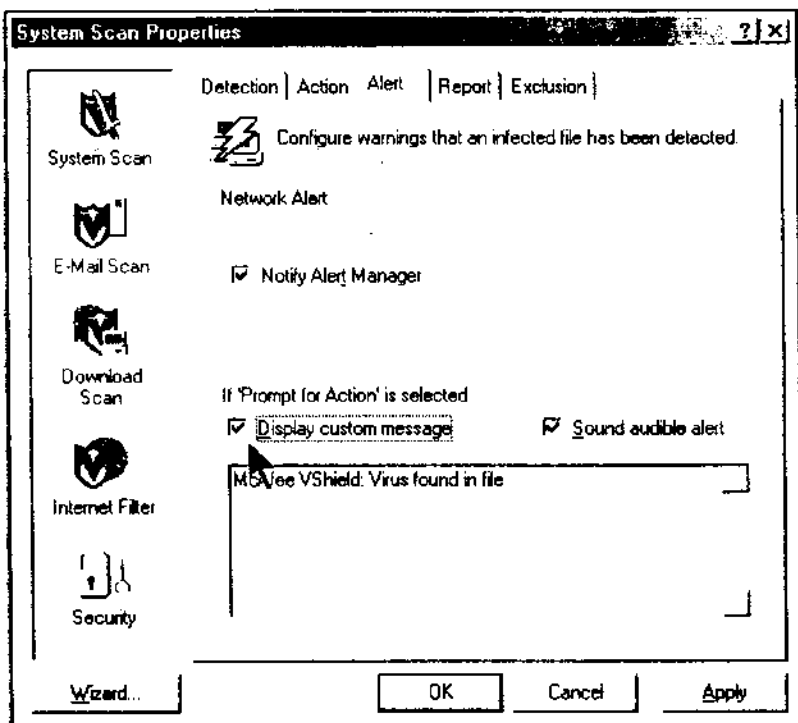
Ngay sau khi bạn cấu hình nó với các tùy chọn phản hồi mà bạn muốn trong trang Action, bạn có thể để cho module System Scan tìm và loại bỏ virus ra khỏi hệ thống một cách tự động khi nó tìm thấy chúng. Nhưng nếu bạn muốn module cho bạn biết ngay khi nó tìm thấy virus để bạn có thể thực hiện hành động thích hợp, hãy cấu hình để nó gửi một thông tin cảnh báo cho bạn hay cho những người khác.

Để thay đổi các tùy chọn cấu hình, hãy thực hiện các bước sau đây:

1. Chọn hộp kiểm Notify Alert Manager để nhờ module gửi các thông tin cảnh báo đến Alert Manager để phân phối.



2. Chọn hộp kiểm Shound audible alert để nhờ module phát ra tiếng bíp khi nó tìm thấy một file bị nhiễm.
3. Chọn hộp kiểm Display custom message để nhờ module bổ sung một thông báo tùy biến vào hộp alert mà nó hiển thị khi nó tìm thấy một file bị nhiễm.
4. Nhập thông báo mà bạn muốn module hiển thị trong hộp text được cho. Bạn có thể nhập tối đa đến 250 ký tự.



5. Kế tiếp, bạn có thể:

- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại System Scan Properties.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút này để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại:

Detection options

Action options

Report

Exclusion

- ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại System Scan Properties.
- ❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.

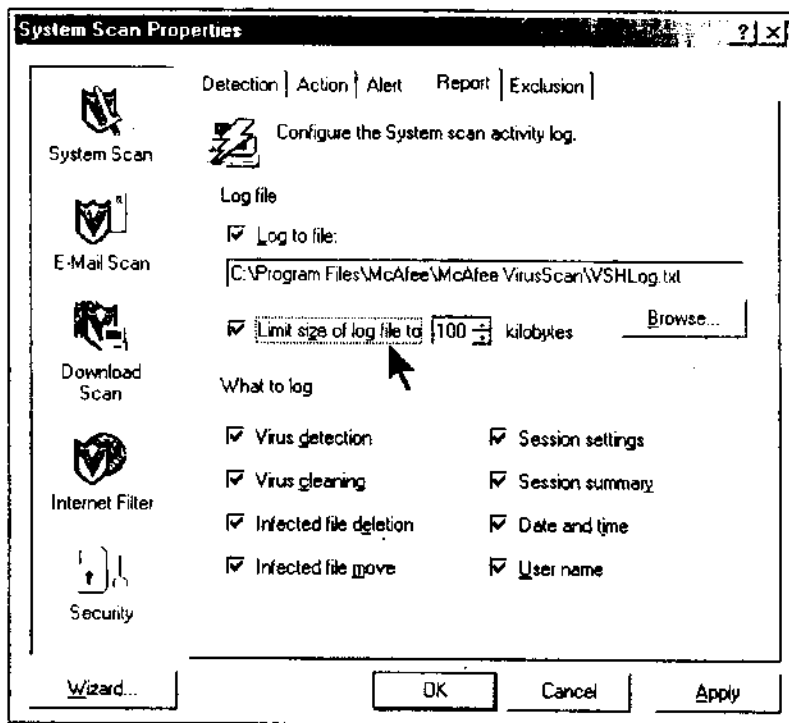
4. Chọn các tùy chọn Report dành cho module System Scan

Module System Scan liệt kê các xác lập hiện hành và tóm tắt tất cả các hành động mà nó thực hiện trong suốt mỗi tác vụ quét trong một log file được gọi là VSHLOG.TXT. Bạn có thể nhờ module ghi log vào file này, hoặc bạn có thể sử dụng bất kỳ bộ chỉnh sửa text nào để tạo một file text sau đó sử dụng. Sau đó bạn có thể mở và in log file để xem lại.

File VSHLOG.TXT có thể là một công cụ quản lý quan trọng giúp bạn thay đổi virus trên hệ thống và chú ý các xác lập nào mà bạn đã sử dụng để dò tìm và phản hồi các file bị nhiễm mà module System Scan đã tìm thấy. Bạn cũng có thể sử dụng các báo cáo về sự cố được ghi trong file để xác định những file nào mà bạn cần thay thế từ các bản sao lưu dự phòng, kiểm tra hay xóa khỏi máy tính.

Để quyết định module sẽ ghi lại dữ liệu nào và kích cỡ của log file là bao nhiêu, hãy thực hiện các bước sau đây:

1. Chọn hộp kiểm Log to file.
2. Chọn hộp kiểm Limit size of log file to để giảm thiểu kích cỡ của log file. Nếu bạn không chọn hộp kiểm này, log file có thể tăng đến kích cỡ mà khoảng trống đĩa hay hệ thống file của bạn cho phép.
3. Nhập một giá trị dành cho kích cỡ file, theo đơn vị kilobyte, vào hộp text được cho.
4. Chọn các hộp kiểm tương ứng với thông tin mà bạn muốn ghi lại.



5. Kế tiếp, bạn có thể:

- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại System Scan Properties.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút này để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại:

Detection options

Action options

Report

Exclusion

- ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại System Scan Properties.
- ❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.

5. Chọn các tùy chọn Exclusion dành cho module System Scan

Ngay sau khi bạn sử dụng phần mềm VirusScan để quét hệ thống, bạn có thể yêu cầu module System Scan bỏ qua các file và các folder không thay đổi hoặc thường không thể bị nhiễm virus.

Để thực hiện điều này, hãy thực hiện các bước sau đây:

1. Nhấp Add để loại ra một hạng mục mới.

Thao tác này sẽ mở hộp thoại Add Exclude Item. Để tìm hiểu cách chỉ định các hạng mục mà bạn muốn loại ra trong suốt các tốc độ quét, hãy nhấp [here](#):

2. Chọn một trong các hạng mục hiển thị, sau đó nhấp Edit để thay đổi định nghĩa hạng mục.

Thao tác này sẽ mở hộp thoại Edit Exclude Item. Thực hiện các thay đổi cần thiết, sau đó nhấp OK để đóng hộp thoại.

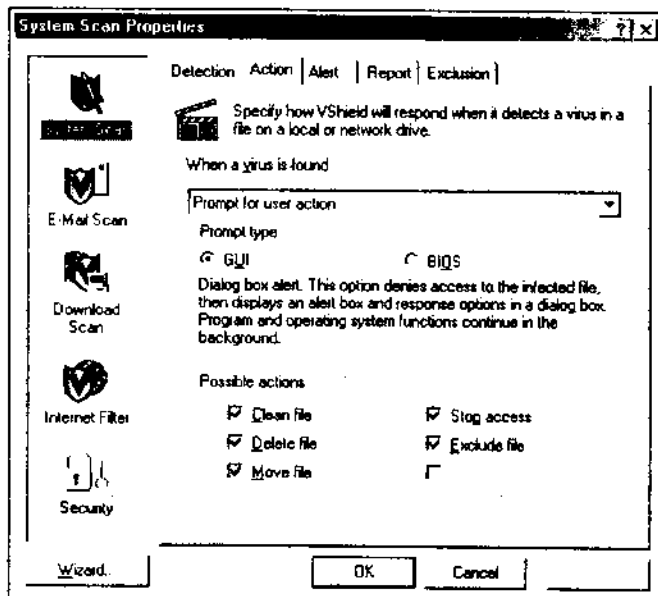
3. Chọn một trong các hạng mục hiển thị, sau đó nhấp Remove để xóa một hạng mục ra khỏi danh sách. Điều này có nghĩa là module System Scan sẽ quét hạng mục trong suốt tác vụ quét này.

4. Kế tiếp, bạn có thể:

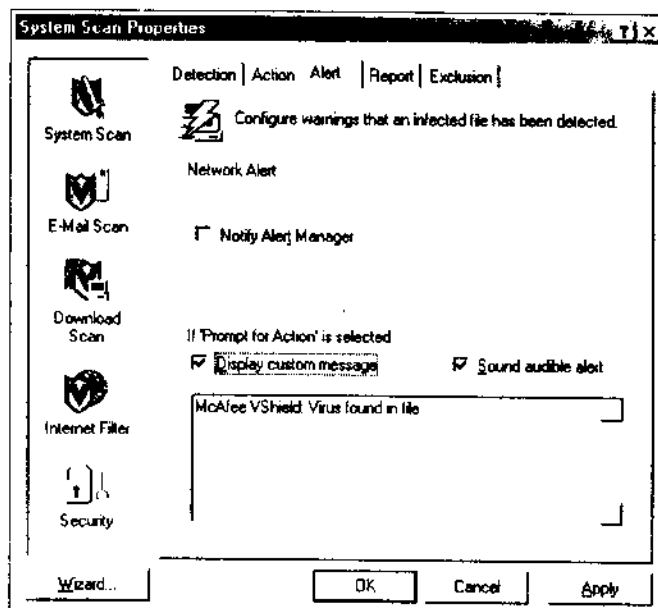
- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại System Scan Properties.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ các nút sau đây để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại:

Detection options

Action options

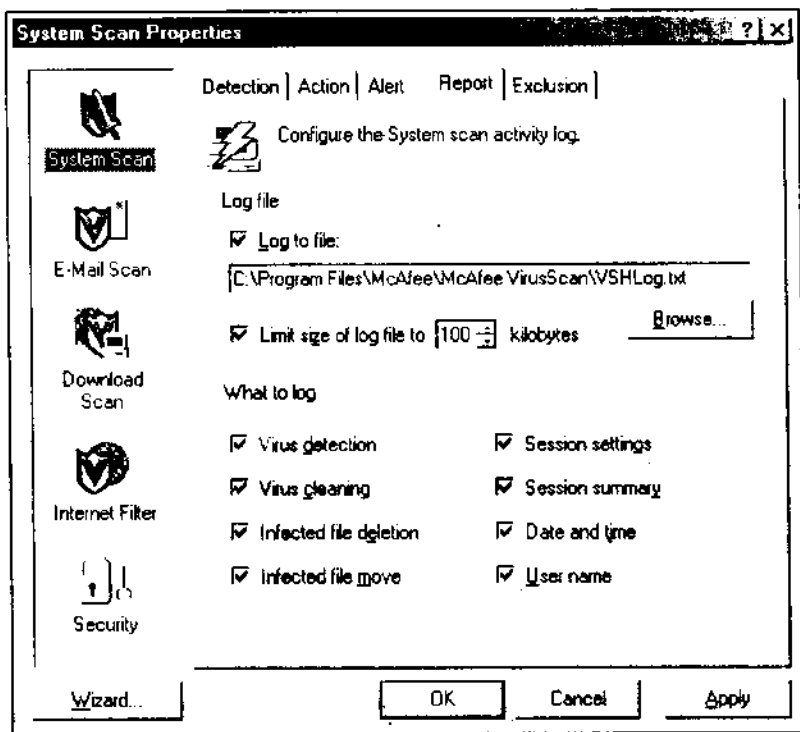


Alert options



Report

- ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại System Scan Properties.



- ❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.

XI. Cấu hình module E-Mail Scan

Module VShield E-mail Scan tìm virus trong các file đính kèm với các thông báo e-mail mà bạn nhận được thông qua các hệ thống e-mail của công ty theo tiêu chuẩn MAPI (Messaging Application Programming Interface), chẳng hạn như Microsoft Exchange, Microsoft Outlook, hay các phiên bản sau này của Lotus cc:Mail. Nó cũng có một chế độ quét đặc biệt để tìm virus trong các phiên bản cc:Mail trước đây.

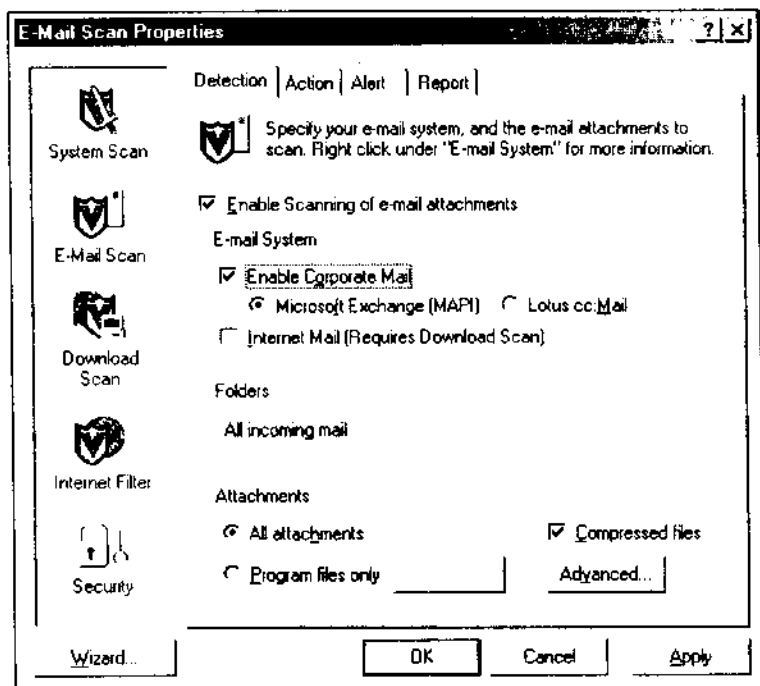
Module này có thể hoạt động kết hợp với module Download Scan để kiểm tra các thông báo đến thông qua các chương trình e-mail client POP-3 hoặc SMTP chẳng hạn như Eudora, Netscape Mail, hay Microsoft Outlook Express. Module này đặc biệt chú ý đến các file đính kèm với e-mail, là nơi tiềm ẩn nhiều virus nhất. Bởi vì nó có thể quét e-mail ngay sau khi nó xuất hiện trên màn hình nên module có thể ngăn chặn virus trước khi chúng có cơ hội lây lan.

Khi nó tìm thấy virus, module có thể hỏi bạn muốn nó thực hiện điều gì, hoặc nó có thể thực hiện nhiều hành động tự động để phản hồi. Bạn có thể nhờ nó báo cáo những gì mà nó đã thực hiện bằng một thông tin cảnh báo khi nó thực hiện hành động hoặc bằng một log file mà bạn có thể kiểm tra khi bạn có thời gian rảnh. Thậm chí nó có thể gửi một thông báo đến người đã gửi một thông báo e-mail đã nhiễm virus, giúp cho việc theo dõi nguồn gốc lây nhiễm virus trở nên tương đối đơn giản.

Để chọn các tùy chọn, hãy nhấp vào biểu tượng E-Mail Scan ở phía bên trái của hộp thoại System Scan Properties để hiển thị các trang đặc tính dành cho module này.

Ghi chú

Biểu tượng E-Mail Scan sẽ không xuất hiện ở đây trừ khi bạn đã sử dụng tùy chọn Custom Setup khi bạn đã cài đặt phần mềm VirusScan và đã chỉ định rằng bạn muốn cài đặt module E-Mail Scan. Theo mặc định, VShield scanner không bật module E-Mail Scan khi nó khởi động lần đầu tiên - bạn phải cho module biết những hệ thống e-mail nào mà bạn sử dụng trước khi nó có thể kích hoạt.



Kế tiếp, hãy nhấp vào các nút được liệt kê phía dưới để tìm hiểu cách chọn các tùy chọn dành cho mỗi trang đặc tính:

Detection

Action

Alert

Report

1. Chọn các tùy chọn Detection dành cho module E-Mail Scan

VShield scanner không khởi động với module E-Mail Scan được bật theo mặc định bởi vì nó cần biết bạn sử dụng hệ thống e-mail nào. Ngay sau khi bạn cấu hình nó để sử dụng với e-mail client của bạn, module sẽ sử dụng profile MAPI, hoặc user name và password cc:Mail, để nối với mail account bất kỳ khi nào nó khởi động một tác vụ quét.

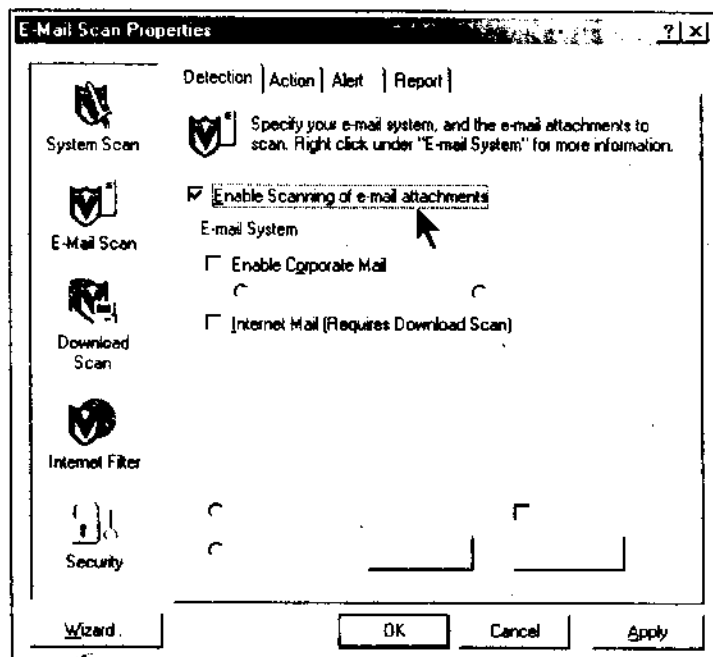
Nếu bạn đã khởi động vào hệ thống e-mail, module sẽ làm việc trong tác vụ mà bạn đã tạo. Tuy nhiên, nếu bạn chưa vào hệ thống e-mail, module sẽ nhắc bạn chọn một profile hoặc nhập một thông tin account ngay sau khi một tác vụ quét khởi động, ngay trước khi bạn vào e-mail account. Điều này cũng có thể xảy ra khi bạn khởi động máy tính, nếu bạn không xác lập chương trình e-mail client để nó tải vào lúc khởi động.

Nếu bạn chuyển đổi profile hoặc log vào một account khác - có thể trong một domain khác - module sẽ yêu cầu bạn chọn profile mà bạn muốn sử dụng hoặc cung cấp một user name và password mới để nối kết với hệ thống mail.

Để chọn các tùy chọn cấu hình cho trang này, hãy thực hiện các bước sau đây:

1. Chọn hộp kiểm Enable Scanning of e-mail attachments

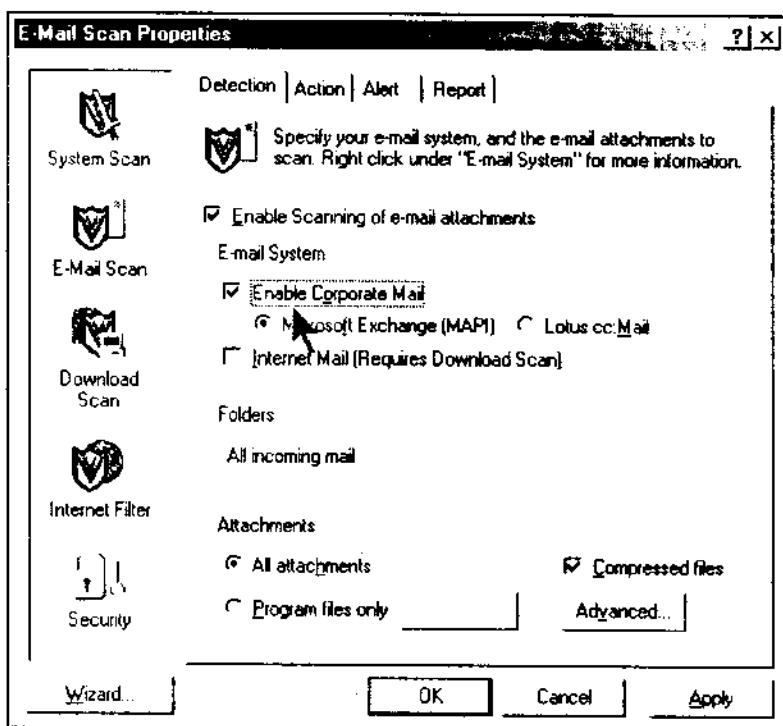
Các tùy chọn còn lại trong phần của trang đặc tính sẽ kích hoạt.



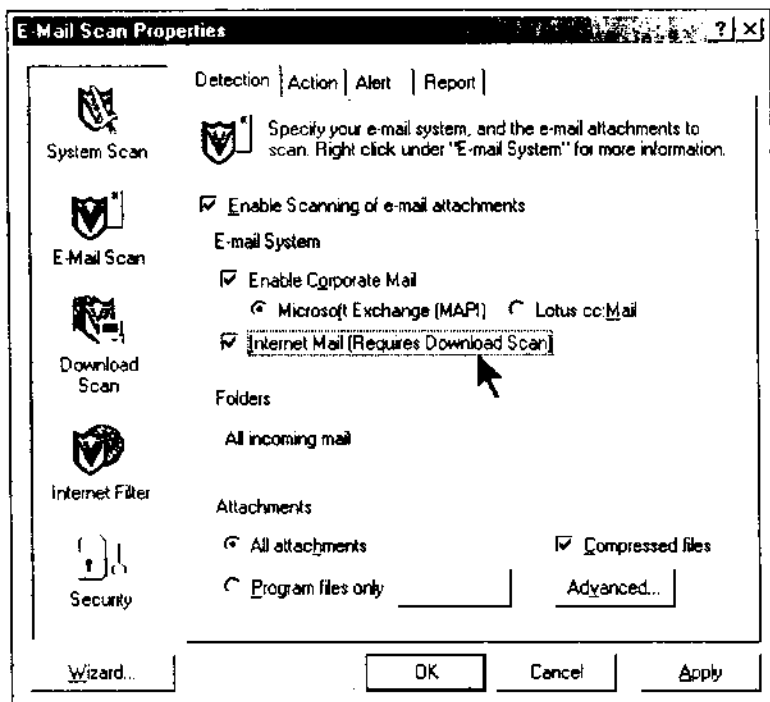
2. Chọn loại hệ thống e-mail mà bạn sử dụng. Các tùy chọn bao gồm:

❖ **Enable Corporate Mail.** Chọn hộp kiểm này để nhờ module E-Mail Scan quét các file đính kèm mà bạn nhận được thông qua một hệ thống mail đang chạy trong mạng văn phòng của bạn. Thông thường những hệ thống như thế này sử dụng một giao thức mail độc quyền và có một mail server chính để bạn gửi mail đến đó. Những hệ thống này thường gửi và nhận Internet mail, nhưng chúng thì thực hiện điều này thông qua một trình ứng dụng cổng. Module E-Mail Scan hỗ trợ hai loại hệ thống e-mail công ty:

- Microsoft Exchange (MAPI).
- Lotus cc:Mail.



- ❖ **Internet Mail (Requires Download Scan).** Chọn hộp kiểm này để nhờ module E-Mail Scan quét các file đính kèm Internet mail mà bạn gửi và nhận thông qua Post Office Protocol (POP-3) hoặc Simple Mail Transfer Protocol (SMTP). Chọn tùy chọn này nếu bạn đang làm việc tại nhà hoặc thông qua một nhà cung cấp dịch vụ Internet với phần mềm chẳng hạn như Eudora Pro của Qualcomm, Outlook Express của Microsoft, hoặc Netscape Mail.

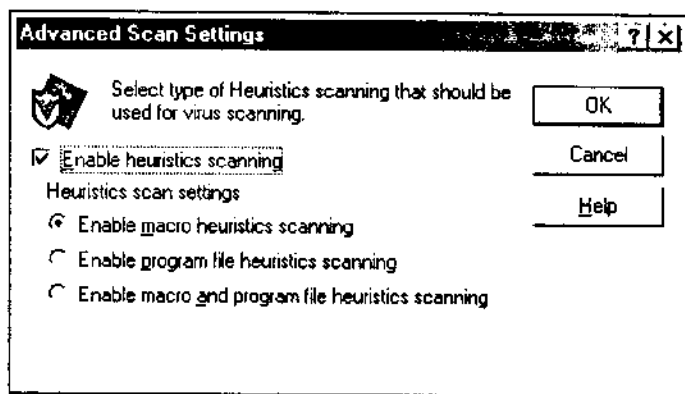


3. Thông báo cho module E-Mail Scan biết nó phải giám sát những nguồn mail nào. Các tùy chọn bao gồm:
 - ❖ Nếu bạn đã chọn Microsoft Exchange (MAPI) làm hệ thống e-mail của công ty, Folder sẽ hiển thị All incoming mail, điều này có nghĩa là module sẽ tìm virus trong các file đính kèm của mỗi thông báo e-mail khi nó đến hộp thư MAPI hoặc qua các dịch vụ MAPI khác.

- ❖ Nếu bạn đã chọn Lotus cc: Mail là hệ thống e-mail của công ty, bạn sẽ cần cho module biết nó phải quét cc:Mail Inbox thường xuyên như thế nào.

Trong vùng Folder, hãy nhập số giây mà module E-Mail Scan phải chờ trước khi nó kiểm tra cc: Mail Inbox để tìm mail mới. Theo mặc định, module kiểm tra mỗi phút một lần. Nhớ xác lập một thời khoảng ngắn hơn thời khoảng mà bạn đã xác lập để nhận e-mail để module có cơ hội dò tìm virus trước khi chúng xâm nhập vào máy tính.

4. Chỉ định các file đính kèm e-mail mà bạn muốn module E-Mail Scan kiểm tra.
5. Bật tiến trình quét dò tìm. Nhấp Advanced để mở hộp thoại Advanced Scan Settings.



6. Kế tiếp, bạn có thể:

- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không cần phải đóng hộp thoại E-Mail Scan Properties.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ các nút sau đây để tìm hiểu cách cấu hình trong các trang bảng tính còn lại.

Detection

Action

Alert

Report

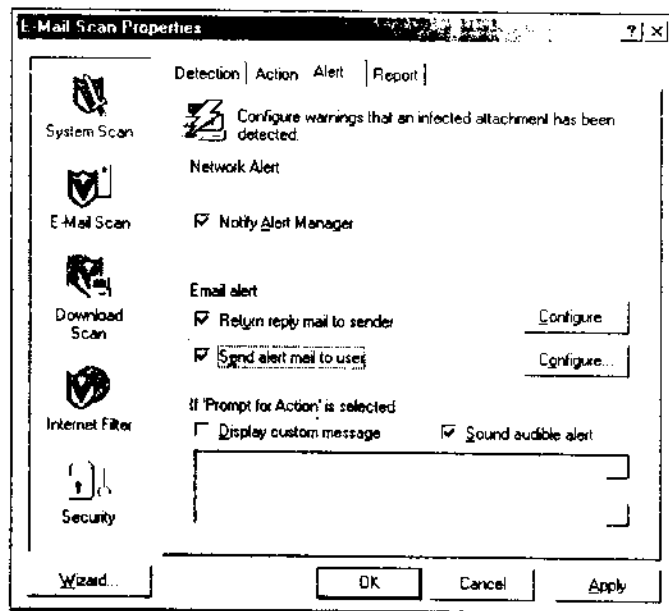
- ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại E-Mail Scan Properties.
- ❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.

2. Chọn các tùy chọn Action dành cho module E-Mail Scan

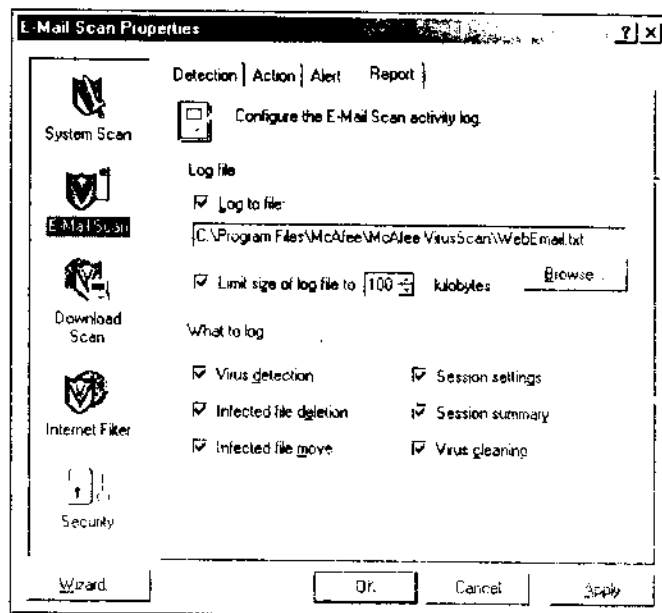
Module E-Mail Scan phản hồi các virus, chỉ khi bạn chọn một hệ thống e-mail của công ty để nó quét. Nếu bạn chọn chỉ Internet mail, các tùy chọn ở đây sẽ không có sẵn. Nếu bạn chỉ nhận Internet mail, bạn phải chọn các tùy chọn phản hồi trong bảng tính Action dành cho module Download Scan.

Để thay đổi các tùy chọn cấu hình, hãy thực hiện các bước sau đây:

1. Chọn một trong các tùy chọn phản hồi sau đây từ danh sách When a virus is found:
 - ❖ Prompt for user action.
 - ❖ Move infected files to a folder.
 - ❖ Clean infected files.
 - ❖ Delete infected files.
 - ❖ Continue scanning.
2. Kế tiếp, bạn có thể:
 - ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại E-Mail Scan Properties.
 - ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào trong bất kỳ các nút sau đây để tìm hiểu cách cấu hình các tùy chọn trong các trang bảng tính còn lại:
 - Detection
 - Alert



Report

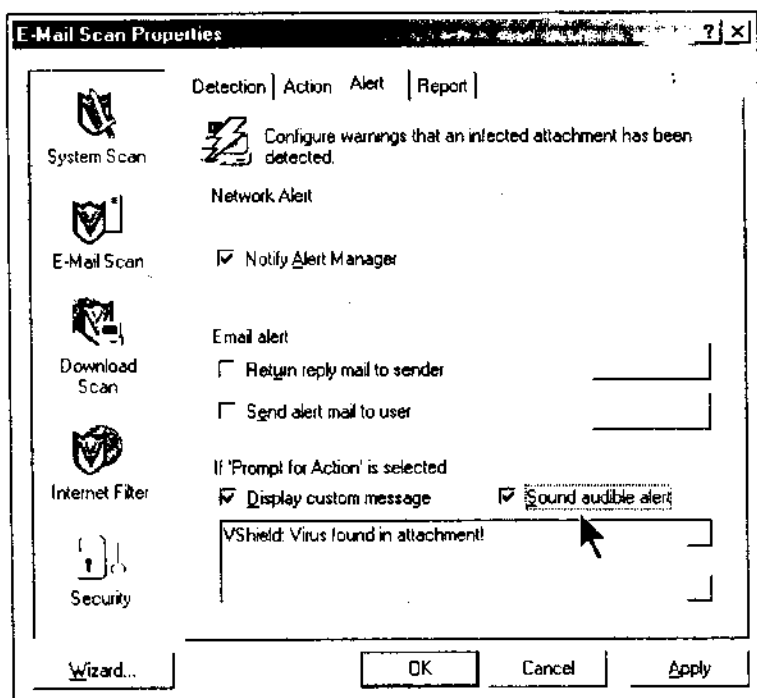


- ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại E-Mail Scan Properties.
- ❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.

3. Chọn các tùy chọn Alert dành cho module E-Mail Scan

Để thay đổi các tùy chọn cấu hình, hãy thực hiện các bước sau:

1. Chọn hộp kiểm Notify Alert Manager để mở module gửi các thông tin cảnh báo đến Alert Manager để phân phối.
2. Để gửi thông tin qua thông báo e-mail cho người đã gửi file đính kèm e-mail bị nhiễm hoặc đến những người nhận khác, hãy chọn một hoặc cả hai hộp kiểm trong vùng Email Alert, sau đó nhấp nút Configure tương ứng để soạn một thông báo cần gửi.
3. Chọn hộp kiểm Sound audible alert để nhờ module phát ra tiếng beep khi nó tìm thấy một file bị nhiễm.



4. Chọn hộp kiểm Display custom message để nhờ module bổ sung một thông báo tùy biến vào hộp alert mà nó hiển thị khi nó tìm thấy một file bị nhiễm.
5. Nhập thông báo mà bạn muốn module hiển thị vào một text được cho. Bạn có thể nhập tối đa đến 250 ký tự.
6. Kế tiếp, bạn có thể:
 - ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại E-Mail Scan Properties.
 - ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các tùy chọn sau đây để tìm hiểu cách cấu hình các tùy chọn trong các trang bảng tính còn lại:

Detection

Action

Report

- ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại E-Mail Scan Properties.
- ❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.

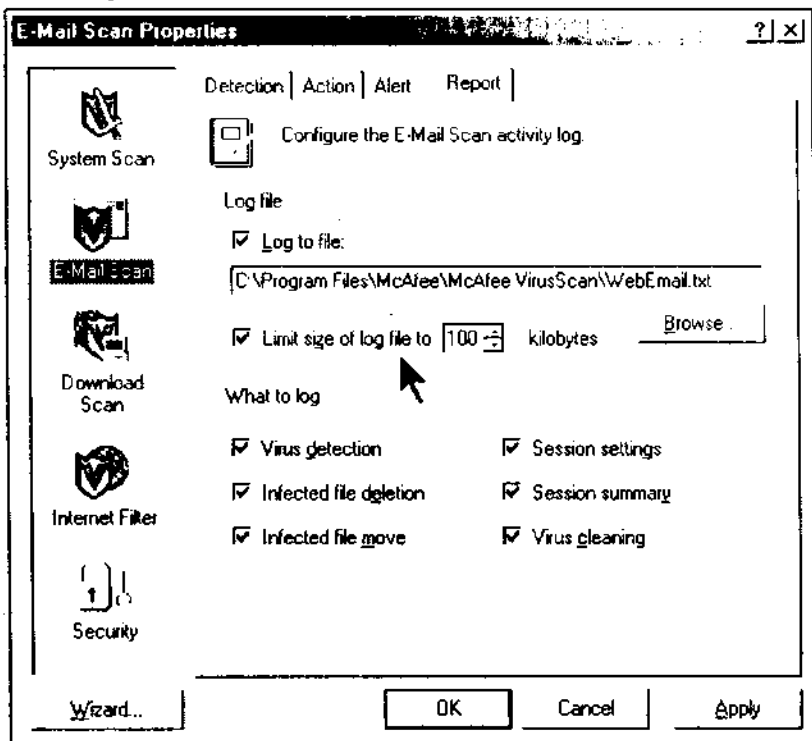
4. Chọn các tùy chọn Report dành cho module E-Mail Scan

Module E-Mail Scan liệt kê các xác lập hiện hành và tóm tắt tất cả các hành động mà nó thực hiện trong suốt mỗi tác vụ quét trong một lúc file được gọi là WEBEMAIL.TXT. Bạn có thể nhờ module ghi log của nó vào file này, hoặc bạn có thể sử dụng bất kỳ bộ chỉnh sửa text nào để tạo một file text cho nó sử dụng. Sau đó bạn có thể mở và in log file để xem lại.

Để quyết định module sẽ ghi lại dữ liệu nào và kích cỡ của log file là bao nhiêu, hãy thực hiện các bước sau đây:

1. Chọn hộp kiểm Log to file.
2. Chọn hộp kiểm Limit size of log file to để giảm thiểu kích cỡ của log file. Nếu bạn không chọn hộp kiểm này, log file có thể tăng đến kích cỡ mà khoảng trống đĩa hay hệ thống file của bạn cho phép.

3. Nhập một giá trị cho kích cỡ file, theo đơn vị kilobyte, vào hộp text được cho.



4. Chọn các hộp kiểm tương ứng với thông tin mà bạn muốn module ghi lại.
5. Kế tiếp, bạn có thể:
- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại E-Mail Scan Properties.
 - ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút sau đây để tìm hiểu các cấu hình các tùy chọn trong các trang đặc tính còn lại:

Detection

Action

Alert

- ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại E-Mail Scan Properties.
- ❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.

XII. Cấu hình module Download Scan

Module Download Scan có thể kiểm tra các file mà bạn tải xuống từ Internet khi bạn xem các website, các site FTP, và các site Internet khác. Module này cũng là nơi bạn xác lập các tùy chọn cần thiết để phản hồi các file đính kèm e-mail để diệt virus mà bạn nhận được qua các chương trình e-mail client POP-3 hoặc SMTP chẳng hạn như Eudora, Netscape Mail, hay Microsoft Outlook Express. Để kích hoạt chức năng này, bạn cũng phải chọn hộp kiểm Internet Mail trong trang Detection của module E-Mail Scan.

Khi nó tìm thấy một virus, module có thể hỏi bạn muốn nó thực hiện điều gì, hoặc nó có thể thực hiện nhiều hành động tự động để phản hồi. Bạn có thể nhờ nó báo cáo về những gì mà nó đã thực hiện bằng một thông tin cảnh báo khi nó thực hiện hành động hoặc bằng một log file mà bạn có thể xem xét khi bạn có thời gian rảnh. Thậm chí nó có thể gửi một thông báo đến người đã gửi thông báo e-mail bị nhiễm, giúp cho việc theo dõi nguồn gốc lây nhiễm virus trở nên tương đối đơn giản.

Để chọn các tùy chọn, hãy nhấp biểu tượng Download Scan ở phía bên trái của hộp thoại E-Mail Scan Properties để hiển thị các trang đặc tính dành cho module này.

Ghi chú

Biểu tượng Download Scan sẽ không xuất hiện ở đây trừ khi bạn đã sử dụng tùy chọn Custom Setup để cài đặt phần mềm VirusScan và đã chỉ định rằng bạn muốn cài đặt module Download Scan.

Kế tiếp, hãy nhấp vào các nút được liệt kê ở phía dưới để tìm hiểu cách chọn các tùy chọn dành cho mỗi trang đặc tính:

Detection

Action

Alert

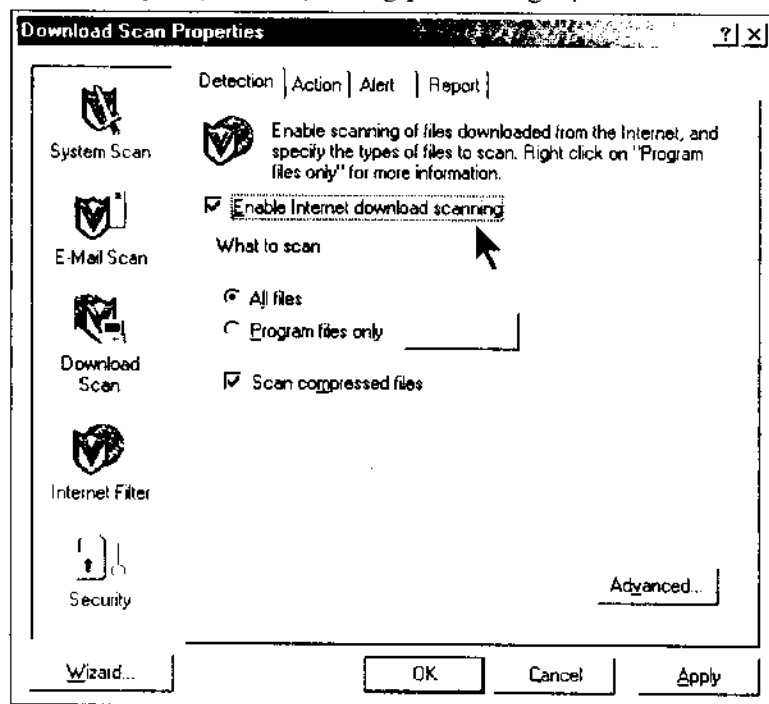
Report

1. Chọn các tùy chọn Detection dành cho module Download Scan

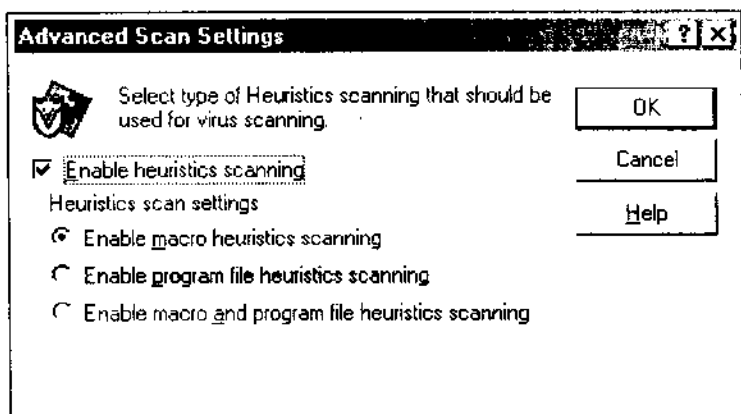
Để chọn các tùy chọn cấu hình dành cho trang này, thực hiện các bước sau đây:

1. Chọn hộp kiểm Enable Internet download scanning.

Các tùy chọn còn lại trong phần trang đặc tính sẽ kích hoạt.



2. Chỉ định các kiểu file mà bạn muốn module Download Scan kiểm tra.
3. Bật tiến trình quét dò tìm. Nhấp Advanced để mở hộp thoại Advanced Settings.



4. Kế tiếp, bạn có thể:

- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại Download Scan Properties.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào một trong các nút sau đây để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại:

Action

Alert

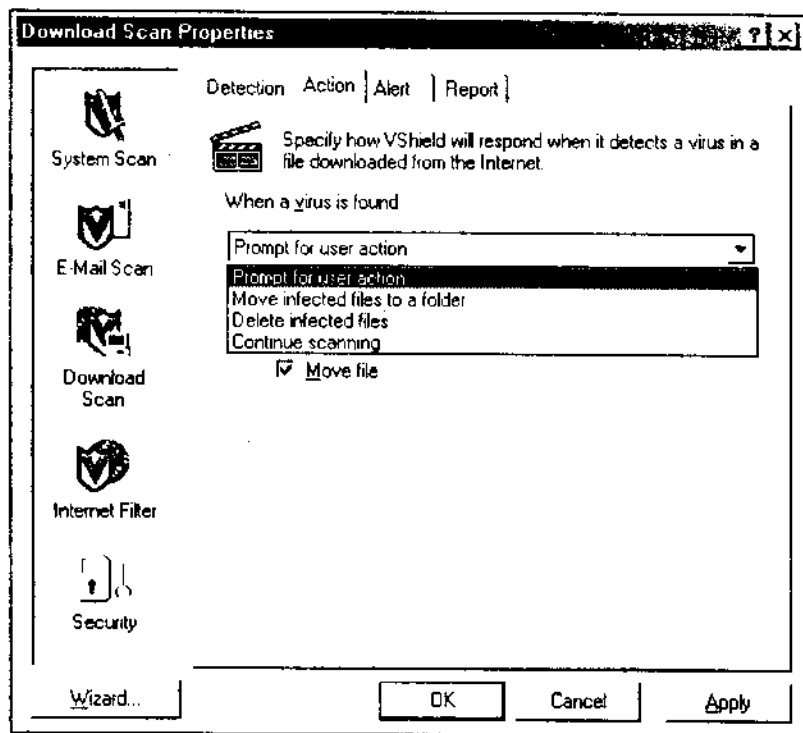
Report

- ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại Download Scan Properties.
- ❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.

2. Chọn các tùy chọn Action dành cho module Download Scan

Để thay đổi các tùy chọn cấu hình, thực hiện các bước sau đây:

1. Chọn một trong các tùy chọn phản hồi sau đây từ danh sách When a virus is found.
 - ❖ Prompt for user action.
 - ❖ Move infected files to a folder.
 - ❖ Delete infected files.
 - ❖ Continue scanning.



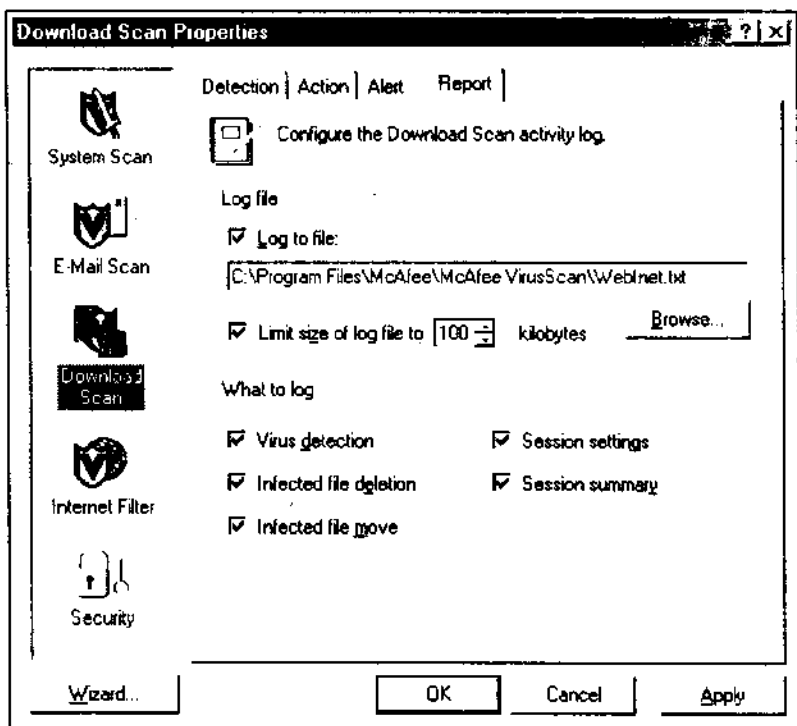
2. Kế tiếp, bạn có thể:

- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không cần đóng hộp thoại Download Scan Properties.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút sau đây để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại:

Detection

Alert

Report



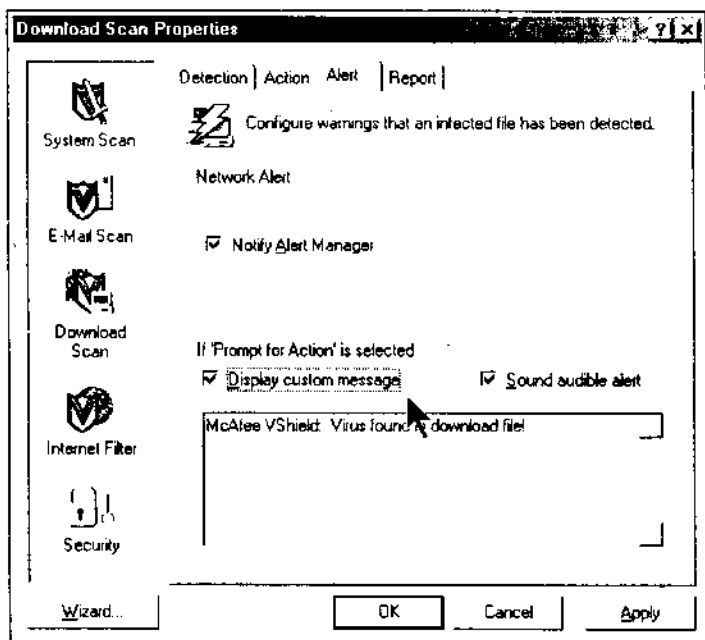
❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại Download Scan Properties.

❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.

3. Chọn các tùy chọn Alert dành cho module Download Scan

Để thay đổi các tùy chọn cấu hình, thực hiện các bước sau đây:

1. Chọn hộp kiểm Notify Alert Manager để nhờ module gửi các thông tin cảnh báo đến Alert Manager để phân phối.
2. Chọn hộp kiểm Sound audible alert để nhờ module phát ra tiếng beep khi nó tìm thấy một file bị nhiễm.
3. Chọn hộp kiểm Display custom message để nhờ module bổ sung một thông báo tùy biến vào hộp alert mà nó hiển thị khi nó tìm thấy file bị nhiễm.



4. Nhập thông báo mà bạn muốn module hiển thị trong hộp text được cho. Bạn có thể nhập tối đa đến 250 ký tự.
5. Kế tiếp, bạn có thể:
 - ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại Download Scan Properties.
 - ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút này để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại.

Detection

Action

Report

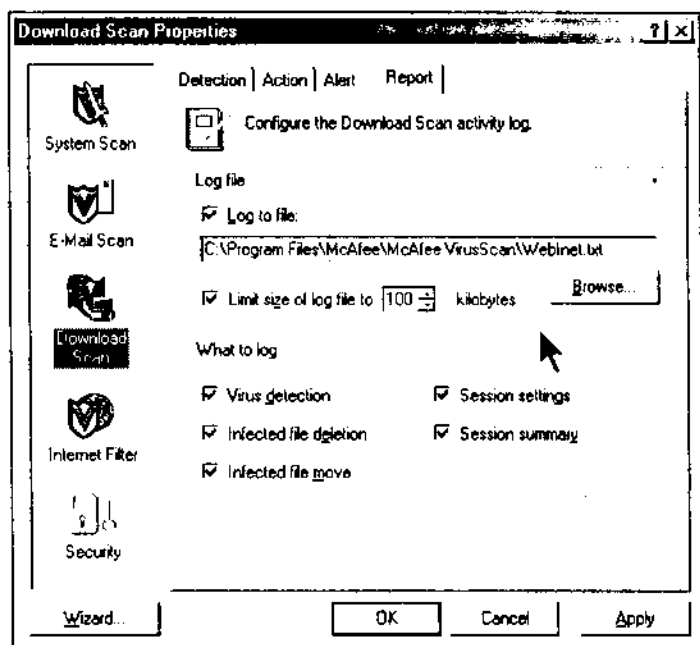
- ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại Download Scan Properties.
- ❖ Nhấp Scancel để đóng hộp thoại mà không lưu các thay đổi.

4. Chọn các tùy chọn Report dành cho module Download Scan

Module Download Scan liệt kê các xác lập hiện hành và tóm tắt tất cả các hành động mà nó thực hiện trong suốt mỗi tác vụ quét cho một log file được gọi là WEBINET.TXT. Bạn có thể nhờ module ghi log của nó vào file này, hoặc bạn có thể chỉnh sửa bất kỳ bộ chỉnh sửa text nào để tạo một file text cho nó sử dụng. Sau đó bạn có thể mở và in log file để xem lại.

Để quyết định module sẽ ghi lại dữ liệu nào và kích cỡ của log file là bao nhiêu, hãy thực hiện các bước sau đây:

1. Chọn hộp kiểm Log to file.
2. Chọn hộp kiểm Limit size of log file to để giảm thiểu kích cỡ của log file. Nếu bạn không chọn hộp kiểm này, log file có thể tăng đến kích cỡ mà khoảng trống đĩa và hệ thống file của bạn cho phép.
3. Nhập một giá trị cho kích cỡ file, theo đơn vị kilobyte, vào hộp text được cho.



4. Chọn các hộp kiểm tương ứng với thông tin mà bạn muốn module ghi lại.
5. Kế tiếp, bạn có thể:
 - ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không đóng hộp thoại Download Scan Properties.
 - ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút sau đây để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại:

Detection

Actuion

Alert
 - ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại Download Scan Properties.
 - ❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.

XIII. Cấu hình module Internet Filter

Module Internet Filter cung cấp một phương pháp hiện hữu hơn. Nó sử dụng một cơ sở dữ liệu cập nhật gồm các đối tượng đã được xác định là gây hư hại cho các lớp Java và các ActiveX control mà bạn gặp khi trình duyệt.

Khi nó tìm thấy một virus, module có thể hỏi bạn muốn nó thực hiện điều gì, hoặc nó có thể ngăn chặn đối tượng hay site nguy hiểm một cách tự động. Bạn có thể nhờ nó báo cáo những gì mà nó đã thực hiện bằng một thông tin cảnh báo khi nó thực hiện hành động hoặc bằng một log file mà bạn có thể xem xét khi bạn có thời gian rảnh.

Để chọn các tùy chọn, hãy nhấp vào biểu tượng Internet Filter ở phía bên trái của hộp thoại Download Scan Properties để hiển thị các trang đặc tính dành cho module này.

Ghi chú

Biểu tượng Internet Filter sẽ không xuất hiện ở đây trừ khi bạn đã sử dụng tùy chọn Custom Setup để cài đặt phần mềm VirusScan và đã chỉ định rằng bạn muốn cài đặt module Internet Filter.

Kế tiếp, hãy nhấp vào các nút được liệt kê ở phía dưới để tìm hiểu cách chọn các tùy chọn dành cho mỗi trang đặc tính:

Detection

Action

Alert

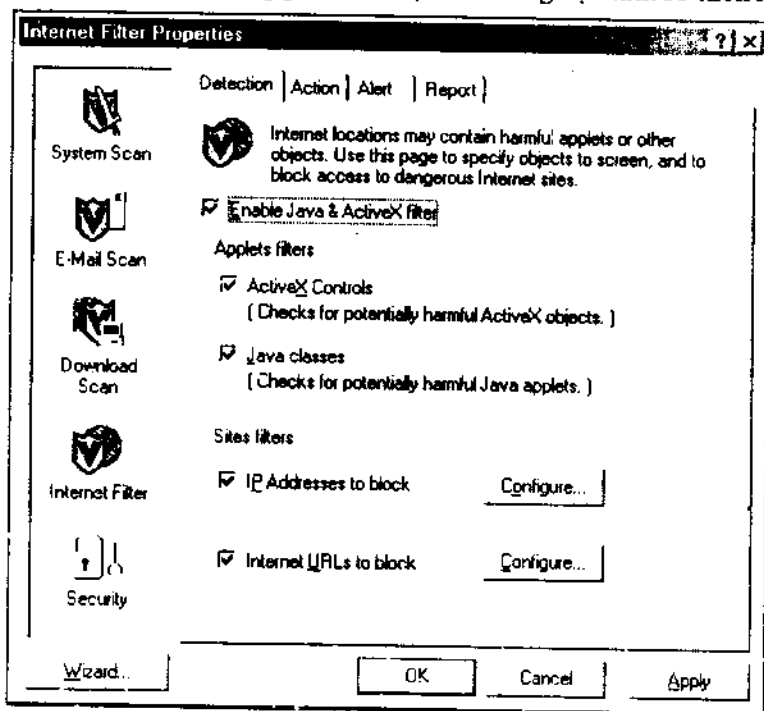
Report

1. Chọn các tùy chọn Detection dành cho module Internet Filter

Để thay đổi các tùy chọn cấu hình, hãy thực hiện các bước sau đây:

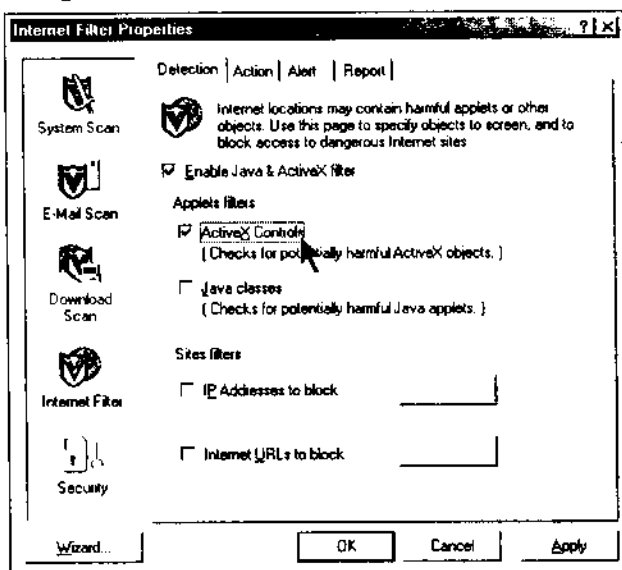
1. Chọn hộp kiểm Enable Java & ActiveX Filter.

Các tùy chọn trong phần còn lại của trang đặc tính sẽ kích hoạt.

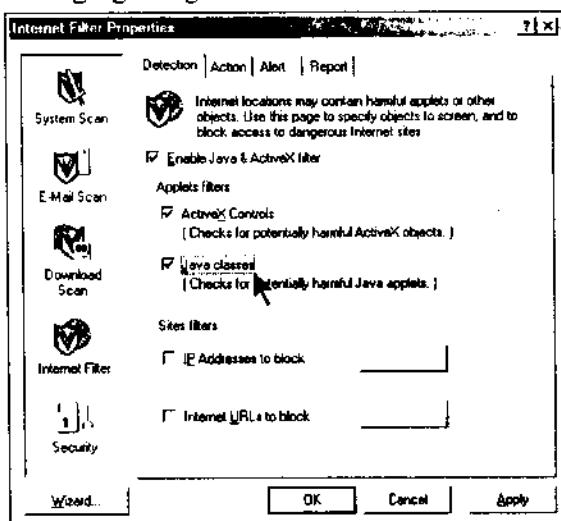


2. Chỉ định các đối tượng nào mà bạn muốn module Internet Filter để kiểm tra. Các tùy chọn bao gồm:

- ❖ **ActiveX Control.** Chọn một hộp kiểm này để nhờ module tìm và ngăn chặn các control ActiveX hoặc OCX nguy hiểm.

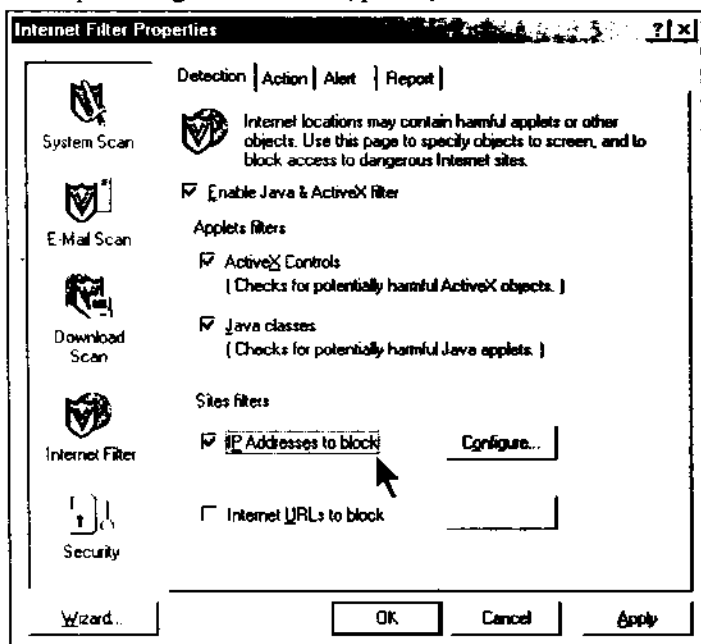


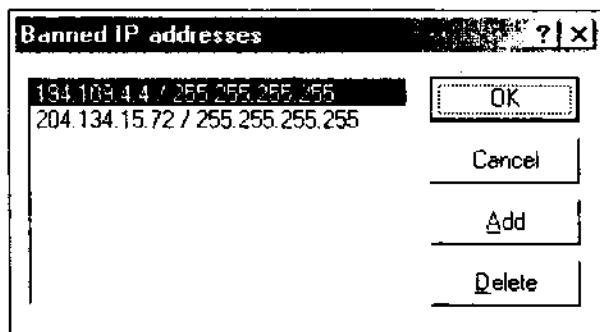
- ❖ **Java classes.** Chọn hộp kiểm này để module tìm và ngăn chặn các lớp Java classe hay các applet nguy hiểm được viết bằng ngôn ngữ Java.



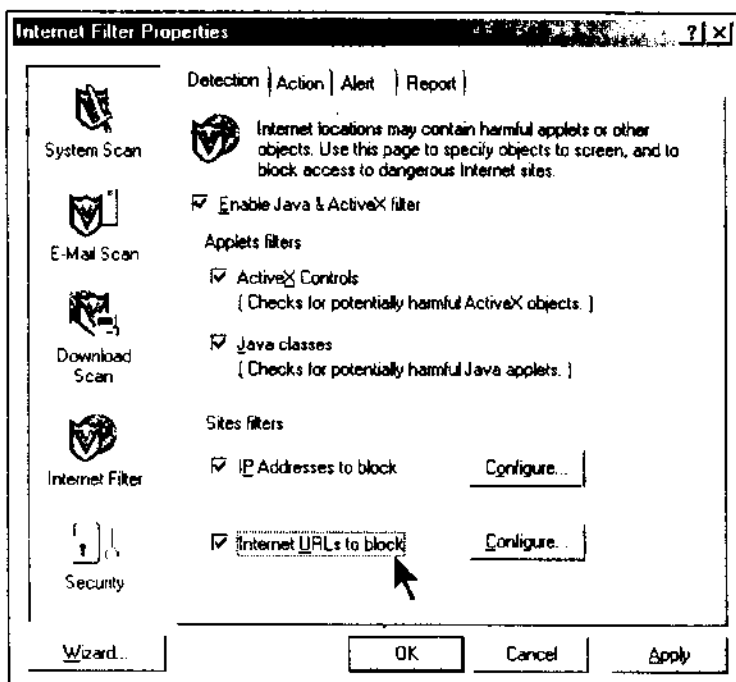
Module Internet Filter sẽ so sánh các đối tượng mà bạn gặp khi xem các file Internet với một cơ sở dữ liệu nội bộ vốn liệt kê các đặc điểm của các đối tượng đã được xác định là các đối tượng nguy hiểm. Khi nó tìm thấy một điểm phù hợp, module có thể cảnh báo bạn và để cho bạn quyết định việc cần thực hiện, hoặc nó có thể tự động ngăn chặn việc tải xuống đối tượng này.

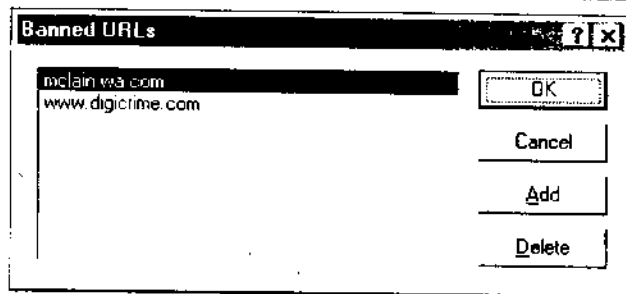
3. Cho module biết các file nào cần lọc. Chương trình sử dụng một danh sách các danh sách site Internet nguy hiểm để quyết định cần ngăn chặn bộ trình duyệt của bạn vào những site nào. Bạn có thể bật chức năng này và bổ sung vào danh sách các site “bị cấm” bằng hai cách:
 - ❖ IP Addresses to block. Chọn hộp kiểm này để yêu cầu module nhận biết các site Internet nguy hiểm bằng cách sử dụng các địa chỉ Internet Protocol (IP) của chúng. Để xem hay chỉ định việc bạn biết module ngăn cấm các địa chỉ nào, hãy nhấp Configure để mở hộp thoại Banned IP Addresses.





- ❖ Internet URLs to block. Chọn hộp kiểm này để yêu cầu module nhận biết các file Internet nguy hiểm bằng cách sử dụng phần chỉ định Uniform Resource Locator của chúng. Để xem hay chọn các địa chỉ nào mà bạn muốn các module ngăn cấm, hãy nhấp Configure để mở hộp thoại Bannel URLs.





4. Kế tiếp, bạn có thể:

- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại Internet Filter Properties.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút sau đây để tìm hiểu cách cấu hình các tùy chọn trên các trang đặc tính còn lại:

Action

Alert

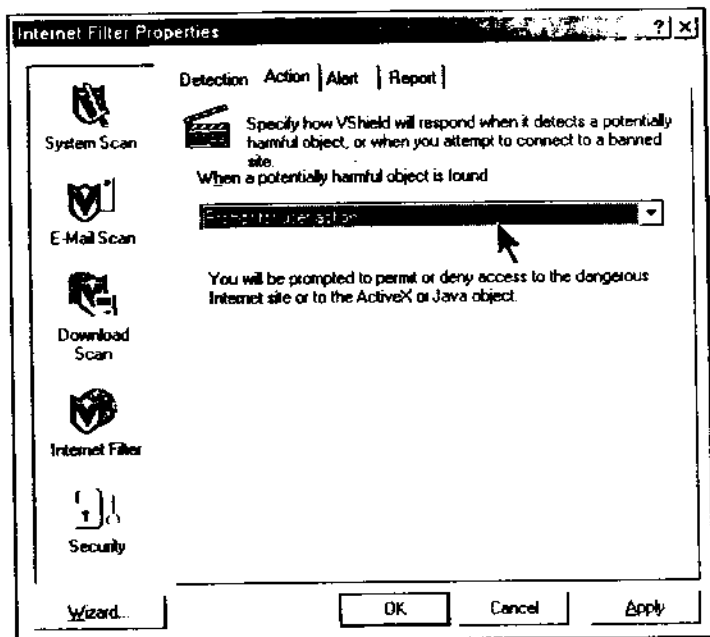
Report

- ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại Internet Filter Properties.
- ❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.

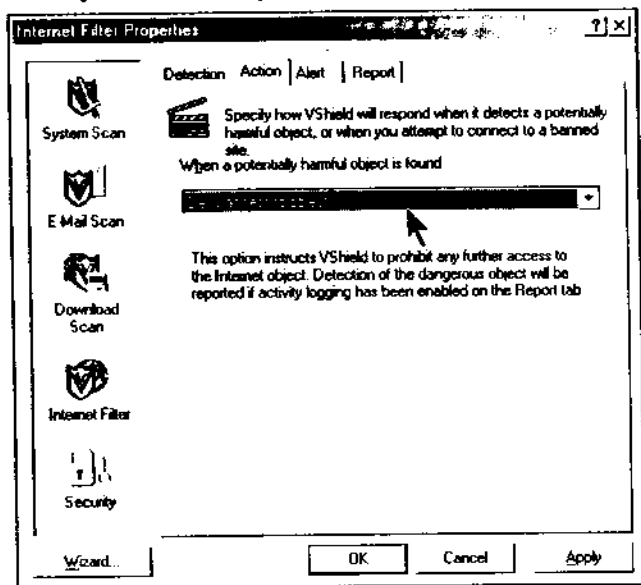
2. Chọn các tùy chọn Action dành cho module Internet Filter

Để thay đổi các tùy chọn cấu hình, hãy thực hiện các bước sau đây:

1. Chọn một trong các tùy chọn phản hồi sau đây từ danh sách When a potentially harmful is found:
 - ❖ Prompt for user action.



❖ Deny access to objects.



2. Kế tiếp, bạn có thể:

- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại Internet Filter Properties.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút sau đây để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại:

Detection

Alert

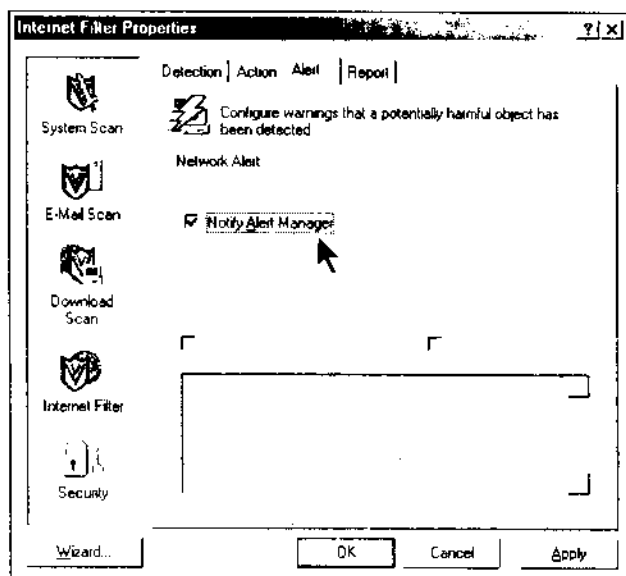
Report

- ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại Internet Filter Properties.
- ❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.

3. Chọn các tùy chọn Alert dành cho module Internet Filter

Để thay đổi các tùy chọn cấu hình, hãy thực hiện các bước sau đây:

1. Chọn hộp kiểm Notify Alert Manager để nhờ module gửi các thông tin cảnh báo đến Alert Manager để phân phối.



2. Chọn hộp kiểm Sound audible alert để nhờ module phát ra một tiếng beep khi nó tìm thấy một file bị nhiễm.
3. Chọn hộp kiểm Display custom message để nhờ module bổ sung một thông tin tùy biến vào hộp alert mà nó hiển thị khi nó tìm thấy một file bị nhiễm.
4. Nhập thông báo mà bạn muốn module hiển thị trong hộp text được cho. Bạn có thể nhập tối đa đến 250 ký tự.
5. kế tiếp, bạn có thể:
 - ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại Internet Filter Properties.
 - ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút sau đây để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại.

Detection

Action

Report

- ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại Internet Filter Properties.
- ❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.

4. Chọn các tùy chọn Report dành cho module Internet Filter

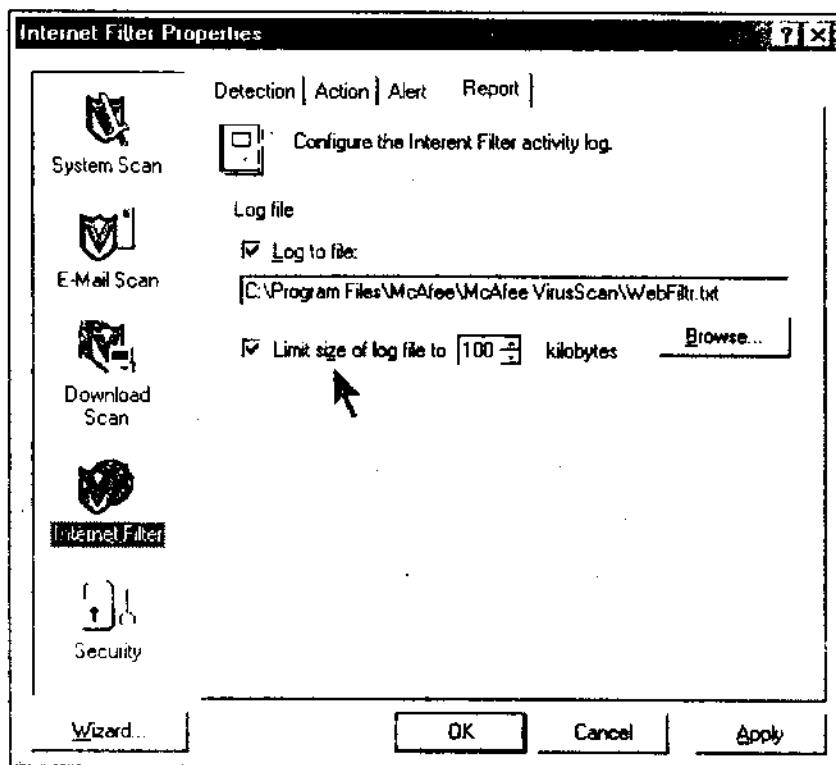
Module Internet Filter liệt kê các xác lập hiện hành và tóm tắt tất cả các hành động mà nó thực hiện trong suốt mỗi tác vụ quét trong một log file được gọi là WEBFLTR.TXT. Bạn có thể nhờ module ghi log của nó vào file này, hoặc bạn có thể sử dụng bất kỳ bộ chỉnh sửa text nào để tạo một file text cho nó sử dụng. Sau đó bạn có thể mở và in log file để xem lại.

Để quyết định module sẽ ghi lại dữ liệu nào và kích cỡ của log file là bao nhiêu, hãy thực hiện các bước sau đây:

1. Chọn hộp kiểm Log to file
2. Chọn hộp kiểm Limit size of log file to để giảm thiểu kích cỡ của log file. Nếu bạn không chọn hộp kiểm này, log file có

thể tăng đến kích cỡ mà khoảng trống đĩa hay hệ thống file của bạn cho phép.

3. Nhập một giá trị cho kích cỡ file theo đơn vị kilobyte, vào hộp text được cho.



4. kế tiếp, bạn có thể:

- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại Internet Filter Properties.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút sau đây để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại:

Detection

Action

Alert

- ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại Internet Filter Properties.
- ❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.

XIV. Cấu hình module Security

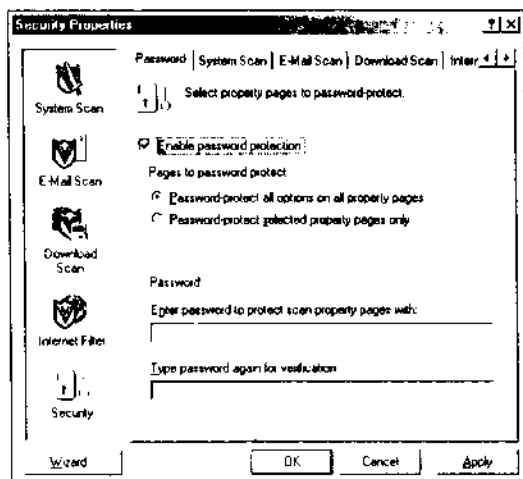
Để giữ an toàn các xác lập mà bạn đã chọn cho mỗi modul VShield nhằm tránh sự thay đổi khi không được phép, bạn có thể bảo vệ một hoặc tất cả các trang đặc tính module bằng một password. Những người quản lý hệ thống có thể ngăn chặn việc những người sử dụng mạng tắt VShield scanner, sau đó bảo vệ xác lập đó trong trang System Scan Detection bằng một password, nhằm giúp cho việc phòng chống virus trở nên dễ dàng và hiệu quả hơn.

Module Security không được bật theo mặc định, bởi vì có cần biết bạn muốn gán password nào cho các xác lập.

Để kích hoạt và cấu hình chế độ bảo vệ password module Security, hãy thực hiện các bước sau đây:

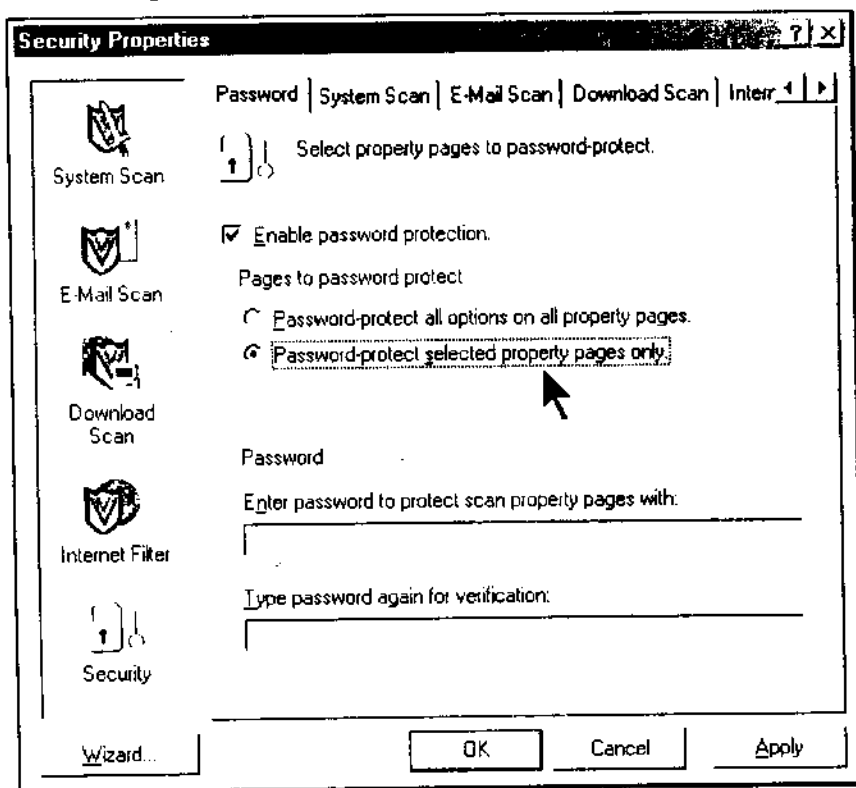
1. Chọn hộp kiểm Enable password protection.

Các tùy chọn còn lại trong phần của trang đặc tính sẽ kích hoạt.



2. Quyết định bảo vệ các trang đặc tính cho tất cả các module VShield, hay bảo vệ các trang riêng lẻ. Các mục chọn bao gồm:

- ❖ **Password-protect all options on all property pages.** Nhấp vào nút này để khóa mọi thứ cùng một lúc.
- ❖ **Password-protect selected property pages only.** Nhấp vào nút này để chọn các trang đặc tính nào mà bạn muốn khóa trong các module riêng lẻ. Các trang đặc tính còn lại trong hộp thoại Security Properties cho phép bạn bảo vệ các trang riêng lẻ trong các module VShield khác.



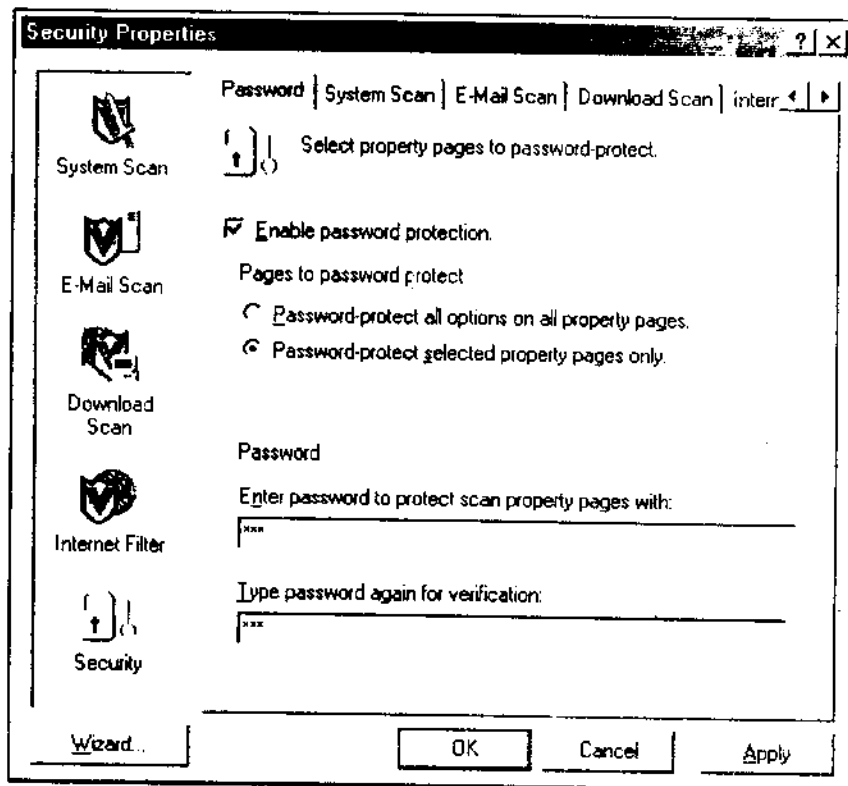
3. Nhập một password cần sử dụng để khóa các xác lập. Gõ nhập một tổ hợp bất kỳ lên đến 20 ký tự vào hộp text ở phía

trên trong vùng Password, sau đó nhập tổ hợp đó một lần nữa vào hộp text ở phía dưới để xác nhận sự chọn lựa của bạn.

Ghi chú

Việc bảo vệ bằng password trong VShield scanner khác với sự bảo vệ bằng password mà bạn có thể gán cho các thành phần VirusScan khác. Việc chọn một password trong một thành phần không gán password đó cho các thành phần khác - bạn phải chọn các password cho mỗi thành phần độc lập.

Ngay sau khi bạn đã bảo vệ các xác lập bằng một password, module Security sẽ yêu cầu bạn nhập password đó bất kỳ khi nào bạn mở hộp thoại VShield Properties.



4. kế tiếp, bạn có thể:

- ❖ Nhấp vào Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại Security Properties.
- ❖ Nhấp vào bất kỳ trong các nhãn module Security khác để bảo vệ các trang đặc tính riêng lẻ.
- ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại Security Properties.
- ❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.

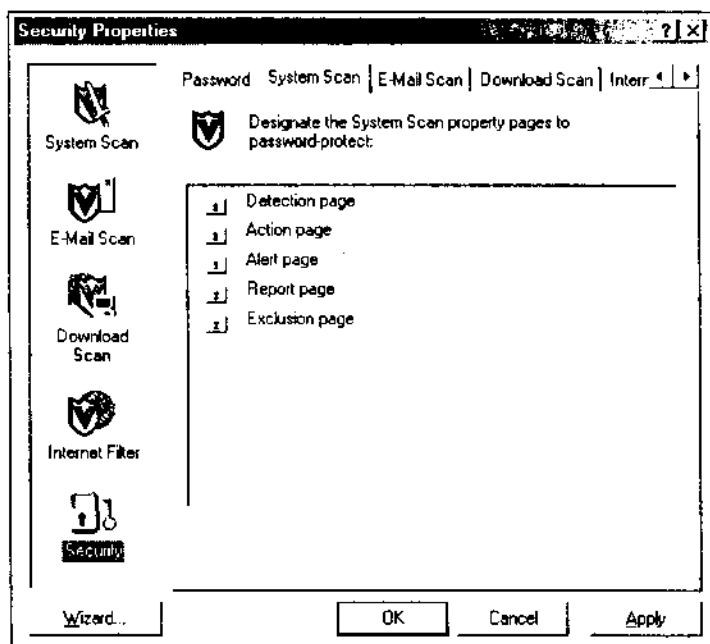
XV. Bảo vệ các trang đặc tính riêng lẻ trong các module VShield

Nếu bạn đã chọn Password-protect selected property pages only trong trang đặc tính Password, bạn có thể chọn các trang module VShield mà bạn muốn khóa.

Thực hiện các bước sau đây:

1. Nhấp vào nhãn dành cho module có các xác lập mà bạn muốn bảo vệ. Nếu bạn không nhìn thấy nhãn mà bạn muốn nhấp  hoặc  để đưa nó vào khung xem.
2. Chọn các xác lập mà bạn muốn bảo vệ trong danh sách hiển thị.

Bạn có thể bảo vệ một hoặc tất cả các trang đặc tính của một module. Các trang đặc tính đã được bảo vệ sẽ hiển thị một biểu tượng  ấn khóa đã khóa cho danh sách bảo vệ. Để loại bỏ sự bảo vệ ra khỏi một trang bảng tính, hãy nhấp vào biểu tượng này để mở khóa nó.



3. Kế tiếp, bạn có thể:

- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại Security Properties.
- ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại Security Properties.
- ❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.



TÌM HIỂU VIRUSSCAN CONSOLE

VirusScan Console được sử dụng chủ yếu để chạy các hoạt động quét và các tác vụ khác vào ngày và giờ mà bạn chọn, hoặc vào các thời khoảng mà bạn xác lập. Bạn có thể sử dụng Console để chạy một hoạt động quét khi bạn vắng mặt, ở dạng một thành phần trong một loạt các tác vụ tự động, hoặc theo những cách khác phù hợp với nhu cầu của bạn. VirusScan Console có thể trở thành phần thiết yếu trong chiến dịch phòng chống virus nếu bạn cài đặt nó để chạy nhiều tác vụ đan xen hay liên quan. Các tác vụ riêng biệt trong các chu kỳ khác nhau có thể quét các phần khác nhau của hệ thống, hoặc cung cấp sự bao hàm cho các event hoạt động đều đặn và có thể dự đoán trước.

Console còn cho phép bạn khởi động và ngưng nhiều hoạt động VirusScan quan trọng khác, bao gồm cả các tác vụ quét VShield, các hoạt động Auto Upgrade và AutoUpdate. Bạn có thể nối kết với Web site MacAfee AVERT Labs để tìm hiểu thông tin về virus, mở và xem các log file, sao chép và dán các định nghĩa tác vụ trong cửa sổ Console. Để tìm hiểu phần tổng quan về các chức năng có sẵn từ trong cửa sổ Console, hãy nhấp [here](#).

I. Tại sao bạn nên lập thời biểu cho các hoạt động quét

Mặc dù phần mềm VirusScan có các thành phần tìm virus liên tục hoặc cho phép bạn quét hệ thống bất kỳ khi nào bạn muốn, nhưng bạn nên lập thời biểu cho các hoạt động quét đều đặn và các hoạt

động phần mềm khác nếu bạn cần:

- ❖ Xác lập một cơ sở định kỳ cho hệ thống. Nếu bạn muốn theo dõi hệ thống hay mạng để tránh việc virus hoạt động trở lại, hãy lập thời biểu cho một hoạt động quét toàn bộ hệ thống vào các thời khoảng đều đặn. Các tính năng báo cáo của phần mềm VirusScan có thể cung cấp cho bạn một bản báo cáo đầy đủ về số lượng, loại, kích cỡ và các đặc điểm khác của bất kỳ virus nào mà nó tìm thấy.
- ❖ Bổ sung hay thay thế hoạt động quét vào lúc truy cập. McAfee đề nghị bạn sử dụng phần mềm VShield để quét virus liên tục, nhưng nếu môi trường của bạn không cho phép bạn sử dụng phần mềm VShield hoặc nếu bạn có các mối quan tâm khác về sự thực thi của hệ thống, hãy lập thời biểu cho các hoạt động quét thường xuyên để ngăn chặn sự lây nhiễm virus. Thậm chí nếu bạn sử dụng phần mềm VShield, việc lập thời biểu cho các hoạt động quét toàn bộ hệ thống theo định kỳ sẽ giảm bớt khả năng không tìm thấy các file bị nhiễm.
- ❖ Thay đổi luân phiên giữa các hoạt động quét. Các hoạt động quét theo thời biểu giúp bạn có khả năng linh hoạt trong việc chọn các hoạt động khác nhau cho các mục đích khác nhau hay các thời điểm khác nhau. Chẳng hạn, nếu bạn muốn sử dụng phần mềm VShield để quét hệ thống của bạn một cách liên tục và quét các ổ đĩa mạng được ánh xạ ít thường xuyên hơn, bạn có thể lập thời biểu cho một tác vụ dành cho mục đích này.

Console có một tập hợp các tác vụ mặc định đã được cấu hình, nhưng chưa được lập thời biểu. Tập hợp này bao gồm các tác vụ khởi động VShield scanner khi bạn khởi động máy tính, các tác vụ quét tất cả các ổ đĩa nằm trong nhóm My Computer, các tác vụ quét ổ đĩa C:, và các tác vụ cập nhật các file dữ liệu phần mềm VirusScan và các thành phần chương trình. Bạn có thể khởi động bất kỳ một trong các tác vụ mặc định này, hoặc bạn có thể tạo các tác vụ riêng phù hợp với thói quen làm việc của bạn.

II. Xác định VirusScan Console trên hệ thống

VirusScan Console scanner có một file khả thi chính, AVCONSOLE.EXE, mà bạn sẽ tìm thấy trong vị trí sau đây:

C:\Program Files\McAfee\VirusScan\VirusScan

Tuy nhiên, bạn không thể nhấp đúp vào file này để chạy nó. Để tìm hiểu cách khởi động chương trình, hãy nhấp [here](#).

Console làm việc với nhiều file khác nhằm cho phép bạn cấu hình và chạy các tác vụ quét, cập nhật và nâng cấp. Để xem các danh sách file dành cho mỗi loại tác vụ, hãy nhấp vào mỗi nút ở phía dưới:

Files for the VirusScan application

Files for the VShield scanner

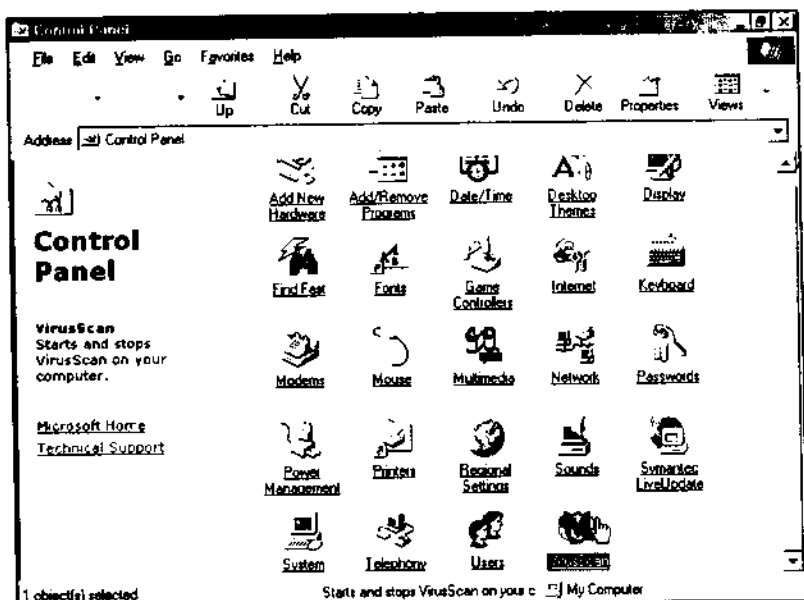
Files for the AutoUpdate and AutoUpgrade tasks

III. Khởi động VirusScan Console

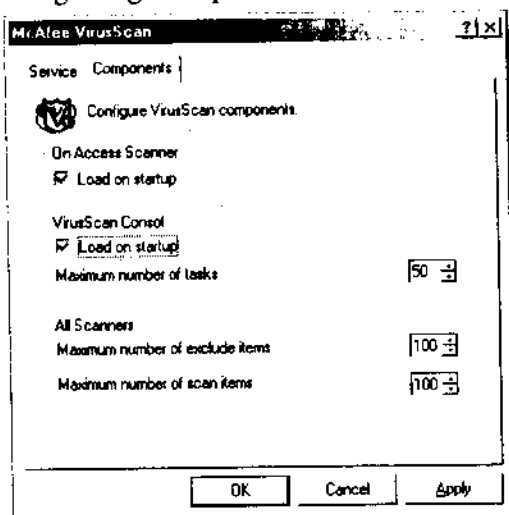
Bạn phải đang chạy VirusScan Console để chạy bất kỳ tác vụ nào mà bạn đã lập thời biểu. McAfee đề nghị bạn xác lập Console để nó khởi động tự động, ngay sau khi bạn khởi động máy tính.

Để thực hiện điều này, hãy thực hiện các bước sau đây:

1. Nhấp Start trong thanh tác vụ Windows, trở đến Settings, sau đó chọn Control Panel.
2. Xác định và nhấp đúp vào VirusScan control panel để mở nó.



3. Nhấp nhấn Components trong hộp thoại VirusScan control panel.
4. Chọn hộp kiểm Load on startup trong vùng VirusScan Console trong trang Components.



5. Nhấp OK để đóng control panel.

Khi bạn khởi động lại máy tính vào lần kế tiếp, Console cũng sẽ khởi động, nhưng nó vẫn ở dạng biểu tượng trong khay hệ thống Windows.

Để hiển thị cửa sổ Console, hãy nhấp đúp biểu tượng Console. Để xem diện mạo của cửa sổ Console khi nó xuất hiện, hãy nhấp [here](#).

Ghi chú

Nếu biểu tượng này không xuất hiện trong khay hệ thống, hãy nhấp Start trong thanh tác vụ Windows, trở đến Programs, sau đó trở đến McAfee VirusScan. Kế tiếp, hãy chọn VirusScan Console để hiển thị cửa sổ Console.

Ngay sau khi bạn hiển thị cửa sổ Console, bạn cũng có thể bảo đảm rằng nó sẽ tải tự động vào lúc khởi động bằng cách chọn Load at startup từ menu View.

IV. Ngưng VirusScan Console

Theo mặc định, Setup bật VirusScan Console ngay sau khi nó thực hiện xong việc cài đặt. Nó hiển thị biểu tượng của nó trong khay hệ thống Windows để dễ truy cập.

Ghi chú

Để chạy bất kỳ tác vụ nào mà bạn đã lập thời biểu, Console phải hoạt động.

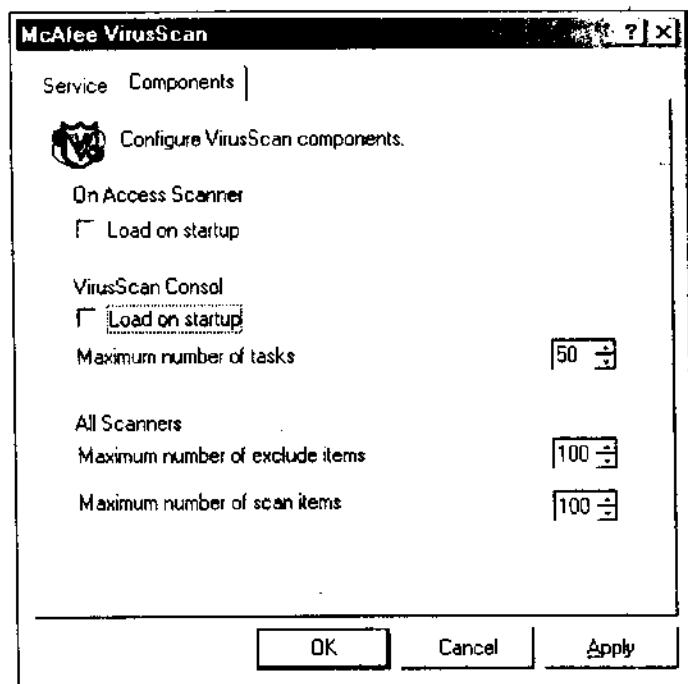
Ngăn chặn VirusScan Console khởi động tự động

Nếu bạn không muốn VirusScan Console khởi động tự động, bạn có thể ngăn chặn điều này trong VirusScan control panel.

Thực hiện các bước sau đây:

1. Nhấp Start trong thanh tác vụ Windows, trở đến Settings, sau đó chọn Control Panel.
2. Xác định và nhấp đúp VirusScan control panel để mở nó.
3. Nhấp nhãn Components.

4. Hủy, chọn hộp kiểm Load on startup ở cuối trang đặc tính Components.
5. Nhấp OK để đóng control panel. VirusScan Console sẽ không ngưng hay hủy tải vào lúc này, nhưng nó sẽ không khởi động khi bạn khởi động máy tính của mình vào lần kế tiếp.



Ngưng hẳn VirusScan Console

Bạn có thể ngưng VirusScan Console ngay lập tức bằng một trong ba cách sau đây.

Ghi chú

Việc ngưng hẳn Console có nghĩa là hủy kích hoạt nó và loại nó ra khỏi bộ nhớ. Biểu tượng Console sẽ biến mất khỏi khay hệ thống. Để tìm hiểu cách khởi động lại Console, hãy nhấp [here](#).

Sử dụng menu tắt Console. Hãy thực hiện các bước sau đây:

1. Nhấp phải biểu tượng Console () trong khay hệ thống Windows để hiển thị menu tắt của nó.
2. Chọn Exit.

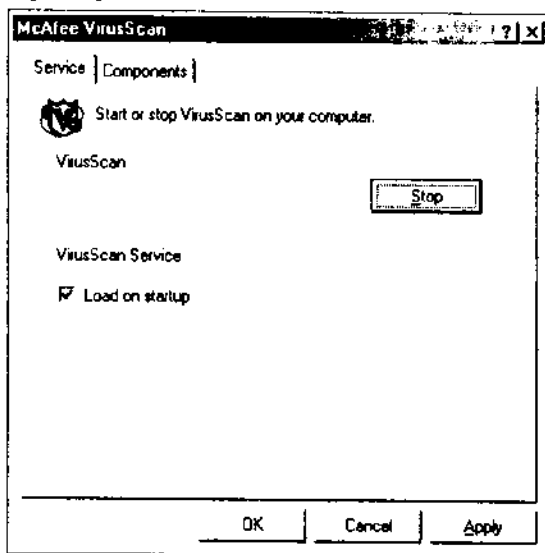
VirusScan Console sẽ ngưng và hủy tải chính nó từ bộ nhớ. Biểu tượng Console sẽ biến mất khỏi thanh tác vụ Windows.

Thoát khỏi cửa sổ Console. Từ cửa sổ Console đang mở, hãy chọn Exit từ menu Task.

Console sẽ ngưng và hủy tải từ bộ nhớ. Biểu tượng Console sẽ biến mất khỏi thanh tác vụ Windows.

Sử dụng VirusScan Console control panel. Thực hiện các bước sau đây:

1. Nhấp Start trong thanh tác vụ Windows, trở đến Settings, sau đó chọn Control Panel.
2. Xác định và nhấp đúp vào VirusScan control panel để mở nó.
3. Nhấp nhấn Service.
4. Nhấp Stop.



Tất cả các thành phần VirusScan đang hoạt động sẽ ngưng, đóng tất cả các cửa sổ hay các hộp thoại đang mở, loại bỏ các biểu tượng của chúng ra khỏi khay hệ thống Windows, và hủy tải từ bộ nhớ.

5. Nhấp OK để đóng control panel.

V. Khởi động lại VShield scanner và Console từ control panel

Thực hiện các bước sau đây:

1. Nhấp Start trong thanh tác vụ Windows, trở đến Settings, sau đó chọn Control Panel.
2. Xác định và nhấp đúp vào VirusScan control panel để mở nó.
3. Nhấp nhấn Service.
4. Nhấp Stop.

Tất cả các thành phần VirusScan đang hoạt động sẽ ngưng, đóng tất cả các cửa sổ hay các hộp thoại đang mở, loại bỏ các biểu tượng của chúng ra khỏi khay hệ thống Windows, và hủy tải từ bộ nhớ.

5. Nhấp Start trong cùng một trang đặc tính.
6. VShield scanner và VirusScan Console sẽ khởi động lại và hiển thị các biểu tượng của chúng trong khay hệ thống Windows.
7. Nhấp OK để đóng control panel.

VI. Làm việc với cửa sổ Console

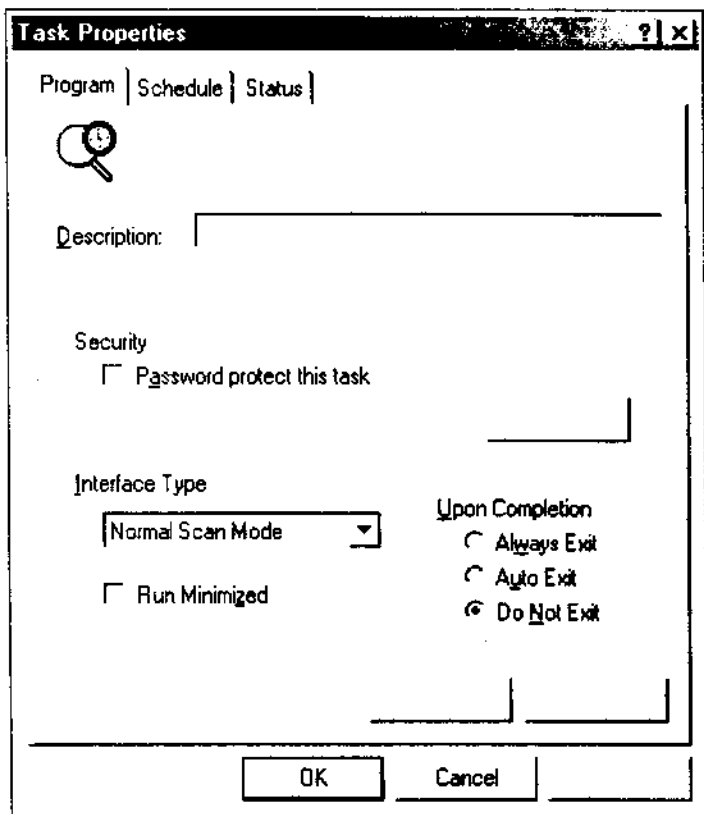
Cửa sổ Console ban đầu hiển thị một tập hợp mặc định gồm các tác vụ đã được cấu hình sẵn để sẵn sàng chạy. Một "tác vụ" là một tập hợp các chỉ dẫn để chạy các thành phần VirusScan cụ thể, trong một cấu hình nhất định, tại một thời điểm nhất định. Để tìm hiểu thêm về tập hợp tác vụ mặc định, hãy nhấp [here](#)..

Cùng với tên dành cho mỗi tác vụ, cửa sổ Console còn hiển thị đường dẫn và tên file dành cho chương trình mà tác vụ sẽ chạy theo

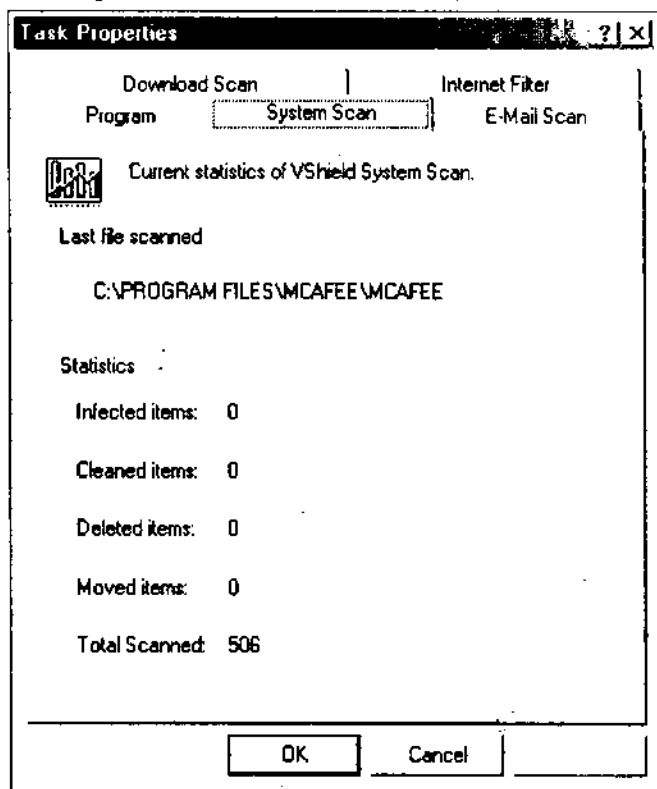
thời biểu đã lập. Các tác vụ mà bạn tạo sẽ luôn luôn chạy trình ứng dụng VirusScan. Các tác vụ vừa mới được tạo sẽ xuất hiện ở cuối cửa sổ Console. Console cũng hiển thị thời gian và ngày tháng mà mỗi tác vụ đã chạy vào lần sau cùng, thời gian và ngày tháng mà nó sẽ chạy vào lần kế tiếp.

Từ cửa sổ Console, bạn có thể:

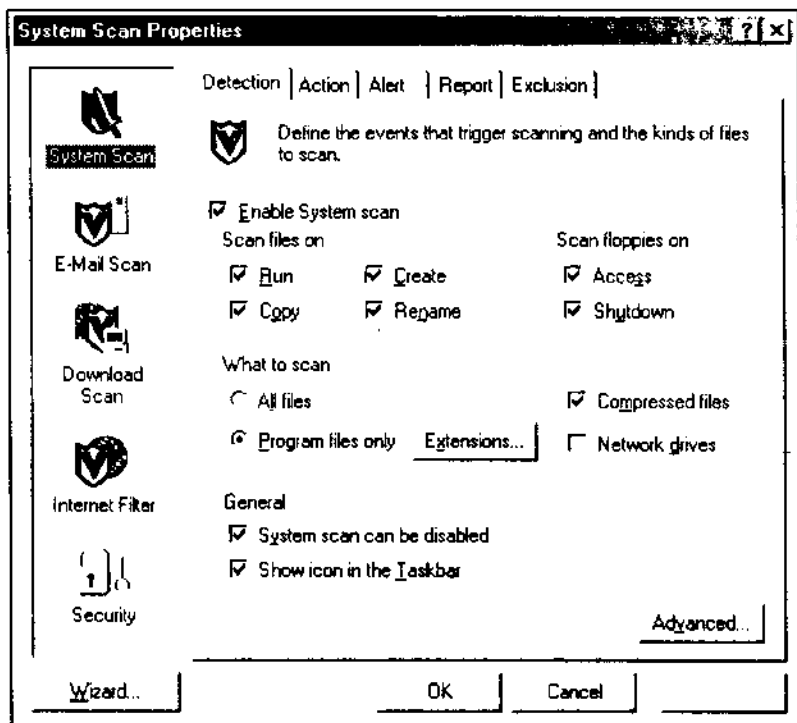
- ❖ Tạo một tác vụ mới  . Nhấp trong thanh công cụ Console, hoặc chọn New Task từ menu Task. Một hộp thoại Task Properties sẽ xuất hiện. Để tìm hiểu cách đặt tên và xác lập các đặc tính khác cho tác vụ mới.



- ❖ **Lập thời biểu và bật một tác vụ.** Chọn một trong các tác vụ được liệt kê trong cửa sổ Console, sau đó nhấp trong thanh công cụ Console, hoặc chọn Properties  từ menu Task. Một hộp thoại Task Properties sẽ xuất hiện. Để tìm hiểu cách lập thời biểu và bật một tác vụ.

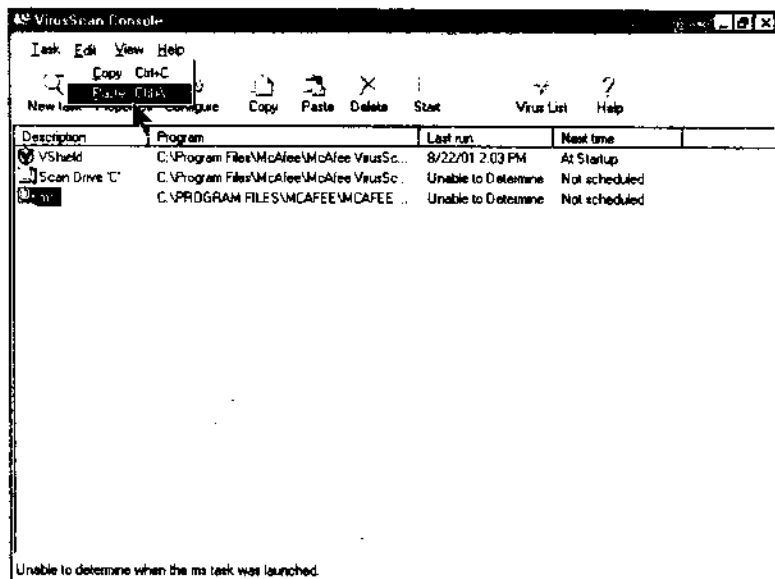


- ❖ **Cấu hình tác vụ.** Chọn một trong các tác vụ được liệt kê trong cửa sổ Console , sau đó nhấp trong thanh công cụ Console để hiển thị một trang đặc tính dành cho thành phần VirusScan mà nó sẽ chạy tác vụ. Diện mạo của trang đặc tính này phụ thuộc vào thành phần phần mềm VirusScan nào mà bạn chọn để cấu hình.



- ❖ Sao chép một tác vụ. Chọn một trong các tác vụ được liệt kê trong cửa sổ Console, sau đó nhấp trong thanh công cụ Console, hoặc chọn Copy  từ menu Edit. Thao tác này sẽ sao chép tác vụ vào Windows clipboard.

Kế tiếp, hãy nhấp vào bên trong cửa sổ Console, sau đó nhấp trong thanh công cụ Console, hoặc chọn Paste  từ menu Edit, để dán một bản sao của tác vụ vào danh sách Console. Sử dụng tính năng này để sao chép các xác lập tác vụ mà bạn muốn sử dụng làm template cho các tác vụ tương tự khác.



- ❖ Xóa một tác vụ. Chọn một trong các tác vụ được liệt kê trong cửa sổ Console, sau đó nhấp trong thanh công cụ Console, hoặc chọn Delete  từ menu Task.

Bạn có thể xóa chỉ các tác vụ mà bạn tạo - bạn không thể xóa bất kỳ tác vụ nào trong tập hợp các tác vụ mặc định đi kèm với Console. Tuy nhiên, bạn có thể tắt bất kỳ tác vụ mặc định mà bạn không muốn chạy.

- ❖ Khởi động một tác vụ. Chọn một trong các tác vụ được liệt kê trong cửa sổ Console, sau đó nhấp trong thanh công cụ Console, hoặc chọn Start  từ menu Task. Tác vụ mà bạn đã chọn sẽ khởi động ngay lập tức và sẽ chạy với các tùy chọn mà bạn đã chọn.

Để khởi động VShield scanner và tải nó vào bộ nhớ, hãy chọn tác vụ VShield trong danh sách, sau đó nhấp trong thanh công cụ Console, hoặc chọn Enable từ menu Task. Để tìm

hiểu các cách khởi động VShield scanner khác, hãy nhấp [here](#)..

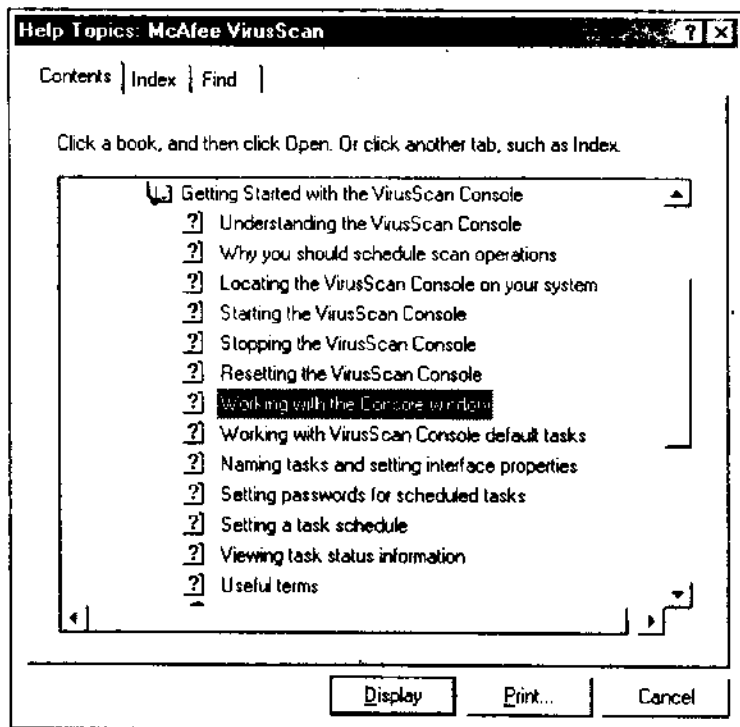
- ❖ Ngưng một tác vụ. Chọn một trong các tác vụ được liệt kê trong cửa sổ Console, sau đó nhấp  hoặc chọn Stop Now từ menu tắt.

Để ngưng VShield scanner, hãy chọn tác vụ VShield trong danh sách, sau đó nhấp  trong thanh công cụ Console, hoặc chọn Disable từ menu Task. Để tìm hiểu các cách ngưng VShield scanner khác, hãy nhấp [here](#)..

- ❖ Nối kết với McAfee Virus Information Library. Nhấp  trong thanh công cụ Console, hoặc chọn Virus List từ menu View. Phần mềm VirusScan sẽ khởi động trình ứng dụng bộ trình duyệt mà bạn ưa thích và nối kết với website McAfee AVERT.

Để nối kết với Virus Information Library, bạn phải có một nối kết Internet và phần mềm trình duyệt Web có sẵn trên hệ thống.

- ❖ Mở file trợ giúp trực tuyến. Nhấp  trong thanh công cụ Console, hoặc chọn Help Topics từ menu Help, để xem danh sách các chủ điểm trợ giúp phần mềm VirusScan. Bạn cũng có thể nhấp phải vào phần lớn các nút trong hộp thoại, các danh sách, các menu, và các hạng mục khác để hiển thị các chủ điểm trợ giúp nhạy ngữ cảnh. Nhấp hạng mục What's This? vốn hiển thị khi bạn nhấp phải vào bên trong một hộp thoại để xem chủ điểm trợ giúp. Để tìm hiểu thêm về tài liệu đi kèm với sản phẩm VirusScan.



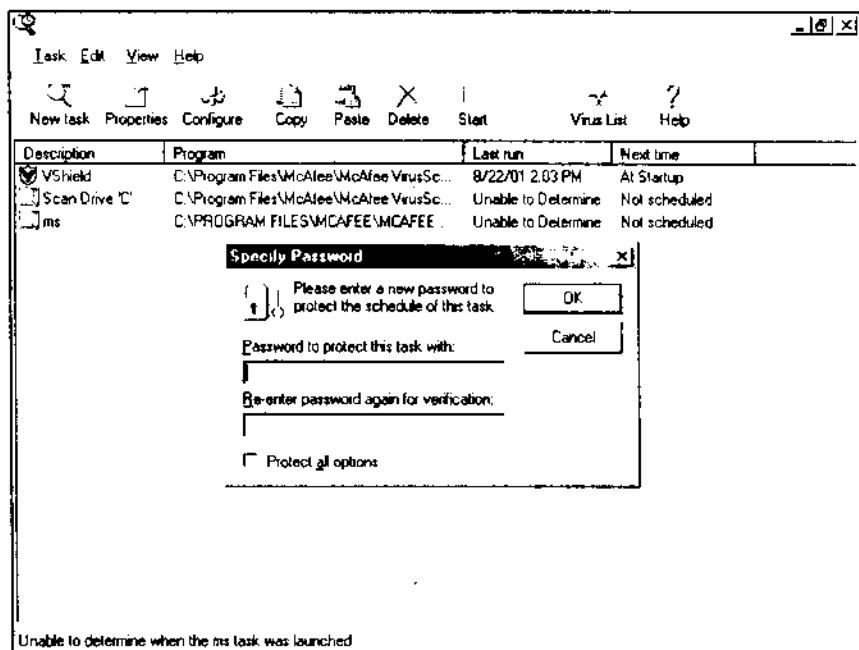
- ❖ Xem một activity log. Chọn một trong các tác vụ được liệt kê trong cửa sổ Console, sau đó chọn View Activity Log từ menu Task. Không phải tất cả các tác vụ đều có một log file thích hợp, nhưng phần mềm VirusScan sẽ mở log file dành cho các tác vụ thực hiện trong cửa sổ Windows Notepad. Bạn có thể in, chỉnh sửa, sao chép, hoặc xử lý file này giống như bạn thực hiện đối với bất kỳ file text bình thường khác. Để tìm hiểu thêm về những gì mà log file của trình ứng dụng VirusScan ghi lại.

Để tìm hiểu thêm về những gì mà các log file của VShield scanner ghi lại.

- ❖ Bảo vệ các tác vụ bằng một password. Chọn bất kỳ một trong các tác vụ được liệt kê trong cửa sổ Console ngoại trừ tác vụ VShield, sau đó chọn Password Protect Task từ menu

Task để mở hộp thoại Specify Password. Nhập một password lên đến 20 ký tự vào hộp text được cho, sau đó nhập lại password này vào hộp text ở phía dưới. Nhấp OK để đóng hộp thoại.

- ❖ Bất kỳ khi nào bạn hay một người nào khác cố cấu hình các đặc tính tác vụ cho tác vụ mà bạn bảo vệ, Console sẽ yêu cầu password mà bạn đã chỉ định. Việc chọn tùy chọn này cung cấp cho bạn các kết quả tương tự như việc chọn hộp kiểm Password protect this task trong hộp thoại Task Properties.



- ❖ Khởi động VirusScan Console một cách tự động. Chọn Load at startup từ menu View để VirusScan Console khởi động bất kỳ khi nào bạn khởi động máy tính. Console có tùy chọn này được bật theo mặc định. Bởi vì nó phải chạy để thực thi bất kỳ tác vụ nào mà bạn đã lập thời biểu, nên bạn phải chọn để Console khởi động tự động sao cho các tác vụ đã

lập thời biểu sẽ bắt đầu vào các thời điểm đã định. Bạn cũng có thể điều khiển tùy chọn này từ VirusScan control panel. Để tìm hiểu thêm về control panel, hãy nhấp [here](#)..

- ❖ **Hiển thị và che giấu các phần của cửa sổ Console.** Nhấp menu View, trở đến Toolbars, sau đó chọn các tùy chọn hiển thị mà bạn thích cho các nút trên thanh công cụ. Các hạng mục có một dấu kiểm ở kế bên chúng là các hạng mục hoạt động. Bạn có thể xác lập các nút để chúng xuất hiện ở dạng các biểu tượng, ở dạng text, hoặc ở cả dạng text và biểu tượng.

Bạn cũng có thể chọn Status Bar từ menu View để hiển thị hoặc che giấu thanh trạng thái ở cuối cửa sổ Console, và chọn Title Bar từ cùng một menu để hiển thị hoặc che giấu các nhãn text nằm ở ngay phía trên danh sách tác vụ.

- ❖ **Hiển thị biểu tượng khay hệ thống Console,** chọn Show System Tray Icon từ menu View để nhờ Console hiển thị biểu tượng này  trong khay hệ thống Windows. Việc nhấp đúp vào biểu tượng này sẽ hiển thị cửa sổ Console. Việc nhấp phải vào biểu tượng này sẽ hiển thị một menu tắt.
- ❖ **Thoát khỏi VirusScan Console.** Chọn Exit từ menu Task để thoát khỏi Console. Nếu có bất kỳ tác vụ nào đang chờ xử lý, bạn nên giảm kích cỡ Console xuống tối đa thay vì thoát khỏi nó. Để tìm hiểu cách khởi động lại Console, hãy nhấp [here](#)..

VII. Làm việc với các tác vụ mặc định VirusScan Console

Console có năm tác vụ mặc định. Đó là:

- ❖ **VShield.** Tác vụ này chạy VShield scanner. Theo mặc định, nó chạy tự động ngay sau khi bạn khởi động máy tính. Bạn không thể lập thời biểu để VShield scanner chạy vào bất kỳ lúc nào khác, nhưng bạn có thể chọn các tùy chọn quét khác.

Bạn không thể đặt lại tên hay xóa tác vụ này, nhưng bạn có thể xem các thông tin thống kê từ tác vụ quét gần đây nhất của nó, bạn có thể bật hoặc tắt nó, và bạn có thể mở hộp thoại VShield Properties để cấu hình nó.

- ❖ **AutoUpgrade** Tác vụ này cho phép bạn lập thời biểu cho các hoạt động nâng cấp chương trình tự động dành cho phần mềm VirusScan. Các hoạt động nâng cấp này có thể bao gồm các file công cụ quét mới hoặc các hoạt động nâng cấp file khác. Để nó nâng cấp các file của bạn, bạn phải cấu hình tác vụ này để nó nối kết với một server mạng cục bộ hoặc site FTP mà bạn chỉ định, sau đó bạn phải lập thời biểu và kích hoạt nó. Bạn không thể đặt lại tên hay xóa tác vụ này, nhưng bạn có thể bật và tắt nó, lập thời biểu cho nó, cấu hình nó, và bảo vệ các xác lập của nó bằng một password.
- ❖ **AutoUpdate.** Tác vụ này cho phép bạn lập thời biểu cho các hoạt động cập nhật file định nghĩa virus tự động (.DAT). Để nó thực hiện điều này, bạn phải cấu hình tác vụ để nó nối kết với một server hay site FTP (File Transfer Protocol) mà bạn chỉ định. Tác vụ này được cấu hình để nối kết với một server McAfee, nhưng bạn cũng có thể xác lập để nó tải xuống các file trong nội bộ. Bạn cũng phải lập thời biểu và kích hoạt tác vụ để nó cập nhật các file. Về các khía cạnh khác, tác vụ này hầu như giống với tác vụ AutoUpgrade.
- ❖ **Scan My Computer.** Tác vụ này chạy một hoạt động quét cơ bản trên tất cả các ổ đĩa cứng và các ổ đĩa khác được nối kết với máy tính, cùng với RAM và đĩa cứng hay các sector khởi động đĩa mềm. Bạn không thể đặt lại tên hay xóa tác vụ này, nhưng bạn có thể chỉnh sửa cấu hình của nó, lập thời biểu cho nó, xem các thông tin thống kê từ hoạt động Web gần đây nhất của nó, và bảo vệ các xác lập của nó bằng một password. Bạn phải kích hoạt tác vụ này để chạy nó, nhưng bạn có thể chạy nó trong cấu hình mặc định cho chế độ bảo vệ gần như toàn diện.

- ❖ **Scan Drive C.** Tác vụ này chạy một hoạt động quét cơ bản trên ổ đĩa C: của máy tính. Về mặt khác, nó hầu như giống với tác vụ Scan My Computer.

Cả hai tác vụ Scan My Computer và Scan Drive C đều đòi hỏi phải chạy trình ứng dụng VirusScan. Để tìm hiểu cách cấu hình trình ứng dụng để sử dụng với VirusScan Console, hãy nhấp [here](#):

VIII. Đặt tên cho các tác vụ và xác lập các đặc tính giao diện

Mặc dù các tác vụ trong tập hợp các tác vụ mặc định có thể cung cấp cho hệ thống một chế độ phòng chống virus gần như toàn diện, nhưng bạn có thể vẫn muốn tạo và chạy các tác vụ riêng của mình sau khi bạn đã có kinh nghiệm sử dụng phần mềm VirusScan và có một ý tưởng hay về việc bạn muốn nó quét những vùng nào và vào lúc nào.

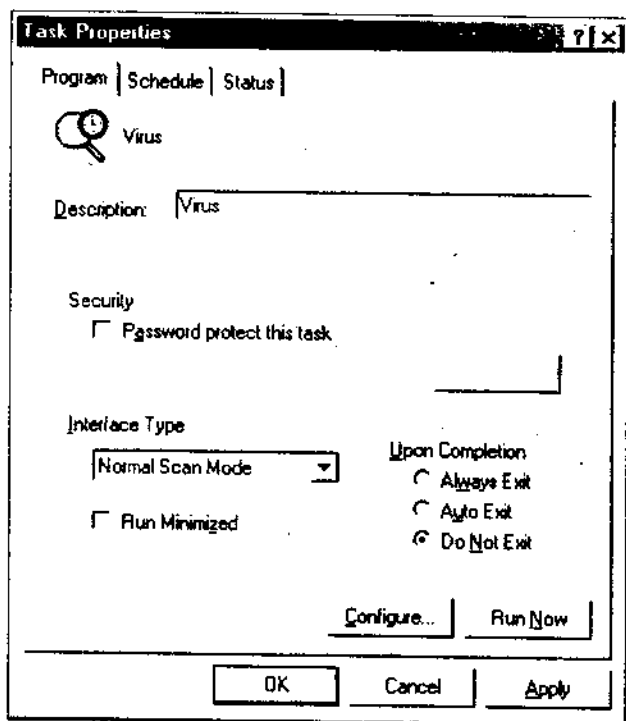
Bạn có thể chỉnh sửa một số khía cạnh của các tác vụ mặc định đi kèm với VirusScan Console, nhưng bạn không thể xóa, đặt lại tên - ngoại trừ các tác vụ Scan My Computer và Scan Drive C - hoặc tạo các trường hợp mới của chúng. Bạn có thể sao chép các tùy chọn cấu hình hiện có từ các tác vụ Scan My Computer và Scan Drive C, sử dụng chúng làm các xác lập cơ bản cho các tác vụ mới của bạn.

Tuy nhiên, Console cho phép bạn tạo đến 50 tác vụ mới phù hợp với các nhu cầu của bạn. Bạn có thể tăng giới hạn này bằng cách thay đổi số trong VirusScan control panel.

Để tạo một tác vụ quét mới, hãy mở cửa sổ Console, sau đó thực hiện các bước sau đây:

1. Nhấp  trong thanh công cụ Console, hoặc chọn New Task từ menu Task.

Hộp thoại Task Properties sẽ xuất hiện.



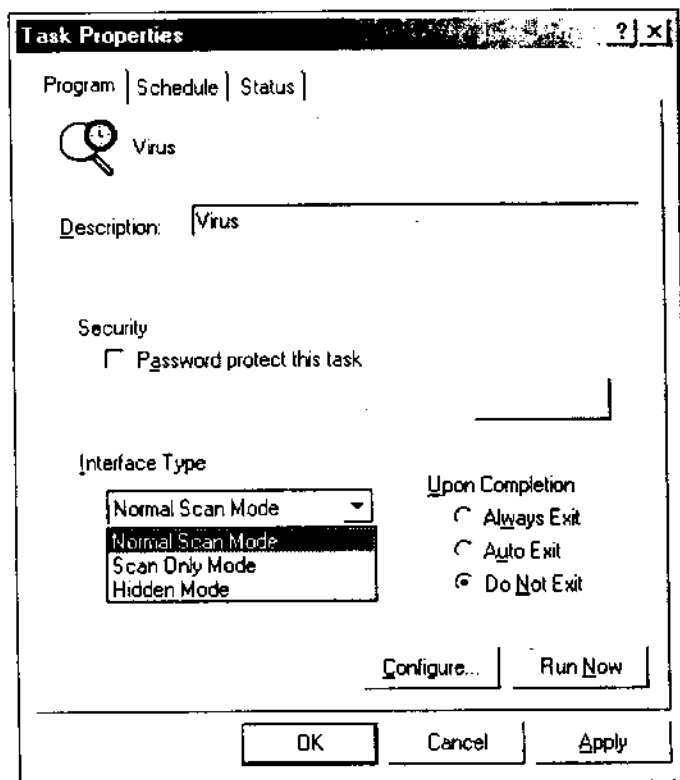
2. Gõ nhập một tên cho tác vụ vào hộp text Description.

Bảo đảm tên mà bạn gõ nhập mô tả đúng tác vụ để bạn có thể phân biệt nó với các tác vụ khác trong cửa sổ Console và để bạn có thể xem lượt qua chức năng của nó.

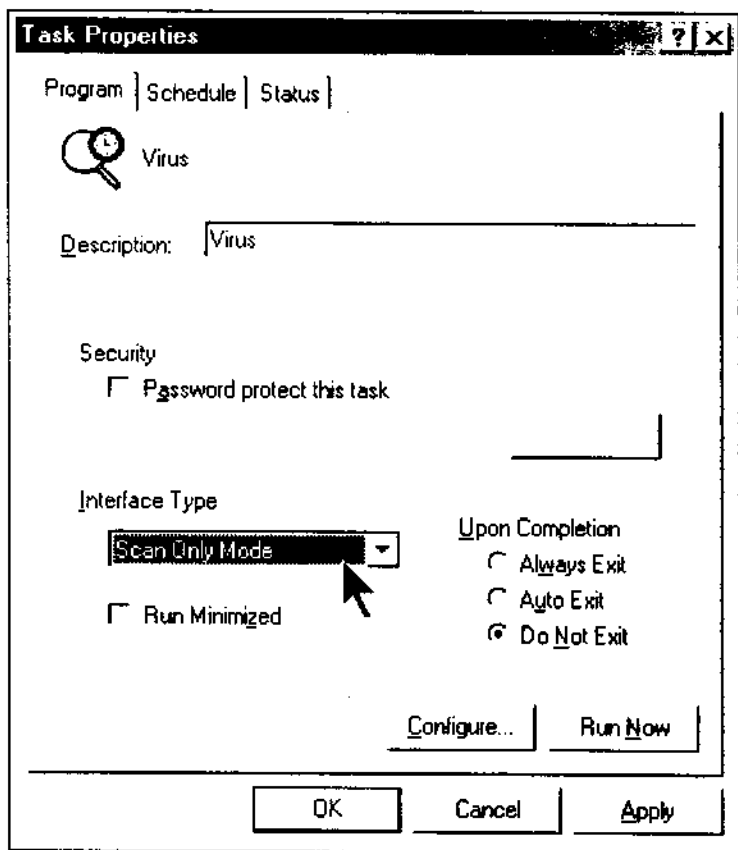
3. Xác lập một password để bảo vệ tác vụ này và ngăn chặn những người khác thực hiện bất kỳ thay đổi nào đối với các xác lập của tác vụ quét. Để tìm hiểu cách thực hiện điều này, hãy nhấp [here](#).
4. Chỉ định cách bạn muốn giao diện tác vụ xuất hiện và mức độ điều khiển đối với tác vụ mà bạn muốn có khi nó chạy. Các tùy chọn bao gồm:

- ❖ **Normal Scan Mode.** Tùy chọn này hiển thị cửa sổ chính dành cho trình ứng dụng VirusScan trong suốt các hoạt động

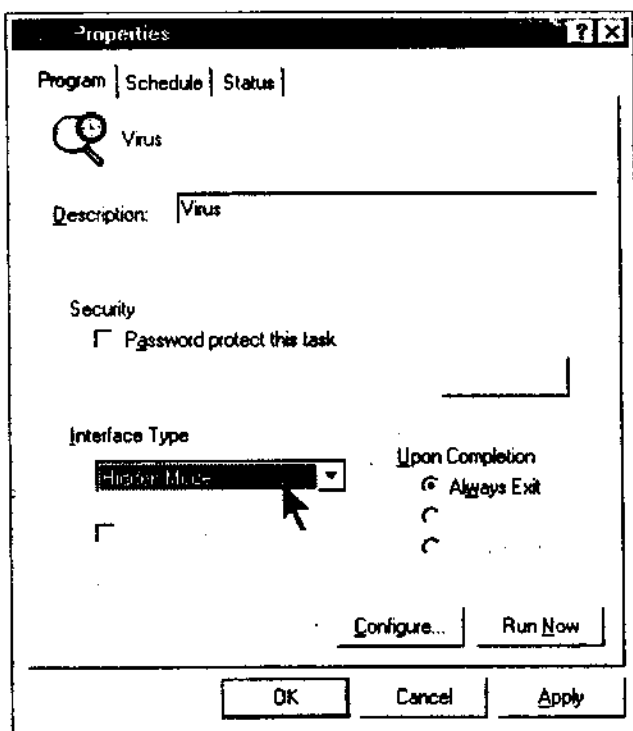
quét. Nó cho phép bạn hay người sử dụng xem - nhưng không thay đổi - các tùy chọn cấu hình mà tác vụ sử dụng khi nó chạy, xem các kết quả của hoạt động quét, hoặc ngưng hoạt động vào bất kỳ lúc nào. Bạn cũng có thể chọn bất kỳ một trong các lệnh từ các menu của cửa sổ chính. Chọn hộp kiểm Run Minimized để mở cửa sổ ở dạng một biểu tượng thu nhỏ trong thanh tác vụ Windows.



- ❖ **Scan only mode.** Tùy chọn này hiển thị một cửa sổ thu nhỏ để cho biết tác vụ đang chạy. Bạn có thể ngưng, tạm dừng hoặc bắt đầu lại tác vụ vào bất kỳ lúc nào. Chọn hộp kiểm Run Minimized để mở hộp kiểm ở dạng một nút thu nhỏ trong thanh tác vụ Windows.

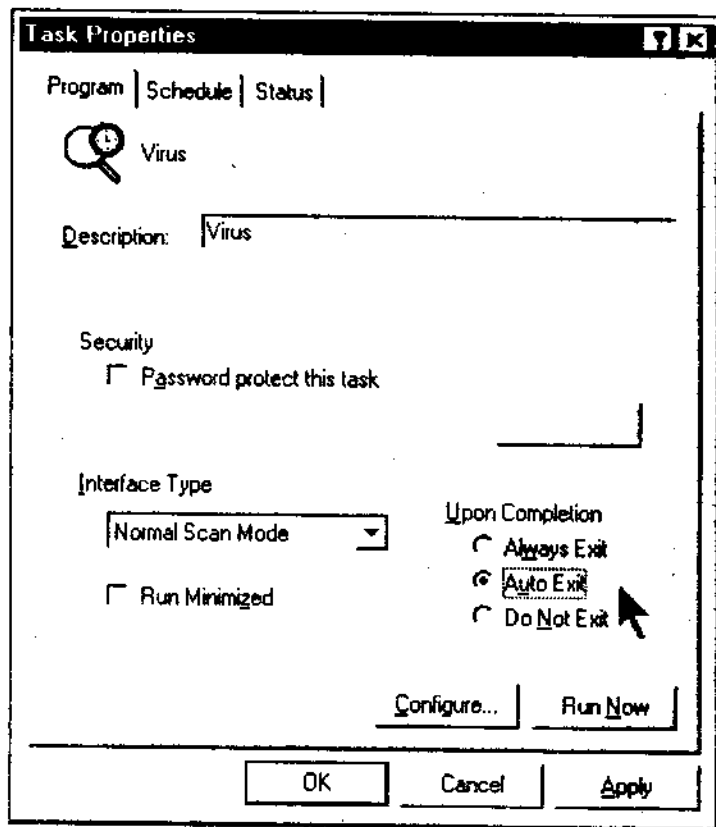


- ❖ **Hidden mode.** Tùy chọn này không hiển thị giao diện nào khi tác vụ quét chạy. Bạn không thể ngưng hay tạm dừng tác vụ trừ khi hộp thoại VirusScan Console hay Task Properties đang hoạt động. Trình ứng dụng VirusScan vẫn sẽ thông báo cho bạn biết khi nào nó tìm thấy một virus, nếu bạn đã cấu hình bất kỳ tùy chọn cảnh báo nào dành cho tác vụ. Tác vụ này luôn thoát khỏi trình ứng dụng khi nó hoàn tất.



5. Chỉ định bạn muốn tác vụ thực hiện điều gì khi nó hoàn tất. Các tùy chọn bao gồm:

- ❖ **Always Exit.** Nhấp vào nút này để yêu cầu trình ứng dụng VirusScan luôn thoát ngay sau khi nó thực hiện xong tác vụ quét này. Nếu bạn chọn Hidden Mode trong danh sách Interface Type, thì đây là tùy chọn duy nhất.
- ❖ **Auto Exit.** Nhấp nút này để yêu cầu trình ứng dụng VirusScan thoát tự động nếu nó chưa tìm thấy bất kỳ virus nào trong suốt tác vụ quét nào. Nếu trình ứng dụng tìm thấy một virus, nó vẫn mở để hiển thị các kết quả quét.



Nếu bạn chạy tác vụ trong chế độ quét bình thường, nó cũng sẽ cho phép bạn loại bỏ bất kỳ virus nào mà nó tìm thấy, nếu bạn chưa xác lập trình ứng dụng để loại bỏ chúng một cách tự động.

- ❖ **Never Exit.** Nhấp vào nút này để chỉ định việc bạn muốn trình ứng dụng VirusScan luôn luôn mở sau khi nó thực hiện xong tác vụ này.

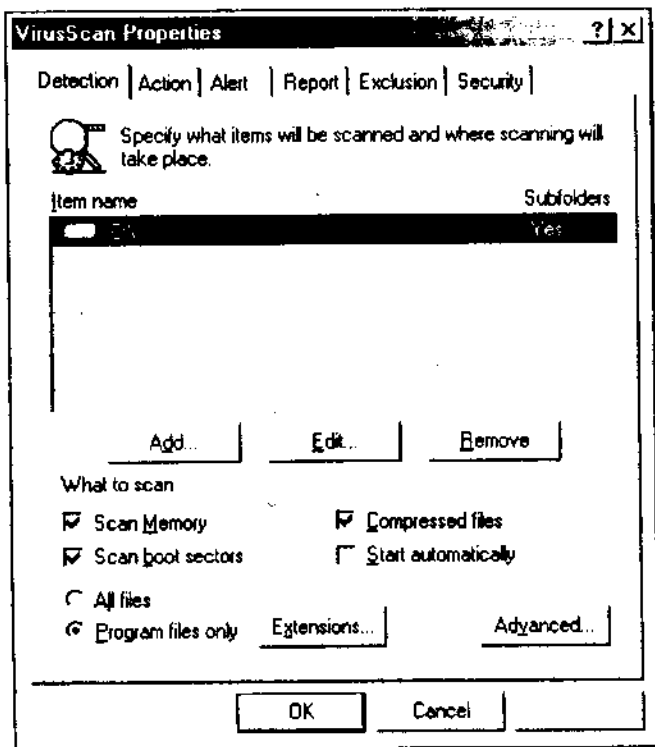
Nếu bạn chạy tác vụ trong chế độ quét bình thường, nó sẽ hiển thị kết quả của hoạt động quét và cho phép bạn loại bỏ bất kỳ virus mà nó đã tìm thấy, nếu bạn chưa xác lập nó để loại bỏ chúng một cách tự động. Sau đó bạn có thể chạy lại

tác vụ ngay lập tức, nếu bạn muốn.

Vào lúc này, bạn đã có đủ thông tin để tạo tác vụ, nhưng bạn chưa chọn các tùy chọn chương trình hay lập thời biểu để chạy nó. Bạn có thể:

- ❖ Nhấp Configure để xác lập các đặc tính cho tác vụ này.

Thao tác này sẽ mở hộp thoại VirusScan Properties. Ở đây, bạn có thể cho trình ứng dụng VirusScan biết nơi mà vùng cần tìm virus trong suốt hoạt động này, cách phản hồi đối với bất kỳ virus nào mà nó tìm thấy, cách thông báo cho bạn khi nó tìm thấy một virus, thông tin nào cần ghi trong activity log, những hạng mục nào cần loại ra khỏi các tác vụ quét, và có bảo vệ các tùy chọn cấu hình mà bạn đã xác lập cho tác vụ hay không. Để tìm hiểu cách xác lập các tùy chọn này.



- ❖ Nhấp Run Now để chạy tác vụ này ngay lập tức. Tác vụ sẽ chạy với các tùy chọn cấu hình mặc định hoặc các tùy chọn cấu hình mà bạn đã xác định cho nó. Sau đây là những gì xảy ra khi bạn nhấp vào nút này:

Nếu bạn đã chọn một tác vụ quét mà bạn đã xác lập để khởi động tự động, tác vụ sẽ chạy ngay lập tức. Để điều này xảy ra, bạn phải đã chọn hộp kiểm Start Automatically trong hộp thoại VirusScan Properties. Để xem hộp kiểm này, hãy nhấp Configure nằm ở ngay bên trái, sau đó xác định hộp kiểm trong vùng What to Scan trong trang đặc tính Detection.

Nếu bạn đã chọn một tác vụ quét mà bạn chưa xác lập để khởi động tự động, cửa sổ trình ứng dụng VirusScan sẽ xuất hiện. Nhấp Scan Now trong cửa sổ này để chạy tác vụ.

- ❖ Nhấp Apply để lưu các thay đổi mà không phải đóng hộp thoại Task Properties, sau đó nhấp nhấn Schedule. Để tìm hiểu cách xác lập một thời biểu cho tác vụ, hãy nhấp here:.
- ❖ Nhấp OK để lưu các thay đổi của bạn và trở lại cửa sổ VirusScan Console. Bạn sẽ cần xác lập một thời biểu cho tác vụ để chạy nó.

Để thực hiện điều này, hãy chọn tác vụ từ danh sách trong cửa sổ Console, sau đó nhấp  để mở hộp thoại Task Properties.

- ❖ Nhấp Cancel để đóng hộp thoại mà không tạo tác vụ.

IX. Xác lập password cho các tác vụ đã lập thời biểu

Bạn có thể bảo vệ các tác vụ AutoUpgrade, AutoUpdate, các tác vụ VirusScan mặc định, hay bất kỳ các tác vụ nào mà bạn tạo bằng một password để ngăn chặn sự thay đổi khi không được phép.

Để xác lập một password cho một tác vụ đã lập thời biểu, bạn có thể:

- ❖ Chọn một tác vụ từ danh sách hiển thị trong cửa sổ Console, sau đó chọn Password Protect Task từ menu Task.
- ❖ Nhấp đúp vào một trong các tác vụ được liệt kê, sau đó chọn hộp kiểm Password protect this task trong hộp thoại Task Properties.

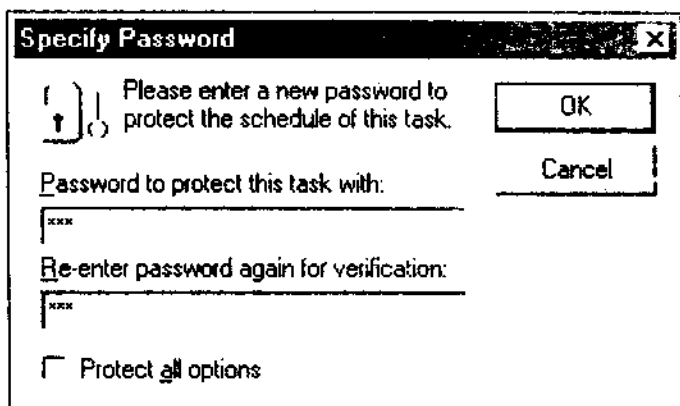
Nếu bạn chưa nhập password cho tác vụ này, mỗi tùy chọn sẽ mở hộp thoại Specify Password. Nếu bạn đã xác lập một password cho tác vụ này và muốn thay đổi nó, bạn sẽ nhìn thấy hộp thoại Change Password.

Thực hiện các bước sau đây:

1. Nhập một password duy nhất vào hộp text được cho.

Bạn có thể nhập tối đa đến 20 ký tự. Nhớ chọn một password dễ nhớ. Nếu bạn muốn thay đổi một password hiện có, hãy nhập password mà bạn vừa sử dụng để bảo vệ tác vụ này trong hộp text đầu tiên, sau đó nhập password mới mà bạn muốn sử dụng trong hộp text kế tiếp. VirusScan Console sẽ không cho phép bạn thay đổi một password hiện có nếu chưa xác nhận việc bạn biết password đó.

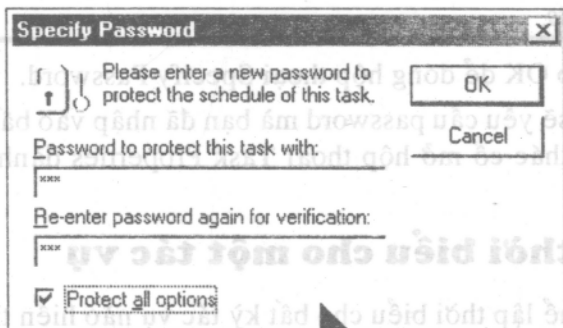
2. Nhập lại password một cách chính xác như bạn đã gõ nhập nó trong hộp text trước.



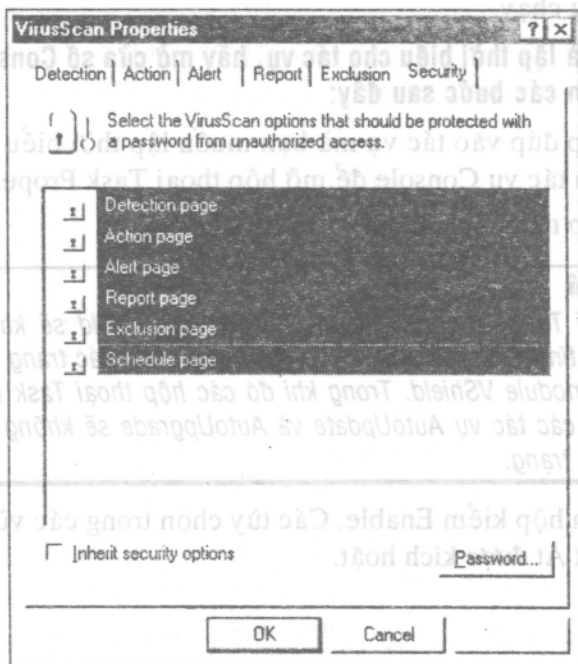
The image shows a Windows-style dialog box titled "Specify Password". It contains the following elements:

- A message: "Please enter a new password to protect the schedule of this task."
- Two "OK" and "Cancel" buttons on the right.
- A label "Password to protect this task with:" followed by a text input field containing "xxx".
- A label "Re-enter password again for verification:" followed by a text input field containing "xxx".
- A checkbox at the bottom labeled "Protect all options", which is currently unchecked.

3. Chọn hộp kiểm Protect all options để bảo vệ tất cả các tùy chọn mà bạn xác lập cho tác vụ này.



Thao tác này ngay lập tức sẽ khóa tất cả các trang đặc tính dành cho tác vụ trong trang Security trong hộp thoại VirusScan Properties. Việc xóa chọn hộp kiểm này cho phép bạn nhấp vào nhãn Security, sau đó chọn các trang đặc tính riêng lẻ mà bạn muốn bảo vệ.



Ghi chú

Tùy chọn này không có sẵn đối với các tác vụ AutoUpgrade và AutoUpdate.

4. Nhấp OK để đóng hộp thoại Specify Password.

Console sẽ yêu cầu password mà bạn đã nhập vào bất kỳ khi nào một người khác cố mở hộp thoại Task Properties dành cho tác vụ này.

X. Lập thời biểu cho một tác vụ

Bạn có thể lập thời biểu cho bất kỳ tác vụ nào hiển thị trong cửa sổ VirusScan Console, ngoại trừ tác vụ VShield, vốn chạy liên tục kể từ khi bạn khởi động máy tính hoặc ngay sau khi bạn tự khởi động tác vụ.

Để tác vụ chạy, bạn phải bật nó và lập một thời biểu cho nó. Bạn cũng phải bảo đảm VirusScan Console đang hoạt động vào lúc bạn muốn tác vụ chạy.

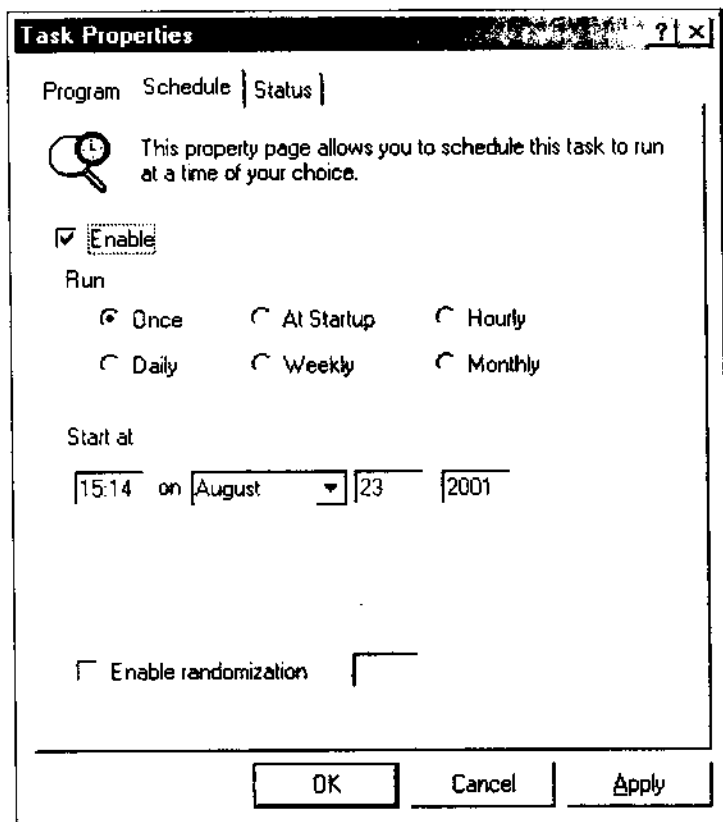
Để bật và lập thời biểu cho tác vụ, hãy mở cửa sổ Console, sau đó thực hiện các bước sau đây:

1. Nhấp đúp vào tác vụ mà bạn muốn lập thời biểu trong danh sách tác vụ Console để mở hộp thoại Task Properties.
2. Nhấp nhấn Schedule.

Ghi chú

Hộp thoại Task Properties dành cho tác vụ VShield sẽ không chứa trang đặc tính Schedule - thay vào đó, nó sẽ chứa các trạng tình trạng của mỗi module VShield. Trong khi đó các hộp thoại Task Properties dành cho các tác vụ AutoUpdate và AutoUpgrade sẽ không chứa các trang tình trạng.

3. Chọn hộp kiểm Enable. Các tùy chọn trong các vùng Run và Start At được kích hoạt.



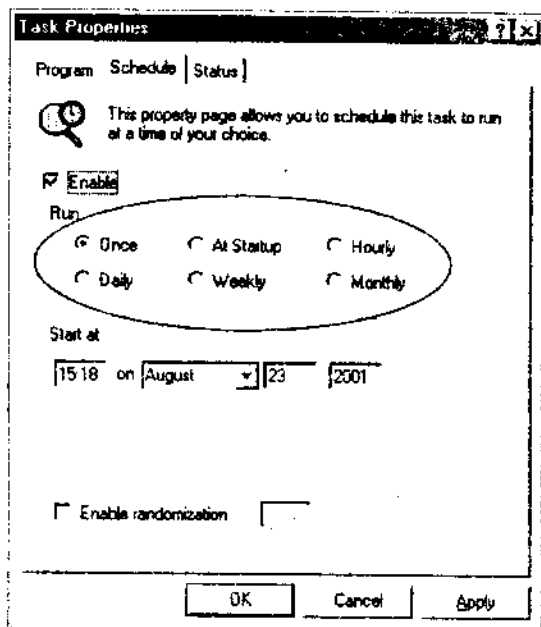
4. Chỉ định bạn muốn tác vụ chạy thường xuyên như thế nào trong vùng Run.

Phụ thuộc vào thời khoảng mà bạn chọn, vùng Start At cung cấp cho bạn một tập hợp các tùy chọn khác để lập thời biểu cho tác vụ. Các tùy chọn bao gồm:

- ❖ **Once.** Tùy chọn này chạy tác vụ một lần đúng vào ngày và giờ mà bạn chỉ định. Nhập thời gian vào hộp text ở gần bên trái nhất trong vùng Start At, sau đó chọn một tháng từ danh sách ở bên phải. Kế tiếp, hãy nhập ngày tháng và năm trong các hộp text được cho.
- ❖ **Daily.** Tùy chọn này chạy tác vụ hằng ngày vào thời điểm mà bạn chỉ định. Hãy nhập thời gian vào hộp text được cho,

sau đó chọn các hộp kiểm trong vùng Start At mà bạn muốn các tác vụ hàng ngày.

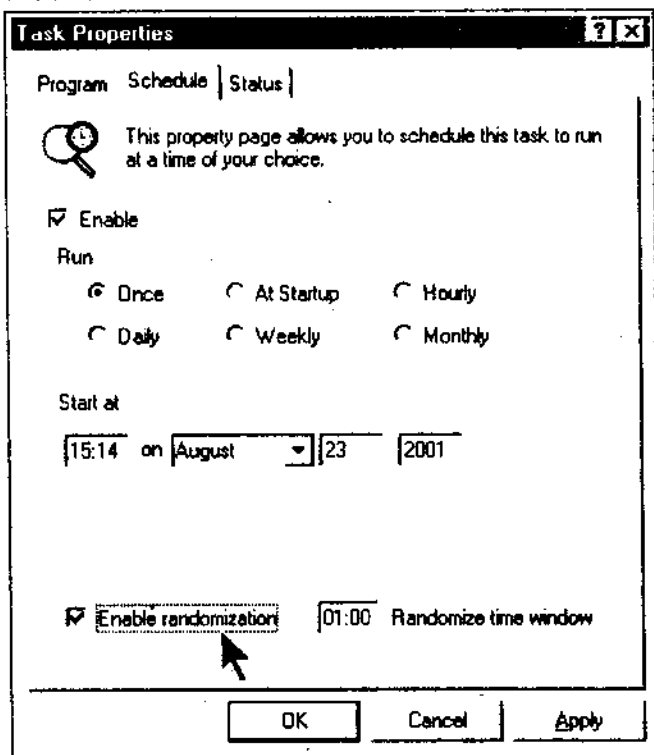
- ❖ **At Startup.** Chọn hộp kiểm này để chạy tác vụ một lần mỗi khi bạn khởi động máy tính và VirusScan Console. Chỉ định số giờ và số phút mà bạn muốn Console chờ trước khi nó chạy tác vụ. Bạn không thể ngẫu nhiên hóa thời biểu này.
- ❖ **Weekly.** Tùy chọn này chạy tác vụ mỗi tuần một lần vào ngày và giờ mà bạn chỉ định. Hãy nhập thời gian vào hộp text được cho, sau đó chọn ngày từ danh sách ở bên phải.
- ❖ **Hourly.** Tùy chọn này chạy tác vụ mỗi giờ một lần ngay sau khi bạn bật máy tính và Console đang chạy. Chỉ định số phút mà Console sẽ chờ sau mỗi giờ trong hộp text được cho để chạy tác vụ.
- ❖ **Monthly.** Tùy chọn này chạy tác vụ mỗi tháng một lần vào ngày và giờ mà bạn chỉ định. Nhập thời gian vào hộp text ở gần bên trái nhất, sau đó nhập ngày trong tháng mà bạn muốn tác vụ chạy vào ngày đó.



Ghi chú

Hãy nhập thời gian dựa vào đồng hồ 24 giờ. Nếu bạn muốn tác vụ chạy vào lúc 9 giờ 30 tối, hãy nhập 21:30.

5. Để tác vụ chạy trong một thời khoảng ngẫu nhiên mà bạn xác lập, hãy chọn hộp kiểm Enable randomization, sau đó nhập một thời khoảng lên đến 8 giờ vào hộp text Randomize time window.



Trừ khi bạn đã xác lập tác vụ này để chạy vào lúc khởi động, bạn có thể sử dụng tính năng này để giảm bớt sự lưu thông và các chi phí khác của hệ thống mà có thể phát sinh do có nhiều máy tính chạy các hoạt động quét hay cập nhật cùng lúc. Tác vụ sẽ chạy vào một thời điểm ngẫu nhiên trong “cửa sổ” thời gian mà bạn chỉ định. Cửa sổ này tập trung vào thời gian mà

bạn đã lập để chạy tác vụ. Chẳng hạn, nếu bạn xác lập tác vụ này để chạy hàng ngày vào lúc 15:00, thì có nghĩa là bạn đã chọn Enable randomization và đã chỉ định một cửa sổ thời gian là một giờ, tác vụ sẽ chạy vào bất kỳ thời điểm nào trong thời khoảng giữa 14:30 và 15:30. Bạn có thể xác lập một cửa sổ thời gian lên đến 480 phút, hoặc tám giờ.

6. Kế tiếp, bạn có thể:

- ❖ Nhấp Apply để lưu các thay đổi mà không phải đóng hộp thoại Task Properties. Bạn có thể nhấp nhấn Status để xem một bảng tóm tắt về các thông tin thống kê dành cho tác vụ này.
- ❖ Nhấp OK để lưu các thay đổi và trở lại cửa sổ VirusScan Console.
- ❖ Nhấp Cancel để đóng hộp thoại mà không tạo tác vụ.

Ghi chú

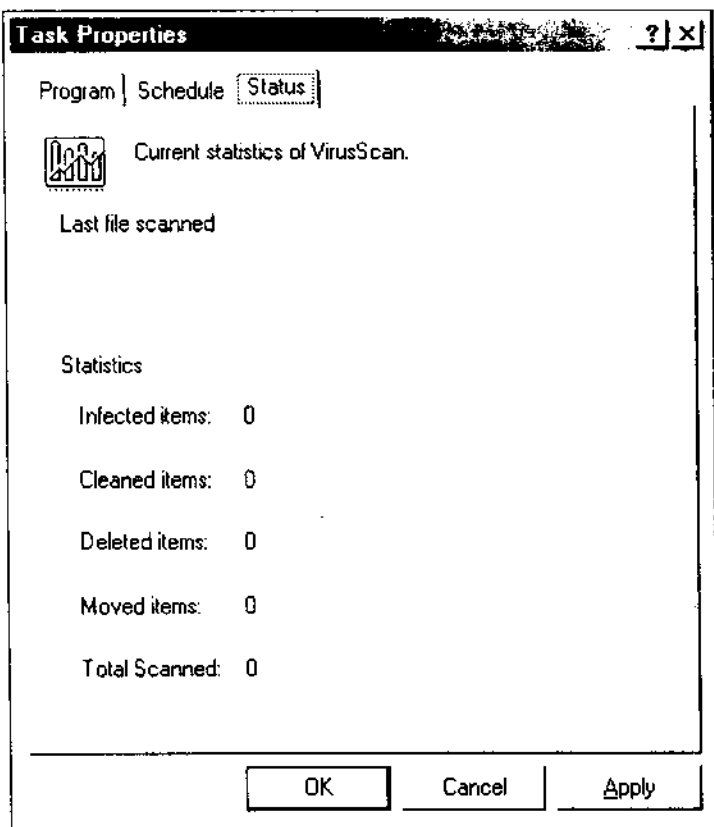
Để khởi động tác vụ, máy tính của bạn phải đang hoạt động và VirusScan Console phải đang chạy. Nếu máy tính của bạn không đang hoạt động hoặc Console không đang chạy vào lúc tác vụ khởi động, tác vụ sẽ khởi động vào thời điểm kế tiếp đã được lập trong thời biểu. Bạn có thể thu nhỏ Console để nó xuất hiện ở dạng một biểu tượng trong thanh tác vụ Windows. Nếu bạn dự định nhờ phần mềm VirusScan chạy một tác vụ quét trên một máy tính khi bạn hay một người nào đó vắng mặt, bạn cũng phải cấu hình chương trình để khởi động hoạt động quét một cách tự động. Để tìm hiểu cách thực hiện điều này, hãy nhấp [here](#).

XI. Xem thông tin về tình trạng tác vụ

Cửa sổ VirusScan Console tóm tắt thời gian và ngày tháng mà các tác vụ của bạn đã chạy vào lần sau cùng, thời gian và ngày tháng mà bạn đã lập thời biểu để chúng khởi động lại - hãy tìm thông tin này ở bên phải của mỗi tác vụ được liệt kê. Bạn cũng có thể xem một bản tóm tắt về số lượng file mà mỗi tác vụ đã quét, nó đã tìm thấy bất kỳ tác nhân nào nguy hiểm hay chưa, và các hành động mà nó đã thực hiện.

Để xem kết quả của tác vụ, hãy thực hiện các bước sau đây:

1. Nhấp đúp vào một trong các tác vụ được liệt kê trong cửa sổ Console, hoặc chọn một tác vụ, và sau đó nhấp  trong thanh công cụ Console.
Hộp thoại Task Properties sẽ xuất hiện.
2. Nhấp vào nhãn Status. Nếu bạn nhấp đúp vào tác vụ VShield để đến hộp thoại này, bạn có thể nhấp vào bất kỳ một trong các trang module VShield để xem các kết quả của tác vụ.



Trang tình trạng sẽ liệt kê các kết quả của hoạt động quét sau cùng mà tác vụ này đã điều khiển, và tên của file sau

cùng mà nó đã quét. Để xem một phần mô tả ngắn gọn của mỗi hạng mục xuất hiện trong trang này, hãy nhấp phải vào một hình hay nhãn, sau đó chọn What's This? từ menu tắt, hoặc nhấp nút ? ở góc phía trên bên phải của hộp thoại, sau đó nhấp vào hạng mục mà bạn muốn xem nội dung mô tả của nó.

3. Nhấp OK hoặc Cancel để đóng hộp thoại Task Properties.

Bài 9

TÌM HIỂU PHẦN MỞ RỘNG E-MAIL SCAN

Phần mềm VirusScan cung cấp cho bạn hai phương pháp bổ sung để bảo vệ hệ thống e-mail Microsoft Exchange hoặc Outlook.

- ❖ VShield scanner có một module E-Mail Scan chạy các hoạt động quét liên tục trong nền trên e-mail khi nó đến server.
- ❖ Phần mở rộng E-Mail Scan cho phép bạn quét hộp thư (mail-box) của bạn trên server Exchange theo khả năng sáng tạo của bạn, và vào những lúc tiện lợi cho bạn.

Một cấu trúc plug-in cung cấp cho bạn sự truy cập vào phần mở rộng E-Mail Scan trực tiếp từ trong trình ứng dụng client Exchange hay Outlook.

I. Khi nào và tại sao bạn phải sử dụng phần mở rộng E-Mail Scan

Phần lớn virus lây lan nhanh nhất qua e-mail. E-mail cung cấp một môi trường mà những người diệt virus có thể sử dụng để phân phối các file đính kèm bị nhiễm, họ thường lôi kéo người sử dụng vào việc mở và kích hoạt chúng. Các virus mới hơn, chẳng hạn như VBS/BUBBLEBOY, thậm chí có thể hoạt động ngay cả khi người sử dụng chưa mở hay đọc thông báo e-mail.

Các e-mail client Microsoft Exchange và Outlook rất dễ bị nhiễm virus thuộc loại này do chúng có các tính năng chuyển dịch script và macro mạnh. Đối với phần còn lại của bộ trình ứng dụng Microsoft Office, phần mềm client Exchange sử dụng nhiều macro, text đã được

đánh dấu, các lệnh script, và các tính năng tương tự, và virus có thể xâm nhập vào một cách dễ dàng.

Sử dụng module VShield E-Mail Scan để chạy các hoạt động quét trong nền trên hệ hống e-mail và để duy trì một mức độ nhất định giữa các hoạt động quét mà bạn chạy với phần mở rộng E-Mail Scan. Trong phần lớn các trường hợp, điều này sẽ bảo đảm tính toàn vẹn cho hệ thống của bạn.

Nếu bạn có một backlog lớn dành cho thư trên server mà bạn chưa quét virus, nếu bạn ngắt nối kết với server Exchange, hoặc nếu bạn ngưng module E-Mail Scan vào bất kỳ lúc nào, bạn nên sử dụng phần mở rộng E-Mail Scan để quét mailbox của mình nhằm bảo đảm tính toàn vẹn cho hệ thống. Virus vẫn có thể tồn tại trong các thông báo e-mail cũ được chứa trên server ngay trong các thông báo e-mail đến trong suốt khoảng thời gian bạn ngắt nối kết với hệ thống e-mail.

Các biện pháp phòng chống virus tốt là thực hiện đầy đủ và điều đặn các hoạt động quét trên mailbox của bạn, bởi vì:

- ❖ Module VShield E-Mail Scan tìm mã virus khi e-mail của bạn đến server, hoặc khi các file đính kèm khả thi chạy sau khi chúng đã tải đến hệ thống. Tuy nhiên, phần mở rộng E-Mail Scan có thể quét e-mail cũ trên server và module E-Mail Scan không nhìn thấy, tìm virus trong e-mail đến giữa những lần bạn nối kết với server Exchange, hoặc có thể quét mailbox nếu bạn đã ngắt tạm thời module VShield E-Mail Scan.
- ❖ Sự phòng chống virus đều đặn luôn luôn bảo đảm sự an toàn cho máy tính. Với các nối kết e-mail nhanh giữa phần mềm client mạnh, việc vận hành bởi web, được tạo script, virus lây nhiễm chỉ trong một vài giây, thậm chí ngay trước khi bạn mở mail. Các hoạt động web đều đặn thường có thể giúp ngăn chặn việc virus lây lan hay gây ra bất kỳ nguy hại nào.

II. Khởi động phần mở rộng E-Mail Scan

Để sử dụng phần mở rộng E-Mail Scan, bạn phải cài đặt phần mềm VirusScan với một tiến trình cài đặt Custom hòa trộn thành phần E-Mail Scan để cài đặt.

Để sử dụng phần mở rộng E-Mail Scan với các xác lập mặc định của nó:

1. Khởi động phần mềm client Microsoft Exchange hoặc Microsoft Outlook.
2. Nối kết với mail server như bình thường.
3. Chọn Scan for Viruses từ menu Tool trong trình ứng dụng client, hoặc nhấp () trong thanh công cụ Exchange hoặc Outlook.

Ghi chú

Nếu bạn sử dụng Microsoft Exchange 5.0, một giới hạn về cách chương trình cập nhật thanh công cụ của nó sẽ ngăn chặn việc phần mở rộng và E-Mail Scan hiển thị các nút của nó ngay lập tức. Để bổ sung nút Scan for Viruses vào thanh công cụ, hãy chọn Customize Toolbar từ menu Tools, sau đó bổ sung các nút E-Mail Scan từ danh sách các nút có sẵn trong hộp thoại Customize Toolbar.

Ngay sau khi bạn đã khởi động nó, phần mở rộng E-Mail Scan ngay lập tức sẽ bắt đầu việc quét mailbox Exchange hay Outlook, và bất kỳ folder công cộng nào trên server mà bạn có sự truy cập vào đó. Để tìm hiểu các cấu hình phần mở rộng sao cho nó đáp ứng các nhu cầu của bạn tốt hơn, hãy nhấp [here](#):

III. Ngưng phần mở rộng E-Mail Scan

Bởi vì nó có chức năng như là một phần bổ sung vào e-mail client Microsoft Exchange hoặc Outlook nên phần mở rộng E-Mail Scan không đang chạy thật sự trừ khi nó đang ở giữa một hoạt động quét và đang tích cực tìm một virus trong mailbox Exchange của bạn.

Để ngưng một hoạt động quét đang diễn ra, bạn có thể:

❖ Nhấp 

Để tạm ngưng hoạt động, Hãy nhấp . Nhấp  để bắt đầu lại nó.

❖ Nhấp Stop khi tùy chọn đó xuất hiện trong một thông tin cảnh báo đã tìm thấy virus. Tùy chọn này xuất hiện chỉ khi bạn đã yêu cầu phần mở rộng hiển thị nó.

IV. Các file phụ thuộc và liên quan dành cho phần mở rộng E-Mail Scan

Phần mở rộng E-Mail Scan chạy ở dạng một phần bổ sung vào hệ thống e-mail MAP. Nếu bạn sử dụng client Microsoft Exchange hay Outlook, phần mở rộng này sẽ tải vào trình ứng dụng client và xuất hiện ở dạng các hạng mục menu trong menu Tools và dưới dạng các nút trong thanh công cụ trình ứng dụng. Bạn có thể sử dụng phần mở rộng này để chạy các hoạt động quét bất kỳ khi nào bạn muốn. Phần mở rộng này cần nhiều file hỗ trợ để thực hiện chức năng, bao gồm cả một số file liên quan đến công cụ quét McAfee. Bảng sau đây liệt kê phần mở rộng và các file liên quan:

Các file chương trình

File	Chức năng	Vị trí
SCANEMAIL.DLL	Quét e-mail trên server Microsoft Exchange hoặc hệ thống e-mail MAPI khác. File này chạy ở dạng phần mở rộng Exchange hay Outlook vốn tải vào trình ứng dụng e-mail client. File tương tự này cung cấp các dịch vụ quét trong module VShield E-Mail	C:\Program Files\ McAfee VirusScan\ VirusScan

Scan.

Các file phụ thuộc

Phần mở rộng E-Mail Scan cần các file này để chạy vào các thời điểm khác nhau, nhưng đây không phải là các file phần mở rộng, hoặc không dành riêng cho việc hỗ trợ phần mở rộng E-Mail Scan.

File	Chức năng	Vị trí
AVSYNMGR .EXE	Dịch vụ quản lý VirusScan. Khởi tạo, khởi động và ngưng tất cả các thành phần và các dịch vụ VirusScan. Phải chạy để bật tắt tất cả các thành phần VirusScan.	C:\Program Files\ McAfee VirusScan\ VirusScan
AVSYNCH.DLL	Điều khiển sự giao tiếp giữa các thành phần thông qua bộ nhớ dùng chung.	C:\Program Files\ McAfee VirusScan\ VirusScan
SYNCUTIL.DLL	Chứa dữ liệu dùng chung giữa các thành phần.	C:\Program Files\ McAfee VirusScan\ VirusScan
VSUTIL.DLL	Cung cấp các tiện ích chung cho các thành phần.	C:\Program Files\ McAfee VirusScan\ VirusScan
AVSMCPA.CPL	VirusScan control panel applet.	C:\Windows\System or C:\Winnt\System 32
RESDLL.DLL	File nguồn tài nguyên dành cho thành phần VirusScan.	C:\Program Files \ Common Files\ McAfee VirusScan\ VirusScan\ McPal
MCSCAN32.DLL	File công cụ McAfee Scan	C:\Program Files \ Common Files\ McAfee VirusScan\ VirusScan\

		VirusScan Engine\ 4.0.xx
RWABS16.DLL	File hỗ trợ dành cho công cụ quét.	C:\Program Files \ Common Files\ McAfee VirusScan\ VirusScan Engine\ 4.0.xx
RWABS32.DLL	File hỗ trợ dành cho công cụ quét.	C:\Program Files \ Common Files\ McAfee VirusScan\ VirusScan Engine\ 4.0.xx
MESSAGES.DAT	File hỗ trợ dành cho công cụ quét. Cung cấp các thông báo dò tìm virus cho công cụ.	C:\Program Files \ Common Files\ McAfee VirusScan\ VirusScan Engine\ 4.0.xx

Các file tạm thời

Phần mở rộng E-Mail Scan và các file liên quan của nó sử dụng các file liệt kê trong bảng này là “các bản đồ bộ nhớ” để chứa các tùy chọn cấu hình đã sao chép từ phần đăng ký Windows theo chương trình chạy. Các file này bắt đầu với một kích cỡ file chuẩn và dữ liệu có thể, mở rộng hoặc thu nhỏ khi cần thiết để chứa dữ liệu cấu hình.

File	Chức năng	Vị trí
SYNC_MAP .MMF	File bản đồ bộ nhớ dành cho AVSYNCH.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
AVCONSOLE .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
DAV_CONS	File bản đồ bộ nhớ dành	C:\Program Files\

.MMF	cho SYNCUTIL.DLL	McAfee VirusScan\ VirusScan
DAV_EXCL .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
DAV_SCAN .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
DEXCLDEF .MFF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
DSCANDEF .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
DVS_EXCL .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
VSCANGEN .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
VSCANOAS .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
VSCANODS .MMF	File bản đồ bộ nhớ dành cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan

V. Cấu hình phần mở rộng E-Mail Scan

Để phần mở rộng E-Mail Scan bảo vệ Microsoft Exchange hoặc MAPI Inbox, bạn phải cho nó biết:

- ❖ Bạn muốn nó quét vùng nội dung nào
- ❖ Bạn muốn nó thực hiện điều gì khi nó tìm thấy một virus

- ❖ Nó sẽ cho bạn biết bằng cách nào khi nó tìm thấy một virus
- ❖ Bạn có muốn theo dõi các hành động của nó hay không

Một loạt các trang đặc tính trong hộp thoại E-Mail Scan Properties điều khiển các tùy chọn dành cho mỗi hoạt động quét bạn chạy. Bạn có thể lần lượt nhấp vào mỗi nhãn để chọn các tùy chọn cho phần mở rộng sử dụng để quét e-mail của bạn.

Để hiển thị hộp thoại này, hãy thực hiện các bước sau đây:

1. Khởi động client Microsoft Exchange hoặc Outlook và nối kết với e-mail server.

Ghi chú

Nếu bạn đã vào domain mạng điều khiển e-mail server của bạn, bạn có thể không cần nối kết trực tiếp với e-mail server - thêm vào đó, bạn chỉ cần khởi động Exchange hoặc Outlook. Hãy gặp người điều hành mạng để tìm hiểu các yêu cầu nối kết vào server của bạn.

2. Chọn E-Mail Scan Properties từ menu Tools, hoặc nhấp  trong thanh công cụ dành cho trình ứng dụng client.

Hộp thoại E-Mail Scan Properties đã xuất hiện. Để xem diện mạo của hộp thoại này, hãy nhấp [here](#):

Hộp thoại này cung cấp cho bạn các tùy chọn cần thiết để quét e-mail Inbox. Nhấp vào các nút được liệt kê ở phía dưới để tìm hiểu cách chọn các tùy chọn trong mỗi trang đặc tính:

Choosing Detection options

Choosing Action options

Choosing Alert options

Choosing Report options

1. Chọn các tùy chọn Detection dành cho phần mở rộng E-Mail Scan

Khi lần đầu tiên bạn mở hộp thoại E-Mail Scan Properties để cấu hình một hoạt động quét, phần mở rộng E-Mail Scan cho rằng bạn muốn nó quét tất cả các thông báo trong mailbox Exchange của bạn,

quét tất cả các file đính kèm thông báo, quét các file đã nén, và quét chỉ các file dễ bị nhiễm virus.

Thật ra, phần mở rộng E-Mail Scan thực hiện quét ngay trên các thông báo e-mail, vì các file Microsoft Exchange có thể chuyển tải các macro đã nhúng, Các tag HTML (Hyper Text Markup Language) và các applet VBScript, tất cả chúng có thể là nơi ẩn náu của các virus riêng biệt.

Ghi chú

Phần mở rộng E-Mail Scan nối kết trực tiếp với mailbox trên mail server Microsoft Exchange để chạy các hoạt động quét của nó. Bạn cũng có thể quét bất kỳ folder công cụ nào mà bạn có sự truy cập vào đó, nhưng phần mở rộng không quét các thông báo được chứa trong các folder cá nhân Microsoft Outlook (Các file PST) hay các hạng mục lưu trữ. Tuy nhiên, các thành phần VirusScan khác sẽ quét các file .PST trong suốt các hoạt động quét đều đặn của chúng trừ khi bạn loại bỏ chúng.

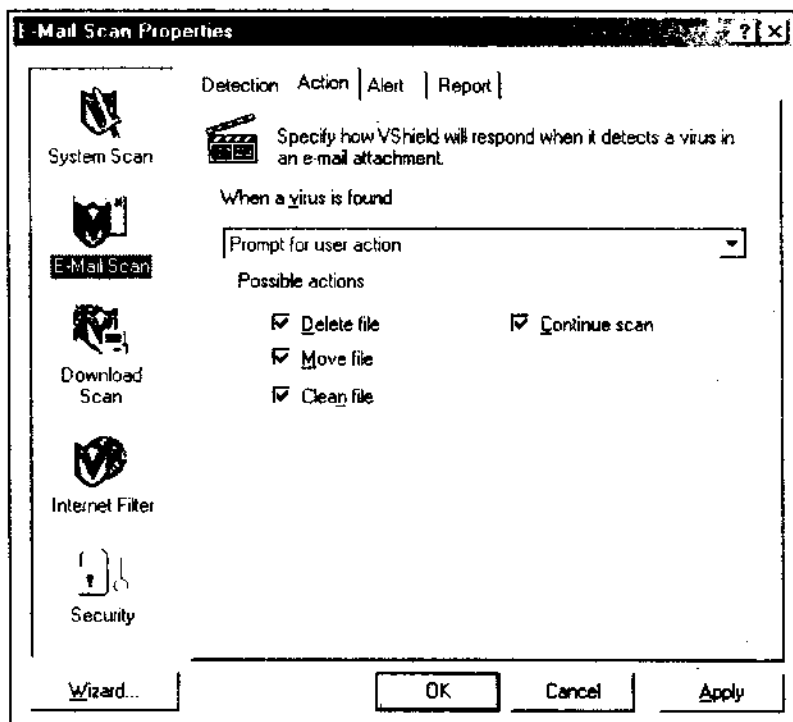
Để xác lập hay thay đổi các tùy chọn dành cho hoạt động quét này, hãy thực hiện các bước sau đây:

1. Chọn các thông báo e-mail mà bạn muốn phần mở rộng E-Mail Scan kiểm tra để tìm virus. Bạn có thể quét:
 - ❖ **All messages in the "Inbox" folder.** Nhấp nút này để nhờ phần mở rộng tìm virus trong tất cả các thông báo e-mail được chứa trong Microsoft Exchange hoặc Microsoft Outlook, dù bạn đã đọc chúng hay chưa.

Nếu Inbox của bạn có chứa nhiều thông báo, một hoạt động quét như thế có thể mất một lượng thời gian đáng kể. Tuy nhiên, nếu bạn đã cài đặt phần mở rộng E-Mail Scan sau khi bạn đã cài đặt và sử dụng hệ thống mail được một lúc, McAfee đề nghị bạn thực hiện ít nhất một hoạt động quét như thế thì bảo đảm các thông báo mail cũ hơn không có chứa virus.
 - ❖ **All highlighted messages.** Nhấp nút này để nhờ phần mở rộng tìm virus trong chỉ các thông báo e-mail mà bạn chọn

từ các thông báo được chứa trong Microsoft Exchange hay Microsoft Outlook Inbox.

2. Để giới hạn hoạt động quét này sao cho nó kiểm tra chỉ các thông báo chưa được đọc, hãy chọn hộp kiểm Scan unread messages only. Phụ thuộc vào việc bạn đã chọn tùy chọn nào ở bước 1, phần mở rộng sẽ quét tất cả thông báo chưa được đọc trong Inbox hoặc tất cả các thông báo chưa được đọc trong dãy mà bạn đã chọn.
3. Chỉ định các kiểu file nào mà bạn muốn phần mở rộng kiểm tra.
4. Kế tiếp, bạn có thể:
 - ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại E-Mail Scan Properties.
 - ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút sau đây để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại:
Action
Alert
Report
 - ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại E-Mail Scan Properties.



❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.

Ghi chú

Việc nhấp Cancel sẽ không undo bất kỳ thay đổi nào mà bạn đã lưu bằng cách nhấp Apply.

2. Chọn các tùy chọn Action dành cho phần mở rộng E-Mail Scan

Khi lần đầu tiên bạn tạo một tác vụ mới, phần mở rộng E-Mail Scan cho rằng bạn muốn nó hỏi bạn nó phải làm gì với một virus mà nó tìm thấy. Bạn có thể tiếp tục nhờ nó nhắc bạn về một tùy chọn phản hồi, hoặc bạn có thể nhờ nó tự động thực hiện một hành động mà bạn đã xác định trước.

Để xác lập hay thay đổi dành cho tác vụ này:

1. Chọn một trong các tùy chọn phản hồi sau đây từ danh sách

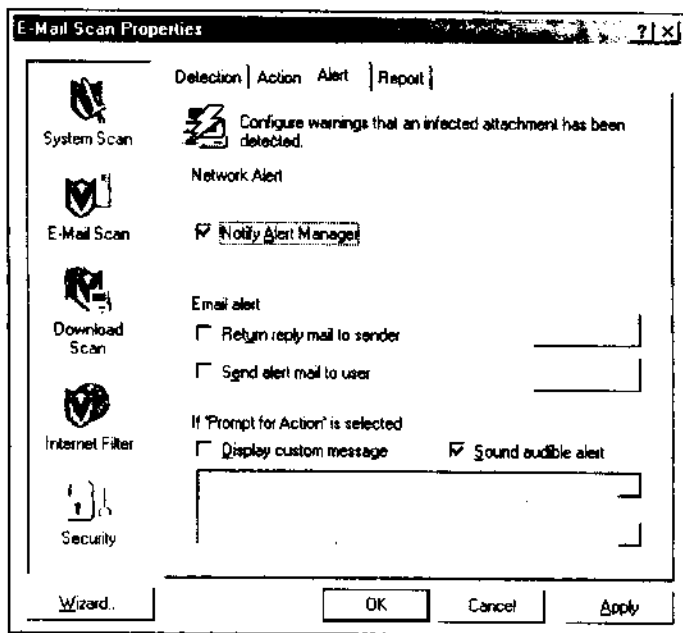
When a virus is found:

- ❖ Prompt for user action.
 - ❖ Move infected attachment automatically.
 - ❖ Clean infected attachment automatically.
 - ❖ Delete infected attachment automatically.
 - ❖ Continue scanning.
2. Kế tiếp, bạn có thể:
- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại E-Mail Scan Properties.
 - ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút sau đây để tìm cách cấu hình các tùy chọn trong các trang đặc tính còn lại:

Detection

Alert

Report



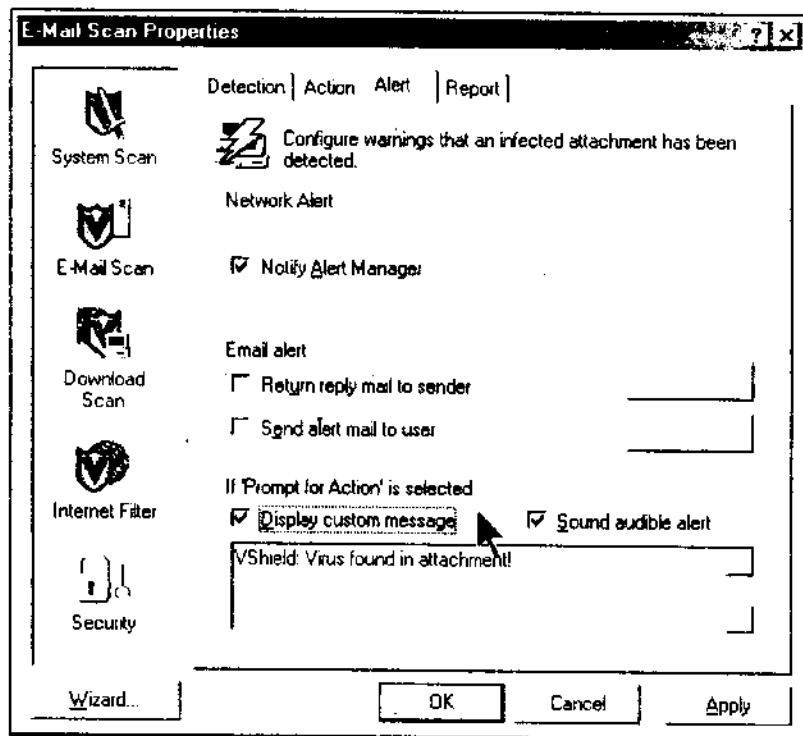
- ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại E-Mail Scan Properties.
- ❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.

3. Chọn các tùy chọn Alert dành cho phần mở rộng E-Mail Scan

Ngay sau khi bạn cấu hình nó với các tùy chọn phản hồi mà bạn muốn, bạn có thể để cho phần mở rộng E-Mail Scan tìm và loại bỏ virus ra khỏi mailbox Exchange một cách tự động, khi nó tìm thấy chúng. Tuy nhiên, để phần mở rộng thông báo cho bạn biết ngay khi nó tìm thấy một virus để bạn có thể thực hiện hành động thích hợp, hãy cấu hình để nó gửi cho bạn một thông tin cảnh báo.

Thực hiện các bước sau đây:

1. Chọn hộp kiểm Notify Alert Manager để nhờ phần mở rộng gửi thông tin cảnh báo đến Alert Manager để phân phối.
2. Để gửi các thông tin cảnh báo qua e-mail đến người đã gửi cho bạn file đính kèm e-mail bị nhiễm virus hay đến những người nhận khác, hãy chọn một hoặc cả hai hộp kiểm trong vùng E-mail Alert, sau đó nhấp vào nút Configure tương ứng để soạn một thông báo cần gửi.
3. Chọn hộp kiểm Sound audible alert để nhờ phần mở rộng phát ra tiếng beep khi nó tìm thấy một file bị nhiễm.
4. Chọn hộp kiểm Display custom message để nhờ phần mở rộng bổ sung một thông báo tùy biến vào hộp alert mà nó hiển thị khi nó tìm thấy một file bị nhiễm.
5. Nhập thông báo mà bạn muốn module hiển thị trong hộp text được cho. Bạn có thể nhập tối đa đến 250 ký tự.



6. Kế tiếp, bạn có thể:

- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại E-Mail Scan Properties.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút sau đây để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại.

Detection

Action

Report

- ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại E-Mail Scan Properties.
- ❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi.

4. Chọn các tùy chọn Report dành cho phần mở rộng E-Mail Scan

Phần mở rộng E-Mail Scan liệt kê các xác lập hiện hành và tóm tắt tất cả các hành động mà nó thực hiện trong suốt mỗi tác vụ quét trong một log file được gọi là MAILSCAN.TXT. Bạn có thể nhờ phần mở rộng ghi log của nó vào file này, hoặc bạn có thể sử dụng bất kỳ bộ chỉnh sửa text nào để tạo một file text cho nó sử dụng. Sau đó bạn có thể mở và in log file để xem lại từ bộ chỉnh sửa text.

Để quyết định phần mở rộng sẽ ghi lại những tài liệu nào và kích cỡ của file bao nhiêu, hãy thực hiện các bước sau đây:

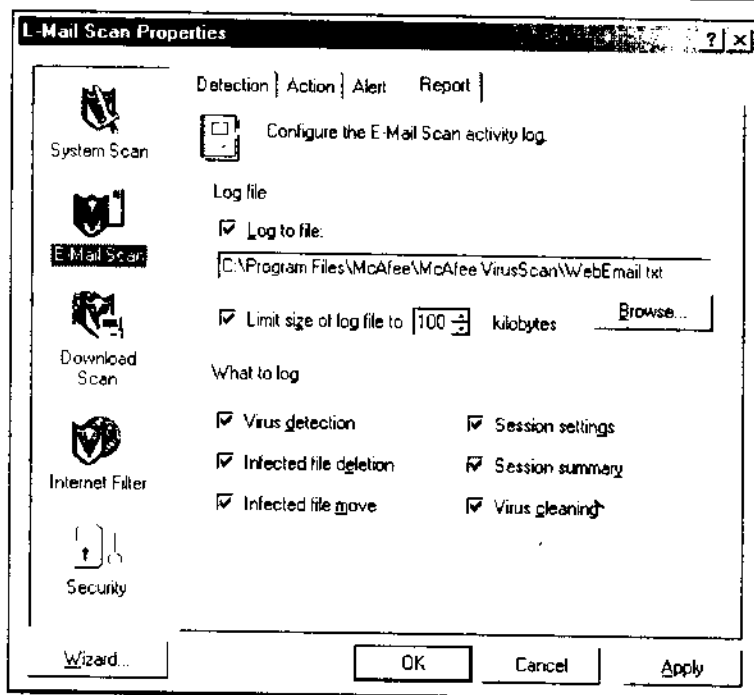
1. Chọn hộp kiểm Log to file

Theo mặc định, phần mở rộng ghi thông tin log vào file MAILSCAN.TXT trong thư mục chương trình VirusScan. Bạn có thể nhập một tên khác vào hộp text được cho, hoặc nhấp Browse để xác định một file thích hợp ở nơi khác trên đĩa cứng hay trên mạng. Bạn có thể sử dụng một file khác nhưng bạn phải có file text này. Phần mở rộng sẽ không tạo một file mới.

Ghi chú

Nếu bạn chọn một vị trí khác cho log file riêng trên hệ thống Windows NT Workstation v4.0 hoặc Windows 2000 Professional, hãy xác nhận rằng bạn chọn một vị trí mà bạn có sự truy cập ở cấp độ người dùng. Bởi vì phần mở rộng E-Mail Scan chạy với các quyền truy cập tương tự giống như chương trình e-mail client, nên nó không thể ghi vào log file này một cách chính xác nếu file tồn tại trong một vị trí đòi hỏi phải có các quyền truy cập Administrator, và bạn đã nối kết ở dạng một user để chạy chương trình e-mail client. Thêm vào đó, phần mở rộng E-Mail Scan sẽ cung cấp cho bạn một thông báo "Activity Log Access Error" khi nó tìm thấy một virus.

2. Chọn hộp kiểm Limit size of log file để giảm thiểu kích cỡ của log file. Nếu bạn không chọn hộp kiểm này, log file có thể tăng đến kích cỡ mà khoảng trống đĩa của bạn cho phép.
3. Nhập một giá trị cho kích cỡ file, theo đơn vị kilobyte, vào một text được cho.



4. Chọn các hộp kiểm tương ứng với thông tin mà bạn muốn phần mở rộng ghi lại.

5. Kế tiếp, bạn có thể :

- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không phải đóng hộp thoại E-Mail Scan Properties.
- ❖ Chọn các tùy chọn cấu hình khác. Nhấp vào bất kỳ một trong các nút sau đây để tìm hiểu cách cấu hình các tùy chọn trong các trang đặc tính còn lại:

Detection

Action

Alert

- ❖ Nhấp OK để lưu các tùy chọn cấu hình và đóng hộp thoại E-Mail Scan Properties.
- ❖ Nhấp Cancel để đóng hộp thoại mà không lưu các thay đổi

Bài 10

TÌM HIỂU TIỆN ÍCH ALERT MANAGER

Tất cả phần mềm chống virus McAfee bao gồm nhiều phương pháp để cảnh báo bạn khi nó tìm thấy một virus hoặc phần mềm nguy hiểm khác. Các phương pháp bao gồm:

- ❖ Các cảnh báo mang tính đồ họa và chế độ màn hình vốn xuất hiện trên máy tính cục bộ của bạn, thường với các tùy chọn phản hồi.
- ❖ Hệ thống các tiếng beep và các thông tin tùy biến mà bạn có thể biên soạn.
- ❖ Các thông tin e-mail gửi dưới dạng khi trả lời đến những người mà họ đã gửi cho bạn các hạng mục bị nhiễm, hoặc dưới dạng các cảnh báo đến những người mà bạn nhận một hạng mục bị nhiễm.
- ❖ Các log file vốn ghi các hoạt động hợp thành virus, bao gồm sự phát hiện ra virus và các event phản hồi.
- ❖ Các màn hình hiển thị bảng tóm tắt và số liệu thống kê vốn cập nhật sự phát hiện và các event phản hồi.

Nhiều phương pháp cảnh báo bạn trừ phi bạn đang sử dụng máy tính và xem lúc một hoạt động quét thực hiện. Nếu bạn quản lý một mạng của workstation mà bạn muốn yên tâm, tuy nhiên, bạn thường cần một phương pháp mà sẽ báo cho bạn về một sự nhiễm nếu bạn ở tại bất kỳ workstation khác trên mạng của bạn, hoặc ngay cả nếu bạn không nối kết với mạng nào cả. Bạn cũng có thể cần một phương pháp để tập hợp và quản lý các thông tin cảnh báo từ tất cả các mạng

khác trong một nơi lưu trữ chính để bạn có thể phản hồi bất cứ khi nào workstation phát hiện một file bị nhiễm.

McAfee cung cấp phần mềm server Alert Manager khi cần. Phần mềm cho phép bạn tập hợp bộ truy cập và tiến trình các thông tin cảnh báo, các thiết kế ưu tiên và các thông tin tùy biến đến các thông tin này, và chỉ định lên đến 11 phương pháp khác nhau để phân bổ chúng cho bạn hoặc cho những người khác. Bạn có thể cài đặt server Alert Manager này cùng với phần mềm Netshield, hoặc cài đặt riêng lẻ trên một máy tính mà bạn muốn sử dụng dưới dạng một điểm tập hợp cảnh báo.

Bạn có thể cài đặt nhiều server Alert Manager, một domain, có thể, hoặc một server trên mỗi máy trong một bộ server. Nếu bạn làm điều đó, bạn cũng có thể gửi các thông tin cảnh báo giữa các server Alert Manager và vì vậy đến các máy tính khác trên mạng của bạn hoặc đến các hệ thống thông báo được tập trung.

Phần mềm VirusScan dưới dạng một client Alert Manager

Phần mềm VirusScan làm việc như là một chương trình client liên quan đến phần mềm NetShield và một server Alert Manager. Nó có thể gửi (các event) cảnh báo bất cứ khi nào nó phát hiện một virus hoặc phần mềm nguy hiểm vào bất server Alert Manager mà bạn xác định. Server Alert Manager sau đó tạo lại các event này - và bất kỳ các event khác nó nhận từ các workstation khác - dưới dạng các thông tin cảnh báo, qua các phương pháp mà bạn hoặc các nhà quản lý hệ thống của bạn xác định về sự phân bổ cảnh báo. Phần mềm VirusScan có thể gửi các thông tin cảnh báo này bằng các file (.ALR) text đến một thư mục Centralized Alerting hiển thị đối với server Alert Manager. Server Alert Manager kiểm tra thư mục Centralized Alerting định kỳ, tìm các file .ALR mới, và phân bổ các thông tin cảnh báo từ bất kỳ file tìm thấy.

Ghi chú

McAfee lưu ý rằng bạn gửi các event cảnh báo trực tiếp đến một server Alert Manager hơn là Centralized Alerting, trừ khi cấu hình mạng của bạn không cho phép bạn sử dụng các server Alert Manager.

Server Alert Manager có thể làm việc cùng với phần mềm McAfee VirusScan Event Orchestrator để nối kết các thông tin cảnh báo vào trình ứng dụng McAfee VirusScan Magic HelpDesk và các tính năng khác.

Các thông báo Alert Manager cũng chứa nhiều dữ liệu phong phú hơn những thông báo được gửi qua Centralized Alerting. Việc sử dụng các bẫy SNMP cho Alert Manager sẽ thu thập nhiều thông tin về máy tính vốn tạo thông tin cảnh báo vào cấu hình phần mềm của nó.

Client VirusScan có thể bổ sung phương pháp có các cảnh báo đến Desktop Management Interface (DMI) cho phần mềm quản lý mạng chẳng hạn như Hewlett-Packard OpenView, để xử lý.

Cấu hình client Alert Manager

Phần mềm VirusScan bao hàm một tiện ích cấu hình client đơn giản vốn cho phép bạn chọn server Alert Manager mà bạn muốn nhận được các event cảnh báo, chỉ định một thư mục Centralized Alerting để nhận các thông tin cảnh báo và xác định giá trị số của các thông tin cảnh báo DMI mà bạn muốn gửi.

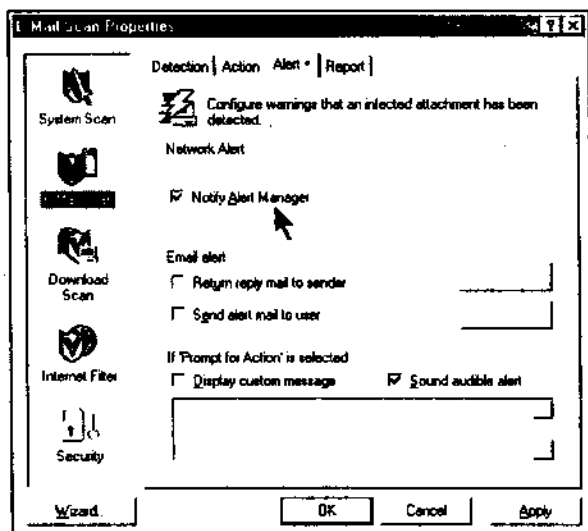
Để khởi động trình tiện ích này, hãy thực hiện các bước sau đây:

1. Nhấp Start trong tác vụ Windows, trở vào programs, sau đó trở vào McAfee VirusScan. Kế tiếp chọn VirusScan Alerting Configuration.

Trang Alert Manager Client Configuration xuất hiện.

2. Chọn phương pháp cảnh báo mà bạn muốn sử dụng.
3. Nhấp OK để lưu cấu hình và đóng hộp thoại.

Việc cài đặt một hệ thống cảnh báo hoàn chỉnh là một tiến trình gồm hai phần: Đầu tiên, bạn phải chạy trình tiện ích Alert Manager Client Configuration và trở nó sang đúng server Alert Manager hoặc vị trí Centralized Alerting. Kế tiếp, bạn phải xác minh rằng bạn đã chọn hộp kiểm Notify Alert Manager trong trang đặc tính VirusScan Advanced Alert trong trang Alert cho phần mở rộng E-mail Scan và trong các trang Alert cho mỗi module VShield mà bạn đã chạy.



Điều này yêu cầu mỗi thành phần VirusScan gửi một thông tin cảnh báo đến trình tiện ích client Alert Manager mỗi lần nó phát hiện một virus hay đối tượng có hại. Lần lượt trình tiện ích client truyền thông tin cảnh báo đến server Alert Manager mà bạn chỉ định. Nếu bạn không cài đặt phần mềm để tạo ra các thông tin cảnh báo ở vị trí đầu tiên, trình tiện ích client sẽ không có gì để truyền đến server Alert Manager để phân phối.

Để tìm hiểu thêm về trình tiện ích Alert Manager Client Configuration, hãy nhấp các nút bên dưới mỗi chủ điểm đã liệt kê:

1. Các file cấu hình client Alert Manager

Trình tiện ích cấu hình client Alert Manager yêu cầu các file sau đây để chạy:

File	Chức năng	Vị trí
ADSLOOKUP.DLL	File thư viện. Cho phép trình tiện ích server Alert Manager thông qua các dịch vụ Microsoft Active directory.	C:\Program Files\Common Files\McAfee VirusScan\McPal

AMG.MIF	Management Information File để sử dụng với phần mềm trình ứng dụng client Desktop Management Interface	C:\Program Files\Common Files\McAfee VirusScan \McPal
NAARCHIV.DLL	File thư viện dành cho các thủ tục nén dữ liệu	C:\Program Files\Common Files\McAfee VirusScan \McPal
NAEVENT.DLL	File thư viện. Điều khiển việc xử lý event từ phần mềm chống virus client desktop đến trình tiện ích Alert Manager và phần mềm McAfee ePolicy Orchestrator	C:\Program Files\Common Files\McAfee VirusScan\McPal
NAGUI32.DLL	File thư viện đồ họa dành cho các trình tiện ích VirusScan khác nhau	C:\Program Files\Common Files\McAfee VirusScan\McPal
NAKRNL32.DLL	File thư viện dành cho các các trình tiện ích VirusScan khác nhau	C:\Program Files\Common Files\McAfee VirusScan \McPal
NAUTIL32.DLL	File thư viện dành cho các trình tiện ích VirusScan khác nhau	C:\Program Files\Common Files\McAfee VirusScan \McPal

2. Cấu hình các cài đặt client Alert Manager

Để chọn và cấu hình một phương pháp cảnh báo, hãy thực hiện một trong các bước sau đây:

1. Hãy xác minh rằng hộp kiểm Disable Alerting được xóa. Điều này kích hoạt các tùy chọn còn lại trong hộp thoại này.

Chỉ chọn hộp kiểm này nếu bạn muốn trình tiện ích Alert Manager Client Configuration không truyền các thông tin cảnh báo từ phần mềm chống virus của bạn đến server Alert Manager hoặc đến phần mềm quản lý Desktop Management Interface (DMI).

Theo mặc định, hộp kiểm này được xóa. McAfee đề nghị bạn nên để trống hộp kiểm này để client truyền các thông tin cảnh báo đến server Alert Manager và đến phần mềm DMI của bạn.

Ghi chú

Nếu bạn sử dụng phần mềm McAfee ePolicy Orchestrator trong môi trường mạng, phần mềm VirusScan sẽ vẫn gửi các thông tin cảnh báo đến thành phần báo cáo ePolicy Orchestrator cho dù bạn có kích hoạt hoặc hủy kích hoạt tính năng cảnh báo ở đây hay không.

2. Xác định một đích cho các event cảnh báo thành phần VirusScan. Sau đây là các tùy chọn của bạn:

❖ **Enable Alert Manager alerting.** Nhấp nút này để gửi các event cảnh báo đến một server Alert Manager tại một vị trí nào đó trên mạng của bạn. Việc chọn tùy chọn này sẽ ngăn cản bạn khỏi gửi các event cảnh báo đến một thư mục Centralized Alerting.

Để chọn một server đích, hãy nhấp Configure để mở hộp thoại Select Alert Manager Server. Kế đó, nhận đường đến thư mục vốn điều khiển server Alert Manager mà bạn muốn sử dụng hoặc nhấp Browse để xác định server trên mạng.

Bạn có thể sử dụng ký hiệu Universal Naming Convention (UNC) trong hộp text để chỉ định máy tính điều khiển server Alert Manager hoặc bạn chỉ nhập tên máy tính. Trình tiện ích Alert Manager Client Configuration sẽ hiệu lực hóa form của tên mà bạn nhập ở đây, nhưng sẽ không xác minh rằng server Alert Manager hữu hiệu trên máy tính. Điều này cho phép laptop và những người dùng từ xa khác chỉ định một server Alert Manager ngay cả khi họ không được nối kết

với mạng của bạn.

Nếu bạn đã cài đặt Active Directory Services trên máy tính, việc nhấp Browse sẽ hiển thị một danh sách liệt kê các tên server Alert Manager logic. Nếu bạn không cài đặt Active Directory, màn hình sẽ hiển thị toàn bộ cây thư mục. Trong trường hợp đó, hãy hỏi ý kiến của nhà quản lý hệ thống của bạn để biết được máy tính nào điều khiển server Alert Manager mà bạn muốn sử dụng.

Theo mặc định, trình tiện ích client sẽ sử dụng tính năng dò tìm Active Directory để định vị một server Alert Manager đã xuất nếu bạn đã cài đặt Active Directory Services trên máy tính này và chạy trên mạng của bạn. Để ngăn cản trình tiện ích client khỏi thực hiện điều này, hãy chọn hộp kiểm Disable Active Directory Lookup, khi nó xuất hiện.

Khi bạn đã chọn một đích, hãy nhấp OK để đóng hộp thoại.

- ❖ **Enable Centralized alerting.** Nhấp nút này để yêu cầu các thành phần VirusScan gửi các thông tin cảnh báo đến một thư mục Central Alerting tại bất kỳ vị trí nào trên mạng của bạn. Chọn tùy chọn này sẽ ngăn cản bạn khỏi gửi các thông tin cảnh báo đến một server Alert Manager.

Để chọn một thư mục đích, hãy nhấp Configure để mở hộp thoại Central Alerting Configuration. Kế đó, nhập đường dẫn đi đến thư mục Central Alerting mà bạn muốn sử dụng, hoặc nhấp Browse để xác định thư mục trên mạng của bạn. Khi bạn đã chọn một đích, hãy nhấp OK để đóng hộp thoại.

Bạn có thể chỉ định bất kỳ thư mục trên mạng làm một đích cho các thông báo Centralized Alerting, nhưng thư mục phải chứa một bản sao của file CENTALRT.TXT để một server Alert Manager tiếp cận các thông tin cảnh báo mà bạn gửi đến đó.

Nếu bạn chạy Centralized Alerting, phần mềm VirusScan gửi các thông tin và báo dưới dạng các thao tác với phần mở rộng .ALR đến thư mục đích. Để biết được dạng file cho một file .ALR.

Sau đó bạn có thể trở một server Alert Manager đã chỉ định sang thư mục, nếu nó chứa file CENTALRT.TXT, để nó kiểm tra để tìm ra các file .ALR theo định kỳ. Nếu nó tìm thấy một file, nó trích nội dung của thông tin cảnh báo từ file này, phân phối thông báo bằng cách thực hiện một trong những phương pháp cảnh báo đã cấu hình sẵn của nó, sau đó xóa file .ALR. Sau đó nó kiểm tra thư mục Centralized Alerting để bắt giữ bất kỳ thông tin cảnh báo khác.

- ❖ **Additionally Enable DMI Alerts.** Chọn hộp kiểm này để bổ sung một trong những phương pháp cảnh báo khác. Kế đó, hãy nhấp Configure để mở hộp thoại DMI Configuration, trong đó bạn có thể nhập số nhận dạng mà trình ứng dụng client Desktop Management Interface (DMI) đã gán vào phần mềm VirusScan của bạn khi bạn đã cài đặt nó.

Để sử dụng tùy chọn này, bạn phải cài đặt một trình ứng dụng file DMI, chẳng hạn như Hewlett-Packard OpenView trên máy tính cục bộ và phần mềm quản lý DMI chạy trên bất kỳ vị trí nào trên mạng của bạn.

Phần mềm VirusScan đi kèm với một Management Information File (AMG.MIF) vốn nhận biết các thuộc tính cảnh báo VirusScan đối với trình ứng dụng DMI. Lần lượt, DMI gán một số nhận dạng vào phần mềm VirusScan, để nó có thể thu thập các event cảnh báo VirusScan và gửi chúng đến một trình ứng dụng quản lý DMI. Để phần mềm VirusScan gửi các thông tin cảnh báo với một số nhận dạng mà trình ứng dụng quản lý có thể nhận biết và xử lý, bạn phải nhập đúng số ID ở đây. Tư vấn với nhà quản lý hệ thống của bạn để biết thêm chi tiết có thể áp dụng vào phần mềm DMI của bạn.

Khi bạn đã nhập một số, hãy nhấp OK để đóng hộp thoại.

3. Nhấp OK để lưu các thay đổi rồi đóng hộp thoại Alert Manager Client Configuration.



TÌM HIỂU TRÌNH TIỆN ÍCH SCREENSCAN

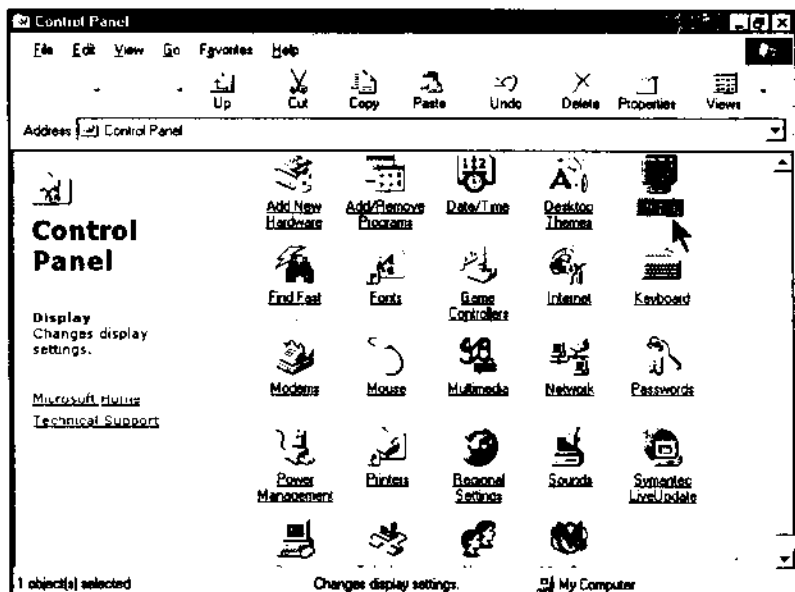
Trình tiện ích ScreenScan quét hệ thống của bạn trong nền khi bộ dưỡng màn hình của bạn chạy. Với nó, bạn có thể chuyển thời gian nghỉ của máy tính sang thời gian làm việc có hiệu quả bằng cách cho phép máy tự kiểm tra để tìm các phần nhiễm virus. ScreenScan sẽ không thực hiện bất kỳ tác động nào đối với các virus mà nó phát hiện, nhưng nó sẽ ghi lại các kết quả của các thao tác quét của nó trong một log file mà bạn có thể xem lại lúc rảnh rỗi.

Ghi chú

- Để sử dụng ScreenScan, bạn phải chọn tùy chọn cài đặt Custom trong suốt quá trình cài đặt - trình tiện ích Setup không cài đặt thành phần này theo mặc định. Một khi được cài đặt, ScreenScan hiển thị một trang đặc tính trong hộp thoại Windows Display Properties.

Để mở hộp thoại Display Properties và xác định trang đặc tính ScreenScan, hãy thực hiện những bước sau đây:

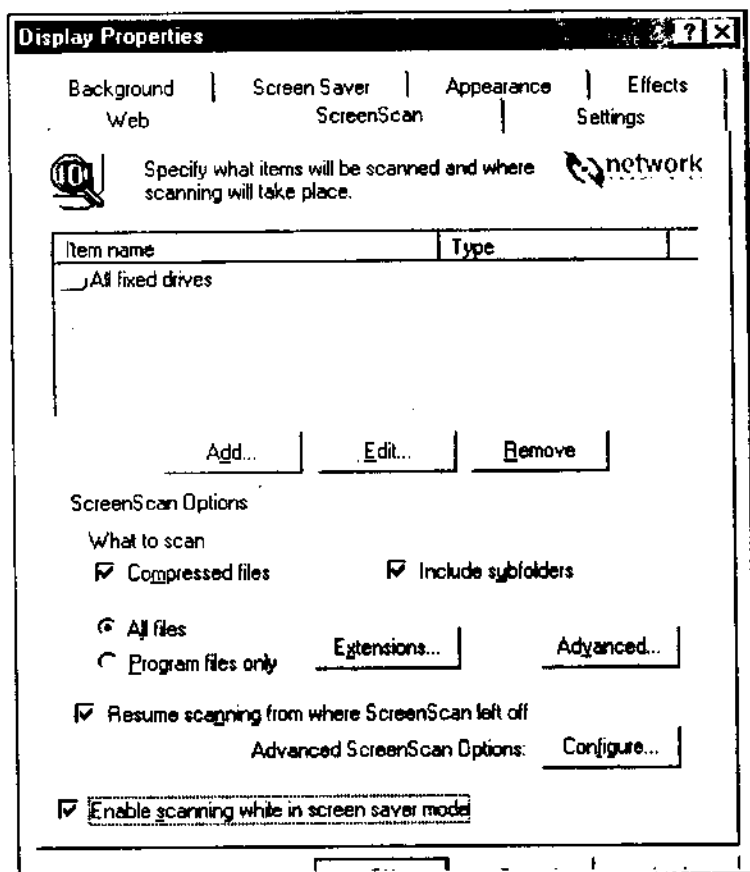
1. Nhấp Start trong thanh tác vụ Windows, trở vào Settings, sau đó chọn Control Panel.
2. Định vị và nhấp đôi panel điều khiển Display trong cửa sổ vừa xuất hiện.



3. Nhấp nhấn ScreenScan trong hộp thoại Display Properties. Để xem hình dạng của trang đặc tính này.

Tại đây bạn có thể chọn các tùy chọn phát hiện và báo cáo mà bạn muốn ScreenScan sử dụng. Để biết cách cấu hình những tùy chọn này, hãy nhấp here.

Miễn là bạn đã cấu hình và chạy nó, trình tiện ích sẽ khởi động bất cứ khi nào bộ dưỡng màn hình của máy tính khởi động và nó sẽ ngưng lại bất cứ khi nào bạn di chuyển chuột, nhấn một phím trên bàn phím hoặc thực hiện bất kỳ thao tác khác vốn làm gián đoạn bộ dưỡng màn hình.



Để biết thêm về trình tiện ích ScreenScan và cách khởi động với nó, hãy nhấp các nút bên cạnh mỗi chủ điểm đã liệt kê.

I. Các file phụ thuộc và các file liên quan dành cho trình tiện ích ScreenScan

Trình tiện ích ScreenScan chạy dưới dạng một file thực thi vốn khởi động bất cứ khi nào bộ dưỡng màn hình chạy. Trình tiện ích yêu cầu một số file hỗ trợ để chạy, kể cả một số file liên quan đến máy quét McAfee. Bản sau đây liệt kê trình tiện ích ScreenScan và các file liên quan:

Các file chương trình

Những file này chạy trực tiếp dưới dạng các file ScreenScan hoặc là các file hỗ trợ hay các file thư viện ScreenScan chuyên dụng.

File	Chức năng	Vị trí
SCRSCAN.EXE	File thực thi trình tiện ích ScreenScan. Chạy thao tác quét thật sự.	C:\Program File\ McAfee VirusScan\ VirusScan
SCRCANP.DLL	Phần mở rộng panel điều khiển ScreenScan. Cung cấp trang đặc tính cấu hình ScreenScan trong hộp thoại Windows Display Properties.	C:\Program File\ McAfee VirusScan\ VirusScan

Các file phụ thuộc

Trình tiện ích ScreenScan yêu cầu những file sau đây để chạy tại các thời điểm khác nhau trong suốt quá trình hoạt động của nó, nhưng đây không là các file chương trình ScreenScan hoặc không được chuyên dụng cho sự hỗ trợ trình tiện ích ScreenScan.

File	Chức năng	Vị trí
RESDLL.DLL	File nguồn tài nguyên cho tất cả thành phần VirusScan	C:\Program File\ Common Files\ McAfee VirusScan\ McPal
MCSCAN32.DLL	File máy quét McAfee	C:\Program File\ Common Files\ McAfee VirusScan\ VirusScan Engine\ 4.0.xx
RWABS16.DLL	File hỗ trợ cho máy quét	C:\Program File\ Common Files\ McAfee VirusScan\

		VirusScan Engine\4.0.xx
RWABS32.DLL	File hỗ trợ cho máy quét	C:\Program File\Common Files\McAfee VirusScan\VirusScan Engine\4.0.xx
MESSAGES.DAT	File hỗ trợ cho máy quét Cung cấp các thông báo phát hiện virus cho máy.	C:\Program File\Common Files\McAfee VirusScan\VirusScan Engine\4.0.xx

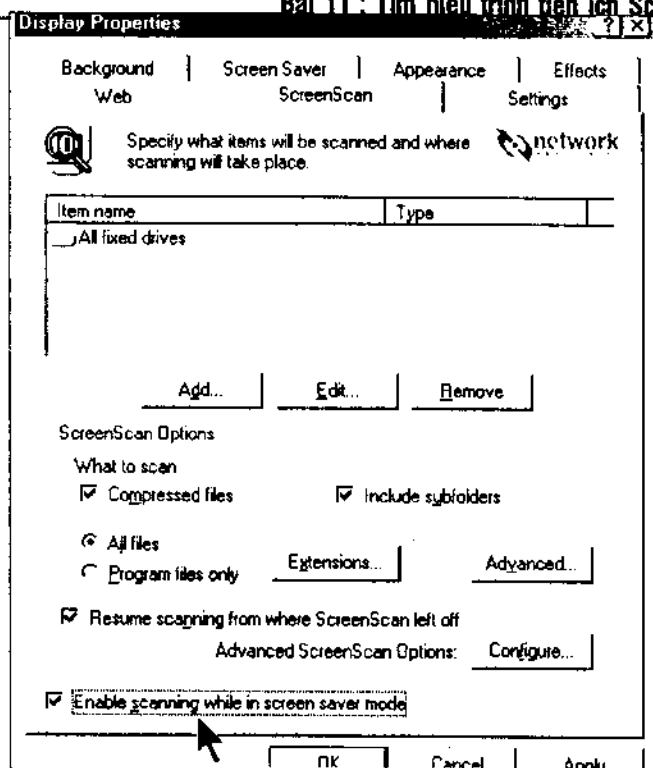
II. Cấu hình trình tiện ích ScreenScan

Ban đầu khi bạn mở trang đặc tính ScreenScan, trình tiện ích giả định rằng bạn muốn quét tất cả file trên tất cả ổ đĩa cố định trên hệ thống, cùng với các folder con của chúng, để quét các file nén và để báo cáo các tác động của nó trong file SCREENSCAN ACTIVITY LOG.TXT.

Để cài đặt hoặc thay đổi những tùy chọn đó, hãy thực hiện những bước sau đây:

1. Chọn hộp kiểm Enable scanning while in screen server mode để yêu cầu trình tiện ích ScreenScan khởi động khi bộ dưỡng màn hình khởi động.

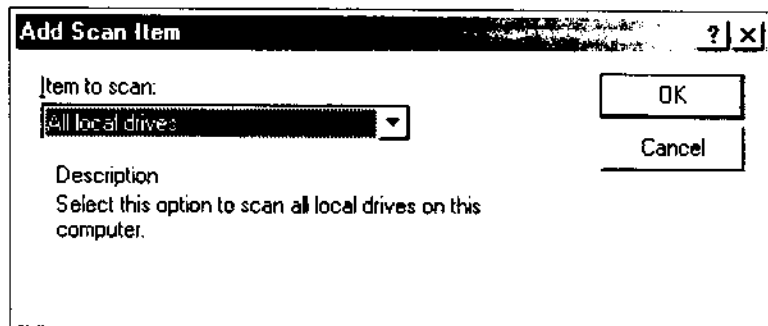
Các tùy chọn lại trong trang đặc tính trở nên được kích hoạt.



2. Chọn các phần nào của hệ thống mà bạn muốn trình tiện ích ScreenScan kiểm tra để tìm virus. Bạn có thể:

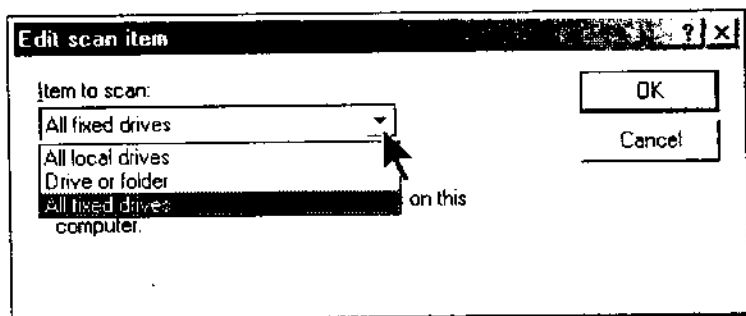
- ❖ Thêm các đích quét. Nhấp Add để mở hộp thoại Add Scan Item.

Để biết cách xác định các đích quét.

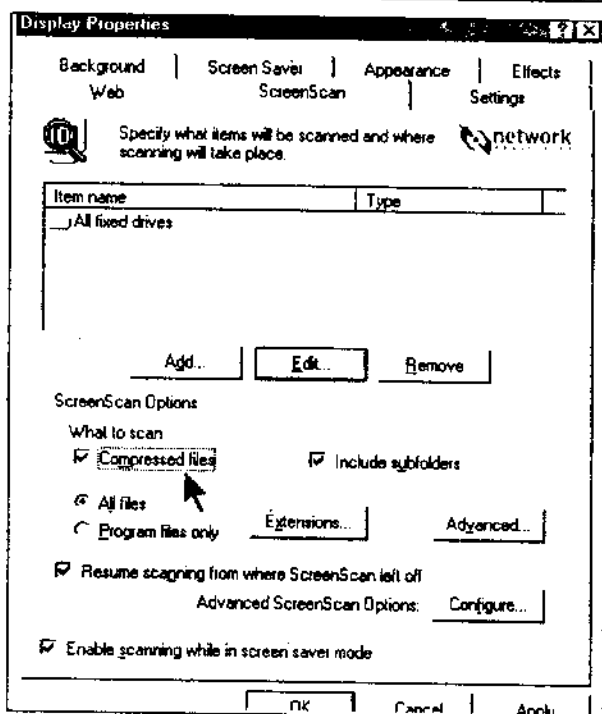


- ❖ Thay đổi các đích quét. Chọn một trong các đích quét đã liệt kê, sau đó nhấn Edit để mở hộp thoại Edit Scan Item.

Hộp thoại xuất hiện với đích quét hiện có đã xác định. Chọn hoặc nhập mục đích quét mới rồi sau đó nhấn OK để đóng hộp thoại.



- ❖ Loại bỏ các đích quét. Chọn một trong những đích quét đã liệt kê rồi sau đó nhấn Remove để xóa nó.
3. Xác định các loại file nào mà bạn muốn trình tiện ích kiểm tra. Bạn có thể
- ❖ Quét các file nén. Chọn hộp kiểm Compressed files để yêu cầu trình tiện ích tìm kiếm các virus trong các file nén hay các file archives. Để xem một danh sách các loại file hay archives mà trình tiện ích quét, hãy nhấn [here](#).
 - ❖ Quét các folder con trong đích đã chỉ định. Chọn hộp kiểm Include subfolders để yêu cầu trình tiện ích tìm các virus trong bất kỳ folder nào nằm trong đích quét của bạn.



Ghi chú

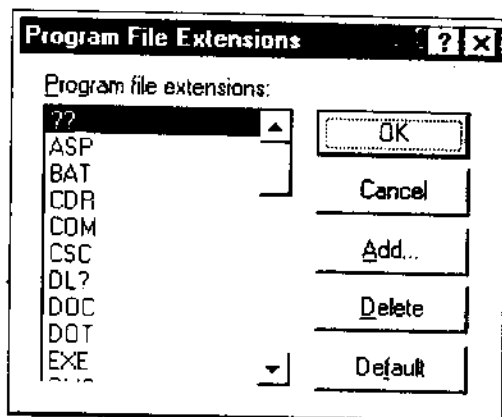
Việc chọn *Include subfolders* sẽ làm cho trình tiện ích chỉ quét các file đó đã lưu trữ trong chính folder con. Trình tiện ích sẽ không quét các file được lưu trữ tại cấp gốc của folder mà bạn chỉ định. Để quét các file đó, hãy hủy chọn hộp kiểm *Include subfolders*.

- ❖ Quét tất cả file. Chọn hộp kiểm *All Files* để yêu cầu trình tiện ích quét tất cả file trong mailbox hay folder chung mà bạn đã xác định, cho dù các phần mở rộng của chúng là gì đi nữa.

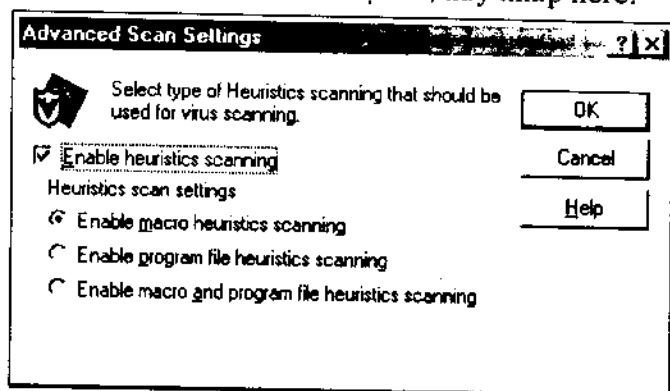
Ghi chú

McAfee đề nghị bạn nên chọn tùy chọn này cho thao tác quét đầu tiên của bạn hoặc theo định kỳ để bảo đảm rằng hệ thống của bạn không có virus. Sau đó bạn có thể giới hạn phạm vi của các thao tác quét sau này.

- ❖ Chọn các loại file. Các virus không thể lây nhiễm các file không chứa mã thực thi, cho dù là script, macro, hay mã nhị phân. Do đó bạn có thể thu hẹp an toàn phạm vi của các thao tác quét của bạn đối với những file dễ bị nhiễm virus nhất. Để thực hiện điều này, hãy nhấp nút Program file only. Để xem hoặc chỉ định các phần mở rộng tên file mà trình tiện ích sẽ kiểm tra, hãy nhấp Extensions. Điều này mở hộp thoại Program File Extensions. Để tìm hiểu về các file đã liệt kê ở đó, hãy nhấp here.



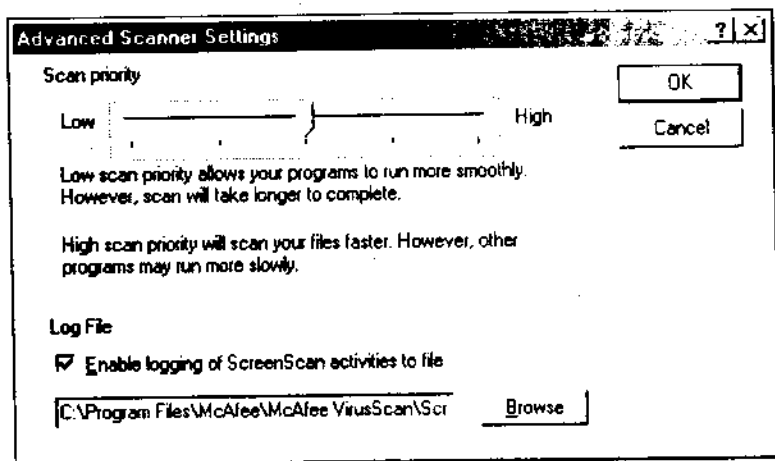
- ❖ Để mở tính năng quét suy nghiệm. Nhấp Advanced để mở hộp thoại Advanced Scan Settings. Để tìm hiểu về việc quét suy nghiệm và cách kích hoạt nó, hãy nhấp here.



4. Nếu bạn muốn trình tiện ích ScreenScan tiếp tục thực hiện bất kỳ thao tác quét vốn bị gián đoạn từ thời điểm mà nó được ngừng lại, hãy chọn Resume scanning from where ScreenScan left off.

Nếu bạn không chọn hộp kiểm này, trình tiện ích sẽ bắt đầu lại thao tác quét của nó từ cấp góc của ổ đĩa đầu tiên mà bạn đã xác định dưới dạng một đích quét mỗi lần bộ đường màn hình bắt đầu chạy. Điều này có thể có nghĩa rằng trình tiện ích sẽ quét một số phần của hệ thống lập đi lập lại nhưng sẽ hoàn toàn bỏ qua các phần khác.

5. Cài đặt các tùy chọn Advanced ScreenScan. Nhấp Configure để mở hộp thoại Advanced Scanner Settings. Sau đây là các tùy chọn của bạn:



- ❖ Cài đặt một chế độ ưu tiên thực thi cho các tác vụ ScreenScan. Trượt control điều khiển chế độ ưu tiên quét hướng sang High để cung cấp một chế độ ưu tiên cao hơn cho các nguồn tài nguyên hệ thống và thời gian cho trình tiện ích ScreenScan thay vì cho các hoạt động nền khác chẳng hạn như các thao tác xử lý phân đoạn đĩa vốn hoạt động trong suốt thời gian nghỉ trên máy tính. Điều này làm cho các hoạt động khác chạy chậm hơn.

Trước control hướng sang Low để cung cấp cho các tác vụ nền khác chế độ ưu tiên cao hơn mà bạn thực hiện đối với trình tiện ích ScreenScan. Điều này làm cho trình tiện ích ScreenScan chạy chậm hơn.

- ❖ Yêu cầu trình tiện ích nhập các thao tác của nó. Chọn hộp kiểm Enable logging of ScreenScan activities to file để yêu cầu trình tiện ích ScreenScan tổng hợp các thao tác mà nó đã thực hiện khi nó chạy trong file SCREENSCAN ACTIVITY LOG.TXT.

Trình tiện ích sẽ ghi lại tất cả thao tác của nó bất cứ khi nào bạn ngưng tác vụ hoặc khi bạn tắt hệ thống. Nếu bạn thích nhập dữ liệu này hơn file text khác, hãy nhập đường dẫn và tên file của nó trong hộp text đã cung cấp hoặc nhấp Browse để định vị file. Trình tiện ích Screencan sẽ không tạo một file text - nó sẽ chỉ ghi sang một file hiện có.

6. Kế tiếp, bạn có thể:

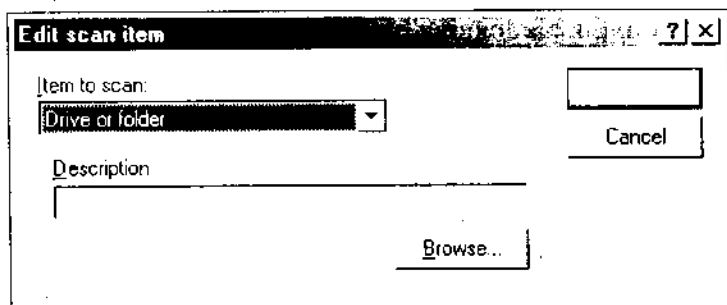
- ❖ Nhấp Apply để lưu các tùy chọn cấu hình mà không đóng hộp thoại Display Properties.
- ❖ Nhấp OK để lưu các tùy chọn cấu hình rồi đóng hộp thoại Display Properties.
- ❖ Nhấp Cancel để đóng hộp thoại Display Properties mà không lưu các thay đổi của bạn.

III. Xác định các đích quét cho trình tiện ích ScreenScan

Để quét tất cả hay một tập hợp con của các ổ đĩa trên hệ thống của bạn, hãy thực hiện những bước sau đây:

1. Chọn một đích quét từ danh sách đã cung cấp. Sau đây là các tùy chọn của bạn:
 - ❖ **All local drives.** Tùy chọn này yêu cầu trình tiện ích quét tất cả ổ đĩa đã gắn vào máy tính của bạn, kể cả các ổ đĩa phương tiện có thể tháo rời.

- ❖ **Drive or folder.** Tùy chọn này yêu cầu trình tiện ích quét các file hay folder cụ thể trên hệ thống của bạn. Gõ nhập vào hộp text đã cung cấp chữ cái ổ đĩa hay đường dẫn đi đến folder mà bạn muốn quét, hoặc nhấp Browse để định vị đích quét trên máy tính của bạn.



- ❖ **All fixed drive.** Tùy chọn này yêu cầu trình tiện ích quét các đĩa cứng đã nối kết với máy tính của bạn.
2. Khi bạn đã chọn đích, hãy nhấp OK để đóng hộp thoại.

 Bài 12

TÌM HIỂU CÁC TRÌNH TIỆN ÍCH AUTOUPDATE VÀ AUTOUPGRADE

Các trình tiện ích AutoUpdate và AutoUpgrade là những phương pháp để bảo đảm rằng bạn có sẵn các file (.DAT) xác định virus và các file chương trình mới nhất cho phần mềm VirusScan của bạn. Hai trình tiện ích này tạo nên nền tảng cho một loạt chiến thuật cập nhật cho phần mềm của bạn.

Theo mặc định, tác vụ AutoUpdate đi kèm với VirusScan Console được cấu hình để tải xuống các thông tin cập nhật file .DAT một cách trực tiếp từ McAfee VirusScan FTP site. Cấu hình này có thể làm cho việc quản lý trở nên đơn giản đối với các mạng nhỏ hay các cài đặt VirusScan riêng lẻ. Nếu bạn có một mạng lớn, tuy nhiên việc giữ lại cấu hình này có thể làm hao tổn nghiêm trọng dải băng tần bên ngoài của bạn nếu bạn để cấu hình mặc định được sử dụng, mỗi nút mạng cố gắng cập nhật các file .DAT của nó cùng một lúc.

Thay vào đó, McAfee yêu cầu nên sử dụng AutoUpdate cùng với một dịch vụ đi kèm đó là kênh Enterprise SecureCast. Một khi bạn cài đặt phần mềm client của nó trên một server quản lý, dịch vụ SecureCast có thể gửi hoặc đẩy các file đã cập nhật đến bạn một cách tự động ngay khi McAfee làm cho chúng trở nên có sẵn. Nếu bạn làm cho các file mà bạn tải xuống trở nên có sẵn trên một hoặc nhiều server trung tâm trên mạng của bạn, thì sau đó hãy cấu hình các nút mạng còn lại để kéo các file cập nhật từ các server đó, bạn có thể

- ❖ Lập biểu các lần chuyển ra file .DAT toàn mạng cho các thời điểm thuận tiện và với sự can thiệp tối thiểu từ các nhà quản lý hay những người sử dụng mạng. Sử dụng hộp thoại AutoUpdate Task Properties để xác định khi nào mỗi nút mạng sẽ kiểm tra server để tìm ra các file được cập nhật. Ví dụ, bạn có thể xác định một thời điểm cập nhật thuận lợi khi ban đầu bạn triển khai phần mềm VirusScan, nhưng cài đặt AutoUpdate để kích khởi tại một khoảng thời gian ngẫu nhiên trong vòng 60 phút của thời điểm đó hoặc cài đặt một thời biểu vốn thực hiện từng bước hoặc luân phiên thực hiện các thao tác cập nhật file .DAT giữa các phần khác nhau của mạng.
- ❖ Phân chia các nhiệm vụ quản lý giữa các server hay các bộ điều khiển domain khác nhau, giữa các vùng khác nhau của các mạng vùng rộng hay qua các vùng phân chia mạng khác. Việc giữ sự lưu thông cập nhật chủ yếu ở bên trong có thể giảm đi khả năng vi phạm sự an toàn mạng.
- ❖ Giảm đi khả năng mà bạn sẽ cần đợi để tải xuống các file .DAT mới. Sự lưu thông trên các server McAfee VirusScan tăng đáng kể vào các ngày xuất file .DAT thường lệ.

Ghi chú

Để biết thêm thông tin về việc tải xuống, cài đặt và đăng ký với dịch vụ McAfee VirusScan SecureCast, hãy xem website McAfee VirusScan tại: http://www.nai.com/asp_set/anti_virus/alerts/enterprise.asp

Những tùy chọn AutoUpdate cao cấp khác cho phép bạn sao lưu dự phòng các file .DAT hiện có, cài đặt thông tin cập nhật file .DAT, khởi động lại máy tính đã cập nhật, nếu cần thiết, hoặc chạy các chương trình đặc biệt sau khi cập nhật.

Ghi chú

Việc cập nhật phần mềm VirusScan sẽ có nghĩa là tải xuống và cài đặt các phiên bản file .DAT mới; việc nâng cấp phần mềm VirusScan sẽ có nghĩa là tải xuống và cài đặt các bản chỉnh sửa phần mềm sản phẩm, các file máy quét mới và trong một số trường hợp, là các file

.DAT mới. McAfee cung cấp các thông tin cập nhật file .DAT miễn phí cho tuổi thọ của sản phẩm. Tuy nhiên, điều này không bảo đảm rằng các phiên bản file .DAT trong tương lai sẽ tương thích với các phiên bản sản phẩm trước đây.

Các trình tiện ích AutoUpdate và AutoUpgrade chạy riêng biệt dưới dạng các tác vụ từ trong VirusScan Console. Để sử dụng chúng để cập nhật hay nâng cấp phần mềm VirusScan của bạn, bạn phải:

- ❖ Xác định vị trí trên mạng hay trên Internet mà các trình tiện ích sẽ đi để tải xuống các file mới.
- ❖ Cấu hình mỗi trình tiện ích để sử dụng một phương pháp truyền tải riêng biệt và xác định bất kỳ sự truy cập account nào mà chúng cần để nối kết với các site cập nhật và nâng cấp của bạn.
- ❖ Báo cho các trình tiện ích biết những gì cần thực hiện với các file mà chúng tải xuống và những gì cần thực hiện sau khi chúng tải đặt thành công các file mới.
- ❖ Chạy tác vụ và cài đặt một thời biểu cho nó.

Để tìm hiểu thêm về các trình tiện ích AutoUpdate và AutoUpgrade và cách bắt đầu với chúng, hãy nhấp các nút bên cạnh mỗi chủ điểm được liệt kê.

I. Bắt đầu và ngưng các thao tác AutoUpdate và AutoUpgrade

Bởi vì các trình tiện ích AutoUpdate và AutoUpgrade hoạt động dưới dạng các tác vụ trong VirusScan Console, thông thường bạn sẽ không bắt đầu hay ngưng chúng như bạn có thể thực hiện đối với các thành phần chương trình VirusScan khác. Thay vào đó, bạn có thể truy cập một thời biểu cho mỗi tác vụ và cho phép mỗi tác vụ chạy. Để học cách cài đặt một thời biểu tác vụ, hãy nhấp [here](#).

Sau đó VirusScan Console quản lý việc bắt đầu tác vụ tại thời điểm mà bạn cài đặt.

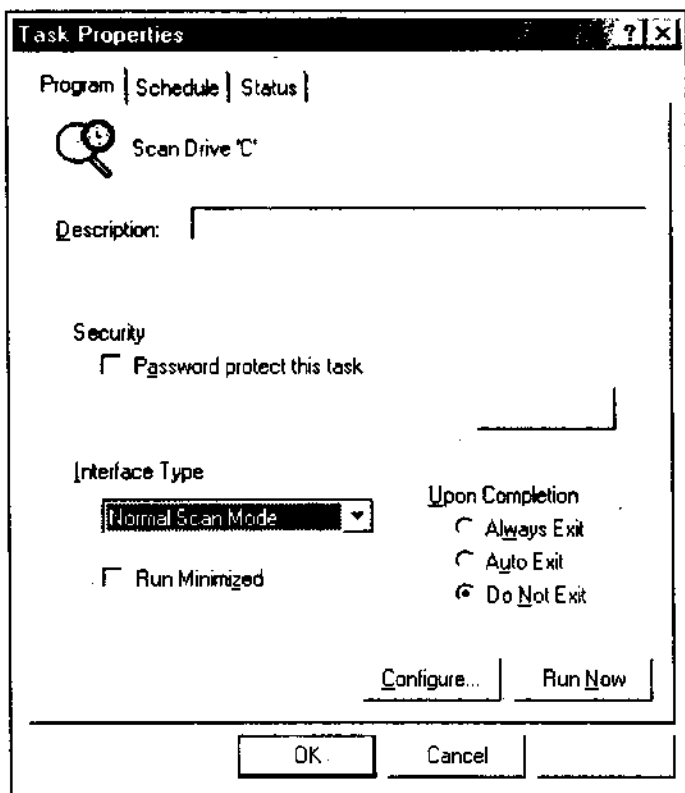
Ghi chú

Bạn phải chạy máy tính và chạy VirusScan Console để những tác vụ này bắt đầu. Để biết thêm về cách khởi động Console.

Bạn cũng có thể khởi chạy một hoạt động nâng cấp hay cập nhật một cách trực tiếp từ cửa sổ Task Properties.

Để thực hiện điều này, hãy thực hiện những bước sau đây;

1. Nhấp đúp tác vụ AutoUpdate hay AutoUpgrade trong cửa sổ Console để mở hộp thoại Task Properties.
2. Nhấp Run Now.



Điều này yêu cầu trình tiện ích tải xuống các file từ các server hay các site mà bạn đã chỉ định bằng cách sử dụng các tùy chọn cấu hình mà bạn đã chọn.

Để ngưng hoạt động này trước khi nó kết thúc, hãy nhấp Cancel trong hộp thoại tiến độ mà mỗi trình tiện ích hiển thị khi nó chạy.

Trong các tình huống riêng biệt - khi bạn muốn chạy một hoạt động nâng cấp hay cập nhật từ một script login hay một file lô chẳng hạn - bạn cũng có thể chạy các trình tiện ích từ dòng lệnh. Script login hay file lô sẽ gọi file MCUPDATE.EXE cùng với các tùy chọn dòng lệnh mà bạn muốn sử dụng.

II. Xác định các file AutoUpdate và AutoUpgrade trên hệ thống

Các trình tiện ích AutoUpdate và AutoUpgrade gồm có một file thực thi chính đó là file MCUPDATE.EXE mà bạn sẽ tìm thấy trong vị trí sau:

C:\Program File\Common Files\McAfee VirusScan\McUpdate

Thông thường, bạn sẽ không sử dụng trực tiếp file này để chạy một hoạt động cập nhật hay nâng cấp.

Đối với các mục đích riêng biệt, chẳng hạn như việc sử dụng một login script để cập nhật hay nâng cấp phần mềm khi khởi động, tuy nhiên, bạn chạy MCUPDATE.EXE từ dòng lệnh.

MCUPDATE.EXE làm việc với hai file khác, MCURIAL.DLL và PATCHW32.DLL để cung cấp việc cập nhật file .DAT gia tăng. Bạn sẽ tìm thấy những file đó trong cùng một thư mục mà bạn sẽ tìm thấy MCUPDATE.EXE.

III. Các tùy chọn dòng lệnh cho các trình tiện ích AutoUpdate và AutoUpgrade

Trong hầu hết các trường hợp, bạn có thể cấu hình và chạy một tác vụ AutoUpdate hay AutoUpgrade từ trong VirusScan Console. Việc thực hiện điều này sẽ cung cấp cho bạn sự truy cập đầy đủ đến tất cả tùy chọn cấu hình và lập biểu có sẵn với mỗi trình tiện ích.

Nếu bạn muốn chạy một tác vụ AutoUpdate hay AutoUpgrade từ một file lô hay một login script, tuy nhiên thay vào đó bạn có thể gọi

file tiện ích MCUPDATE.EXE và bổ sung các tùy chọn dòng lệnh được trình bày trong bảng dưới đây. Theo mặc định, việc thực hiện điều này sẽ chỉ chạy một tác vụ đã ấn định sẵn mà bạn đã tạo từ trong cửa sổ Console. Tuy nhiên một số tùy chọn dòng lệnh sẽ cho phép bạn hiển thị các hộp thoại cấu hình cho trình tiện ích trước khi tác vụ chạy, để bạn có thể thay đổi bất kỳ phần định nghĩa mà bạn từng thực hiện.

Để sử dụng MCUPDATE.EXE để chạy một tác vụ, hãy đưa một lệnh gọi vào file cùng với bất kỳ tùy chọn dòng lệnh mà bạn muốn sử dụng, dưới dạng một file lô hay lệnh login script. Để chạy trực tiếp MCUPDATE.EXE từ dòng lệnh, hãy thực hiện những bước sau đây:

Để chạy trực tiếp MCUPDATE.EXE từ dòng lệnh, hãy thực hiện những bước sau đây:

1. Nhấp Start trong thanh tác vụ Windows, trở vào Programs, sau đó chọn MS-DOS Prompt nếu máy tính của bạn chạy Windows 95 hay Windows 98. Nếu máy tính chạy Windows NT Workstation v4.0 hay Windows 2000 Professional, hãy chọn Command Prompt.

Windows hiển thị một cửa sổ dòng nhắc lệnh. Nếu bạn đã cài đặt phần mềm VirusScan sang vị trí mặc định của nó, hãy chuyển sang thư mục sau:

C:\Program File\Common Files\McAfee VirusScan\McUpdate

2. Kế đó, gõ nhập dòng sau tại dòng nhắc lệnh:

mcupdate.exe /<configuration options>

Ghi chú

Tại đây, <configuration options> có nghĩa là bất kỳ tùy chọn dòng lệnh nào mà bạn muốn sử dụng từ bản bên dưới. Đặt chữ A trước mỗi tùy chọn. Mặc dù trình ứng dụng sẽ cho phép bạn xác định một số tùy chọn mà không có dấu nhập, việc xác định các tùy chọn khác sẽ gây ra một lỗi. Bạn có thể xác định bất kỳ tham số cần thiết nào cho các tùy chọn của bạn mà không có ký hiệu đặc biệt.

Tùy chọn	Mô tả
/CONFIG	Tùy chọn này yêu cầu MCUPDATE.EXE hiển thị hộp thoại Automatic Update cho trình tiện ích AutoUpdate hoặc các hộp thoại Automatic Update cho trình tiện ích AutoUpgrade trước khi nó bắt đầu một hoạt động. Các hộp thoại này cho phép bạn thêm, loại bỏ hoặc thay đổi các định nghĩa cho các site cập nhật hay nâng cấp mà bạn đã xác định khi bạn cấu hình tác vụ. Để chạy tác vụ sau khi bạn thay đổi các tùy chọn, hãy nhấp Update Now hay Upgrade Now. Để xác định xem AutoUpdate hoặc AutoUpgrade sẽ chạy hay không và do đó hộp thoại nào sẽ xuất hiện - khởi động MCUPDATE.EXE bằng tùy chọn /TASK.
/TASK <TYPE> <TYPE> UPDATE	Tùy chọn này báo cho MCUPDATE.EXE biết một trong hai trình tiện ích - AutoUpdate hay AutoUpgrade - mà bạn muốn chạy. Nếu bạn muốn sử dụng tùy chọn này để xác định một trình tiện ích, MCUPDATE.EXE chạy trình tiện ích AutoUpdate theo mặc định. Để chạy một tác vụ AutoUpdate đã ấn định sẵn, hãy đặt giá trị UPDATE sau /TASK. Để chạy một tác vụ AutoUpgrade đã ấn định sẵn, hãy đặt giá trị UPGRADE sau /TASK.
UPGRADE	Bạn có thể kết hợp tùy chọn này với các tùy chọn khác để đạt được những mục đích khác nhau. Ví dụ việc chạy /TASK với /CONFIG sẽ cho phép bạn thay đổi các tùy chọn cấu hình một trình tiện ích hay trình tiện ích khác thay vì chỉ bắt đầu một tác vụ đã ấn định. Việc chạy /TASK với /QUIET sẽ bắt đầu với

một tác vụ đã ấn định sẵn vốn sẽ chạy êm hoặc không có một giao diện có thể nhìn thấy được.

/VSPOLICY

Tùy chọn này yêu cầu MCUPDATE.EXE chạy trình tiện ích AutoUpdate với các tùy chọn cấu hình mà bạn đã xác định. Trình tiện ích sẽ chỉ hiển thị thông tin tiến triển khi nó chạy. Bạn có thể chạy một tác vụ AutoUpgrade đã ấn định sẵn nếu bạn xác định trình tiện ích đó với tùy chọn /TASK.

Nếu bạn chạy tùy chọn này với tùy chọn /CONFIG, MCUPDATE.EXE sẽ hiển thị hộp thoại Automatic Update, nhưng sẽ vô hiệu hóa nút Update Now. Điều này cho phép bạn thay đổi các tùy chọn cấu hình cho tác vụ, nhưng yêu cầu bạn chạy lại MCUPDATE.EXE để bắt đầu tác vụ thật sự.

Dĩ nhiên bạn có thể kết hợp /VSPOLICY, /CONFIG và /TASK để hiển thị hộp thoại Automatic Upgrade để cấu hình các tùy chọn ở đó. Điều này sẽ vô hiệu hóa nút Upgrade Now.

/QUIET

Tùy chọn này yêu cầu MCUPDATE.EXE chạy một tác vụ AutoUpdate hoặc tác vụ mà bạn đã xác định bằng tùy chọn /TASK, không có giao diện hiển thị. Bạn sẽ không thấy một hộp thoại cấu hình hoặc bất kỳ thông tin tiến triển nào.

/NOPRESTART

Tùy chọn này yêu cầu MCUPDATE.EXE không cố gắng khởi động lại tất cả thành phần VirusScan sau khi nó hoàn tất một tác vụ nâng cấp hay cập nhật. Nếu bạn không xác định tùy chọn này, tác vụ sẽ chạy với các cài đặt

mà bạn đã chọn trong các trang tùy chọn
Advanced Update hay Advanced Upgrade.

IV. Cấu hình trình tiện ích AutoUpdate

Để cập nhật các file xác định virus cho phần mềm VirusScan, bạn phải thông báo cho trình tiện ích AutoUpdate biết:

- ❖ Các site cập nhật nào có các file mới mà bạn muốn tải xuống.
- ❖ Phương pháp truyền tải nào mà bạn muốn nó sử dụng để tải xuống.
- ❖ Bạn có sử dụng một proxy server hay không và nếu có thì cổng nào mà bạn đã gán cho nó.
- ❖ Bạn có muốn nó sao lưu dự phòng các file .DAT hiện có hay không.
- ❖ Những gì mà bạn muốn nó thực hiện với các file mà nó tải xuống - cài đặt chúng, lưu chúng để sử dụng sau này hoặc cả hai.
- ❖ Những gì mà bạn muốn nó thực hiện sau khi nó tải xuống các file - áp buộc sự cập nhật, khởi động lại hệ thống sau khi cập nhật hoặc chạy một chương trình sau khi cập nhật.
- ❖ Bạn có muốn nó theo dõi các hoạt động của nó trong một log file hay không.

Các trang đặc tính trong hộp thoại Automatic Update Properties điều khiển các tùy chọn cho tác vụ cập nhật của bạn. Bạn có thể nhấp mỗi tab để lần lượt cấu hình tác vụ này.

Để hiển thị hộp thoại Automatic Update, hãy thực hiện những bước sau đây:

1. Nhấp đúp tác vụ AutoUpdate trong danh sách tác vụ Console để mở hộp thoại Task Properties.
2. Nhấp Configure.
Hộp thoại Automatic Update xuất hiện.
Danh sách các site cập nhật trình bày các site nào mà bạn đã

yêu cầu trình tiện ích sử dụng. Nó cũng thông báo trạng thái hiện hành của mỗi site dưới dạng Enable hay Disabled. Một site được vận hành nếu bạn đã chọn hộp kiểm Enabled trong hộp thoại Automatic Update Properties. Một site bị hủy vận hành nếu bạn xóa hộp kiểm này. Sự chỉ định này không thay đổi việc trình tiện ích AutoUpdate có thể nối kết với site hay không.

Trình tiện ích AutoUpdate có thể tải xuống các file chương trình mới từ bất kỳ site FTP hay site dùng chung mạng mà bạn xác định. Bạn có thể chỉ định nhiều site mà từ đó trình tiện ích có thể cố gắng tải xuống các file mới. Trình tiện ích sẽ lần lượt thử mỗi site phải bắt đầu từ trên cùng của danh sách, đến khi nó tải xuống thành công các file mới hoặc xác định rằng các file mới không hiện hữu.

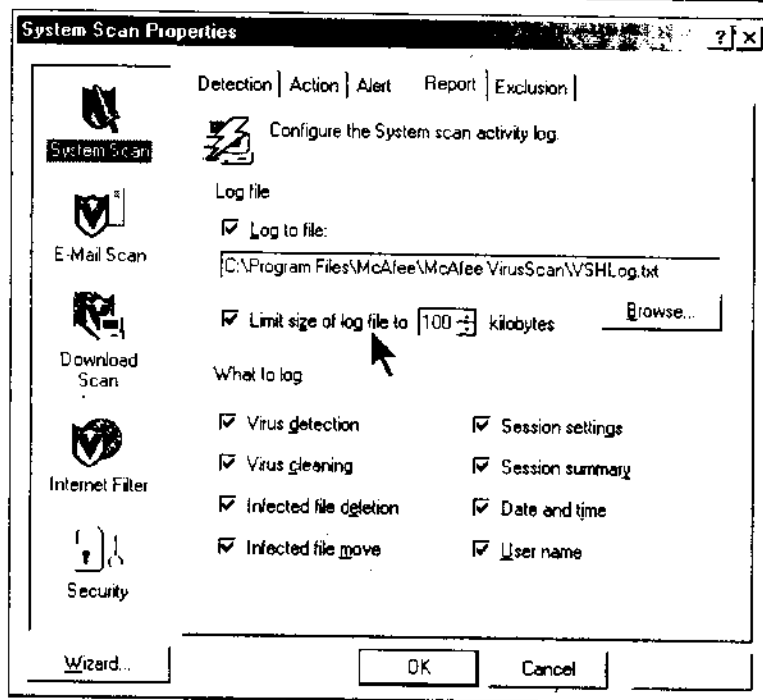
Trình tiện ích đi kèm với một site cập nhật đã xác định và được vận hành - site McAfee VirusScan FTP.

3. Từ đây, bạn có thể:

- ❖ Thêm một site mới vào danh sách site cập nhật. Nhấp Add để mở hộp thoại Automatic Update Properties.
- ❖ Thay đổi các định nghĩa cho một site cập nhật hiện có. Chọn một site được trình bày trong danh sách site cập nhật, sau đó nhấp Edit để mở hộp thoại Automatic Update Properties. Thực hiện các thay đổi mà bạn muốn, sau đó nhấp OK để lưu chúng và quay trở lại hộp thoại này.
- ❖ Loại bỏ một site hiện có ra khỏi danh sách site cập nhật. Chọn một site được trình bày trong danh sách site cập nhật, sau đó nhấp Delete.
- ❖ Xác định thứ tự trong đó trình tiện ích AutoUpdate sẽ nối kết với các site đã liệt kê. Để định vị một site để trình tiện ích thử nó sớm hơn, chọn site, sau đó nhấp Move Up. Để chỉ định một site với chế độ ưu tiên thấp hơn, hãy chọn site rồi sau đó nhấp Move Down.

- ❖ Cập nhật các file ngay từ các site được liệt kê trong danh sách cập nhật, bằng cách sử dụng các tùy chọn cấu hình mặc định hoặc các tùy chọn mà bạn đã chọn cho tác vụ này. Nhấp Update Now.
- ❖ Xác định một log file và giới hạn kích cỡ của nó. Nhấp nhấn Log Activity. Theo mặc định, trình tiện ích ghi lại các hoạt động của nó trong file UPDATE UPGRADE ACTIVITY LOG.TXT bất cứ khi nào bạn ngưng tác vụ hoặc khi bạn tắt hệ thống. Nếu bạn thích nhập dữ liệu này hơn file text khác, hãy nhập đường dẫn và tên file của nó trong hộp text đã cung cấp hoặc nhấp Browse để định vị file. Trình tiện ích AutoUpdate sẽ không tạo một file text - nó sẽ chỉ ghi sang một file hiện có.

Tiếp theo, hãy chọn hộp kiểm Limit size of log file to để giới hạn kích cỡ của file UPDATE UPGRADE ACTIVITY LOG.TXT hoặc một log file khác mà bạn xác định trong hộp text đã cung cấp. Theo mặc định, log file có thể tăng kích cỡ đến 100K.



Nhấp () để cài đặt một kích cỡ hoặc nhập kích cỡ tối đa mà bạn thích hơn, tính bằng các kilobyte, vào hộp text đã cung cấp. Nếu bạn xóa hộp kiểm này, log file có thể tăng kích cỡ đến khi giới hạn khoảng trống đĩa hay giới hạn hệ thống file ngưng nó lại. Khi file đạt được kích cỡ tối đa mà bạn cài đặt, trình tiện ích AutoUpdate trước tiên sẽ xóa nó, sau đó khởi động lại log từ vị trí mà nó được ngừng lại.

4. Khi bạn đã chọn một tùy chọn, hãy nhấp OK để lưu các cài đặt và quay trở về hộp thoại Task Properties hoặc nhấp Cancel để đóng hộp thoại này mà không lưu các cài đặt của bạn.

V. Cài đặt các đặc tính Automatic Update

Để thêm một site mới mà từ đó trình tiện ích AutoUpdate có thể tải xuống các file .DAT mới, hãy thực hiện những bước sau đây:

1. Nhập một tên mô tả trong hộp text Site Name vốn nhận biết

rõ ràng site mới.

Ví dụ: Internal .DAT File Update Site.

2. Chọn hộp kiểm Enabled để chấp nhận site này để trình tiện ích AutoUpdate sử dụng.

Việc xóa hộp kiểm này sẽ làm cho trình tiện ích bỏ qua site này khi nó cố tải xuống các file .DAT mới.

3. Xác định phương pháp truyền tải nào mà trình tiện ích phải sử dụng để tải xuống các file mới. Sau đây là các tùy chọn của bạn:

- ❖ Copy from a local network computer. Nhấp nút này để yêu cầu trình tiện ích AutoUpdate sử dụng cấu hình mạng chuẩn của bạn để tìm các file mới trên máy tính cục bộ hoặc trên một máy tính tại vị trí khác trên mạng.

Kế đó, hãy sử dụng ký hiệu Universal Naming Convention (UNC) để nhập đường dẫn đi đến máy tính vốn chứa các file mới mà bạn muốn tải xuống trong hộp text có nhãn là Select a computer and directory. Bạn cũng có thể nhấp Browse để định vị thư mục mà bạn muốn.

Để sử dụng một ký hiệu UNC, bạn phải sử dụng cùng một account mà bạn đã dùng để nhập vào mạng, hãy xác định tên người dùng và password đã nhập vào mạng. Để sử dụng account hiện hành, hãy chọn hộp kiểm Use Logged In Account.

Ghi chú

Trên các hệ thống Windows NT Workstation v4.0 và Windows 2000 Professional, việc chọn hộp kiểm Use Logged In Account sẽ có những tác dụng hơi khác nhau. Nếu bạn đã lập biểu sự cập nhật file của bạn, trình tiện ích AutoUpdate sẽ sử dụng account dịch vụ riêng của nó để nhập vào server nâng cấp và tải xuống các file mới. Nếu bạn nhấp Update Now, trình tiện ích AutoUpdate sẽ sử dụng cùng một account mà bạn đã dùng để nhập vào mạng để nối kết với server nâng cấp.

Để sử dụng một account tùy ý, hãy hủy chọn hộp kiểm Use Logged In Account, sau đó nhấp UNC Login information để

nhập một tên người dùng và password trong một account vốn có các quyền truy cập đến server đích.

- ❖ **FTP from a remote network computer.** Nhấp nút này để yêu cầu trình tiện ích AutoUpdate tìm kiếm các file mới trên một FTP site mà bạn chỉ định. Theo mặc định, trình tiện ích này sẽ tải xuống các site mới từ McAfee VirusScan FTP site vốn chấp nhận các FTP login nặc danh. Bạn có thể nhấp Default để xác định site này vào bất cứ lúc nào.

Để sử dụng một FTP site khác, hãy nhập URL cho site mà bạn muốn sử dụng trong hộp text có nhãn là Enter and FTP computer name and directory. Bạn phải nối kết với một site đã cài đặt cho FTP login nặc danh hoặc bạn phải chỉ định tên người dùng và password cho một account trên site.

Để yêu cầu trình tiện ích sử dụng một login nặc danh, hãy chọn hộp kiểm Use anonymous FTP login. Để xác định một account, hãy hủy chọn hộp kiểm use anonymous FTP login, sau đó nhấp FTP login information để nhập một tên người dùng và password vốn có các quyền truy cập đến server đích.

Nếu mạng của bạn sử dụng một proxy server, hãy chọn hộp kiểm use proxy server, sau đó nhập tên server và cổng mà nó sử dụng trong các hộp text đã cung cấp.

4. Nhấp nhãn Advanced Update Option để xác định những gì mà trình tiện ích sẽ sử dụng với các file mà nó tải xuống. Sau đây là các tùy chọn của bạn;

- ❖ **Backup the existing .DAT files.** Chọn hộp kiểm này để yêu cầu trình tiện ích AutoUpdate sao chép và lưu trữ các file .DAT mà bạn đã cài đặt trên hệ thống trước khi nó tải xuống các file mới.
- ❖ **Retrieve the Update file but do not perform the update.** Chọn hộp kiểm này để tải xuống các file mới .DAT, sau đó chờ để chạy hoạt động cập nhật vào thời điểm sau.

Nếu bạn chọn hộp kiểm này, trình tiện ích AutoUpdate tự

động chọn **Save the Update files for later usage** nằm bên dưới trên trang đặc tính này. Nhập vị trí mà bạn muốn trình tiện ích lưu các file mà nó tải xuống hoặc nhấp **Browse** để xác định thư mục thích hợp.

Việc chọn hộp kiểm này cũng sẽ làm cho các hộp kiểm **Backup the existing .DAT files**, **Force Update** và **Reboot system, if needed, after a successful update** trở nên không có sẵn.

- ❖ **Force Update.** Chọn hộp kiểm này để yêu cầu trình tiện ích **AutoUpdate** cài đặt các file .DAT mà nó tải xuống, ngay cả nếu chúng có cùng một số phiên bản với số phiên bản mà bạn đã cài đặt.

Thông thường, trình tiện ích sẽ không tải xuống các file .DAT vốn có cùng một số phiên bản, hoặc một số cũ hơn các file .DAT đã được cài đặt trên hệ thống. Nếu các file .DAT bị hư và bạn muốn thay thế chúng, tuy nhiên, hoặc nếu bạn muốn phục hồi một phiên bản file .DAT ban đầu, hãy chọn hộp kiểm này để áp buộc trình ứng dụng cài đặt các file mà nó tải xuống.

- ❖ **Reboot system, if needed, after a successful update.** Chọn hộp kiểm này để khởi động lại hệ thống một cách tự động khi trình tiện ích **AutoUpdate** cài đặt xong các file .DAT mới.

Trong hầu hết các trường hợp, bạn sẽ không cần khởi động lại để phần mềm **VirusScan** sử dụng các file .DAT mới, nhưng một số hệ thống sẽ đòi hỏi bạn thực hiện điều này để các file mới kích hoạt. Nếu bạn khởi động lại hệ thống vào một thời điểm thuận lợi hơn, hãy hủy chọn hộp kiểm này.

- ❖ **Save the Update file for later usage.** Chọn hộp kiểm này để lưu các file .DAT mới mà trình tiện ích **AutoUpdate** tải xuống để sử dụng sau này.

Kế đó, hãy nhập vị trí mà bạn muốn trình tiện ích lưu các file mà nó tải xuống hoặc nhấp **Browse** để xác định một thư

mục thích hợp.

- ❖ Run a Program after a succesful Update. Chọn hộp kiểm này để chạy một chương trình sau khi trình tiện ích AutoUpdate cài đặt các file .DAT mới mà nó tải xuống.

Tiếp theo, nhập đường dẫn và tên của file thực thi mà bạn muốn chạy vào hộp text đã cung cấp hoặc nhấp Browse để xác định file chương trình.

5. Khi bạn đã chọn các tùy chọn của mình có thể nhấp OK để lưu các cài đặt và quay trở về hộp thoại Task Properties hoặc nhấp Cancel để đóng hộp thoại này mà không lưu các cài đặt của bạn.

VI. Cấu hình trình tiện ích AutoUpdate

Để cập nhật các file chương trình cho phần mềm VirusScan, bạn phải thông báo cho trình tiện ích AutoUpgrade biết:

- ❖ Các site cập nhật nào có các file mới mà bạn muốn tải xuống
- ❖ Phương pháp truyền tải nào mà bạn muốn nó sử dụng để tải xuống
- ❖ Bạn có sử dụng một proxy server hay không và nếu có thì cho biết cổng nào mà bạn đã gán vào nó.
- ❖ Những gì mà bạn muốn nó thực hiện với các file mà nó tải xuống - cài đặt chúng, lưu chúng để sử dụng sau này hoặc cả hai.
- ❖ Bạn có muốn nó khởi động lại hệ thống sau khi nâng cấp hay không
- ❖ Bạn có muốn nó theo dõi các hoạt động của nó trong một log file hay không

Các trang đặc tính trong hộp thoại Automatic Upgrade Properties điều khiển các tùy chọn cho tác vụ nâng cấp của bạn. Bạn có thể nhấp lần lượt mỗi nhãn để cấu hình tác vụ này.

Để hiển thị hộp thoại Automatic Upgrade, hãy thực hiện những bước sau đây:

1. Nhấp đúp tác vụ AutoUpgrade trong danh sách tác vụ Console để mở hộp thoại Task Properties.
2. Nhấp Configure.

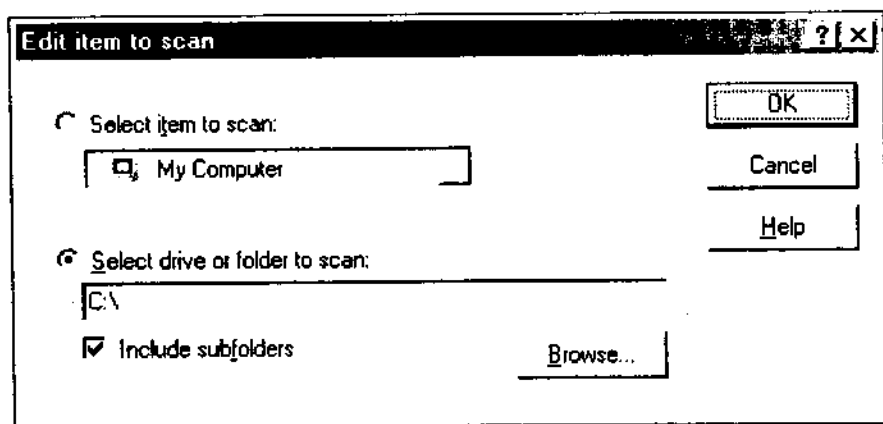
Hộp thoại Automatic Update xuất hiện.

Danh sách các site cập nhật trình bày các site nào mà bạn đã yêu cầu trình tiện ích sử dụng. Nó cũng thông báo trạng thái hiện hành của mỗi site dưới dạng Enable hay Disabled. Một site được vận hành nếu bạn đã chọn hộp kiểm Enabled trong hộp thoại Automatic Update Properties. Một site được hủy vận hành nếu bạn hủy chọn hộp kiểm này. Sự chỉ định này không thay đổi việc trình tiện ích AutoUpdate có thể nối kết với site hay không.

Trình tiện ích AutoUpgrade có thể tải xuống các file chương trình mới từ bất kỳ FTP site hay site dùng chung mạng nào mà bạn xác định. Bạn có thể chỉ định nhiều site mà từ đó trình tiện ích có thể cố gắng tải xuống các file mới. Trình tiện ích sẽ lần lượt thử mỗi site phải bắt đầu từ trên cùng của danh sách, đến khi nó tải xuống thành công các file mới hoặc xác định rằng các file mới không hiện hữu.

3. Từ đây, bạn có thể:

- ❖ Thêm một site mới vào danh sách site nâng cấp. Nhấp Add để mở hộp thoại Automatic Upgrade Properties.
- ❖ Thay đổi các định nghĩa cho một site cập nhật hiện có. Chọn một site được trình bày trong danh sách site cập nhật, sau đó nhấp Edit để mở hộp thoại Automatic Upgrade Properties. Thực hiện các thay đổi mà bạn muốn, sau đó nhấp OK để lưu chúng và quay trở lại hộp thoại này.



- ❖ Loại bỏ một site hiện có ra khỏi danh sách site cập nhật. Chọn một site được trình bày trong danh sách site cập nhật, sau đó nhấn Delete.
- ❖ Xác định thứ tự mà trình tiện ích AutoUpgrade sẽ nối kết với các site đã liệt kê. Để định vị một site để trình tiện ích thử nó sớm hơn, chọn site, sau đó nhấn Move Up. Để chỉ định một site với chế độ ưu tiên thấp hơn, hãy chọn site rồi sau đó nhấn Move Down.
- ❖ Cập nhật các file ngay từ các site được liệt kê trong danh sách cập nhật, bằng cách sử dụng các tùy chọn cấu hình mặc định hoặc các tùy chọn mà bạn đã chọn cho tác vụ này. Nhấp Update Now.
- ❖ Xác định một log file và giới hạn kích cỡ của nó. Nhấp nhấn Log Activity. Theo mặc định, trình tiện ích ghi lại các hoạt động của nó trong file UPDATE UPGRADE ACTIVITY LOG.TXT bất cứ khi nào bạn ngưng tác vụ hoặc khi bạn tắt hệ thống. Nếu bạn thích nhập dữ liệu này hơn file text khác, hãy nhập đường dẫn và tên file của nó trong hộp text đã cung cấp hoặc nhấn Browse để định vị file. Trình tiện ích AutoUpdate sẽ không tạo một file text - nó sẽ chỉ ghi sang một file hiện có.

Tiếp theo, hãy chọn hộp kiểm Limit size of log file to để giới hạn kích cỡ của file UPDATE UPGRADE ACTIVITY LOG.TXT hoặc một log file khác mà bạn xác định trong hộp text đã cung cấp. Theo mặc định, log file có thể tăng kích cỡ đến 100K.

Nhấp () để cài đặt một kích cỡ hoặc nhập kích cỡ tối đa mà bạn thích hơn, tính bằng các kilobyte, vào hộp text đã cung cấp. Nếu bạn xóa hộp kiểm này, log file có thể tăng kích cỡ đến khi giới hạn khoảng trống đĩa hay giới hạn hệ thống file ngưng nó lại. Khi file đạt được kích cỡ tối đa mà bạn cài đặt, trình tiện ích AutoUpgrade trước tiên sẽ xóa nó, sau đó khởi động lại log từ vị trí mà nó được ngưng lại.

4. Khi bạn đã chọn một tùy chọn, hãy nhấp OK để lưu các cài đặt và quay trở về hộp thoại Task Properties hoặc nhấp Cancel để đóng hộp thoại này mà không lưu các cài đặt của bạn.

VII. Cài đặt các đặc tính của Automatic Upgrade

Để thêm một site mới mà từ đó trình tiện ích AutoUpgrade có thể tải xuống các file .DAT mới, hãy thực hiện những bước sau đây;

1. Nhập một tên mô tả trong hộp text Site Name vốn nhận biết rõ ràng site mới.

Ví dụ: Internal .DAT File Update Site.

2. Chọn hộp kiểm Enabled để chấp nhận site này để trình tiện ích AutoUpgrade sử dụng.

Việc hủy chọn hộp kiểm này sẽ làm cho trình tiện ích bỏ qua site này khi nó cố tải xuống các file .DAT mới.

3. Xác định phương pháp truyền tải nào mà trình tiện ích phải sử dụng để tải xuống các file mới. Sau đây là các tùy chọn của bạn:

❖ **Copy from a local network computer.** Nhấp nút này để yêu cầu trình tiện ích AutoUpgrade sử dụng cấu hình mạng

chuẩn của bạn để tìm các file mới trên máy tính cục bộ hoặc trên một máy tính tại vị trí khác trên mạng của bạn.

Kế đó, hãy sử dụng ký hiệu Universal Naming Convention (UNC) để nhập đường dẫn đi đến máy tính vốn chứa các file mới mà bạn muốn tải xuống trong hộp text có nhãn là Select a computer and directory. Bạn cũng có thể nhấp Browse để định vị thư mục mà bạn muốn.

Để sử dụng một ký hiệu UNC, bạn phải sử dụng cùng một account mà bạn đã dùng để nhập vào mạng, hãy xác định một tên người dùng và password đã nhập vào mạng. Để sử dụng account hiện hành, hãy chọn hộp kiểm Use Logged In Account.

Ghi chú

Trên các hệ thống Windows NT Workstation v4.0 và Windows 2000 Professional, việc chọn hộp kiểm Use Logged In Account sẽ có những tác dụng hơi khác nhau. Nếu bạn đã lập biểu sự cập nhật file của bạn, trình tiện ích AutoUpgrade sẽ sử dụng account dịch vụ riêng của nó để nhập vào server nâng cấp và tải xuống các file mới. Nếu bạn nhấp Update Now, trình tiện ích AutoUpgrade sẽ sử dụng cùng một account mà bạn đã dùng để nhập vào mạng nhằm nối kết với server nâng cấp.

Account phải có các quyền quản lý trên máy tính cục bộ của bạn - hoặc nói cách khác account phải là một phần của nhóm Local Administrators - để cài đặt máy quét mới hoặc bất kỳ file chương trình vốn thay thế các dịch vụ VirusScan hiện có.

Để sử dụng một account tùy ý, hãy hủy chọn hộp kiểm Use Logged In Account, sau đó nhấp UNC Login information để nhập một tên người dùng và password trong một account vốn có các quyền truy cập đến server đích.

- ❖ **FTP from a remote network computer.** Nhấp nút này để yêu cầu trình tiện ích AutoUpgrade tìm kiếm các file mới trên một FTP site mà bạn chỉ định.

Kế đó, nhập URL cho site mà bạn muốn sử dụng vào hộp text có dạng là Enter an FTP computer name and directory. Bạn phải nối kết với một site đã cài đặt cho FTP login nặc danh hoặc bạn phải chỉ định tên người dùng và password cho một account trên site.

Để yêu cầu trình tiện ích sử dụng một login nặc danh, hãy chọn hộp kiểm Use anonymous FTP login. Để xác định một account, hãy hủy chọn hộp kiểm use anonymous FTP login, sau đó nhập FTP login information để nhập một tên người dùng và password vốn có các quyền truy cập đến server đích.

Nếu mạng của bạn sử dụng một proxy server, hãy chọn hộp kiểm use proxy server, sau đó nhập tên server và cổng mà nó sử dụng trong các hộp text đã cung cấp.

4. Nhấp nhấn Advanced Update Option để xác định những gì mà trình tiện ích sẽ thực hiện với các file mà nó tải xuống. Sau đây là các tùy chọn của bạn:

❖ **Retrieve the Upgrade file but do not perform the upgrade.** Chọn hộp kiểm này để tải xuống các file mới .DAT, sau đó chờ để chạy hoạt động cập nhật vào thời điểm sau này.

Nếu bạn chọn hộp kiểm này, trình tiện ích AutoUpgrade tự động chọn Save the Update files for later usage nằm bên dưới trên trang đặc tính này. Nhập vị trí mà bạn muốn trình tiện ích lưu các file mà nó tải xuống hoặc nhấp Browse để xác định thư mục thích hợp.

❖ **Reboot system, if needed, after a successful update.** Chọn hộp kiểm này để khởi động lại hệ thống một cách tự động khi trình tiện ích AutoUpgrade cài đặt xong các file .DAT mới.

Trong hầu hết các trường hợp, bạn sẽ không cần khởi động lại để phần mềm VirusScan sử dụng các file chương trình mới. Cấu trúc mới trong phần mềm VirusScan 4.5 sẽ tự động

ngừng bất kỳ dịch vụ hoạt động, cập nhập các file mới, sau đó khởi động lại các dịch vụ một lần nữa.

- ❖ **Save the Upgrade file for later usage.** Chọn hộp kiểm này để lưu các file chương trình mới mà trình tiện ích AutoUpgrade tải xuống để sử dụng sau này.

Kế đó, hãy nhập vị trí mà bạn muốn trình tiện ích lưu các file mà nó tải xuống hoặc nhấp Browse để xác định một thư mục thích hợp.

5. Khi bạn đã chọn các tùy chọn của mình, nhấp OK để lưu các cài đặt và quay trở về hộp thoại Task Properties hoặc nhấp Cancel để đóng hộp thoại này mà không lưu các cài đặt của bạn.

Bài 13

TÌM HIỂU TRÌNH TIỆN ÍCH TẠO EMERGENCY DISK

Khi nó tự cài đặt, phần mềm VirusScan sẽ kiểm tra bộ nhớ của máy tính và các boot sector của đĩa cứng để xác minh rằng nó có thể an toàn sao chép các file của nó sang đĩa cứng mà không có nguy cơ làm lây nhiễm. Trong suốt tiến trình cài đặt đó, Setup cung cấp cho bạn tạo một Emergency Disk mà bạn có thể dùng để khởi động hệ thống trong một môi trường không có virus. Nếu phần mềm VirusScan phát hiện nhiễm hoặc nếu bạn muốn bảo đảm máy tính của bạn sạch trước khi bạn cài đặt bất kỳ phần mềm khác, hãy tạo và sử dụng một Emergency Disk để khởi động máy tính của bạn.

Emergency Disk mà bạn tạo chứa BOOTSCAN.EXE mà bạn có thể dùng để quét các boot sector đĩa cứng và Master Boot Record (MBR). BOOTSCAN.EXE hoạt động với tập hợp các file xác định virus (.DAT). Nó chuyên biệt vốn tập trung việc tìm kiếm các virus boot-sector. Nếu bạn đã cài đặt phần mềm VirusScan bằng các tùy chọn setup mặc định, bạn sẽ tìm thấy những file .DAT này trong vị trí sau trên đĩa cứng:

C:\Program Files\Common Files\McAfee VirusScan\VirusScan Engine\4.0.xx

Các file .DAT đặc biệt có các tên sau đây:

- ❖ EMCLEAN.DAT
- ❖ EMNAMES.DAT
- ❖ EMSCAN.DAT

Theo định kỳ, McAfee cập nhật các file .DAT này để phát hiện các virus boot-sector mới. Bạn có thể tải xuống các file

Emergency.DAT đã cập nhật từ vị trí sau;

http://www.nai.com/asp/set/anti_virus/avert/tools.asp

Ghi chú

McAfee đề nghị bạn nên tải xuống trực tiếp các file Emergency.DAT mới sang một đĩa mềm vừa mới định dạng để giảm nguy cơ gây nhiễm.

Emergency Disk mà bạn tạo cũng sẽ chứa các file khởi động cần thiết để khởi động máy tính của bạn. Nếu máy tính của bạn chạy Windows 95 hay Windows 98 và bạn có một đĩa được định dạng dưới dạng một FAT-16 partition, bạn có thể sử dụng các file hệ thống Windows để khởi động máy tính. Nếu máy tính của bạn chạy Window NT Workstation v4.0 hay Windows 2000 Professional, bạn phải sử dụng các file hệ điều hành NAI-OS độc quyền với Emergency Disk vì các file hệ thống cho những hệ điều hành này sẽ không sắp xếp vừa trên một đĩa mềm đơn.

Phần mềm VirusScan đi kèm với một wizard Emergency Disk vốn làm cho việc tạo đĩa trở nên đơn giản và nhanh. Để tìm hiểu thêm về trình tiện ích Emergency Disk và về cách sử dụng wizard, hãy nhấp các nút bên cạnh mỗi chủ điểm được liệt kê.

1. Các file VirusScan Emergency Disk

Wizard Emergency Disk sẽ sao chép các file mà bạn cần để khởi động máy tính và quét đĩa cứng để tìm các virus boot-sector. Những file này một trình quét dòng lệnh footprint được thu nhỏ, một tập hợp các file (.DAT) xác định virus khẩn cấp và các file khởi động vốn cho phép bạn khởi động máy tính từ Emergency Disk.

Bảng sau đây liệt kê các file xuất hiện trên Emergency Disk khi bạn tạo nó:

File	Chức năng	Vị trí
AUTOEXEC .BAT	File lô MS-DOS. File này hướng dẫn bạn hoạt động quét ngay tức thì ngay khi Emergency Disk khởi	A:\

	động xong máy tính	
BIOS.SYS	File hệ thống	A:\
BOOTSCAN.EXE	Trình quét dòng lệnh McAfee. File này thực hiện hoạt động quét trên đĩa cứng.	A:\
CLEAN.DAT	File xác định virus McAfee. File này là một phiên bản chuyên biệt nhỏ hơn của file CLEAN.DAT mà các thành phần VirusScan sử dụng. Bạn không thể sử dụng một file CLEAN.DAT từ thư mục chương trình VirusScan dành cho Emergency Disk.	A:\
COMMAND.COM	Trình thông dịch lệnh. File này là một vỏ lệnh vốn trả lời dữ liệu nhập tại dòng lệnh nhập.	A:\
GETREPLY.EXE	File trình ứng dụng. File này xử lý dữ liệu xuất từ hoạt động quét.	A:\
KERNEL.SYS	File hệ thống	A:\
LICENSE.DAT	File McAfee License. Trình quét dòng lệnh sử dụng file này để theo dõi tính đủ điều kiện sử dụng sản phẩm này.	A:\
MESSAGES.DAT	File nguồn tài nguyên McAfee. File này lưu trữ các thông báo trình ứng dụng để sử dụng trong suốt các hoạt động quét.	A:\
NAMES.DAT	File xác định virus McAfee. File này là một phiên bản chuyên biệt nhỏ hơn của file NAMES.DAT mà các thành phần VirusScan khác sử dụng. Bạn không thể sử dụng	A:\

một file NAMES.DAT từ thư mục chương trình VirusScan dành cho Emergency Disk.

SCAN.DAT	File xác định virus McAfee. File này là một phiên bản chuyên biệt nhỏ hơn của file NAMES.DAT mà các thành phần VirusScan khác sử dụng. Bạn không thể sử dụng một file NAMES.DAT từ thư mục chương trình VirusScan dành cho Emergency Disk.
----------	--

II. Sử dụng wizard tạo Emergency Disk

Trình tiện ích VirusScan Setup cho bạn cơ hội tạo một Emergency Disk trong suốt quá trình cài đặt, nếu bạn muốn. Bạn cũng có thể tạo một Emergency Disk mới tại bất kỳ thời điểm nào nếu bạn đã làm mất một Emergency Disk mà bạn đã tạo.

Để tạo Emergency Disk, hãy thực hiện những bước sau đây;

1. Nhấp Start trong thanh tác vụ Windows, trở vào Programs, sau đó trở vào McAfee VirusScan. Kế đó, chọn Create Emergency Disk.
Panel wizard Emergency Disk đầu tiên sẽ xuất hiện.
2. Nhấp Next> để tiếp tục.
3. Nếu máy tính của bạn chạy Windows NT Workstation v4.0 hay Windows 2000 Professional, wizard sẽ thông báo cho bạn biết rằng bạn phải định dạng Emergency Disk bằng NAI-OS độc quyền. Nhấp Next để tiếp tục, sau đó nhảy sang bước 5.
4. Nếu máy tính của bạn chạy Windows 95 hay Windows 98, wizard sẽ định dạng đĩa Emergency Disk bằng NAI-OS hoặc bằng các file khởi động Windows. Chọn các file hệ điều hành nào mà bạn muốn sử dụng, sau đó nhấp Next để tiếp tục.
5. Chèn một đĩa mềm 1.44MB chưa được khóa và chưa định dạng vào ổ đĩa mềm. McAfee đề nghị bạn nên sử dụng một đĩa hoàn

toàn mới mà bạn đã chưa định dạng trước đây để tránh khả năng gây nhiễm virus trên Emergency Disk của bạn.

6. Nhấp Next để tiếp tục.

Wizard Emergency Disk sẽ sao chép các file của nó từ một ảnh đĩa được lưu trữ trong thư mục chương trình VirusScan. Khi nó thực hiện điều này, nó sẽ hiển thị tiến trình của nó trong một wizard panel.

7. Nhấp Finish để thoát wizard khi nó đã tạo đĩa tiếp theo, lấy đĩa ra ổ đĩa mềm, khóa nó, tạo nhãn cho nó là McAfee Emergency Boot Disk và lưu trữ nó tại một nơi an toàn.

III. Chạy một hoạt động quét Emergency Disk

Để khởi động máy tính và quét đĩa cứng trong một môi trường không có virus, hãy thực hiện những bước sau đây:

1. Tắt máy tính theo cách thông thường, sau đó tắt nguồn điện hoàn toàn. Không được cài đặt lại hoặc khởi động lại máy tính.
2. Chèn Emergency Disk đã khóa trong ổ đĩa mềm, chờ ít nhất 15 giây, sau đó mở điện.

Ghi chú

Nếu bạn đã cấu hình BIOS của máy tính để tìm kiếm mã khởi động của nó trước tiên trên ổ đĩa C:, bạn nên thay đổi các cài đặt BIOS để máy tính tìm kiếm trên ổ đĩa A: hay ổ đĩa B: trước tiên. Tham khảo tài liệu phần cứng để biết cách cấu hình các cài đặt BIOS.

3. Sau khi nó khởi động máy tính, Emergency Disk chạy một file lô vốn hướng dẫn bạn thực hiện hoạt động quét khẩn cấp. Trước tiên file lô hỏi bạn có khởi động máy tính theo chu kỳ hay không. Gõ nhập y để tiếp tục.
4. File lô cho bạn biết rằng nó sẽ bắt đầu một hoạt động quét. Đọc thông báo được hiển thị trên màn hình, sau đó nhấn bất kỳ phím nào trên bàn phím để tiếp tục.

Emergency Disk tải các file mà nó cần để thực hiện hoạt động quét vào bộ nhớ. Nếu bạn có bộ nhớ mở rộng trên máy tính, nó sẽ tải các file cơ sở dữ liệu của nó vào bộ nhớ đó để thực thi nhanh hơn. BOOTSCAN.EXE, trình quét dòng lệnh vốn đi kèm với Emergency Disk, sẽ thực hiện bốn tiến trình quét để kiểm tra các boot sector đĩa cứng, Master Boot Record (MBR), các Thư mục hệ thống, file chương trình và các Nơi có thể bị lây nhiễm trên tất cả đĩa cứng của máy tính.

Ghi chú

McAfee đề nghị bạn không nên làm gián đoạn trình quét BOOTSCAN.EXE khi nó chạy hoạt động quét của nó.

Emergency Disk sẽ không phát hiện các virus macro, các virus script hay các chương trình ngựa thành Trojan, nhưng nó sẽ phát hiện các virus gây nhiễm file và các virus boot sector.

Nếu BOOTSCAN.EXE tìm thấy một virus, nó sẽ cố làm sạch file bị nhiễm. Nếu nó không thực hiện được, nó sẽ không thể truy cập đến file và tiếp tục hoạt động quét. Sau khi nó hoàn tất tất cả giai đoạn quét của nó, nó trình bày một báo cáo tổng hợp về các hoạt động mà nó thực hiện cho mỗi đĩa cứng trên màn hình. Báo cáo này sẽ cho bạn biết:

- ❖ Bao nhiêu file mà trình quét đã kiểm tra
- ❖ Bao nhiêu file của số đó trở nên sạch hoặc không bị nhiễm
- ❖ Bao nhiêu file chứa các phần lây nhiễm tiềm ẩn
- ❖ Bao nhiêu file của số đó mà trình quét đã làm sạch
- ❖ Bao nhiêu file MBR và boot sector mà trình quét đã kiểm tra.
- ❖ Bao nhiêu file MBR và boot sector có chứa các phần nhiễm tiềm ẩn

Nếu trình quét phát hiện một virus, nó phát ra tín hiệu và thông báo tên và vị trí của virus trên màn hình.

Khi trình quét kiểm tra xong đĩa cứng, hãy lấy Emergency Disk ra khỏi ổ đĩa mềm, sau đó tắt lại máy. Khi bạn khởi động lại, hãy sử dụng trình ứng dụng VirusScan để quét hoàn toàn hệ thống của bạn nhằm bảo đảm rằng hệ thống của bạn không bị nhiễm virus.

 Bài 14

TÌM HIỂU PANEL ĐIỀU KHIỂN VIRUSSCAN

Panel điều khiển VirusScan phục vụ như front end đồ họa cho dịch vụ quản lý VirusScan, dịch vụ này khởi chạy và điều khiển tất cả tiến trình xử lý thành phần cấp cao nhất, kể cả trình ứng dụng VirusScan, Console và trình quét VShield. Dịch vụ quản lý VirusScan cũng cung cấp một cấu trúc bộ nhớ chung cho tất cả các thành phần VirusScan, điều này cho phép các thành phần dùng chung dữ liệu với nhau và hoạt động trên dữ liệu đó.

Theo các thuật ngữ thực tế, bạn có thể sử dụng panel điều khiển để:

- ❖ Khởi động và ngưng tất cả thành phần VirusScan bằng một nút duy nhất
- ❖ Yêu cầu trình quét VShield và VirusScan Console phải tải ngay khi máy tính khởi động
- ❖ Cài đặt một ceiling (trần giới hạn) cho số đích quét mà trình ứng dụng VirusScan có thể kiểm tra và loại trừ trong suốt một tác vụ quét.
- ❖ Giới hạn số tác vụ quét mà bạn có thể tạo, cấu hình và chạy từ VirusScan Console

Bạn cũng có thể chọn để yêu cầu dịch vụ quản lý VirusScan tự tải khi máy tính khởi động.

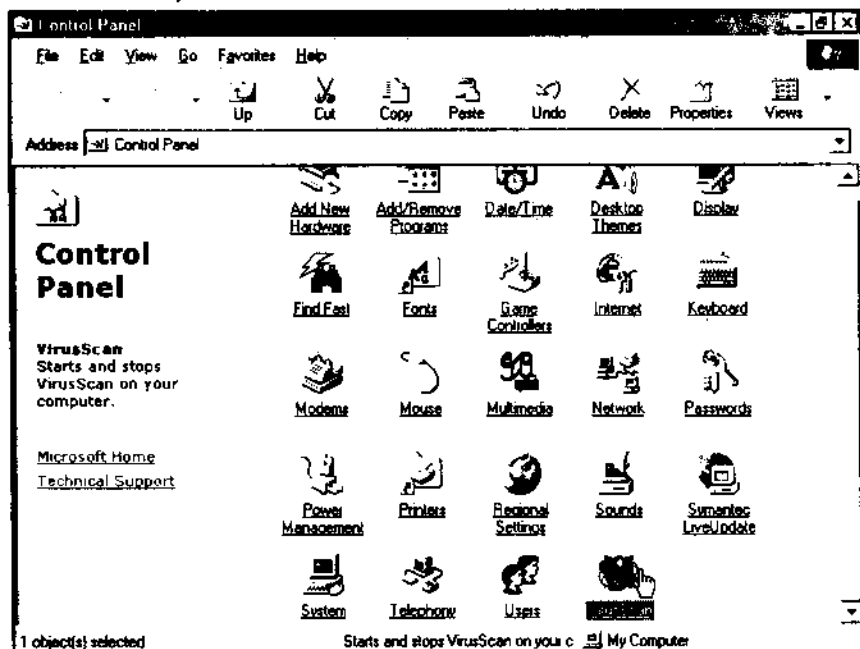
Ghi chú

McAfee yêu cầu bạn nên cài đặt dịch vụ quản lý VirusScan để tải lúc khởi động. Nếu không bạn không thể khởi động một số thành phần

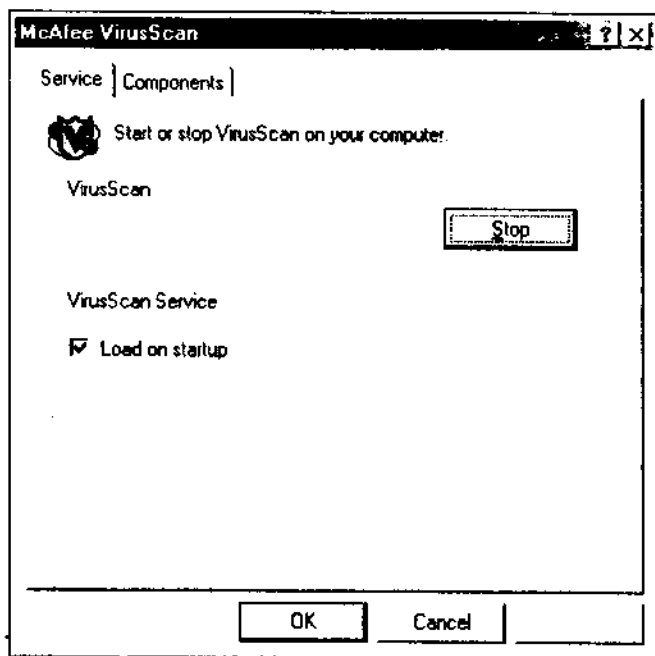
VirusScan, và bạn sẽ mất quyền lợi dùng chung dữ liệu giữa các thành phần.

Để mở panel điều khiển VirusScan, hãy thực hiện các bước sau đây:

1. Nhấp Start trong thanh tác vụ Windows, trở vào Settings, sau đó chọn Control Panel.



2. Định vị và nhấp đôi panel điều khiển VirusScan để mở nó.



I. Các file panel điều khiển VirusScan

Là tiến trình ban đầu cho tất cả thành phần VirusScan, dịch vụ quản lý VirusScan không phụ thuộc vào các thành phần VirusScan khác. Nó phụ thuộc vào một số thành phần hệ thống Windows để chạy.

Bảng sau đây liệt kê một file panel điều khiển VirusScan và chỉ dẫn những nơi mà bạn có thể tìm thấy chúng.

File	Chức năng	Vị trí
AVSYNMGR .EXE	Dịch vụ quản lý VirusScan. Khởi chạy, khởi động và ngưng tất cả dịch vụ và thành phần VirusScan. Phải chạy để vận hành tất cả thành phần VirusScan.	C:\Program Files\ McAfee VirusScan\ VirusScan

AVSYNCH.DLL	Điều khiển sự giao tiếp giữa các thành phần thông qua bộ nhớ dùng chung	C:\Program Files\McAfee VirusScan\
SYNCUTIL.DLL	Lưu trữ dữ liệu được dùng chung giữa các thành phần	C:\Program Files\McAfee VirusScan\
VSUTIL.DLL	Cung cấp các tiện ích thông thường cho các thành phần	C:\Program Files\McAfee VirusScan\
AVSMCPA.CPL	Applet panel điều khiển VirusScan	C:\Windows\System hay C:\Winnt\System

32

Các file tạm thời

Panel điều khiển VirusScan và các file liên quan của nó sử dụng các file này dưới dạng “memory maps” để lưu trữ các tùy chọn cấu hình được sao chép từ bộ ghi Windows khi chương trình chạy. Những file này bắt đầu với một kích cỡ file chuẩn và dữ liệu tối thiểu và tăng lên hoặc thu nhỏ khi cần thiết để chứa dữ liệu cấu hình

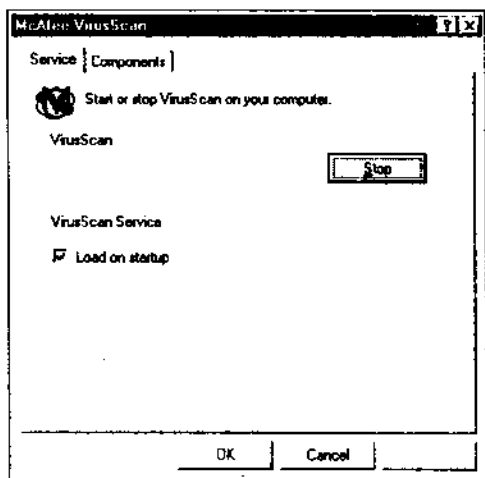
File	Chức năng	Vị trí
SYNC_MAP.MMF	File ánh xạ bộ nhớ cho AVSYNCH.DLL	C:\Program Files\McAfee VirusScan\
AVCONSOLE.MMF	File ánh xạ bộ nhớ cho SYNCUTIL.DLL	C:\Program Files\McAfee VirusScan\
DAV_CONS.MMF	File ánh xạ bộ nhớ cho SYNCUTIL.DLL	C:\Program Files\McAfee VirusScan\
DAV_EXCL.MMF	File ánh xạ bộ nhớ cho SYNCUTIL.DLL	C:\Program Files\McAfee VirusScan\

DAV_SCAN .MMF	File ánh xạ bộ nhớ cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
DEXCLDEF .MMF	File ánh xạ bộ nhớ cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
DSCANDEF .MMF	File ánh xạ bộ nhớ cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
DVS_EXCL .MMF	File ánh xạ bộ nhớ cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
VSCANGEN .MMF	File ánh xạ bộ nhớ cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
VSCANOAS .MMF	File ánh xạ bộ nhớ cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan
VSCANODS .MMF	File ánh xạ bộ nhớ cho SYNCUTIL.DLL	C:\Program Files\ McAfee VirusScan\ VirusScan

II. Làm việc với panel điều khiển VirusScan

Để chọn các tùy chọn panel điều khiển VirusScan, hãy thực hiện những bước sau đây:

1. Mở panel điều khiển, sau đó nhấp nhấn Service.
2. Để ngưng tất cả thành phần VirusScan hoạt động, hãy nhấp Stop.



Nếu tất cả thành phần VirusScan vốn thường tải vào bộ nhớ - VirusScan và trình quét VShield - không hoạt động, nút này sẽ là nút Start. Nhấp nó để tải lại các thành phần VirusScan không hoạt động. Bạn cũng có thể khởi động lại trình ứng dụng VirusScan và Console từ menu Start của Windows.

3. Chọn hộp kiểm Load on startup trong vùng VirusScan Service để khởi động dịch vụ quản lý VirusScan (AVSYNMGR.EXE) ngay khi bạn khởi động máy tính.

Dịch vụ quản lý thấy được tất cả sự giao tiếp giữa các thành phần chương trình VirusScan, xác định những thành phần nào phải tải để hoàn thành các tác vụ chương trình, và cho phép bạn bắt đầu và ngưng tất cả thành phần chương trình cùng một lúc.

Nếu máy tính của bạn chạy Windows NT Workstation v4.0 hay Windows 2000 Professional, dịch vụ này xuất hiện trong hộp thoại Services dưới dạng AvSync Manager. Nếu máy tính của bạn chạy Windows 95 hay Windows 98, dịch vụ này trực tiếp không thể truy cập được.

Ghi chú

McAfee đề nghị bạn nên cài đặt dịch vụ quản lý VirusScan để tải lúc khởi động, nếu không bạn không thể khởi động một số thành phần

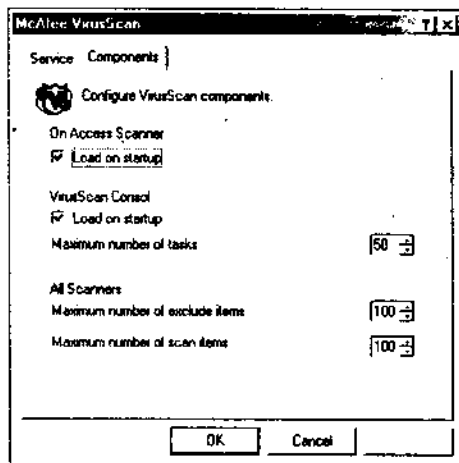
VirusScan, và bạn sẽ mất quyền lợi dùng chung dữ liệu giữa các thành phần.

4. Nhấp nhấn Components để tiếp tục.
5. Để yêu cầu trình quét VShield tải khi bạn khởi động máy tính, hãy chọn hộp kiểm Load VShield on startup. Cài đặt tương tự này xuất hiện trong trang System Scan module's Detection. Cài đặt sẽ tải trình quét khi bạn khởi động máy tính.

Ghi chú

McAfee đề nghị bạn nên để lại hộp kiểm này được chọn. Trình quét VShield là sự phòng ngự liên tục tốt nhất chống lại việc nhiễm virus.

6. Nhấp  hoặc nhập một số trong hộp text Exclude Items để xác định bao nhiêu hạng mục có thể xuất hiện trong danh sách loại trừ của module VShield System Scan module.
Cài đặt này cũng xác định bao nhiêu hạng mục có thể xuất hiện trong danh sách loại trừ cho bất kỳ tác vụ quét của trình ứng dụng VirusScan hoặc bất kỳ tác vụ quét mà bạn cấu hình từ trong VirusScan Console. Theo mặc định, 100 hạng mục có thể xuất hiện trong danh sách. Bạn không thể cài đặt giá trị ở đây ít hơn năm thành phần.



7. Nhấp  hoặc nhập một số trong hộp Scan Items để xác định bao nhiêu đích mà trình ứng dụng VirusScan có thể kiểm tra cùng một lúc.

Cài đặt này xác lập một số hạng mục tối đa vốn có thể xuất hiện dưới dạng các đích quét cho bất kỳ tác vụ quét mặc định - hoặc bất kỳ tác vụ mà bạn cấu hình - từ bên trong VirusScan Console. Theo mặc định, 100 hạng mục có thể xuất hiện trong danh sách. Nếu bạn thêm hơn 100 hạng mục riêng biệt vào danh sách loại trừ, trình ứng dụng VirusScan có thể ảnh hưởng đến sự hoạt động của hệ thống. Bạn không thể cài đặt giá trị ở đây ít hơn năm hạng mục.

8. Chọn hộp kiểm Load on startup trong vùng Console để yêu cầu VirusScan Console khởi động ngay khi bạn khởi động máy tính.

Console phải chạy để thực thi bất kỳ tác vụ mà bạn đã lập biểu, kể cả các tác vụ quét, các tác vụ AutoUpgrade và tác vụ AutoUpdate. Bạn không cần khởi động Console để khởi động trình quét VShield.

9. Nhấp  hoặc nhập một số vào hộp text Maximum Number of Tasks để cho biết bao nhiêu tác vụ quét có thể xuất hiện trong cửa sổ VirusScan Console.

Theo mặc định, 50 hạng mục có thể xuất hiện trong danh sách. Nếu bạn thêm hơn 50 hạng mục, sự thực thi tác vụ có thể tác động đến hoạt động của hệ thống. Bạn không thể cài đặt giá trị ở đây ít hơn năm hạng mục.

10. Nhấp Apply để lưu các thay đổi mà bạn thực hiện đối với những cài đặt này mà không đóng panel điều khiển. Nhấp OK để lưu các thay đổi của bạn và đóng panel điều khiển. Nhấp Cancel để đóng panel điều khiển mà không lưu các thay đổi của bạn.

Ghi chú

Dịch vụ quản lý VirusScan phải tự khởi động lại và tất cả thành phần VirusScan hoạt động để thực thi bất kỳ thay đổi mà bạn thực hiện.

Bài 15

TÌM HIỂU CÁC TRÌNH QUÉT ĐỒNG LỆNH VIRUSSCAN

Phần mềm chống virus VirusScan đi kèm với một tập hợp các trình quét dòng lệnh mà bạn có thể dùng để chạy trực tiếp các hoạt động quét trong một môi trường dòng lệnh. Tập hợp này gồm có:

- ❖ SCAN.EXE, một trình quét chỉ dành cho các môi trường 32 bit. Đây là giao diện dòng lệnh chính. Khi bạn chạy file này, trước tiên nó kiểm tra môi trường của nó để xem nó có thể tự chạy hay không. Nếu máy tính của bạn chạy trong chế độ 16 bit hay chế độ được bảo vệ, nó sẽ truyền sự điều khiển đến một trong những chương trình quét khác.
- ❖ SCANPM.EXE, một trình quét cho các môi trường 16 và 32 bit. Trình quét này cung cấp cho bạn một tập hợp các tùy chọn quét dành cho các môi trường DOS có chế độ bảo vệ 32 bit và 16 bit. Nó cũng bao hàm sự hỗ trợ cho bộ nhớ mở rộng và các phần cấp phát bộ nhớ linh động. SCAN.EXE sẽ truyền sự điều khiển đến trình quét này khi các tính năng chuyên biệt của nó có thể cho phép hoạt động quét của bạn chạy một cách hiệu quả hơn.
- ❖ SCAN86.EXE, một trình quét chỉ dành cho các môi trường 16 bit. Trình quét này gồm có một tập hợp các tính năng giới hạn dành cho các môi trường 16 bit. SCAN.EXE sẽ truyền sự điều khiển đến trình quét này nếu máy tính của bạn chạy trong chế độ 16 bit, nhưng không có các cấu hình bộ nhớ đặc biệt.

- ❖ BOOTSCAN.EXE, một trình quét chuyên dụng nhỏ hơn để sử dụng chủ yếu với trình tiện ích Emergency Disk. Trình quét này thường chạy từ một đĩa mềm mà bạn tạo để cung cấp cho bạn một môi trường khởi động không có virus.

Khi bạn chạy wizard tạo Emergency Disk, phần mềm VirusScan sao chép BOOTSCAN.EXE, một tập hợp các file .DAT chuyên dụng và các file khởi động sang một đĩa mềm. Với đĩa này, bạn có thể khởi động máy tính, sau đó quét bộ nhớ của nó và Master Boot Record, boot sector, và các file hệ thống trên đĩa cứng. BOOTSCAN.EXE sẽ không phát hiện hoặc làm sạch các virus macro, nhưng nó sẽ phát hiện hoặc làm sạch các virus khác vốn có thể gây hại cho tiến trình cài đặt phần mềm VirusScan của bạn hoặc gây nhiễm các file lúc khởi động hệ thống. Một khi bạn nhận biết và phản ứng lại những virus đó, bạn có thể an toàn chạy phần mềm VirusScan để làm sạch phần còn lại của hệ thống, miễn là bạn không chạy bất kỳ chương trình khác trong thời gian đó.

Tất cả trình quét dòng lệnh cho phép bạn khởi chạy tất cả hoạt động quét từ cửa sổ MS-DOS Prompt hoặc Command Prompt, hoặc từ chế độ MS-DOS được bảo vệ. Thông thường, bạn sẽ sử dụng giao diện người dùng đồ họa (GUI) của trình ứng dụng VirusScan để thực hiện hầu hết các hoạt động quét, nhưng nếu bạn gặp sự cố trong việc khởi động Windows hoặc nếu các thành phần VirusScan GUI sẽ không chạy trong môi trường của bạn, bạn có thể sử dụng các trình quét dòng lệnh làm một bản sao lưu dự phòng.

Để bắt đầu một hoạt động quét từ dòng lệnh, hãy thực hiện các bước sau đây:

Để bắt đầu một hoạt động quét từ dòng lệnh, hãy thực hiện những bước sau đây:

1. Nhấp Start trong thanh tác vụ Windows, trở đến Programs, sau đó chọn Command Prompt trên các hệ thống Windows NT Workstation 4.0 và Windows 2000 Professional hoặc MS-DOS Prompt trên các hệ thống Windows 95 và Windows 98.
2. Chuyển sang thư mục VirusScan Engine. Nếu bạn đã cài đặt

phần mềm VirusScan bằng các tùy chọn Setup mặc định của nó, bạn sẽ tìm thấy thư mục trong đường dẫn sau:

C:\Program Files\Common Files\McAfee VirusScan\
VirusScan Engine\4.0.xx

Ghi chú

Nếu bạn thêm thư mục này vào câu lệnh đường dẫn cho hệ thống, bạn không cần chuyển sang thư mục này để chạy phần mềm VirusScan Command Line.

3. Gõ nhập dòng sau đây tại dòng nhắc lệnh:

scan [target: drive, path, or filename] [/option]

Tại đây, bạn có thể xác định đích quét dưới dạng một ổ đĩa trên hệ thống, ví dụ C:, dưới dạng một đường dẫn đi đến một thư mục mà bạn muốn quét, hoặc dưới dạng một tên file cụ thể. Đặt một ký tự gạch chéo (/) trước mỗi tùy chọn lệnh mà bạn muốn viện dẫn cho tác vụ quét này để phân biệt chúng với những phần khác của dòng lệnh. Một nội dung thảo luận về các tùy chọn lệnh cho trình quét VirusScan Command Line nằm ngoài phạm vi của file trợ giúp này, nhưng bạn có thể tìm thấy một nội dung mô tả tổng hợp về các tùy chọn có sẵn.

Trình quét Command Line cũng cho ra một mã cấp độ lỗi khi nó thực hiện xong hoạt động quét của nó. Cấp độ lỗi tổng hợp những gì đã xảy ra trong suốt hoạt động quét. Bạn có thể sử dụng mã này trong các file lô và các trình ứng dụng khác để thực hiện những hoạt động được qui định trên giá trị mà trình quét cho ra.

I. Các tùy chọn dành cho trình quét dòng lệnh VirusScan

Bảng sau đây liệt kê các tùy chọn hoặc các lệnh mà bạn có thể thêm vào dòng lệnh khi bạn chạy trình quét VirusScan Command Line. Bạn có thể sử dụng những tùy chọn này khi bạn chạy một hoạt động quét theo yêu cầu hoặc bắt đầu một tác vụ quét khi truy cập, trừ khi nội dung mô tả tùy chọn lưu ý.

Khi bạn xác định các đích quét, hãy nhớ đưa vào đầy đủ đường

dẫn đi đến file đích hay thư mục nếu nó nằm bên ngoài thư mục hoạt động.

Tùy chọn dòng lệnh	Giới hạn	Mô tả
/? hoặc HELP	Không có	Hiển thị một danh sách các tùy chọn dòng lệnh VirusScan, mỗi tùy chọn có một nội dung mô tả ngắn gọn.
/AD	Chỉ quét theo yêu cầu	Kết hợp các tùy chọn /ADL và /ADN để quét tất cả ổ đĩa cục bộ và ổ đĩa mạng.
/ADL	Chỉ quét theo yêu cầu	Quét tất cả các ổ đĩa cục bộ - kể cả ổ đĩa nén và các card PC, nhưng không phải các đĩa - ngoài bất kỳ ổ đĩa khác đã xác định trên dòng lệnh. Để quét cả ổ đĩa cục bộ và ổ đĩa mạng, hãy sử dụng tùy chọn /AD. OS/2: /ADL bao hàm ổ đĩa CD-ROM trong tác vụ quét khi được sử dụng với /NODDA.
/ADN	Chỉ quét theo yêu cầu	Quét tất cả ổ đĩa mạng để tìm các virus, ngoài bất kỳ ổ đĩa khác đã xác định trên dòng lệnh. Để quét cả ổ đĩa cục bộ và ổ đĩa mạng, hãy sử dụng tùy chọn /AD.
/ALERTPATH <dir>	Chỉ quét theo yêu cầu	Chỉ định thư mục <dir> làm một đường dẫn mạng cho

		các thông tin cảnh báo Centralized Alerting.
/ALL	Chỉ quét theo yêu cầu	Thay thế cài đặt quét mặc định bằng cách quét tất cả file có thể bị nhiễm - kể cả phần mở rộng. Việc sử dụng tùy chọn /ALL sẽ tăng thời gian quét được yêu cầu. Chỉ sử dụng nó nếu bạn tìm thấy một virus hoặc nghi ngờ rằng bạn có một virus.
/ANALYZE	Chỉ quét theo yêu cầu	Cài đặt trình quét để sử dụng các phương pháp suy nghiệm của nó, kể cả chương trình và macro.
	Yêu cầu bộ nhớ mở rộng	/MANALYZE chỉ nhắm vào các virus macro. /PANALYZE chỉ nhắm vào các virus gây nhiễm file.
/ANYACCESS	Chỉ quét khi truy cập	❖ boot sector bất cứ khi nào một đĩa được đọc hoặc được ghi sang ❖ các file thực thi ❖ bất kỳ file mới được tạo
/APPEND	Chỉ quét theo yêu cầu	Thêm text thông báo vào một file báo cáo được xác định bằng /REPORT thay vì ghi đè nó.
/BOOT	Chỉ quét theo yêu cầu	Chỉ quét boot sector và boot record chính
/BOOTACCESS	Chỉ quét khi truy cập	Quét boot sector của đĩa để tìm các virus bất cứ khi nào

		đĩa được truy cập (kể cả các hoạt động ghi/đọc)
/CLEAN	Chỉ quét theo yêu cầu	Loại bỏ mã virus ra khỏi tất cả file và các vùng hệ thống bị nhiễm.
/CLEANDOCALL	Chỉ quét theo yêu cầu	Yêu cầu SCAN.EXE xóa sạch tất cả macro ra khỏi các tài liệu Microsoft Word và Office bị nhiễm. SCAN.EXE chỉ thực hiện điều này nếu nó phát hiện ít nhất một virus macro trên hệ thống trong suốt hoạt động quét. Tùy chọn này xóa tất cả macro, kể cả macro không bị nhiễm virus.
/CONTACT <message>	Chỉ quét khi truy cập	Hiển thị thông tin đã xác định khi SCAN.EXE phát hiện một virus. Thông báo này không thể vượt quá 255 ký tự.
/CONTACTFILE	Không có	Hiển thị nội dung của <filename> khi SCAN.EXE tìm thấy một virus. Sử dụng tùy chọn này để cung cấp thông tin liên lạc và các hướng dẫn cho người dùng khi trình quét tìm thấy một virus. Tùy chọn này đặc biệt hữu dụng trong các môi trường mạng, bởi vì bạn có thể dễ dàng duy trì text thông báo

trong một file trung tâm thay vì trên mỗi trạm làm việc.

Bất kỳ ký tự hợp lệ trong một thông báo liên lạc ngoại trừ một dấu backslash (\). Các thông báo bắt đầu với một dấu slash (/) hay một dấu nối (-) sẽ được đặt trong các dấu trích dẫn.

/DAM	Chỉ quét theo yêu cầu	Xóa tất cả macro trong các file bị nhiễm. Nếu bạn kết hợp tùy chọn này với /FAM, sự kết hợp này sẽ xóa tất cả macro trong tất cả file, cho dù có bị nhiễm hay không, ngay khi trình quét tìm thấy một file bị nhiễm.
/DEL	Chỉ quét theo yêu cầu	Xóa vĩnh viễn các file bị nhiễm.
/EXCLUDE <filename>	Chỉ quét theo yêu cầu	Bỏ qua các file được liệt kê trong <filename> Sử dụng tùy chọn này để loại bỏ các file riêng biệt ra khỏi một hoạt động quét, liệt kê đầy đủ đường dẫn đi đến mỗi file mà bạn muốn loại bỏ trên dòng riêng của nó. Bạn có thể sử dụng các ký tự thay thế * và ?.

/FAM	Chỉ quét theo yêu cầu	Tìm tất cả các mã macro trong các file Microsoft Office bị nhiễm, cho dù các file có bị nhiễm hay không. Nếu bạn kết hợp tùy chọn này với /DAM, sự kết hợp này sẽ xóa tất cả macro trong tất cả file, cho dù nó có bị nhiễm hay không, ngay khi trình quét tìm thấy một file bị nhiễm.
/FILEACCESS	Chỉ quét khi truy cập	Quét các file thực thi khi bạn chỉnh sửa chúng theo bất kỳ cách nào, kể cả việc thực thi chúng. Hoạt động quét này sẽ không kiểm tra boot sector.
/FREQUENCY <n>	Chỉ quét theo yêu cầu	Ngăn cản một hoạt động quét mới trong các giờ <n> sau hoạt động quét trước đó. Trong các môi trường trong đó nguy cơ lây nhiễm rất thấp hoặc nơi mà việc sử dụng nguồn tài nguyên là một mối quan tâm, hãy sử dụng tùy chọn này để ngăn cản các hoạt động quét không cần thiết. Chú ý rằng tần số quét càng cao, thì khả năng bảo vệ chống lại việc lây nhiễm sẽ càng cao.
/HELP hay /?	Không có	Hiển thị một danh sách các

		tùy chọn dòng lệnh trình quét VirusScan, mỗi tùy chọn có một nội dung mô tả ngắn gọn.
/IGNORE <drive(s)>	Chỉ quét khi truy cập	Bỏ qua tất cả file được tải từ ổ đĩa đã xác định.
/IGNORE <filename>	Chỉ quét theo yêu cầu	Tải các tùy chọn quét từ file đã đặt tên. Sử dụng tùy chọn này để bắt đầu một hoạt động quét mà bạn đã cấu hình bằng cách tải các cài đặt tùy ý đã lưu trong một file có dạng ASCII. File này chỉ việc thu thập các tùy chọn dòng lệnh mà bạn muốn sử dụng.
/LOCK	Không có	Hoàn toàn tạm ngưng hệ thống khi SCAN.EXE tìm thấy một virus. /LOCK thích hợp trong các môi trường mạng để bị hư hỏng. McAfee đề nghị bạn nên sử dụng /LOCK với tùy chọn /CONTACTFILE để cho những người sử dụng biết những gì cần thực hiện hoặc những người nào cần liên lạc nếu VirusScan khóa hệ thống.
/MANALYZE	Chỉ quét theo yêu cầu	Cài đặt các tính năng quét suy nghiệm của trình quét để chỉ nhắm vào các virus

		macro.
	Yêu cầu bộ nhớ mở rộng	/PANALYZE chỉ nhắm vào các virus chương trình. /ANALYZE nhắm vào cả virus chương trình và virus macro.
/MAXFILESIZE <xxx.x>	Chỉ quét theo yêu cầu	Quét các file có kích cỡ không lớn hơn các mega-byte <xxx.x>
/MEMEXCL	Chỉ quét theo yêu cầu	Loại trừ địa chỉ bộ nhớ A000.0000 ra khỏi tiến trình quét.
/MOVE <dir> hay *.???	Không có sẵn cho Windows Chỉ quét theo yêu cầu /MOVE <directory>	Di chuyển tất cả file bị nhiễm mà SCAN.EXE tìm thấy trong suốt hoạt động quét sang thư mục đã chỉ định. Giữ lại chữ cái ổ đĩa và cấu trúc thư mục. Tùy chọn này không có tác dụng nếu Master Boot Record hay boot sector bị nhiễm, vì đây không phải là các file thực sự. /MOVE*.???
		SCAN.EXE sẽ thay đổi phần mở rộng của file bị nhiễm, nhưng không di chuyển chúng. Ví dụ, việc sử dụng tùy chọn /MOVE*.BAD sẽ yêu cầu trình quét đổi tên bất kỳ file bị nhiễm có phần mở rộng

		.BAD nhưng không di chuyển chúng sang một thư mục khác.
/NOBEEP	Chỉ quét theo yêu cầu	Tắt tone vốn phát ra bất cứ khi nào trình quét tìm thấy một virus.
/NOBREAK	Chỉ quét theo yêu cầu	Tắt CTRL-C và CTRL-BREAK trong suốt các hoạt động quét. Với tùy chọn này được kích hoạt, bạn không thể ngưng các hoạt động quét đang tiến triển.
/NOCOMP	Chỉ quét theo yêu cầu Yêu cầu bộ nhớ mở rộng	Yêu cầu SCAN.EXE không kiểm tra các file nén tự trích được tạo bằng các trình tiện ích LZEXE hoặc PKLite. Tùy chọn này giảm đi thời gian quét khi bạn không cần chạy toàn bộ một hoạt động. Nếu không, theo mặc định, trình quét kiểm tra bên trong các file thực thi hay file tự giải nén bằng cách giải nén mỗi file cho bộ nhớ và kiểm tra để tìm các virus signature.
/NODDA	Chỉ quét theo yêu cầu	Ngăn cản sự truy cập đĩa trực tiếp. SCAN.EXE sẽ không quét boot record. Đặc tính này đã được bổ sung để cho phép trình quét chạy bên dưới Windows NT Workstation 4.0 và

		Windows 2000 Professional. Bạn có thể cần sử dụng tùy chọn này trên một ổ đĩa được điều khiển bằng thiết bị.
/NODELETE	Chỉ quét theo yêu cầu	Ngăn cản SCAN.EXE khỏi xóa các chương trình ngựa thành Trojan mà nó tìm thấy. Nếu bạn sử dụng nó cùng với /DEL, SCAN.EXE vẫn xóa các file bị nhiễm virus.
/NODISK	Chỉ quét khi truy cập	Bỏ qua boot sector trong khi trình quét VShield tải.
/NODOC	Chỉ quét theo yêu cầu	Bỏ qua các file Microsoft Office.
/NOEMS	Chỉ quét khi truy cập	Ngăn cản trình quét VShield khỏi sử dụng bộ nhớ mở rộng (XMS).
/NOEXPIRE	Chỉ quét theo yêu cầu	Tắt thông báo "expiration date" xuất hiện nếu các file .DAT hết hạn sử dụng.
/NOJOKES	Không	Ngăn cản SCAN.EXE khỏi đưa ra một thông tin cảnh báo khi nó tìm thấy các file virus joke hay hoax.
/NOMEM	Không có	Bỏ qua RAM máy tính trong suốt các hoạt động quét. Tùy chọn này có thể gây nguy cơ lây nhiễm từ các virus thường trú trong bộ nhớ.

/NOREMOVE	Chỉ quét khi truy cập	Ngăn cản những người dùng khỏi loại bỏ trình quét VShield ra khỏi bộ nhớ bằng lệnh chuyển đổi /RE-MOVE.
/NORENAME	Chỉ quét theo yêu cầu	Ngăn cản SCAN.EXE khỏi đổi tên các file mà nó không thể làm sạch bằng một phần mở rộng khác.
/NOWARMBOOT	Chỉ quét khi truy cập	Bỏ qua boot sector đĩa của đĩa mềm trong ổ đĩa A: trong suốt quá trình khởi động nóng (khởi động lại hệ thống hoặc CTRL+ALT+DEL).
/NOXMS	Chỉ quét khi truy cập	Không sử dụng bộ nhớ mở rộng (XMS).
/ONLY <drive(s)>	Chỉ quét khi truy cập	Chỉ kiểm tra các file đã tải từ ổ đĩa đã xác định.
/PANALYZE	Chỉ quét theo yêu cầu	Cài đặt trình quét VirusScan để sử dụng các phương pháp suy nghiệm chương trình.
	Yêu cầu bộ nhớ mở rộng	/MANALYZE chỉ nhằm vào các virus macro; /ANALYZE nhằm vào cả virus chương trình và virus macro.
/PAUSE	Chỉ quét theo yêu cầu	Mở tính năng tạm ngưng màn hình. Dòng nhắc Press any key to continue sẽ xuất hiện khi trình quét lấp đầy một màn

hình bằng các thông báo. Nếu không, theo mặc định, trình quét lấp đầy và cuộn một màn hình một cách liên tục mà không ngừng lại, điều này cho phép nó chạy trên các máy tính có nhiều ổ đĩa hoặc bị nhiễm nghiêm trọng, mà không cần dữ liệu nhập của bạn.

McAfee đề nghị bạn nên bỏ qua /PAUSE khi bạn sử dụng các tùy chọn thông báo (/REPORT, /RPTCOR, và /RPTERR).

/PLAD	Chỉ quét theo yêu cầu	Giữ lại ngày tháng truy cập sau cùng trên các ổ đĩa Novell NetWare. Thông thường, các ổ đĩa mạng đọc quyền cập nhật ngày tháng sau cùng khi trình quét mở và kiểm tra một file. Tuy nhiên, một số hệ thống sao lưu dự phòng bằng sử dụng ngày tháng truy cập sau cùng này để quyết định xem có nên sao lưu dự phòng file hay không. Sử dụng /PLAD để bảo đảm rằng ngày tháng truy cập sau cùng không thay đổi kết quả của hoạt động quét.
/RECONNECT	Chỉ quét khi truy cập	Phục hồi trình quét VShield sau khi nó bị vô hiệu hóa

		bởi các trình điều khiển hay các chương trình thường trú trong bộ nhớ.
/REMOVE	Chỉ quét khi truy cập	Hủy tải trình quét VShield từ bộ nhớ
/REPORT <filename>	Chỉ quét theo yêu cầu	Tạo một báo cáo về các file bị nhiễm và các lỗi chương trình và lưu dữ liệu sang <filename> theo dạng text ASCII. Nếu <filename> đã hiện hữu, /REPORT sẽ ghi đè nó. Để tránh ghi đè, hãy sử dụng tùy chọn /APPEND với /REPORT: Trình quét sẽ thêm thông tin báo cáo vào cuối file, thay vì ghi đè nó. Bạn cũng có thể sử dụng /RPTALL, /RPTCOR, và /RPTERR để bổ sung các file được quét, các file bị hỏng, các file được chỉnh sửa và các lỗi chương trình vào thông báo. Bạn có thể đưa vào ổ đĩa và thư mục đích (chẳng hạn như D:\VSREPT\ ALL.TXT), nhưng nếu đích là một ổ đĩa mạng, bạn phải có quyền tạo và xóa các file trên ổ đĩa đó. McAfee đề nghị bạn nên bỏ qua /PAUSE nếu bạn sử

		dụng bất kỳ tùy chọn thông báo nào.
/RPTALL	Chỉ quét theo yêu cầu	Đưa vào các tên của tất cả file mà SCAN.EXE kiểm tra trong file /REPORT. Khi được sử dụng với /REPORT, tùy chọn này thêm tên của các file bị hỏng vào file thông báo. Bạn có thể sử dụng /RPTCOR với /RPTERR trên cùng một dòng lệnh. McAfee đề nghị bạn nên bỏ qua /PAUSE nếu bạn sử dụng bất kỳ tùy chọn thông báo nào.
/RPTCOR	Chỉ quét theo yêu cầu	Đưa vào tên của bất kỳ file bị hỏng mà SCAN.EXE tìm thấy trong file mà bạn xác định bằng /REPORT. Các file bị hỏng có thể cho biết sự hủy hoại của virus. Bạn có thể sử dụng /RPTCOR với /RPTERR trên cùng một dòng lệnh. Có thể có các chỉ số đọc file trong một số file vốn đòi hỏi một file xếp chồng hay một file thực thi khác để chạy một cách thích hợp - nghĩa là các file không thực thi riêng biệt. McAfee đề nghị bạn nên

		bỏ qua /PAUSE nếu bạn sử dụng bất kỳ tùy chọn thông báo.
/RPTERR	Chỉ quét theo yêu cầu	Đưa vào bất kỳ thông báo lỗi mà SCAN.EXE tạo ra trong suốt một hoạt động quét trong file mà bạn xác định bằng /REPORT. Các lỗi như vậy có thể bao hàm các sự cố về việc đọc hay ghi sang một đĩa, các sự cố về hệ thống file hay mạng, các sự cố về việc tạo các báo cáo và các sự cố liên quan đến hệ thống. McAfee đề nghị bạn nên bỏ qua /PAUSE nếu bạn sử dụng bất kỳ tùy chọn thông báo nào.
/SAVE	Chỉ quét khi truy cập	Lưu các tùy chọn dòng lệnh mà bạn đã chọn cho tác vụ quét khi truy cập sang file VSHIELD.INI.
/SILENT	Chỉ quét theo yêu cầu	Vô hiệu hóa tất cả dữ liệu xuất sang màn hình trong suốt các hoạt động quét. McAfee đề nghị bạn nên sử dụng tùy chọn này với /REPORT để ghi lại những gì mà hoạt động quét đã thực hiện.

/SUB	Chỉ quét theo yêu cầu	Quét các thư mục con nằm bên trong một thư mục. ❖ Theo mặc định, khi bạn xác định một thư mục để quét thay vì một ổ đĩa, trình quét sẽ kiểm tra chỉ các file mà nó chứa, chứ không phải các thư mục con của nó. ❖ Sử dụng /SUB để quét tất cả thư mục con nằm trong bất kỳ thư mục mà bạn đã xác định. Tùy chọn này bỏ qua các file được lưu trữ tại cấp độ gốc của thư mục đích. ❖ Bạn không cần phải sử dụng SUB nếu bạn quét cả một ổ đĩa.
/TIMEOUT <seconds>	Không có	Cài đặt một thời gian tối đa cho trình quét sử dụng để kiểm tra bất kỳ một file nào.
/UNZIP	Chỉ quét theo yêu cầu Yêu cầu bộ nhớ mở rộng	Quét bên trong các file archive được nén.
/VIRLIST	Chỉ quét theo yêu cầu	Hiển thị tên của các họ virus mà trình quét phát hiện. Danh sách này không bao hàm các biến virus. Bạn có thể sử dụng tùy chọn /PAUSE trên cùng một dòng lệnh với /

VIRLIST để đọc danh sách virus mỗi lần một màn hình. Để định hướng lại dữ liệu xuất /VIRLIST sang một file text:

Tại dòng nhắc lệnh, hãy nhập

scan /VIRLIST

Bởi vì trình quét có thể phát hiện nhiều virus, file này sẽ dài hơn 250 trang. File này quá lớn đối với chương trình MS-DOS Edit để mở; McAfee đề nghị bạn nên sử dụng một bộ biên soạn text khác để mở danh sách virus.

/XMSDATA	Chỉ quét khi truy cập	Tải các file dữ liệu VShield vào bộ nhớ XMS.
----------	-----------------------	--

II. Các cấp độ lỗi cho trình quét VirusScan Command Line

Khi bạn chạy trình quét VirusScan Command Line, nó cho ra một mã cấp độ lỗi khi nó hoàn tất hoạt động quét. Bạn có thể sử dụng mã đó trong các file lô hoặc trong các trình ứng dụng khác để thực hiện các hoạt động khác nhau dựa vào các kết quả của hoạt động quét của bạn.

Trình quét VirusScan Command Line có thể cho ra những mã cấp độ lỗi sau đây

Cấp độ lỗi	Mô tả
0	Các lỗi không xuất hiện, trình quét không tìm thấy các virus
1	Lỗi truy cập file. Điều này có thể có nghĩa rằng

	máy tính đang sử dụng một file hệ thống hay file khác mà nó không cho phép truy cập đến
2	Không thể kiểm tra tính toàn vẹn của file dữ liệu
3	Lỗi truy cập đĩa
4	Lỗi trong khi đọc kết quả xuất từ AF
5	Không đủ bộ nhớ
6	Một sự cố thông thường
7	Lỗi đọc thông báo MCAFEE.MSG bên trong
8	Không thể tìm thấy một file dữ liệu
9	Các tùy chọn không tương thích trong dòng lệnh
10	Trình quét tìm thấy một virus trong bộ nhớ
11	Lỗi chương trình bên trong
12	File CLEAN.DAT bị thất thoát hoặc bị hỏng
13	Trình quét tìm thấy một hoặc nhiều virus hay các đối tượng gây hại
14	File .DAT hết hạn sử dụng
15	Trình quét không thể tự kiểm tra; nó có thể bị gây nhiễm hoặc bị hư hỏng
16	Sự cố về truy cập ổ đĩa hay file
17	Đích quét không được xác định
18	File hợp lệ được chỉnh sửa
19	Một hoặc nhiều virus được tìm thấy, tất cả bị xóa
20	Tùy chọn lệnh /FREQUENCY ngăn cản trình quét khỏi tiếp tục thực hiện
100	Một sự cố DOS xảy ra
102	Người dùng thoát thông qua các tổ hợp phím ESC-X, ^C, hay Exit. Bạn có thể vô hiệu hóa tính năng này bằng cách chạy trình bằng bằng tùy chọn dòng lệnh /NOBREAK.

Bài 16

TÌM HIỂU CÁC DẠNG FILE .ALR VÀ .VSC

I. Tìm hiểu dạng file .ALR

File .ALR là thông báo Centralized Alerting có chứa các biến event. Mỗi biến trong file có một tên được theo sau bằng dấu bằng (=) và một giá trị. Bảng sau đây mô tả mỗi biến trong dạng file Centralized Alerting:

[CentralAlert]

Biến	Mô tả
uFileVersion	Loại: Integer Biến này chứa số phiên bản Centralized Alerting
uStatus	Dự trữ
szVirusName	Loại: String Biến này chứa tên của virus lây nhiễm.
szItemName	Loại: String Biến này liệt kê tên và đường dẫn đi đến file bị nhiễm.
szUserName	Loại: String Biến này liệt kê tên của người dùng được nhập vào máy tính vào thời điểm mà phần mềm VirusScan đã phát hiện virus.
szSoftware	Loại: String

	Biến này liệt kê tên của phần mềm chống virus McAfee được cài đặt trên máy tính báo cáo.
szSoftwareVersion	Loại: String Biến này liệt kê số phiên bản cho phiên bản chống virus McAfee được cài đặt trên máy tính.
szComputerName	Loại: String Biến này liệt kê tên máy tính cho máy báo cáo.
uYear	Loại: Integer Các giá trị có thể chấp nhận: 0000 đến 9999. Biến này ghi lại năm mà event (sự kiện) xảy ra.
uMonth	Loại: Integer Các giá trị có thể chấp nhận: 1 đến 12. Biến này sử dụng Greenwich Mean Time để ghi lại tháng mà event đã xảy ra.
uDay	Loại: Integer Các giá trị có thể chấp nhận: 1 đến 31 Biến này sử dụng Greenwich Mean Time để ghi lại ngày mà event đã xảy ra.
uHour	Loại: Integer Các giá trị có thể chấp nhận: 0 đến 23. Biến này sử dụng Greenwich Mean Time để ghi lại giờ mà event đã xảy ra.
uMinute	Loại: Integer Các giá trị có thể chấp nhận: 0 đến 59 Biến này sử dụng Greenwich Mean Time để ghi lại phút mà event đã xảy ra.
uSecond	Loại: Integer Các giá trị có thể chấp nhận: 0 đến 59 Biến này sử dụng Greenwich Mean Time để ghi lại giây mà event đã xảy ra.

szGMTTime	Loại: String Biến này sử dụng Greenwich Mean Time để ghi lại cả thời gian và ngày tháng mà event đã xảy ra.
szAlertPath	Loại: String Biến này liệt kê đường dẫn đi đến thư mục Centralized Alerting mà bạn đã xác định dưới dạng một đích cho file này.
uSeverity	Loại: Integer Các giá trị có thể chấp nhận: 0 đến 4 Giá trị = 0 - Thông báo tin tức 1 - Thông báo có mức độ ưu tiên thấp 2 - Thông báo có mức độ ưu tiên trung bình 3 - Thông báo có mức độ ưu tiên cao 4 - Thông báo có mức độ ưu tiên tối hạn Biến này gán một mức độ ưu tiên hoặc mức độ nghiêm trọng vào thông tin cảnh báo, dựa vào mức độ nghiêm trọng mà bạn gán vào mỗi loại thông báo trong hộp thoại cấu hình Alert Manager. Để tìm hiểu thêm về những tùy chọn này, hãy xem NetShield Administrator's Guide.
szSourceIP	Loại: String Biến này ghi địa chỉ IP cho máy tính vốn tạo ra thông tin cảnh báo.
uMessageID	Loại: Integer Biến này ghi số nhận dạng duy nhất mà trình ứng dụng tạo gán vào thông tin cảnh báo.
szTaskName	Loại: String Biến này ghi tên của thành phần VirusScan vốn tạo ra thông tin cảnh báo, nếu thành phần đó cung cấp tên của nó.

szOS	Loại: String Biến này ghi tên của hệ điều hành chạy trên máy tính vốn tạo thông tin cảnh báo.
szEngineVersion	Loại: String Biến này ghi số phiên bản máy quét khi thông tin cảnh báo lưu ý đến việc phát hiện virus.
szDatVersion	Loại: String Biến này ghi số phiên bản file (.DAT) xác định virus khi thông tin cảnh báo lưu ý đến việc phát hiện virus.
dwWinStaClientID	Loại: String Biến này ghi số nhận dạng cho server client đầu cuối vốn tạo ra thông tin cảnh báo, nếu máy tính chạy phần mềm VirusScan từ một server đầu cuối Windows.
pszWinStaClientName	Loại: String Biến này ghi tên của server đầu cuối vốn nhận và truyền thông tin cảnh báo, nếu bạn chạy phần mềm VirusScan từ một server đầu cuối Windows.
uSpecificTrap	Loại: Integer Biến này ghi một số nhận dạng bất duy nhất cho mỗi thông tin cảnh báo.
szActualMessage	Loại: String

Biến này ghi toàn bộ text của thông tin cảnh báo mà thành phần VirusScan tạo ra. Theo mặc định, toàn bộ text bao hàm: tên của file bị nhiễm; tên của virus gây nhiễm; các số phiên bản của máy quét hoạt động và các file .DAT; tên và địa chỉ IP của máy tính vốn tạo ra thông báo; tên của người dùng được nhập vào máy tính đó; và số phiên bản của thành phần VirusScan vốn tạo ra thông tin cảnh báo.

II. Tìm hiểu dạng file .VSC

Khi bạn lưu các cài đặt từ cửa sổ trình ứng dụng VirusScan, trình

ứng dụng tạo ra một file cấu hình có phần mở rộng .VSC và tên mà bạn đã chọn cho nó. Thông thường, bạn sẽ tìm thấy file này trong thư mục chương trình VirusScan, nhưng bạn có thể lưu nó tại bất kỳ vị trí nào mà bạn muốn. File .VSC là một file text cấu hình vốn ghi các cài đặt mà bạn đã chọn cho hoạt động quét của bạn và cho phép bạn chạy một hoạt động sau này với các cài đặt tương tự chính xác đó.

File được định dạng theo một cách tương tự như các file .INI của Windows. Bạn có thể hiệu chỉnh trực tiếp file này để thay đổi các tùy chọn đã ghi ở đó - chỉ việc mở file với một bộ hiệu chỉnh text chẳng hạn như Windows Notepad. Nếu bạn bảo vệ các cài đặt VirusScan bằng password, chương trình sẽ mã hóa file .VSC để ngăn cản việc chỉnh sửa không mong muốn - bạn phải loại bỏ chế độ bảo vệ bằng password để hiệu chỉnh file.

Bạn có thể phân phối các bản sao của file .VSC đã chỉnh sửa đến những người dùng phần mềm VirusScan khác tại các máy tính khác, và do đó phân phối những cài đặt này để những người dùng khác có thể chạy. Những người dùng khác đó sẽ cần định vị và nhấp đôi file .VSC mà bạn đã gửi để khởi động VirusScan bằng các tùy chọn mà bạn đã mã hóa sang chúng.

Mỗi biến trong file có một tên được theo sau bằng một dấu bằng (=) và một giá trị. Các giá trị tương ứng với các cài đặt mà bạn đã chọn khi bạn cấu hình VirusScan. Các biến được sắp xếp thành tám nhóm xuất hiện bên dưới các tiêu đề riêng của chúng trong file .VSC. Các bảng sau đây liệt kê mỗi biến, cùng với các giá trị mặc định và các giá trị có thể có của nó.

Mỗi biến có một tên, được đứng trước bằng một mã kiểu biến được chọn từ một trong những biến sau:

- | | |
|-----------|--|
| b | Một biến Boolean. Các giá trị có thể có cho các biến Boolean là 0 và 1. Giá trị 0 yêu cầu trình ứng dụng VirusScan vô hiệu hóa cài đặt, trong khi một yêu cầu trình ứng dụng vận hành cài đặt. |
| sz | Một biến chuỗi (string). Các giá trị có thể có cho các biến chuỗi là một loạt các ký |

- u hay n tự chữ - số hay các ký tự ASCII khác.
 Một biến số nguyên (integer). Các giá trị có thể có cho các số nguyên file .VSC nằm trong một dãy các số vốn được ấn định sẵn trong phần mềm VirusScan. Những biến này cho phép tính tương thích ngược với các phiên bản trước đây của file .VSC.
- dw Một biến số nguyên "double word". Những biến này cho phép sử dụng một dãy giá trị lớn hơn nhiều so với các biến số nguyên u hay n.

[ScanOptions]

Biến	Mô tả
UIType	Loại: Boolean Xác định giao diện nào mà trình ứng dụng hiển thị - một trình ứng dụng chạy trên Windows NT Workstation 4.0 và Windows 2000 Professional, hoặc một trình ứng dụng chạy trên Windows 95 và Window 98. Việc chỉnh sửa giá trị mặc định sẽ làm cho trình ứng dụng hiển thị một giao diện khác. Giá trị = 0 - Hiển thị cửa sổ trình ứng dụng VirusScan (mặc định) Giá trị = 1 - hiển thị giao diện chỉ quét trình ứng dụng VirusScan
nPriority	Loại: Integer Xác định một mức độ ưu tiên cho chuỗi quét hiện hành. Giá trị = 0 - Mức độ ưu tiên chuỗi thông thường (mặc định) 1 - Mức độ ưu tiên chuỗi thấp nhất 2 - Mức độ ưu tiên chuỗi thông thường bên dưới

	3 - Mức độ ưu tiên chuỗi thông thường
	4 - Mức độ ưu tiên chuỗi thông thường cao hơn
	5 - Mức độ ưu tiên chuỗi cao nhất
nChecksum	Dự trữ: Không được chỉnh sửa
bAutoStart	Loại: Boolean Yêu cầu trình ứng dụng VirusScan bắt đầu hoạt động quét của nó ngay khi nó khởi chạy. Giá trị = 1 - Mở AutoStart Giá trị = 0 - Tắt AutoStart (mặc định)
bAutoExit	Loại: Boolean Yêu cầu trình ứng dụng VirusScan thoát khi nó thực hiện xong hoạt động quét nếu nó không tìm thấy bất kỳ virus nào. Giá trị = 1 - Thoát sau hoạt động quét trừ phi trình ứng dụng tìm thấy một virus Giá trị = 0 - Không tự động thoát (mặc định). Các biến khác có thể thay đổi cách hoạt động của trình ứng dụng.
bAlwaysExit	Loại: Boolean Yêu cầu trình ứng dụng VirusScan thoát khi nó thực hiện xong hoạt động quét cho dù có tìm thấy một virus hay không. Giá trị = 1 - Trình ứng dụng luôn thoát Giá trị = 0 - Trình ứng dụng không tự động thoát (mặc định). Các biến khác có thể thay đổi cách hoạt động của trình ứng dụng.
bSkipMemoryScan	Loại: Boolean Yêu cầu trình ứng dụng VirusScan không quét bộ nhớ của máy tính. Giá trị = 1 - Trình ứng dụng sẽ không quét bộ nhớ Giá trị = 0 - Trình ứng dụng quét bộ nhớ

	(mặc định)
bSkipBootScan	Loại: Boolean Yêu cầu trình ứng dụng VirusScan không quét boot sector trên đĩa cứng hoặc trên các đĩa khác. Giá trị = 1 - Trình ứng dụng sẽ không quét các boot sector Giá trị = 0 - Trình ứng dụng quét các boot sector (mặc định)
bSkipSplash	Loại: Boolean Yêu cầu trình ứng dụng VirusScan không hiển thị màn hình “splash” nhận biết ban đầu của nó khi nó khởi động. Giá trị = 1 - Trình ứng dụng sẽ không hiển thị màn hình splash Giá trị = 0 - Trình ứng dụng hiển thị màn hình splash.
bConfigurationGuiMode	Loại: Boolean Yêu cầu trình ứng dụng VirusScan sử dụng giao diện người dùng VirusScan Advanced. Giá trị = 0 - Trình ứng dụng xuất hiện với giao diện người dùng Advanced Giá trị = 1 - Trình ứng dụng xuất hiện với giao diện VirusScan Classic (mặc định)
bTemporary	Dự trữ. Không được chỉnh sửa
szTaskName	Dự trữ. Không được chỉnh sửa
szScanItem	Chưa đưa sử dụng. Không được chỉnh sửa

[DetectionOptions]

Biến	Mô tả
bRemoveAllMacros	Loại: Boolean Yêu cầu trình ứng dụng VirusScan xóa tất cả các macro ra khỏi các file bị nhiễm.

	Giá trị = 1 - Trình ứng dụng loại bỏ tất cả mã macro Giá trị = 0 - Trình ứng dụng để lại nguyên vẹn mã macro (mặc định)
bScanAllFiles	Loại: Boolean Yêu cầu trình ứng dụng VirusScan quét tất cả file, cho dù phần mở rộng tên file của chúng là gì đi nữa. Giá trị = 1 - Trình ứng dụng quét tất cả file Giá trị = 0 - Trình ứng dụng quét các file đã chọn (mặc định)
bScanCompressed	Loại: Boolean Yêu cầu trình ứng dụng VirusScan quét các file bị nén. Giá trị = 1 - Trình ứng dụng quét các file bị nén (mặc định) Giá trị = 0 - Trình ứng dụng không quét các file bị nén.
bDetectTrojans	Loại: Boolean Yêu cầu trình ứng dụng VirusScan quét để tìm các chương trình ngựa thành Troia. Giá trị = 1 - Trình ứng dụng quét để tìm các chương trình ngựa thành Troia (mặc định) Giá trị = 0 - Trình ứng dụng không quét để tìm các chương trình ngựa thành Troia.
bDetectJoke	Loại: Boolean Yêu cầu trình ứng dụng VirusScan quét để tìm các file "joke" hay các file virus hoax. Giá trị = 1 - Trình ứng dụng quét để tìm các file joke (mặc định) Giá trị = 0 - Trình ứng dụng không quét để tìm các file joke.

- bDetectCorrupted** Loại: Boolean
Yêu cầu trình ứng dụng VirusScan quét để tìm các file bị hỏng. Các loại file bị hỏng cụ thể có thể chỉ định sự xuất hiện của một virus.
Giá trị = 1 - Trình ứng dụng quét để tìm các file bị hỏng
Giá trị = 0 - Trình ứng dụng không quét để tìm các file bị hỏng (mặc định)
- bDetectMaybe** Loại: Boolean
Yêu cầu trình ứng dụng VirusScan quét để tìm các biến thể của virus mà nó đã biết.
Giá trị = 1 - Trình ứng dụng quét để tìm các biến thể virus (mặc định)
Giá trị = 0 - Trình ứng dụng không quét để tìm các biến thể virus
- bProgFileHeuristics** Loại: Boolean
Yêu cầu trình ứng dụng VirusScan sử dụng phương pháp quét dò tìm để kiểm tra các file chương trình nhằm tìm ra các virus. Phương pháp quét dò tìm nhận biết các đặc tính giống như virus nhất định trong các file như một cách để nhận biết các phần gây nhiễm có thể xảy ra.
Giá trị = 1 - Trình ứng dụng sử dụng phương pháp quét dò tìm
Giá trị = 0 - Trình ứng dụng quét mà không sử dụng các phương pháp dò tìm (mặc định)
- bMacroHeuristics** Loại: Boolean
Yêu cầu trình ứng dụng VirusScan sử dụng các kỹ thuật dò tìm để tìm các virus trong các file tài liệu có chứa các macro. Kỹ thuật quét dò tìm nhận biết các đặc điểm

giống như virus nhất định trong các file như là một cách để nhận biết các phần lây nhiễm có thể xảy ra.

Giá trị = 1 - Trình ứng dụng sử dụng một kỹ thuật quét dò tìm cho các file tài liệu

Giá trị = 0 - Trình ứng dụng quét các file tài liệu mà không sử dụng các kỹ thuật dò tìm (mặc định)

bFindAllMacros

Loại: Boolean

Yêu cầu trình ứng dụng VirusScan tìm kiếm tất cả file tài liệu có chứa các macro.

Giá trị = 1 - Trình ứng dụng tìm kiếm tất cả file tài liệu có chứa các macro

Giá trị = 0 - Trình ứng dụng không tìm kiếm tất cả file tài liệu có chứa các macro (mặc định)

bScanAllOLE

Loại: Boolean

Yêu cầu trình ứng dụng VirusScan tìm kiếm các virus trong tất cả file được nhúng trong các file khác bằng cách sử dụng công nghệ Object Linking and Embedding (liên kết và nhúng đối tượng)

Giá trị = 1 - Trình ứng dụng quét tất cả file được nhúng trong các file khác thông qua OLE

Giá trị = 0 - Trình ứng dụng không quét các file được nhúng (mặc định)

bIncludesSubFolders

Loại: Boolean

Yêu cầu trình ứng dụng VirusScan quét các file được chứa trong các folder con nằm bên trong đích quét mà bạn xác định. Chú ý rằng tùy chọn này yêu cầu trình ứng dụng bỏ qua các file tại cấp gốc của thư mục đích ngoại trừ các file được lưu trữ trong các thư mục con.

Giá trị = 1 - Trình ứng dụng quét các file trong thư mục con, nhưng không phải các file tại cấp gốc của thư mục đích

Giá trị = 0 - Trình ứng dụng quét các file tại cấp gốc của thư mục đích, nhưng bỏ qua các file trong các thư mục con (mặc định)

bBootRepair

Loại: Boolean

Yêu cầu trình ứng dụng VirusScan cố sửa chữa boot sector trên đĩa cứng hay trên một đĩa mềm khi nó phát hiện rằng một virus đã gây hại hoặc làm hỏng nó.

Giá trị = 1 - Trình ứng dụng cố sửa chữa boot sector

Giá trị = 0 - Trình ứng dụng không cố sửa chữa boot sector (mặc định)

dwHeuristicSensitivity

Loại: Integer

Cài đặt một thời điểm mà qua đó số đặc điểm giống như virus trong một file sẽ làm cho trình ứng dụng VirusScan khai báo file bị nhiễm.

Giá trị =

0 - Kỹ thuật quét dò tìm không hoạt động (mặc định)

1 - Độ nhạy thấp. Các file phải trình bày nhiều đặc điểm giống như virus

2 - Độ nhạy thấp. Các file phải trình bày nhiều đặc điểm giống như virus

3 - Độ nhạy trung bình. Các file phải trình bày một số đặc điểm giống như virus

4 - Độ nhạy cao. Các file phải trình bày một số bằng chứng về các đặc điểm giống như virus

5 - Độ nhạy cao nhất. Các file phải trình bày bất kỳ bằng chứng về các đặc điểm

giống như virus. Với cấp độ này, trình ứng dụng sẽ đánh dấu cờ cho nhiều file vốn chỉ có mã macro trong chúng.

szProgramExtensions Loại: String

Xác định các phần mở rộng tên file nào mà trình ứng dụng sẽ kiểm tra để tìm các phần lây nhiễm tiềm ẩn. Biến này trình bày danh sách tên file mà bạn tạo, kể cả bất kỳ các phần mở rộng tên file mà bạn đã thêm vào danh sách mặc định và không có bất kỳ các phần mở rộng tên file mà bạn đã loại bỏ ra khỏi danh sách mặc định.

**szDefaultProgram
Extensions**

Loại: String

Xác định các phần mở rộng tên file nào mà trình ứng dụng sẽ kiểm tra để tìm ra các phần gây nhiễm tiềm ẩn theo mặc định. Danh sách này không thay đổi kết quả của bất kỳ phần bổ sung hay trích dẫn mà bạn thực hiện trong hộp thoại Program File Extensions. Việc nhấp nút Default trong hộp thoại đó sẽ phục hồi danh sách các giá trị đã lưu trữ ở đây.

**szEngineCommand
LineOptions**

Dự trữ. Không được chỉnh sửa

[AlertOptions]

Biến

Mô tả

bNetworkAlert

Loại: Boolean

Yêu cầu trình ứng dụng VirusScan gửi các thông tin cảnh báo dưới dạng các file text (.ALR) đến một thư mục Centralized Alerting. Bạn phải sử dụng trình tiện ích Alert Manager Client Configuration để xác định thư mục đích.

Giá trị = 1 - Trình ứng dụng gửi các thông tin cảnh báo dưới dạng các file .ALR

Giá trị = 0 - Trình ứng dụng không gửi các thông báo .ALR (mặc định)

bSoundAlert

Loại: Boolean

Yêu cầu trình ứng dụng VirusScan phát ra tiếng beep khi nó tìm thấy một virus. Trình ứng dụng sử dụng âm thanh beep hệ thống hoặc file file .WAV mà bạn đã gắn vào máy tính dưới dạng âm thanh beep báo động của nó.

Giá trị = 1 - Trình ứng dụng phát ra tiếng beep khi nó phát hiện một virus

Giá trị = 0 - Trình ứng dụng vẫn im lặng khi nó phát hiện một virus (mặc định)

bAlert

Loại: Boolean

Yêu cầu trình ứng dụng VirusScan gửi một thông tin cảnh báo đến server Alert Manager mà bạn đã chỉ định bất cứ khi nào phát hiện một virus. Bạn phải sử dụng tiện ích Alert Manager Client Configuration để xác định server Alert Manager mà bạn muốn sử dụng.

Giá trị = 1 - Trình ứng dụng gửi một thông tin cảnh báo khi nó phát hiện một virus

Giá trị = 0 - Trình ứng dụng không gửi một thông tin cảnh báo khi nó phát hiện một virus (mặc định)

dwAlertPriority

Loại: Integer

Hiện chưa được sử dụng. Không được chỉnh sửa.

szSuggestMessage

Loại: String

Xác định một thông tin cảnh báo mặc định cho trình ứng dụng VirusScan hiển thị khi nó phát hiện một virus. Thông tin cảnh báo

xuất hiện nếu bạn chọn tùy chọn trả lời Prompt user for action và hộp kiểm Display Custom Message trong các trang đặc tính VirusScan Advanced.

Value = Insert Custom Message Here (mặc định)

Các giá trị cần thiết trong các biến khác
bDisplayMessage = 1

ScanAction = 0

szCustomMessage

Loại: String

Xác định một thông báo tùy ý cho trình ứng dụng VirusScan để hiển thị khi nó phát hiện một virus. Thông tin cảnh báo xuất hiện khi bạn nhập nó vào hộp text thông báo tùy ý nếu bạn chọn tùy chọn trả lời Prompt user for action và hộp kiểm Display Custom Message trong các trang đặc tính VirusScan Advanced.

Value = [user defined - no defined]

Các giá trị trong các biến khác:

bDisplayMessage = 1

ScanAction = 0

szNetworkAlertPath

Loại: String

Xác định đường dẫn đi đến thư mục Centralized Alerting mà bạn chọn trong trình tiện ích cấu hình Alert Manager Client. Để server Alert Manager phân phối bất kỳ các thông báo .ALR mà trình ứng dụng VirusScan gửi đi. Thư mục đích phải chứa file CENTALRT.TXT.

Value = [user defined - no default]

[ActionOptions]

Biến	Mô tả
bDisplayMessage	Loại: Boolean Yêu cầu trình ứng dụng VirusScan hiển thị một thông tin cảnh báo tùy ý khi nó phát hiện một virus. Để cài đặt này hoạt động, bạn phải chọn Prompt user for action trong trang đặc tính VirusScan Advanced Action. Giá trị = 0 - Trình ứng dụng không hiển thị thông báo tùy ý (mặc định) Giá trị = 1 - Trình ứng dụng hiển thị một thông báo tùy ý Các giá trị cần thiết trong các biến khác: ScanAction = 0 szCustomMessage = [user defined]
bButtonClean	Loại: Boolean Yêu cầu trình ứng dụng VirusScan đưa một nút Clean vào thông tin cảnh báo mà nó hiển thị khi nó tìm thấy một virus. Thông tin cảnh báo này xuất hiện nếu bạn chọn tùy chọn trả lời Prompt user for action trong trang đặc tính VirusScan Action. Giá trị = 1 - Thông tin cảnh báo hiển thị nút Clean (mặc định) Giá trị = 0 - Thông tin cảnh báo không hiển thị nút Clean Các giá trị cần thiết trong các biến khác: ScanAction = 0
bButtonDelete	Loại: Boolean Yêu cầu trình ứng dụng VirusScan đưa một nút Delete vào thông tin cảnh báo mà nó xuất hiện khi tìm thấy một virus. Thông tin cảnh báo này xuất hiện nếu bạn chọn

tùy chọn trả lời Prompt user for action trong trang đặc tính VirusScan Action.

Giá trị = 1 - Thông tin cảnh báo hiển thị nút Delete (mặc định)

Giá trị = 0 - Thông tin cảnh báo không hiển thị nút Delete

Các giá trị cần thiết trong các biến khác:
ScanAction = 0

bButtonExclude

Loại: Boolean

Yêu cầu trình ứng dụng VirusScan thêm một nút Exclude vào thông tin cảnh báo mà nó hiển thị khi nó tìm thấy một virus. Thông tin cảnh báo này xuất hiện nếu bạn chọn tùy chọn trả lời Prompt user for action trong trang đặc tính VirusScan Action.

Giá trị = 1 - Thông tin cảnh báo hiển thị nút Exclude

Giá trị = 0 - Thông tin cảnh báo không hiển thị nút Exclude (mặc định)

Các giá trị cần thiết trong các biến khác:
ScanAction = 0

bButtonMove

Loại: Boolean

Yêu cầu trình ứng dụng VirusScan thêm một nút Move file to vào thông tin cảnh báo mà nó hiển thị khi nó tìm thấy một virus. Thông tin cảnh báo này xuất hiện nếu bạn chọn tùy chọn trả lời Prompt user for action trong trang đặc tính VirusScan Action.

Giá trị = 1 - Thông tin cảnh báo hiển thị nút Move file to (mặc định)

Giá trị = 0 - Thông tin cảnh báo không hiển thị nút Move file to

Các giá trị được yêu cầu trong các biến khác:

bButtonContinue

ScanAction = 0

Loại: Boolean

Yêu cầu trình ứng dụng VirusScan thêm một nút Continue vào thông tin cảnh báo mà nó xuất hiện khi nó tìm thấy một virus. Thông tin cảnh báo này xuất hiện nếu bạn chọn tùy chọn trả lời Prompt user for action trong trang đặc tính VirusScan Action

Giá trị = 1 - Thông tin cảnh báo hiển thị nút Continue (mặc định)

Giá trị = 0 - Thông tin cảnh báo không hiển thị nút Continue

Các giá trị cần thiết trong các biến khác:

ScanAction = 0

bButtonStop

Loại: Boolean

Yêu cầu trình ứng dụng VirusScan thêm một nút Stop vào thông tin cảnh báo mà nó hiển thị khi nó tìm thấy một virus. Thông tin cảnh báo này hiển thị nếu bạn chọn tùy chọn trả lời Prompt user for action trong trang đặc tính VirusScan Action.

Giá trị = 1 - Thông tin cảnh báo hiển thị nút Stop (mặc định)

Giá trị = 0 - Thông tin cảnh báo không hiển thị nút Stop

Các giá trị cần thiết trong các biến khác:

ScanAction = 0

ScanAction

Loại: Integer

Yêu cầu trình ứng dụng VirusScan phản ứng lại bất kỳ virus mà nó tìm thấy bằng một trong những thao tác mà bạn xác định.

Giá trị =

1 - Tiếp tục quét

	2 - Nhắc về thao tác của người dùng 3 - Tự động di chuyển các file bị nhiễm 4 - Tự động xóa các file bị nhiễm 5 - Tự động xóa sạch các file bị nhiễm
dwScanActionButtons	Loại: Integer Chỉ sử dụng bên trong. Không được chỉnh sửa.
szMoveToFolder	Loại: String Xác định đường dẫn thư mục mà trình ứng dụng VirusScan sẽ di chuyển bất kỳ file bị nhiễm mà nó tìm thấy vào đó. Value = \Infected (mặc định)
szcustomMessage	Loại: String Xác định một thông báo tùy ý cho trình ứng dụng VirusScan để hiển thị khi nó phát hiện một virus. Thông tin cảnh báo xuất hiện khi bạn nhập nó vào hộp text thông báo tùy ý nếu bạn chọn tùy chọn trả lời Prompt user for action và hộp kiểm Display Custom Message trong các trang đặc tính VirusScan Advanced. Value = [user defined - no default] Các giá trị cần thiết trong các biến khác: bdisplayMessage = 1 ScanAction = 0

[ReportOptions]

Biến	Mô tả
bLogToFile	Loại: Boolean Yêu cầu trình ứng dụng VirusScan ghi lại các hoạt động của nó trong một log file. Giá trị = 1 - Trình ứng dụng ghi lại các hoạt động của nó trong log file (mặc định) Giá trị = 0 - Trình ứng dụng không ghi lại các hoạt động của nó trong một log file

bLimitSize

Loại: Boolean

Yêu cầu trình ứng dụng VirusScan giới hạn kích cỡ của file log của nó đối với kích cỡ tối đa mà bạn cài đặt.

Giá trị = 1 - Trình ứng dụng giới hạn kích cỡ log file (mặc định)

Giá trị = 0 - Trình ứng dụng không giới hạn kích cỡ log file

bLogDetection

Loại: Boolean

Yêu cầu trình ứng dụng VirusScan theo dõi bao nhiêu virus mà nó phát hiện. Trình ứng dụng ghi thông tin này sang một log file riêng biệt.

Giá trị = 1 - Trình ứng dụng ghi lại số virus mà nó phát hiện (mặc định)

Giá trị = 0 - Trình ứng dụng không ghi lại số virus mà nó phát hiện.

Các giá trị cần thiết trong các biến khác:

bLogToFile = 1

szLogFileName = [user defined or default]

bLogclean

Loại: Boolean

Yêu cầu trình ứng dụng VirusScan theo dõi bao nhiêu file bị nhiễm mà nó xóa sạch hoặc cố xóa sạch. Trình ứng dụng ghi thông tin này sang một log file riêng biệt.

Giá trị = 1 - Trình ứng dụng ghi lại số file bị nhiễm mà nó xóa sạch hoặc cố gắng xóa sạch (mặc định)

Giá trị = 0 - Trình ứng dụng không ghi lại số file bị nhiễm mà nó xóa sạch hoặc cố gắng xóa sạch

Các giá trị cần thiết trong các biến khác:

bLogToFile = 1

szLogFileName = [user defined or default]

bLogDelete

Loại: Boolean

Yêu cầu trình ứng dụng VirusScan ghi lại bao nhiêu file bị nhiễm mà nó xóa. Trình ứng dụng ghi thông tin này sang một log file riêng biệt.

Giá trị = 1 - Trình ứng dụng ghi lại số file bị nhiễm mà nó xóa (mặc định)

Giá trị = 0 - Trình ứng dụng không ghi lại số file bị nhiễm mà nó xóa

Các giá trị cần thiết trong các biến khác:

bLogToFile = 1

szLogFileName = [user defined or default]

bLogMove

Loại: Boolean

Yêu cầu trình ứng dụng VirusScan ghi lại bao nhiêu file bị nhiễm mà nó di chuyển sang một folder được cách ly. Trình ứng dụng ghi thông tin này sang một log file riêng biệt.

Giá trị = 1 - Trình ứng dụng ghi lại số file bị nhiễm mà nó di chuyển sang một folder được cách ly (mặc định)

Giá trị = 0 - Trình ứng dụng không ghi lại số file bị nhiễm mà nó di chuyển sang một folder được cách ly

Các giá trị cần thiết trong các biến khác:

bLogToFile = 1

szLogFileName = [user defined or default]

szMoveToFolder = [value is user defined;

Uninfected is default. Required only if ScanAction = 1]

bLogDateTime

Loại: Boolean

Yêu cầu trình ứng dụng VirusScan ghi lại ngày tháng và thời gian mà nó bắt đầu hoạt động quét hiện hành. Trình ứng dụng ghi thông tin này sang một log file riêng biệt.

Giá trị = 1 - Trình ứng dụng ghi lại ngày tháng và thời gian hoạt động quét (mặc định)

Giá trị = 0 - Trình ứng dụng không ghi lại ngày tháng và thời gian hoạt động quét

Các giá trị cần thiết trong các biến khác:

bLogToFile = 1

szLogFileName = [user defined or default]

bLogUserName

Loại: Boolean

Yêu cầu trình ứng dụng VirusScan ghi lại tên của người dùng được nhập vào máy tính đích vào thời điểm mà hoạt động quét hiện hành bắt đầu. Trình ứng dụng viết thông tin này sang một log file riêng biệt.

Giá trị = 1 - Trình ứng dụng ghi lại tên người dùng (mặc định)

Giá trị = 0 - Trình ứng dụng không ghi lại tên người dùng

Các giá trị cần thiết trong các biến khác:

bLogToFile = 1

szLogFileName = [user defined or default]

uMaxKilobytes

Loại: szLogFileName

Yêu cầu trình ứng dụng VirusScan xóa log file hiện hành và bắt đầu ghi lại dữ liệu từ thời điểm mà nó được dừng lại khi kích cỡ log file đạt đến giới hạn đã xác định ở đây.

Giá trị là kích cỡ tính bằng các kilobyte.

Value = [user defined; 100 is default]

Các giá trị cần thiết trong các biến khác:

bLogToFile = 1

bLimitSize = 1

szLogFileName = [user defined or default]

szLogFileName

Loại: String

Xác định đường dẫn thư mục và tên file cho file text mà trình ứng dụng VirusScan

sẽ dùng để ghi dữ liệu log.

Value = [user defined; mặc định là C:\Program Files\Common Files\McAfee Virus\Scan\On Demand Scanner\Scan32\VSCLog.TXT

[ScanItems]

Biến	Mô tả
NumScanItems	Loại: Integer Xác định số đích quét mà trình ứng dụng VirusScan sẽ kiểm tra trong suốt hoạt động quét hiện hành. Value = [user defined; default is 1]
szScanItem_x	Loại: String Xác định các đích quét và các loại file mà trình ứng dụng VirusScan sẽ kiểm tra trong suốt hoạt động quét này Chuỗi (string) được chia thành các trường có ký tự pipe . Các giá trị có thể có cho mỗi trường là: Trường 1 - Nhóm ổ đĩa hay thư mục mà trình ứng dụng sẽ quét. Để trống giá trị này nếu bạn muốn chỉ quét một file duy nhất tại bất cứ vị trí nào trong hệ thống. Trường 2 - Tên của file riêng biệt mà trình ứng dụng sẽ quét. Để trống giá trị này nếu bạn muốn quét một nhóm ổ đĩa hay thư mục trên hệ thống. Trường 3 - Số nguyên với các giá trị sau: 1 - Quét file 2 - Quét boot record 3 - Quét từ cả boot record và file Trường 4 - Boolean với các giá trị sau: 1 - Yêu cầu trình ứng dụng VirusScan quét các file trong các thư mục con trong đích quét

0 - Yêu cầu trình ứng dụng VirusScan bỏ qua các file trong các thư mục con trong đích quét

Trường [n] - Các chuỗi vốn liệt kê các phần mở rộng tên file để trình ứng dụng VirusScan có thể quét

[SecurityOptions]

Biến	Mô tả
bComplainOneMonth	Loại: Boolean Hiện không được sử dụng. Không được chỉnh sửa.
bInheritsSecurity	Loại: Boolean Yêu cầu trình ứng dụng VirusScan sử dụng các cài đặt an toàn từ file .VSC này cho bất kỳ tác vụ quét mà bạn tạo bằng cách sao chép tác vụ này trong VirusScan Console. Giá trị = 0 - Các tác vụ quét được tạo bằng cách sao chép tác vụ quét này sẽ không thừa kế các cài đặt an toàn của nó (mặc định) Giá trị = 1 - Các tác vụ quét được tạo bằng cách sao chép tác vụ quét này sẽ thừa kế các cài đặt an toàn của nó.
szPasswordProtect	Loại: Boolean Yêu cầu trình ứng dụng VirusScan đòi hỏi password mà bạn đã gán bất cứ khi nào một người nào đó cố mở các cài đặt cấu hình cho file này. Giá trị = 0 - Trình ứng dụng không yêu cầu password để truy cập các cài đặt cấu hình (mặc định) Giá trị = 1 - Trình ứng dụng yêu cầu password bất cứ khi nào một người nào đó cố

dwComplainYear	gắt mở các trang đặc tính VirusScan Hiện không được sử dụng. Không được chỉnh sửa
dwComplainMonth	Hiện không được sử dụng. Không được chỉnh sửa
dwComplainDay	Hiện không được sử dụng. Không được chỉnh sửa
szPasswordCRC	Dự trữ. Không được chỉnh sửa

[ExcludedItems]

Biến	Mô tả
NumExcludeItems	Loại: Integer Xác định số hạng mục mà trình ứng dụng VirusScan sẽ loại bỏ ra khỏi hoạt động quét này Value = [user defined; default is 1, maxi- mum number permitted is 100 by default]
ExcludeItem_x where x is a zero-based index	Loại: String Yêu cầu trình ứng dụng VirusScan loại bỏ các hạng mục đã liệt kê ra khỏi hoạt động quét này Value = \Recycled (default) Chuỗi được chia thành các trường có ký tự pipe . Các giá trị cho mỗi trường là: Trường 1 - Phần folder của hạng mục để loại bỏ. Để trống cho một file đơn ở bất kỳ vị trí nào trên hệ thống. Trường 2 - Phần file của hạng mục để loại bỏ. Để trống nếu một folder được loại bỏ mà không có tên file. Trường 3 - Số nguyên với các giá trị sau: 1 - Loại bỏ từ quá trình quét khi truy cập file 2 - Loại bỏ từ quá trình quét boot record

3 - Loại bỏ từ quá trình quét khi truy cập file và quá trình quét boot record

Trường 4 - Boolean với các giá trị sau:

1- Yêu cầu trình ứng dụng VirusScan loại bỏ các file trong các thư mục con trong đích quét

0 - Yêu cầu trình ứng dụng VirusScan quét các file trong các folder con trong đích quét

Bài 17

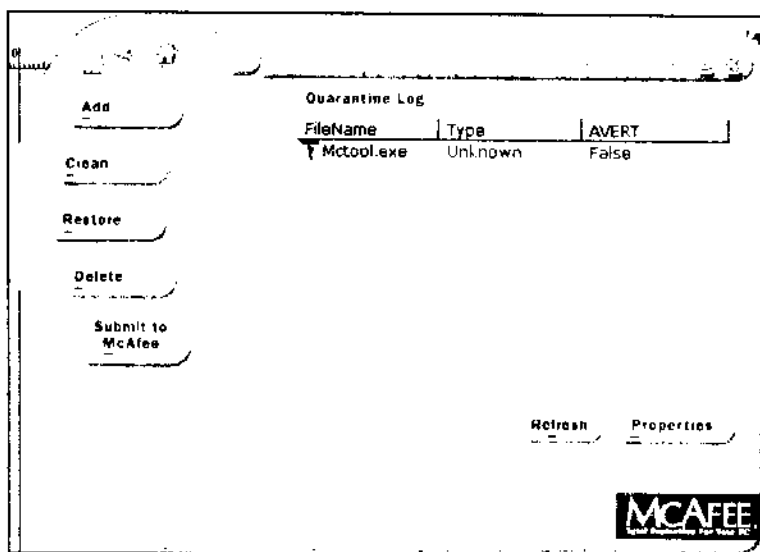
SỬ DỤNG QUARANTINE

I. Sử dụng Quarantine

Nhiều thành phần VirusScan cho phép bạn di chuyển các file bị nhiễm đến một folder cách ly. Thành phần này di chuyển các file bị nhiễm ra khỏi các vùng mà chúng có thể được truy cập và cho phép bạn tùy ý xử lý hay xóa chúng.

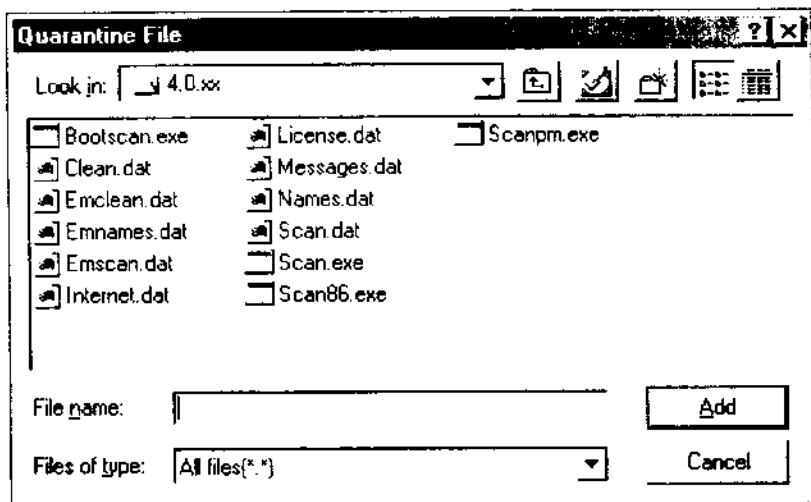
Để Quarantine Explorer làm việc với các file bị nhiễm đã được cách ly, hãy thực hiện các bước sau đây:

1. Khởi động VirusScan Console.
2. Nhấp Quarantine. Cửa sổ Quarantine Explorer xuất hiện.

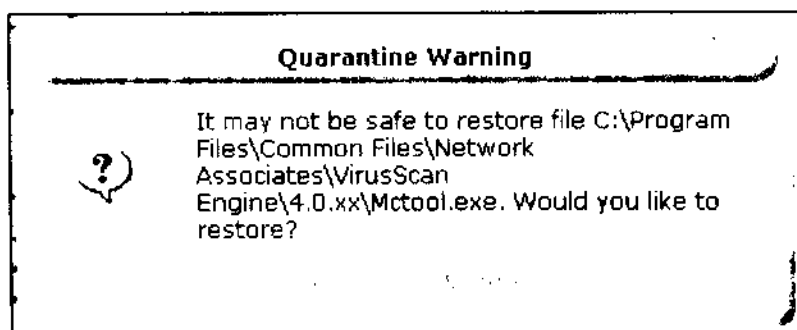


3. Chọn một file bị nhiễm và chọn từ các tùy chọn sau đây:

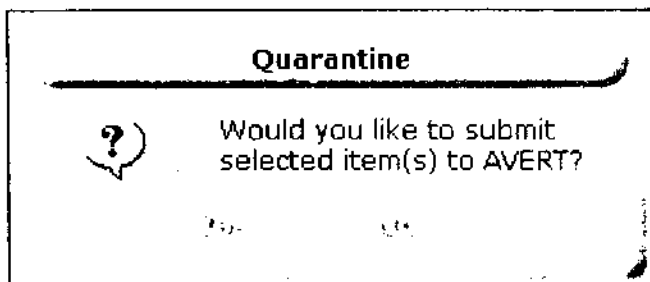
- ❖ Add. Chọn tùy chọn này để cách ly file bị nghi là đã nhiễm virus.



- ❖ Clean. Chọn tùy chọn này để loại bỏ mã virus ra khỏi file bị nhiễm. Nếu không thể loại bỏ virus này, nó sẽ cho bạn biết trong vùng thông báo của nó.
- ❖ Restore. Chọn tùy chọn này để phục hồi một file trở lại folder ban đầu của nó. Tùy chọn này không làm sạch file. Bảo đảm file không bị nhiễm trước khi sử dụng tùy chọn này.



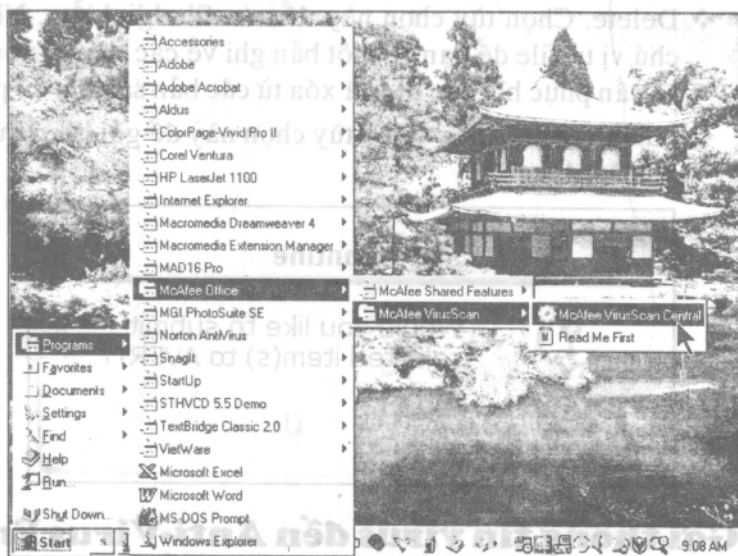
- ❖ Delete. Chọn tùy chọn này để xóa file bị nhiễm. Nhớ ghi chú vị trí file để bạn có một bản ghi về các file đã xóa. Bạn sẽ cần phục hồi các file đã xóa từ các bản sao lưu dự phòng.
- ❖ Submit to McAfee. Chọn tùy chọn này để gửi các virus mới đến McAfee.



II. Gửi thông tin virus đến Anti-Virus Emergency Response Team

Nếu bạn đã tìm thấy file mà bạn nghi là đã bị nhiễm một loại virus mới hay chưa nhận biết. Hãy gửi file bị nhiễm này đến McAfee Labs Anti-Virus Emergency Response Team để phân tích bằng cách sử dụng Submit to McAfee Wizard.

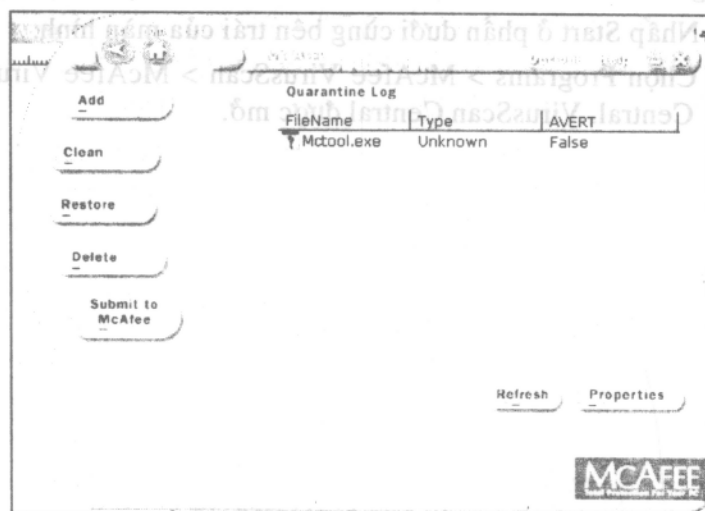
1. Nhấp Start ở phần dưới cùng bên trái của màn hình.
2. Chọn Programs > McAfee VirusScan > McAfee VirusScan Central. VirusScan Central được mở.



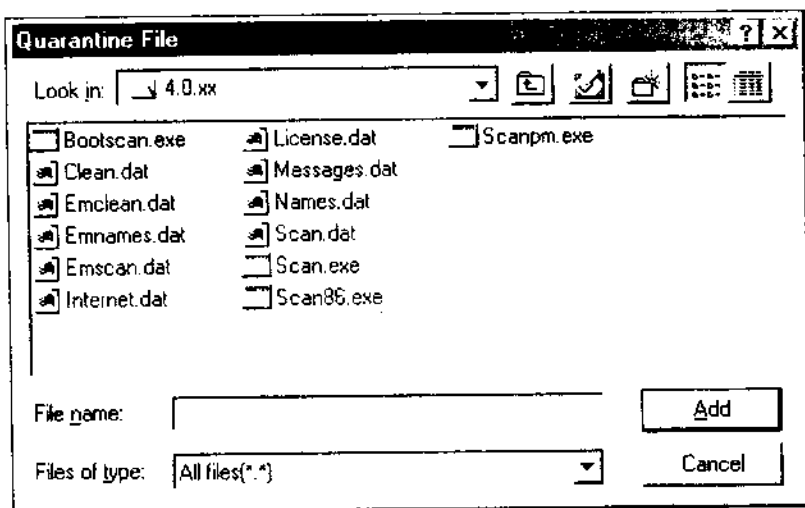
3. Nhấp Quarantine. Quarantine Explorer xuất hiện.

4. Chọn một file trong danh sách hoặc nhấp Add để bổ sung một file bị nhiễm vào danh sách.

5. Nhấp Submit to McAfee. McAfee Labs A.V.E.R.T Wizard xuất hiện.



6. Nhấp Next. Một trang xuất hiện. Bạn có thể gõ nhập một thông báo vào trang này để gửi đến A.V.E.R.T. Nếu bạn muốn, hãy đưa vào thông tin liên hệ cá nhân. Thông tin này hữu ích, nhưng tùy ý.
7. Nhấp Next. Một danh sách xuất hiện.
8. Nhấp Add để chọn file cần gửi.
 - ❖ Cách khác là bạn có thể rê và thả một file từ My Computer hay Windows Explorer đến hộp danh sách.



- ❖ Nếu bạn muốn loại bỏ một file ra khỏi danh sách, chọn nó và nhấp Delete.
9. Nhấp Next. Trang Choose Upload Options xuất hiện.
 10. Chọn Remove Data From File nếu bạn muốn bảo mật dữ liệu.
 11. Nhấp Next. Trang hệ thống phụ e-mail xuất hiện.
 - ❖ Nếu được yêu cầu bởi cấu hình hệ thống, hãy chọn SMTP và nhập tên của server SMTP.
 - ❖ Chọn Send mail through MAPI nếu bạn sử dụng một mail server tương thích MAPI chẳng hạn như Microsoft Outlook.
 12. Nhấp Finish để gửi file.

III. Cập nhật các file dữ liệu VirusScan

Hàng tháng có trên 200 virus mới cũng như các ActiveX control và các lớp Java nguy hiểm xuất hiện. Thông thường, các virus và các đối tượng mới này không thể được tìm thấy bởi các file dữ liệu cũ hơn. Các chuyên viên nghiên cứu virus Network Associates đang làm việc liên tục để cập nhật các file dữ liệu có các định nghĩa virus mới nhất. Các file dữ liệu mới, hay các file .DAT, được ấn hành khoảng bốn đến sáu tuần một lần. Bạn sẽ được thông báo theo định kỳ về thời gian cập nhật các file dữ liệu. Để đạt được sự bảo vệ tối đa, bạn nên cập nhật đều đặn các file VirusScan .DAT.

Để cập nhật các file dữ liệu, hãy nhấp nút Update trên màn hình dành cho trang chủ McAfee VirusScan. Thủ tục cập nhật này cũng bao hàm cả tùy chọn để tải xuống bất kỳ trình cập nhật có sẵn nào trên phần mềm McAfee VirusScan đã cài đặt trên máy tính của bạn.

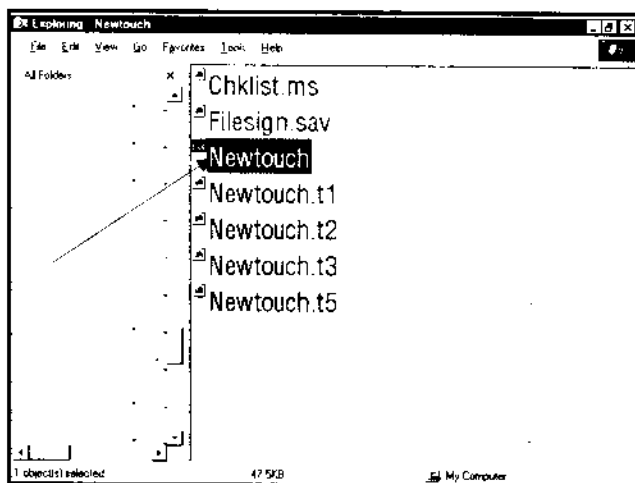
Phụ lục

HƯỚNG DẪN SỬ DỤNG BÀN PHÍM VỚI PHẦN MỀM NEWTOUCH

I. Chép phần mềm touch.exe

- Chương trình NEWTOUCH chỉ chiếm khoảng 200KB và không đòi hỏi phải cài đặt (Install), do đó bạn chỉ cần mở một thư mục NEWTOUCH rồi chép tất cả tập tin vào là được.

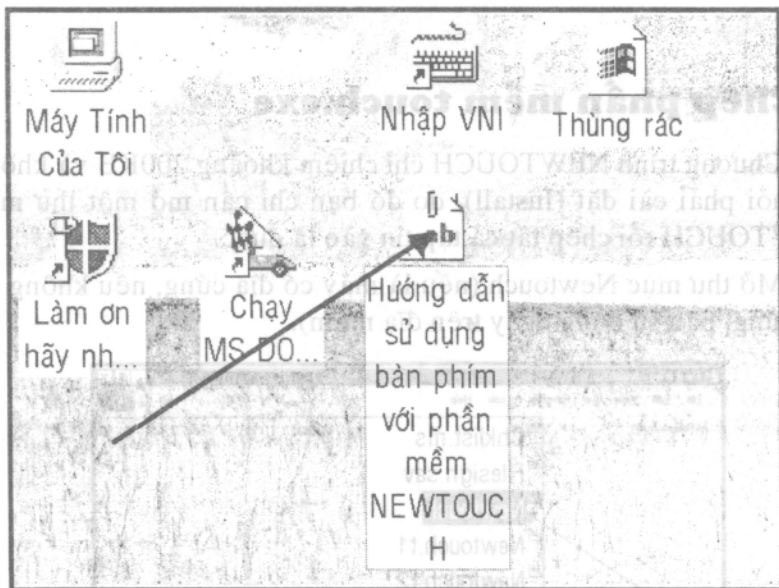
- Mở thư mục Newtouch (nếu là máy có đĩa cứng, nếu không có đĩa cứng, bạn sử dụng ngay trên đĩa mềm).



Tạo thư mục NEWTOUCH trên ổ đĩa cứng máy bạn. Chép chương trình Newtouch vào (gồm 7 tập tin)

- ❖ Chklist.ms
- ❖ Filesign.sav
- ❖ Newtouch
- ❖ Newtouch.t1
- ❖ Newtouch.t2
- ❖ Newtouch.t3
- ❖ Newtouch.t5

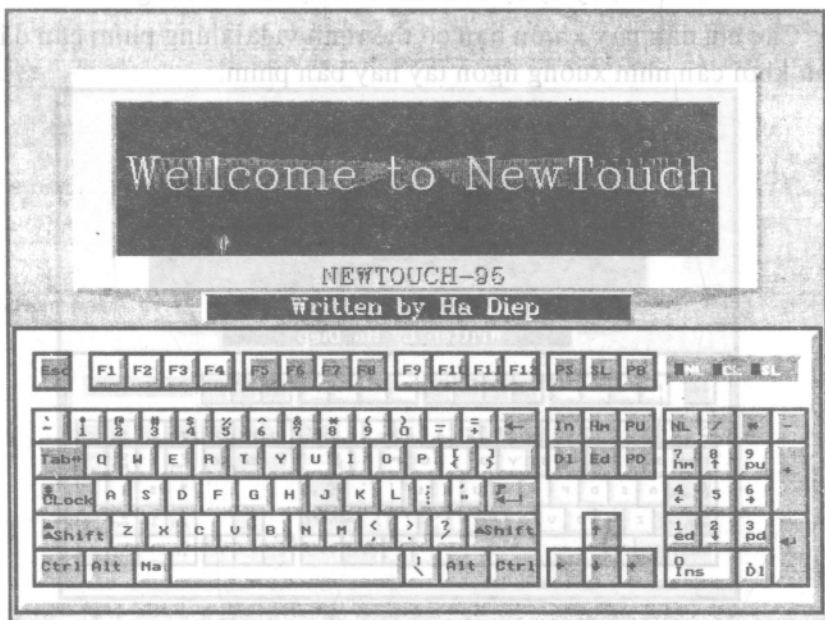
Tạo một Shortcut trên màn hình nền Windows.



II. Vào chương trình newtouch

1. Hiện thị màn hình giới thiệu chương trình NEWTOUCH

Ở đây màn hình có dòng chữ “Press any key to continue” (nhấn bất kỳ phím nào để tiếp tục). Bạn nên nhấn <Spacebar>. Bạn sẽ thường gặp câu thông báo này và sẽ thao tác giống như trên.

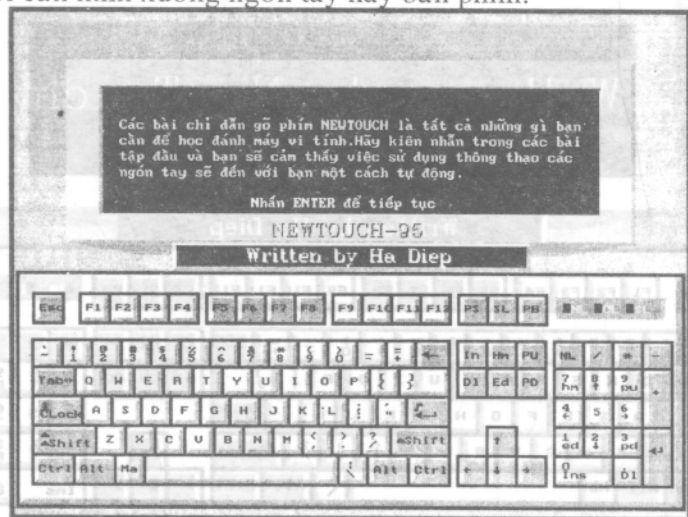


2. Lần lượt bạn sẽ thường gặp các câu thông báo sau:

1. Newtouch Typing tutor is all you will need... Các bài chỉ dẫn gõ phím NEWTOUCH là tất cả những gì bạn cần để học đánh máy tính. Hãy kiên nhẫn trong các bài tập đầu và bạn sẽ thấy việc sử dụng thông thạo các ngón tay sẽ đến với bạn một cách tự động.
2. Một trong những trở ngại đầu tiên đối với người mới học đánh máy là phải làm sao vượt qua được sự cảm dỗ nhìn vào ngón tay của mình trên bàn phím (tập quen không nhìn vào bàn phím).
3. Chương trình này cung cấp cho bạn rất nhiều chỉ dẫn sao cho bạn có thể thao tác thành thạo vừa đúng lại vừa nhanh.
4. Chỉ dẫn:
 - 1/ Ký tự mà bạn sắp phải đánh sẽ được chiếu sáng.
 - 2/ Khi bạn gõ phím sai, bạn sẽ được báo bằng một tiếng bíp.

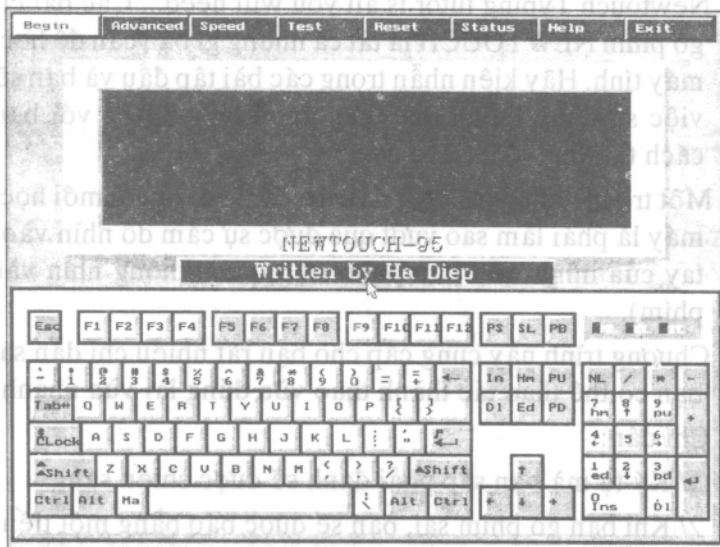
3/ Khi đó, ký tự bị đánh sai sẽ được chiếu sáng.

Các chỉ dẫn này khiến bạn có thể định vị lại đúng phím cần đánh mà khỏi cần nhìn xuống ngón tay hay bàn phím.



3. Có 10 phím chức năng để bạn sử dụng vào bất cứ lúc nào:

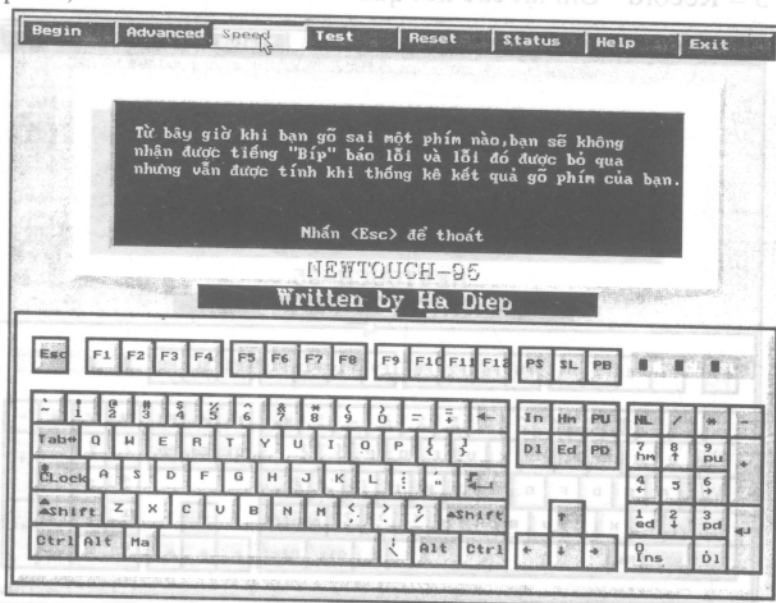
F1 = Begin - Bắt đầu các bài tập



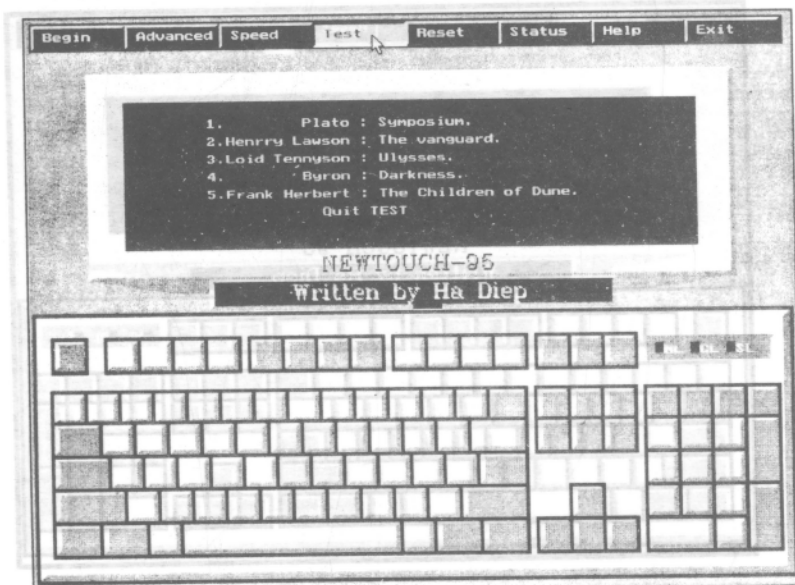
F2 = Next - Bài tập kế tiếp



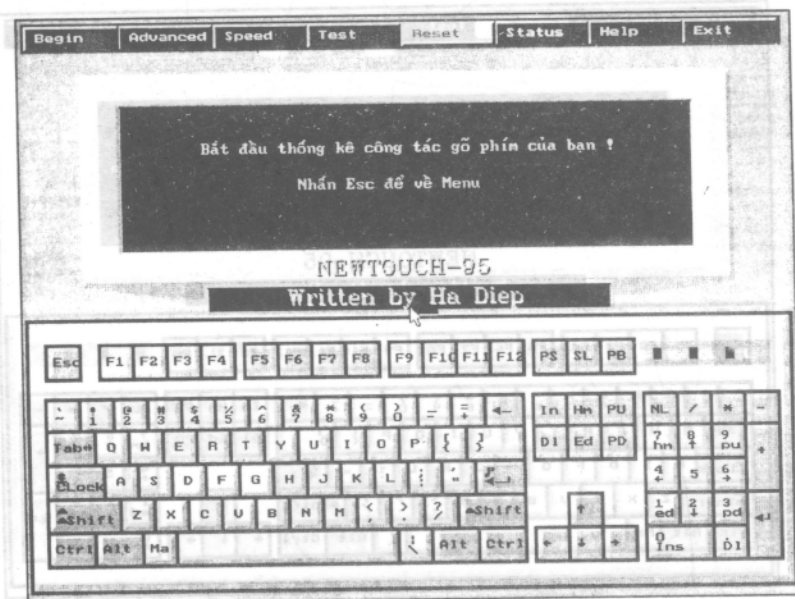
F3 = Advanced - Các bài tập nâng cao (không còn chứa màn hình bàn phím)



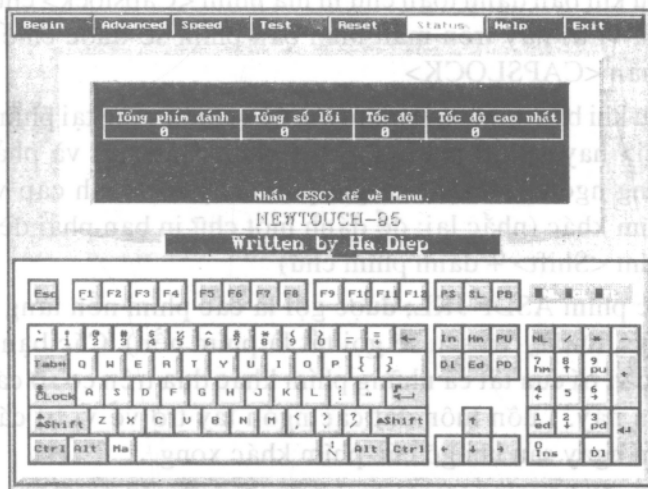
F4 = Speed - Tập đánh nhanh, không kể các lỗi



F5 = Record - Ghi lại các kết quả



F6 = Tests - Gồm 5 bài văn học dùng để thử nghiệm việc đánh nhanh và đúng

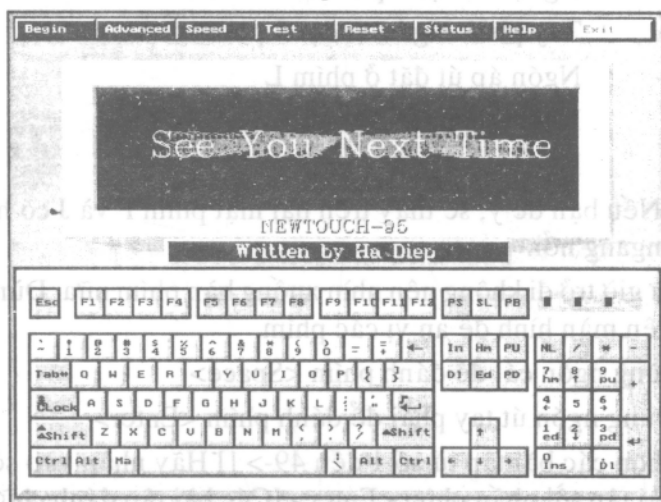


F7 = Report - Báo cáo tình trạng của máy in

F8 = Reset - Bắt đầu việc thống kê công tác gõ phím của bạn

F9 = Status - Thể hiện các thống kê

F10 = Finish - Kết thúc bài tập và thoát.



III. Các ghi chú đặc biệt

1. Nếu khi bạn đánh toàn chữ in mà phím <Capslock> chưa được cài, vị trí này trên màn hình bàn phím sẽ được chiếu sáng. Nhấn <CAPSLOCK>
2. Nếu khi bạn đánh một phím mà đèn chiếu sáng tại phím <Shift trái> hay <Shift phải> (có hai phím Shift trái và phải), bạn dùng ngón út để đề và giữ phím này rồi đánh cặp với một phím khác (nhắc lại: để đánh một chữ in bạn phải đề và giữ phím <Shift> + đánh phím chữ)
3. Các phím ASDF JKL; được gọi là các phím nền tảng (Home keys, từ đây về sau sẽ gọi tắt là phím nền). Các bạn sẽ học các vị trí của tất cả những phím khác dựa trên cơ sở các phím nền này. Luôn luôn đặt các ngón tay trở về vị trí các phím nền ngay sau khi gõ các phím khác xong.
4. Bây giờ hãy đặt các ngón tay ở trên các phím nền
Tay trái: Ngón út đặt ở phím A
Ngón áp út đặt ở phím S
Ngón giữa đặt ở phím D
Ngón trỏ đặt ở phím F
Tay phải: Ngón út đặt ở phím;
Ngón áp út đặt ở phím L
Ngón giữa đặt ở phím K
Ngón trỏ đặt ở phím J
Nếu bạn để ý, sẽ thấy trên hai mặt phím F và J có hai vạch ngang nổi.
5. Từ giờ trở đi không nên nhìn xuống bàn phím nữa. Dùng sơ đồ trên màn hình để an vị các phím.
6. Dùng ngón cái để đánh phím <Space>
Dùng ngón út tay phải để đánh phím <Enter>
7. Chọn các bài tập từ số 1 đến 49-> [] Hãy nhập vào số thứ tự bài tập rồi nhấn phím <Enter> [Các bài tập đánh chữ từ số 1

đến 43, các bài tập đánh số từ 44 đến 49]

IV. Các bài tập

Bài tập 1

FDSAJKL; FDSAJKL;

- ❖ Ba bài tập đầu dành để làm quen các phím nền. Đặt các ngón tay lên đúng vị trí trên các phím nền và bắt đầu - Nhấn phím bất kỳ để tiếp tục.
- ❖ Câu nhận xét: (thí dụ) bạn đã đánh các phím nền tốt. Bạn có muốn tiếp tục qua bài tập kế tiếp không (Y/N)? - Nếu muốn nhấn (Y), nếu không muốn qua bài tập kế mà muốn trở lại bài tập vừa rồi, nhấn (N).
- ❖ Nhận xét tiếp: bài tập số 1 - Lặp lại một lần - Lỗi 3/3, tốc độ 34 (từ/phút).

Bài tập 2

ASDF; LKJ, A;SL DKFJ

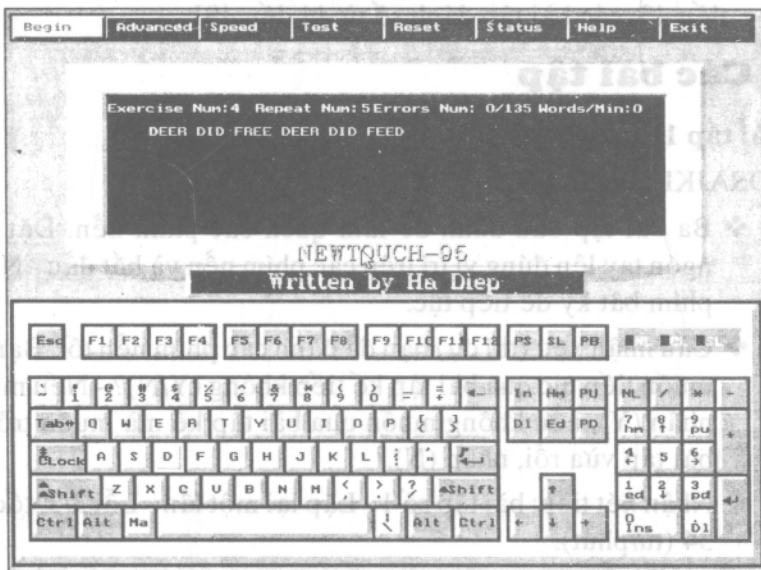
Bài tập 3

LADS JADA FALLS SAD LASS JALK

Bài tập 4

Hai bài tập kế tiếp dành cho các phím E R và I. Dùng ngón gõ phím D để gõ E, phím F cho R và phím K cho I.

DEER DID FREE DEER DID FEED



Bài tập 5

Luôn luôn nhớ trở về vị trí nhóm phím nền. Cố gắng đánh cho đều và chính xác.

RAIJ DID SIRE LIFE RED RIDER RIDES FAR

Bài tập 6

Dùng ngón đánh phím J để đánh phím U

LUKE DIS RUE DRUIDS DID FREE LASS

Bài tập 7

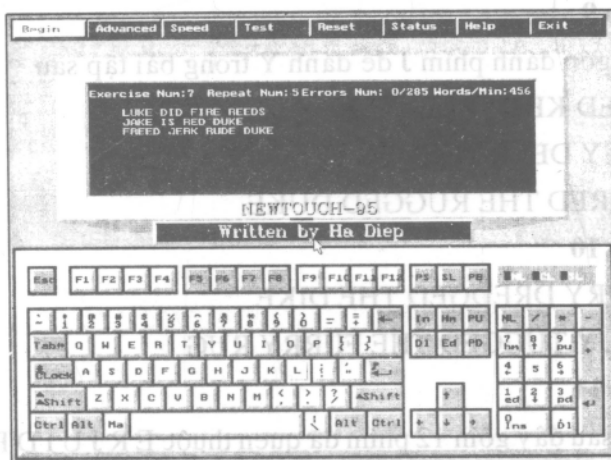
Bài tập tiếp theo sử dụng 8 phím bạn đã quen thuộc từ trước đó là: ERDFUIJK

Nhớ dùng ngón út tay phải để đánh phím <Enter>

LUKE DID FIRE REEDS

JAKE IS RED DUKE

FREED JERK RUDE DUKE



Bài tập 8

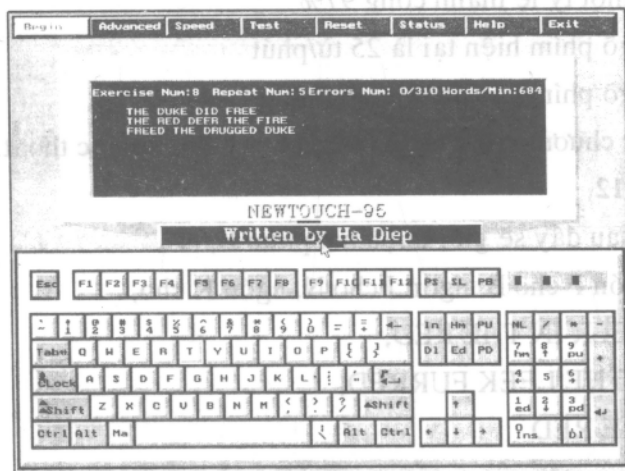
Bài tập tiếp theo dùng các phím T G và H

Dùng ngón đánh phím F để đánh các phím T và G, ngón đánh phím J để đánh phím H

THE DUKE DID FREE

THE RED DEER THE FIRE

FREED THE DRUGGED DUKE



Bài tập 9

Dùng ngón đánh phím J để đánh Y trong bài tập sau

THE RED KEY FREE

THE FEY DEER THEY

DEFERRED THE RUGGED DUKE

Bài tập 10

THE JURY DREDGED THE DIKE

THE GUY TUGGED THE FURRY RUG

Bài tập 11

Bài tập sau đây gồm 12 phím đã quen thuộc E R J U I D F G H J K:

THE GUY DID FIRE THE RED FUR

THE DRUDGERYY FIRED THE JURY

THE DRUGGED DEER DIED

ĐẶC BIỆT: Khi nhấn phím F10 để kết thúc, bạn sẽ nhận được một tổng kết sau:

Bài tập kế tiếp của bạn sẽ là bài 12,

Trong buổi làm việc hôm nay bạn đã đánh 186 phím, gồm có 6 lỗi, đây là một tỷ lệ thành công 97%

Tốc độ gõ phím hiện tại là 25 từ/phút

Tốc độ gõ phím cao nhất là 46 từ/phút

Kết thúc chương trình nhấn phím bất kỳ để tiếp tục thoát.

Bài tập 12

Bài tập sau đây sẽ giới thiệu hai phím B, N

Dùng ngón F cho B, ngón J cho N, ngón K cho,

FREE BEER IN THE RED,

RED IN THE LEEK FURRED,

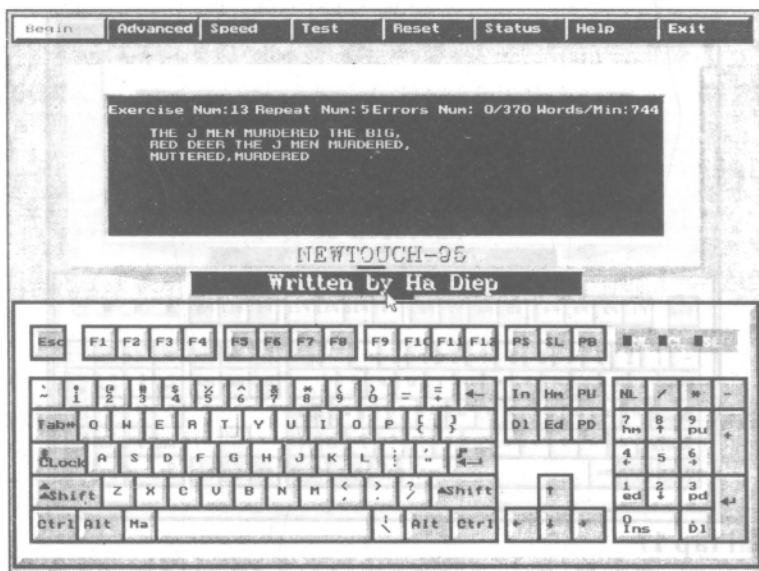
THE FIRE RED

Bài tập 13

Dùng ngón J cho M

THE J MEN MURDERED THE BIG,

RED DEER THE J MEN MURDERED, MUTTERED, MURDERED

**Bài tập 14**

Dùng ngón D cho C và F cho V

THE CIVIC MAN MEETS IN THE CENTURY INN

THREE, FREE MEN DID VILE AND GRIEVED

Bài tập 15

Ôn lại các phím nền “Home keys”

THE BIG MEN CEDED THE FIGHT

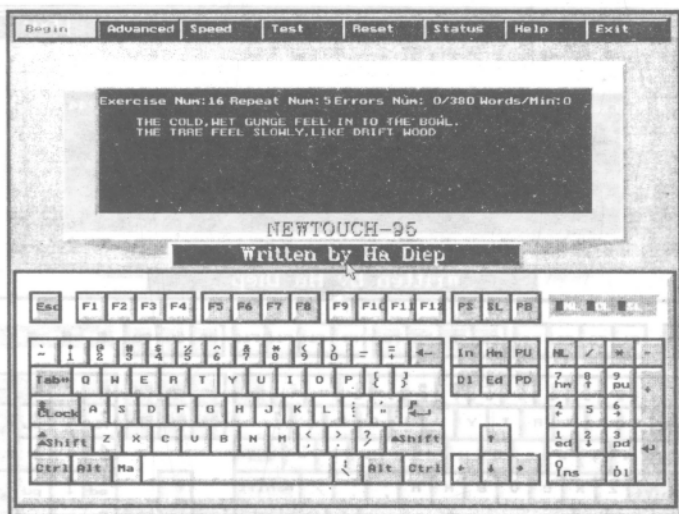
HE NEEDED THE CENT TO FEED THE METER

THE CIVIC DEAR MEETS HER FRIEND

Bài tập 16

Dùng ngón áp út (nhấn) trái cho S và W, dùng ngón áp út phải cho L O và (.)

THE COLD, WET GUNGE FELL INTO THE BOWL.
THE TREE FELL SLOWLY, LIKE DRIFT WOOD.

**Bài tập 17**

Dùng ngón S cho X

THE VET SOON FIXED THE FOX FOR MONEY.
TEXT BOOKS FEED VEXED HUNGRY MINDS.

Bài tập 18

SEXTET IS THE CIRCLE OF SIX NOT SEX.

THE WHIRL WIND FELLE THE GLISTENING TREES.

Bài tập 19

TELL ME, SHE MUTTERED, OF THE GRIFFIN
THE OLD GODS LONG FORGOTTEN, EXILED NOW,
THEY KEEN IN HUNGER.

Bài tập 20

Dùng ngón út phải cho P

HIS HEART PULSATED, TIME FRAGMENTS.

THE DEER PLAYED AND PASSED THE PORT.

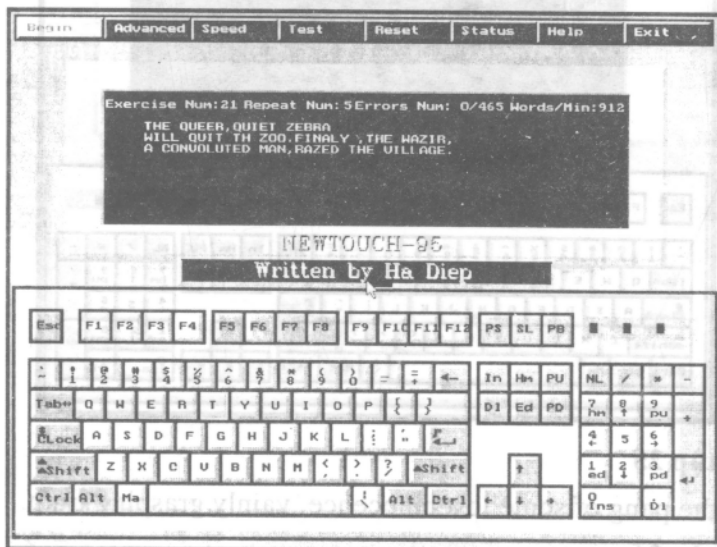
Bài tập 21

Dùng ngón A để đánh Z và Q

THE QUEER, QUIET ZEBRA

WILL QUIT THE ZOO, FINALLY, THE WAZIR,

A CONVOLUTED MAN, RAZED THE VILLAGE.

**Bài tập 22**

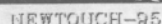
IMAGES OF THE MULTIVERSE, GLORIOUS,

SEEN THROUGH THE SLEEP BLURRED EYES.

Bài tập 23

WE ARE SAD ONES,

YOU AND I SHAKING



st innocence, vainly grasping truth.

you do falls silently behind. He is nothing
n forgotten mind.

plain where the dragon breeds and dies the
en dance.

trapped in their separate lies.

Bài tập 29

We ran through the blackened mists, till we reached the green glass shore.

Bài tập 30

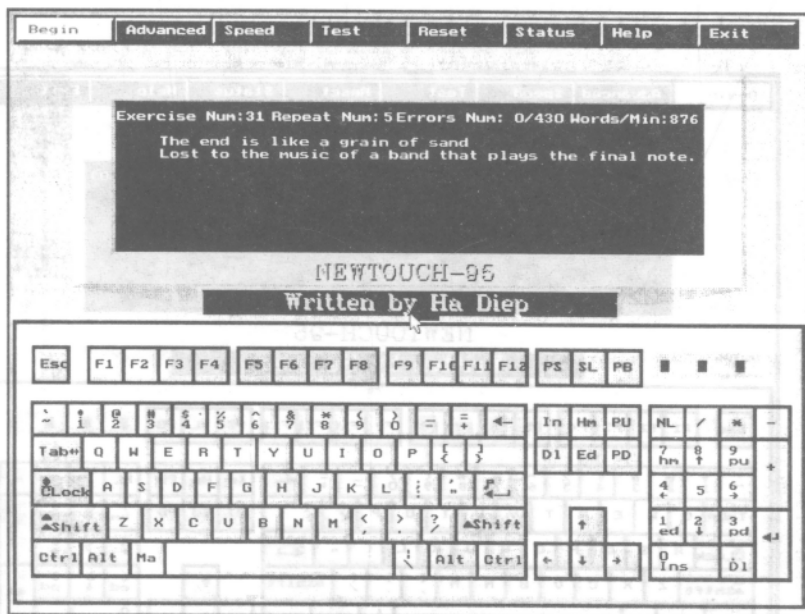
The clouds were mushrooms all round

blessing distant wars.

Bài tập 31

The end is like a grain of sand

Lost to music of a band that plays the final note.



Bài tập 32

The tears groze on our last goodbyes
as we faced the blood red sea.

Bài tập 33

We looked and laughed, as we saw at last
that now the world was free.

Bài tập 34

Once again the jewelled piper, mounted on his dragon steed, found
the lords of chaos

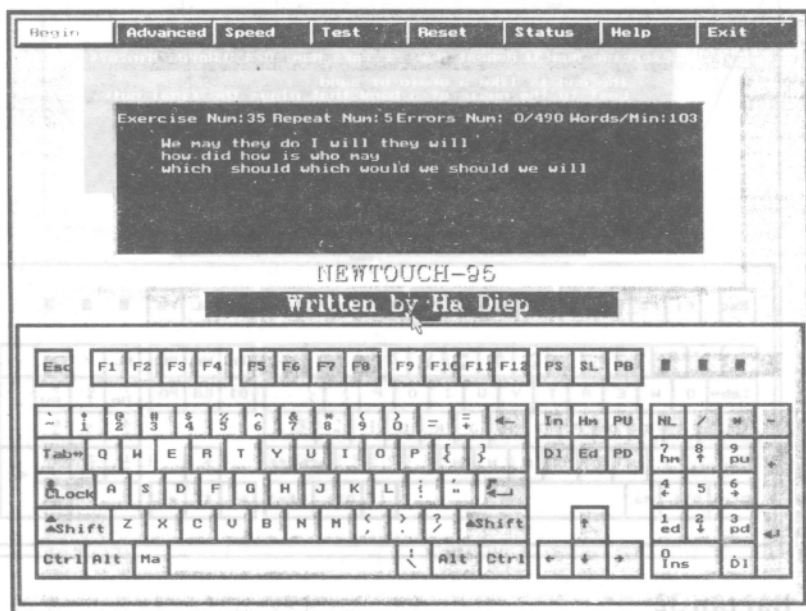
Bài tập 35

Ba bài tập kế tiếp được dùng thường xuyên trong các câu đơn giản

We may they do I will they will

how did how is who may

which should which would we should we will

**Bài tập 36**

I am I will he will I do he does he does not

it is it is not it maybe to the on the

Bài tập 37

For me for you to live to want to see to go
to go out to go down to go up to be able to be

Bài tập 38

Ba bài tập kế tiếp được dùng cho các tiếp đầu ngữ (prefixes): anti, bi, de, etc...

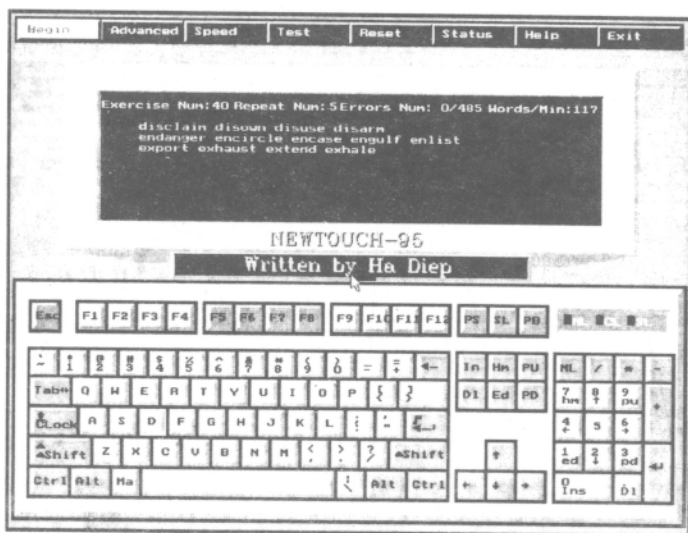
antibody anticyclone antidote anticlimax antipodes
automobile automatic automaton autobiography

Bài tập 39

bicycle bifocal biennial biped circumvent
circumference circumnavigate
defuse defrost devalue decipher decode

Bài tập 40

disclaim disown disuse disarm
endanger encircle encase engulf enlist
export exhaust extend exhale



Bài tập 41

Ba bài tập kế tiếp dành cho các tiếp vĩ ngữ (suffixes): able, en, ed, etc...

taxable durable movable washable

voltage postage foliage breakage

arrival rental trial refusal serial

MỤC LỤC

Phần 1

Norton AntiVirus 2001

Bài 1 : Giới thiệu về Norton AntiVirus 2001	8
I. Thế nào là một virus máy tính?	11
II. Phân loại virus theo vùng bị nhiễm:	12
III. Bàn về Exclusions	12
IV. Bàn về Norton AntiVirus Quarantine	13
V. Bàn về Activity Log	14
VI. Bàn về Repair Wizard	15
VII. Bàn về việc cập nhật các phần định nghĩa virus với LiveUpdate	16
VIII. Những vùng mà virus lây nhiễm và không lây nhiễm	17
IX. Bàn về Virus List	18
Bài 2 : Các tác vụ quan trọng trong Norton AntiVirus	19
I. Quét để tìm virus trên máy tính	19
II. Cài đặt sự bảo vệ tối đa	21
III. Loại bỏ virus ra khỏi máy tính	32
IV. Để cập nhật các định nghĩa virus bằng cách sử dụng LiveUpdate	35
V. Tìm và sử dụng Virus List	39
VI. Hiện thị thông tin về một virus	43
VII. Để cách ly một hạng mục đã bị nhiễm hoặc nghi ngờ là có bị nhiễm:	44
VIII. Xem thông tin về một hạng mục đã cách ly	46
IX. Chỉ định một Quarantine options password	46
X. Chỉ định các hành động Quarantine có thể chấp nhận được	47
XI. Để gửi một file đã cách ly với SARC	48

Bài 3 : Cách hoạt động của Norton Antivirus 49

I. Cách hoạt động của Norton Antivirus	49
II. Sử dụng Norton Antivirus	53
III. Bàn về Norton Antivirus Auto-Protect	54
IV. Các lệnh chuyển đổi dòng lệnh	56
V. Xác định cách hoạt động của chế độ bảo vệ vào lúc khởi động	58
VI. Khởi động lại máy tính đã tắt	59

Bài 4 : Quét các ổ đĩa, các file và các folder 61

I. Quét các ổ đĩa	61
II. Thay đổi các tùy chọn quét đối với các tiến trình quét mà bạn khởi chạy hay lập thời biểu	62
III. Chọn các phần mở rộng file mà Norton Antivirus quét	63
IV. Loại bỏ các file ra khỏi tiến trình quét virus	67
V. Lưu ý về việc quét các ổ đĩa mạng	69
VI. Quét một file riêng lẻ	70
VII. Quét một folder	71
VIII. Quét một đường dẫn	71
IX. Chọn khi nào các file được quét bởi Auto-Protect	71
X. Chọn các file nào cần quét khi bạn khởi chạy một tiến trình quét bằng tay hay quét theo thời biểu.	72
XI. Xác lập các tùy chọn quét	73
XII. Xác lập các tùy chọn quét chung	74

Bài 5 : Xử lý và loại bỏ các file bị nhiễm virus 77

I. Xử lý file hay record khởi động đã bị nhiễm virus	77
II. Thay đổi cách hoạt động của Norton AntiVirus	78
III. Loại bỏ một virus macro Microsoft Word	79
IV. Chọn hành động mà Norton AntiVirus sẽ thực hiện khi một virus được tìm thấy trong suốt tiến trình quét bằng tay hay quét theo thời biểu:	80
V. Loại bỏ một file bị nhiễm	82
VI. Sử dụng Help	83

Phần 2

McAfee VirusScan

Bài 6 : Tìm hiểu trình ứng dụng VirusScan 88

I. Khi nào và tại sao cần sử dụng trình ứng dụng VirusScan	89
II. Xác định trình ứng dụng VirusScan	90
III. Các file phụ thuộc và liên quan đối với trình ứng dụng VirusScan	91
IV. Khởi động trình ứng dụng VirusScan	95
V. Ngưng trình ứng dụng VirusScan	102
VI. Cấu hình các xác lập trình ứng dụng VirusScan	106
VII. Cấu hình giao diện VirusScan Classic	106
VIII. Cấu hình giao diện VirusScan Advanced	114
IX. Cấu hình các tác vụ VirusScan theo thời biểu	126

Bài 7 : Tìm hiểu VShield scanner 143

I. Các bộ trình duyệt web và các e-mail client tương thích	147
II. Tại sao bạn nên sử dụng VShield scanner	148
III. Xác định VShield scanner trên hệ thống	149
IV. Khởi động VShield scanner	149
V. Ngưng hoặc tắt VShield scanner	155
VI. Khởi động lại tại VShield scanner và Console từ control panel	160
VII. Các file phụ thuộc và liên quan dành cho VShield scanner	161
VIII. Xem các số liệu thống kê VShield scanner	167
IX. Cấu hình VShield scanner	170
X. Cấu hình System Scan	172
XI. Cấu hình module E-Mail Scan	189
XII. Cấu hình module Download Scan	201
XIII. Cấu hình module Internet Filter	208
XIV. Cấu hình module Security	218
XV. Bảo vệ các trang đặc tính riêng lẻ trong các module VShield ..	221

Bài 8 : Tìm hiểu VirusScan Console 223

I. Tại sao bạn nên lập thời biểu cho các hoạt động quét	223
II. Xác định VirusScan Console trên hệ thống	225
III. Khởi động VirusScan Console	225
IV. Ngưng VirusScan Console	227
V. Khởi động lại VShield scanner và Console từ control panel	230
VI. Làm việc với cửa sổ Console	230
VII. Làm việc với các tác vụ mặc định VirusScan Console	238
VIII. Đặt tên cho các tác vụ và xác lập các đặc tính giao diện	240
IX. Xác lập password cho các tác vụ đã lập thời biểu	247
X. Lập thời biểu cho một tác vụ	250
XI. Xem thông tin về tình trạng tác vụ	254

Bài 9 : Tìm hiểu phần mở rộng E-Mail Scan 257

I. Khi nào và tại sao bạn phải sử dụng phần mở rộng E-Mail Scan	257
II. Khởi động phần mở rộng E-Mail Scan	259
III. Ngưng phần mở rộng E-Mail Scan	259
IV. Các file phụ thuộc và liên quan dành cho phần mở rộng E-Mail Scan	260
V. Cấu hình phần mở rộng E-Mail Scan	263

Bài 10 : Tìm hiểu tiện ích Alert Manager 273**Bài 11 : Tìm hiểu trình tiện ích ScreenScan 281**

I. Các file phụ thuộc và các file liên quan dành cho trình tiện ích ScreenScan	283
II. Cấu hình trình tiện ích ScreenScan	285
III. Xác định các đích quét cho trình tiện ích ScreenScan	291

Bài 12 : Tìm hiểu các trình tiện ích AutoUpdate và AutoUpgrade .. 283

I. Bắt đầu và ngưng các thao tác AutoUpdate và AutoUpgrade	295
II. Xác định các file AutoUpdate và AutoUpgrade trên hệ thống	297
III. Các tùy chọn dòng lệnh cho các trình tiện ích AutoUpdate và AutoUpgrade	297
IV. Cấu hình trình tiện ích AutoUpdate	301

Mục Lục	405
V. Cài đặt các đặc tính Automatic Update	304
VI. Cấu hình trình tiện ích AutoUpdate	308
VII. Cài đặt các đặc tính của Automatic Updgrade	311
Bài 13 : Tìm hiểu trình tiện ích tạo Emergency Disk	315
I. Các file VirusScan Emergency Disk	316
II. Sử dụng wizard tạo Emergency Disk	318
III. Chạy một hoạt động quét Emergency Disk	319
Bài 14 : Tìm hiểu panel điều khiển VirusScan	321
I. Các file panel điều khiển VirusScan	323
II. Làm việc với panel điều khiển VirusScan	325
Bài 15 : Tìm hiểu các trình quét dòng lệnh VirusScan	329
I. Các tùy chọn dành cho trình quét dòng lệnh VirusScan	331
II. Các cấp độ lỗi cho trình quét VirusScan Command Line	347
Bài 16 : Tìm hiểu các dạng file .ALR và .VSC	349
I. Tìm hiểu dạng file .ALR	349
II. Tìm hiểu dạng file .VSC	352
Bài 17 : Sử dụng Quarantine	375
I. Sử dụng Quarantine	375
II. Gửi thông tin virus đến Anti-Virus Emergency Response Team ...	377
III. Cập nhật các file dữ liệu VirusScan	380
Phụ lục : Hướng dẫn sử dụng bàn phím với phần mềm NEWTOUCH	381
I. Chép phần mềm touch.exe	381
II. Vào chương trình newtouch	382
III. Các ghi chú đặc biệt	388
IV. Các bài tập	389

HƯỚNG DẪN SỬ DỤNG **NORTON ANTIVIRUS 2001** **&** **MCAFEE VIRUSSCAN**

Chịu trách nhiệm xuất bản: **CÁT VĂN THÀNH**
Biên tập : **CÔNG BÌNH**
Trình bày : **TRẦN BÁ PHÚC**
Bìa : **ĐÌNH DUY HÂN**
Thực hiện liên doanh : **Công ty Văn hóa Nhân Văn**

In 2.000 cuốn, khổ 14 x 20cm. Tại XN In Gia Định, số 9D Nơ Trang Long, Q. Bình Thạnh, TP. Hồ Chí Minh - ĐT: 8412644. Giấy phép xuất bản số 151-99/XB-QLXB. Nhà Xuất bản Thống Kê cấp ngày 16.8.2001. In xong và nộp lưu chiểu tháng 9 năm 2001.

KS. Lê Ngọc Cường

Hướng dẫn sử dụng

Norton AntiVirus

2001

&

McAfee VirusScan



NHÀ XUẤT BẢN THỐNG KÊ

NHÀ SÁCH NHÂN VĂN

189 CMT8 - F.7 - Q. TB- Tp. HCM

ĐT : 9702389 - Fax : 9701876

15E Nguyễn Thị Minh Khai - Q. 1 - Tp.HCM

ĐT : 8227365

HƯỚNG DẪN SỬ DỤNG NORTON ANTI VIRUS & MCAFEE



S001

2

23/06/2004

46,000

Giá : 46.000đ