WIN9X013 October 2001

# Using McAfee VirusScan v4.5

Jocelyn Kasamoto

## Introduction

Computer viruses, including worms and Trojan horses, are prevalent in today's computing environment. Since most computers are connected to a network such as a local area network (LAN) and the Internet, viruses can spread rapidly via e-mail attachments (e.g. ILOVEYOU and Melissa viruses); Internet downloads and shared files on network connections. Virus infections cause loss of valuable data and time needed to clean up after an infection. Everyone must be aware of new virus alerts, have an antivirus software installed, and keep the antivirus software current.

This document provides information to help you become "virus-aware" and covers the basics of using McAfee VirusScan v4.5 on the Windows 95/98/2000 Pro/NT Workstation platform. It assumes that you have already installed McAfee VirusScan, which is the antivirus software currently supported by ITS. Please see ITS document WIN9X010, *Installing McAfee VirusScan v4.5*, before continuing. This document is available at the ITS Help Desk in Keller 105 or on the web at www.hawaii.edu/itsdocs.

## What is a Computer Virus?

A computer **virus**, as defined by the Virus-L/comp.virus newsgroup, is

> "a self-replicating program containing code that explicitly copies itself and that can 'infect'other programs by modifying them or their environment such that a call to an infected program implies a call to a possibly evolved copy of the virus."

The program does not have to do outright damage (e.g. deleting or corrupting files) to be called a "virus". Examples are the Michelangelo boot sector virus and the Jerusalem file-infecting virus.

A computer **worm** is a self-contained program or set of programs that can spread functional copies of itself or its segments to other computer systems usually through network connections. Unlike viruses, worms do not need to attach themselves to a host program. Examples are the ILOVEYOU and Pretty Park worms.

A **Trojan horse** is a computer program that does something undocumented that the programmer intended but that the user would not have approved of if he knew about it. The term "Trojan" is usually referred to a "non-replicating" malicious program. For example, BackOrifice allows the programmer to control an infected computer remotely.

A **macro virus** is a computer virus that uses an application's own macro programming language to distribute itself. Unlike previous viruses, a macro virus doesn't infect programs; it infects documents and templates. Examples are the Melissa and Marker Word macro viruses.

Most people use the term "virus" to loosely cover any program that tries to hide its malicious function and spread to as many computers as possible. **ITS will use the term, virus, to represent viruses, worms or Trojan horses.**

## How Computer Viruses Work

Computer viruses are programs which are **executable** files such as .exe and .com files, macros (scripting language found in Microsoft Word, Excel and other applications), Visual Basic scripts and other executable code. The malicious code must be executed (i.e. run) before it can infect the host system and spread. For example, opening a document infected with a macro virus, booting with a diskette infected with boot sector virus or double-clicking on a program file infected with a virus are ways to execute a virus.

Viruses may or may not have a payload (i.e. action programmed by the virus writer to occur on an infected system). The payload could range from irritating text that pops up on your screen, text embedded in your document, deleted or corrupted files to a reformatted hard drive (i.e. losing all your data and programs). Often times the payload is not immediate after being infected but may be triggered by a date, time, number of file opens, etc. so the infection may not be noticed until it is too late.

## How are Computer Viruses Spread?

Network connections give viruses many different avenues to spread themselves. You can spread a virus if you share files with others from a disk, a network drive, external drive media or exchange files over the Internet via e-mail attachment or browsing an infected web server. You could also get virus infections from Internet downloads. Opening a document or template that contains a macro virus will infect your system and will spread to other documents and templates on your system.

Popular computer products are often the favorite targets of virus writers. Examples are Windows 95/98/2000 Pro/NT Workstation, Microsoft Office (Word, Excel, PowerPoint, Access), Outlook, and Outlook Express. If you use these operating systems and applications, be on guard. New viruses and their numerous variants are constantly being introduced. Viruses are typically platform-specific. With new cross-platform macro language for Microsoft Office, it is possible for a PC Word macro virus to infect a Macintosh Word file.  A PC Word document infected with a macro virus could infect a Macintosh if the infected Word document were opened on the Macintosh.

If you receive an e-mail message with an infected attachment, you will not get infected if the attachment is not opened. If you receive suspicious e-mail (e.g. multiple e-mail messages with the same subject header, attachments from unknown users or unexpected attachments from known users), do NOT open the attachment without scanning it first! If in doubt, delete the message and contact the user who sent the attachment.

Unfortunately, we can not predict how the next virus attack will occur. We have already seen an attempt to pass a virus through e-mail without the recipient opening the message or attachment.

## Two is Not Better Than One…

Please make sure that you have only **one** copy of antivirus software installed on your PC. Multiple copies may cause conflicts and system instability when competing antivirus software scan for viruses at the same time.

> **If you have Dr. Solomon's antivirus software, it is no longer on the ITS contract. You must uninstall Dr. Solomon by following details in *Installing McAfee VirusScan v4.5*.**

Some new computers come preinstalled with Norton Antivirus or other antivirus software. It is up to you to decide whether to keep the preinstalled antivirus software or switch to McAfee. It does not matter which antivirus software you use just as long as you have one and keep it updated.

Note: the PDC computers on the current contract come with a 90-day evaluation copy of Norton Antivirus. If you decide to keep Norton Antivirus, you will be responsible for updating your DAT files and paying for a year's subscription of updates once the evaluation period is over.

## How does McAfee VirusScan Work?

McAfee VirusScan uses a two-pronged approach to protect against viruses – 1) an on-access virus scanner working in the background and 2) an on-demand scanner.

**Vshield Scanner** is the component that provides background protection continuously watching for viruses as you work on your computer. It is loaded automatically when your computer is started up and stays in memory until you shut it or your system down. Viruses are detected when you attempt to access a file (read, copy, create, rename) on your hard drive or attempt to access your floppy diskette, zip disk, or CDROM.

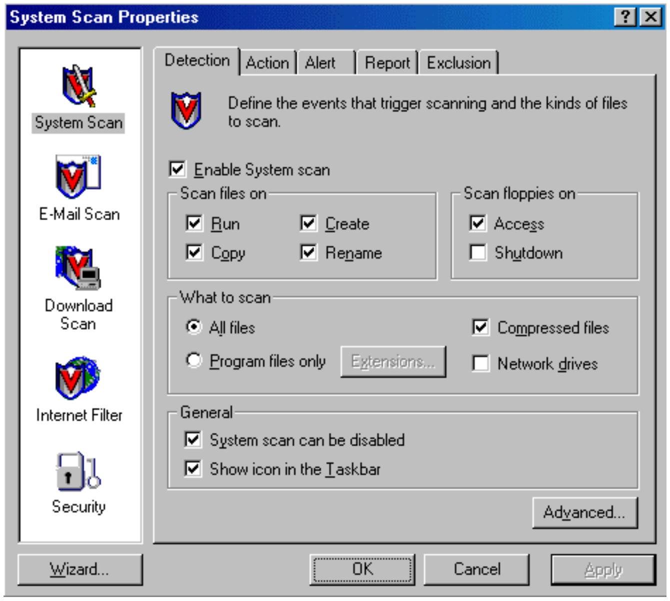
**VirusScan application** is the component that allows you to scan your system on demand or as scheduled in VirusScan Console. VirusScan application should be configured to scan all files and be run initially when VirusScan is installed and once a week thereafter. (Note: if your computer is in a high-traffic environment such as computer labs, you should scan all files more frequently.)

There are five modules in Vshield: System Scan, E-mail Scan, Download Scan, Internet Filter and Security. E-mail Scan, Download Scan and Internet Filter are options available under the custom installation. You must enable E-mail Scan and Internet Filter before they will work. Download Scan must be enabled for E-mail Scan to scan Internet mail.

System Scan scans files when they are run, copied, created or renamed and when floppies are accessed. E-mail Scan works in conjunction with Download Scan to scan e-mail attachments and files while they are being downloaded. Internet Filter scans for potentially harmful Java applets and ActiveX controls and filters Internet sites by IP address and/or URL. The Security module allows you to password protect your scan settings.

## Changing System Scan Settings

1. Right click on the **Vshield icon** in the Windows system tray on the bottom right corner of your screen.
2. Click on **Properties.**
3. Click on **System Scan**.
4. Click on the **Detection** tab.
5. We recommend that you use the scan all files option to prevent virus attacks (default is "program files only"). Click on the **All files** radio button.
   This option may slow down the performance of your computer. If you are not happy with system performance when using the scan all files option, you can select scan program files only AND schedule an all files scan weekly. Use VirusScan Console to schedule your task (see page 6).
6. In the scan floppies on section, uncheck the box for **shutdown** because it has caused problems.



Define the events that trigger scanning and the kinds of files to scan.

☑ Enable System scan

Scan files on

☑ Run ☑ Create

☑ Copy ☑ Rename

Scan floppies on

☑ Access

□ Shutdown

What to scan

● All files ☑ Compressed files

○ Program files only □ Network drives

General

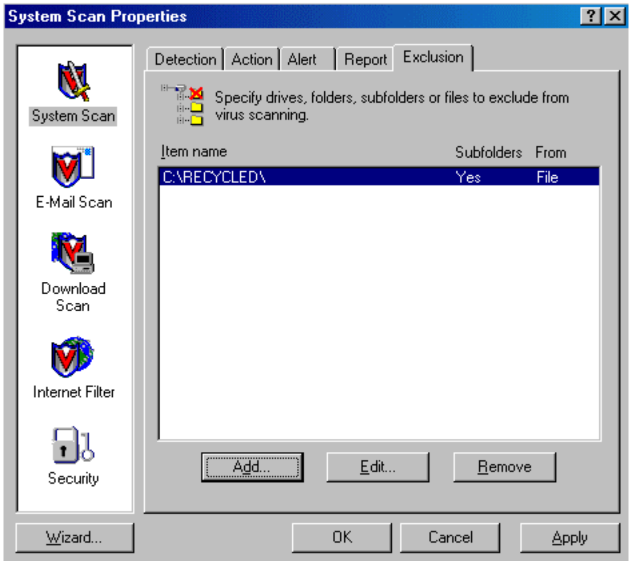
☑ System scan can be disabled

☑ Show icon in the Taskbar

We recommend removing Recycle Bin from the Exclusion tab. The SirCam virus (discovered July 17, 2001) created copies of itself and moved them to the Recycle Bin. The Recycle Bin is normally not scanned for viruses by default since programs stored in the Recycle Bin can not be run.

To remove the Recycle Bin scanning exclusion, in System Scan Properties:

1. Click on the **Exclusion** tab.
2. Highlight **C:\RECYCLED.**
3. Click on **Remove.**
4. Click on **Apply.**
5. Click on **OK**.



Specify drives, folders, subfolders or files to exclude from virus scanning.

| Item name | Subfolders | From |
|---|---|---|
| C:\RECYCLED\ | Yes | File |

## Changing E-mail Scan Settings

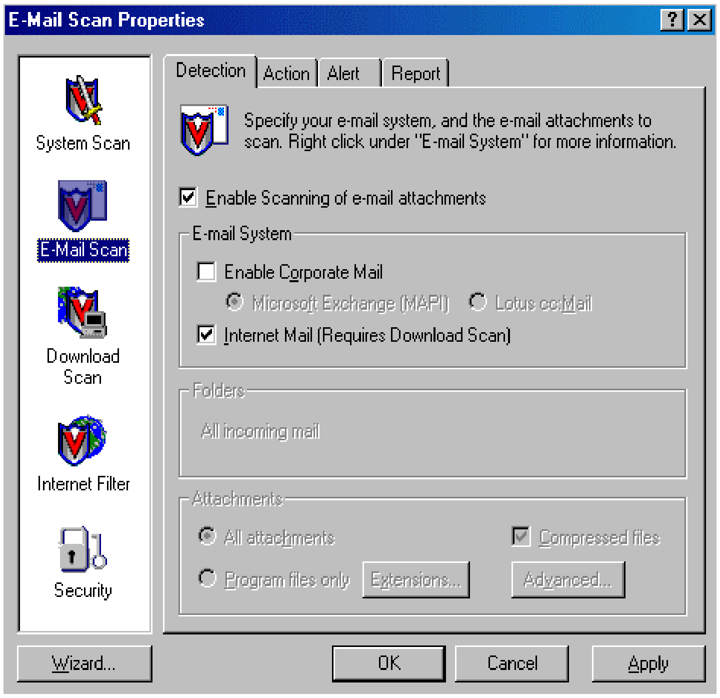
You must enable scanning of e-mail attachments; it is not enabled by default. This will allow you to scan e-mail attachments while you are downloading your message.

1. Right click on the Vshield icon in the Windows system tray.
2. Click on **Properties** and **E-mail Scan**.
3. In the Detection tab, check **Enable Scanning of e-mail attachments**.
4. Check **Internet Mail**.
5. Click on **Apply**.
6. Click on **OK**.

**Note on E-Mail System options**

Click on **Enable Corporate Mail** if you are using Microsoft Exchange, Microsoft Outlook or Lotus cc:Mail.

**Internet Mail** includes Outlook Express, Eudora and Netscape Mail.



Specify your e-mail system, and the e-mail attachments to scan. Right click under "E-mail System" for more information.

☑ Enable Scanning of e-mail attachments

E-mail System

☐ Enable Corporate Mail

● Microsoft Exchange (MAPI) ○ Lotus cc:Mail

☑ Internet Mail (Requires Download Scan)

Folders

All incoming mail

Attachments

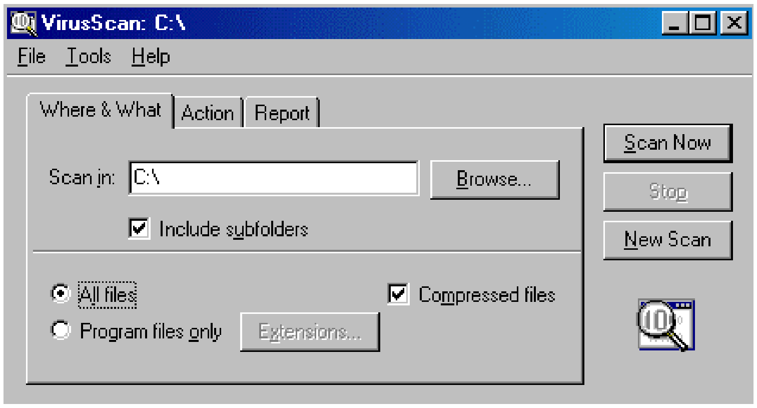
● All attachments ☑ Compressed files

○ Program files only

## How to Scan On-Demand

Use VirusScan application to scan your hard drive, floppy diskette or a selected folder before accessing the files on the media. VirusScan will scan the entire hard drive, floppy diskette or folder, not just one file. This should be done routinely once a week. If you have many files, the scanning process will take time. We recommend scanning your hard drive when you don't need to use the computer.

1. Close all applications.
2. Click on **Start → Programs → Network Associates → VirusScan**.
3. Select the drive or folder you wish to scan.
4. Select scan **all files.**
5. Click on **Scan Now**.



Scan in: C:\

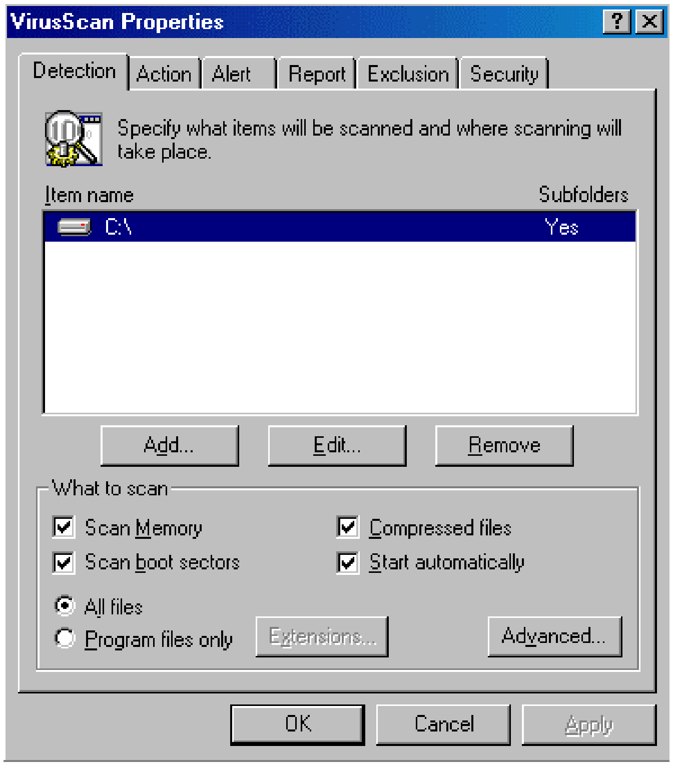
☑ Include subfolders

● All files ☑ Compressed files

○ Program files only

To automate this task, use VirusScan Console to configure your scan job. The following are instructions for configuring the task of automatically scanning your c: drive on a weekly basis.

1. Click on **Start → Programs → Network Associates → VirusScan Console**.
2. Highlight **Scan Drive 'C'.**
3. Click on **Properties**.
4. In the Program tab, click on **Configure**.
5. On the Detection tab, make sure that scan **all files** is selected.
6. On the Exclusion tab, highlight **\Recycled\.**
7. Click on **Remove**.
8. Click on **Apply** and **OK**.
9. On the Schedule tab, click on **Enable**.
10. Click on run **weekly**.
11. Select a time in 24-hour time (e.g. 14:00 is 2:00 p.m.) and a day of the week when you want to run the scan. Pick a day and time when your computer will be on and VirusScan Console is running.
12. Click on **Apply** and **OK**.
13. Close VirusScan Console.



Specify what items will be scanned and where scanning will take place.

| Item name | Subfolders |
|---|---|
| C:\ | Yes |

What to scan

☑ Scan Memory ☑ Compressed files

☑ Scan boot sectors ☑ Start automatically

● All files

○ Program files only

## Keep SDAT/DAT Files Current

There are 200 to 300 new viruses introduced every month. The antivirus software will not protect you against these new threats unless you update your virus definition data (DAT) files and scan engine. The antivirus software uses the DAT file to scan for virus signatures (code identifying the virus).

In order to maintain the best detection and cleaning capability, the DAT files and scan engine must be current. It is important to keep the scan engine current to the level required for using the most current DAT file. Sometimes when you have the latest DAT file with an older scan engine, new viruses are not detected or cleaned properly.

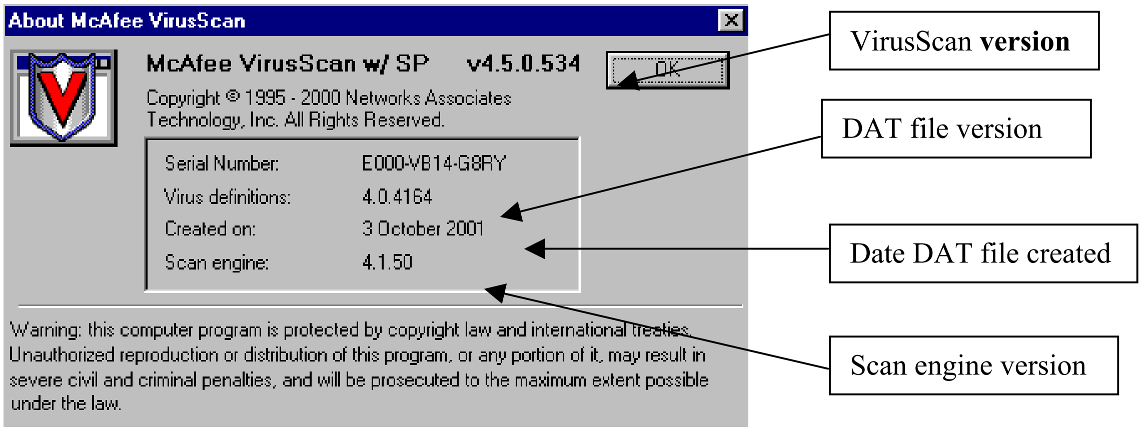
Upgrade refers to the upgrading of the scan engine, which is the part of the antivirus software that detects and cleans virus infections. As new viruses appear and existing viruses evolve, the scan engine needs to be upgraded with new functionality. Update refers to the updating of the virus definition files.

The SuperDAT (SDAT) installer utility automatically loads updated virus definitions and scan engine. SDAT version xxxx contains the virus definition version xxxx with the scan engine associated with that virus definition. For example, SDAT 4164 contains the DAT 4164 and scan engine 4150.

ITS recommends that you update your SDAT files **weekly** to keep it current by using the autoupgrade task in VirusScan Console. NAI normally updates the SDAT/DAT files weekly on Wednesday mornings (HST time). The DAT files are updated more frequently during a high alert virus outbreak. For example, NAI released 4 DAT files within 3 days during the Nimda virus outbreak in Sept. 2001.

## What Version of McAfee am I Running?

To find out what version DAT file and scan engine you are running, right click on the **Vshield icon** in the Windows system tray and click on **About**.



About McAfee VirusScan

McAfee VirusScan w/ SP v4.5.0.534

Copyright © 1995 - 2000 Networks Associates Technology, Inc. All Rights Reserved.

|  |  |
|---|---|
| Serial Number: | E000-VB14-G8RY |
| Virus definitions: | 4.0.4164 |
| Created on: | 3 October 2001 |
| Scan engine: | 4.1.50 |

Warning: this computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

VirusScan **version**

DAT file version

Date DAT file created

Scan engine version

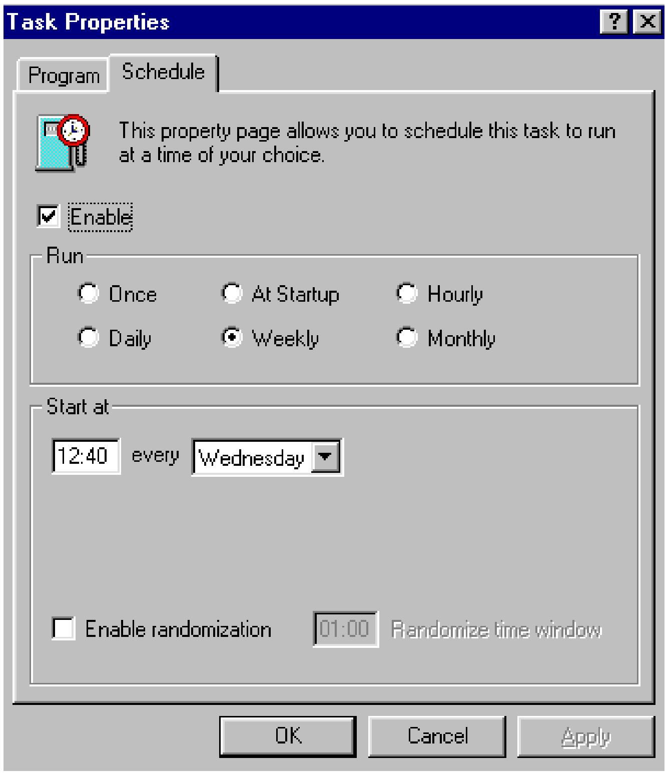
I am running McAfee VirusScan v4.5.0 with SP1 using DAT file 4164 created on October 3, 2001 using scan engine version 4150.

## Configuring AutoUpgrade

To automatically upgrade your scan engine and DAT file, configure the autoupgrade task:

1. Click on **Start → Programs → Network Associates → VirusScan Console**.
2. Click on **AutoUpgrade** then **Properties**.
3. In the Task Properties window, click on the **Schedule** tab.
4. Check **Enable**.
5. Select run **weekly**.
6. Enter the time in 24-hour time (i.e. 1300 is 1:00 p.m.) when you want the task to start.
7. Select a day from the pull-down menu.

   Select a day and time when your computer will be on. Your computer **must be on** and VirusScan Console must be running for the autoupgrade task to start. If your computer is off at the scheduled time, the upgrade will be performed at the next scheduled time.



This property page allows you to schedule this task to run at a time of your choice.

☑ Enable

Run

○ Once ○ At Startup ○ Hourly

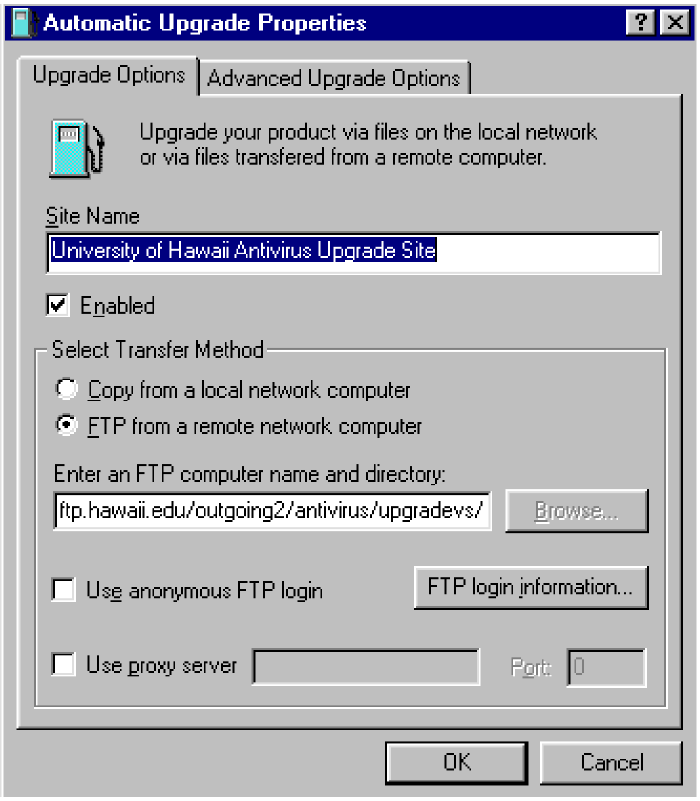
○ Daily ● Weekly ○ Monthly

Start at

12:40 every Wednesday

□ Enable randomization 01:00 Randomize time window

8. Click on the Program tab then **Configure**.
9. In the Upgrade Sites tab, click on **Add**.
10. In the Upgrade Options tab, enter the following information.
11. Site Name: **University of Hawaii Antivirus Upgrade Site**
12. Enter an FTP computer name and directory - **ftp.hawaii.edu/outgoing2/antivirus/**upgradevs/.



Upgrade your product via files on the local network or via files transfered from a remote computer.

Site Name: University of Hawaii Antivirus Upgrade Site

☑ Enabled

Select Transfer Method

○ Copy from a local network computer

● FTP from a remote network computer

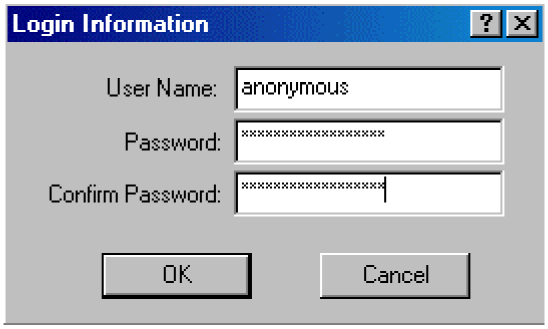
Enter an FTP computer name and directory: ftp.hawaii.edu/outgoing2/antivirus/upgradevs/

□ Use anonymous FTP login

□ Use proxy server

Port: 0

13. Clear **Use anonymous FTP login** and click on **FTP login information**.
14. For User Name, type in **anonymous**.
15. For Password, type in your ITS username (e.g. user@hawaii.edu) which will appear as asterisks.
16. For Confirm Password, type in your ITS username again.
17. Click on **OK** in the login information window.
18. Click on **OK** in the automatic upgrade properties window.
19. Click on **Apply** and **OK**.
20. Close VirusScan Console.



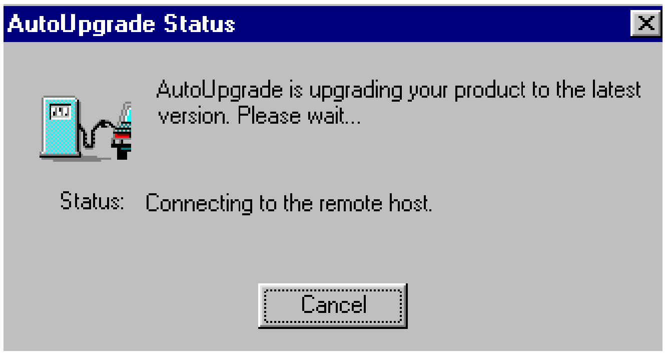
User Name: anonymous

Password: ******************

Confirm Password: ******************

## How to Upgrade Your SDAT Manually

There are two ways to manually upgrade your SDAT. The easier way is to use the autoupgrade task. If your autoupgrade task has been configured as in the previous section, right-click on the VirusScan Console icon in the system tray and select **Restore**. Highlight the **Autoupgrade** task, click on **Properties**, and click on **Run Now**.


AutoUpgrade Status

AutoUpgrade is upgrading your product to the latest version. Please wait...

Status: Connecting to the remote host.

McAfee will disable VirusScan, connect to the ftp site, download the upgrade components, run the SDAT upgrade, and enable VirusScan. Sometimes this will fail if McAfee is unable to login to the ftp site. You should try again later as the ftp site may be busy.

The second way to upgrade your SDAT is to open your web browser to http://www.hawaii.edu/downloads/mcafee/sdat.html. Click on the download SuperDAT link and save the file to your Windows desktop. Double-click on the SDAT icon to run it.

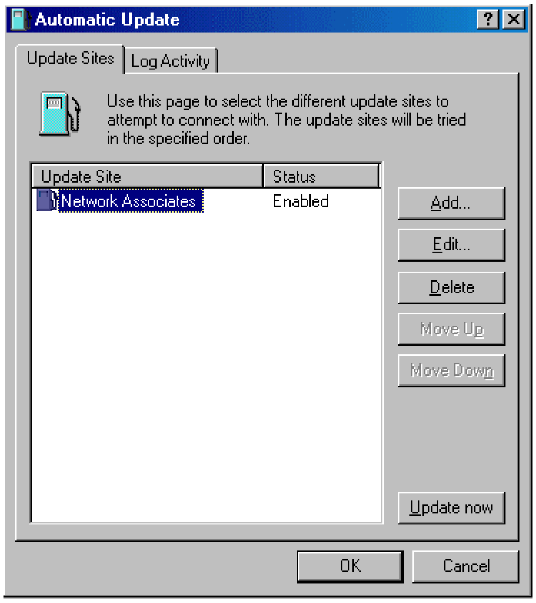
sdat_latest.exe

## Configuring AutoUpdate

The autoupdate task is configured with the default Network Associates (NAI) ftp location, ftp.nai.com/pub/antivirus/datfiles/4.x, for DAT updates when you first install VirusScan. You may also use the UH antivirus update site, ftp.hawaii.edu/outgoing2/antivirus/update/ that may be more accessible during times of high virus alerts.

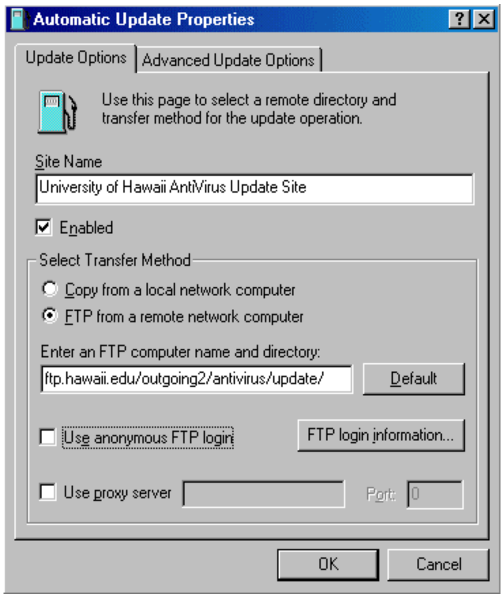
To change from the default NAI site to the UH antivirus update site:

1. Go to **Start → Programs → Network Associates → VirusScan Console**.
2. Click on **AutoUpdate** and **Configure**.
3. In the Update Sites tab, highlight **Network Associates** and click on **Delete**.
4. Click on **Add**.


Automatic Update

Use this page to select the different update sites to attempt to connect with. The update sites will be tried in the specified order.

| Update Site | Status |
|---|---|
| Network Associates | Enabled |


Automatic Update Properties

Use this page to select a remote directory and transfer method for the update operation.

Site Name: University of Hawaii AntiVirus Update Site

☑ Enabled

Select Transfer Method

○ Copy from a local network computer

● FTP from a remote network computer

Enter an FTP computer name and directory: ftp.hawaii.edu/outgoing2/antivirus/update/

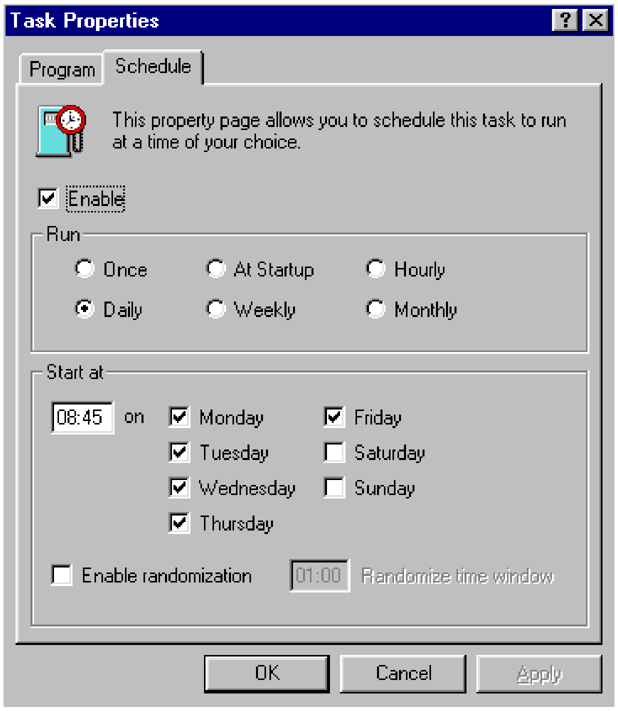
☐ Use anonymous FTP login

☐ Use proxy server

Port: 0

5. In the Update Options tab, enter the following information.
6. Site Name: **University of Hawaii Antivirus Update Site**
7. Enter an FTP computer name and directory - **ftp.hawaii.edu/outgoing2/antivirus/update/.**
8. Clear **Use anonymous FTP login** and click on **FTP login information**.
9. For User Name, type in **anonymous**.
10. For Password, type in your ITS username (e.g. user@hawaii.edu) which will appear as asterisks.
11. For Confirm Password, type in your ITS username again.
12. Click on **OK** in the login information window.
13. Click on **OK** in the automatic update properties window.

14. Click on the Schedule tab.
15. Check **Enable**.
16. Select **Daily** (or Weekly at minimum).
17. Select the days and times you want to run autoupdate. Enter times in 24-hour time, e.g. 16:30 is 4:30 pm. Remember that your computer must be powered on. Autoupdate takes a few minutes.
18. Click on **Apply** and **OK**.
19. Close VirusScan Console.



This property page allows you to schedule this task to run at a time of your choice.

☑ Enable

Run

○ Once ○ At Startup ○ Hourly
● Daily ○ Weekly ○ Monthly

Start at

08:45 on ☑ Monday ☑ Friday
☑ Tuesday ☐ Saturday
☑ Wednesday ☐ Sunday
☑ Thursday

☐ Enable randomization 01:00 Randomize time window

See the "Configuring AutoUpgrade and AutoUpdate" section in ITS document WIN9X010, *Installing McAfee VirusScan v4.5,* for details. Do not schedule autoupgrade and autoupdate for the same day and time.

## In Case of a High Virus Alert

In the event of a fast-breaking high alert virus, NAI usually makes available an EXTRA.DAT virus definition file that will detect the new virus. ITS will make the EXTRA.DAT file available on its antivirus web page (www.hawaii.edu/sitelic/antivirus) for download customized for the UH community.

Note: to receive e-mail notification of high or medium virus alerts, subscribe to the list uhvirus-alert. (Virus risk levels are determined by NAI.) To subscribe, send e-mail to listproc@hawaii.edu with the following in the message body:

Subscribe uhvirus-alert <first name> <last name>

You may also subscribe on-line at www.hawaii.edu/virus.

The EXTRA.DAT file must be copied in the folder where the DAT files are installed. The default location is the C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.XX folder.

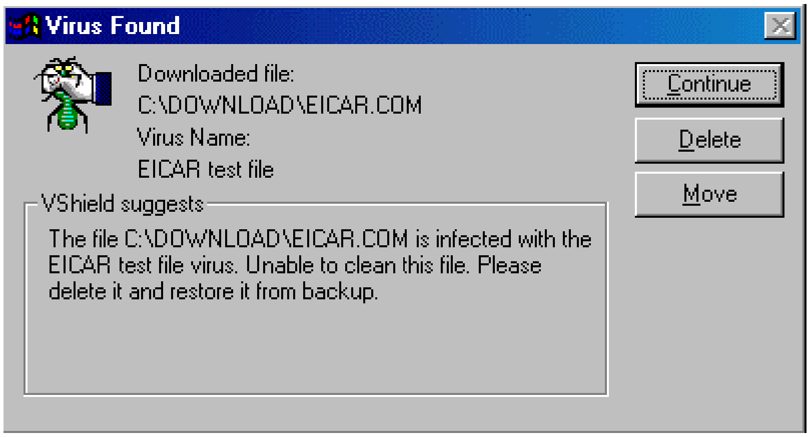
## Installing the EXTRA.DAT File

1. Go to the ITS antivirus web page, www.hawaii.edu/sitelic/antivirus/instructextra.html.
2. Download the EXTRA.DAT file to your Windows desktop or in a temporary folder. (The EXTRA.DAT file will be saved with a filename of the following format: extrammddyy.exe where mmddyy is the month, day and year of the EXTRA.DAT file, e.g. extra052700.exe).
3. Close your web browser (i.e. Netscape or Internet Explorer).
4. Double click on the filename or icon for extra052700.exe in our example.
5. The file is programmed to place the EXTRA.DAT file into the default VirusScan folder mentioned above.
6. If you installed VirusScan in a different folder, extract EXTRA.DAT onto the Windows Desktop by typing in C:\Windows\Desktop instead of C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.XX then copy the file to the appropriate folder.

## I Found a Virus, Now What?

When Vshield detects a virus, you will receive a warning similar to the following:

You will be prompted with several options, which depend on the Vshield component that detected the virus. In this example, Download Scan detected the Eicar test virus. Your options are to continue scanning, delete the file or move the file to a quarantine folder. Vshield also suggests what you should do with the infected file.



Downloaded file:
C:\DOWNLOAD\EICAR.COM
Virus Name:
EICAR test file

VShield suggests

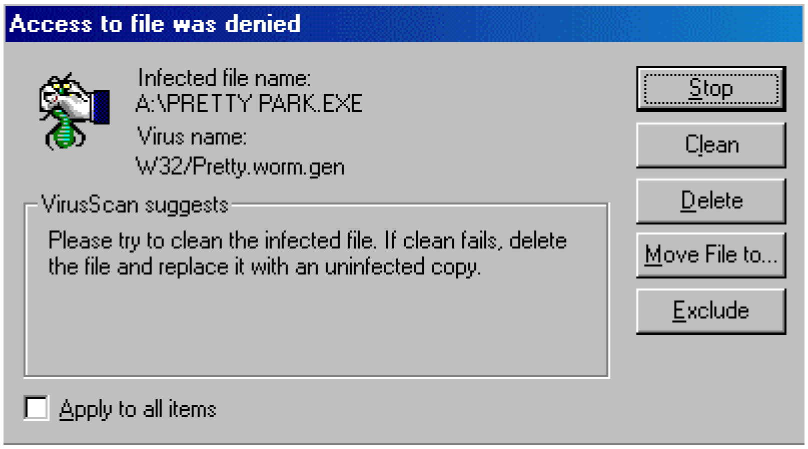
The file C:\DOWNLOAD\EICAR.COM is infected with the EICAR test file virus. Unable to clean this file. Please delete it and restore it from backup.

**Please write down the name of the virus and the infected file for reference.**

If you select to move the file, the infected file is copied to the C:\INFECTED folder and renamed to *original-filename.vir* (e.g. eicar.com.vir). In most cases, you should choose to delete the infected file.

Here is another example of a virus detection, this time by the System Scan module when the user attempted to open the infected file, Pretty Park.exe, on a floppy diskette.

Click on **Clean** to disinfect the virus. VirusScan will tell you whether it was successful in removing the virus.



Access to file was denied

Infected file name:
A:\PRETTY PARK.EXE

Virus name:
W32/Pretty.worm.gen

VirusScan suggests

Please try to clean the infected file. If clean fails, delete the file and replace it with an uninfected copy.

□ Apply to all items

Some viruses (usually boot sector viruses) can not be cleaned while running Windows. You will need to use the McAfee Emergency Disk to clean boot sector viruses in DOS. (See section below on “Using McAfee Emergency Disk”.)

Sometimes when the virus is newly introduced, VirusScan may only be able to detect the virus but may not be able to clean it. In those cases, you should delete the infected file and restore the original file from a clean (pre-infected) backup.

Once the virus is disinfected, a report will be given depending on the status of the virus and whether the virus could be cleaned, deleted or renamed. The log file is saved in c:\Program Files\Network Associates\VirusScan\VSHLog.txt.

Once you have disinfected the virus (or deleted the infected file and restored it from backup), rerun VirusScan scanning with the all files option once more just to be safe.

You should track down the source of your virus infection and notify the appropriate people involved who may have given you the virus and those to whom you may have spread the virus (if not detected in time). For example, if VirusScan detected a virus in your e-mail attachment, notify the persons to whom you may have inadvertently forwarded the infected attachment and the person who sent you the attachment.

**If you detect a virus and need assistance cleaning it, please contact the ITS Help Desk at 956-8883 with the name of the virus, your version of VirusScan, the date of your virus definition, and the version of your scan engine.**

## Using McAfee Emergency Disk

The McAfee Emergency Disk will only detect boot sector and file-infecting viruses. ITS creates a McAfee Emergency Disk with DAT file updates for these viruses on a monthly basis. You can obtain an updated McAfee Emergency Disk at the ITS Help Desk in Keller 105. You can create an Emergency Disk using VirusScan (**Start → Program Files → Network Associates → Create Emergency Disk**) but it will not have the updated virus definitions.)

1. Make sure the McAfee Emergency Disk is write-protected (slide the write-protect tab so a hole appears near the corner of the diskette)
2. Shut down Windows. Click on **Start → Shut Down → Shut Down**.
3. Power off your computer.
4. Insert the McAfee Emergency Disk into the floppy drive (a:).
5. Power on your computer. (Note: cycling the power on your computer is known as a **cold boot**, which will clear any memory resident viruses.)
6. Use the arrow keys to highlight **Next** and press **Enter**. If you don't have McAfee VirusScan installed on your computer, you must use the DAT files on the Emergency Disk (default location) and skip to step 10. To use the DAT files on your hard drive, go to step 7.
7. Use the arrow keys to highlight **Location** and press **Enter**.
8. In the location box, type in "c:\progra~1\common~1\networ~1\viruss~1\40~1.xx" (without the quotes). Press the arrow keys to highlight **OK** and press **Enter**.
9. The "Use DAT files from" box will be filled in with the location you just entered.
10. Use the arrow keys to highlight **Next** and press **Enter**.
11. Use the arrow keys to highlight **Finish** and press **Enter**.
12. The program will begin scanning and cleaning your system using the DAT files on your hard drive or on the Emergency Disk if you selected this option. It may take several passes to complete. Each pass may take several minutes or a couple of hours. When the scan is finished, you will see a report and the a:> prompt. Power off your computer, remove the McAfee Emergency Disk from the floppy drive and power on your computer.

## Performance Issues

As on-access virus scanning becomes more complex and requires more system resources, you may notice degradation in system performance. This was especially noticeable after DAT 4163 was released. Do NOT disable your anti-virus software! This is a tremendous security risk. Here are recommendations on configuring McAfee to improve your system performance:

1. Scan program files only instead of scanning all files and change the program file extensions list to include the following

   ?? 00? 386 A?? BA? BIN BZ CBT CDR CHM CLA CMD CNV COM CP? CRT CSC CX D?B DEV DLL DO? DRV DVB DWG EML EXE GMS HLP HT? INF INP ISP JS? L? LNK MD? MP? MS? NWS O?? PCD PIF POT PP? PS PWZ Q?? REG RTF SH? S?S SC? SMM TLB TM TX? URL V?? VB? W?? X??

   Right-click on VirusScan Console icon in the system tray and select **Restore**. Highlight **Vshield** and click on **Properties** then **Configure**. On the Detection tab, select **Program Files Only**.

Click on the **Extensions** button. Click on **Add**. Type in one of the file extensions (maximum 3 characters) listed above then **OK**. Repeat the process until all the file extensions are added. Click **OK** when done. Click on **Apply** and **OK**.

2. In addition to step 1, configure Download Scan and E-mail Scan to scan for all files and all attachments. Scan all files on your hard drives at least once a week.

## For More Information

For help on installing or using McAfee VirusScan, to report a virus or to request help cleaning up after a virus infection, call the ITS Help Desk at 956-8883, visit the Help Desk at Keller 105 or send e-mail to help@hawaii.edu.

For information about a specific virus, go to URL vil.nai.com/villib/alpha.asp and specify the virus name in the search box.

For VirusScan FAQs on update, install/uninstall, general and virus infection issues, go to URL www.mcafeehelp.com/main.asp?docName=VSFAQList.

McAfee VirusScan *Getting Started* and *User's Guide* manuals are available in PDF format at www.nai.com/asp_set/services/technical_support/docs.asp?pCode=VSCMP.

For additional assistance, please phone the ITS Help Desk at (808) 956-8883,
send email to **help@hawaii.edu**, or fax (808) 956-2108.
The Help Desk's toll-free phone number is (800) 558-2669.

Or see the ITS Help Desk home page at **www.hawaii.edu/help**
The ITS walk-in Help Desk is located in
Keller 105 and Keller 213 on the UH Mānoa Campus.