WIN9X013 August 2003

Using McAfee VirusScan v4.5.1 with SP1

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. Sobig.f virus), Internet downloads, shared files on network connections, and browsing infected web pages. 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 antivirus software installed, and keep the antivirus software current.

Information Technology Services (ITS) has purchased a number of licenses of McAfee VirusScan anti-virus software that active University of Hawaiʻi (UH) faculty, staff and students can use at no extra charge on their Windows computers. UH faculty and staff may use one copy of McAfee VirusScan Enterprise (VSE) or one copy of McAfee VirusScan v4.5.1 with service pack 1 (SP1) for their office computer or for computer labs on campus with a UH decal number. Active UH faculty, staff and students include any student taking a UH credit course and any faculty/staff currently employed by UH.

Copies of the older site license version of McAfee VirusScan 4.x must be uninstalled from UH computers by October 1, 2003 (exceptions are Windows 98 and Windows ME computers with a UH decal number).

UH faculty, staff and students (upon termination or graduation from UH) must uninstall their copy of McAfee VirusScan 4.x and 7.x.

ITS provides in-depth technical support for McAfee VirusScan and limited support for other anti-virus products. Make sure that you have only one anti-virus product installed, that your virus definitions (DAT files) are kept current and your anti-virus software is configured properly.

This document provides information to help you become “virus-aware” and covers the basics of installing, configuring and using McAfee VirusScan v4.5.1 with service pack 1 (SP1) on the Windows 98 and Windows ME platform at the University of Hawaii. It assumes that you have already installed McAfee VirusScan, which is the antivirus software currently supported by Information Technology Services (ITS). See Appendix A for instructions on installing McAfee VirusScan v4.5.1 with SP1.

Note: McAfee VirusScan v4.5.1 with SP1 must be installed on Windows 98 and Windows ME computers on campus with a UH decal number.

For campus computers running Windows NT, Windows 2000 or Windows XP, please install McAfee VirusScan Enterprise 7.0. For home computers running Windows 98, Windows ME, Windows 2000 Pro, Windows XP Home or Windows XP Pro, please install McAfee VirusScan Home Edition 7.0. VirusScan 7 software is available for download at http://www.hawaii.edu/antivirus.

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". An example is the Stoned boot sector virus which displays a message "Your computer is now stoned"on the infected computer.

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 Pretty Park, Klez and Blaster 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.

Blended threats are the newest type of malware, combining characteristics of viruses, worms, Trojan horses, and malicious code taking advantage of server and Internet vulnerabilities to initiate, transmit, and spread an attack. The Nimda worm wrecked havoc in September 2001, crippling large sections of the Internet. It spread rapidly in multiple ways: by opening an infected e-mail attachment, by browsing infected web sites with an unpatched web browser, and by infecting files on open network shares without password protection.

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, Trojan horses or blended threats.**

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 a 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. If your hard drive gets reformatted, you could lose 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.

Newer methods of spreading computer viruses include infecting files on open (not password protected) network shares. Computer viruses can also spread via peer-to-peer filesharing networks such as Kazaa and through instant messaging channels. Accessing web sites that entice users to download infected files (screen savers, games, pictures, etc), run malicious scripts without the user's knowledge or exploit vulnerabilities in web browsers and email clients are other ways that viruses spread.

Popular computer products are often the favorite targets of virus writers. Examples are the Windows operating system (any version of Windows may be affected), Microsoft Office (Word, Excel, PowerPoint, Access), Outlook, Outlook Express and Internet Explorer. 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. (*There is a known MIME header vulnerability that allows an unpatched version of Outlook and Outlook Express to automatically open an attachment in preview mode. You should install the latest security patches for Windows by going to http://windowsupdate.microsoft.com)

Unfortunately, we can not predict how the next virus attack will occur.

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 and install McAfee VirusScan or another antivirus software of your choice.**

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 Dell computers on the WSCA contract may be purchased with 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 initial subscription 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 unload it or shut 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 or attempt to download files from the Internet or via email.

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 your hard drive for viruses 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 installed under the typical installation option. However, E-mail Scan, Download Scan, and Internet Filter modules are not enabled by default. You **must enable** E-mail Scan, Download Scan and Internet Filter before they will work. Download Scan must be enabled for E-mail Scan to scan Internet mail.

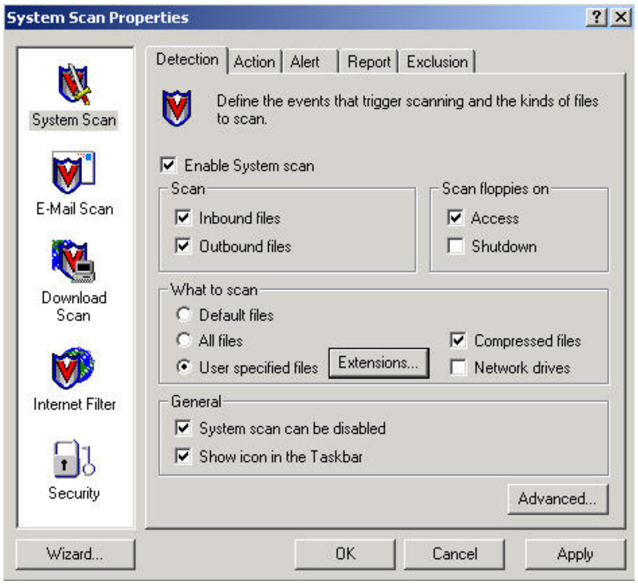
System Scan scans files when they are run, copied, created or renamed and when floppies are accessed. E-mail Scan works in conjunction with Download Scan to scan e-mail attachments and files while they are being downloaded. Internet Filter scans for potentially harmful Java applets and ActiveX controls 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 user specified files option to prevent virus attacks (default is "default files"). Click on the **User specified files** radio button. Click on the **Extensions** button and add the **TX?** extension.

   Make sure you schedule a weekly scan all files task. Use VirusScan Console to schedule your task (see "How to Scan Your Hard Drives Automatically").

6. In the scan floppies on section, uncheck the box for **shutdown** because it has caused problems.
7. Click **Apply** and **OK**.



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

☑ Enable System scan

Scan
☑ Inbound files
☑ Outbound files

Scan floppies on
☑ Access
☐ Shutdown

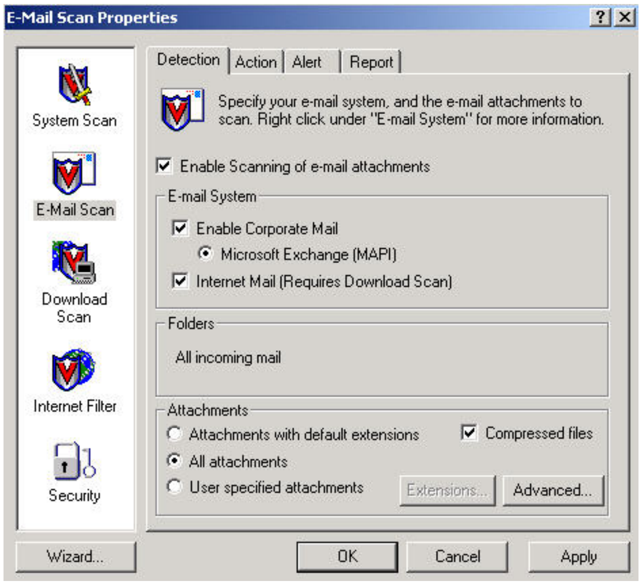
What to scan
○ Default files
○ All files
● User specified files
☑ Compressed files
☐ Network drives

General
☑ System scan can be disabled
☑ Show icon in the Taskbar

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 **Yes** when prompted to enable Download Scan.
6. Click on **Apply**.
7. Click on **OK**.



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)
☑ Internet Mail (Requires Download Scan)

Folders
All incoming mail

Attachments
○ Attachments with default extensions
● All attachments
○ User specified attachments
☑ Compressed files

Note on E-Mail System options

Click on **Enable Corporate Mail** if you are using Microsoft Exchange.

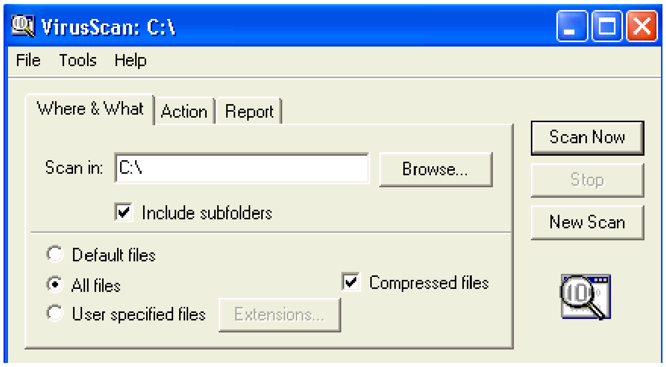
If you check **Enable Corporate Mail**, make sure to select **all attachments** under the Attachments section.

Internet Mail includes Outlook Express, Eudora, Netscape Mail and other POP3 e-mail clients.

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 some 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

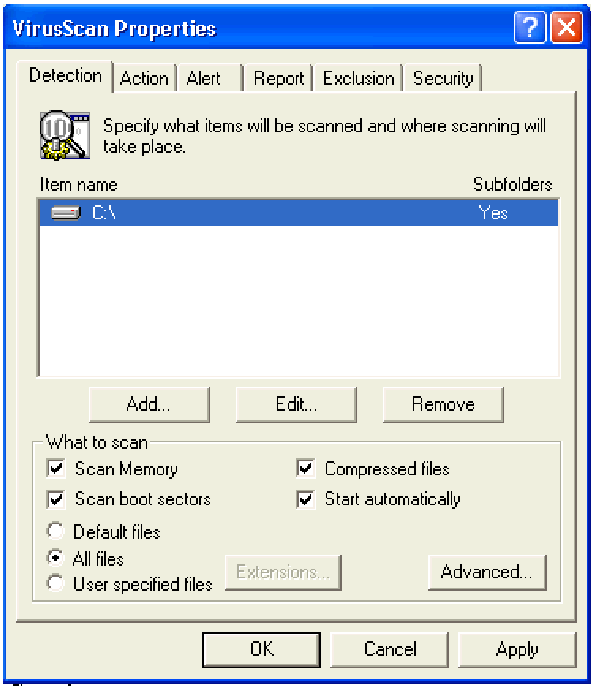
○ Default files
● All files
○ User specified files

☑ Compressed files

How to Scan Your Hard Drives Automatically

To automate this task, use VirusScan Console to create a new task to scan your hard drives. The following instructions are for configuring the task of automatically scanning your hard drives on a weekly basis.

1. Click on **Start → Programs → Network Associates → VirusScan Console**.
2. Click on the **New Task** button.
3. Enter **scan hard drives** in the description box.
4. In the Program tab, click on **Configure**.
5. On the Detection tab, make sure that scan **all files** is selected.
6. Highlight **"C:\"** under item name and click on **Remove**.
7. Click on **Add**.



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

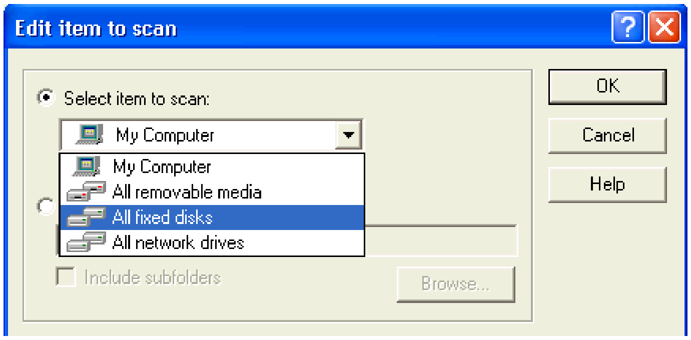
Item name	Subfolders
C:\	Yes

What to scan

☑ Scan Memory
☑ Scan boot sectors
☑ Compressed files
☑ Start automatically

○ Default files
● All files
○ User specified files

8. Select **All fixed disks**. Click **OK**.
9. On the Exclusion tab, highlight **\Recycled\.**
10. Click on **Remove**.
11. On the Schedule tab, click on **Enable**.
12. Click on run **weekly**.
13. 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 powered on and VirusScan Console is running.
14. Click on **Apply** and **OK**.
15. Close VirusScan Console.



Keep SDAT/DAT Files Current

There are over 300 new viruses introduced every month. The antivirus software will not protect your computer against these new threats unless you update your virus definition data (DAT) files and scan engine routinely. 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.

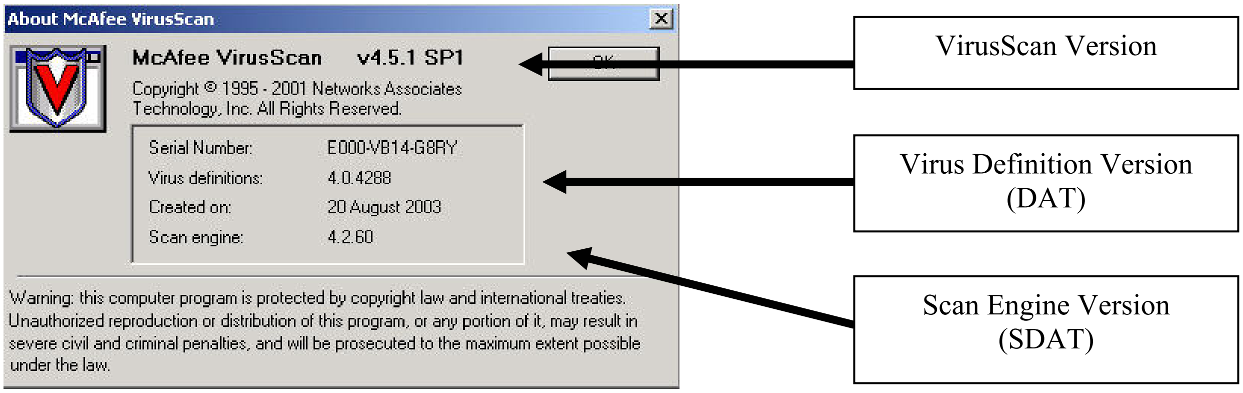
The SuperDAT (SDAT) installer utility automatically loads updated virus definitions and scan engine files. SDAT version xxxx contains the virus definition version xxxx with the scan engine associated with that virus definition. For example, SDAT 4243 contains the DAT 4243 and scan engine 4160. The DAT update only updates the virus definition, not the scan engine.

ITS recommends that you schedule the autoupgrade task in VirusScan Console to update your SDAT files once or twice a week. Select **daily** and any two days of the week, preferably one day at the beginning of the week and another day near the end of the week. The autoupdate task should be scheduled to run **daily** except on the days that autoupgrade is scheduled. This recommended schedule allows you to have the most current scan engine and virus definition file or the most current files within a day.

NAI normally updates the SDAT/DAT files weekly on Wednesday mornings (HST). The DAT files are updated more frequently during a high alert virus outbreak. For example, NAI released four DAT files within three 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 v4.5.1 SP1

Copyright © 1995 - 2001 Networks Associates Technology, Inc. All Rights Reserved.

Serial Number: E000-VB14-G8RY
Virus definitions: 4.0.4288
Created on: 20 August 2003
Scan engine: 4.2.60

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

Virus Definition Version (DAT)

Scan Engine Version (SDAT)

In this example, you are running McAfee VirusScan v4.5.1 with SP1 (service pack 1) using DAT file 4288 created on August 20, 2003 using scan engine version 4260.

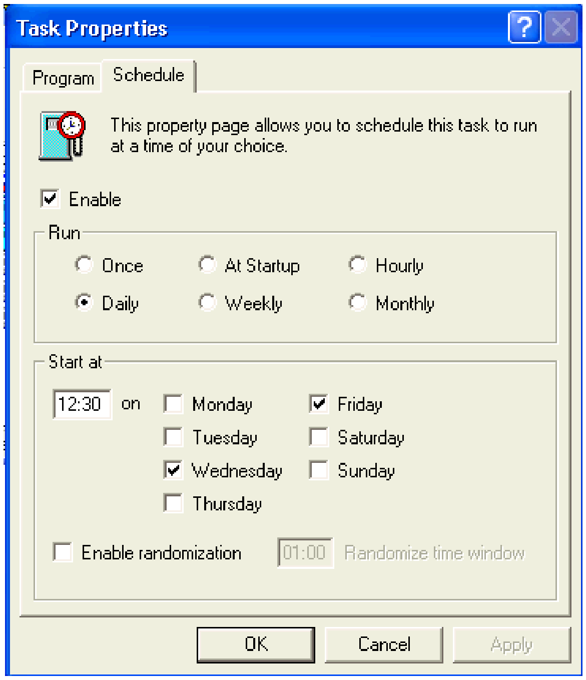
You will need to provide this information when you call the ITS Help Desk for assistance with McAfee VirusScan.

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 **daily**.
6. Enter the time in 24-hour time (i.e. 1300 is 1:00 p.m.) when you want the task to start.
7. Check the days to run the task.

   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.



Task Properties

Program | Schedule

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

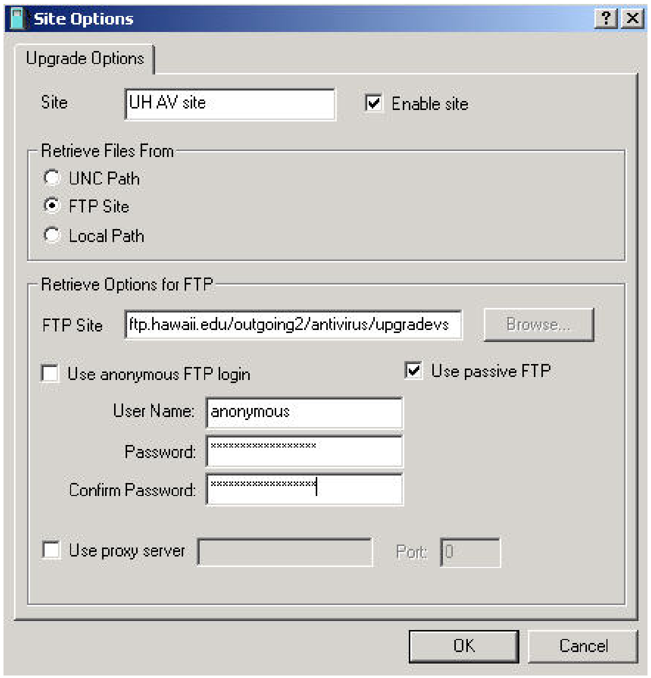
12:30 on

□ Monday ☑ Friday
□ Tuesday □ Saturday
☑ Wednesday □ Sunday
□ Thursday

□ Enable randomization 01:00 Randomize time window

OK Cancel Apply

8. Click on the Program tab then **Configure**.
9. In the Upgrade Sites tab, click on **Add**.
10. In the Site Options tab, enter the following information.
11. Site Name: **UH AV Site**
12. FTP Site: **ftp.hawaii.edu/outgoing2/antivirus/upgradevs/**
13. Clear **Use anonymous FTP login**.
14. For User Name, type in **anonymous**.
15. For Password, type in your UH username (e.g. user@hawaii.edu) which will appear as asterisks.
16. For Confirm Password, type in your UH 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.



Site Options

Upgrade Options

Site UH AV site ☑ Enable site

Retrieve Files From

○ UNC Path
● FTP Site
○ Local Path

Retrieve Options for FTP

FTP Site ftp.hawaii.edu/outgoing2/antivirus/upgradevs Browse...

□ Use anonymous FTP login ☑ Use passive FTP

User Name: anonymous

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

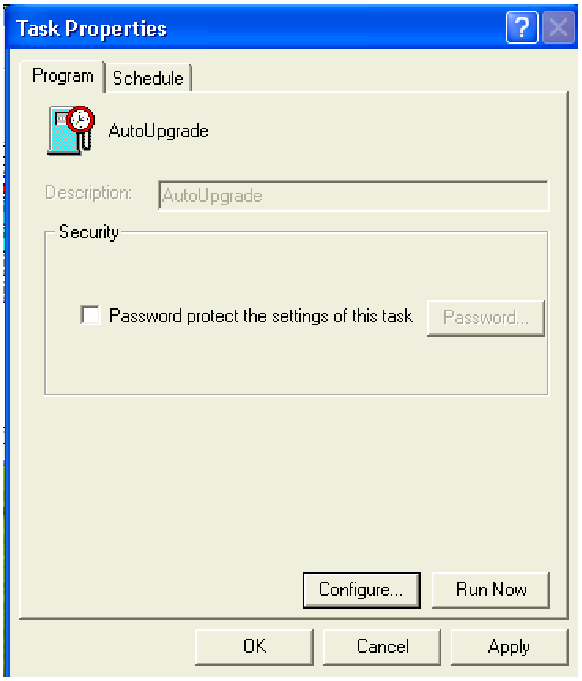
Confirm Password: ****************

□ Use proxy server Port: 0

OK Cancel

How to Upgrade Your SDAT Manually

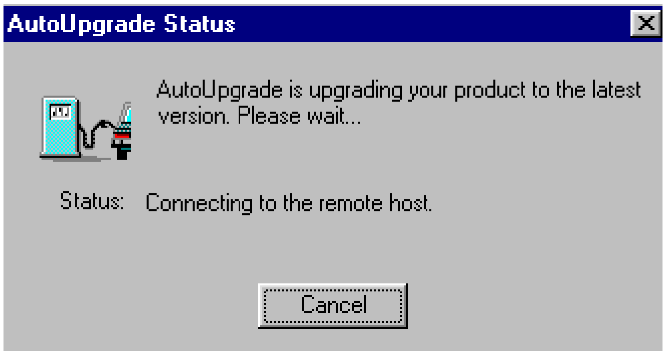
There are two ways to manually upgrade your SDAT. The easier way is to use the autoupgrade task. If your autoupgrade task has been configured as in the previous section, right-click on the VirusScan Console icon in the system tray and select **Restore**. Highlight the **Autoupgrade** task, click on **Properties**,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



Description: AutoUpgrade

□ Password protect the settings of this task

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.



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

Status: Connecting to the remote host.

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_latest icon to run it.

sdat_latest.exe

Configuring AutoUpdate

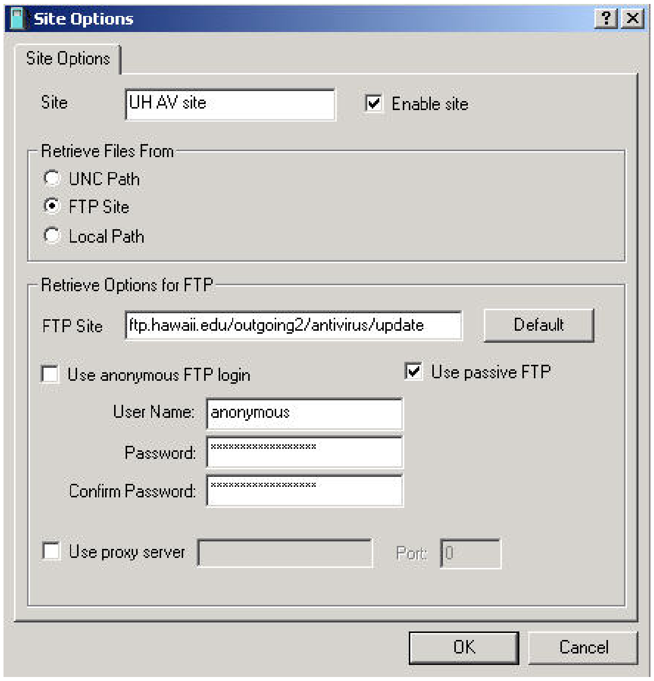
The autoupdate task is configured with the default Network Associates (NAI) ftp location, ftp.nai.com/pub/antivirus/datfiles/4.x, for DAT updates when you first install VirusScan. You should replace the NAI site with the UH antivirus update site, ftp.hawaii.edu/outgoing2/antivirus/update/ that may be 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 **Properties**.
3. Click on the **Configure** button.
4. Highlight **Network Associates** and click **Delete**.
5. Click on **Add**.

Under the **Site Options** tab, enter the following information.

6. Site: **UH AV Site**
7. FTP Site: **ftp.hawaii.edu/outgoing2/antivirus/update/**
8. Clear **Use anonymous FTP login**.
9. For User Name, type in **anonymous**.
10. For Password, type in your UH username (e.g. user@hawaii.edu) which will appear as asterisks.
11. For Confirm Password, type in your UH username again.
12. Click on **OK** in the Site Options window.
13. Click on **OK** in the autoupdate window.



Site Options

Site Options

Site: UH AV site ☑ Enable site

Retrieve Files From
○ UNC Path
● FTP Site
○ Local Path

Retrieve Options for FTP

FTP Site: ftp.hawaii.edu/outgoing2/antivirus/update

□ Use anonymous FTP login ☑ Use passive FTP

User Name: anonymous

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

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

□ Use proxy server Port: 0

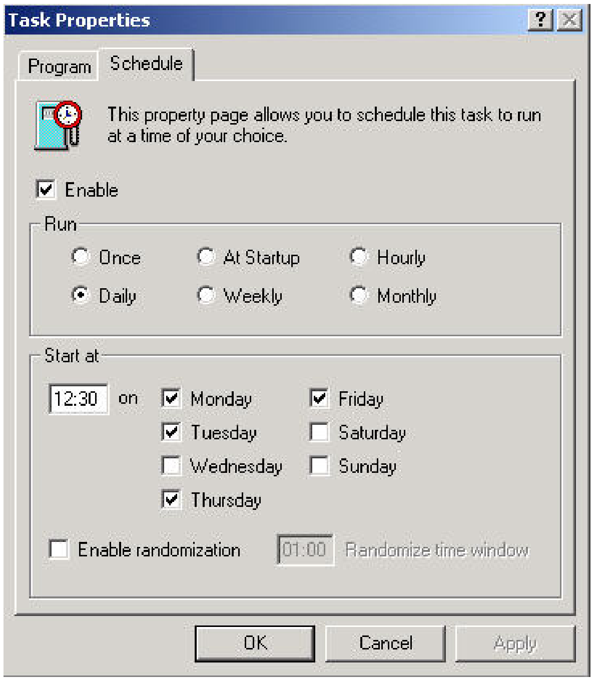
Under the **Schedule** tab, select the following:

14. Check **Enable**.
15. Select **Daily**.
16. Select the days and times you want to run autoupdate.

    Days and times should not conflict with your autoupgrade task.

    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.

17. Click on **Apply** and **OK**.
18. Close VirusScan Console.



Task Properties

Program | Schedule

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
12:30 on ☑ Monday ☑ Friday
☑ Tuesday □ Saturday
□ Wednesday □ Sunday
☑ Thursday

□ Enable randomization 01:00 Randomize time window

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 (http://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 http://www.hawaii.edu/antivirus.

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.

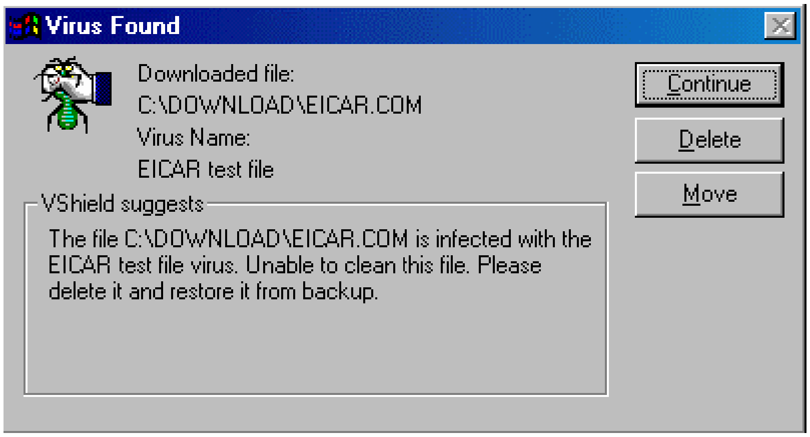
Installing the EXTRA.DAT File

1. Go to the ITS antivirus web page, http://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.



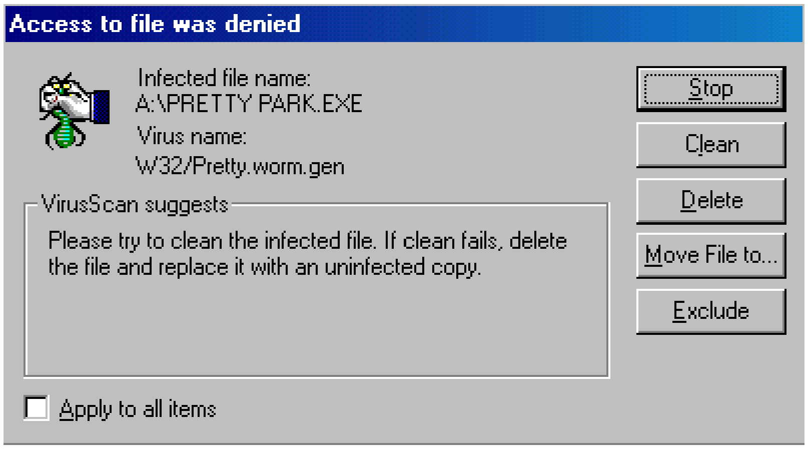
Downloaded file:
C:\DOWNLOAD\EICAR.COM
Virus Name:
EICAR test file

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.



Infected file name:
A:\PRETTY PARK.EXE
Virus name:
W32/Pretty.worm.gen

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

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

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), manually upgrade your SDAT (just to be sure) and 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.

Using McAfee Emergency Disk

The McAfee Emergency Disk will only detect boot sector and file-infecting viruses for computers with **hard drives not formatted with NTFS**. It is not a replacement for the full McAfee VirusScan program. 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 Keller 105 Lab. To create a McAfee Emergency Disk, see Appendix B.

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.)

If you created a McAfee Emergency Disk (NAI-OS formatted) using the Emergency Disk Utility:

> You will be prompted whether you powered off and on. Enter **y** if you did and press **Enter**.
>
> After reading the instructions on the screen, press any key to continue.

If you created a Windows bootable disk (DOS formatted) and copied the EMSCAN files on it:

> At the a:> prompt, type in
>
> **bootscan c: /clean /all**
>
> and press **Enter**. This assumes that c: is your master boot hard disk.

6. The program will begin scanning and cleaning your system using the DAT files on the Emergency Disk. 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.

   After running the McAfee Emergency Disk, run a full scan (scan all files option) using VirusScan to ensure that your computer is clean.

Performance Issues

As on-access virus scanning becomes more complex and requires more system resources, you may notice degradation in system performance. 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 **user specified files** 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 **User Specified Files**.

   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**.

   > ***Warning:*** *virus writers will discover other file types to infect or use to spread viruses. This list of extensions should be reviewed every three months and updated if necessary.*

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 http://vil.nai.com/vil/default.asp and specify the virus name in the search box.

Appendix A – Installing McAfee VirusScan v4.5.1 with SP1

Download McAfee VirusScan v4.5.1 with SP1 from the ITS antivirus download web page at http://www.hawaii.edu/antivirus and save the file to your Windows desktop. You must provide your UH username and password.

1. Close all Windows applications.

2. Double click on the vscan451 icon on your Windows desktop

3. Read the license warning. Click **OK**.

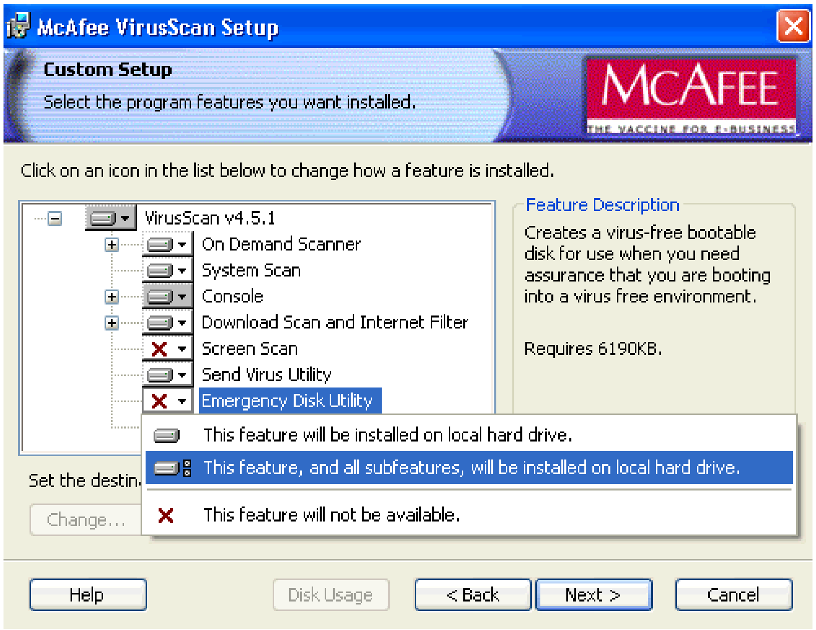
4. In the Product Information window, click **Next**.

5. In the License Agreement window, read the license agreement with NAI. If you agree, darken **I agree to the terms of the License Agreement** and click **Next**.

6. In the Setup Type window, select **Custom Installation** and click **Next**.

   Custom Installation allows you to add options such as the Emergency Disk Utility which is used to create a McAfee Emergency Disk (see Appendix B). If you don't want to add this option, select **Typical Installation**. Skip to step 8.

7. Highlight **Emergency Disk Utility** and select **This feature, and all subfeatures, will be installed on local hard drive** from the drop down menu. The red X should change to a hard drive icon. Click **Next**.



McAfee VirusScan Setup

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- VirusScan v4.5.1
  - On Demand Scanner
  - System Scan
  - Console
  - Download Scan and Internet Filter
  - ✕ Screen Scan
  - Send Virus Utility
  - ✕ Emergency Disk Utility

Feature Description

Creates a virus-free bootable disk for use when you need assurance that you are booting into a virus free environment.

Requires 6190KB.

This feature will be installed on local hard drive.

This feature, and all subfeatures, will be installed on local hard drive.

✕ This feature will not be available.

Set the destin

8. Please wait while VirusScan copies files to your hard drive and updates your registry.
   In the Completing McAfee VirusScan Setup window, uncheck **Scan Boot Record** (unless it is grayed out), uncheck **Create Emergency Disk** (if selected Custom Installation) and uncheck **Run Default Scan After Installation**. Click **Next**.

9. In the Update Virus Definition Files window, darken **Wait and Run AutoUpdate Later**. Click **Next**.

10. Check **Start VirusScan** and click **Finish**.

    VirusScan will be loaded into memory. You should have two icons in your system tray – one for Vshield and the other for VirusScan Console .

11. Download the most current SDAT file from http://www.hawaii.edu/downloads/mcafee/sdat.html. Double click on the SuperDAT (SDAT) link and save the file on your Windows desktop. Double click on the sdat_latest icon to install it. Follow instructions on your screen.

12. Configure System Scan properties in VirusScan Console (see section "Changing System Scan Settings" in the document) and scan **user specified files,** adding files with the TX? extension, on your local hard drives.

13. Configure E-mail Scan (see section "Changing E-mail Scan Settings" in the document).

14. Configure Download Scan properties. On the Detection tab, check **Enable Internet Download Scanning**. Darken **All Files** for what to scan.

15. Configure Internet Filter. On the Detection tab, check Enable **Java and ActiveX filter**. Click **Apply** and **OK**.

16. Complete configuring and scheduling AutoUpgrade, AutoUpdate tasks in VirusScan Console (see sections "Configuring AutoUpgrade" and "Configuring AutoUpdate" in the document).

17. Create a task in VirusScan Console to scan your local hard drives weekly (see section "How to Scan your Hard Drives Automatically" in the document).

18. When you are done updating VirusScan to the most current SDAT, configuring and scheduling autoupgrade, autoupdate, and scan hard drives tasks in VirusScan console, run a full scan of your hard drive(s). Right click on VirusScan Console icon in the system tray, click **Restore**, double click **Scan Hard Drives** task and click **Run Now**.

Appendix B – Create a McAfee Emergency Disk

Create a McAfee Emergency Disk only on a computer known to be free of viruses. An infected computer could infect your McAfee Emergency Disk.

1. Insert a blank floppy disk into your diskette drive.

2. Click **Start**, **All Programs**, **Network Associates**, **Create Emergency Disk**.

   Note: If you don't have the **Create Emergency Disk** option, you need to modify your VirusScan installation to add this option. Click **Start**, **Control Panel**, **Add/Remove Programs**. Click **McAfee VirusScan** then click **Change**. Select the **Modify** option. Add **Emergency Disk Utility**.

3. Follow the instructions on screen for McAfee Emergency Disk Creation Wizard.

   The emergency disk will be formatted in NAI-OS format which will work on FAT16, FAT32, and NTFS partitions.

4. When you are done creating your emergency disk, write-protect the disk by sliding the slider so a hole shows on the bottom left of the disk. Label your diskette "McAfee Emergency Disk".

5. You will need to update the DAT files on the Emergency Disk to the most current version. Open your web browser to www.mcafeeb2b.com/naicommon/avert/avert-research-center/virus-4e.asp.

6. Click on the EMSCAN.ZIP link and save the file on your Windows desktop.

7. Double click on the EMSCAN.ZIP icon to unzip it. You must have Winzip or similar unzip application installed on your computer. Copy the unzipped files onto your McAfee Emergency Disk that you just created. These should include the latest reduced-size scan.dat, clean.dat, and names.dat files.

The Emergency DAT files allow BOOTSCAN.EXE to look for viruses in your hard disk's master boot record and boot sector and in memory for some cases. The Emergency DAT files are compressed files, optimized for use on a floppy disk. They are LIMITED in use and should not be used in place of the full VirusScan product.

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

Or see the ITS Helpdesk 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.

The University of Hawaiʻi is an equal opportunity/affirmative action institution.