



Using McAfee VirusScan Enterprise 7.0

Jocelyn Kasamoto

Introduction	1
Product Overview	2
System Requirements	2
Where to Get the Software.....	3
Installation Instructions.....	3
Which Version of VirusScan am I Running?.....	7
Launching VirusScan Console.....	7
Configuring On-Access Scan Properties.....	8
Editing the AutoUpdate Repository List.....	11
Configuring AutoUpdate Task.....	13
How to Manually Update SDAT/DATs.....	14
Configuring Scan All Fixed Disks Task	15
How to Scan for Viruses	18
Configuring E-mail Scan (Outlook Only).....	21
I Found a Virus, Now What?	23
Appendix A VirusScan Version by Operating System	25
For More Information	26

Introduction

Anti-virus software is the first line of defense against computer viruses that can spread very quickly using your Internet and/or local network connection, through e-mail attachments, network shares and peer-to-peer filesharing. An infected computer could cause your system to malfunction, limiting your productivity. Virus infections could cause loss of valuable data or even more embarrassing – distribution of confidential or personal data. Virus infections can require a lot of man-hours to clean up or rebuild your system. Often when one computer gets infected, it also affects other computers in your office and on your network. **The best way to protect your system from viruses is to update your anti-virus program frequently and scan your hard drive for viruses weekly.**

Information Technology Services (ITS) has purchased a number of licenses of McAfee VirusScan anti-virus software that active University of Hawai'i (UH) faculty, staff and students can use at no extra charge on their Windows computers. **McAfee VirusScan Enterprise is licensed for use on UH owned computers (desktops and laptops), including computer labs on campus.** (See “*System Requirements*” for supported operating systems). 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 on UH owned computers). 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 covers the basics of installing, configuring and using McAfee VirusScan Enterprise 7.0.

Product Overview

McAfee VirusScan Enterprise (VSE) is published by Network Associates Inc. (NAI). It provides anti-virus protection against viruses, trojans and worms for Windows operating systems. VSE is licensed for use on UH owned computers only. It supports Windows NT, Windows 2000, and Windows XP systems. Note: Windows 98 and Windows ME users of UH owned computers should continue to use McAfee VirusScan 4.5.1 with Service Pack 1.

VSE can be installed on both desktop and server platforms. It replaces the Netshield anti-virus product for Windows NT and Windows 2000 servers. It also supports Windows server 2003. Note: Netware servers need to use Netshield for Netware. Exchange servers need to use Groupshield.

VSE product updates, DAT updates, scan engine updates, extra.dat and hotfixes are obtained automatically from NAI through the AutoUpdate task in VirusScan Console. There is no separate AutoUpgrade task.

VSE runs more efficiently than McAfee VirusScan 4.5.1 with Service Pack 1 because code for the Win9x platform has been removed.

System Requirements

McAfee VirusScan Enterprise 7.0 runs on the following Windows platforms:

Workstations

- Windows NT workstation 4.0 with Service Pack 6 or 6a
- Windows 2000 Professional with Service Pack 1, 2, 3 or 4
- Windows XP Home with Service Pack 1
- Windows XP Professional with Service Pack 1

Servers

- Windows NT server 4.0 with Service Pack 6 or 6a
- Windows 2000 server with Service Pack 1, 2, 3 or 4
- Windows server 2003

To run McAfee VirusScan Enterprise, it is recommended that your computer has the following:

- Internet Explorer 5.5 Service Pack 2 or later
- 45 MB of hard disk space (25 MB of temporary disk space is released after installation)
- 32 MB RAM or higher
- Intel Pentium class or Celeron processor rated 166MHz or higher
- CD-ROM drive
- Internet connection (local area network, broadband or modem connection) for getting updates

Check the Microsoft web site at <http://www.microsoft.com> for guidelines for recommended RAM for optimal operating system performance.

You must also have a valid UH username and password to get a copy of the software which is licensed for the University of Hawai'i. Go to <http://www.hawaii.edu/account> to request a UH username.

Where to Get the Software

Open your web browser to <http://www.hawaii.edu/antivirus> to download a copy of McAfee VirusScan Enterprise. Login with your UH username and password. You must login from a computer on campus. VSE is not available for download off campus.

Installation Instructions

1. Download a copy of McAfee VirusScan Enterprise (UHVSE7.exe) from <http://www.hawaii.edu/antivirus> and save it to an **empty** folder on your desktop. For example, create a new folder called Virusscan on the desktop and save the UHVSE7.exe file in there.
2. **If you have an existing anti-virus package, please uninstall it first** by going to **Start, Settings, Control Panel, Add/Remove Programs**. Select **McAfee VirusScan (or your anti-virus product)** and click on the **Add/Remove** button. When the anti-virus package has been removed, close all windows and restart your computer. Check your anti-virus manual if you have other anti-virus products.

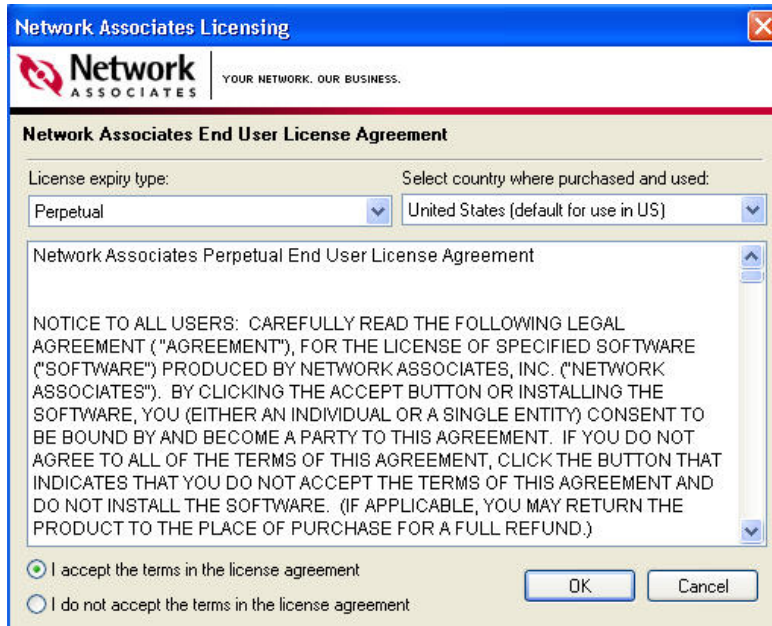
Note: if you install VSE over an existing VirusScan 4.5.1 with SP1 installation, the VSE installer will detect the previous version. When prompted to remove the older version, you should remove it. If you select to preserve the existing settings, some of the settings may not be correct.

3. Make sure that you are logged in with an account that has administrator privileges.
4. Double click on the UHVSE7.exe self-extracting file. Make sure you run the file from an empty folder.
5. Click **View Readme** to show the readme file, if desired. Click **Next**.



- For License Expiry Type, select **Perpetual** from the pull down menu. Leave the country selection as **United States**. Read the license agreement. If you agree with the terms of the license agreement, darken the radio button for “I accept the terms in the license agreement”. Click **OK**.

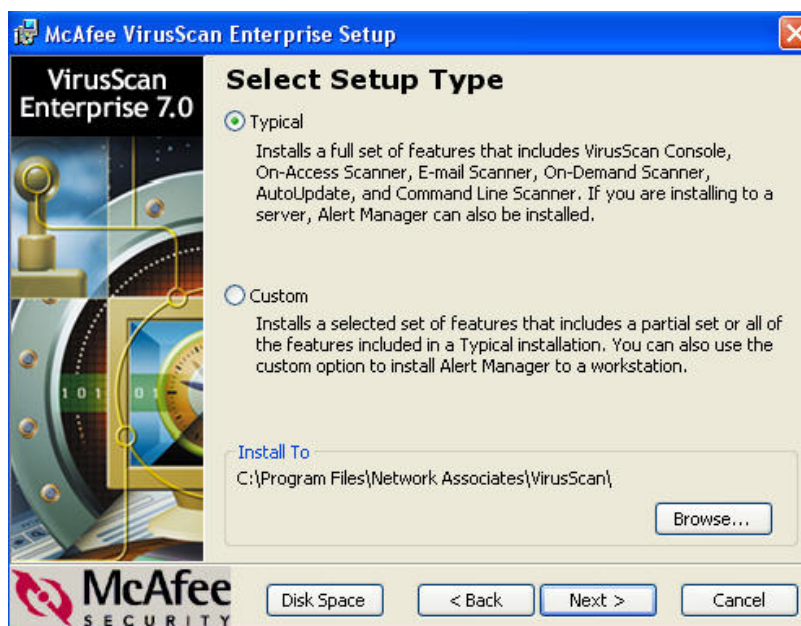
Note: if you decline, you won't be able to install the software and will need to get another anti-virus software.



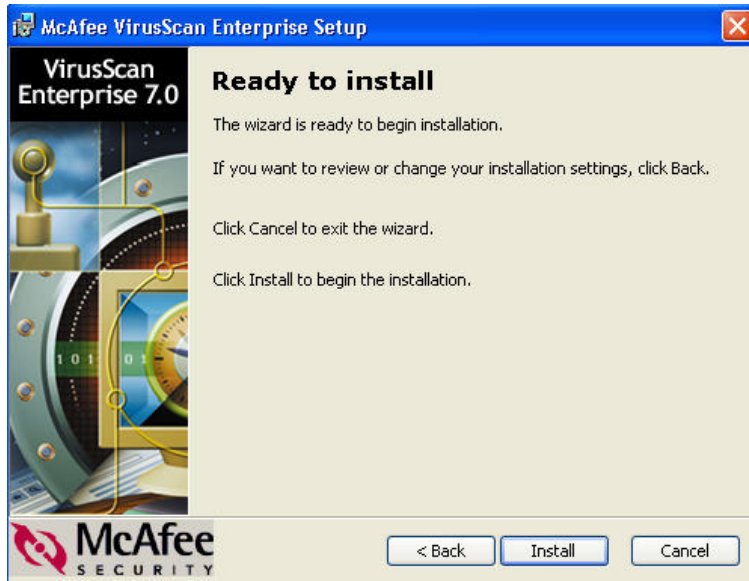
- Select **Typical** for Setup Type.

VSE installs in C:\Program Files\Network Associates\VirusScan\ folder by default. Click **Browse** to specify another folder.

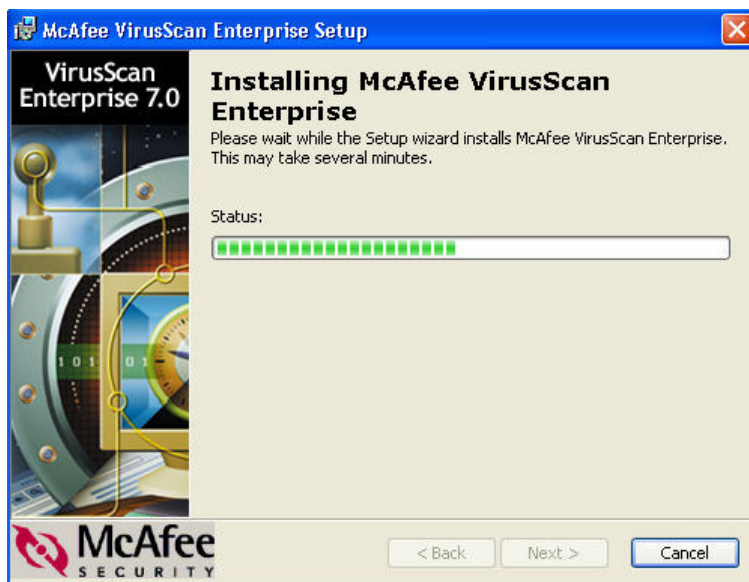
Click **Next**.



8. Click **Install** to begin.



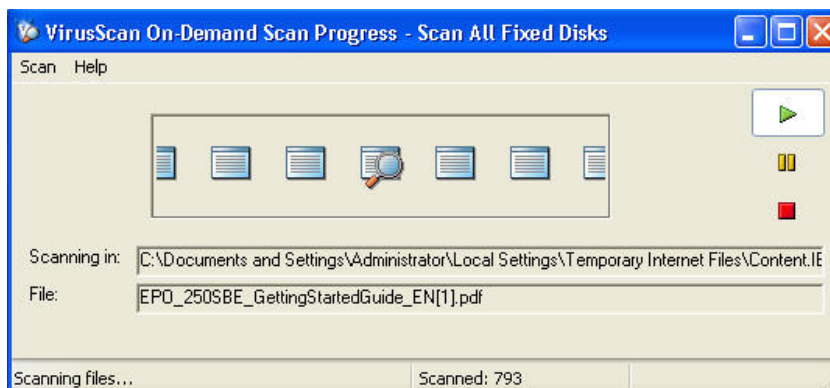
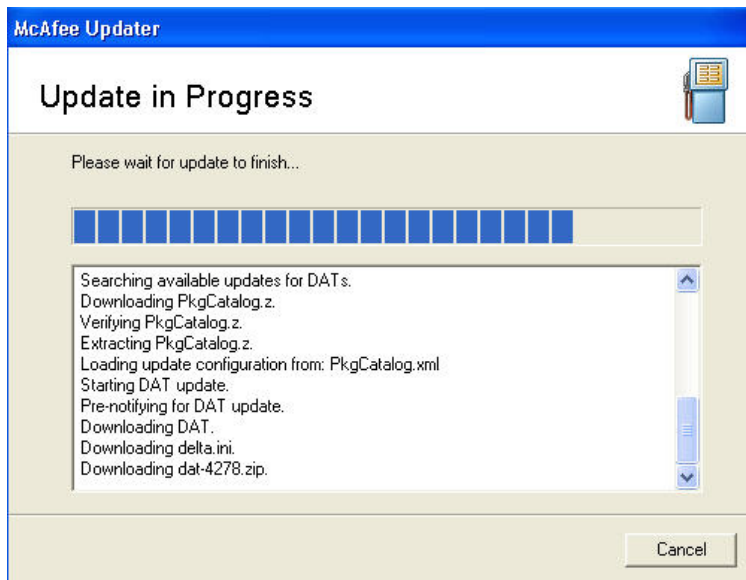
Please wait while VSE copies files to your hard drive and updates your registry.




9. "Update Now" and "Run On-Demand Scan" is checked by default. Click **Finish**.

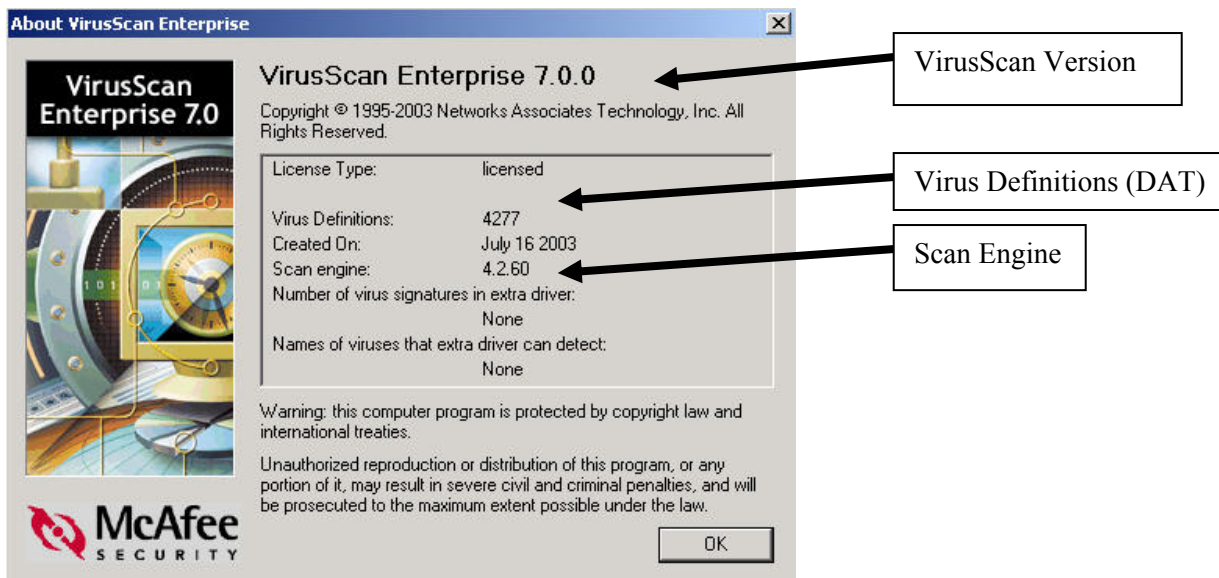


VSE updates to the current DAT and scan engine then runs a scan of all fixed disks.



Which Version of VirusScan am I Running?

Right click on the Vshield icon  in the system tray and click **About VirusScan Enterprise**.

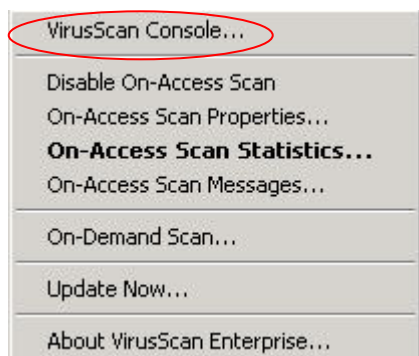


You are running VirusScan Enterprise version 7.0.0 with virus definitions (DAT) 4277 and scan engine 4260. You will need this information when calling the ITS Help Desk for assistance with VirusScan.

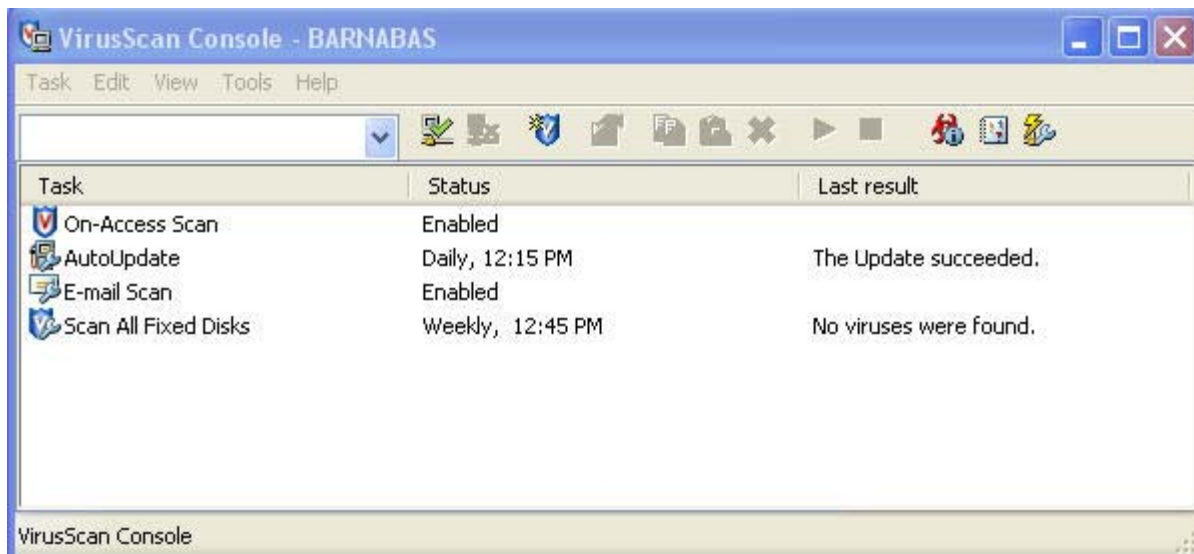
Launching VirusScan Console

VirusScan should load automatically at startup when you boot up Windows.

Right click on the icon with a red Vshield icon  in the system tray. On the pop-up menu, click **VirusScan Console**.



Note: there is no separate system tray icon for VirusScan Console.




VirusScan Console comes with four tasks by default: On-Access Scan, AutoUpdate, E-mail Scan, and Scan All Fixed Disks. Note: there is no separate AutoUpgrade task. All updates (DAT, scan engine, extra.dat, hotfixes and program updates) are done through the AutoUpdate task. Other tasks may be added to VirusScan Console.

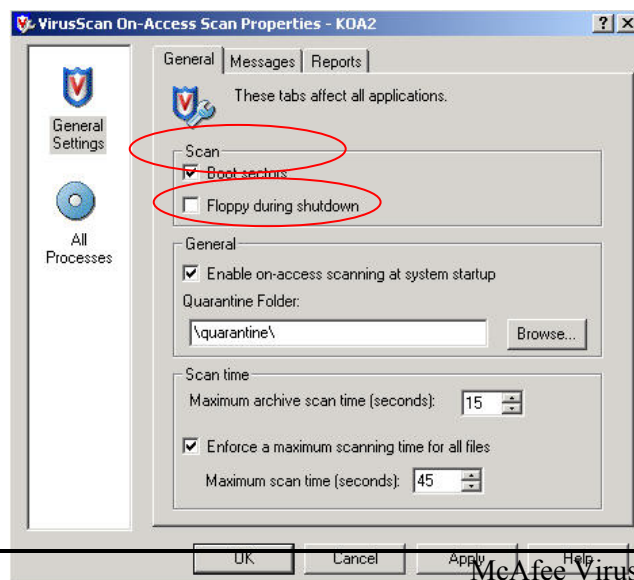
Configuring On-Access Scan Properties

On-access scan properties have been pre-configured for use at UH. In general, the pre-configured settings should be sufficient for anti-virus protection for general business office use. If you have a shared computer or a computer lab environment, you should adjust your scan settings to increase your anti-virus protection levels.

1. In VirusScan Console, right click on the **On-Access Scan** task and click on **Properties**.

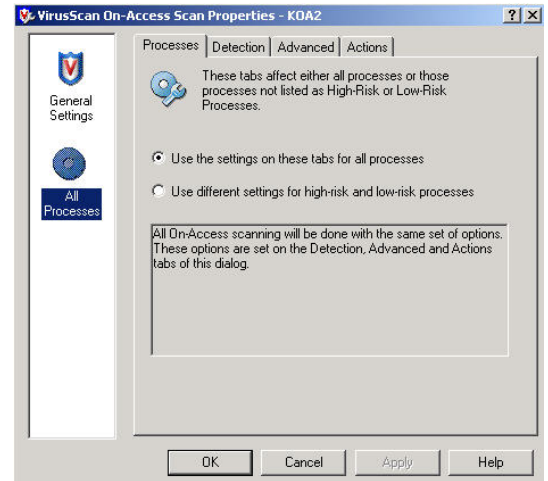
If VirusScan Console is not open, right click on the red Vshield icon  in the system tray and click on **On-Access Scan Properties**.

2. In the General Tab, scan “floppy during shutdown” is unchecked in the pre-configured setting. (Scanning floppies on shutdown has caused shutdown problems with some computers.)



3. Click on the **All Processes** icon in the left pane.

You can use different scan settings for high-risk and low-risk processes. Darken the appropriate setting, according to your situation.



4. Click on the **Detection** tab.

Scan **Default + additional file types** is selected. The **TX?** file extension has been added to the default file extensions list and **Also scan for macro viruses in all files** has been checked. This scan setting is recommended to allow sufficient anti-virus protection without noticeable degradation in system performance.

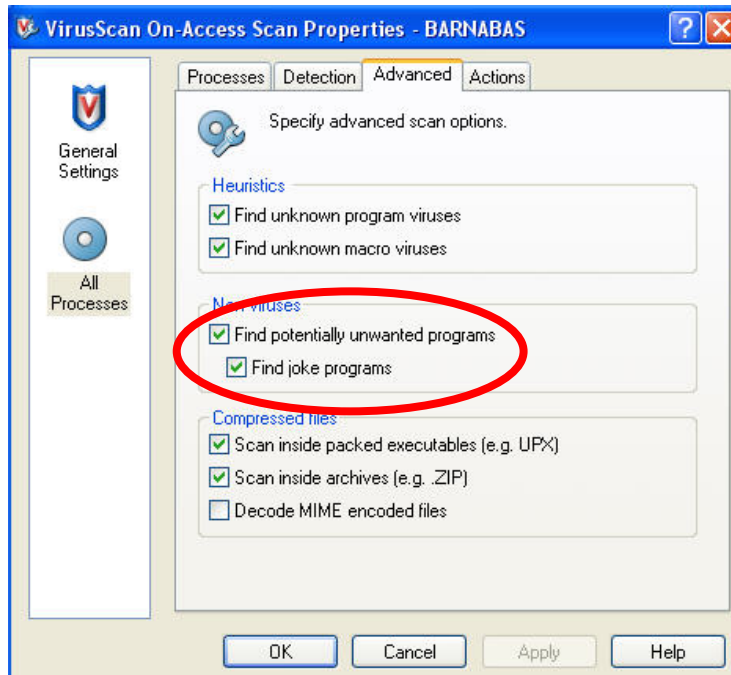


If you have more stringent scan requirements (for shared computers or public computer labs), select scan **All files**. This scan setting may slow down the performance of your computer, depending on your hardware, but allows for maximum anti-virus protection.

5. Click on the **Advanced** tab.

All options, except **Decode MIME encoded files**, are checked.

VSE will scan for potentially unwanted programs, such as adware and spyware (which are not viruses). This is a new feature added in VSE 7.0. If these programs are detected, VSE does not remove them. If you wish to remove them, go to **Start, Settings, Control Panel, Add/Remove Programs**. Select the unwanted program and click **Add/Remove**.



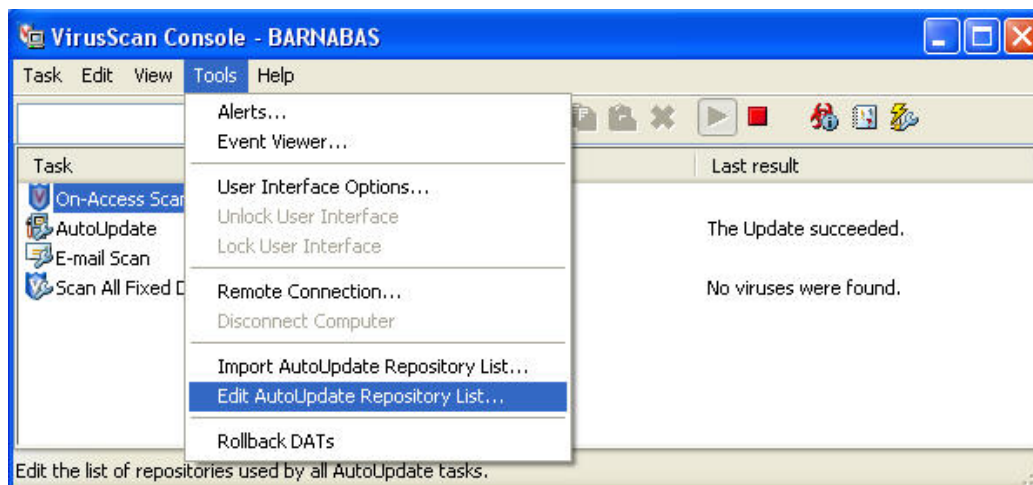
6. Click **Apply** and **OK**.

Editing the AutoUpdate Repository List

VSE has been pre-configured to check repositories at UH for available updates. Repositories are FTP or HTTP sites. The AutoUpdate task in VSE Console or the Update Now task from the Vshield system tray icon is used to check for updates. The default repositories are pre-configured to point to UH FTP and UH FTP 2 sites. **You do not need to make any changes in the pre-configured UH repository settings.**

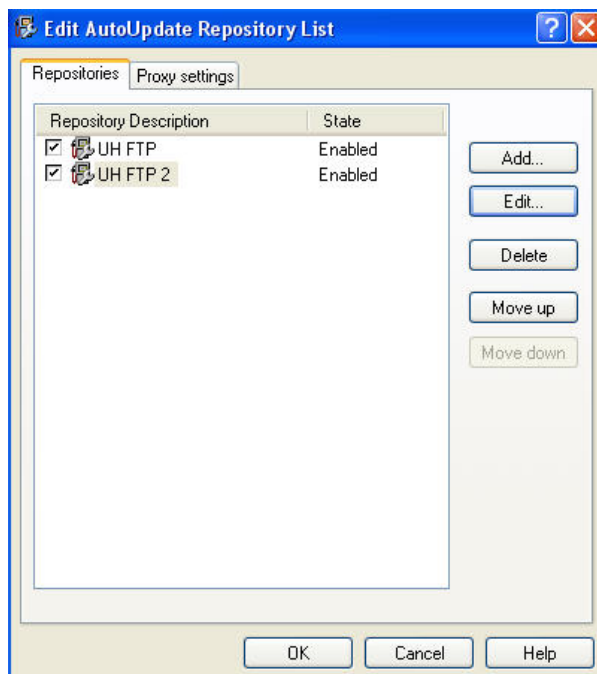
To view the AutoUpdate Repository list:

1. Right click on the **Vshield** icon in the system tray.
2. Click on **VirusScan Console**.
3. On the menu bar, click on **Tools, Edit AutoUpdate Repository List**.



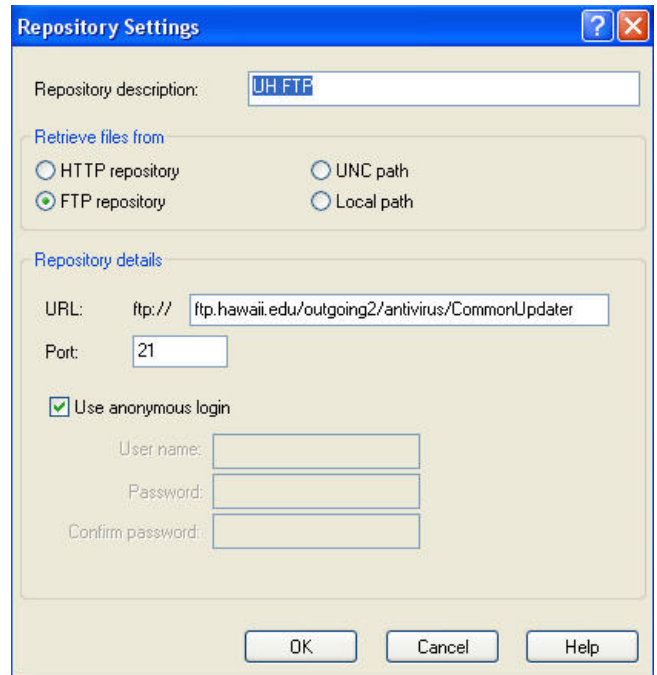
4. Both **UH FTP** and **UH FTP 2** should be checked and enabled.

Highlight **UH FTP** and click on the **Edit** button.



5. These are the settings for the **UH FTP** repository:
- Repository description – **UH FTP**
 - Select **FTP repository**.
 - URL: <ftp://ftp.hawaii.edu/outgoing2/antivirus/CommonUpdater/>
 - Port: **21**
 - Check “**use anonymous login**”.

Click **OK**

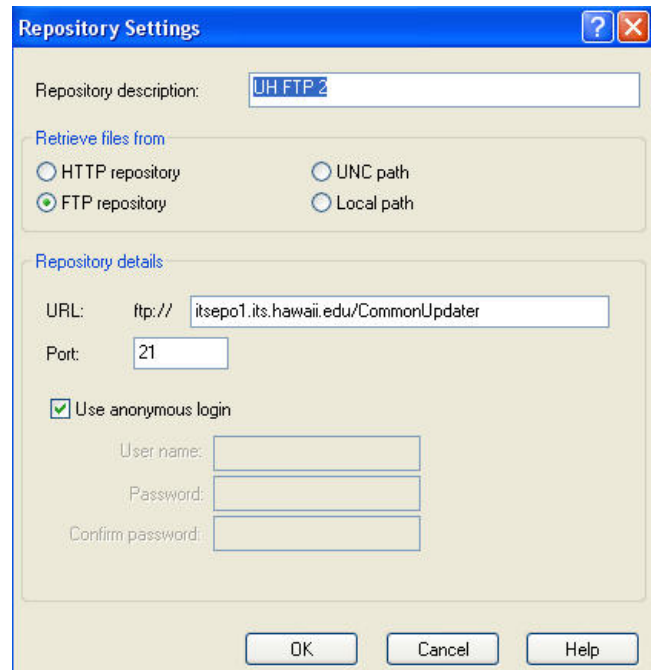


The screenshot shows the 'Repository Settings' dialog box. The 'Repository description' field contains 'UH FTP'. Under 'Retrieve files from', the 'FTP repository' radio button is selected. In the 'Repository details' section, the URL is 'ftp://ftp.hawaii.edu/outgoing2/antivirus/CommonUpdater', the port is '21', and the 'Use anonymous login' checkbox is checked. There are empty input fields for 'User name', 'Password', and 'Confirm password'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

6. Highlight **UH FTP 2** and click on the **Edit** button.

- These are the settings for **UH FTP 2** repository:
- Repository description – **UH FTP 2**
 - Select **FTP repository**.
 - URL: <ftp://itsep01.its.hawaii.edu/CommonUpdater/>
 - Port: **21**
 - Check “**use anonymous login**”.

Click **OK**.

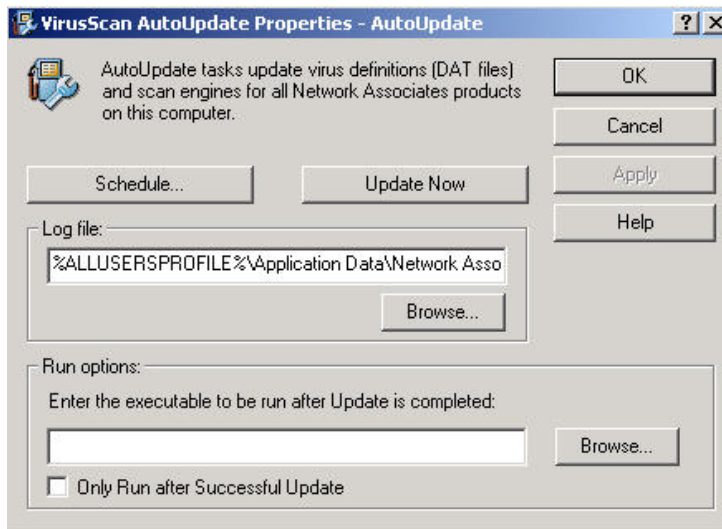


The screenshot shows the 'Repository Settings' dialog box. The 'Repository description' field contains 'UH FTP 2'. Under 'Retrieve files from', the 'FTP repository' radio button is selected. In the 'Repository details' section, the URL is 'ftp://itsep01.its.hawaii.edu/CommonUpdater', the port is '21', and the 'Use anonymous login' checkbox is checked. There are empty input fields for 'User name', 'Password', and 'Confirm password'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Configuring AutoUpdate Task

The AutoUpdate task has been pre-configured for use at UH. In general, you do not need to make any changes in the AutoUpdate task. You may need to change settings in the AutoUpdate schedule to better meet your specific needs.

1. In VirusScan Console, right click on the **AutoUpdate** task and click on **Properties**.
2. Click on **Update Now** to go to the UH repositories to manually check for available updates. If updates are available, they will be automatically downloaded and installed.



To Schedule AutoUpdates

For the best protection, AutoUpdates should be scheduled **daily** (recommended setting) or at minimum, 2 or 3 days per week.

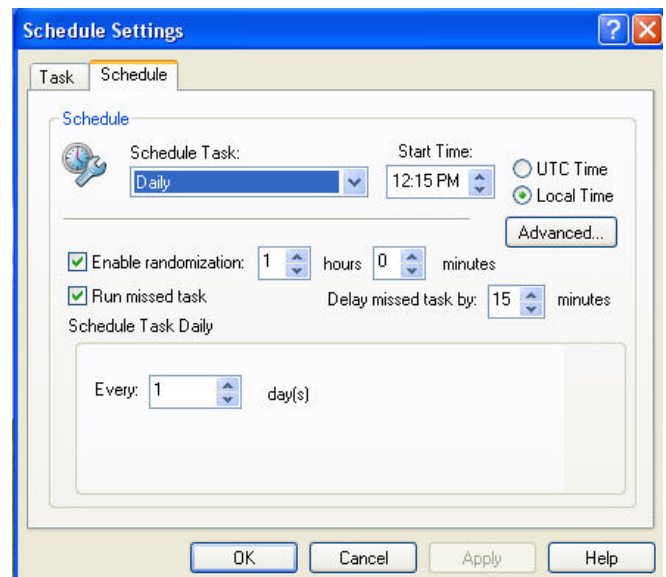
Click on the **Schedule** button then click on the **Schedule** tab.

- Select **Daily** and time of day specifying a.m. or p.m.
- If selecting the **Weekly** option, select 2 or 3 days per week, preferably a day near the beginning of the week and another day near the end of the week.

The pre-configured schedule for AutoUpdate is set to **daily** at 12:15 pm.

Note: Your computer must be powered on and you must be logged in at the scheduled time for the AutoUpdate task to run.

You may adjust the time to run the AutoUpdate task to meet your needs. **Daily** updating is recommended since your DAT file will be at most, one version old. NAI routinely updates DATs once a week but more frequently during virus outbreaks.

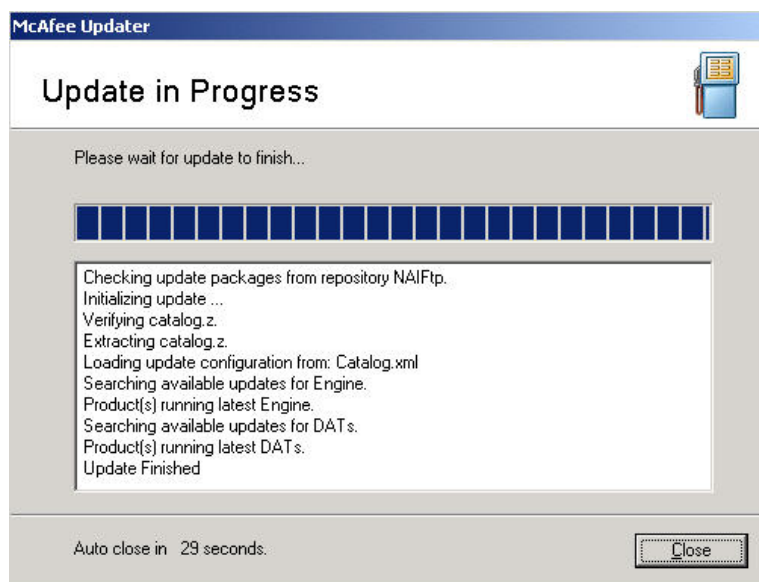


How to Manually Update SDAT/DATs

SDAT is the SuperDAT utility that updates the scan engine and DAT files in one installation package.

There are two ways to manually update your SDAT and DAT files.

- Open VirusScan Console. Right click on **AutoUpdate**, click on **Properties**.
Click on **Update Now**
- Right click on the red Vshield icon in the system tray and click on **Update Now**.



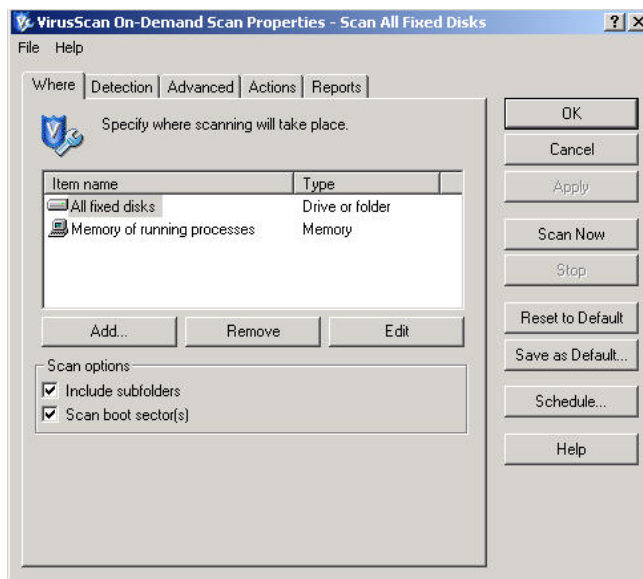
VSE will check the UH repositories for available updates. If updates are available, it will download and install the latest updates. Otherwise, VSE will inform you that you have the latest scan engine and DAT files.

Click **Close** when the update is completed or the message box will automatically close.

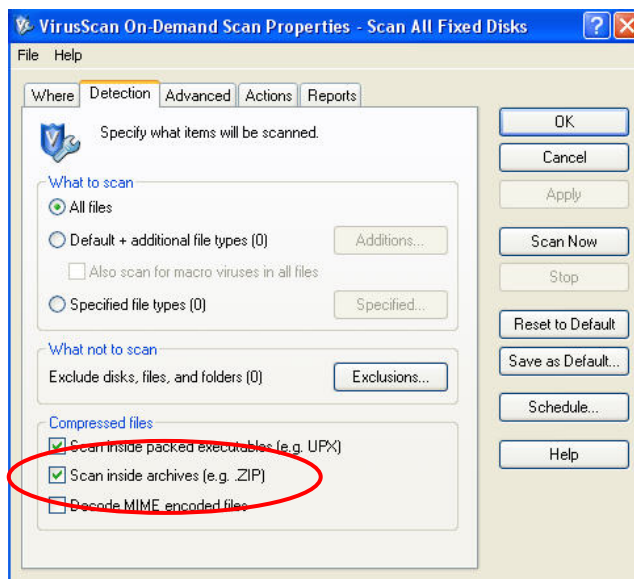
Configuring Scan All Fixed Disks Task

The Scan All Fixed Disks task has been pre-configured for use at UH. In general, you don't have to make any changes. This section shows you the pre-configured options. Adjust the settings, only if needed, to better meet the requirements of your environment.

1. Open VirusScan Console. Right click on the **Scan All Fixed Disks** task and click on **Properties**. Ensure that the Item name is set to **All fixed disks**.

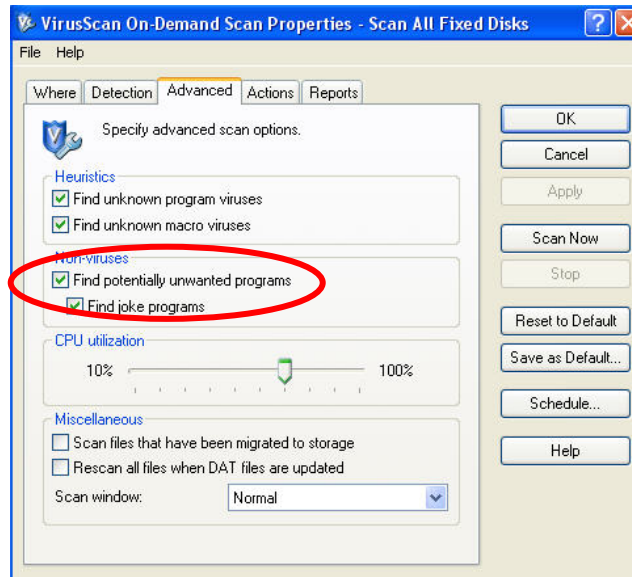


2. Click on the **Detection** tab. By default, **all files** are scanned. This is the recommended option for scanning your hard drives. **Scan inside archives** is also checked for added protection.



3. Click on the **Advanced** tab. **Find potentially unwanted programs** and **Find joke programs** are checked in the pre-configured settings. VirusScan will search for adware and spyware which are

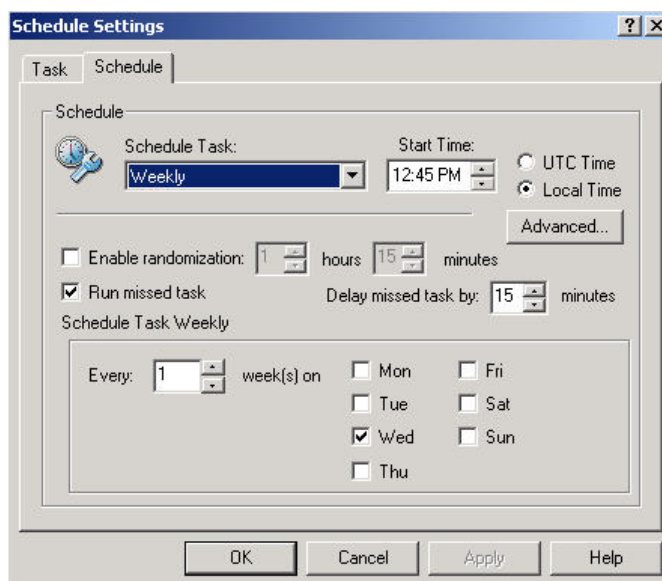
not viruses. Any potentially unwanted program found by VirusScan is not removed. You should remove the unwanted program by going to **Start, Control Panel, Add/Remove Programs**.



4. If you made any changes, click **Apply** then schedule the task.

To Schedule Scan All Fixed Disks

1. Open VirusScan Console. Right click on the **Scan All Fixed Disks** task and click on **Properties**. Click on the **Schedule** button on the right side. On the **Task** tab, check **Enable (scheduled task runs at specified time)**.
2. Click on the **Schedule** tab. In the Schedule Task pull down menu, select **Weekly**. Set the start time and designate a.m. or p.m. Leave as local time. Check a day of the week to scan your fixed disks. This should be a time when your computer is powered on, you are logged in and won't be actively using your computer. The pre-configured scan schedule is set for Wednesdays at 12:45 pm. Make adjustments to day or time, if needed. Click on **Apply** and **OK**.

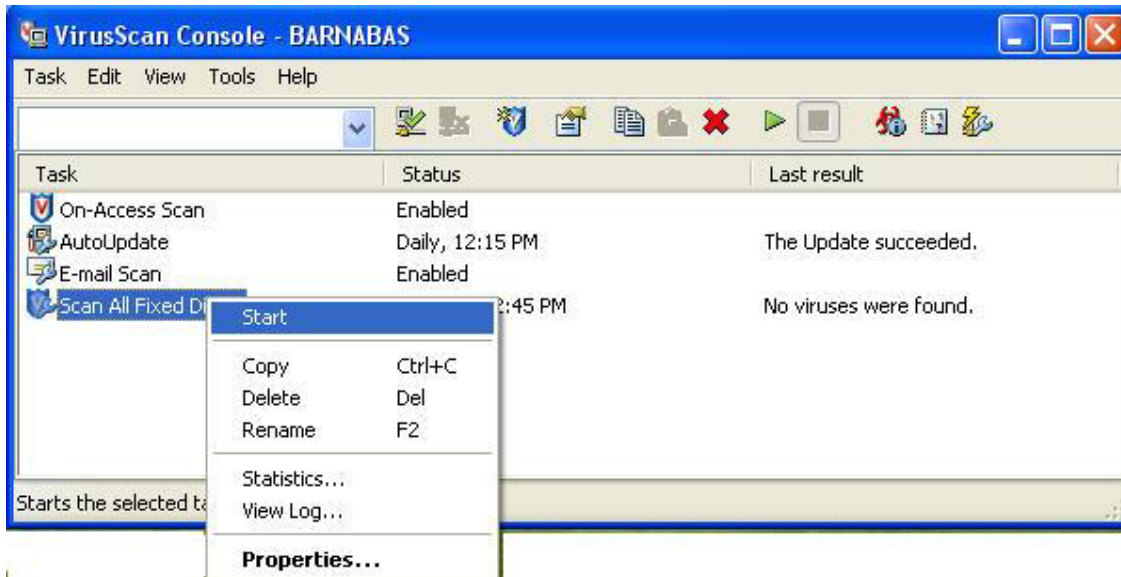


Note: if your computer is shared or in a public computer lab, it is recommended that you scan your fixed disks more frequently (2 or 3 times per week or daily).

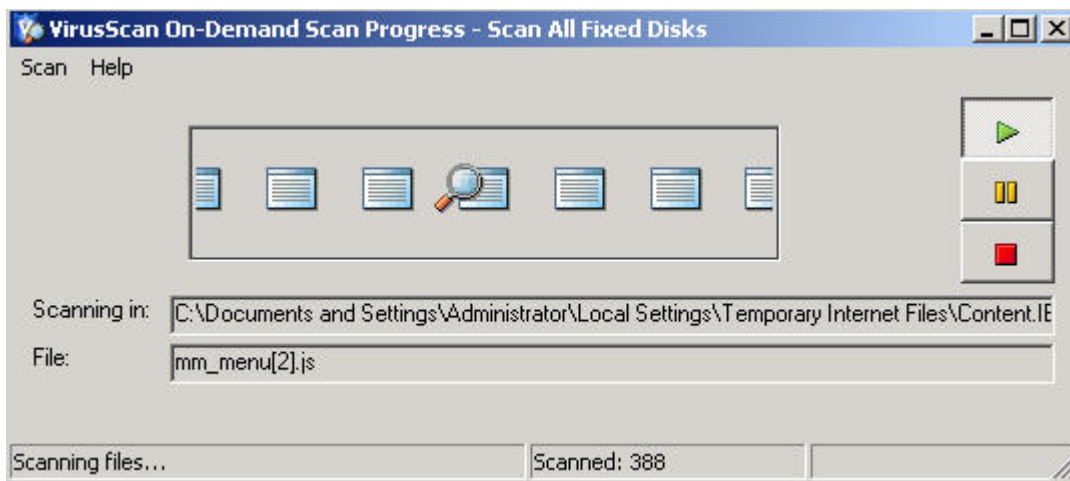
Remember that your computer must be powered on and you must be logged in at the scheduled time for the task to run.

How to Scan for Viruses

Open VirusScan Console. Right click on **Scan All Fixed Disks** task and select **Start**.

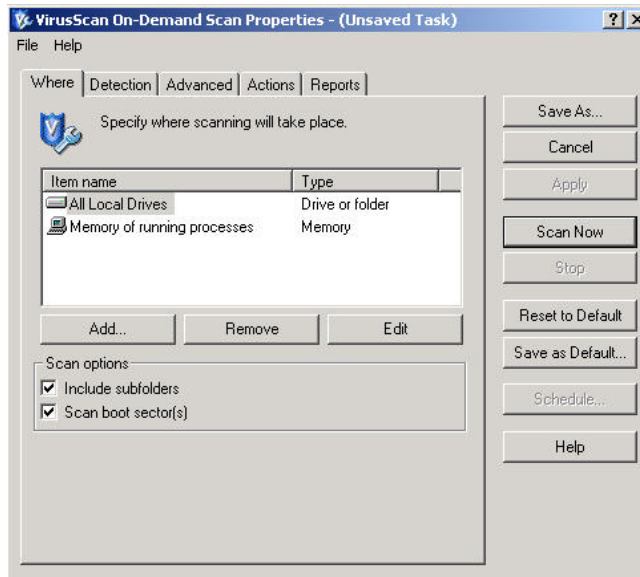


The scan task will start to scan all your fixed disks. Make sure you configured the scan task following the directions in the previous section.

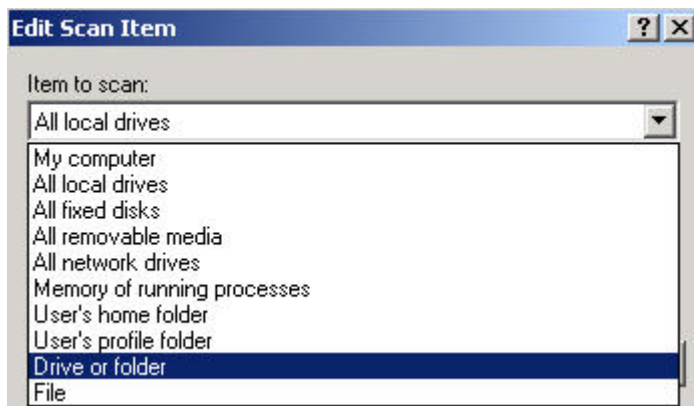


Specifying What to Scan

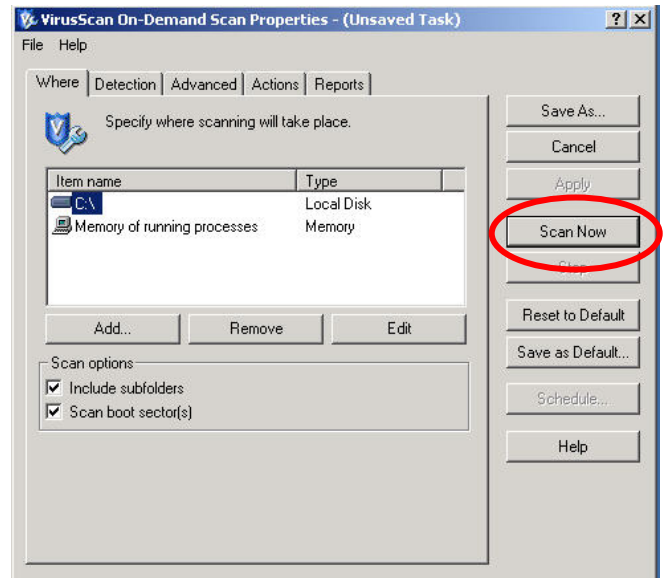
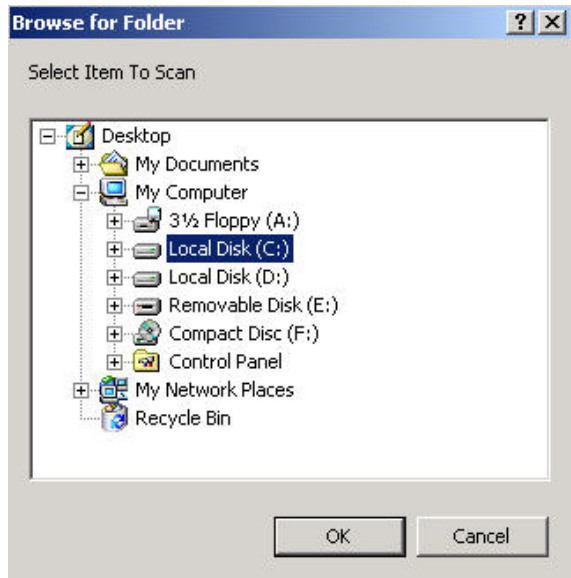
1. If you wish to scan a particular drive or folder, right click on the red Vshield icon in the system tray and click **On-Demand Scan**.
2. In the Where tab, highlight **All Local Drives**, and click on the **Edit** button.



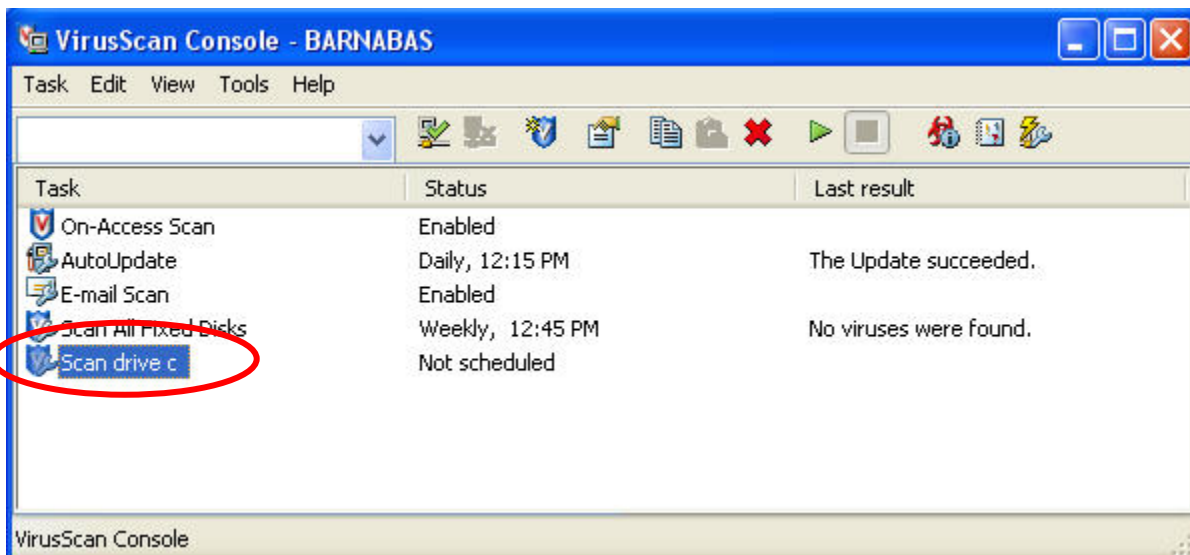
3. In the **Item to Scan** pull down menu, select **Drive or folder** (or the desired location).



4. Click on the **Browse** button and select the drive or folder to scan. Click **OK** until you return to the On-Demand Scan Properties window. Click **Scan Now** to start the scan..



If you wish to save the scan settings to use for future scans, click the **Save As** button. Enter a task name for the new scan (for example, “scan drive c”) and click **OK**. The newly created task will appear in VirusScan Console.



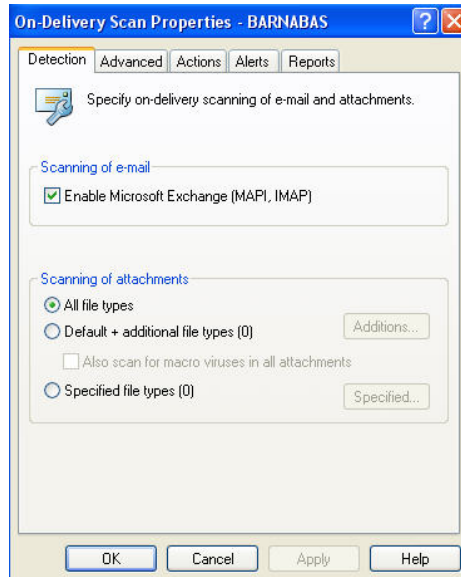
To run the new task, open VirusScan Console, right click on the task and click **Start**.

You can also schedule the new task (follow directions in “Configuring Scan All Fixed Disks Task”) if you scan this location routinely.

Configuring E-mail Scan (Outlook Only)

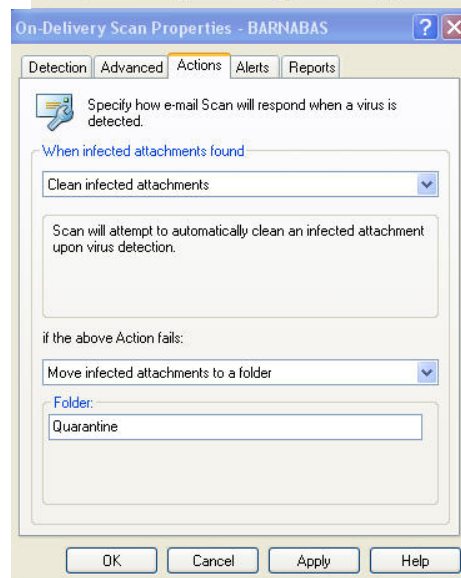
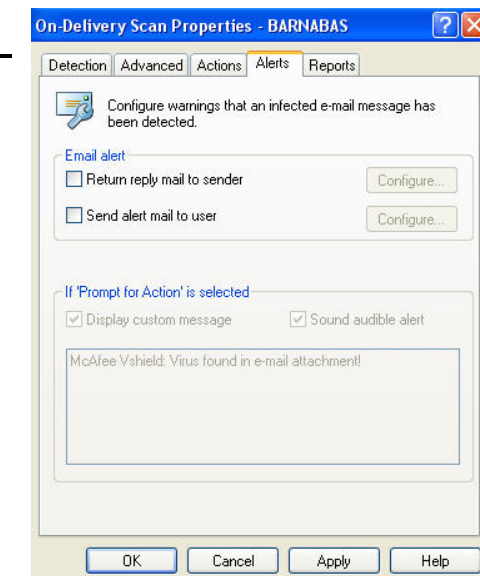
Note: VirusScan Enterprise scans for e-mail viruses when using Microsoft Outlook only.

1. Open VirusScan Console. Highlight **E-mail Scan** and click **Properties**.

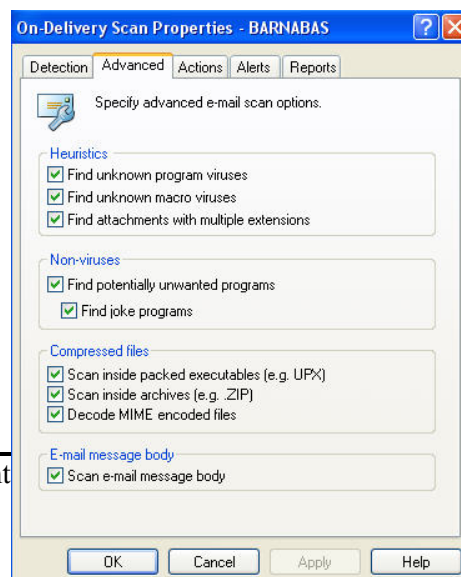


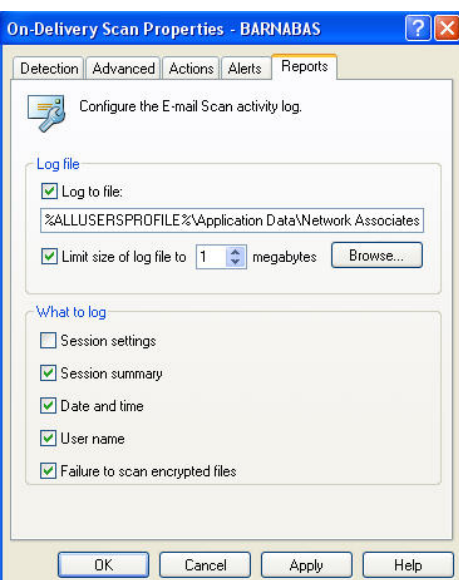
2. In the **Detection** tab, check **Enable Microsoft Exchange (MAPI, IMAP)**.

E-mail Scan Settings in Advanced, Actions, Alerts and Reports Tabs



All the advanced e-mail scan options are selected in the pre-configured settings to ensure maximum protection for Microsoft Outlook (which is a popular vehicle for spreading viruses).

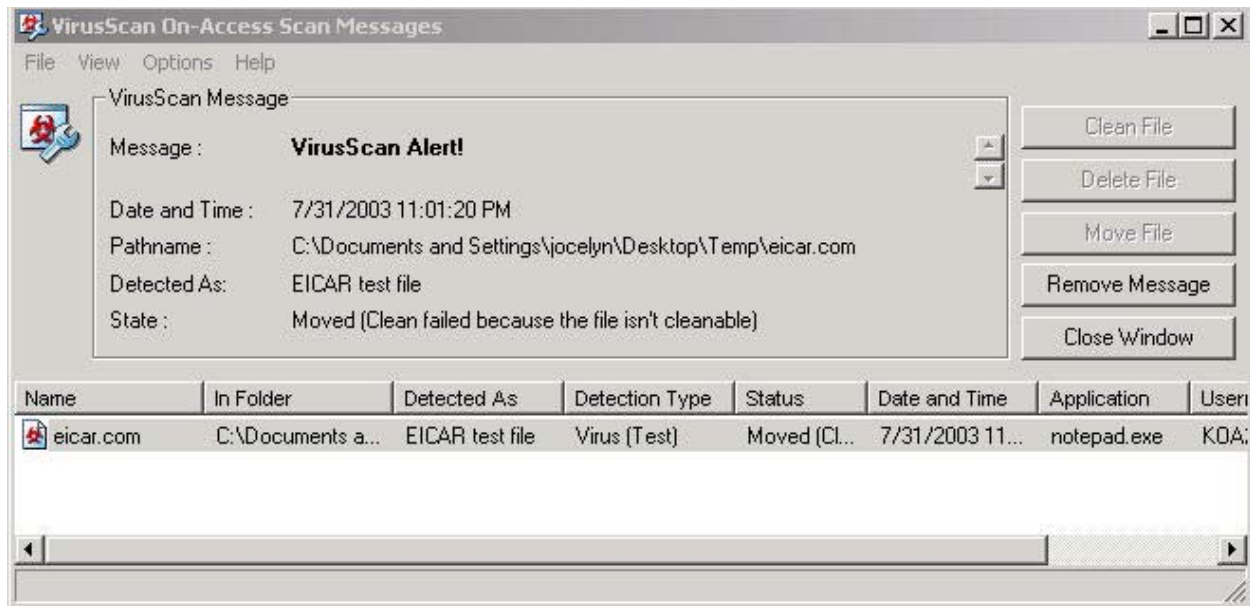




The settings in the Actions, Alerts, and Reports tabs should be left at default unless you have a compelling reason to change them.

I Found a Virus, Now What?

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



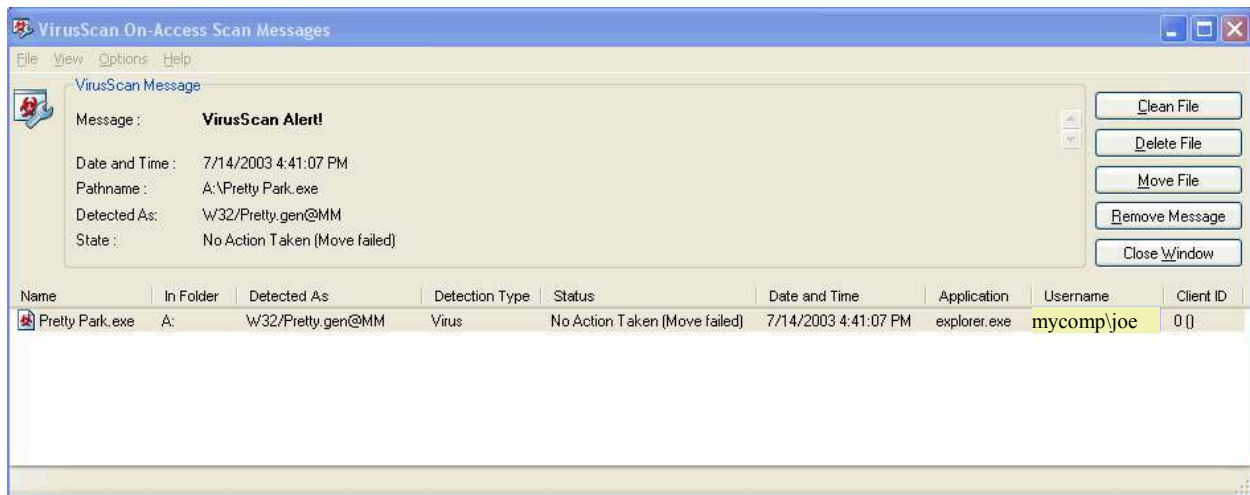
Note: the **Clean File**, **Delete File**, and **Move File** options are not available for this “virus” (eicar.com is not a true virus). VSE tried to clean the virus but couldn’t so the infected file was moved to quarantine.

Normally, you will be prompted with several options. VirusScan will suggest what you should do with the infected file. In general, first try to clean the file, then move it to quarantine then delete it. If you know that the infected file is not needed, you should delete it.

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

If you select to move the file to quarantine, the infected file is copied to the C:\quarantine folder. In most cases, you should choose to delete the infected file. Click **Close Window** to close the Virus Alert window when done.

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



Note: you have several options available for this virus. Click on **Clean File** to disinfect the virus. VirusScan will tell you whether it was successful in removing the virus.

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 or original media.

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 files, OnDemandScanLog.txt and OnAccessScanLog.txt, are saved in the C:\Documents and Settings\All Users\Application Data\Network Associates\VirusScan folder.

Once you have disinfected the virus (or deleted the infected file and restored it from backup), rerun VirusScan with the scan all files option once more to ensure that your system is clean.

If you are able, you should track down the source of your virus infection and notify the appropriate people involved who may have spread the virus to you and 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 infected attachment.

If you detect a virus and need assistance cleaning or removing 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.

Appendix A VirusScan Version by Operating System

-----Faculty/Staff-----

-

OS	Campus	Home Use	Students
Win98	VS 4.5.1 SP1	VSHE	VSHE
WinME	VS 4.5.1 SP1	VSHE	VSHE
WinNTW	VSE	not supported*	not supported*
Win2K Pro	VSE	VSHE	VSHE
WinXP Home	VSE	VSHE	VSHE
WinXP Pro	VSE	VSHE	VSHE

Servers

WinNT	VSE
Win2K	VSE
Win 2003	VSE
Netware 4 and higher.	Netshield for Netware

*user needs to provide own anti-virus software

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 ITS walk-in Help Desk at Keller 105, the PC Lab in Keller 213 or send e-mail to help@hawaii.edu.

For information about a specific virus, go to <http://vil.nai.com/vil/default.asp> and specify the virus name in the search box.

For VirusScan Enterprise FAQs, go to http://www.nai.com/us/support/technical_support. In the Free Knowledge Search section, click on the **See Details** link. In the Product menu box, select VirusScan Enterprise. Enter search keywords and click on the **Search** button.

For additional assistance, please phone the ITS Help Desk at (808) 956-8883, send email 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 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.

The University of Hawai'i is an equal opportunity/affirmative action institution.