

WIN1016

August 2003

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 antivirus 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 antivirus 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 <u>http://www.microsoft.com</u> 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 <u>http://www.hawaii.edu/account</u> to request a UH username.

Where to Get the Software

Open your web browser to <u>http://www.hawaii.edu/antivirus</u> 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

- Download a copy of McAfee VirusScan Enterprise (UHVSE7.exe) from <u>http://www.hawaii.edu/antivirus</u> 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.**



6. 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 antivirus software.

Network YOUR NETWORK, OUR	R BUSINESS.			
Network Associates End User License Agreement				
License expiry type: Select country where purchased and used:				
Perpetual	United States (default for use in US)	-		
NOTICE TO ALL USERS: CAREFULI AGREEMENT ("AGREEMENT"), FOR	LY READ THE FOLLOWING LEGAL			
NOTICE TO ALL USERS: CAREFULI AGREEMENT ("AGREEMENT"), FOR ("SOFTWARE") PRODUCED BY NET ASSOCIATES"). BY CLICKING THE A SOFTWARE, YOU (EITHER AN INDIV BE BOUND BY AND BECOME A PAR AGREE TO ALL OF THE TERMS OF T INDICATES THAT YOU DO NOT ACC	LY READ THE FOLLOWING LEGAL THE LICENSE OF SPECIFIED SOFTWARE WORK ASSOCIATES, INC. ("NETWORK CCEPT BUTTON OR INSTALLING THE IDUAL OR A SINGLE ENTITY) CONSENT TO TY TO THIS AGREEMENT. IF YOU DO NOT THIS AGREEMENT, CLICK THE BUTTON THAT EPT THE TERMS OF THIS AGREEMENT AND			

7. Select **Typical** for Setup Type.

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

Click Next.

🛃 McAfee VirusSca	n Enterprise Setup 🛛 🛛 🛛 🗙
VirusScan Enterprise 7.0	Select Setup Type
9	 Typical Installs a full set of features that includes VirusScan Console, On-Access Scanner, E-mail Scanner, On-Demand Scanner, AutoUpdate, and Command Line Scanner. If you are installing to a server, Alert Manager can also be installed.
	Custom Installs a selected set of features that includes a partial set or all of the features included in a Typical installation. You can also use the custom option to install Alert Manager to a workstation.
	Install To C:\Program Files\Network Associates\Virus5can\ Browse
McAfe	Cancel

Page 4

8. Click **Install** to begin.

🛃 McAfee VirusScar	ı Enterprise Setup 🛛 🔀
VirusScan Enterprise 7.0	Ready to install
	The wizard is ready to begin installation.
-	If you want to review or change your installation settings, click Back.
	Click Cancel to exit the wizard.
	Click Install to begin the installation.
101 01	
MaAfa	
SECURIT	< Back Install Cancel

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

🔀 McAfee VirusScar	ı Enterprise Setup 🛛 🔀
VirusScan Enterprise 7.0	Installing McAfee VirusScan Enterprise Please wait while the Setup wizard installs McAfee VirusScan Enterprise. This may take several minutes.
	Cancel

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.

AcAfee Updater	
Update in Progress	
Please wait for update to finish	
Searching available updates for DATs. Downloading PkgCatalog.z. Verifying PkgCatalog.z. Extracting PkgCatalog.z. Loading update configuration from: PkgCatalog.xml Starting DAT update.	
Pre-notifying for DAT update. Downloading DAT. Downloading delta.ini. Downloading dat-4278.zip.	
	Cancel

<mark>le VirusSca</mark> Scan Help	n On-D	emand !	Scan Pro	ogress -	Scan Al	ll Fixed I	Disks	
				Ş				
Scanning in: File:	C:\Doc EPO_2	cuments ar 250SBE_G	nd Setting: ettingStart	s\Administ edGuide_	rator\Loca EN[1].pdf	al Settings ¹	\Temporary In	ternet Files\Content.IE
canning files	5				Scanned:	793		

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

About VirusScan Enterprise		×	
VirusScan Enterprise 7.0	VirusScan En Copyright © 1995-2003	terprise 7.0.0	VirusScan Version
	Rights Reserved.	licensed	Virus Definitions (DAT)
	Virus Definitions: Created On: Scan engine: Number of virus signa	4277 July 16 2003 4.2.60	Scan Engine
	Names of viruses that	None extra driver can detect: None	
1	, Warning: this computer international treaties.	program is protected by copyright law and	
	Unauthorized reproduct portion of it, may result i be prosecuted to the m	ion or distribution of this program, or any n severe civil and criminal penalties, and will aximum extent possible under the law.	

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 th	e icon with	a red V	shield ic	on
VirusScan Con	sole.			

in the system tray. On the pop-up menu, click

VirusScan Console
Disable On-Access Scan
On-Access Scan Properties
On-Access Scan Statistics
On-Access Scan Messages
On-Demand Scan
Update Now
About VirusScan Enterprise

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

Task Edit View Tools He	ARNABAS	
	🚽 🏖 🖢 💐 🖆 🔷 🗳 💐	K 🕨 📕 👫 🖪 🐉
Task	Status	Last result
V On-Access Scan AutoUpdate E-mail Scan Scan All Fixed Disks	Enabled Daily, 12:15 PM Enabled Weekly, 12:45 PM	The Update succeeded. No viruses were found.
/irusScan 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 **v** 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.)

burbad	General Messages Reports
General	These tabs affect all applications.
	Scan
0	Floppy during shutdown
All rocesses	General Enable on-access scanning at system startup
	Quarantine Folder:
	\quarantine\ Browse
	Scan time Maximum archive scan time (seconds): 15 🔹
	 Enforce a maximum scanning time for all files Maximum scan time (seconds): 45 +

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

You can use different scan settings for high-risk and lowrisk 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.

-	Processes Detection Advanced Actions	
V	Specify what items will be scanned.	
General		
settings	Scan Files	
	When writing to disk	
	When reading from disk	
All	🗹 On network drives	
	What to scan	
	◯ All files	
	O Default + additional file types (1)	ons
	Also scan for macro viruses in all files	
	Specified file types (0)	fied
	What not to scan	
	Exclude disks, files, and folders (1)	ions

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**.

	Processes Detection Advanced Actions
V	Specify advanced scan options.
General Settings	*
0	
Processes	Man wiruses
	Find potentially unwanted programs
	Find joke programs
	Compressed files
	Scan inside packed executables (e.g. UPX)
	Scan inside archives (e.gZIP)
	Decode MIME encoded files

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**.

Task Edit View	Tools Help	
Task -	Alerts Event Viewer	🖻 🏙 🗰 🕨 📕 🚮 🕄 🏇 Last result
♥ On-Access Scar ♥ AutoUpdate ■ E-mail Scan	User Interface Options Unlock User Interface Lock User Interface	The Update succeeded.
🐝 Scan All Fixed D	Remote Connection Disconnect Computer	No viruses were found.
	Import AutoUpdate Repository List	
	Edit AutoUpdate Repository List	
	Rollback DATs	

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

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

Edit AutoUpdate Reposit Repositories Proxy settings	ory List	? 2
Repository Description	State Enabled Enabled	Add Edit Delete Move up Move down
	OK Cano	cel Help

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

Click OK

Retrieve files from			
OHTTP repository	O UNC	path	
FTP repository	O Loca	al path	
Repository details			
IID) Brill Brikawi	ii odu (outaoina)	2 / poblicim o //	Common Indator
	iii.edu/outgoing.	27 anu 11 u s7 u	commonopuater
Port: 21			
🗹 Use anonymous login			
User name:			
Password:			
Confirm password			

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: <u>ftp://itsepo1.its.hawaii.edu/CommonUpdater/</u>
- Port: **21**
- Check "use anonymous login".

Click OK.

lepository de	escription:	UH	FTP 2			
letrieve files	from	N.				
	ository		O UN	IC path		
FTP reporting FTP FTP FTP FTP FTP FTP FTP FTP FTP FTP	sitory		🔿 Lo	cal path		
epository de	etails					
	No. 11 No.	anat ita la	المراجع الأحسام	Common	Undator	
UNL.		eportits.n	awaii.euu/	Commor	lopualei	
Port:	21					
🔽 Use and	onymous lo	gin				
U	ser name:					
	Password:					
8	nassimord					
Confirm (Provinci di	1		-		
Confirm (a a sovy or di					

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.

	AutoUpdate tasks update virus definitions (DAT files) and scan engines for all Network Associates products		
Cance		on this computer.	
Apply	Schedule Update Now		
Help	og file:		
	plication Data\Network Asso	.USERSPROFILE%\A	
	Browse		
		ptions:	
	n after Update is completed:	the executable to be r	
Browse			
	n after Update is completed:	ptions: the executable to be r	

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.

sk Schedule	
Schedule Task: Daily	Start Time: OUTC Time 12:15 PM C OLocal Time OLocal Time
Enable randomization: Enable randomization: Run missed task Schedule Task Daily	hours 0 🗢 minutes Delay missed task by: 15 📚 minutes
Every: 1	day(s)

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.

McAfee Updater	
Update in Progress	
Please wait for update to finish	
Checking update packages from repository NAIFtp. Initializing update Verifying catalog.z. Extracting catalog.z. Loading update configuration from: Catalog.xml Searching available updates for Engine. Product(s) running latest Engine. Searching available updates for DATs. Product(s) running latest DATs. Update Finished	
Auto close in 29 seconds.	[]

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.

Specify wh	ere scanning will	take place.	
			Cancel
Item name		Туре	Apply
All fixed disks	All fixed disks Drive or folder Memory		
			Stop
Add	Remove	Edit	Reset to Defau
Scan options]		Save as Default
 Include subfolde Scan boot secto 	rs r(s)		Schedule
			Help

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.

	epons	ОК
	Cancel	
What to scan		Apply
O Default + additional file types (0)	Additions	Scan Now
Also scan for macro viruses in all files		Stop
Specified file types (0)	Specified	Beset to Defaul
What not to scan Exclude disks, files, and folders (0)	Exclusions	Save as Default
Compressed files	Schedule	
Compressed mes	Help	
✓ Scan inside archives (e.gZIP)		

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.**

Where Detection Ad	vanced Actions Reports	
Specify adva	ОК	
V		Cancel
Find unknown pro	gram viruses	Apply
Find unknown ma	cro viruses	Scan Now
Find potentially un	wanted programs	Stop
Letter I Find joke progra	ams	Reset to Defau
CPU utilization	100%	Save as Default
Missellanasus	() (() () ()	Schedule
Scan files that have	ve been migrated to storage	Help
🔲 Rescan all files wi	nen DAT files are updated	
	1078	

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**.

Schee	lule					
Q 3	Schedu Weekl	ile Task: y	ŀ	Start 12:45	Time:	 UTC Time Local Time
□ E I R Sche	nable rando un missed I dule Task V	omization: [task Weekly	in hou Del	rs 15 📩 ay missed ta	minutes ask by: 15	i initiation minutes
E	very: 1	we	ek(s) on	□ Mon □ Tue ▼ Wed	☐ Fri ☐ Sat ☐ Sur	1
				🗖 Thu		

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.

Constant Con	sole - BARNAB pols Help	AS			
	~	<u>*</u>	V 🕈 🗅 🗳 🗱	Þ 🔳 👫 🖪 🐉	
Task		Status		Last result	
V On-Access Scan AutoUpdate E-mail Scan		Enabled Daily, 12:1 Enabled	5 PM	The Update succeeded.	
Scan All Fixed Di	Start		2:45 PM	No viruses were found.	
-	Copy Delete Rename	Ctrl+C Del F2			
Starts the selected ta	Statistics View Log				
1	Properties				

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.

🌠 VirusScan Scan Help	On-Dema	and Scan	Progress - Sc	an All Fixe	ed Disks		<u>_ ×</u>
			= 🔎				
Scanning in:	C:\Docun	nents and	Settings\Admini	strator\Loca	al Settings\	Temporary Inte	ernet Files\Content.IE
File:	mm_menu	4[2].js					
Scanning files				Scanned:	: 388		

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.

Specify where scal	nning will take place.	Save As
%		Cancel
ltem name	Туре	Apply
All Local Drives	Drive or folder	
Memory of running proc	esses Memory	Scan Now
		Stop
Add	Remove Edit	Reset to Defau
		Save as Defaul
can options		
can options Include subfolders Scan boot sector(s)		Schedule

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

Edit Scan Item	<u>?</u> ×
Item to scan:	
All local drives	•
My computer All local drives All fixed disks All removable media All network drives Memory of running processes User's home folder User's profile folder Drive or folder File	

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..

Select Item To Scan		Where Detection
Desktop Ocuments Over the second secon		Specif
Competent Silv Floppy (A:) Local Disk (C:) Local Disk (D:) Removable Disk (E:)		Memory of
		Add
		Scan boot s
ОК	Cancel	

Specify where scanning	will take place.	Save As
/ >		Cancel
tem name	Туре	Apply
Memory of running processes	Memory	Scan Now
Add Rem	ove Edit	Reset to Default
can options		Save as Default.
Include subfolders Scan boot sector(s)		Schedule
		Help

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.

VirusScan Console - BARNA Task Edit View Tools Help	BAS	
	🏼 🕹 😻 💣 🖻 🖴 🗶	Þ 🔳 🔥 🗓 🐉
Task	Status	Last result
On-Access Scan AutoUpdate E-mail Scan	Enabled Daily, 12:15 PM Enabled	The Update succeeded.
Scan All Fixed Dicks	Weekly, 12:45 PM Not scheduled	No viruses were found.
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)	On-Delivery Scan Properties - BARNABAS 🛛 👔 🗙
	Detection Advanced Actions Alerts Reports
Note: VirusScan Enterprise scans for e-mail viruses	Configure warnings that an infected e-mail message has been detected.
when using Microsoft Outlook only.	Email alert Return reply mail to sender Configure
1. Open VirusScan Console. Highlight E-mail	Send alert mail to user
Scan and click Properties.	If 'Prompt for Action' is selected U Display custom message U Sound audible alert
On-Delivery Scan Properties - BARNABAS	McAfee Vshield: Virus found in e-mail attachment
Detection Advanced Actions Alerts Reports Specify on-delivery scanning of e-mail Scanning of e-mail Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning of e-mail Image: Scanning o-mail Image: Scanning of e-mail Image: Scanning o-mail Image: Scanning o-mail Image: Scanning of e-mail Image: Sc	DK Cancel Apply Help On-Delivery Scan Properties - BARNABAS ? × Detection Advanced Actions Aletts Reports Detected. Specify how e-mail Scan will respond when a virus is detected. When infected attachments found Clean infected attachments ✓ Scan will attempt to automatically clean an infected attachment upon virus detection.
OK Cancel Apply Help 2. In the Detection tab, check Enable Microsoft Exchange (MAPI, IMAP).	if the above Action fails: Move infected attachments to a folder Folder: Quarantine
E-mail Scan Settings in Advanced, Actions, Alerts and Reports Tabs	OK Cancel Apply Help

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).

	On-Delivery Scan Properties - BARNABAS	
	Detection Advanced Actions Alerts Reports	
	Specify advanced e-mail scan options.	
	Heuristics	
	Find unknown program viruses Find unknown macro viruses	
	Indiatachments with multiple extensions	
	 Find potentially unwanted programs Find joke programs 	
	Compressed files	
	 ✓ Scan inside packed executables (e.g. UPX) ✓ Scan inside archives (e.g. ZIP) ✓ Decode MIME encoded files 	
McAfee VirusScan Ent	E-mail message body ♥ Scan e-mail message body	Page 21
	OK Cancel Apply Help	

etection Advanced Actions Alerts Reports	
Configure the E-mail Scan activity log.	
Log file	
✓ Log to file:	
%ALLUSERSPROFILE%\Application Data\Network As	sociates
Limit size of log file to 1 😂 megabytes Brow	wse
What to log	
Session settings	
Session summary	
☑ Date and time	
User name	

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:

\$ }	Message : VirusSo Date and Time : 7/31/20 Pathname : C:\Docu Detected As: EICAR t State : Moved (e VirusSca	Clean File					
			7/31/2003 C:\Docume	7/31/2003 11:01:20 PM C\Documents and Settings\iocelun\Deskton\Temp\eicar.com					
			EICAR test Moved (Cle	t file ean failed because the file isn't cleanable)				Remove Message	
Name		In Folde	er	Detected As		Status	Date and Time	Close Windo	W Use
🛃 eicar	r.com	C:\Doc	uments a	EICAR test file	Virus (Test)	Moved (Cl	7/31/2003 11	notepad.exe	KO/

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.

	VirueScan	Appendix								
-	Vitus/Califiersage Message : VirusScan Alert! Date and Time : 7/14/2003 4:41:07 PM Pathname : A:\Pretty Park.exe Detected As: W32/Pretty.gen@MM State : No Action Taken (Move failed)							lean File elete File		
			7/14/2003 4:41:07 PM							loue File
			A:\Pretty Park.exe							iove File
			W32/Pretty.gen@MM						<u>R</u> emo	we Message
			No A	ction Taken (Move failed)					Clos	e <u>W</u> indow
lame		In Fol	lder	Detected As	Detection Type	Status	Date and Time	Application	Username	Client ID
Pret	ty Park.exe	A:		W32/Pretty.gen@MM	Virus	No Action Taken (Move failed)	7/14/2003 4:41:07 PM	explorer.exe	mycomp\joe	0.0

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.

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	Netshield for							
higher.	Netware							

Appendix A VirusScan Version by Operating System

*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 <u>help@hawaii.edu</u>.

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

For VirusScan Enterprise FAQs, go to <u>http://www.nai.com/us/support/technical_support</u>. 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.