

#### WIN1037

January 2007

University of Hawai'i

# Using McAfee VirusScan Enterprise 8.5i

Jocelyn Kasamoto

Introduction	1
Product Overview	2
System Requirements	4
Where to Get the Software	4
Installation Instructions	5
Which Version of VirusScan am I Running?	8
Launching VirusScan Console	
Configuring On-Access Scanner Properties	9
Viewing the AutoUpdate Repository List	
Configuring AutoUpdate Task	
How to Manually Update DATs	
Configuring Full Scan Task	14
How to Scan for Threats	
Configuring On-Delivery E-mail Scanner	19
Access Protection – Anti-Virus Standard Protection	
Access Protection – Common Standard Protection	
Buffer Overflow Protection	
Unwanted Programs Policy	
Quarantine Manager	
I Found a Virus, Now What?	
Troubleshooting	
Appendix A VirusScan Version by Operating System	
For More Information	

## 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, peer-to-peer filesharing, IRC chat file downloads and browsing infected web sites. 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 daily and scan your hard drive for viruses weekly.** 

Information Technology Services (ITS) has a site license of McAfee VirusScan anti-virus software that active University of Hawai'i (UH) faculty, staff and students may 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, and home computers (one license only) for active UH faculty, staff and students. (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.

UH faculty, staff and students, upon termination of employment or student status at UH, must uninstall all site license copies of McAfee VirusScan and VirusScan Enterprise, per our site license agreement with McAfee. 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 8.5i.

# **Product Overview**

McAfee VirusScan Enterprise (VSE) protects Windows desktops and file servers against viruses, Trojans, worms, potentially unwanted code and programs. VSE is licensed for use on UH owned computers and home computers (one license only) for active UH faculty, staff and students. It supports Windows 2000, Windows XP, Windows Vista and Windows server 2003. It also supports 64-bit Windows.

## New or improved features:

- Support for 64-bit operating systems
  - Buffer overflow protection and scanning of Lotus Notes databases are not supported on 64-bit operating systems.
- Quarantine Manager Policy
  - Before the on-access or on-demand scanner cleans or deletes a file, a backup copy of the original file and its registry value is made in the quarantine directory. The quarantined items can be automatically deleted after a specified number of days or selectively deleted or restored.
- 5100 series scan engine
  - Incremental scan engine updates
  - Two versions of the scan engine, 32-bit and 64-bit
  - Ability to use different sets of detection definition files (DAT) at the same time, providing for faster and more efficient scanning.
- Detection of rootkits in memory
- Enhanced access protection
  - Standard protection level allows installation and execution of legitimate software.
  - Maximum protection level protects most critical settings and files from being modified.

Microsoft Windows Vista (excerpt from VirusScan Enterprise 8.5i readme)

- 1. Before remotely connecting to a computer with the Windows Vista operating system, you must complete these steps:
  - a. From the computer with the Windows Vista operating system, modify the Windows Firewall settings to allow "Remote Service Management" as follows:
    - From the "Start" menu, select "Control Panel | Security | Windows Firewall | Change settings"
    - On the "User Account Control" dialog box, click "Continue."
    - On the "Exception" tab, select "Remote Service Management" on the "Program or port" list.

- b. Start the "Remote Registry" service on the target computer with the Microsoft Windows Vista operating system, before remotely connecting to it. To start the "Remote Registry" service:
  - From the "Start" menu, select "Control Panel | Administrative Tools | Services.
  - If the "User Account Control" dialog box is available, click "Continue."
  - Ensure the status of the "Remote Registry" service is "Started." If necessary, start the service.

We recommend that you stop the "Remote Registry" service on Windows Vista after completing the remote configuration.

2. When using the "Browse" option to connect to a remote console with the Windows Vista operating system, the list of computers does not display for a long period of time or at all. If the list does appear, you can select a computer, but the "OK" button is disabled so the connection cannot be made.

You can make a remote connection to the console of other computers by specifying the full computer name or the IP address of the computer to which you want to remotely connect.

- 3. When running update or mirror tasks from the VirusScan Console on a system using Windows Vista, the task progress dialog box does not display while the task is running. However, the task completes successfully. You can view information about the task in the activity log.
- 4. When a connection is blocked in a share folder on a computer with the Windows Vista operating system, the blocked connection cannot be unblocked using the "Unblock All Connections Now" button in the On-Access Scan Statistics dialog box. The "Unblock All Connections Now" button is disabled in this scenario.

The blocked connection will be unblocked after the default time out.

5. Buffer Overflow Protection is not supported on Microsoft Windows Vista operating systems.

## **System Requirements**

McAfee VirusScan Enterprise 8.5i runs on the following Windows platforms:

#### Workstations

- Windows 2000 Professional with Service Pack 3 or later
- Windows XP Home with Service Pack 1 or later
- Windows XP Professional with Service Pack 1 or later
- Windows XP Tablet PC edition with Service Pack 1 or later
- Windows XP Professional x64 Edition, with Service Pack 1 or later
- Windows Vista

#### Servers

- Windows 2000 server with Service Pack 3 or greater
- Windows server 2003 with Service Pack 1
- Windows Storage 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
- 140 MB of free hard disk space for complete installation with all program features
- 32 MB RAM or more
- 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

Although VSE runs on Windows NT 4.0 SP6 or greater workstation and server, it is strongly advised that Windows NT not be used. Microsoft dropped support for Windows NT on Dec. 31, 2004. Security updates are no longer provided for this operating system.

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.

McAfee VirusScan Enterprise is also available on the ITS CD ROM at the ITS Keller 105 Lab and PC Lab in Keller 213 at UH Mānoa. You must register with your UH username and password to get a copy of the ITS CD ROM. It is strongly recommended that you obtain VirusScan Enterprise on the ITS CD ROM if you have a dial-up connection.

#### **Installation Instructions**

1. Download a copy of McAfee VirusScan Enterprise (**uhvse85.exe**) from http://www.hawaii.edu/antivirus/ and save it to your desktop.

(Or obtain a copy of the ITS CD ROM.)

- 2. Make sure that you are logged in with an account that has administrator privileges. Close all applications.
- 3. If you have an existing anti-virus software (not McAfee VirusScan Enterprise 8.0i), you should uninstall it first. Go to **Start**, **Control Panel**, **Add/Remove Programs**. Select your old anti-virus program and click **Remove**. Make sure that you **restart** your system before proceeding with the installation.
- 4. Double click on the **uhvse85.exe** self-extracting file to extract the contents. It may take awhile to extract the files.

(Insert the ITS CD ROM into your CD ROM drive. Open **My Computer** and select the ITS CD ROM. Double click on the **uhvse85.exe** icon.)

- 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.

Upon termination of employment or student status at UH, you must uninstall all site license copies of McAfee VirusScan Enterprise.

7. **If you have the previous version of McAfee VirusScan Enterprise installed,** the VSE 8.5 installer will detect it. Do **NOT** check **preserve settings.** Click **Next.** 



8. Select **Typical** for Setup Type.

🔀 McAfee VirusScan	i Enterprise Setup 🛛 🔀
	Select Setup Type
<b>McAfee</b> <sup>®</sup>	⊙ Typical
VirusScan <sup>®</sup> Enterprise	Installs the full set of features that includes the Console, On-Access Scanner, E-mail Scanner, On-Demand Scanner, AutoUpdate, Buffer Overflow Protection, and Command Line Scanner. If you are installing to a server, Alert Manager can also be installed.
ver. 8.5/	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.
AntiVirus	
	🖉 Install To
	C:\Program Files\McAfee\VirusScan Enterprise\ Browse
	Disk Space < Back Next > Cancel

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

9. Select Standard Protection for access protection level. Click Next.



10. Click **Install** to begin. Please wait while the VSE installer copies files to your hard drive and updates your registry.

This part takes awhile, especially when McAfee Common Framework is being removed, if you are installing VSE 8.5 over VSE 8.0. Your computer may appear to be hung. Please be patient.

(If you have SpySweeper running, you may get a BHO alert. Click Allow.)

11. VirusScan Enterprise has been successfully installed. Do **NOT** check **Update Now** and **Run On-Demand Scan.** Click **FINISH**.



It is strongly recommended that you manually update your DAT file (if needed) and scan your hard drive after restarting your computer. See *Post Installation Instructions*.

12. At the prompt "Your computer must be restarted to load the new VSE settings", click **Yes.** 

#### **Post Installation Instructions**

- 13. Manually update your scan engine and DAT (if needed) by running **Update Now.** After restarting, please wait until VirusScan has completely loaded (Autoupdate task should appear in VirusScan Console) before running **Update Now**. (See *How to Manually Update DATs* on page 13.)
- 14. Scan your hard drive(s) by running **Full Scan**. (See *How to Scan for Threats* on page 16.)

(If you are running personal firewall software, e.g. ZoneAlarm, you will need to allow access to mcupdate.exe, mcconsol.exe, scan32.exe, and FrameworkService.exe in your personal firewall.)

## Which Version of VirusScan am I Running?

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

🛛 About VirusScan Er	iterprise		
<b>McAfee</b> ®	VirusScan Enterprise Copyright 1995-2006 McAfee, Inc. All R	8.5.0i	VirusScan Version
VirusScan <sup>®</sup>	Anti-virus License Type:	licensed	Scan Engine
	DAT Version: DAT Created On:	4940.0000 January 16 2007	Virus Definitions (DAT)
ver. 8.57	Number of signatures in extra.dat: Names of threats that extra.dat can detect: Buffer Overflow and Access Protection DAT Version:	None None 354	Buffer Overflow
AntiVirus	Installed Patches: Warning: this computer program is protected by copyright law and intern	None ational treaties.	and Access Protection Definitions
	Unauthorized reproduction or distribution of this program, or any portion of penalties, and will be prosecuted to the maximum extent possible under t	of it, may result in severe civil and criminal he law.	Patch Versions
		ОК	

You are running VirusScan Enterprise version 8.5.0i with virus definitions (DAT) 4940.0000, 32-bit scan engine 5100.0194 and no installed patches. Buffer overflow and access protection DAT version is 354. You will need this information when calling the ITS Help Desk for assistance with VirusScan Enterprise.

If you are running 64-bit Windows, the 64-bit scan engine version will be installed. Incremental updates of the scan engine are allowed with the 5100 scan engine series (32-bit and 64-bit).

## Launching VirusScan Console

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

Right click on the icon with a red Vshield icon **VirusScan Console**.

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



🐚 VirusScan Console			
Task Edit View Tools Help			
🖆 🕨 🔳 🛍 🛍 🗱 🦓 🕓	杨 🖭 🕅		
Task	Status	Last Result	Last Run
Second Protection	Enabled		
Buffer Overflow Protection	Enabled		
🖃 On-Delivery E-mail Scanner	Enabled		
Unwanted Programs Policy	8 unwanted progra		
😻 On-Access Scanner	Enabled		
🛞 Quarantine Manager Policy	The quarantine fold		
🔯 Full Scan	Weekly	Nothing found	Wednesday, Januar
📳 AutoUpdate	Daily, 10:45 AM	The Update succeeded	Friday, January 19,
<	111		) <b>&gt;</b>
VirusScan Console			

VirusScan Console comes with eight tasks by default: Access Protection, Buffer Overflow Protection (not in 64-bit Windows or Vista), On-Delivery E-mail Scanner, Unwanted Programs Policy, On-Access Scanner, Quarantine Manager Policy, Full Scan, and AutoUpdate.

Other tasks such as specialized on-demand scans may be added to VirusScan Console.

## **Configuring On-Access Scanner Properties**

On-access scanner 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, double click on the **On-Access Scanner** task.

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.)

General Settings	Scan         Ø Boot sectors
Settings	Scan Boot sectors
	E boor socials
	Floppy during shutdown
All	General
ocesses	Enable on-access scanning at system startup
	Scan time
	Maximum archive scan time (seconds): 15
	Enforce a maximum scanning time for all files
	Maximum scan time (seconds): 45
	Maximum scanning time for all files     Maximum scan time (seconds):

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.

-	Processes Detection Advanced Actions Unwanted Programs
eneral ettings	Specify what items will be scanned.
	When writing to disk
	When reading from disk
Cesses	) (hat to coop
	<ul> <li>✓ All files</li> </ul>
	<ul> <li>Default + additional file types (0)</li> </ul>
	Additions.
	Also scan for macros in all files
	Specified file types (0)
	Specified
	What not to scan
	Exclude disks, files, and folders (0)
	Exclusions

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.

If the default scan all files slows down the performance of your computer too much, you may select scan **Default + additional file types**. Add the **TX?** file extension to the default file extensions list and check **Also scan for macro viruses in all files**. This scan setting is recommended to allow sufficient anti-virus protection without noticeable degradation in system performance.

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



All options are checked.

VSE will scan for potentially unwanted programs, such as adware and spyware (which are not viruses). If these programs are detected, VSE will automatically attempt to clean the file; if it fails, the file will be automatically deleted.

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

## Viewing the AutoUpdate Repository List

VSE has been pre-configured to check repositories at UH and NAI for available updates. Repositories are FTP or HTTP sites. The AutoUpdate task in VirusScan 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, NAI HTTP, and NAI FTP sites. **You do not need to make any changes in the pre-configured 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. All repositories should be checked and enabled.

Repositories Proxy settings	Ory List	
Repository Description	State Enabled Enabled Enabled	Add Edit Delete Move up
		Move down
	OK Can	cel Help

5. Highlight the name of the repository and click on the **Edit** button. Click **OK** when done.

## **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 repositories to manually check for available updates. If updates are available, they will be automatically downloaded and installed.

🕵 McAfee AutoUp	date Properties - AutoUpdate	
AutoUpdate on this com	e tasks update DAT files and scan engines for all McAfee p puter.	products
%DEFLOGDIR%\	UpdateLog.txt Browse.	
Format:	Unicode (UTF8)	
Get newer dete Get newer dete Get other avail Get other avail Update Options Enter the executat Guny run after s	ection definition files if available ection engine and dats if available able updates (service packs, upgrades, etc.) ole to be run after the Update has completed: Browse. uccessful update	
C	Schedule Update	Now

## To Schedule AutoUpdates

For the best protection, AutoUpdates should be scheduled **daily** (recommended setting).

In VirusScan Autoupdate Properties, click on the **Schedule** button. In the Task tab, ensure that **Enable (scheduled task runs at specified time)** is checked. Click on the **Schedule** tab.

- Select **Daily** and time of day specifying a.m. or p.m.
- If your computer is not on most of the time (e.g. laptop), use **At Startup** or **At Logon** options.

The pre-configured schedule for AutoUpdate is set to **daily** at 10:45 a.m. with one hour randomization (connections to the repositories are varied up to one hour, spreading out the load on the update servers.).

sk	Schedule		
R	Run task:	Start Time:	
¢	Daily 🔽	10:45 📶 🔶	OUTC Time
			📀 Local Time
Ena	ble randomization:	1 🚺 Hours	
		0 Minute	*
<b>7</b> D	. Y	· · · · · · · · · · · · · · · · · · ·	•
g nur Dei	n ir missed Iau missed task hu:	5 Minute	s
Cale	al da Taali Dailu		•
Ever	y 1 🛟 Days		
			Advanced

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

Adjust the time to run the AutoUpdate task to meet your needs. **Daily** updating is recommended since McAfee routinely updates DATs daily but more frequently during virus outbreaks.

## How to Manually Update DATs

There are several ways to manually update your scan engine and DAT files.

• Right click on the red Vshield Vicon in the system tray and click on Update Now on the popup menu.

VirusS	can Console
Disable	e On-Access Scan
On-Ac	cess Scan Properties
On-A	ccess Scan Statistics
On-Ac	cess Scan Messages
On-De	mand Scan
Updati	e Now
About	VirusScan Enterprise

- Open VirusScan Console. Do one of the following:
  - 1. Highlight the **AutoUpdate** task. Click the green triangle start icon in the VirusScan Console toolbar.
  - 2. Right click on the AutoUpdate task and click Start in the popup menu.
  - 3. Right click on the AutoUpdate task, click Properties. Click Update Now.

VSE will check the UH repository 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 Full Scan Task**

The **Full Scan** 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 **Full Scan** task and click on **Properties**. Ensure that the Item name is set to **All local drives**.

nere Detection Advanced	Actions Un	wanted Programs	Heports	
Specify where scann	ing takes place.			Cancel
~				Apply
Item name	Тур	e	_	Start
Memory for rootkits	Men	iory ioru		
All local drives	Loca	al drives		Reset to Defa
	200			Save as Defa
Add	Edit	Remove		Schedule
Scan options				[ 1146
Include subfolders				Неір
🗹 Scan boot sectors				

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** and **Decode MIME encoded files** are also checked for added protection.

/here	Detection	Advanced	Actions	Unwanted Progra	ams	Reports	ОК
Specify which items are scanned.						Cancel	
							Apply
Wha	at to scan — Il files						
OD	in nies Iefault + addi	tional file type	es (0)			Valatitions -	Start
- -	Also scan	for macros in	all files			AGUICIONS	Reset to Defa
OS	pecified file t	ypes (0)			ç	pecified	Save as Defa
Wha	at not to scar						Schedule
Exclu	ude disks, file	es, and folder	s (O)		E	xclusions	
~	12						Help
Lom	pressed files Scan inside a	archives (for e	xample, Z	IP)			
	Decode MIM	E encoded fi	les				

- 3. Click on the **Advanced** tab. Both options under Heuristics should be checked.
- 4. Click on the **Unwanted Programs** tab.

**Detect unwanted programs** is 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 deleted if it can't be cleaned.

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



## **To Schedule Full Scan**

- 1. Open VirusScan Console. Right click on the **Full Scan** 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 3:00 p.m. Make adjustments to day or time, if needed. Click on **Apply** and **OK**.

medule settings		
Task Schedule Run task:	Star	t Time: 00 PM 🔹 🔿 UTC Time 📀 Local Time
Enable randomization	0	Hours
Run if missed Delay missed task by Schedule Task Weekly	5	Minutes
Every:	1 🛟 Weeks	
Monday Thursday Sunday	🔲 Tuesday 🛄 Friday	☑ Wednesday □ Saturday
		Advanced
	K Cancel	Apply Help

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

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

## How to Scan for Threats

Threats are viruses and any unwanted programs specified in Unwanted Programs Policy (spyware, adware, key loggers, etc.)

## Scan a File or Folder

To quickly scan a file or folder, right click on the file (or folder) and click **Scan for threats** on the pop-up menu.

	Open	
	Explore	
3	Search	
	Sharing and Security	
9	SnagIt	•
V	Scan for threats	
ą	WinZip	•
0	Sweep with Spy Sweeper (TM)	
	Send To	ł
	Cut	
	Сору	
	Paste	
	Create Shortcut	
	Delete	
	Rename	
	Properties	

## **Full Scan**

Open VirusScan Console. Right click on Full Scan task and select Start.

🐚 VirusSc	an Console			
Task Edit	View Tools Help			
🔮 🕨 🛛	🗉 🗈 🗰 🕹	» 🖪 🕺 🗶 🕅		
Task		Status	Last Result	Last Run
Access P     Buffer O     On-Delive     On-Acces     Quaranti     Full Sca     AutoUp	rotection verflow Protection ery E-mail Scanner ed Programs Policy ss Scanner ine Manager Policy Start Copy Delete	Enabled Enabled Enabled 8 unwanted progra Enabled The quarantine fold Weekly Daily, 10:45 AM	Nothing found The Update succeeded	Wednesday, Januar Friday, January 19,
Start the O	Rename Statistics View Log Properties			

The scan task will start to scan all your local drives. 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.

ere Detection Advanced Action	ns Unwanted Programs Re	ports Save A
Specify where scanning take	s place.	Cance
tem name	Туре	
Memory for rootkits     Neurning processes     All local drives	Memory Memory Local drives	Reset to D Save as D
Add Edit Can options Include subfolders CScan boot sectors	Remove	Schedul Help

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 **Start** to start the scan.

nere Detection Advanced	Actions	Unwanted Programs	Reports	Save As
Specify where scann	iing takes pl	ace.		Cancel
(Juli				Apply
Item name		Туре		Start
Memory for rootkits		Memory Memory		ordir
C:\		Fixed drive		Reset to Defa
				Save as Defa
Add	Edit	Remove		Schedule.
Scan options				Help
Include subfolders           Scan boot sectors         Include subfolders				

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 Full Scan Task") if you scan this location routinely.

# **Configuring On-Delivery E-mail Scanner**

VirusScan Enterprise automatically scans e-mail messages and attachments for Microsoft Outlook and Lotus Notes only. It scans on-delivery for Microsoft Outlook and on-access for Lotus Notes. It does scan e-mail attachments as you download or save them in other POP3 e-mail clients, such as Eudora.

If you do not use Microsoft Outlook or Lotus Notes, disable On-Delivery E-mail Scanner. In VirusScan Console, right click on On-Delivery E-mail Scanner and click Disable.

- 1. Open VirusScan Console. Right click **On-Delivery E-mail Scanner** and click **Properties.**
- 2. In the **Detection** tab, ensure that **all file types** are checked so all e-mail attachments will be scanned for viruses.

The settings in the Actions, Alerts, and Reports tabs should be left at default.

## E-mail Scan Settings - Actions Tab



When a virus is detected, the default action taken by VirusScan is to attempt to clean the file. If cleaning fails, the file is renamed with a .vir extension and moved to quarantine in the c:\quarantine folder. You may inspect the quarantined file and delete it if not needed. Normally, you would delete the infected file. VSE 8.5i has new access protection rules separate for anti-virus (standard, maximum, outbreak), common protection (standard, maximum), and user-defined categories. Open VirusScan Console. Right click on **Access Protection** and click **Properties**.

specified ports, files, nges, lock down sha fanager and ePolicy stive code from acce	folders, and s rres, files, and Orchestrator sssing the cor	shares. This can be critical both before and during outbreaks. I directories to read-only, block the execution of a specific events when attempts are made to access blocked items. If nputer until a DAT file is released. You can also prevent
Block	Report	Rules
1	4	Prevent registry editor and Task Manager from being disable Prevent user rights policies from being altered Prevent remote creation/modification of executable and co Prevent remote creation of autorun files Prevent hijacking of EXE and other executable extensions
<b>▼</b>	4	Prevent Windows Process spooring Prevent mass mailing worms from sending mail Prevent IRC communication Prevent use of the see
<		
>		Edit Delete New
ped		
	specified ports, files, nges, lock down sha lanager and ePolicy tive code from acce	specified ports, files, folders, and rges, lock down shares, files, and lanager and ePolicy Dichestitator tive code from accessing the cor

Under Anti-virus Standard Protection, the rule Prevent mass mailing worms from sending mail blocks outbound SMTP email traffic on port 25 to block mass mailing viruses, such as Bagle and Netsky, from mass mailing from your workstation. A list of legitimate e-mail clients and mail agents, such as Eudora, Outlook, Netscape, and others, are excluded. The default exclusions include the following:

agent.exe	amgrsrvc.exe	apache.exe
ebs.exe	eudora.exe	explorer.exe
firefox.exe	firesvc.exe	iexplore.exe
inetinfo.exe	mailscan.exe	MAPISP32.exe
modulewrapper*	mozilla.exe	msexcimc.exe
msimn.exe	mskdetct.exe	msksrvr.exe
msn6.exe	msnmsgr.exe	neo20.exe
netscp.exe	netscp6.exe	nlnotes.exe
nrouter.exe	nsmtp.exe	ntaskldr.exe
opera.exe	outlook.exe	Owstimer.exe
pine.exe	poco.exe	RESRCMON.EXE
rpcserv.exe	SPSNotific*	thebat.exe
thunde*.exe	tomcat.exe	tomcat5.exe
tomcat5w.exe	VMIMB.EXE	webproxy.exe
WinMail.exe	winpm-32.exe	

If your email client is not included in the default list of exclusions, you may add it by:

- 1. Click Prevent mass mailing worms from sending mail to select it and click Edit.
- 2. In the **Processes to exclude** box, at the end of the list of executables, enter "**,testmail.exe**" (no quotes; don't forget the comma) where testmail.exe is your email client's executable file name. Click **OK**.
- 3. In the Access Protection tab, click **Apply** and **OK**.

## Access Protection – Common Standard Protection

Under Common Standard Protection, the rule Prevent common programs from running files from the Temp folder may be modified if you find it too restrictive.

Access Protection Reports Access Protection Rules Prevent intrusions by restricting access to You can block access to potts and port ra file, and generate log entries and/or Alert h an outbreak occurs, you can block destru McAlee processes from being terminated.	specified ports, files, nges, lock down sha Aanager and ePolicy ctive code from acco	folders, and s ares, files, and Orchestrator essing the cor	shares. This can be critical both before and during outbreaks. I directories to read-only, block the execution of a specific events when attempts are made to access blocked items. If mputer until a DAT file is released. You can also prevent
Enable Access Protection     Categories	Block	Benort	Bules
Anti-virus Standard Protection Anti-virus Maximum Protection Anti-virus Outbreak Control Common Standard Protection Common Maximum Protection User-defined Rules		4	Prevent modification of McAfee files and settings Prevent modification of McAfee Common Management Age Prevent modification of McAfee Scan Engine files and setti Protect Mozilla & Firef ox files and settings Protect Internet Explorer settings Prevent installation of Browser Helper Objects and Shell Ex Protect network settings Prevent common programs from running files from the Temp Prevent termination of McAfee processes
Prevent McAfee services from being stop	ped		Edit Delete New

- 1. Click on **Prevent common programs from running files from the Temp folder** to select and click **Edit**.
- 2. In the **Processes to include** box, at the end of the list of executables, enter "**,testmail.exe**" (no quotes; don't forget the comma) where testmail.exe is your application's executable file name. Click **OK**.
- 3. In the Access Protection tab, click **Apply** and **OK**.

When an access protection violation occurs, the red vshield system tray icon temporarily changes to one with red brackets around it. To reset the icon, open the Access Protection Activity Log from the system tray icon.

## **Buffer Overflow Protection**

VSE 8.5i has buffer overflow protection capabilities (not supported in Windows Vista and 64-bit Windows). Open VirusScan Console. Right click on **Buffer Overflow Protection** and click **Properties**. Ensure that **Enable buffer overflow protection** and **Show the messages dialog box when a buffer overflow is detected** are checked.

ther Overflow Protection	Reports			
Buffer overflow pr code on your com	otection prevents iputer.	exploited app	lications from (	executing arbitrar
Enable buffer overflor	w protection			
🔘 Warning mode				
Protection mode				
Show the messages (	fialog box when a	buffer overflo	w is detected	
Buffer overflow exclusion	IS			
Buffer overflow exclusion Process	15			
Buffer overflow exclusion Process	15			
Buffer overflow exclusion Process	8			
Buffer overflow exclusion Process	8		1	
Buffer overflow exclusion Process	15			
Buffer overflow exclusion Process Add	is Ed	it	Remov	e
Buffer overflow exclusion Process	15			

Some software may conflict with VirusScan's buffer overflow protection. In that case, disable buffer overflow protection. First, uncheck **show the messages dialog box when a buffer overflow is detected**. Then uncheck **enable buffer overflow protection**.

## **Unwanted Programs Policy**

Open VirusScan Console. Right click on **Unwanted Programs Policy** and click **Properties**. On the **Detection** tab, all categories should be checked in the UH pre-configured settings. Clear any unwanted program categories that you don't want to detect. Click **OK**.

Unwant	ed Programs Policy
Detection	User-Defined Detection
	nwanted programs policy allows you to configure categories of nwanted programs to detect in your environment. This policy ust be enabled here and in each scanner individually.
Detection	ons from DATs
These a	re the categories of detections that are in the DATs.
V Ad V Re V Di V Pa V Jo V Ct	ware mote Administration Tools alers ssword Crackers xee y Loggers ner Potentially Unwanted Programs
Unwant	ed program exclusions
Don't de	tect specified detections (0) Exclusions

## **Quarantine Manager**

Quarantine Manager is a new feature in VirusScan Enterprise 8.5i. To access Quarantine Manager, open VirusScan Console. Right click on **Quarantine Manager Policy** task and click **Properties**.

Before On-access or On-demand scanners in VirusScan Enterprise clean or delete a file, it makes a backup copy of the original file in the quarantine folder. The default quarantine folder is c:\quarantine. The default policy is to automatically delete quarantined data after 28 days. You may modify the policy to your liking.

N		
blicy Manager		
Before the On-Access or On- in the quarantine folder. Thes automatically deleted after a	Demand scanner cleans or deletes a file, it creates a backup copy of the original fil se backed-up items can be rescanned, checked for false positives, restored, and specified number of days.	le
Quarantine Folder		
C:\QUARANTINE\		
	Reauro	
	Diovise	
Automatically delete quarantined	data	
Automatically delete quarantined	data p data in the guarantine folder	
Automatically delete quarantined Number of days to keep backed-up	data o data in the quarantine folder	
Automatically delete quarantined Number of days to keep backed-up 28	data o data in the quarantine folder	
Automatically delete quarantined Number of days to keep backed-up 28	i data o data in the quarantine folder	
Automatically delete quarantined Number of days to keep backed-up 28	data o data in the quarantine folder	
Automatically delete quarantined Number of days to keep backed-up     28     2	data o data in the quarantine folder	
Automatically delete quarantined Number of days to keep backed-up 28	data o data in the quarantine folder	
Automatically delete quarantined Number of days to keep backed-up 28	data p data in the quarantine folder	
Automatically delete quarantined Number of days to keep backed-up 28	data in the quarantine folder	
Automatically delete quarantined Number of days to keep backed-up 28	data in the quarantine folder	

In the Manager tab, you can manage (restore, check for false positive, rescan, delete) quarantined data. Right click on the quarantined entry and select the desired option. Click **Apply** and **OK**.

properties.		check for raise positive, r	estore, delete, or view		
Time Quarantined	Detection Type	Detected as	Number of obie	DAT Version	Engin
1/17/2007 1:04 PM 1/17/2007 1:07 PM 1/17/2007 1:08 PM 1/17/2007 1:09 PM	Test Test Test Test	EICAR test file EICAR test file EICAR test file EICAR test file	1 1 1	4941.0000 4941.0000 4941.0000 4941.0000	5100.0 5100.0 5100.0 5100.0
1/5/2007 5:40 PM	Test Re: Chi Re: Del Pro	scan eck for false positive store ete perties	2	4933.0000	5100.0 5100.0

## I Found a Virus, Now What?

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

	Message							
4	<u>M</u> essage :	VirusScan Alert!					<u>C</u> lean File	
30	Date and <u>T</u> ime :	1/17/2	007 1:04:12 PM			× 1	Delete <u>F</u> ile	
	<u>N</u> ame :	C:\Doc	uments and Settings	uments and Settings\jocelyn\Local Settings\Temp\8hzgp5ln.com				
	Detected As:	EICAR	test file					
	<u>S</u> tate :	Deleted	l (Clean failed becau	use the detection isn't cl	eanable)	ſ	Close <u>W</u> indow	
lame	In Fol	der	Source	Detected As	Detection Type	Status	Date and Time	
8hzg	gp5ln.com C:\Do	cuments a	a	EICAR test file	Test	Deleted (.	1/17/2007 1:	

Note: eicar is not a true virus. Upon detection, VSE on-access scanner made a backup of the original file in the quarantine folder (c:\quarantine). Then VSE tried to clean the virus but couldn't so the infected file was deleted.

For help with virus clean up, we need to know the name of the virus. Please write down the name of the virus detection.

Both on-access scanner and on-demand scanner are configured to attempt cleaning the file first; if that fails, the file will be deleted. If you discover that VirusScan deleted a legitimate file by mistake, go to Quarantine Manager to restore it from the quarantine folder.

Here is another example of a virus detection when the user attempted to save an email attachment infected with the W32/SirCam@MM virus.

🦻 On-Access Scan Messages								
File Vi	ew Options Help	5						
1	Message							
	Message :	VirusSca	n Alert!				Clean File	
25							Delete File	
~	Date and Time :	te and Time : 1/19/2007 6:52:13 PM						
	Name :	C:\DOCU	MENTS AND SETTINGS JOCELYN \DESKTOP \ADVANCED.XLS.P				Remove Message	
	Detected As: W32/SirC		am@MM					
	State :	Deleted					Close Window	
Name	In Fol	der	Source	Detected As	Detection Type	Status	Date and Time	
ADV ADV	ANCED C:\DC	CUMENT		W32/SirCam	Virus	Deleted	1/19/2007 6: 0	
<			1007			j.	>	

In this case, it is known that W32/SirCam@MM is a virus and the infected file can be deleted. Open Quarantine Manager and delete the infected file from the quarantine folder.

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) and emptied your Recycle Bin, rerun VirusScan with the scan all files option once more to ensure that your system is clean.

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.

## Troubleshooting

- **Q:** While checking for an update for VirusScan, I get this message: "Error occurred while downloading file SiteStat.xml." What does that error mean?
- A: It usually means that there is a problem connecting to the repository (server) for DAT updates. Some possible items to check:
  - 1. Is your network connection working properly? Can you get to other sites via a web browser? (If yes, your network connection is ok.) If on the campus wireless, are you properly logged in to the wireless network?

- 2. Do you have a personal firewall that might be blocking access to the server? (If you disabled your personal firewall program, are you then able to update your DAT files?)
- 3. It might be due to many people accessing the server and trying to update their files at the same time. Try again in 15 minutes.
- Q: After installing VSE 8.5i, one of my programs stopped working properly. What should I do?
- A: There may be a conflict with VSE 8.5i's buffer overflow protection. To disable buffer overflow protection, open VirusScan Console. Double click on Buffer Overflow Protection, clear Show the messages dialog box when a buffer overflow is detected then clear Enable buffer overflow protection. Please clear the check boxes in this order. Click Apply and OK. Buffer Overflow Protection should be Disabled in VirusScan Console. If this does not resolve your problem, contact the ITS Help Desk at 956-8883 or email help@hawaii.edu.
- **Q:** I've noticed McAfee VirusScan is not autoupdating. I am running MS Windows XP SP2. How do I fix this?
- A: Please check to see if you are running the Windows XP SP2 firewall. To disable the firewall:
  - 1. Click Start.
  - 2. Click on Control Panel.
  - 3. Double-click on **Security Center**.
  - 4. Click on the **Windows Firewall** link.
  - 5. Check Off.
  - 6. Click OK.
- Q: I got error message: "Failed to initiate Common Updater subsystem. Make sure the McAfee Framework Services is running. McAfee Common Framework returned error fffff95b@2" after I clicked on **Update Now** from the vshield system tray icon. I had just installed VirusScan Enterprise 8.5i and restarted Windows. What does this mean?
- A: VirusScan Enterprise 8.5i may take awhile to load completely during startup. Open VirusScan Console and ensure that the Autoupdate task is listed. If the Autoupdate task is not listed, please wait until it appears. If Autoupdate task is listed, run **Update Now** from the vshield system tray icon or right click Autoupdate in VirusScan Console and click **Start**.

More McAfee VirusScan tips are available in Ask Us at http://www.hawaii.edu/askus/.

Appendix A	VirusScan	Version	by Op	erating Sy	stem
------------	-----------	---------	-------	------------	------

Faculty/Staff							
OS	Campus	Home Use	Students	Affiliates			
Win2K Pro	VSE	VSE	VSE	VSHE			
WinXP Home	VSE	VSE	VSE	VSHE			
WinXP Pro	VSE	VSE	VSE	VSHE			
Win Vista	VSE 8.5 or higher	VSE 8.5 or higher	VSE 8.5 or higher				
Win 64-bit	VSE 8.5 or higher	VSE 8.5 or higher	VSE 8.5 or higher				
Servers							
Win2K	VSE						
Win 2003 Netware 4 and higher	VSE Netshield for Netware						

VSE = VirusScan Enterprise, VSHE = VirusScan Home Edition

## **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.aspx</u> and specify the virus name in the search box.

For VirusScan Enterprise FAQs, go to

<u>http://knowledge.mcafee.com/SupportSite/supportcentral/supportcentral.do?id=m1</u>. In the Product menu box, select VirusScan Enterprise. For type of content, select FAQs. Enter search keywords and click on the **Search** button.

VirusScan has a built-in help file. Open VirusScan Console. Click **Help, Help Topics**. You may need to install the help file the first time you use it.

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.