Using McAfee VirusScan Home Edition 8.0 for Windows

Jocelyn Kasamoto

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 or chat channels. 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, students and affiliates can use at no extra charge on their Windows computers. Active UH faculty, staff, students, and affiliates may use one license of McAfee VirusScan Home Edition on their home computer (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. Active affiliated users include current East West Center (EWC) participants, Research Corporation of the University of Hawai‘i (RCUH) employees, and University of Hawai‘i Foundation (UHF) employees.

Copies of the older site license version of McAfee VirusScan 4.x must be uninstalled from UH computers (exceptions are Windows 98 and Windows ME on UH owned computers). UH faculty, staff, and students, upon termination of employment or student status at UH, and affiliated users, upon termination from UH affiliation, must uninstall all site license copies of McAfee VirusScan, VirusScan Home Edition, and VirusScan Enterprise.
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 software 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 Home Edition 8.0.

Product Overview

VirusScan Home Edition (VSHE) is published by McAfee, Inc. It provides anti-virus protection against viruses, trojans and worms for Windows operating systems. As its name implies, VSHE is intended for home use. It is designed for ease of use with easy point and click options.

VSHE comes with a one-year subscription of free virus definitions and software updates through the ITS site license contract with McAfee. You must register your copy of VSHE (your e-mail address is required for registration) with McAfee in order to get automatic virus definition updates. The virus definition updates for VSHE are obtained directly from McAfee repositories. **Note: you do not need to upgrade to the professional version of VirusScan or purchase a yearly subscription.** Your VirusScan subscription is paid by ITS for the McAfee site license. Please contact the ITS Help Desk if you have questions about the McAfee site license.

Product and DAT updates are obtained automatically through McAfee Security Center or manually through a VirusScan point and click task. You can schedule scan tasks but can not schedule the autoupdating process.

Some VSHE Features

- **New! Email Scanning**
  VirusScan automatically scans inbound (POP3) and outbound (SMTP) email and email attachments for most popular email clients, including Microsoft Outlook, Outlook Express, Netscape Mail, Eudora, Pegasus and others. E-mail scanning is not supported for web-based, IMAP, AOL, POP3 SSL, and Lotus Notes. However, ActiveShield scans e-mail attachments when they are opened.

- **New! Instant Message Scanning**
  VirusScan scans Instant Message attachments sent via AOL Instant Messenger, Yahoo Messenger and Windows Messenger.

- **New! ScriptStopper™**
  Many of the fastest spreading viruses, like I Love You, use scripts to infect your PC. ScriptStopper detects then stops these threats.

- **New! WormStopper™**
  WormStopper stops mass-mailing worms like Sobig by detecting activity that may indicate a new, undetected worm is active on your PC. Like email sent to more than 40 recipients or more than five emails sent in less than 30 seconds.

- **New! Detects Spyware**
  Protecting loss of data and privacy, VirusScan detects potentially malicious desktop applications like spyware, adware, Web dialers and more.
• **New! Windows Explorer integration**
  Access VirusScan directly by selecting files and clicking the VirusScan icon in the Windows Explorer window.

• **New! AutoClean**
  VirusScan automatically attempts to clean virus-infected files when a malicious threat is detected.

• **New! MS Outlook Scanning**
  VirusScan integrates directly on the MS Outlook toolbar for instant, on-demand scanning of older email or folders.

• **New! Silent Updating**
  VirusScan silently updates virus definitions (DATs), without interrupting your work, ensuring your computer is always up-to-date.

• **New! Submit Files to AVERT™**
  VirusScan sends suspicious files directly to the McAfee Antivirus Emergency Response Team (AVERT) for assessment.

• **Virus Map & Information Library**
  See how the latest threats are infecting computers worldwide, then research them via direct links to the McAfee Virus Information Library.

**System Requirements**

McAfee VirusScan Home Edition 8.0 runs on the following operating systems:

- Windows 98
- Windows ME
- Windows 2000 Professional*
- Windows XP Home*
- Windows XP Professional*

Note: VSHE does not support Windows NT workstation. You are strongly advised to migrate to another operating system as Microsoft ended support for Windows NT workstation on June 30, 2004.

*Active UH faculty, staff and students with Windows 2000 Professional, Windows XP Home and Windows XP Professional may install McAfee VirusScan Enterprise (one license only) on their home computer. Affiliated users must install McAfee VirusScan Home Edition, regardless of their operating system.

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

- Internet Explorer 5.5 Service Pack 2 or later
- 61 MB of hard disk space or more
- 32 MB RAM or more
- Intel Pentium class or compatible processor rated 133MHz or higher
- CD-ROM drive
- Internet connection (local area network, broadband or modem connection) for getting updates

You must also have a valid UH username and password to get a copy of the software which is licensed to the University of Hawai‘i. Go to [http://www.hawaii.edu/account](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 Home Edition. Login with your UH username and password. If you have a dial-up connection, it is strongly recommended that you get the anti-virus software on the ITS CD ROM.

McAfee VirusScan Home Edition is also available on the ITS CD ROM at the ITS Keller 105 Lab and PC Lab in Keller 213 at UH Manoa. You must register with your UH username and password to get a copy of the ITS CD ROM.

Installation Instructions

1. Download a copy of McAfee VirusScan Home Edition from http://www.hawaii.edu/antivirus and save it to your desktop or obtain a copy of the ITS CD ROM.

2. **If you have an existing anti-virus package, you must uninstall it first** by going to Start, Settings, Control Panel, Add/Remove Programs. Select McAfee VirusScan or VirusScan (or your non-McAfee anti-virus program) and click on the Remove button. When the anti-virus package has been removed, close all windows and restart your computer.

   **Warning:** If you do not uninstall the existing anti-virus software before installing McAfee VirusScan Home Edition, you will encounter serious problems that may require editing your registry or reinstalling Windows.

3. If you are using Windows 2000 or Windows XP, make sure that you are logged in with an account that has administrator privileges.

4. Double click on the VirusScan HE8026en.exe icon on the desktop.

   (Insert the ITS CD ROM into your CD ROM drive. Open My Computer and select the ITS CD ROM. Double click on the VirusScan HE8026en.exe icon.)

5. In the License Agreement window, select United States in the country pull down menu. Read the license agreement. If you agree to the terms of the license agreement, click Accept. If you decline, you won’t be able to install the software and will need to get another anti-virus software.

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

6. The McAfee VirusScan Installation Wizard opens. Check Create a VirusScan desktop icon if you wish. Click Next.

7. In the Virus Map Reporting window, darken radio button for either Yes, I want to participate or No, I don’t want to participate, depending on whether you wish to anonymously submit virus information to McAfee for tracking on world-wide infection rates.
If you select Yes, fill in your country, state and zip code. Click Next.

8. In the Completing VirusScan Wizard window, click Finish.

When the installation is complete, McAfee Security Center loads and brings up the Product Registration wizard.

Product Registration

9. McAfee automatically checks for updates when you connect to the Internet. If an update is found, it will download and apply the update automatically, if your product is registered. Click Next to continue with registration. If you click Cancel, VirusScan will not be updated automatically when you connect to the Internet.
10. Complete the registration form (all fields are required). The e-mail address needs to be a valid address. Choose a password (do not use the password for your UH username). Click Next.

11. In the McAfee Notification window, check the options you want. It’s recommended that you keep the option Keep me posted on the latest virus threats checked. Click Submit.

If you have a personal firewall, allow McAfee Security HTML dialog, MGHTML.exe.

12. At the Product registration successfully completed window, click Finish.

Note: If you have a personal firewall, allow McAfee Security Center Update Engine, MCUPDATE.exe, and MCINFO.exe to access the Internet. You will also need to allow access to us.mcafee.com in your personal firewall for manual DAT updates.

Getting Updates

13. Open McAfee Security Center by double clicking on the red McAfee Security Center shortcut on your desktop or the red McAfee icon in the system tray in the lower right corner.
14. When you first open McAfee Security Center after installing VSHE, read the information about McAfee Security Center and click **Next**.

15. McAfee Security Center will load. VirusScan installs with an old scan engine and virus definition DAT file. To update your DAT file, click on **Updates** in the upper right panel.

16. Click **Check Now**. Close all other McAfee VirusScan windows and click the **Update** button.

17. You will be prompted to login to McAfee Security. Enter your e-mail address and password that you used to register your product. Uncheck **remember me** (for security reasons) and click **Log In**.

MyAntivirus Index should be 10.0 if VirusScan is up-to-date.
18. You may be prompted to **Install McAfee Security Installer Control**? Click Yes.

![](image)

After the Installer Control is installed, you will need to restart your computer.

19. Right click on the red McAfee icon in the system tray and click **Updates**. Click **Check Now** and **Update**. If any updates are available, they will be downloaded and installed on your computer. When done, close all applications and restart your computer.

![](image)
Which Version of VirusScan am I Running?

Right click on the red McAfee icon in the system tray in the lower right corner of your screen. On the popup menu, point to VirusScan and click About.

You are running VirusScan Home Edition version 8.0, build 8.0.41 with scan engine 4.3.20 and virus definitions (DAT) 4370 created on 6/25/2004. You will need this information when you call the ITS Help Desk for assistance.

Launching McAfee Security Center

McAfee Security Center should load automatically at startup when you boot up Windows. If VirusScan is running and enabled, you should see a red McAfee icon in the system tray. If for some reason, VirusScan is disabled, you will see a black McAfee icon in the system tray.

Open McAfee Security Center by double clicking on the McAfee Security Center shortcut on your desktop or the red McAfee icon in the system tray.

McAfee Security Center is the one-stop security center that allows you to:

- Get free security analysis for your computer.
- Launch, manage, and configure your all your McAfee security subscriptions, including anti-virus, personal firewall, privacy service and spam killer.
- See updated virus alerts and latest product information.
- Receive trial subscriptions to download and install trial versions from McAfee.
- Get quick links to frequently asked questions and account details on the McAfee web site.

The ITS site license provides only McAfee anti-virus software. It is assumed that you only have VirusScan, not other McAfee security products, installed in this document.
Using VirusScan Home Edition

To access a VirusScan feature:

1. Right click on the McAfee icon in the system tray.
2. Point to VirusScan in the main popup menu then click on the feature you want to use in the VirusScan popup menu.

### Getting Updates

VirusScan will automatically check for updates (if you registered your product) when your computer is booted up. If any updates are available, they will be automatically downloaded and installed. You will see a yellow down arrow in the system tray followed by a McAfee web service window. Click Continue what I was doing.
Manually Checking for Updates

To manually check for updates, right click on the red McAfee icon in the system tray and click Updates. In the Security Center Updates window, click Check Now. McAfee Security Center will check for updates. If any updates are available, VirusScan will automatically download and install the updates.

If your McAfee VirusScan is up-to-date, you will get the following message. Click OK.
Configuring VirusScan Options

1. Open McAfee Security Center by double clicking on the red McAfee icon in the system tray. Click on VirusScan icon in the left panel.

3. Click Configure VirusScan Options.

**ActiveShield**

4. In the ActiveShield tab, leave all options checked. Click Advanced.
**ActiveShield** is the on-access scanning component of VirusScan. Whenever a file is accessed by you or the computer (for example, when you read or write a file), ActiveShield scans it for viruses.

**Warning**

VirusScan and ActiveShield are not upgrades from McAfee VirusScan v4.x-7.x and VShield. If you have a previously installed McAfee VirusScan on your computer, you must remove it so ActiveShield runs properly.

Software packages such as McAfee Internet Security, Guard Dog, Nuts & Bolts, First Aid, McAfee Office, and Microsoft Plus! might have versions of McAfee VirusScan bundled with them. You must remove the anti-virus components from these applications before ActiveShield can function properly.

**ActiveShield Advanced Options**

5. It is recommended that you leave ActiveShield scan options at the default setting. If your computer performance degrades significantly, you may select scan **program files and documents only** in the ActiveShield tab. Click **OK**.
These are the default settings for e-mail scan.

If the default e-mail scan settings are used, ActiveShield automatically scans and attempts to clean inbound (POP3) and outbound (SMTP) infected e-mail messages and attachments for the following e-mail clients:

- Microsoft Outlook Express 4.0 or later
- Microsoft Outlook 97 or later
- Netscape Messenger 4.0 or later
- Netscape Mail 6.0 or later
- Eudora Light 3.0 or later
- Eudora Pro 4.0 or later
- Eudora 5.0 or later
- Pegasus 4.0 or later

**Note:** e-mail scanning is not supported for web-based, IMAP, AOL, POP3 SSL and Lotus Notes e-mail clients. ActiveShield doesn’t scan e-mail for the UH mail server (mail.hawaii.edu) which supports IMAP and POP3 SSL e-mail clients. However, ActiveShield does scan e-mail attachments when they are downloaded or opened.

If the inbound e-mail message or attachment is infected, ActiveShield tries the following (for the default settings) in this order:

1. tries to clean the infected e-mail
2. tries to quarantine or delete the uncleanable e-mail
3. includes an alert file in the inbound e-mail with information about actions performed to remove the infection

If the outbound e-mail message or attachment is infected, ActiveShield tries the following (for the default settings) in this order:

1. tries to clean the infected e-mail
2. tries to quarantine or delete the uncleanable e-mail
3. sends an alert file to you in a new e-mail containing information about the actions performed to remove the infection

Choose **Prompt me when an attachment needs to be cleaned** to disable auto-cleaning of infected e-mail, only if needed.
When ActiveShield detects an infected e-mail, you will be prompted with options to clean, quarantine or delete infected e-mail. In general, you should choose to clean first then quarantine or delete uncleanable e-mail. However, if you don’t want the infected e-mail, select delete immediately without trying to clean the e-mail first.

VirusScan scans email attachments as you try to open them or save them to your hard drive. This scanning is done in the background.

**Tip: For best results, don't open email attachments directly from an email message.** Save them to your hard drive first, and then open them. If an attachment contains a virus, VirusScan detects it when you try to save it to your hard drive. A window alerts you about the virus and provides options to handle it.

**ScriptStopper and WormStopper**

These are the default settings for ScriptStopper and WormStopper. You should leave the settings at default unless you have a compelling reason to change them.

7. Click on Virus Map Reporting tab. Select Yes, I want to participate and fill in your country, state and zip code. Otherwise, select No, I don’t want to participate. You may select either option during installation or using this configuration window to change your settings.
8. Click on Scheduled Scan tab. Make sure Scan My computer at a scheduled time is checked to enable automatic scanning. Click Edit.

9. The recommended setting is a weekly scan. Select Weekly. Type in the time that you want the scan to start. Check the day(s) of the week to scan your hard drive. Click OK, Apply and OK.

Note: your computer must be powered on for the scheduled scan to run. Select a day and time when your computer will be powered on.
If you have a shared computer or the computer is used in an environment more susceptible to getting infected, such as in a public computer lab, you should schedule to scan your computer daily.

Note: the schedule tasks **At system startup**, **When idle**, and **Show multiple schedules** are not supported. The last supported scan schedule remains enabled until you select another option from the valid options.

**Manually Scanning for Viruses**

There are several ways to manually scan on-demand for viruses.
- In Windows Explorer
- Run **Scan My Computer for Viruses**.

**Scanning for Viruses in Windows Explorer**

1. Open **My Computer**.
2. Drill down to the drive or folder you wish you scan.
3. Right click on the drive or folder.
4. On the pop-up menu, select **Scan for viruses**. VirusScan scan will automatically start.
5. When the scan is completed, a report of infected files will be displayed. Click **Close** to close the window.

**Scanning My Computer for Viruses**

1. Right click on the red McAfee icon in the system tray, point to **VirusScan** and click **Scan for Viruses**.

A window will appear in the left pane displaying your drives and folders. By default, **My Computer** components are selected.

2. Highlight the drive or folder you wish to scan. If the folder is hidden, click on the **plus sign** to expand the location, showing the folders.
3. The scan options are all checked by default. These options provide the most thorough scan. Click in the box to clear the check mark to deselect the option you don’t want to use.

**Scan subfolders** – uncheck if you wish to scan only files within the selected folder or drive.

**Scan all files** – uncheck if you wish to scan program files and documents only.

**Scan within compressed files** – This option scans for infected files within .ZIP and other compressed files. Sometimes virus writers hide viruses in a .ZIP file, then place that .ZIP file within another .ZIP file to try to bypass anti-virus scanners. VirusScan can detect these viruses if this option is checked.

**Scan for new unknown viruses** – This option uses advanced heuristic techniques to match files to signatures of known viruses and signs of unidentified viruses in the files. This option provides the most thorough scan but is generally slower than a normal scan.

**Scan for potentially unwanted applications** – This option detects spyware, adware, dialers and other applications that you did not intend to install on your computer.

4. Click on the **Scan** button to start scanning the selected location. When the scan is completed, a list of any infected files detected appears in the dialog box.
Check the box before the infected file. Click **Clean**, **Delete** or **Quarantine**. If you wish to do the same action for all infected files listed, check the box at the top by File Name. Then click **Clean**, **Delete** or **Quarantine**. Click **Close** when done.

5. If VirusScan finds no viruses, click **Close**.
I Found a Virus, Now What?

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

For this example, VirusScan detected and deleted W32/Bagle.af@MM virus. It will display the options available to you. Click **continue what I was doing**.

In this example, VirusScan detected the eicar test “virus” (eicar isn’t a true virus). VirusScan reports that the file eicar.com is infected and cannot be cleaned. VirusScan then gives you options to either delete or quarantine the file. In this case, you should delete the infected file.

For most viruses, Trojans, and worms, VirusScan automatically tries to clean the file first. If the file cannot be cleaned, VirusScan gives you options on what to do next. In general, you should delete the infected file. Quarantine the file, if you wish to submit the sample to AVERT for analysis or to look up more information about it later.
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, if it is a file you need.

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.

**Why Quarantine?**

(From McAfee Help FAQ)

**Quarantining is a way to safely isolate and neutralize an infected file until future action can be taken.**

There are several situations when it may be advisable to quarantine a file. The first is when an infected file cannot be cleaned by VirusScan. This can happen when the update needed to clean the file is either not yet available or has not yet been downloaded. Quarantining isolates and neutralizes the file, protecting your system and other files until the proper update can be downloaded.

Sometimes the damage caused by the virus makes the file unable to be cleaned. In this situation it is advisable to delete the file and recover from a backup. If no backup is available or you need to attempt to salvage the data from the file, it is advisable to quarantine the file to avoid the risk of infecting other files on the PC until further action can be taken.

Lastly, VirusScan's heuristic scanning feature may flag a file as likely to contain a virus, even though it does not match any known virus. In this situation it is recommended to quarantine the file until it can be reported to AVERT and a more thorough assessment of the file can be made.

When a file is quarantined, there are three things that VirusScan does to render the file virtually harmless.
1. The file is encrypted with an algorithm that can only be decrypted by VirusScan.
2. The extension of the file is changed to .mcq and the file is locked.
3. The file is moved to the quarantine directory.
For More Information

For help 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 or Keller 213 or send e-mail to help@hawaii.edu.

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

For VirusScan FAQs on update, install/uninstall, general and virus infection issues go to http://www.mcafeehelp.com. In the Product pull down menu, select VirusScan 8 and select the category that you need information for.

You may also get online technical help via a chat session with a McAfee technical support person at http://www.mcafeehelp.com if Hot Topics or a search of the FAQs doesn’t answer your question.


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.