INFORMATION TECHNOLOGY SERVICES University of Hawai‘i

WIN1049 October 2009

Using McAfee VirusScan Enterprise 8.7i

Jocelyn Kasamoto

Introduction

Anti-virus software is the first line of defense against computer viruses and other malware threats. **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 8.7i.

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, Windows 7, Windows server 2003, Windows server 2008, and Windows Server 2008 Release 2. It also supports 64-bit Windows.

VSE 8.7 with patch 2 is required for Windows 7 and Windows server 2008 Release 2 support.

New or Improved Features in VSE 8.7 (excerpt from Release Notes for VSE 8.7)

Architectural changes
VirusScan Enterprise incorporates some significant architectural changes that affect the manner in which the VirusScan Enterprise 8.7i core components work. These changes result in greater security benefits to customers, including:

- **Better rootkit detection and cleaning without system restart** — Safe memory patching, better IRP repair support at the system core, and the ability to read locked files at the kernel level provide better rootkit detection and the ability to clean detections without restarting the system.
- **On-access scan performance improvements during system startup** — A new boot cache process improves on-access scan performance during system startup.
- **Greater self-protection** — The self-protection feature has been enhanced to protect against a wider range of mal-processes that can terminate McAfee processes. This provides greater VirusScan Enterprise self-protection and product stability.

Real-time malware protection (uses Artemis Technology)
A new feature, **Heuristic network check for suspicious files**, provides customers with real-time detections for malware.

- This feature uses sensitivity levels that can be configured, based on your risk tolerance, to look for suspicious files on your endpoints that are running VirusScan Enterprise 8.7i.
- When enabled, this feature detects a suspicious program and sends a DNS request containing a fingerprint of the suspicious file to McAfee Avert Labs, which then communicates the appropriate action back to VirusScan Enterprise 8.7i.
- The real-time defense feature also provides protection for classes of malware for which signatures might not be available.
- This protection is in addition to the world-class DAT-based detection VirusScan Enterprise has always provided. The user experience remains the same and no additional client software is required.
- In this release, this feature is available only for on-demand scans and email scanning and is disabled by default. You must select a sensitivity level to enable the feature.

Performance improvements
These changes improve performance.

- New scan deferral options improve local control of on-demand scans, including the ability to defer scans when using battery power or during presentations. One option can be configured to allow end users to defer scheduled on-demand scans for the increment of time you specify. You can specify hourly increments up to twenty-four hours, or forever.

- Enhanced system throttling now includes registry and memory scanning in addition to file scanning.

Improved email scanner
The email scanner now supports double-byte and multi-byte languages. This improves detection reliability.

Buffer overflow protection exclusions by API
The ability to specify buffer overflow exclusions by API was removed from VirusScan Enterprise 8.5i, but has been reinstated for the VirusScan Enterprise 8.7i release. The API exclusion name is case-sensitive.

On-access scanner — Scan processes on enable
A new feature, **Scan processes on enable**, scans processes that are already running when the McShield service becomes enabled. When the McShield service starts, the scanner examines any process that is already running and any process as it is launched.

On-demand scan usability improvements
When initiating an on-demand right-click scan, you can now choose an action to take on items detected by the scan. These options are available:

- **Clean** — Report and clean the detection.
- **Continue** — Report the detection and continue scanning.

System Requirements

McAfee VirusScan Enterprise 8.7i is supported on the following Windows platforms (32-bit and 64-bit, if applicable):

Workstations

- Windows 2000 SP4*
- Windows XP Home with Service Pack 2 or 3
- Windows XP Professional with Service Pack 2 or 3
- Windows Vista Home (Basic, Premium), Business, Enterprise, Ultimate
- Windows 7

Servers

- Windows 2000 Server SP4*
- Windows Server 2003 with Service Pack 1 or 2
- Windows Server 2008
- Windows Server 2008 Release 2

McAfee Knowledgebase article KB51111 has the complete list of supported operating systems.
https://kc.mcafee.com/corporate/index?page=content&id=KB51111

*Note: ITS no longer supports Windows 2000.

Minimum system requirements (but not optimal) to run VirusScan Enterprise:

- Internet Explorer 6 or later
- Windows Installer – Microsoft Windows Installer (MSI) version 3.1 or later
- 240 MB of free hard disk space for complete installation with all program features
- 512 MB RAM (minimum); 1 GB RAM (or more) highly recommended
- Intel Pentium class or Celeron processor rated 166MHz or higher
- CD-ROM drive
- Internet connection (local area network, broadband or modem connection) for getting updates

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

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

Where to Get the Software

Open your web browser to http://www.hawaii.edu/antivirus/ to download a copy of McAfee VirusScan Enterprise. Login with your UH username and password.

McAfee VirusScan Enterprise is also available on the ITS CD ROM at the ITS walk-in Help Desks located on the first floor of Hamilton Library and first floor of Sinclair Library 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 or a slow broadband connection.

Installation Instructions

Please read the instructions completely as some steps have changed since the previous UH installer.

1. Download a copy of McAfee VirusScan Enterprise (**uhvse87p2.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. Temporarily disable Webroot Spy Sweeper.

3. If you have an existing anti-virus software (not McAfee VirusScan Enterprise 8.5i), you should uninstall it first. Go to **Start**, **Control Panel**, **Add/Remove Programs**. Select your old anti-virus program and click **Remove**.

   R**estart your system** before proceeding with the installation. Some registry items may not be removed until your system is rebooted.

4. Double click on the **uhvse87p2.exe** self-extracting file to extract the contents. It may take awhile to extract the files.

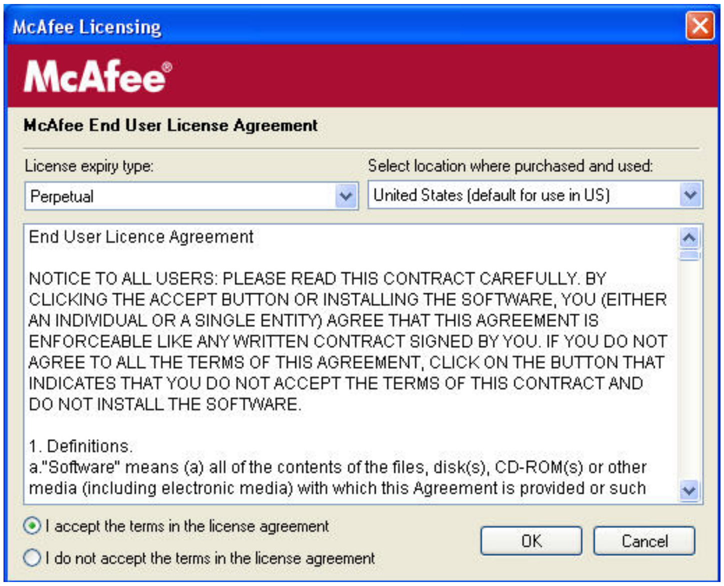
   (Insert the ITS CD ROM into your CD ROM drive. Open **My Computer** and select the ITS CD ROM. Double click on the **uhvse87p2.exe** icon.)

   Vista/Windows 7:

- You will receive the User Account Control (UAC) prompt "an unidentified program wants to access to your computer" for uhvse87p2.exe.
- Click **Allow**.
- When prompted to remove Windows Defender, click **No**.

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**.



McAfee End User License Agreement

License expiry type: Perpetual

Select location where purchased and used: United States (default for use in US)

End User Licence Agreement

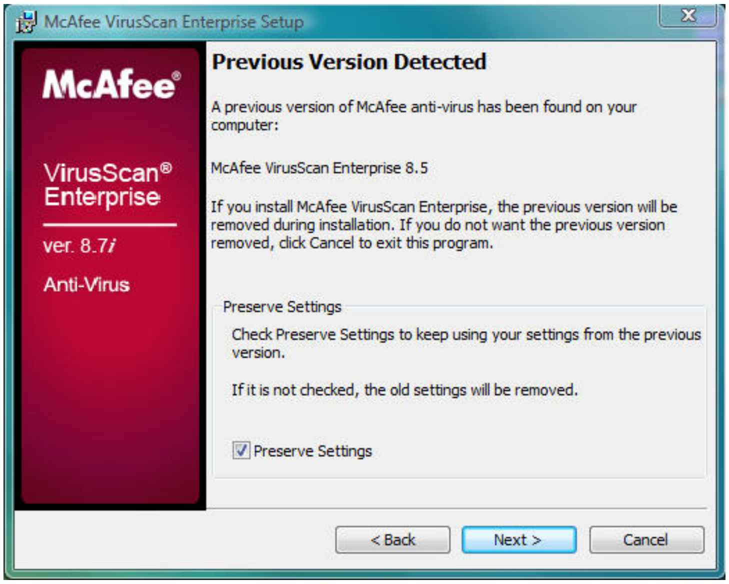
NOTICE TO ALL USERS: PLEASE READ THIS CONTRACT CAREFULLY. BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU. IF YOU DO NOT AGREE TO ALL THE TERMS OF THIS AGREEMENT, CLICK ON THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS CONTRACT AND DO NOT INSTALL THE SOFTWARE.

1. Definitions.
a."Software" means (a) all of the contents of the files, disk(s), CD-ROM(s) or other media (including electronic media) with which this Agreement is provided or such

● I accept the terms in the license agreement
○ I do not accept the terms in the license agreement

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 8.7 installer will detect it. Check **preserve settings.** Click **Next.**



Previous Version Detected

A previous version of McAfee anti-virus has been found on your computer:

McAfee VirusScan Enterprise 8.5

If you install McAfee VirusScan Enterprise, the previous version will be removed during installation. If you do not want the previous version removed, click Cancel to exit this program.

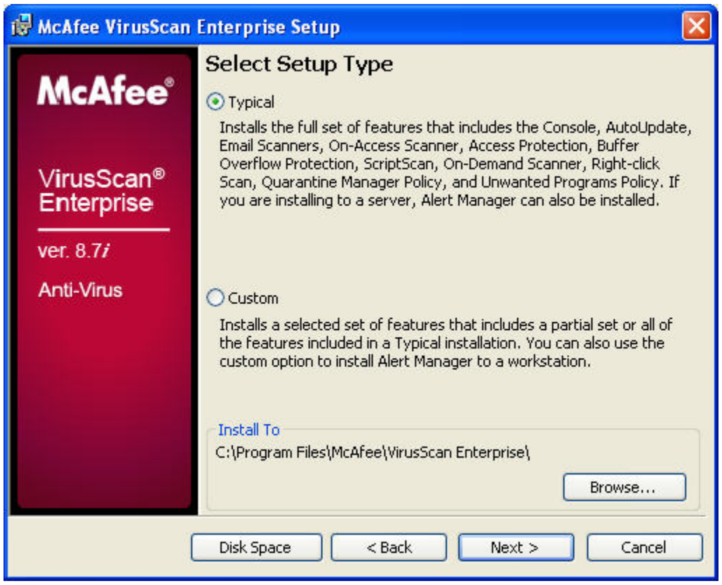
Preserve Settings

Check Preserve Settings to keep using your settings from the previous version.

If it is not checked, the old settings will be removed.

☑ Preserve Settings

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



Select Setup Type

● Typical

Installs the full set of features that includes the Console, AutoUpdate, Email Scanners, On-Access Scanner, Access Protection, Buffer Overflow Protection, ScriptScan, On-Demand Scanner, Right-click Scan, Quarantine Manager Policy, and Unwanted Programs Policy. If you are installing to a server, Alert Manager can also be installed.

○ Custom

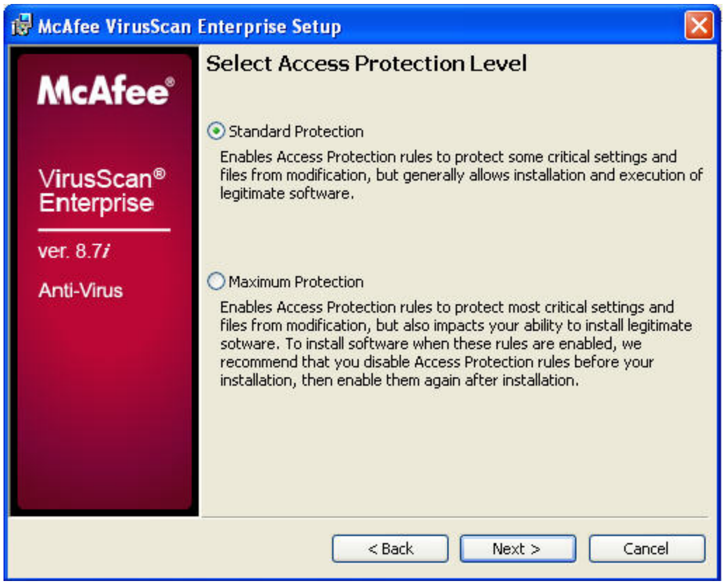
Installs a selected set of features that includes a partial set or all of the features included in a Typical installation. You can also use the custom option to install Alert Manager to a workstation.

Install To

C:\Program Files\McAfee\VirusScan Enterprise\

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

Note: when installing VSE 8.7 over an existing VSE 8.5, the installer doesn't prompt for access protection level.



Select Access Protection Level

● Standard Protection

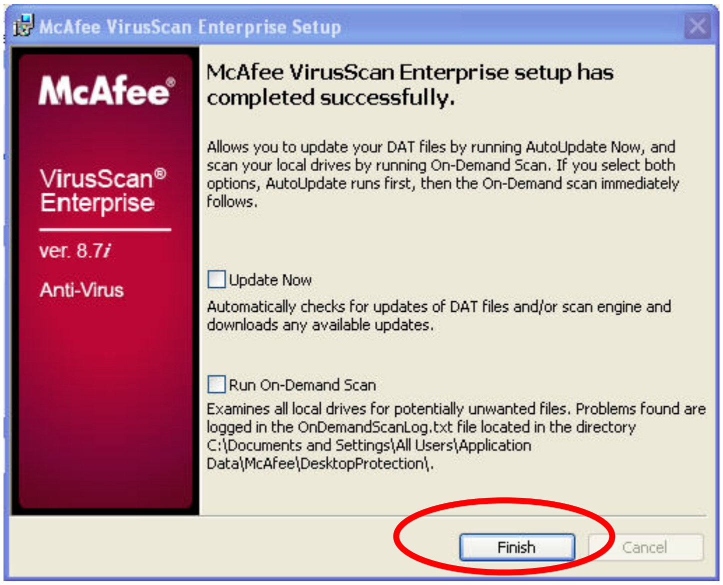
Enables Access Protection rules to protect some critical settings and files from modification, but generally allows installation and execution of legitimate software.

○ Maximum Protection

Enables Access Protection rules to protect most critical settings and files from modification, but also impacts your ability to install legitimate sotware. To install software when these rules are enabled, we recommend that you disable Access Protection rules before your installation, then enable them again after installation.

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

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



McAfee VirusScan Enterprise setup has completed successfully.

Allows you to update your DAT files by running AutoUpdate Now, and scan your local drives by running On-Demand Scan. If you select both options, AutoUpdate runs first, then the On-Demand scan immediately follows.

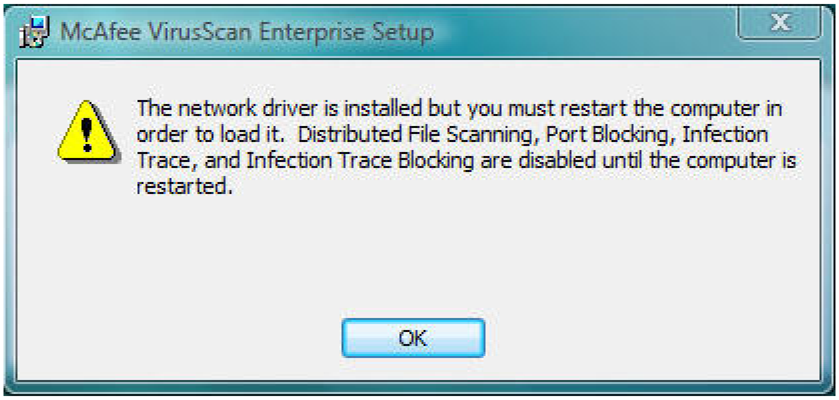
□ Update Now

Automatically checks for updates of DAT files and/or scan engine and downloads any available updates.

□ Run On-Demand Scan

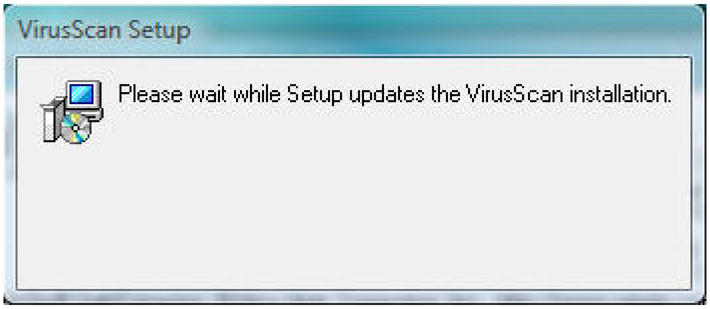
Examines all local drives for potentially unwanted files. Problems found are logged in the OnDemandScanLog.txt file located in the directory C:\Documents and Settings\All Users\Application Data\McAfee\DesktopProtection\.

12. The following message will appears. Click **OK**.


McAfee VirusScan Enterprise Setup

The network driver is installed but you must restart the computer in order to load it. Distributed File Scanning, Port Blocking, Infection Trace, and Infection Trace Blocking are disabled until the computer is restarted.

13. Patch 2 will be installed. Please wait until the installation is completed.


VirusScan Setup

Please wait while Setup updates the VirusScan installation.

When the VSE installation is completed, you will be returned to the Windows desktop. A red vshield icon will appear in the system tray.

14. **Restart** your computer. You must reboot to load VirusScan settings.

Post Installation Instructions

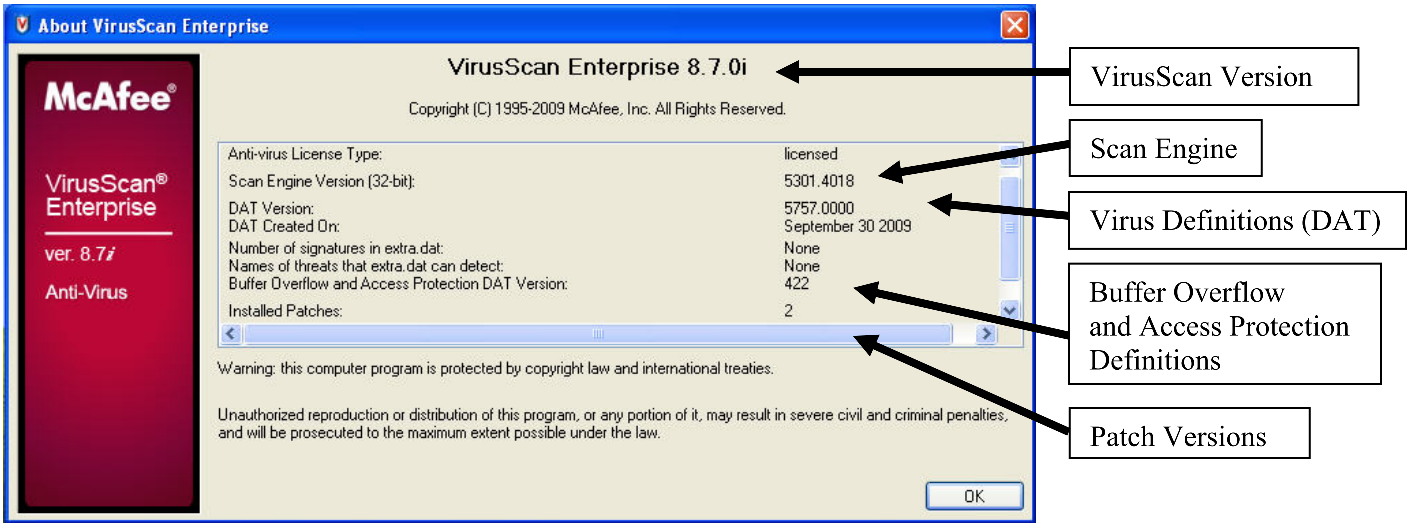
15. Manually update your scan engine and DAT by running **Update Now.**

    After restarting, you may need to wait until VirusScan is completely loaded (Autoupdate task should appear in VirusScan Console) before running **Update Now**. (See *How to Manually Update DATs* on page 14.)

16. Scan your hard drive(s) by running Full Scan. (See *How to Scan for Threats* on page 17.)

Which Version of VirusScan am I Running?

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



About VirusScan Enterprise

McAfee®
VirusScan® Enterprise
ver. 8.7*i*
Anti-Virus

VirusScan Enterprise 8.7.0i

Copyright (C) 1995-2009 McAfee, Inc. All Rights Reserved.

```
Anti-virus License Type:                              licensed
Scan Engine Version (32-bit):                         5301.4018
DAT Version:                                          5757.0000
DAT Created On:                                       September 30 2009
Number of signatures in extra.dat:                    None
Names of threats that extra.dat can detect:           None
Buffer Overflow and Access Protection DAT Version:    422
Installed Patches:                                    2
```

Warning: this computer program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

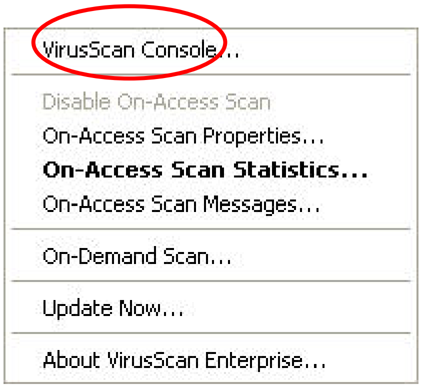
You are running VirusScan Enterprise version 8.7i with virus definitions (DAT) 5757.0000, 32-bit scan engine 5301.4018 and patch 2 installed. Buffer overflow and access protection DAT version is 422. You will need this information when calling the ITS Help Desk for assistance with VirusScan Enterprise.

If you are running 64-bit Windows, the 64-bit scan engine version will be listed. Incremental updates of the scan engine are allowed with the 5300 scan engine series (32-bit and 64-bit).

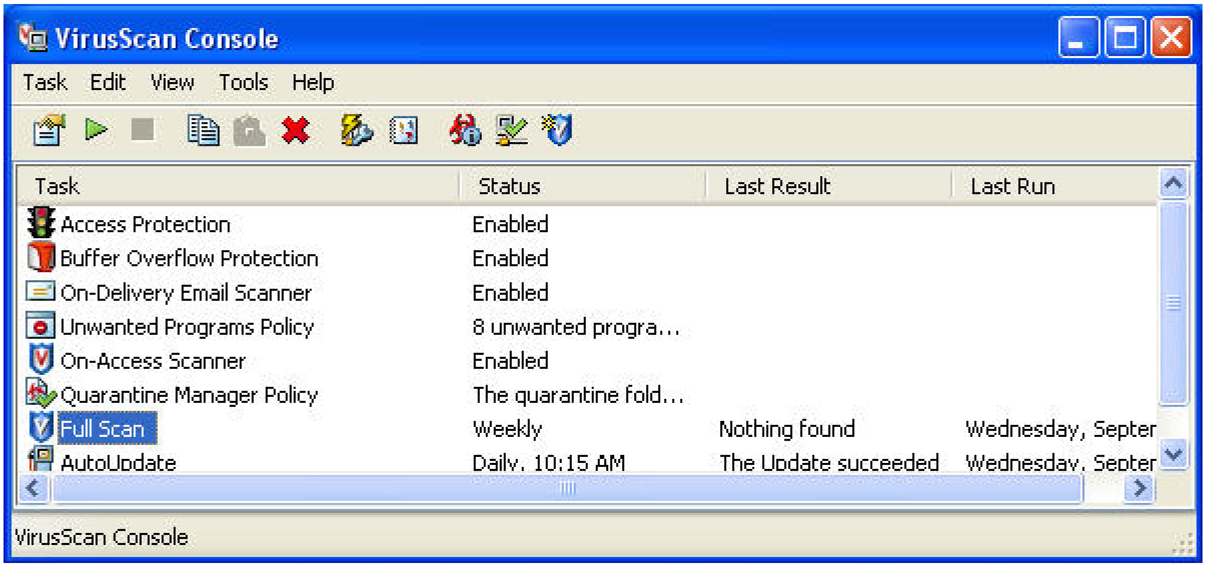
Launching VirusScan Console

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

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



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...



Task	Status	Last Result	Last Run
Access Protection	Enabled		
Buffer Overflow Protection	Enabled		
On-Delivery Email Scanner	Enabled		
Unwanted Programs Policy	8 unwanted progra...		
On-Access Scanner	Enabled		
Quarantine Manager Policy	The quarantine fold...		
Full Scan	Weekly	Nothing found	Wednesday, Septer
AutoUpdate	Daily, 10:15 AM	The Update succeeded	Wednesday, Septer

VirusScan Console comes with eight tasks by default: Access Protection, Buffer Overflow Protection, 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

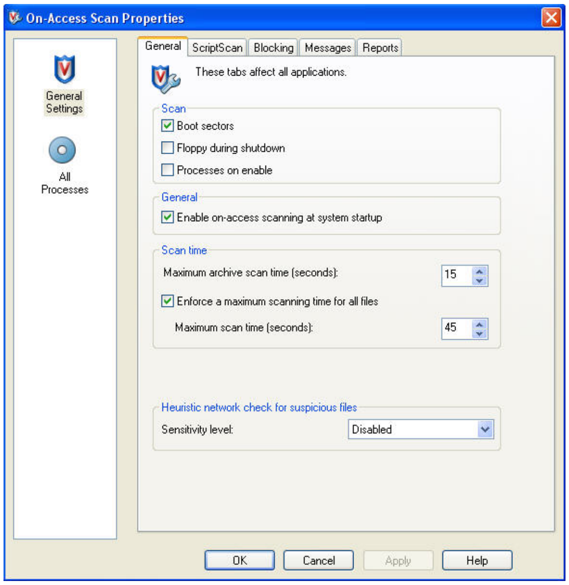
On-access scanner properties have been pre-configured for use at UH. In general, the pre-configured settings should be sufficient for anti-virus protection for general business office use. If you have a shared computer or a computer lab environment, you should adjust your scan settings to increase your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

   New: Sensitivity Level (Artemis Technology) is disabled by default.



These tabs affect all applications.

Scan

☑ Boot sectors

□ Floppy during shutdown

□ Processes on enable

General

☑ 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

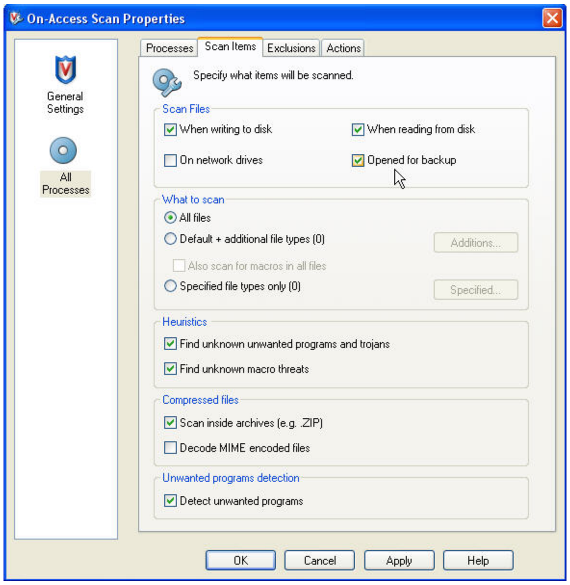
Heuristic network check for suspicious files

Sensitivity level: Disabled

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 **Scan Items** tab.



Specify what items will be scanned.

Scan Files

☑ When writing to disk ☑ When reading from disk

□ On network drives ☑ Opened for backup

What to scan

● All files

○ Default + additional file types (0)

□ Also scan for macros in all files

○ Specified file types only (0)

Heuristics

☑ Find unknown unwanted programs and trojans

☑ Find unknown macro threats

Compressed files

☑ Scan inside archives (e.g. .ZIP)

□ Decode MIME encoded files

Unwanted programs detection

☑ Detect unwanted programs

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.

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.

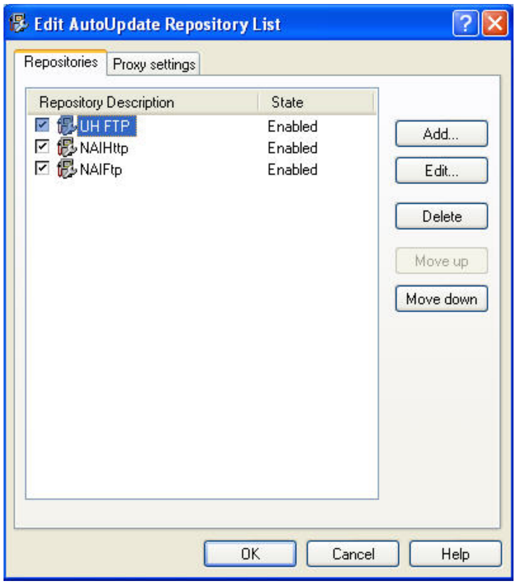
5. Click **Apply** and **OK**.

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.



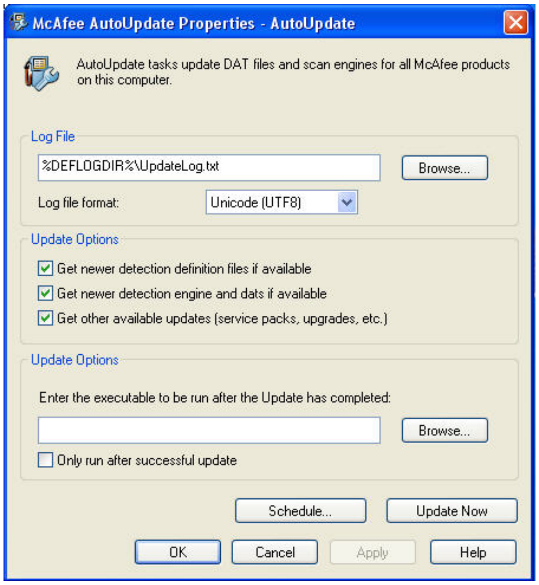
Repository Description	State
☑ UH FTP	Enabled
☑ NAIHttp	Enabled
☑ NAIFtp	Enabled

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 AutoUpdate Properties - AutoUpdate

AutoUpdate tasks update DAT files and scan engines for all McAfee products on this computer.

Log File

%DEFLOGDIR%\UpdateLog.txt [Browse...]

Log file format: Unicode (UTF8)

Update Options

☑ Get newer detection definition files if available
☑ Get newer detection engine and dats if available
☑ Get other available updates (service packs, upgrades, etc.)

Update Options

Enter the executable to be run after the Update has completed:

[Browse...]

□ Only run after successful update

[Schedule...] [Update Now]

[OK] [Cancel] [Apply] [Help]

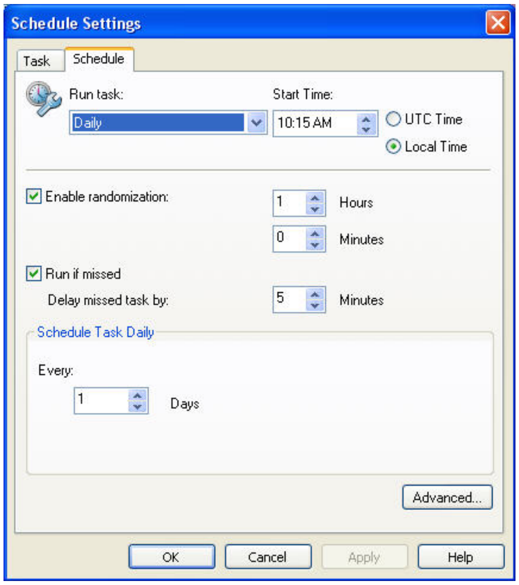
To Schedule AutoUpdates

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 10:15 a.m.** with one hour randomization (connections to the repositories are varied up to one hour, spreading out the load on the update servers.).



Schedule Settings

Task | Schedule

Run task: Daily

Start Time: 10:15 AM

○ UTC Time
● Local Time

☑ Enable randomization: 1 Hours

0 Minutes

☑ Run if missed

Delay missed task by: 5 Minutes

Schedule Task Daily

Every: 1 Days

[Advanced...]

[OK] [Cancel] [Apply] [Help]

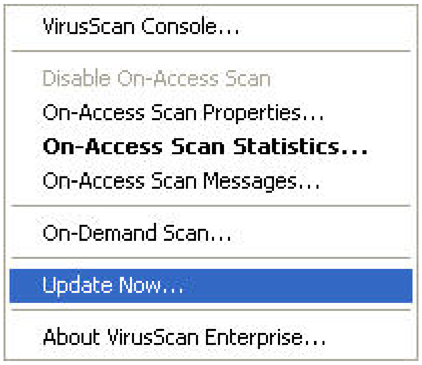
Note: Your computer must be powered on at the scheduled time for the AutoUpdate task to run.

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

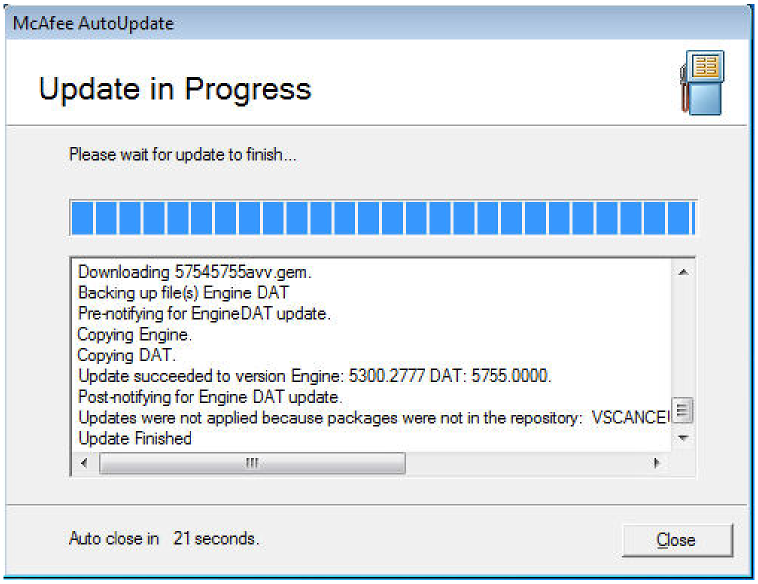
There are several ways to manually update your scan engine and DAT files.

- Right click on the red Vshield 🛡 icon in the system tray and click on **Update Now** on the popup menu.


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...

- 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.



Please wait for update to finish...

```
Downloading 57545755avv.gem.
Backing up file(s) Engine DAT
Pre-notifying for EngineDAT update.
Copying Engine.
Copying DAT.
Update succeeded to version Engine: 5300.2777 DAT: 5755.0000.
Post-notifying for Engine DAT update.
Updates were not applied because packages were not in the repository:  VSCANCE
Update Finished
```

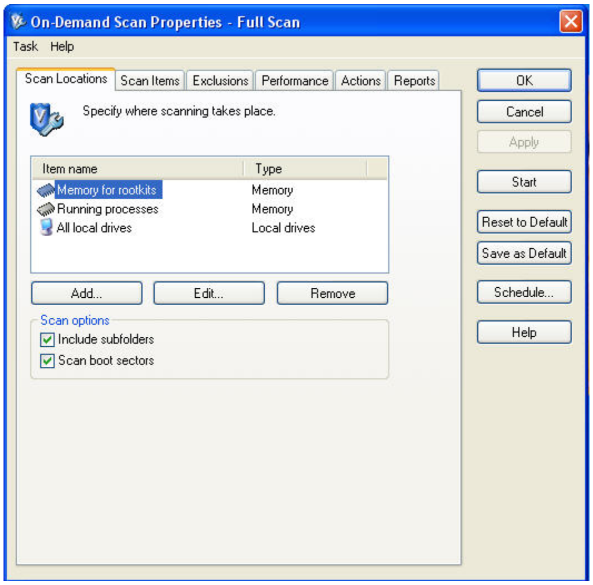
Auto close in 21 seconds.

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, 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**.



On-Demand Scan Properties - Full Scan

Specify where scanning takes place.

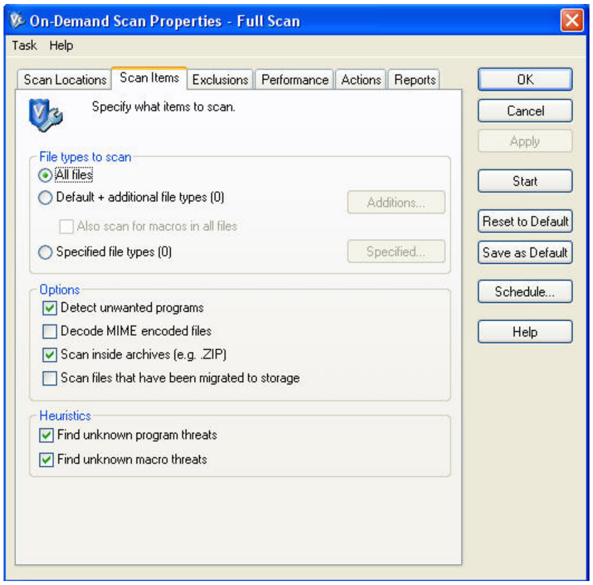
Item name	Type
Memory for rootkits	Memory
Running processes	Memory
All local drives	Local drives

Scan options

☑ Include subfolders

☑ Scan boot sectors

2. Click on the **Scan Items** 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. It will do a heuristic scan for unknown program threats and macro threats.



On-Demand Scan Properties - Full Scan

Specify what items to scan.

File types to scan

● All files

○ Default + additional file types (0)

□ Also scan for macros in all files

○ Specified file types (0)

Options

☑ Detect unwanted programs

□ Decode MIME encoded files

☑ Scan inside archives (e.g. .ZIP)

□ Scan files that have been migrated to storage

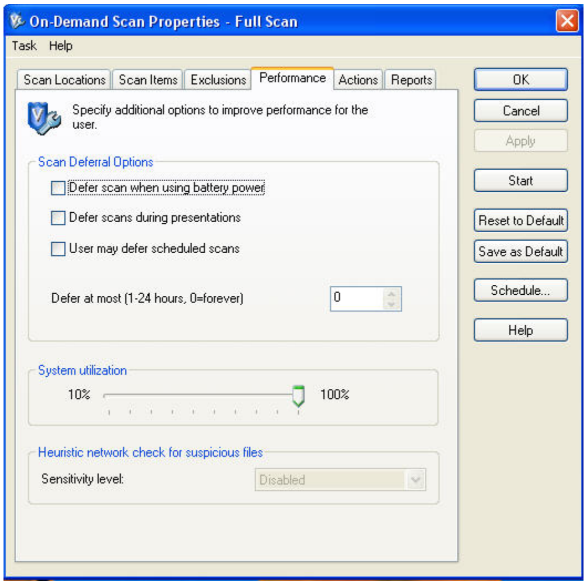
Heuristics

☑ Find unknown program threats

☑ Find unknown macro threats

3. Click on the **Performance** tab.

   You may check options to defer an on-demand scan, if needed.



Specify additional options to improve performance for the user.

Scan Deferral Options

☐ Defer scan when using battery power

☐ Defer scans during presentations

☐ User may defer scheduled scans

Defer at most (1-24 hours, 0=forever) 0

System utilization

10% 100%

Heuristic network check for suspicious files

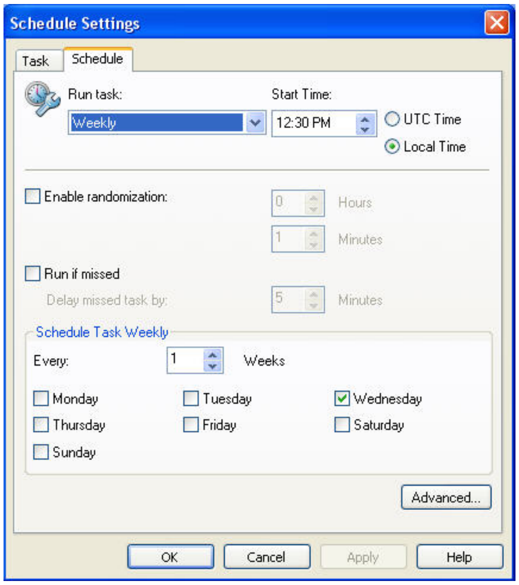
Sensitivity level: Disabled

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, and you won't be actively using your computer. **The pre-configured scan schedule is set for Wednesdays at 12:30 p.m.** Make adjustments to day or time, if needed. Click on **Apply** and **OK**.

   Depending on your hardware and the amount of data you have, the on-demand scan may take several hours to complete. **If the scan significantly slows down computer or does not complete before you leave at the end of the day, schedule the scan to start after work hours and leave your computer powered on overnight.**



Run task: Weekly

Start Time: 12:30 PM

○ UTC Time

● Local Time

☐ Enable randomization: 0 Hours

1 Minutes

☐ Run if missed

Delay missed task by: 5 Minutes

Schedule Task Weekly

Every: 1 Weeks

☐ Monday ☐ Tuesday ☑ Wednesday

☐ Thursday ☐ Friday ☐ Saturday

☐ Sunday

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

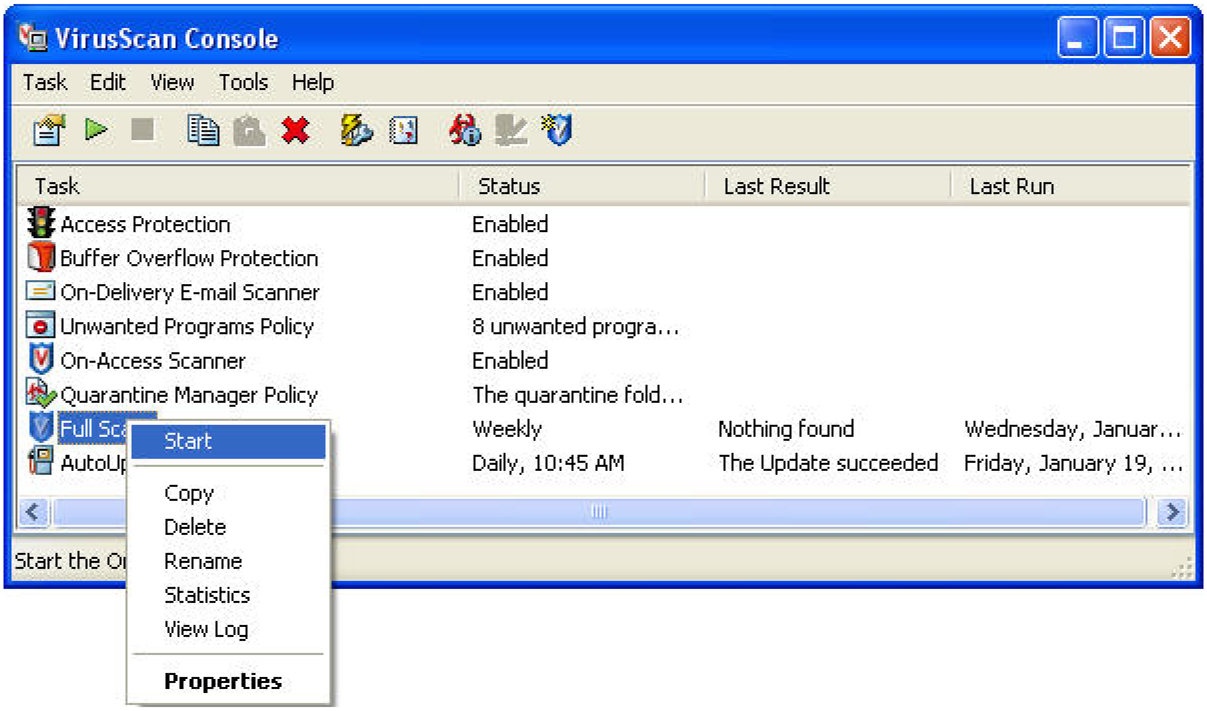
Threats are viruses and any unwanted programs specified in Unwanted Programs Policy (spyware, adware, key loggers, etc.)

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.

Full Scan

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



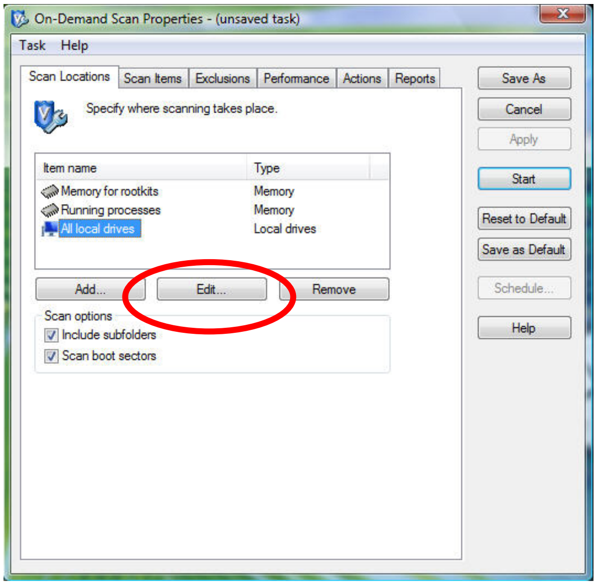
Task	Status	Last Result	Last Run
Access Protection	Enabled		
Buffer Overflow Protection	Enabled		
On-Delivery E-mail Scanner	Enabled		
Unwanted Programs Policy	8 unwanted progra...		
On-Access Scanner	Enabled		
Quarantine Manager Policy	The quarantine fold...		
Full Sca	Weekly	Nothing found	Wednesday, Januar...
AutoUp	Daily, 10:45 AM	The Update succeeded	Friday, January 19, ...

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 **Scan Locations** tab, highlight **All Local Drives**, and click on the **Edit** button.



Specify where scanning takes place.

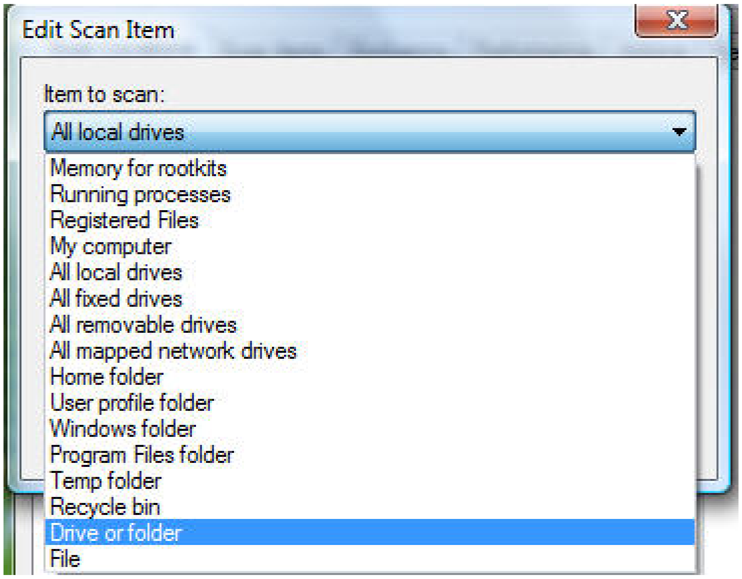
Item name	Type
Memory for rootkits	Memory
Running processes	Memory
All local drives	Local drives

Scan options

☑ Include subfolders

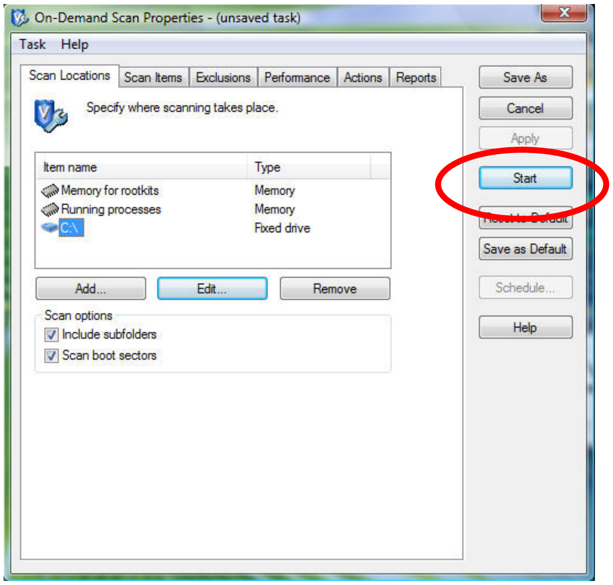
☑ Scan boot sectors

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



Item to scan: All local drives

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.



Specify where scanning takes place.

Item name	Type
Memory for rootkits	Memory
Running processes	Memory
C:\	Fixed drive

Scan options

☑ Include subfolders

☑ Scan boot sectors

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.

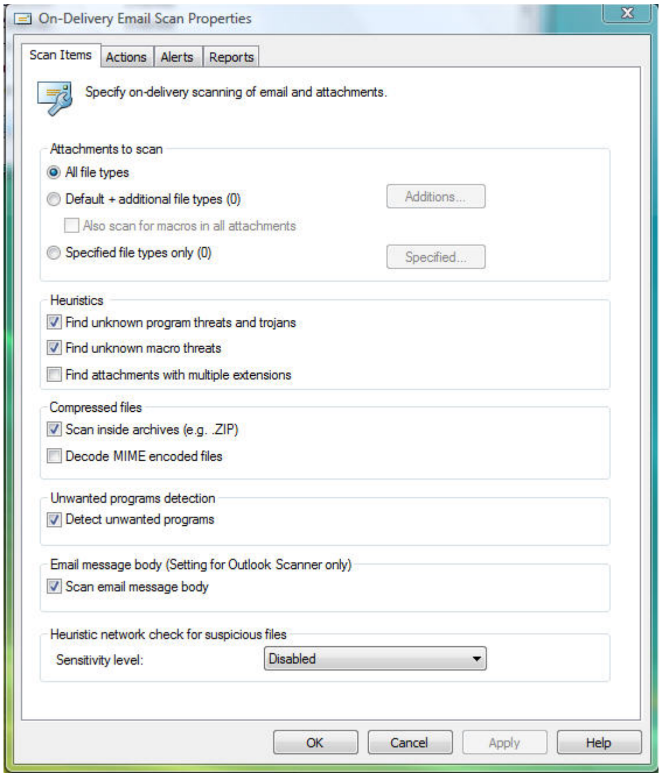
Configuring On-Delivery E-mail Scanner

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 Thunderbird.**

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.**

If you use Microsoft Outlook, please check your on-delivery e-mail scanner properties.

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


On-Delivery Email Scan Properties

Scan Items | Actions | Alerts | Reports

Specify on-delivery scanning of email and attachments.

Attachments to scan
- ● All file types
- ○ Default + additional file types (0) — Additions...
- □ Also scan for macros in all attachments
- ○ Specified file types only (0) — Specified...

Heuristics
- ☑ Find unknown program threats and trojans
- ☑ Find unknown macro threats
- □ Find attachments with multiple extensions

Compressed files
- ☑ Scan inside archives (e.g. .ZIP)
- □ Decode MIME encoded files

Unwanted programs detection
- ☑ Detect unwanted programs

Email message body (Setting for Outlook Scanner only)
- ☑ Scan email message body

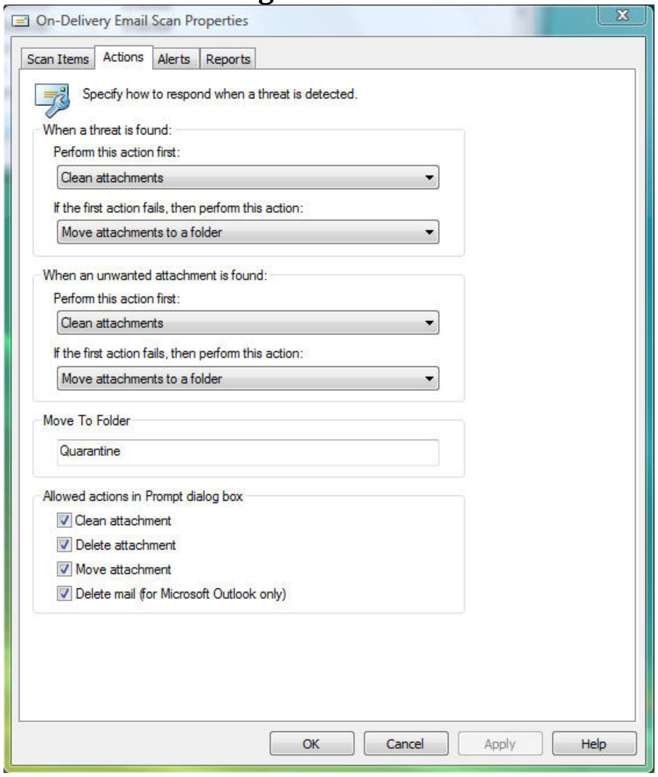
Heuristic network check for suspicious files
- Sensitivity level: Disabled

Heuristic network check for suspicious files (Artemis):

Artemis technology is disabled by default. To turn it on, set the sensitivity level to the desired level.

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

E-mail Scan Settings - Actions Tab


On-Delivery Email Scan Properties

Scan Items | Actions | Alerts | Reports

Specify how to respond when a threat is detected.

When a threat is found:
- Perform this action first: Clean attachments
- If the first action fails, then perform this action: Move attachments to a folder

When an unwanted attachment is found:
- Perform this action first: Clean attachments
- If the first action fails, then perform this action: Move attachments to a folder

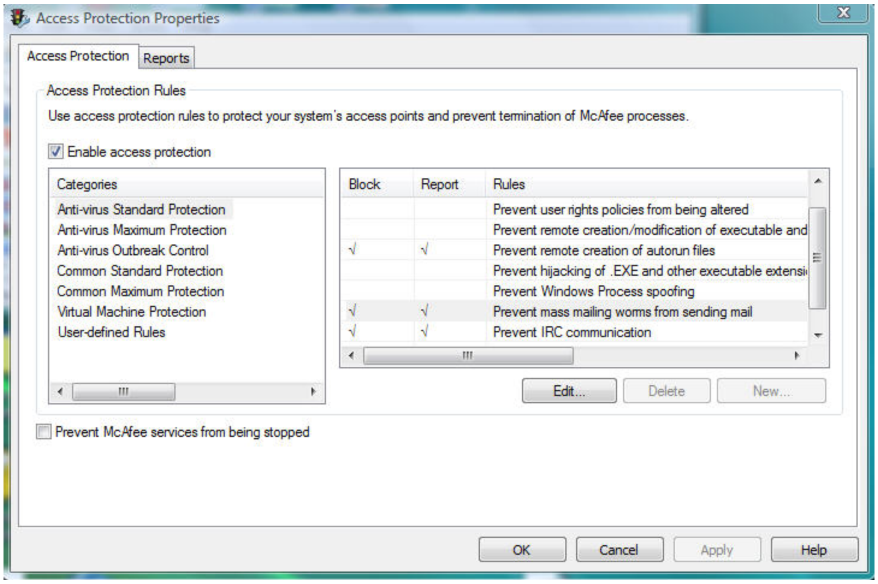
Move To Folder
- Quarantine

Allowed actions in Prompt dialog box
- ☑ Clean attachment
- ☑ Delete attachment
- ☑ Move attachment
- ☑ Delete mail (for Microsoft Outlook only)

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.

Access Protection – Anti-Virus Standard Protection

VSE 8.7i has 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**.



Access Protection Rules

Use access protection rules to protect your system's access points and prevent termination of McAfee processes.

☑ Enable access protection

Categories
Anti-virus Standard Protection
Anti-virus Maximum Protection
Anti-virus Outbreak Control
Common Standard Protection
Common Maximum Protection
Virtual Machine Protection
User-defined Rules

Block	Report	Rules
		Prevent user rights policies from being altered
		Prevent remote creation/modification of executable and
√	√	Prevent remote creation of autorun files
		Prevent hijacking of .EXE and other executable extensi
		Prevent Windows Process spoofing
√	√	Prevent mass mailing worms from sending mail
√	√	Prevent IRC communication

☐ Prevent McAfee services from being stopped

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 Outlook, Thunderbird, 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
mdaemon.exe	modulewrapper*	mozilla.exe
msexcimc.exe	msimn.exe	mskdetct.exe
msksrvr.exe	msn6.exe	msnmsgr.exe
neo20.exe	netscp.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	Worldclient.exe
wspsrv.exe		

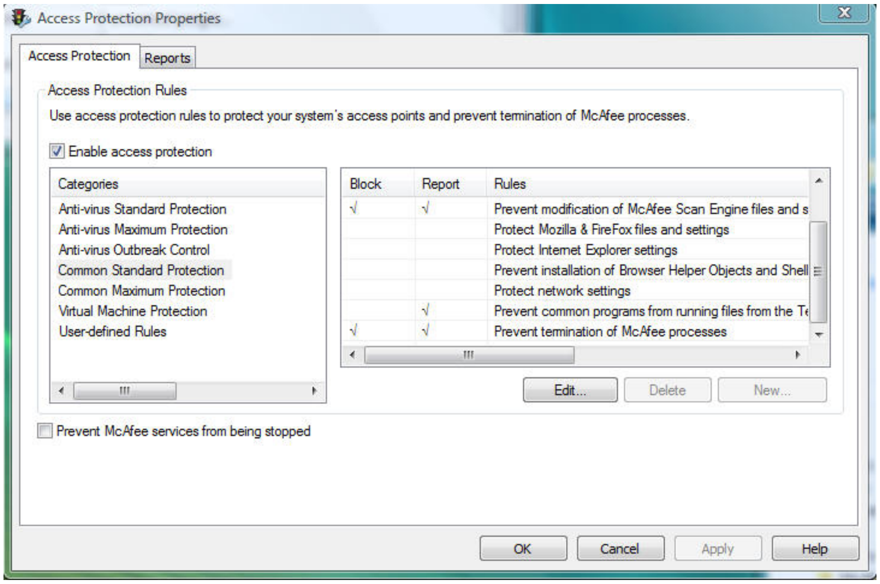
If your email client is not included in the default list of exclusions, you may add it by:

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 Rules

Use access protection rules to protect your system's access points and prevent termination of McAfee processes.

☑ Enable access protection

Categories
Anti-virus Standard Protection
Anti-virus Maximum Protection
Anti-virus Outbreak Control
Common Standard Protection
Common Maximum Protection
Virtual Machine Protection
User-defined Rules

Block	Report	Rules
√	√	Prevent modification of McAfee Scan Engine files and s
		Protect Mozilla & FireFox files and settings
		Protect Internet Explorer settings
		Prevent installation of Browser Helper Objects and Shell
		Protect network settings
	√	Prevent common programs from running files from the Te
√	√	Prevent termination of McAfee processes

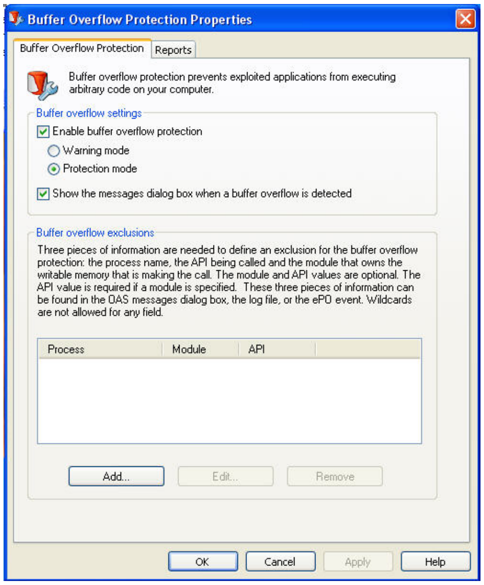
☐ Prevent McAfee services from being stopped

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 8.7i has buffer overflow protection capabilities. 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.



Buffer Overflow Protection Properties

Buffer overflow protection prevents exploited applications from executing arbitrary code on your computer.

Buffer overflow settings

☑ Enable buffer overflow protection

○ Warning mode

● Protection mode

☑ Show the messages dialog box when a buffer overflow is detected

Buffer overflow exclusions

Three pieces of information are needed to define an exclusion for the buffer overflow protection: the process name, the API being called and the module that owns the writable memory that is making the call. The module and API values are optional. The API value is required if a module is specified. These three pieces of information can be found in the OAS messages dialog box, the log file, or the ePO event. Wildcards are not allowed for any field.

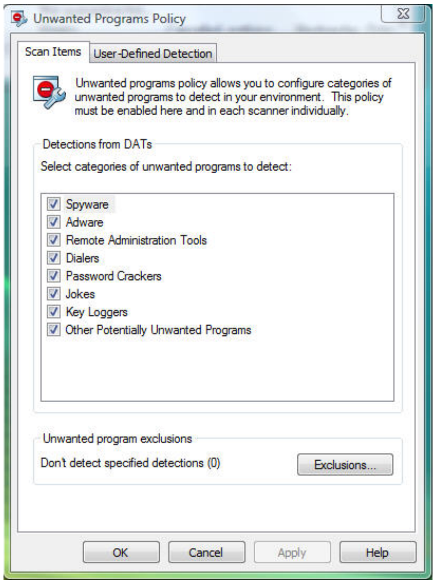
Process	Module	API

Some software may conflict with VirusScan’s buffer overflow protection. In that case, add an exclusion by process name (module and API may also be specified).

If specifying an exclusion does not work, you may need to 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**.



Unwanted Programs Policy

Unwanted programs policy allows you to configure categories of unwanted programs to detect in your environment. This policy must be enabled here and in each scanner individually.

Detections from DATs

Select categories of unwanted programs to detect:

☑ Spyware
☑ Adware
☑ Remote Administration Tools
☑ Dialers
☑ Password Crackers
☑ Jokes
☑ Key Loggers
☑ Other Potentially Unwanted Programs

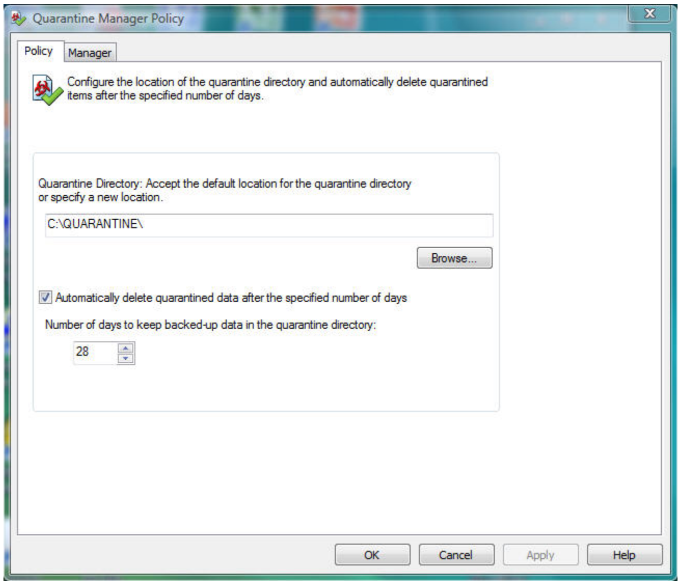
Unwanted program exclusions

Don't detect specified detections (0)

Quarantine Manager

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.



Configure the location of the quarantine directory and automatically delete quarantined items after the specified number of days.

Quarantine Directory: Accept the default location for the quarantine directory or specify a new location.

C:\QUARANTINE\

☑ Automatically delete quarantined data after the specified number of days

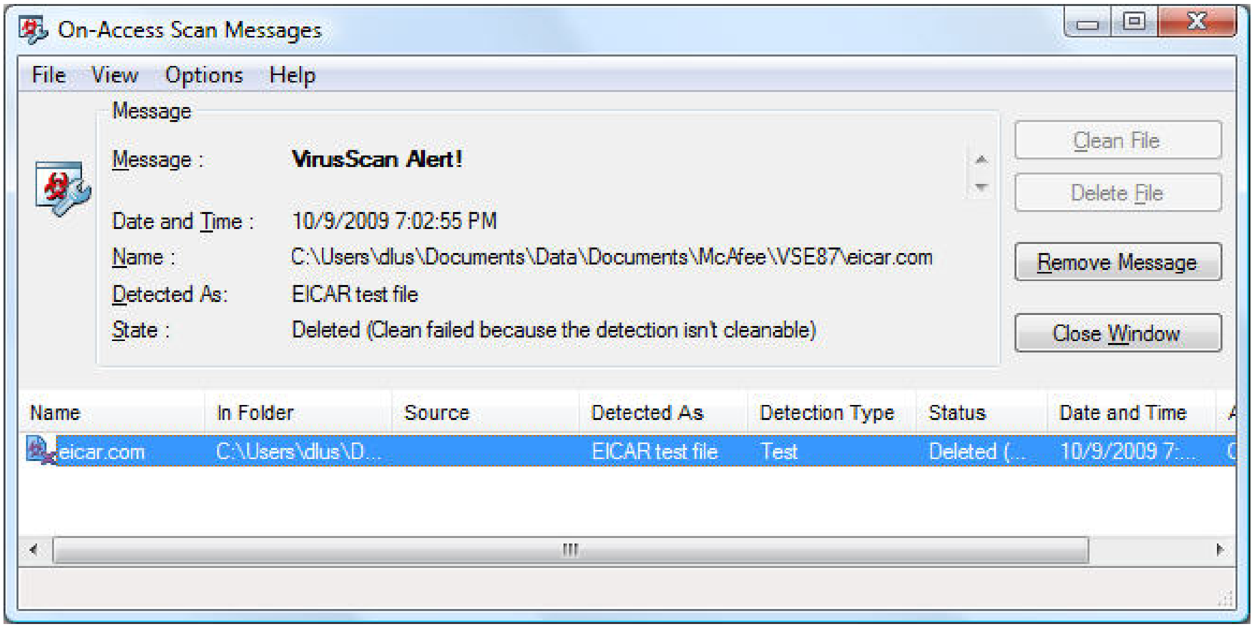
Number of days to keep backed-up data in the quarantine directory:

28

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**.

I Found a Virus, Now What?

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



Message : **VirusScan Alert!**

Date and Time : 10/9/2009 7:02:55 PM

Name : C:\Users\dlus\Documents\Data\Documents\McAfee\VSE87\eicar.com

Detected As: EICAR test file

State : Deleted (Clean failed because the detection isn't cleanable)

Name	In Folder	Source	Detected As	Detection Type	Status	Date and Time	A
eicar.com	C:\Users\dlus\D...		EICAR test file	Test	Deleted (...	10/9/2009 7:...	C

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.

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\McAfee\DesktopProtection 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 8.7i, one of my programs stopped working properly. What should I do?

A: There may be a conflict with VSE 8.7i'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 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 8.7i and restarted Windows. What does this mean?

A: VirusScan Enterprise 8.7i 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 Operating System

	---------Faculty/Staff-------------			
OS	**Campus**	**Home Use**	**Students**	**Affiliates**
WinXP	VSE 8.5 or higher	VSE 8.5 or higher	VSE 8.5 or higher	VSP
Win Vista	VSE 8.5 or higher	VSE 8.5 or higher	VSE 8.5 or higher	VSP
Win 7	VSE 8.7	VSE 8.7	VSE 8.7	VSP
Win 64-bit	VSE 8.7	VSE 8.7	VSE 8.7	VSP
Servers				
Win 2003	VSE 8.5 or higher			
Win 2008	VSE 8.5 or higher			
Win 2008 R2	VSE 8.7			

VSE = VirusScan Enterprise, VSP = VirusScan Plus

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 CLIC Lab in Hamilton Library or Sinclair Library or send e-mail to help@hawaii.edu.

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

For VirusScan Enterprise FAQs, go to http://knowledge.mcafee.com/SupportSite/supportcentral/supportcentral.do?id=m1. 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 **http://www.hawaii.edu/its**
The ITS walk-in Help Desks are located at
Hamilton Library (first floor) and CLIC Lab (Sinclair Library first floor)
on the UH Mānoa Campus.

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