SECTION 11
VIRUS SCANNING

11. VIRUS SCANNING

A virus is a program that corrupts data in a system. It does not exist physically, but is a set of software codes that can attach themselves to executable files, system files or documents, which can eventually lead to the destruction of data.

Software viruses do not occur by accident – they are written by people specifically to destroy files or cause frustration. They are being written every day, hence the need to continually update virus protection programs such as Symantec Endpoint Protection. Viruses can only be disinfected once they are known – that is to say, we have to find viruses before we can write protection programs to disinfect them.

11.1 HOW CAN MY COMPUTER BECOME INFECTED?

Malware

Malware is a category of malicious code that includes viruses, worms, and Trojan horses. Destructive malware will utilise popular communication tools to spread, including worms sent through email and instant messages, Trojan horses dropped from web sites, and virus-infected files downloaded from peer-to-peer connections or transmitted via USB drives. Malware will also seek to exploit existing vulnerabilities on systems making their entry quiet and easy.

What is a Trojan Horse?

Trojans are mostly used as the first stage of an attack, and their primary purpose is to stay hidden while downloading and installing a stronger threat such as a bot. Unlike viruses and worms, Trojan horses cannot spread by themselves. They are often delivered to a victim through an email message where it masquerades as an image or joke, or by a malicious website, which installs the Trojan horse on a computer through vulnerabilities in web browser software. After it is installed, the Trojan horse lurks silently on the infected machine, invisibly carrying out its misdeeds, such as downloading spyware, while the victim continues on with their normal activities.

Spyware Attacks

Spyware can be downloaded from Web sites, email messages, instant messages, and from direct file-sharing connections. Additionally, a user may unknowingly receive spyware by accepting an End User License Agreement from a software program.

Spam Attacks

Email Spam is the electronic version of junk mail. It involves sending unwanted messages, often unsolicited advertising, to a large number of recipients. Spam is a serious security concern as it can be used to deliver Trojan horses, viruses, worms, spyware, and targeted phishing attacks.

Phishing Attacks

Phishing is essentially an online con game and phishers are nothing more than tech-savvy con artists and identity thieves. They use SPAM, malicious Web sites, email messages and instant messages to trick people into divulging sensitive information, such as bank and credit card accounts.

Misleading Applications

Misleading applications intentionally misrepresent the security status of a computer. Misleading applications attempt to convince the user that he or she must remove potential malware or security risks (usually nonexistent or fake) from the computer. The application will hold the user hostage by refusing to allow him or her to remove or fix the phantom problems until the "required" software is purchased and installed. Misleading applications often look convincing the programs may look like legitimate security programs and often have corresponding websites with user testimonials, lists of features, etc.

Misleading applications typically strike people when they are surfing the web. There is not a single type of website where these applications are found, but they are more common from sites offering pirated goods and adult content, as well as blogs and forums. They can even sneak into advertisements on legitimate sites, usually through banner ads at the top of a Web page. In order to get installed onto a system, a person is usually either tricked into downloading the program (thinking it's something else) or a small program called a "Downloader" is installed by the attacker through an un-patched flaw in the person's web browser. This is often known as a "drive-by" install.

11.2 PROTECTING MY COMPUTER AND FILES

New viruses can be found almost on a daily basis, so it is important to use up-to-date virus protection software. Victoria University's version of Symantec Endpoint Protection is updated regularly. How old is the virus protection software on your home computer? Do you have Auto-Protect activated? (Refer to Section 11.4) If you use a friend's computer, do they have up-to-date virus protection software? Read on in this section about how to install and update Symantec Endpoint Protection and how to scan files using this program.

11.3 CAN I CATCH A VIRUS BY READING MY E-MAILS?

You cannot catch a virus when receiving or reading an email message. A virus can only be contained in a file, which may be sent as an attachment, or can be hyperlinked to something malicious within the email. It is important that you know the exact contents of what you are receiving and to scan all email attachments before you open them. You also need to be careful of clicking on hyperlinks as they may not always direct you to where they appear to.

11.4 WHAT IS SYMANTEC ENDPOINT PROTECTION AND WHAT DOES IT DO?

Symantec™ Endpoint Protection (SEP) combines Symantec AntiVirus™ with advanced threat prevention to deliver an unmatched defence against malware for laptops, desktops, and servers. It provides protection against even the most sophisticated attacks that evade traditional security measures, such as rootkits, zero-day attacks, and mutating spyware.

Real Time Protection

This will scan each file for viruses whenever you open it (eg. if you open a Word file, Symantec Endpoint Protection will immediately check that the Word file has no known viruses). This has been enabled for all local files - that is, files on your own computer.

Auto-Protect

Auto-Protect scans all files that are received from any source, such as the Internet, removable disks, or email attachments. Auto-Protect scans files for viruses, Trojan horses, and worms anytime that the files are accessed, such as when they are copied, moved, run, or opened.

Symantec Endpoint Protection intercepts any run, open, or create activity and scans the file before allowing the action to continue. These scans are transparent to the user and have little, if any, noticeable effect on system performance. If Auto-Protect detects a virus, then you are prompted to repair the file.

When shutting down or starting Windows, Symantec Endpoint Protection Auto-Protect will scan the boot record of any floppy left in drive A for boot sector viruses. If a floppy disk is not in the floppy drive during shut down or restart, then Windows will time out and the shutdown or restart process proceeds normally. If Symantec Endpoint Protection detects a virus, then you are prompted to repair the infected floppy disk boot record.

11.5 SHOULD A CUSTOM SCAN BE UNDERTAKEN BY EACH USER?

If you have any reason to suspect that your computer has a virus, you should immediately conduct a scan on your local drive. To do this, start up Symantec Endpoint Protection (from the "gold shield" icon  on your system tray or click the Start Menu, Go to Programs and select Symantec Endpoint Protection) and select the Scan for threats option from the menu.

You can also easily configure Symantec Endpoint Protection to automatically schedule a scan of your local disks at a regular interval - say once a week. To do this, start up Symantec Endpoint Protection as described above, select the Scan for threats option from the menu and select Create a New Scan option. Follow the prompts to set the properties of the scan. Remember to save the schedule.

11.6 HOW WILL SYMANTEC ENDPOINT PROTECTION BE TO DATE?

It is obviously critical that the Symantec Endpoint Protection software regularly updates its virus files so that it can detect the latest viruses. To achieve this, the Symantec Endpoint Protection software on your computers connected to the network, will automatically update itself on a regular basis. You do not need to be logged on to the AD network for this to happen.

11.7 HOW DO I OBTAIN A COPY OF SYMANTEC ENDPOINT PROTECTION TO INSTALL AT HOME?

1. Visit the Intranet site: http://intranet.vu.edu.au/antivirus/.
2. Refer to the Software section of the Student User Guide CD.
3. Borrow a copy from IT Support Staff on your campus or contact the IT Service Desk on 9919 2777.

This software is only for use by currently enrolled students of VU. If at any time the computer on which this is installed is used as part of a personal business or company which intends to create an income or cash flow outside of the University's audited budget, you must purchase your own licensed copy. If you are no longer enrolled at Victoria University, this software must be uninstalled and deleted.

Please Note: To install Symantec Endpoint Protection you must uninstall any other Antivirus program first.

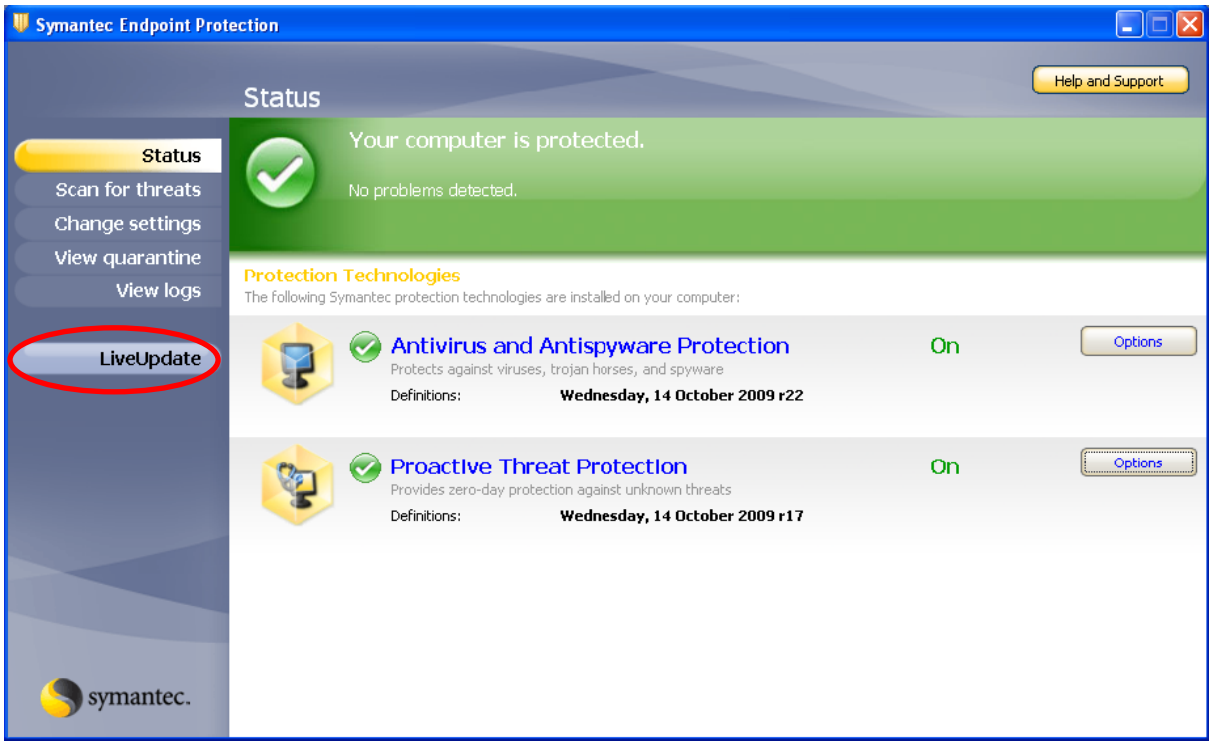
11.8 HOW DO I INSTALL SYMANTEC ENDPOINT PROTECTION?

Refer to installation guides available at http://intranet.vu.edu.au/antivirus

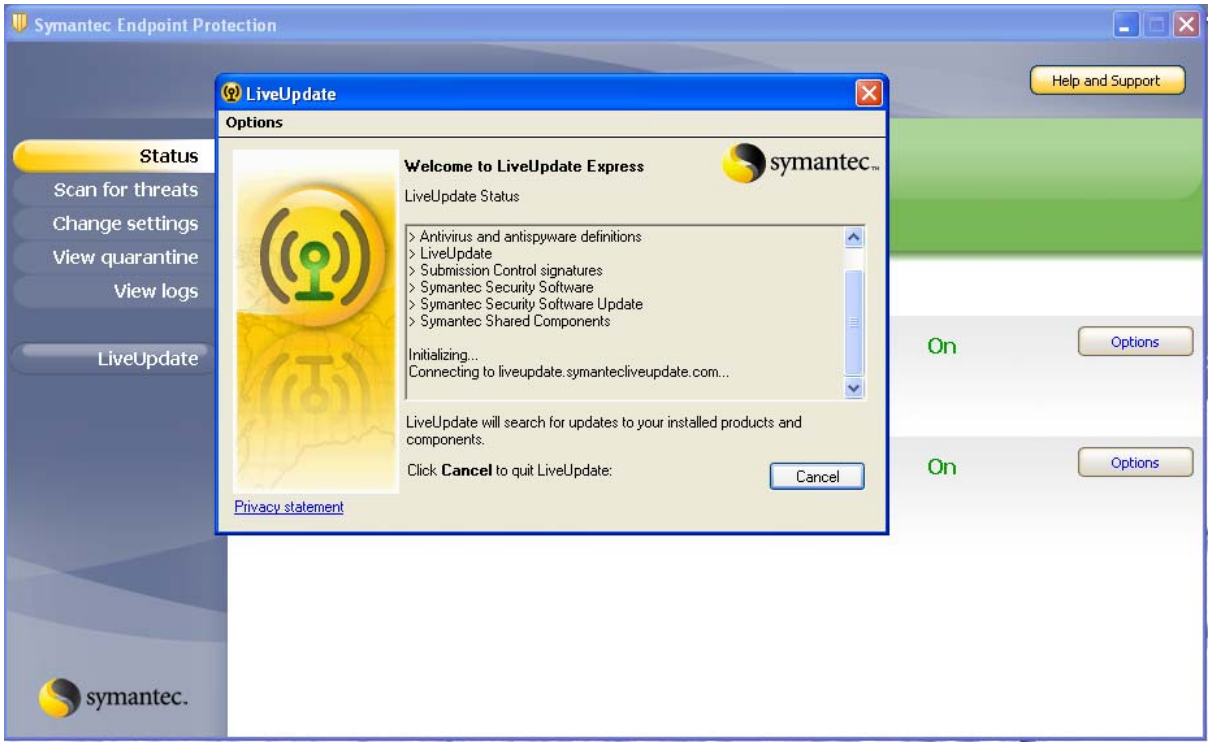
11.9 HOW DO I INSTALL THE LATEST UPDATE OF SYMANTEC ENDPOINT PROTECTION WITH INTERNET ACCESS AT HOME?

1. Open the Symantec Endpoint Protection program. To do this you can double click on the golden shield icon  , which can be found in the bottom right hand corner of your computer screen.

2. Use the **Live Update** button to obtain and install the latest update.



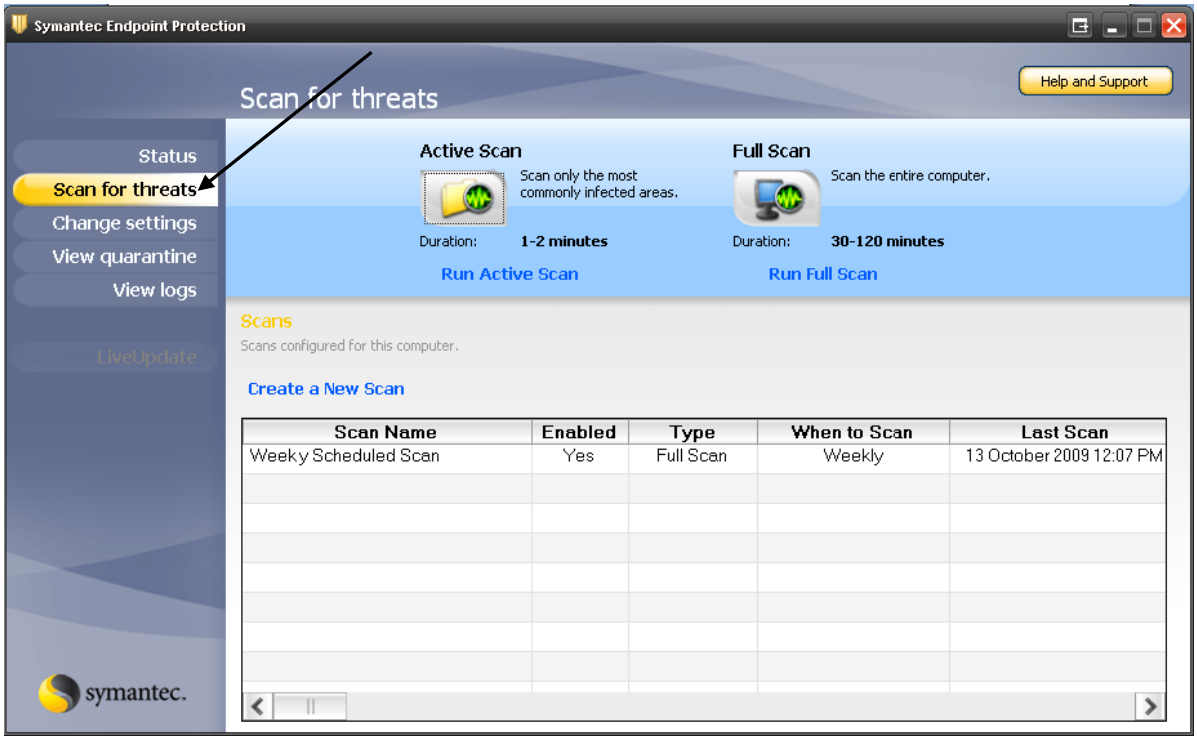
3. The Live Update window will disappear once the installation is complete.



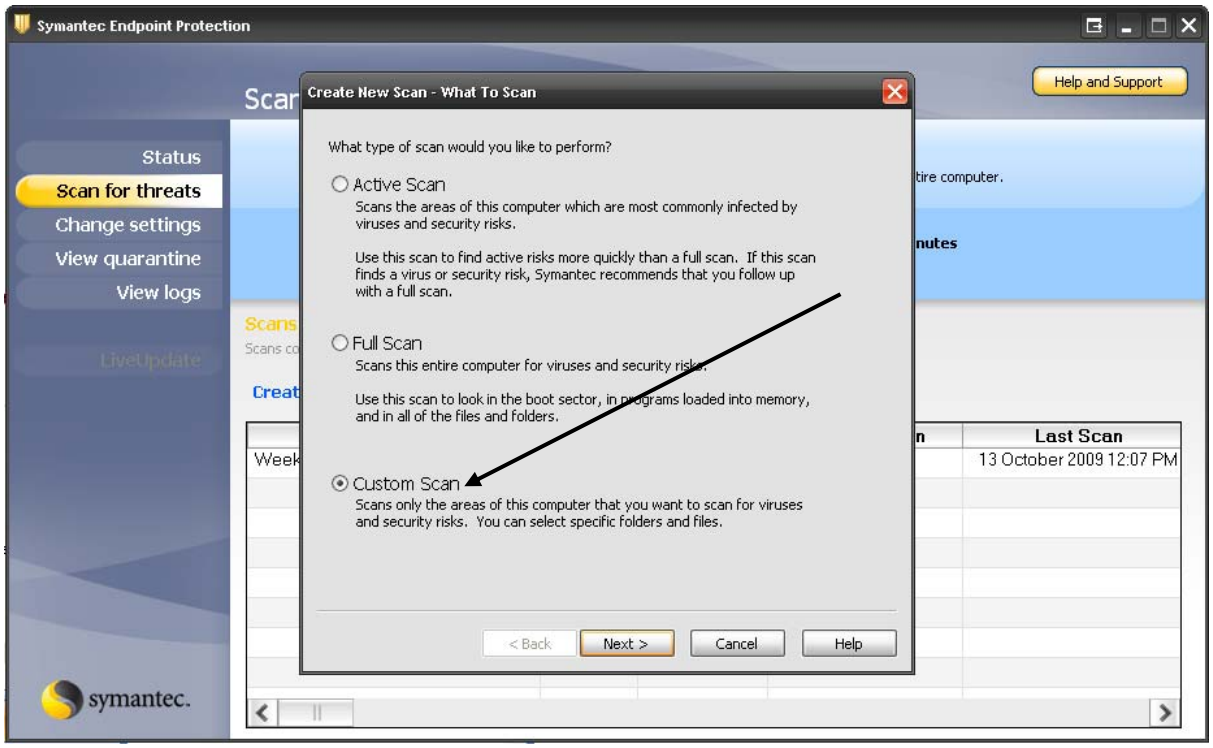
Note: If you do not have Internet access at home, then you can download the latest update file from the University Intranet http://intranet.vu.edu.au/antivirus/ or see IT Support Staff on campus to borrow a CD.

11.10 HOW DO I CHECK MY DRIVES FOR VIRUSES USING SYMANTEC ENDPOINT PROTECTION?

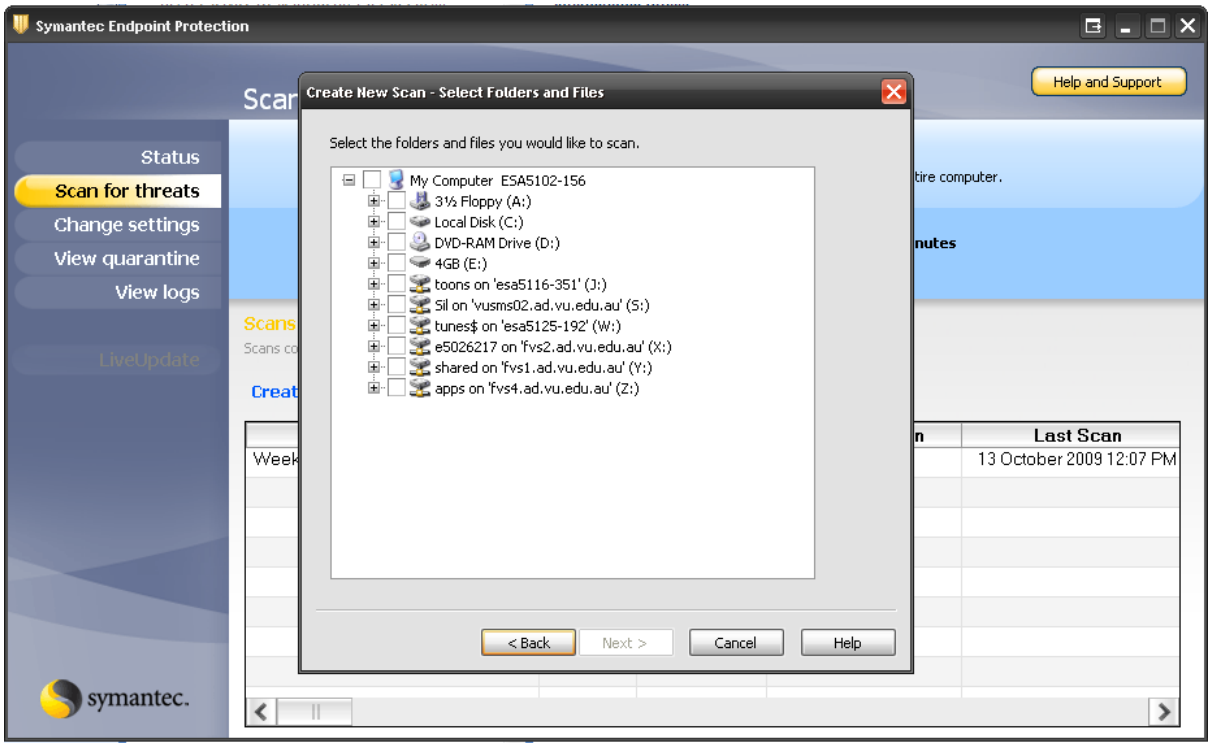
1. Open Symantec Endpoint Protection software.
2. From the menu on the left hand side select Scan for threats, and then choose Active Scan or Full Scan.



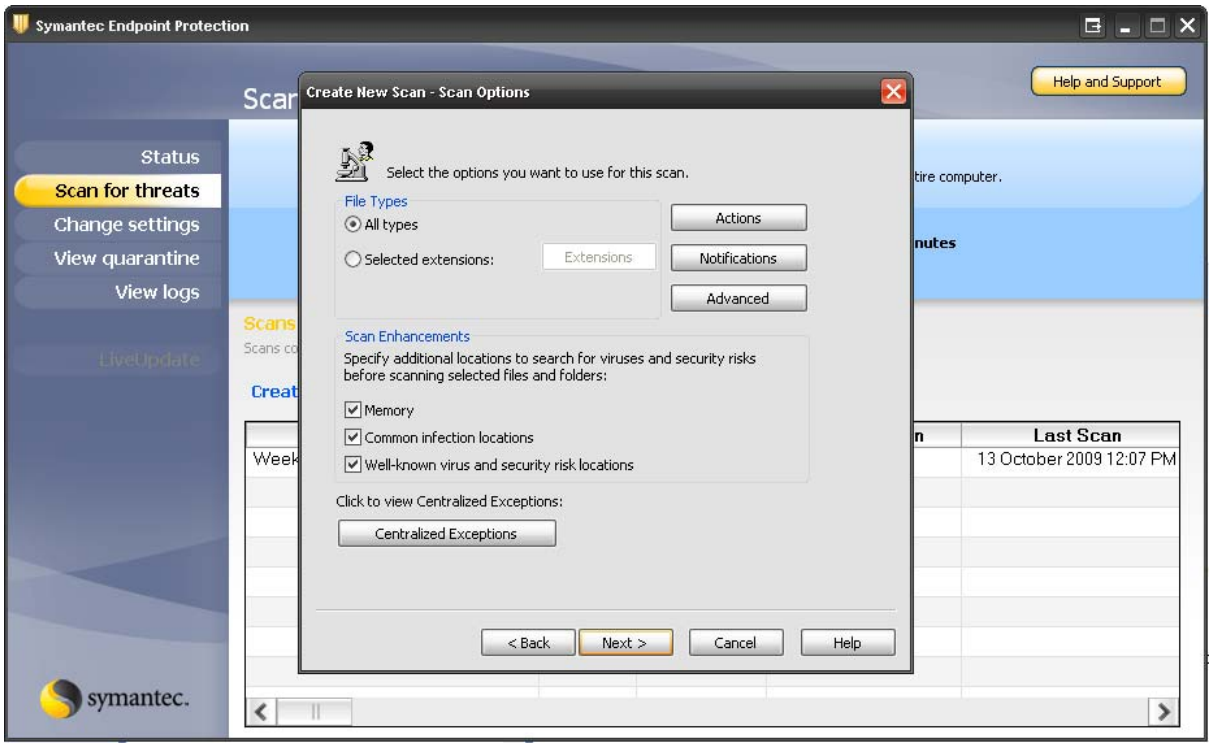
3. If you want to set up a scan for only selected drives or folders located on your PC or Network, select Create a New Scan, and then select Custom Scan, and click Next.



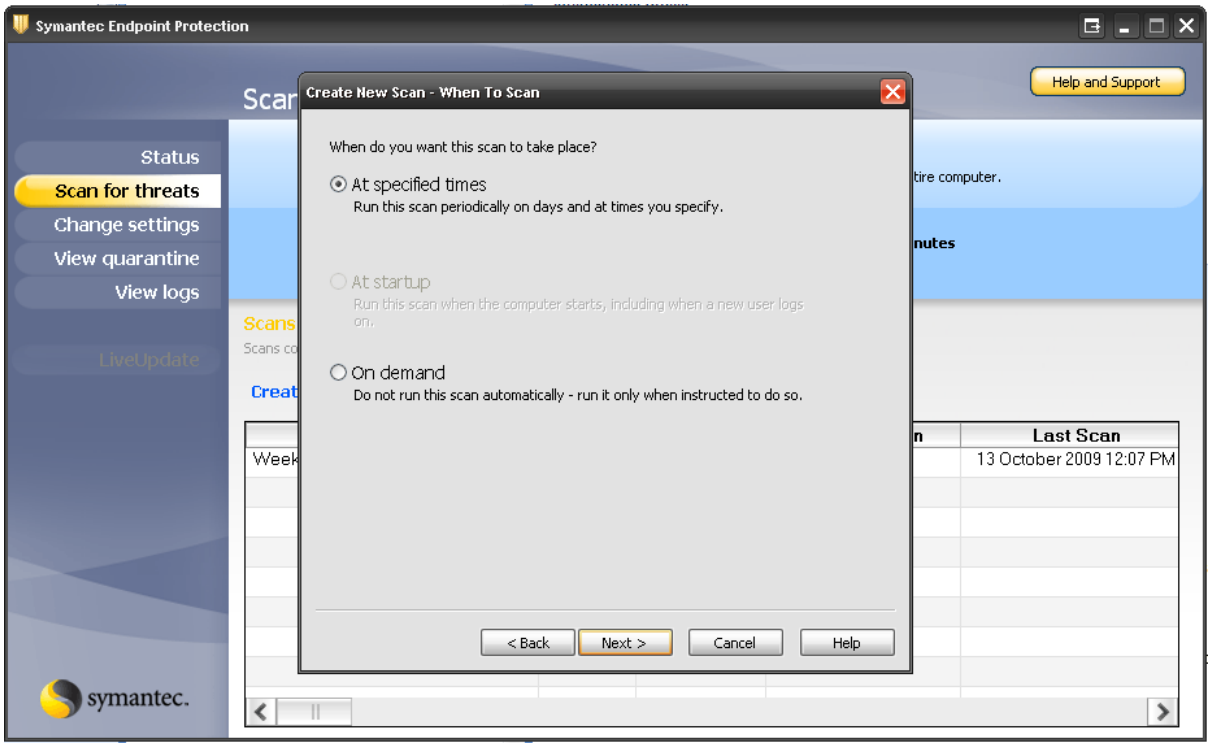
4. Once the scan has completed, the dialogue box will display any files that may be infected and any action that was taken.



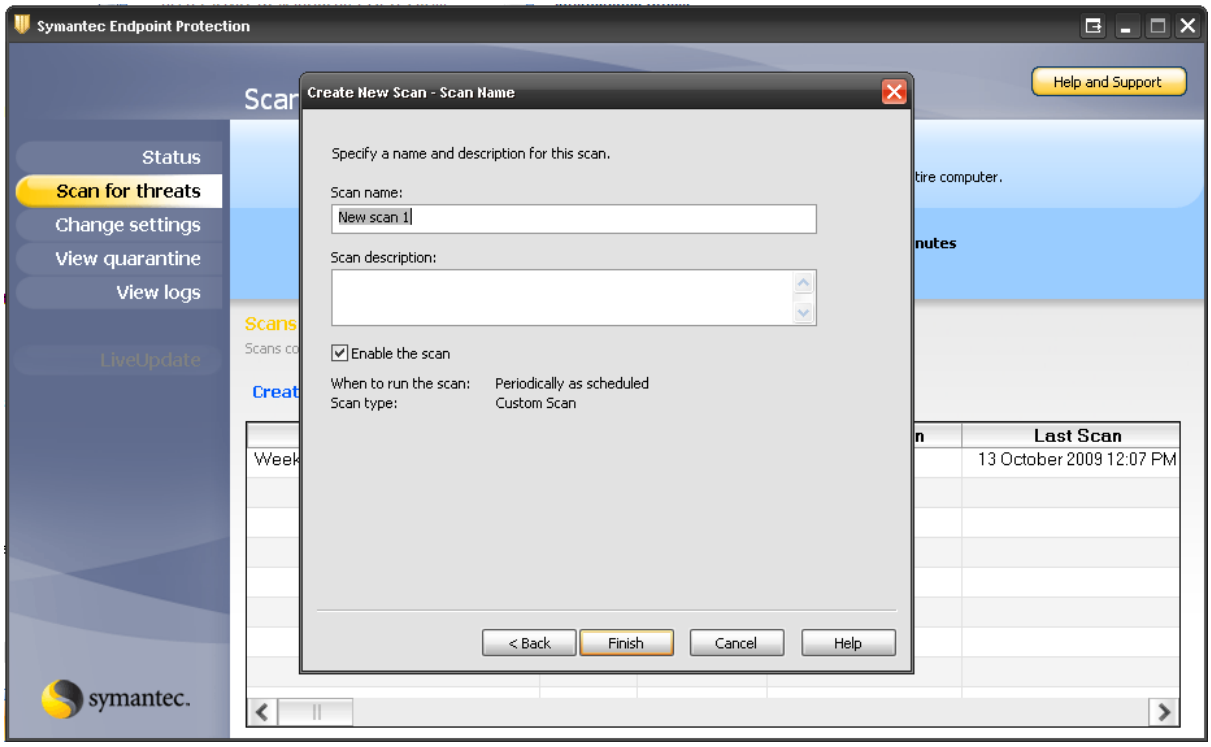
5. Tick the box, or expand the drive by clicking the + to locate the folder/s that you wish to check and click Next.



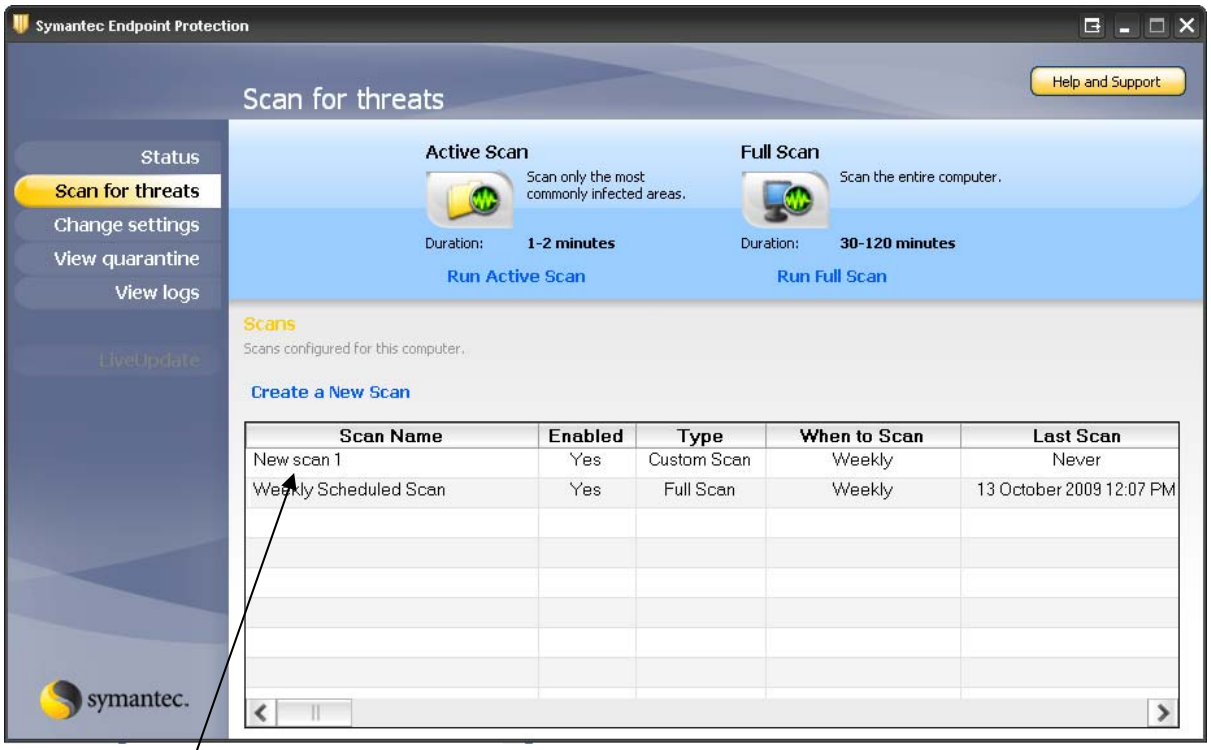
6. Select the options for scanning, unless selecting advanced options, the settings can be left as default, click **Next**.



7. Decide whether you want the scan to be run when you choose, by selecting **On Demand**, or at a schedualed time by selecting **At specified times**.



8. Enter the details for the newly created scan, and click **Finish.**



9. You can now choose to run this scan by right clicking on the scan and choosing **Scan Now**.

11.11 FURTHER INFORMATION ON SYMANTEC™ ENDPOINT PROTECTION

Please see the following links for further information regarding Symantec™ Endpoint Protection and virus removal http://intranet.vu.edu.au/Antivirus/ and http://www.symantec.com/