

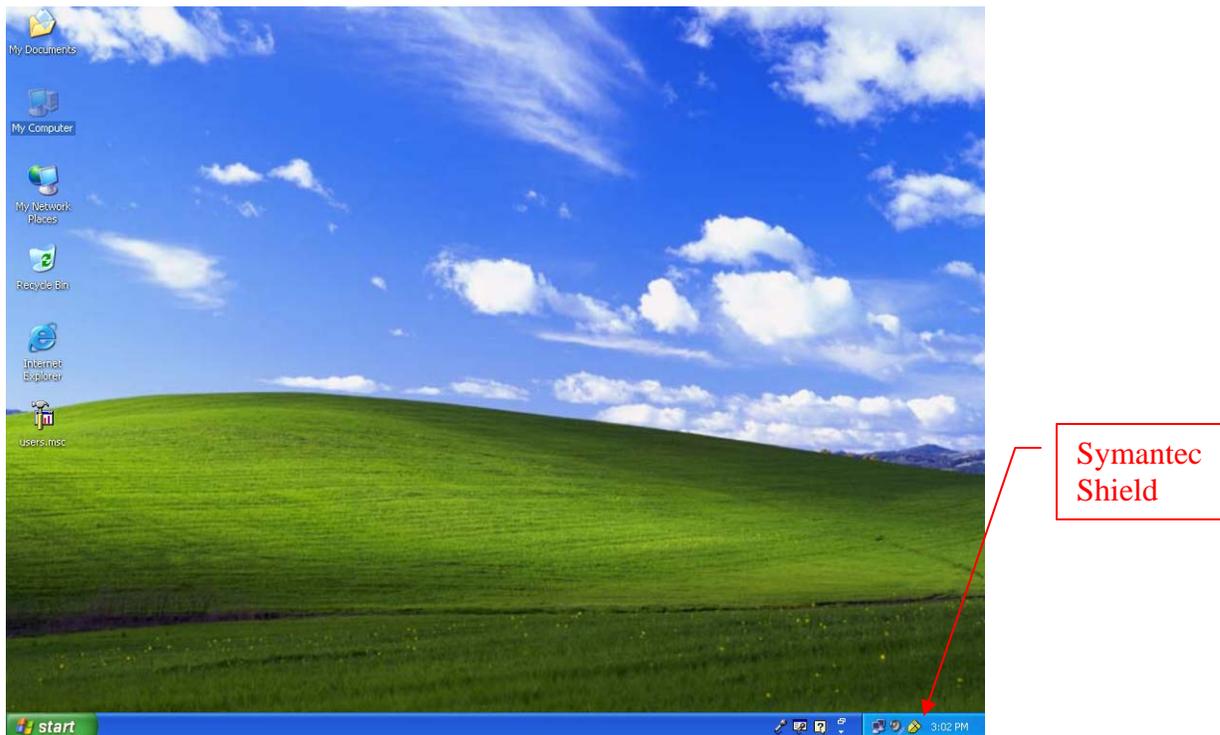
Symantec Anti-Virus Software at FNAL

Computers are susceptible to a proliferation of attacks. The lab has taken steps to lessen the number of attacks by blocking offsite NetBIOS probes, scanning all incoming email for viruses, and providing anti-virus software on all the major windows fileservers on site.

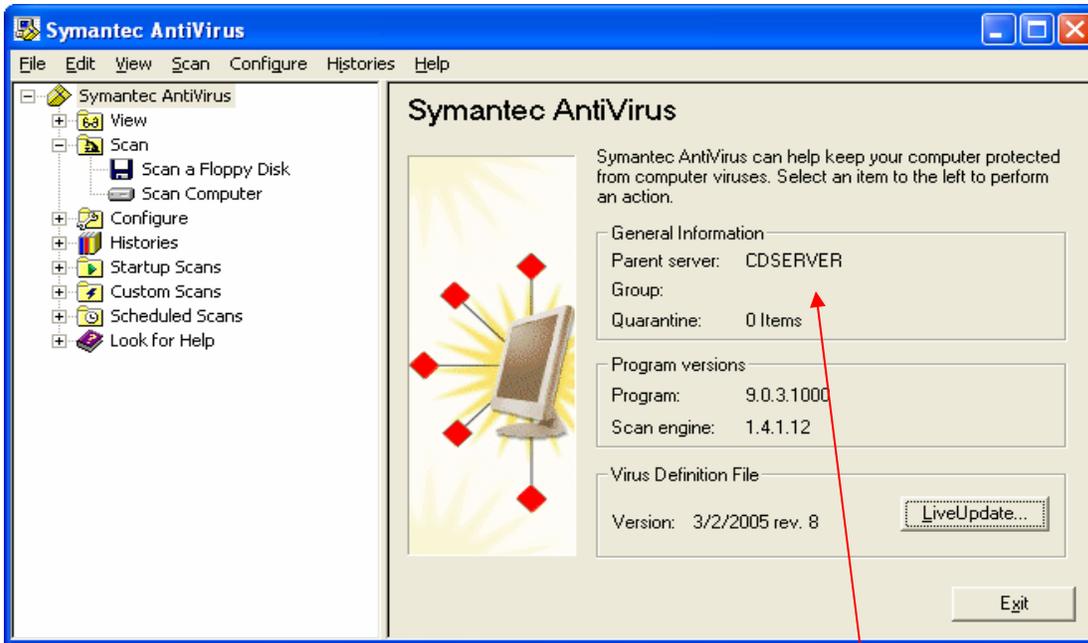
The lab divisions, sections and major experiments all have centralized anti-virus solutions. Fermi domain member systems are required to participate in the existing infrastructure. User benefit by having their systems get up to date Virus signature files almost instantly when the vendor provides new up dates.

Is Your System Centrally Managed?

Most of the lab divisions, sections and major experiments use Symantec's latest Anti-Virus software. To see if your systems is managed and is up to date with the latest virus signature protection files, look for a 'shield' in the lower right hand portion of your screen:

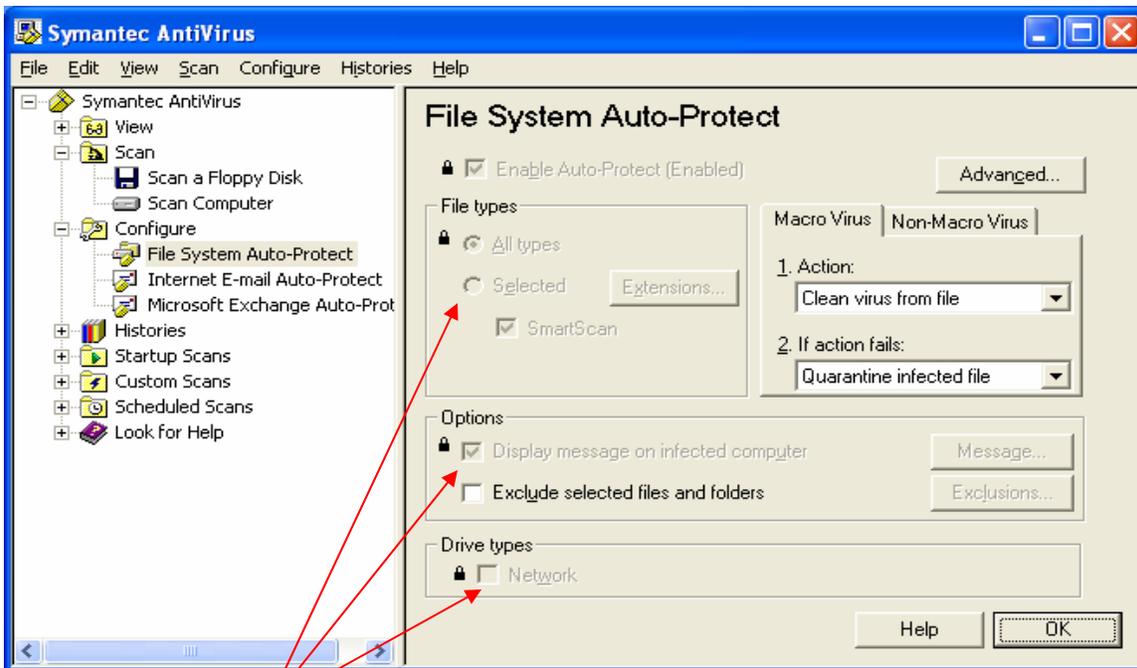


If you double click on the shield, you will be presented with the main interface screen to the anti-virus software.



If your system is 'managed', you will have an entry in the 'Parent Server' field.

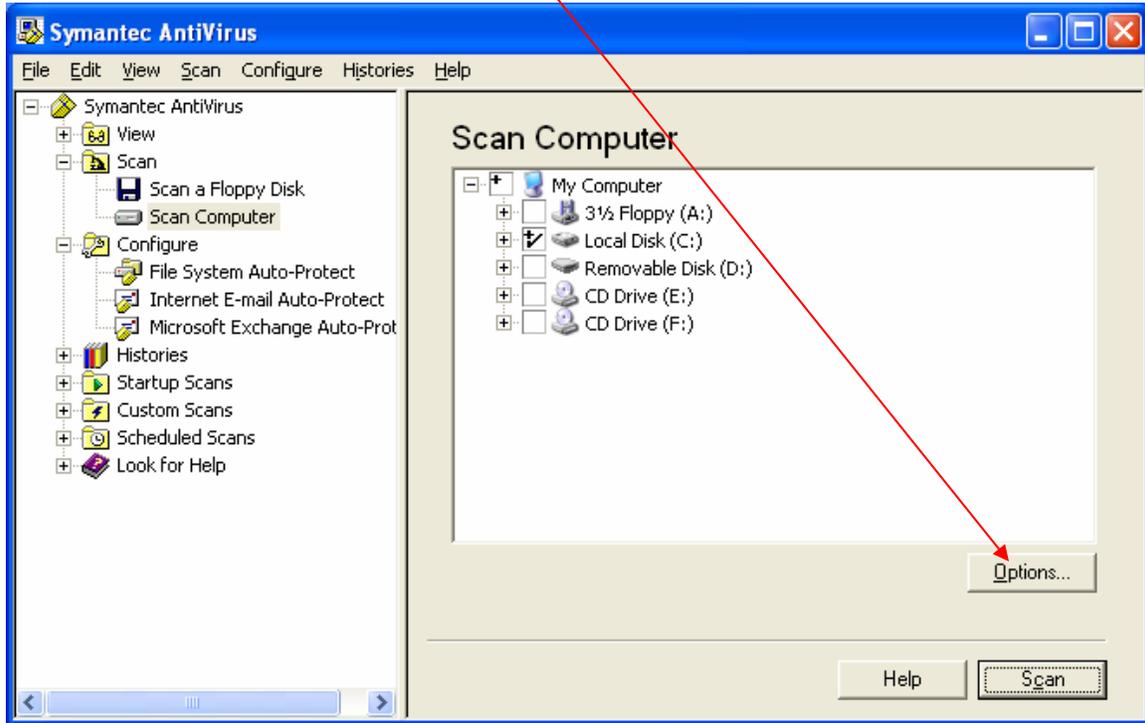
Managed systems have the 'Auto Protect (Real time scanning)' turned on. This setting and other details regarding real time scanning are viewed with the 'Configure/File System Auto-Protect' tab:



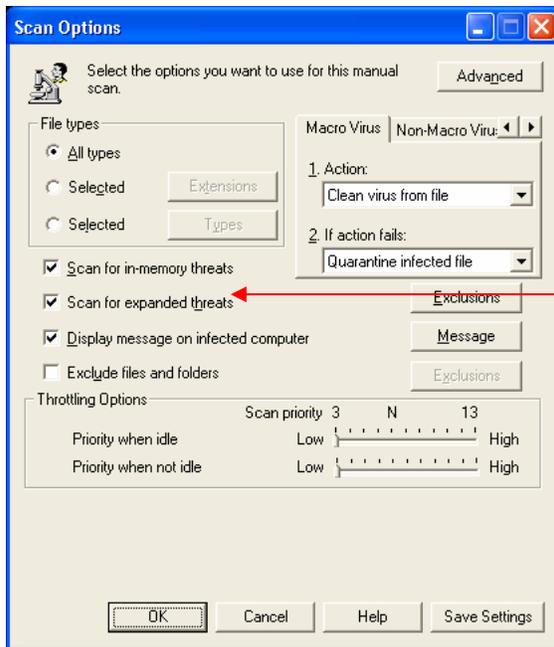
Some fields are *grayed out* as they are set and locked by the managing server. This helps prevent accidentally turning off the anti-virus protection, or preventing clever 'bad' applications from disabling the anti-virus software without your permission.

Scanning for Viruses and Spyware

A new feature in Version 9 of the product is to allow you to scan for Adware/Spyware. This is accomplished by using the Options feature of the manual scan of the product:

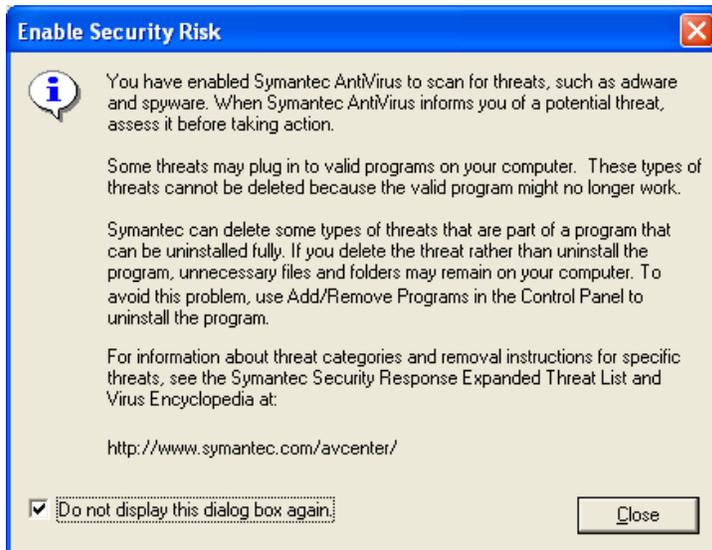


Managed systems are routinely scanned, but you can invoke a scan anytime. The new Adware/Spyware detection system is not done in real-time, so you will need to run a scan to check for adware/spyware. The managed systems when scanned by the parent automatically are scanning for adware/spyware. To scan for adware/spyware, you must activate the 'Expanded' threats option.

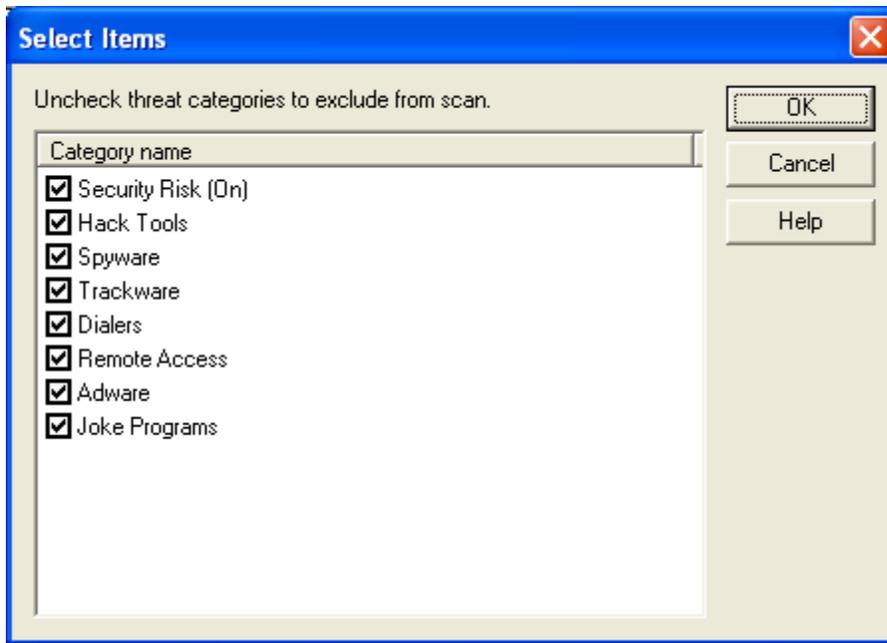


Be sure to click the *Scan for in-memory threats* and *Scan for expanded threats* boxes!

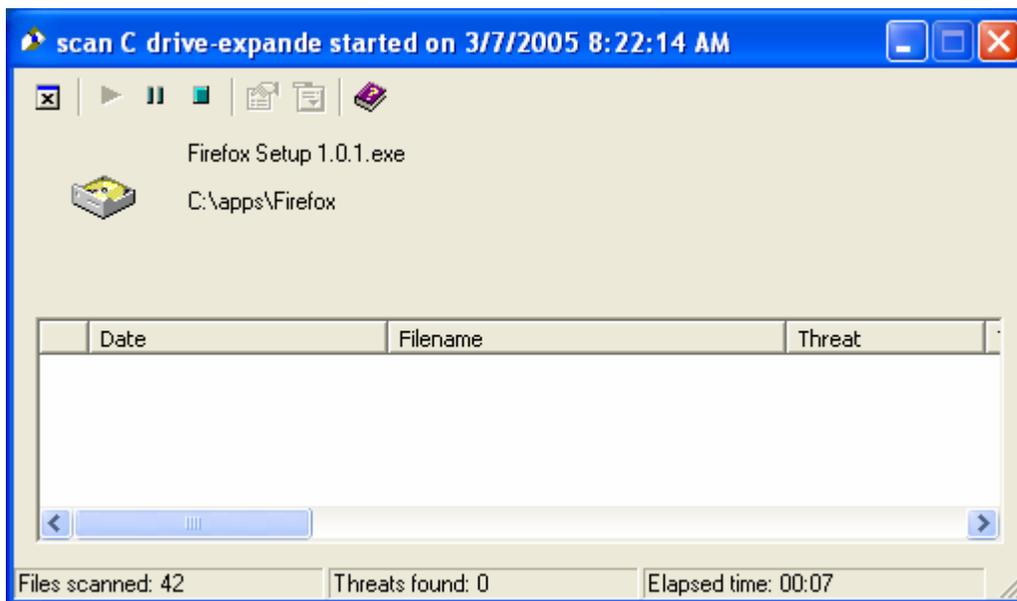
By default, the ‘Scan for in-memory threats’ and ‘Scan for expanded threats’ is not turned on, so make sure you select these if you do a manual scan. If this is the first time you have requested an expanded scan, you will receive a message like the following:



If you do select, “Scan for Expanded threats”, you can exclude/include various sub-categories of threats. Simply press the, “Exclusions” button to see the following:



In general, it is best to allow the default of scanning all sub-categories of adware/spyware. Once the scan starts, you will be presented with a pop-up box that looks similar to the following:



If any virus and/or adware/spyware are found, details will be in the pop-up box. You can go to the Symantec site with the name of the virus to gain more detailed information.