

TECHNICAL GUIDE No. 10

SCREENSHOTS

What To Do When Symantec AntiVirus Corporate Edition or Norton AntiVirus Corporate Edition Detects A Virus

Firstly you need to view the Virus History from the Symantec System Center Console, this is normally installed on your server computer.

1. On the machine that has your system centre console (SSC) installed, Start the SSC by Clicking Start, Programs, Symantec System Centre Console, and Symantec System Centre Console.
2. Unlock the server group by following the tree on the left down by clicking the small plus symbols as you go down to expand the level below starting at Console Root, then Symantec System Centre, then System Hierarchy, then right click on your main server group directly below System Hierarchy and click unlock server group. If you see small minus signs against items in the tree they are already expanded and you do not need to click them to reveal the items below.
3. Enter your antivirus server group password, and the padlock icon against the group should unlock.
4. Right-click the server group in the window on the left to view information for all machines in the group, or right-click a client computer in the window on the right to view information for that client only.

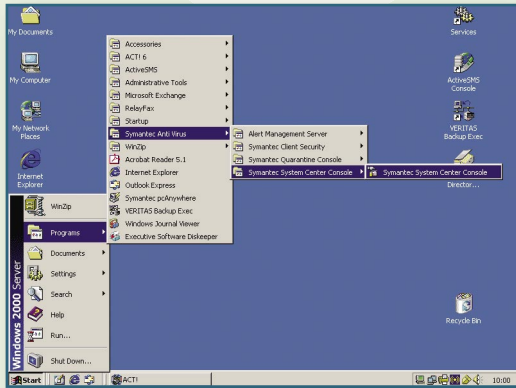
NOTE: You can only view information from a specific client if that computer is currently communicating with the SSC, so if you are looking at one workstation in particular then that workstation will need to be turned on and connected to the network before you proceed.

5. Click All Tasks > Symantec AntiVirus > Logs, and then click Virus History. The Virus History window appears. This provides a list of recent virus events on either the whole group, or your selected computer only depending on where you made the selection above in step 4.
6. Use the horizontal scroll bar to view the Virus Name, Action Taken, and Scan Type columns.

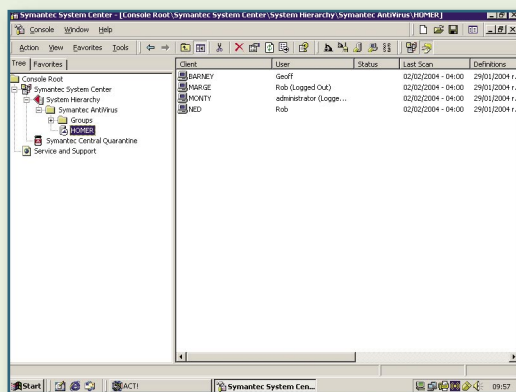
NOTE: It may be helpful to resize the Virus History window for easier viewing.

Examine the Action Taken for the new entries in the log

If the Action Taken is Repaired or Deleted, the virus has been successfully eliminated from your system and you need to take no further action. If the action taken is Quarantined then the virus has been successfully extracted from the machine, and is now stored safely in Quarantine, and the only action you need take is remove the file from the Quarantine folder (See our Technical Document - Clearing files from Symantec Central Quarantine). If the Action Taken is Left Alone, and the infected file is not in Quarantine, then the computer is probably already infected and the virus is loading into memory when Windows starts. To resolve this, either contact Conquest Wildman or restart the computer in Safe mode and run a full system scan. If you are using Windows NT, perform a clean boot, and run a full system scan. *For more information see our Technical Document "Starting Your Computer In Safe Mode", for more details.*



Loading System Centre Control



System Centre Control