How to manually uninstall Symantec Endpoint Protection client from Windows Vista, Windows 7, and Windows 2008 32-bit

Question/Issue:

This document describes how to remove Symantec Endpoint Protection client from 32-bit versions of Windows Vista, Windows 7, and Windows 2008 manually.

Solution:

Warning: These removal steps can disable other Symantec products that are installed on the computer. It is recommended that all Symantec products be uninstalled by using Add or Remove Programs before starting this process.

Log on as Administrator

Manual removal of Symantec Endpoint Protection must be done from the Administrator account. To enable the Administrator account, read the following document from the Microsoft Knowledge Base: <u>Enable and Disable the Built-in Administrator Account</u>.

When the Administrator account is enabled, log on to that account.

Stop Symantec Endpoint Protection

- 1. Click **Start** > **Run.**
- 2. Type msconfig
- 3. Click OK.
- 4. On the Startup tab, uncheck Symantec Security Technologies.
- 5. In the Services tab, uncheck the following (not all may be present):
 - Symantec Event Manager
 - Symantec Settings Manager
 - LiveUpdate
 - Symantec Management Client
 - Symantec Network Access Control
 - Symantec Endpoint Protection
- 6. Click **OK**, and then restart the computer.
- 7. After the computer starts up, an alert appears. Check the box and click **OK**.

Remove the Teefer2 driver

- 1. Click Start > Settings > Control Panel > Network Connections.
- 2. Click a connection.
- 3. In the dialog, click **Properties**.
- 4. Select **Teefer2 Driver** and click **Uninstall.**
- 5. You will need to repeat these steps for each Network Connection.
- 6. Restart the computer.

Remove Symantec Endpoint Protection from the registry

1. Run the Windows Installer Cleanup Utility to remove Symantec Endpoint Protection 11.0.

The Windows Installer Cleanup Utility can be found at the following URL: <u>http://support.microsoft.com/default.aspx?scid=kb;en-us;290301</u>

Notes:

After removing Symantec endpoint Protection with the Windows Installer Cleanup Utility:

- Symantec Endpoint Protection does not appear in Add/Remove Programs.
- Symantec Endpoint Protection services are still present.
- Symantec Endpoint Protection may still be operational.
- 2. Click Start > Run.
- 3. Type regedit and Click **OK**.
- 4. In the Windows registry editor, in the left pane, delete the following keys if they are present. If one is not present, proceed to the next one.
 - HKEY_CLASSES_ROOT*\Shellex\ContextMenuHandlers\LDVPMenu
 - HKEY_CURRENT_USER\Software\Symantec\Symantec Endpoint Protection
 - HKEY_LOCAL_MACHINE\SOFTWARE\Sygate Technologies, Inc.
 - HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\InstalledApps, SAVCE value only
 - HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection
 - HKEY_LOCAL_MACHINE\SOFTWARE\Whole Security
 - HKEY_LOCAL_MACHINE\SOFTWARE\Intel\LANDesk
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentV ersion\Uninstall\LiveUpdate
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentV ersion\Uninstall\SevInst
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Virtua lDeviceDrivers
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ccEvt Mgr
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ccSet Mgr

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\eeCtr
 l
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Erase rUtilRebootDrv
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Live Update
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NAV ENG
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NAV EX15
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SmcS ervice
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNA C
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Snac Np
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SPB BCDrv
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SRTS
 P
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SRTS PL
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SRTS PX
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Syma ntec AntiVirus
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sym Event
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SYM REDRV
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SYM TDI
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Teefe r2
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Wps
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Wps Helper
- HKEY_LOCAL_MACHINE\SYSTEM\Symantec
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Event log\Application\ccSvcHst
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Event log\Application\LiveUpdate
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Event log\Application\SescLU
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Event log\Application\Symantec AntiVirus

- 5. Navigate to the following key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ Uninstall
- 6. Select Uninstall.
- 7. Select Edit
- 8. Click **Find**.
- 9. Type symantec
- 10. Click **Find Next**.

A value appears in the right pane that includes the word Symantec, in a key that is still in

 $HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ Current \ Version \ Uninstall.$

If the key that is selected is still in

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ Uninstall, delete the key (in the left pane), and then repeat the search. If the key that is selected is not in

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ Uninstall, continue to the next step.

11. Remove any values with "Symantec" in the path from the following key:

 $HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ Current \ Version \ Shared Dlls$

- 12. Search for the following strings, and delete any registry keys that contain them:
 - 331D64B67B1D6024FAD99FA7FAAE8F3
 - Vpshell2
 - VpShellEx
- 13. Navigate to

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\I nstaller\UserData\S-1-5-18\Components\.

14. Under the following registry keys, delete the registry key

12AD9A2D657B7654F96A2EA43F3166B3:

- 0E3118066B3FEE6C0AF18C3B9B1A1EE8
- 2A31EAB9FA7E3C6D0AF18C3B9B1A1EE8
- 6EC3DF47D8A2C9E00AF18C3B9B1A1EE8
- 7ABFE44842C12B390AF18C3B9B1A1EE8
- C9AE13788D0B61F80AF18C3B9B1A1EE8
- DA42BC89BF25F5BD0AF18C3B9B1A1EE8

Remove Symantec Endpoint Security files and folders

- 1. Restart the computer into Safe Mode. To enter Safe Mode on Windows Vista and Windows 7, read the Microsoft article <u>Start your computer in safe mode</u>.
- 2. In Safe Mode, log on as the Administrator account.
- 3. Delete the following files and folders. If a file or folder is not present, proceed to the next one.

- C:\Program Files\Symantec\Symantec Endpoint Protection (Or the appropriate directory if you installed in a different one)
- C:\Program Files\Symantec\LiveUpdate (Or the appropriate directory if you installed in a different one)
- C:\Program Files\Symantec\ (Or the appropriate directory if you installed in a different one)
- C:\Program Files\Common Files\Symantec Shared
- C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\Symantec Endpoint Protection
- C:\ProgramData\Symantec
- 4. Delete the following driver files in C:\Windows\System32\drivers. In all cases delete the files with the extensions .sys, .cat, and .inf with the following prefixes:
 - Coh_Mon
 - SrtSp
 - SrtSp64
 - SrtSpl
 - SrtSpl64
 - SrtSpx
 - SrtSpx64
 - SymDns
 - SymDns64
 - SymEvent
 - SymEvent64x86
 - SymFw
 - SymIds
 - SymNdis
 - SymNdisv
 - SymRedir
 - SymRedrv
 - SymTdi
 - SysPlant
 - Teefer2
 - Wgx
 - WpsDrvnt
 - WpsHelper
- 5. Delete the following driver files in both C:\Windows\System32 and C:\Windows\SysWOW64:
 - BugslayerUtil.dll
 - Cba.dll
 - FwsVpn.dll
 - Loc32Vc0.dll
 - MsgSys.dll
 - Nts.dll
 - Pds.dll
 - SysFer.dll
 - SymVPN.dll

- 6. Go to C:\Windows\Installer\.
- 7. For each file in C:\Windows\Installer, right-click the file and select **Properties**.
- 8. On the Summary tab, check to see whether the file was created by Symantec. If it was, delete the file.
- 9. Repeat steps 6-9 for every file in the folder.

Remove the Teefer driver

- 1. Click **Start** > **Search**, type **cmd**, and press **Ctrl+Shift+Enter** to start a command prompt with Administrator privileges.
- 2. Type **pnputil -e** to list the Symantec drivers in the driver store.
- 3. Type **pnputil -f -d oem**<*n*>.inf to remove Symantec drivers from driver store, where <*n*> is a number corresponding to one of the Symantec drivers listed in the previous step.
- 4. Type **exit** to close the command prompt.
- 5. In the Windows registry editor, navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36 E972-E325-11CE-BFC1-08002bE10318}.
- 6. Delete any keys that have a value of **ComponentId** that is set to **symc_teefer2mp**.
- Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasse s\{ad498944-762f-11d0-8dcb-00c04fc3358c}.
- 8. Delete any sub keys that have a name containing **SYMC_TEEFER2MP**.
- Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasse s\{cac88424-7515-4c03-82e6-71a87abac361}.
- 10. Delete any sub keys that have a name containing SYMC_TEEFER2MP.
- 11. Close the Windows Registry Editor.
- 12. In the Device Manager (devmgmt.msc), go to Network Adapters, and delete all entries with "teefer" in them.
- 13. Delete any network adapters to which teefer was attached. This causes the adapters to be reinstalled. This step must be done in order for there to be network connectivity after you restart the computer.
- 14. Restart the computer into normal mode.