Write Protect USB Devices in Windows XP

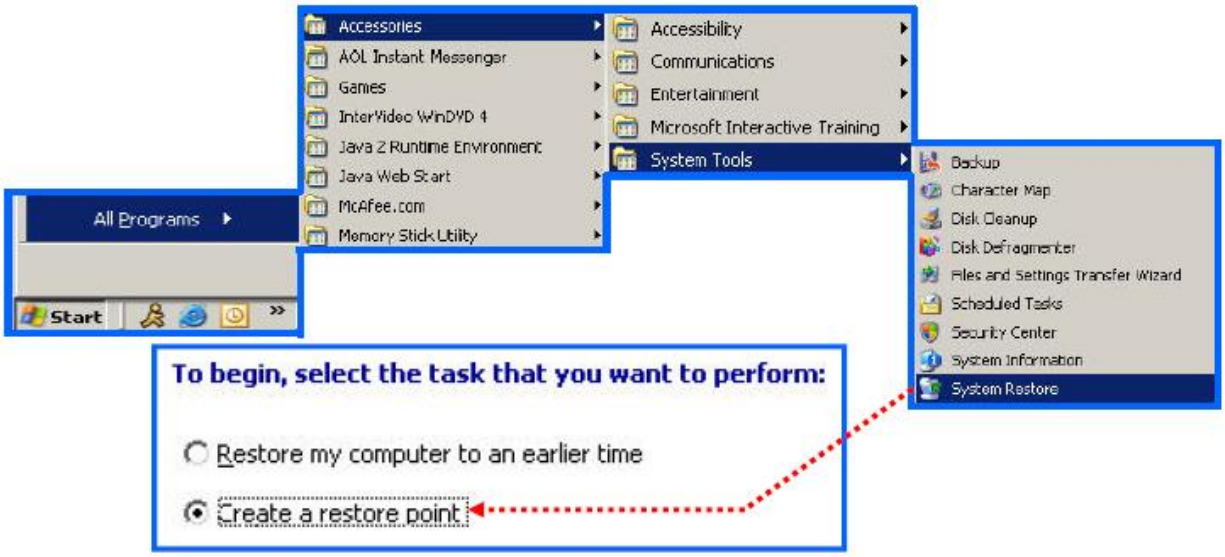
Dustin Hurlbut

For more information contact: info@syntricate.com

In the release of Windows XP Service Pack 3 (SP3), a feature was added by Microsoft to allow the write protection of USB block storage devices. This entails a simple Registry modification that requires no hardware devices to write protect thumb drives. This allows us to examine and duplicate USB devices with write protection that previously didn't exist.

To enable this feature, we'll go step by step to modify the Registry. As in all Registry operations, it is advisable to back up your Registry files prior to modification. You can do this easily by either creating a Restore Point in XP or by using FTK Imager to look at your own drive and export the Registry Files.

To create a Restore Point, go to Start > Programs > Accessories > System Tools > System Restore (see below). Once at the System Restore dialog box, select "Create a restore point" and follow the steps. This creates a backup of selected system files that can then be enabled to restore the system back to the state it was in.



SYNTRICATE

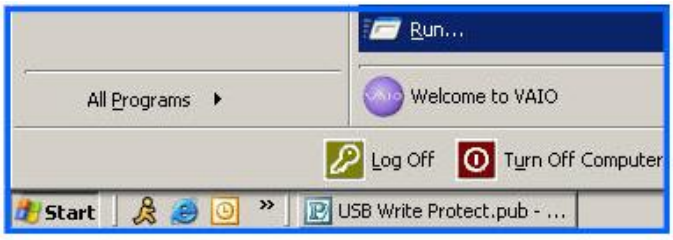
Write Protect USB Devices in Windows XP

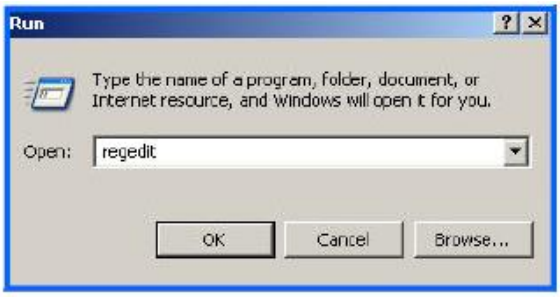
Dustin Hurlbut

For more information contact: info@syntricate.com

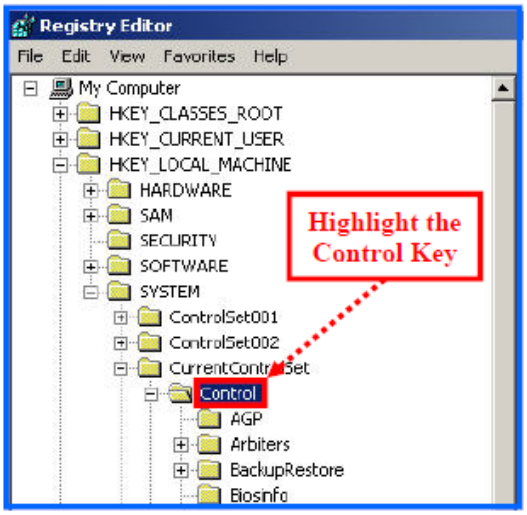
To create the necessary Registry values to enable USB write protection, follow these steps:

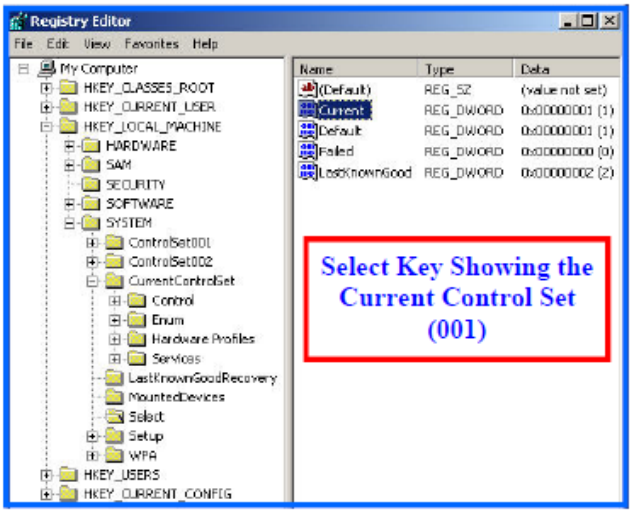
Step 1 - Go to Start > Run and type in regedit.





Step 2 - Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet and highlight the Control key. The CurrentControlSet key has system information about the current configuration of the machine. The system keeps a backup of this key. You will see the current and backup listed as ControlSet001 and 002 in this example. The select key will show which is valid. The key CurrentControlSet is the one being used at this moment and is the one you want to modify.





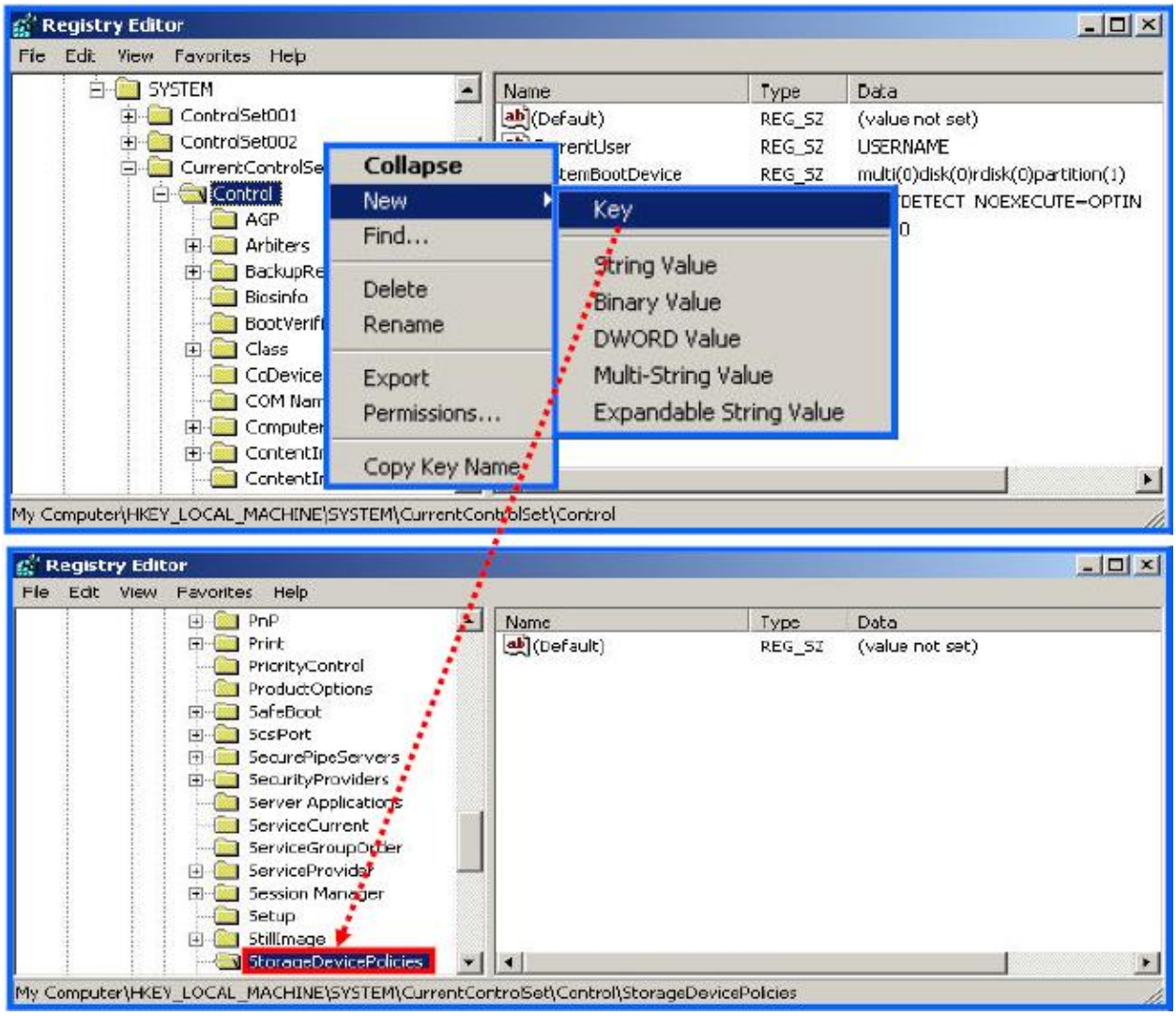
SYNTRICATE

Write Protect USB Devices in Windows XP

Dustin Hurlbut

For more information contact: info@syntricate.com

Step 3 - Right click on Control and select New > Key. Name the key ***StorageDevicePolicies***.



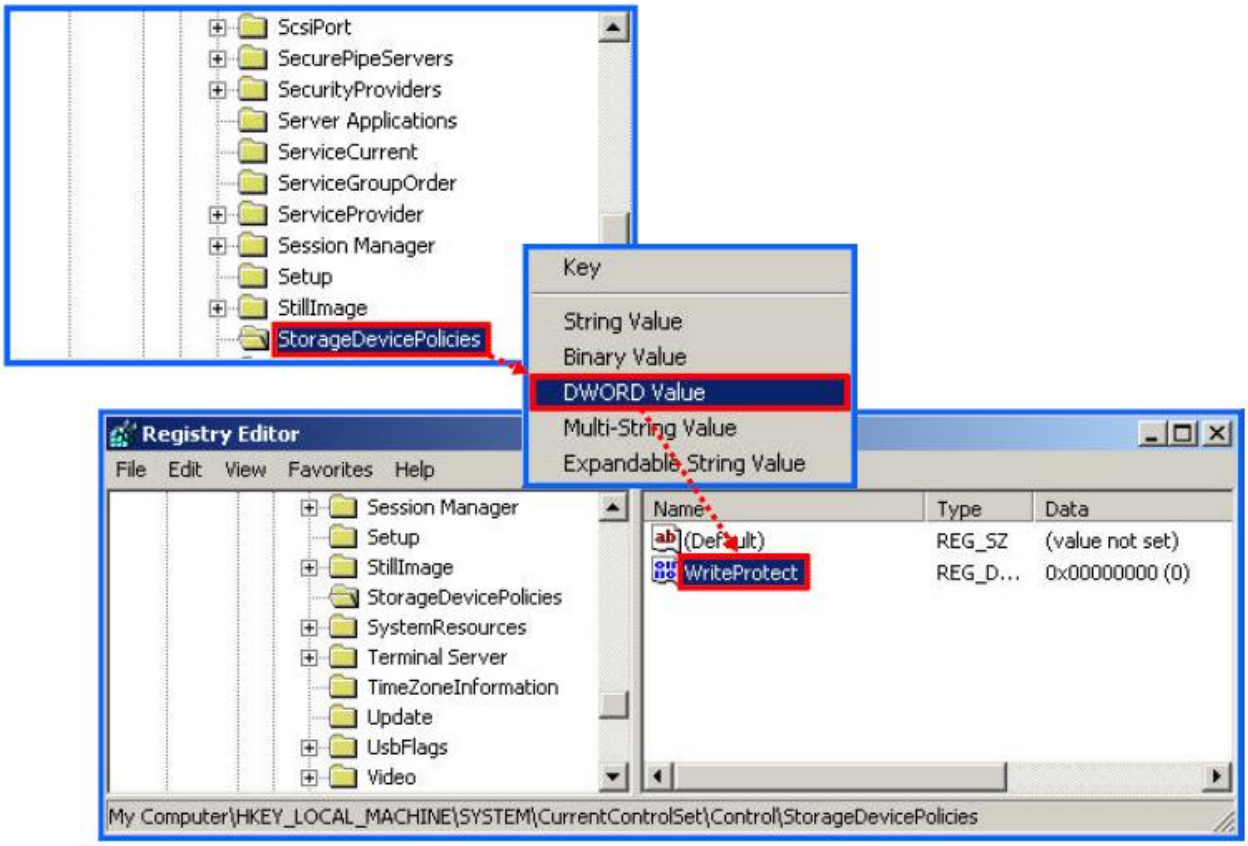
SYNTRICATE

Write Protect USB Devices in Windows XP

Dustin Hurlbut

For more information contact: info@syntricate.com

Step 4 - Right click on StorageDevicePolicies and select DWORD. Name the value ***WriteProtect***.



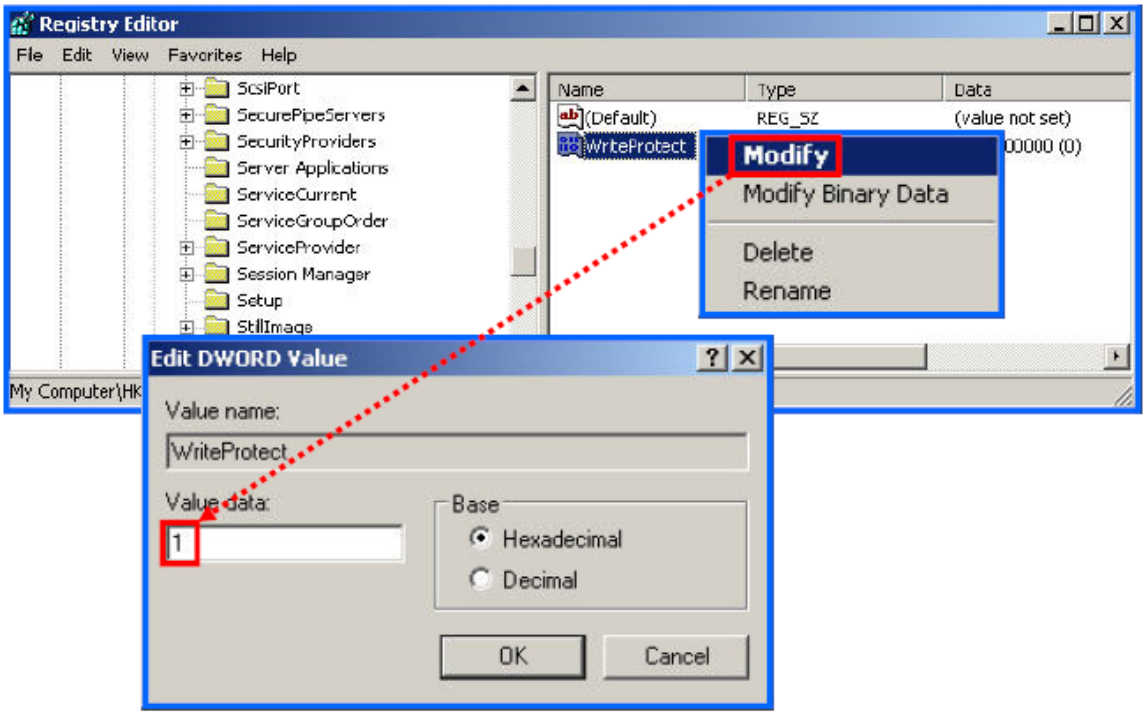
SYNTRICATE

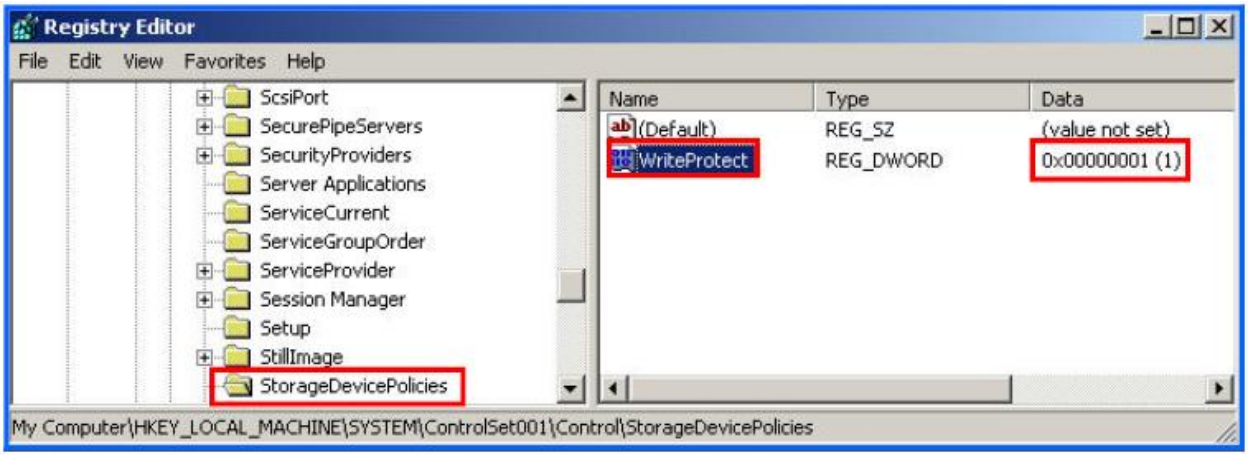
Write Protect USB Devices in Windows XP

Dustin Hurlbut

For more information contact: info@syntricate.com

Step 5 - Right click (or double click) on WriteProtect and select Modify. To write protect USB devices select 1 as the value. To turn off write protection, change this value to 0.





SYNTRICATE

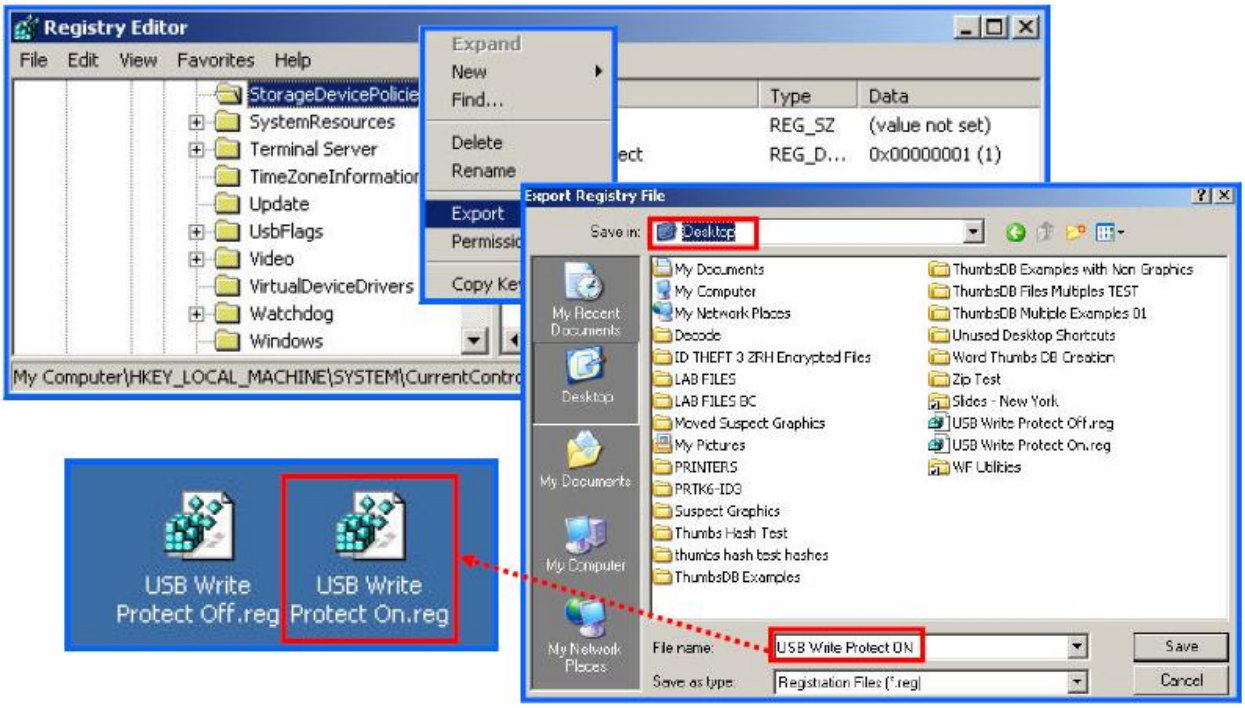
Write Protect USB Devices in Windows XP

Dustin Hurlbut

For more information contact: info@syntricate.com

We have created a new key and value in the Registry that will write protect USB devices. You may want to place this on your examination machine full time. However, if you need to be able to switch back and forth from a write protected state to an non write protected state, it is cumbersome to have to go through this procedure each time. To automate this process, create a .REG file to enable you to select either on or off.

To create a write protect switch, right click on the key StorageDevicePolicies we just modified and select "Export". Name it and you can send a file with the extension of .reg to your Desktop. Name it "USB Write Protect ON".



Recreate the key with the switch turned off to un-write protect the USB making another .reg file. You can activate either .reg file by clicking on it to modify the Registry key.

SYNTRICATE

Write Protect USB Devices in Windows XP

Dustin Hurlbut

For more information contact: info@syntricate.com

Be sure to test and verify this procedure and write protect function. The National Center for Forensic Science (NCFS) has a free program available to automate this function. They also have a five step validation process for verification that the program functions properly. This would also work for validation of the process described in this paper.

References:

1. Change to Functionality in Microsoft Windows XP Service Pack 2 - Part 7: Other Technologies
   Published: August 9, 2004 | Updated: September 15, 2004
   By Starr Andersen, Technical Writer; Vincent Abella, Technical Editor
   Microsoft TechNet Article:
   http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2otech.mspx

2. National Center for Forensic Science (NIJ)
   http://ncfs.ucf.edu/home.html - Reference the Link: NCFS Software Write-block XP

SYNTRICATE