ISCS Gatekeeper Keymaster

Last Reboot	4/18/2011 3:15:00 PM
Current Time	4/23/2011 12:45:10 AM
Uptime	4 days 9 hours 30 minutes 10 seconds

Enable USB [Enable] [Disable]

USB Drivers [Enable] [Disable]

Disabling Registry Edit [Enable] [Disable] [Not Configured]

No Control Panel [Enable] [Disable] [Not Configured]

Password [********]   [Reboot Now]

[Check Status]

Enable USB: DISABLED
USB Drivers: INF Driver disable
USB Drivers: INF file not found
USB Drivers: PNF Driver disable
USB Drivers: PNF file not found
DisableRegistryTool is ENABLED at HKEY_LOCAL_MACHINE
DisableRegistryTool is ENABLED at HKEY_CURRENT_USER
NoControlPanel is ENABLED at HKEY_LOCAL_MACHINE
NoControlPanel is ENABLED at HKEY_CURRENT_USER
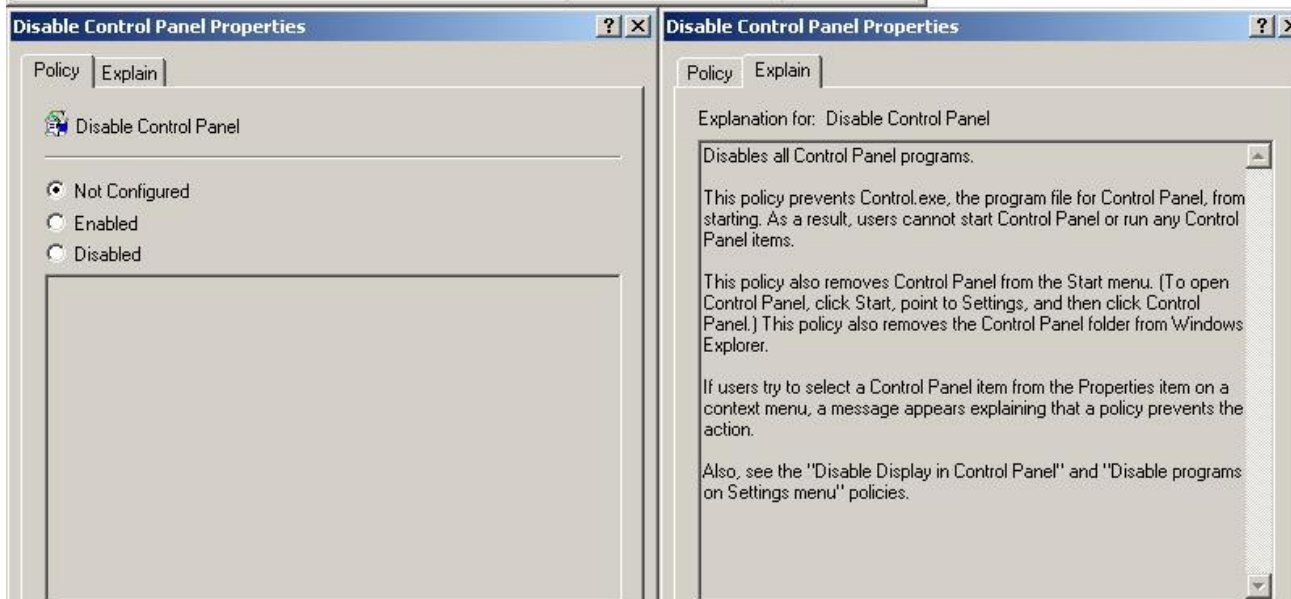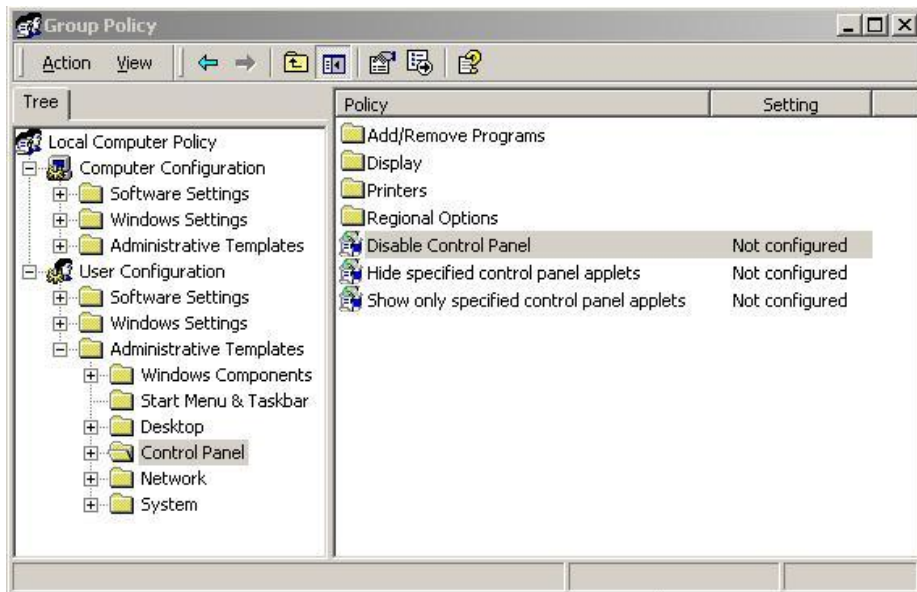
Check Status Function

1. Click on [Check Status] button to check on current configuration of Win2K settings.
2. Verify that all results showed **GREEN** to confirm that all access is blocked and proceed to reboot MFT, to enforce changes.
3. Following are examples of [Check Status] button output and respective button functions.
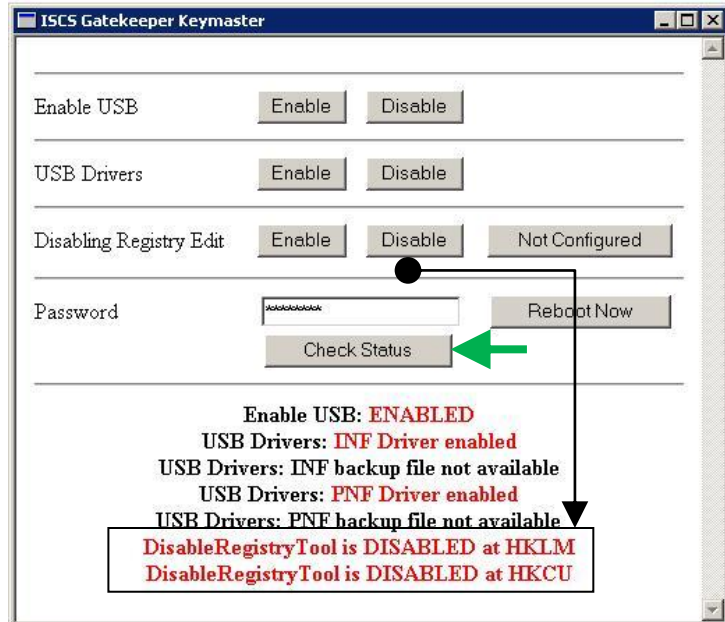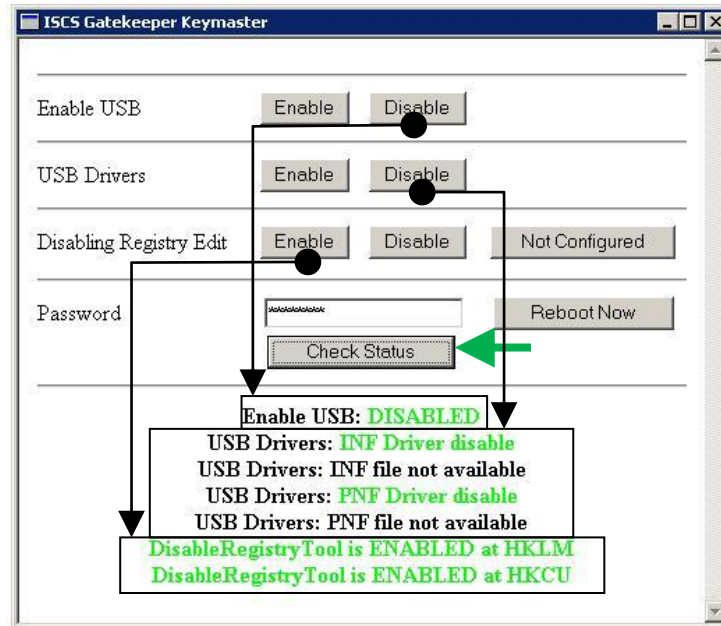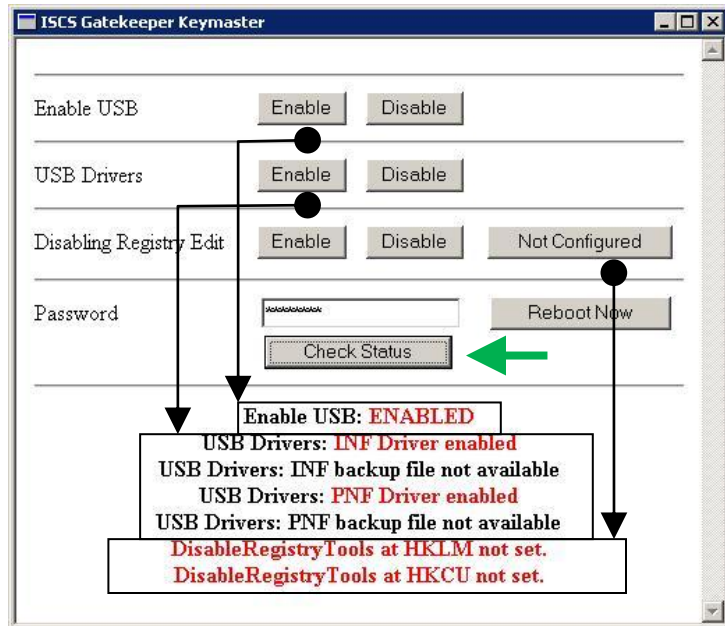
Enable/Disable/Remove NoControlPanel Function

1) This provides one click action to disable Control Panel access. It uses Group Policy function called **NoControlPanel.**

2) [Enable] button will disable Control Panel access from Start Menu and Settings.

3) [Disable] button will enable back Control Panel access.

4) [Not Configured] button will return all configurations back to original setting. Means that **NoControlPanel** will be removed.

5) Location of registry entry to <u>enable</u> **NoControlPanel**.

    a. HKEY_CURRENT_USER \ Software\Microsoft\Windows\CurrentVersion\Policies\Explorer \NoControlPanel REG_DWORD:1

    b. HKEY_LOCAL_MACHINE\ Software\Microsoft\Windows\CurrentVersion\Policies\Explorer \ NoControlPanel REG_DWORD:1

6) Location of registry entry to <u>disable</u> **NoControlPanel**.

    c. HKEY_CURRENT_USER \ Software\Microsoft\Windows\CurrentVersion\Policies\Explorer \ NoControlPanel REG_DWORD:0

    d. HKEY_LOCAL_MACHINE\ Software\Microsoft\Windows\CurrentVersion\Policies\Explorer \ NoControlPanel REG_DWORD:0

7) **NoControlPanel** settings can also be changed by running Group Policy gpedit.msc if required to check or edit manually.

Group Policy

Action View

Tree

Local Computer Policy
- Computer Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates
- User Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates
    - Windows Components
    - Start Menu & Taskbar
    - Desktop
    - Control Panel
    - Network
    - System

Policy	Setting
Add/Remove Programs	
Display	
Printers	
Regional Options	
Disable Control Panel	Not configured
Hide specified control panel applets	Not configured
Show only specified control panel applets	Not configured

Disable Control Panel Properties

Policy | Explain

Disable Control Panel

- Not Configured
- Enabled
- Disabled

Disable Control Panel Properties

Policy | Explain

Explanation for: Disable Control Panel

Disables all Control Panel programs.

This policy prevents Control.exe, the program file for Control Panel, from starting. As a result, users cannot start Control Panel or run any Control Panel items.

This policy also removes Control Panel from the Start menu. (To open Control Panel, click Start, point to Settings, and then click Control Panel.) This policy also removes the Control Panel folder from Windows Explorer.

If users try to select a Control Panel item from the Properties item on a context menu, a message appears explaining that a policy prevents the action.

Also, see the "Disable Display in Control Panel" and "Disable programs on Settings menu" policies.

Password and Reboot Now Function

Password	✱✱✱✱✱✱✱✱	Reboot Now

1) All button functions except for [Check Status], need password.

2) Password is set to present date with YYYYMMDD format, in numeric. Example on 17 April 2011; password will be 20110417.

3) Most registry configuration changes need a reboot to take proper effect; as such [Reboot Now] function is available for convenience.
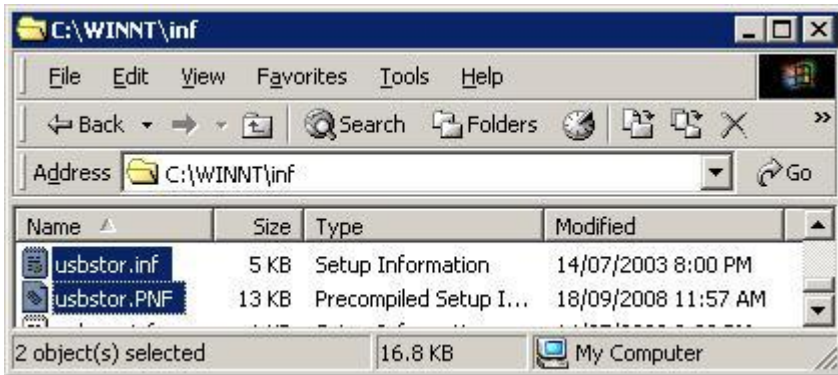

Enable/Disable USB Function

Enable USB	Enable	Disable

1) USB storage access restriction is done by editing on Windows Registry.

2) To Enable USB storage access. Registry entry will be HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR\Start REG_DWORD:3

3) To Disable USB storage access. Registry entry will be HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR\Start REG_DWORD:4

Enable/Disable USB Drivers

USB Drivers   [Enable]   [Disable]

1) USB access for attached storage may still function even with registry entry disabled. Since two USB drivers are still present.

2) When Enable button is click, it will rename usbstor files back to original.

3) When Disable button is click, it will rename usbstor files to C:\winnt\inf**UsbStor.inf.backup** and C:\winnt\inf**UsbStor.pnf.backup**

Enable/Disable/Remove DisableRegistryTools Function

Disabling Registry Edit   [Enable]   [Disable]   [Not Configured]
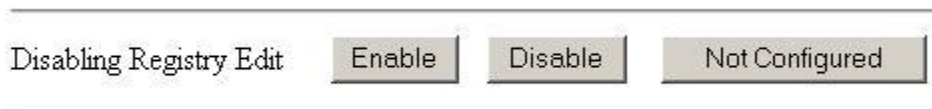
1) This provides one click action to disable registry editor. It uses Group Policy function called **DisableRegistryTools.**

2) [Enable] button will disable Regedit.exe and Regedt32.exe.

Registry Editor

❌ Registry editing has been disabled by your administrator.

[OK]

3) Location of Registry Editor. C:\WINNT\SYSTEM32\REGEDT32.exe & C:\WINNT\REGEDIT.exe
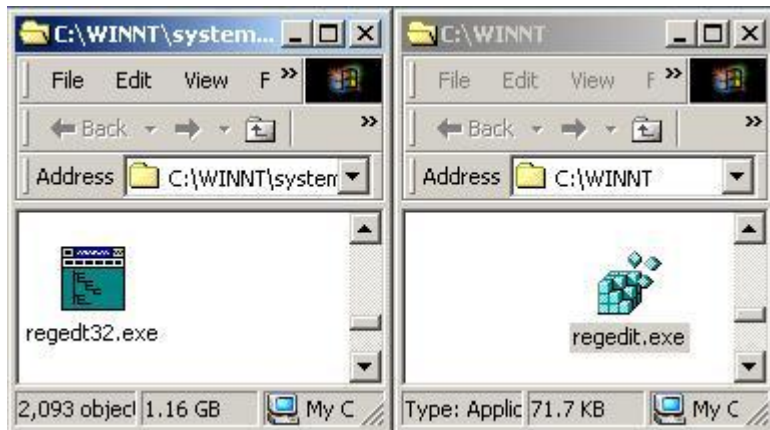
4) [Disable] button will enable Regedit.exe and Regedt32.exe.

5) [Not Configured] button will return all configurations back to original setting. Means that **DisableRegistryTools** will be removed.

6) Location of registry entry to <u>enable</u> **DisableRegistryTools**.

    a. HKEY_CURRENT_USER \Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools REG_DWORD:1

    b. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools REG_DWORD:1

7) Location of registry entry to <u>disable</u> **DisableRegistryTools**.

    a. HKEY_CURRENT_USER \Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools REG_DWORD:0

    b. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools REG_DWORD:0

8) **DisableRegistryTools** can also be changed by running Group Policy gpedit.msc if required to check or edit manually.

Group Policy

Action | View | ← → | 🔼 🔢 | 🖳 🗒 | 🖳

Tree

- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Windows Components
      - Start Menu & Taskbar
      - Desktop
      - Control Panel
      - Network
      - System
        - Logon/Logoff
        - Group Policy

Policy	Setting
Logon/Logoff	
Group Policy	
Don't display welcome screen at logon	Not configured
Century interpretation for Year 2000	Not configured
Code signing for device drivers	Not configured
Custom user interface	Not configured
Disable the command prompt	Not configured
Disable registry editing tools	Not configured
Run only allowed Windows applications	Not configured
Don't run specified Windows applications	Not configured
Disable Autoplay	Not configured
Download missing COM components	Not configured

Disable registry editing tools Properties

Policy | Explain

🖳 Disable registry editing tools

- ⦿ Not Configured
- ○ Enabled
- ○ Disabled

[Previous Policy] [Next Policy]

[OK] [Cancel] [Apply]

Disable registry editing tools Properties

Policy | **Explain**

Explanation for: Disable registry editing tools

Disables the Windows registry editors, Regedt32.exe and Regedit.exe.

If this policy is enabled and the user tries to start a registry editor, a message appears explaining that a policy prevents the action.

To prevent users from using other administrative tools, use the "Run only allowed Windows applications" policy.

[Previous Policy] [Next Policy]

[OK] [Cancel] [Apply]