Secure Endpoint with Group Policy

Group Policy is an important mechanism in the network security process. Here are some very useful settings to block network access.

Group Policy is an important mechanism in the network security process. Here are some very useful settings to block network access.

Set up mobile storage control

Universal Serial Bus (USB) storage devices pose a major threat to the security of workstations. These devices make it easy for crooks to steal information or install unauthorized software on the network.

Although no tools in Group Policy help control access to these USB storage devices, there are some settings that prevent users from using these devices.

One method involves the process of creating a customized administrative template containing a Group Policy Template, providing access to an installation that can be used to turn off the USB port.

Import this template into Group Policy as a **.adm** file.

```
CLASS MACHINE
CATEGORY !! category
CATEGORY !! categoryname
POLICY !! policynameusb
KEYNAME "SYSTEMCurrentControlSetServicesUSBSTOR"
EXPLAIN !! explaintextusb
PART !! labeltextusb DROPDOWNLIST REQUIRED

"Start" VALUENAME
ITEMLIST
NAME !! Disabled VALUE NUMERIC 3 DEFAULT
NAME !! Enabled VALUE NUMERIC 4
END ITEMLIST
END PART
END POLICY
POLICY !! policynamecd
KEYNAME "SYSTEMCurrentControlSetServicesCdrom"
EXPLAIN !! explaintextcd
PART !! labeltextcd DROPDOWNLIST REQUIRED

"Start" VALUENAME
```

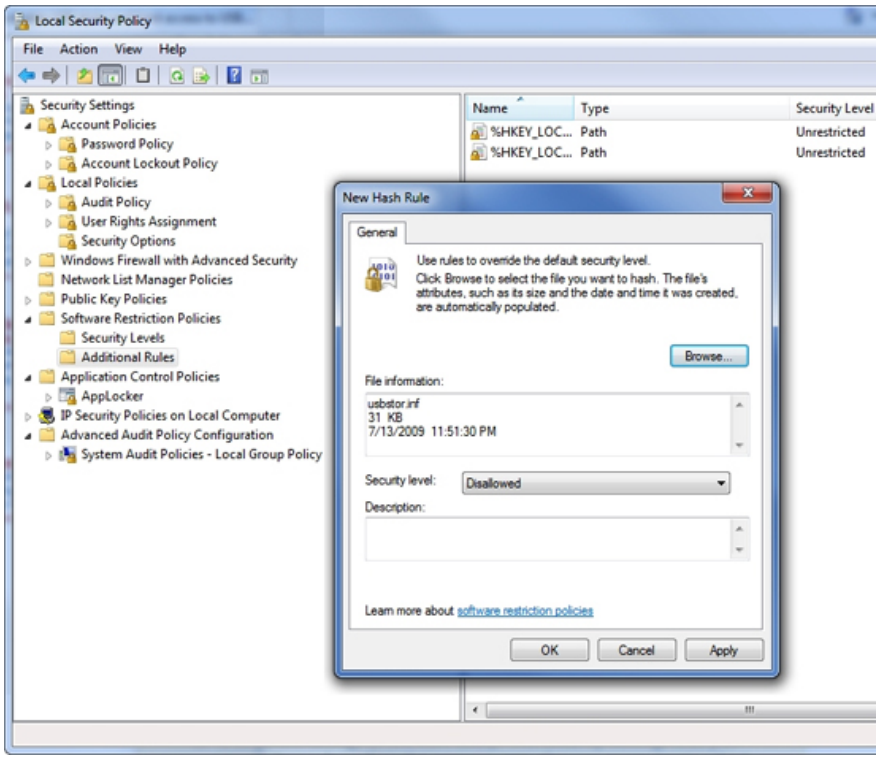
```
ITEMLIST
NAME !! Disabled VALUE NUMERIC 1 DEFAULT
NAME !! Enabled VALUE NUMERIC 4
END ITEMLIST
END PART
END POLICY
POLICY !! policynameflpy
KEYNAME "SYSTEMCurrentControlSetServicesFlpydisk"
EXPLAIN !! explaintextflpy
PART !! labeltextflpy DROPDOWNLIST REQUIRED

"Start" VALUENAME
ITEMLIST
NAME !! Disabled VALUE NUMERIC 3 DEFAULT
NAME !! Enabled VALUE NUMERIC 4
END ITEMLIST
END PART
END POLICY
POLICY !! policynamels120
KEYNAME "SYSTEMCurrentControlSetServicesSfloppy"
EXPLAIN !! explaintextls120
PART !! labeltextls120 DROPDOWNLIST REQUIRED

"Start" VALUENAME
ITEMLIST
NAME !! Disabled VALUE NUMERIC 3 DEFAULT
NAME !! Enabled VALUE NUMERIC 4
END ITEMLIST
END PART
END POLICY
END CATEGORY
END CATEGORY

[strings]
category = "Custom Policy Settings"
categoryname = "Restrict Drives"
policynameusb = "Disable USB"
policynamecd = "Disable CD-ROM"
policynameflpy = "Disable Floppy"
policynamels120 = "Disable High Capacity Floppy"
explaintextusb = "Disables the USB ports by disabling the usbstor.sys driver"
explaintextcd = "Disables the CD-ROM computers Drive by disabling the cdrom.sys driver"
explaintextflpy = "Disables the computers Floppy Drive by disabling the flpydisk.sys driver"
explaintextls120 = "Disables the computers High Capacity Floppy Drive by disabling the
sfloppy.sys driver"
labeltextusb = "Disable USB Ports"
labeltextcd = "Disable CD-ROM Drive"
labeltextflpy = "Disable Floppy Drive"
```

labeltextls120 = "Disable High Capacity Floppy Drive"
Enabled = "Enabled"
Disabled = "Disabled"

(Source Microsoft).

To create the .adm file, download the .msi file containing the .adm files here, then double-click the .msi file to install.
Note: Select the appropriate .msi download for the system.

In addition, USB storage devices may be turned off with software restriction policies. When a user connects a USB drive to the system, Windows will download the diver **% SystemRoot% InfUSBSTOR.INF file** . A Hash Rule can be created to block access to this file as shown in the image below.



Block the USB drive from accessing the USBSTOR.INF file.

Although this is not a policy-based approach, this is a fairly simple method to use NT system file permissions to deny access to the USBSTOR.INF file.

In addition, third-party tools, such as GFI EndPoint Security, can provide more control over mobile storage devices than Windows built-in tools.

Enable local security policy

Local security policies provide many of the same settings as network-level policies, but they are designed to protect the system when it is not authenticated in a domain. Therefore, a computer will not appear weak if someone finds a local login method.

These privacy policies are often ignored because they cannot be centrally managed, so it is difficult to update.

Furthermore, each computer on the network needs a local security policy with important settings enabled. If this policy becomes outdated, network policy settings will override local policy settings when users are online. When a user does not log on to the network, the local security policies protect the system. There is the protection of an outdated policy that is better protected anyway.

Windows Mobile

Typically, Endpoint Security is often focused on desktops or laptops and servers. Mobile devices are often left open because they are used very little and their capabilities are limited. However, now things have changed.

Smart phones that can perform computer functions appear more and more often, leading to widespread mobile phone applications.

The result is an insecure mobile device that can cause network security problems like an unsecured laptop. If a user wants to use a mobile device to hack into the network, there will be an application that serves as an effective assistant. In fact, now we have heard a lot of information about virus spreads on mobile devices.

Group Policy settings can be used to block mobile devices similar to when locking a desktop system. However, not all mobile devices are compatible with Group Policy platform security.

Network-level Group Policy settings can only be applied to domain members. Therefore, only devices that can join the domain will be secured by Group Policy. Currently, only mobile devices that use Windows Mobile 6.1 and 6.5 can join the domain.

Group Policy settings for mobile devices are not included in Windows Server. To get the necessary administrative templates, we need to install System Center Mobile Device Manager. This tool adds about 125 Group Policy settings, accessible via **Group Policy Object Editor** at **Administrative Templates / Windows Mobile Settings** .

In short, just using some of the existing Group Policy settings, we can block Endpoint for added security.