Group Policies

Commands

Update GPOs on host

```
gpupdate /force
```

Check GPOs applied

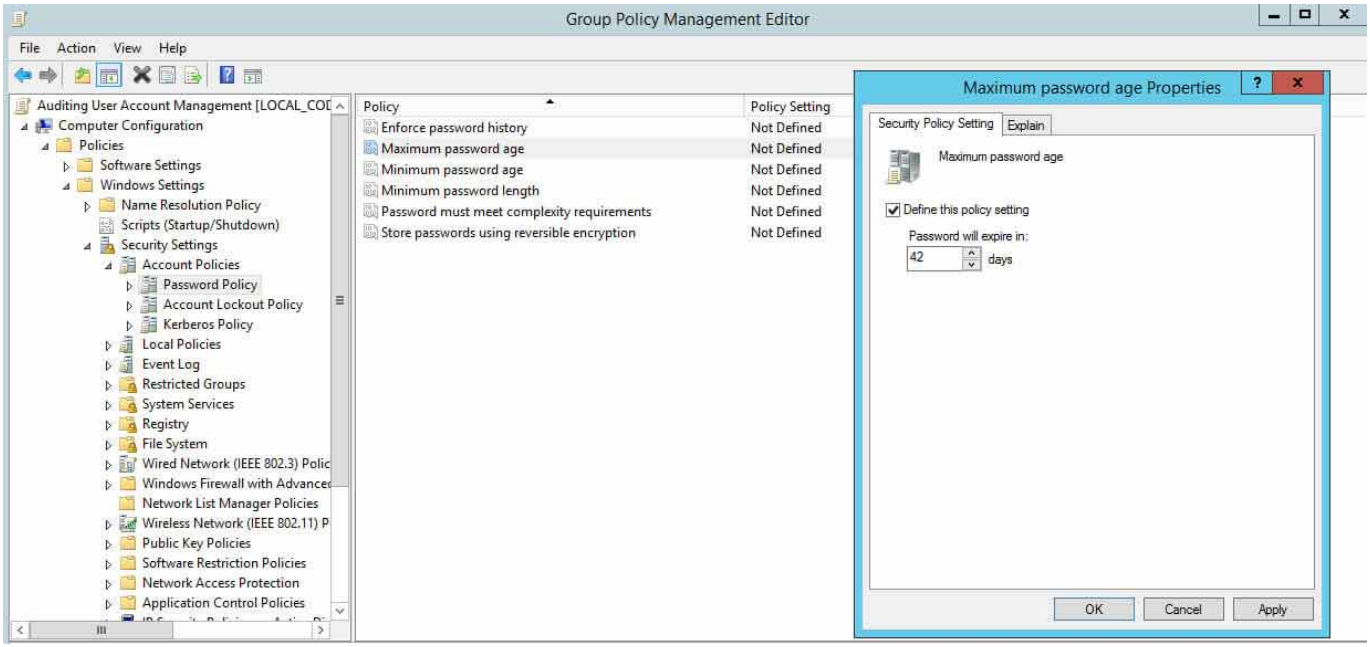
```
gpresult /R
```

1. Set Maximum Password Age to Lower Limits

If you set the password expiration age to a lengthy period of time, users will not have to change it very frequently, which means it’s more likely a password could get stolen. Shorter password expiration periods are always preferred.

Windows’ default maximum password age is set to 42 days. The following screenshot shows the policy setting used for configuring “Maximum Password Age”. Perform the following steps:

1. In Group Policy Management Editor window (opened for a custom GPO), go to “Computer Configuration” “Windows Settings” “Security Settings” “Account Policies” “Password Policy”.
2. In the right pane, double-click “Maximum password age” policy.
3. Select “Define this policy setting” checkbox and specify a value.
4. Click “Apply” and “OK”.

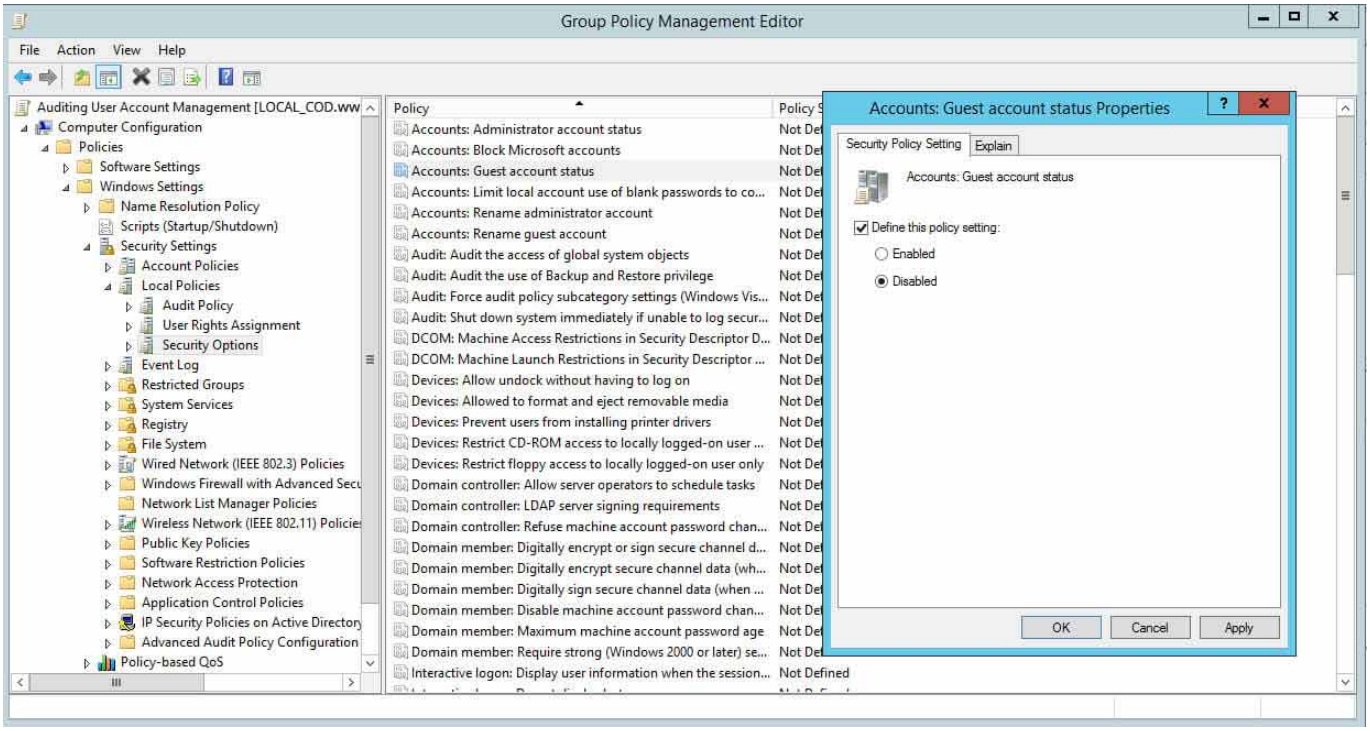


2. Disable Guest Account

Through a Guest Account, users can get access to sensitive data. Such accounts grant access to a Windows computer and do not require a password. Enabling this account means anyone can misuse and abuse access to your systems.

Thankfully, these accounts are disabled by default. It’s best to check that this is the case in your IT environment as, if this account is enabled in your domain, disabling it will prevent people from abusing access:

1. In Group Policy Management Editor (opened for a custom GPO), go to “Computer Configuration” “Windows Settings” “Security Settings” “Local Policies” “Security Options”.
2. In the right pane, double-click “Accounts: Guest Account Status” policy.
3. Select “Define this policy setting” checkbox and click “Disabled”.
4. Click “Apply” and “OK”.

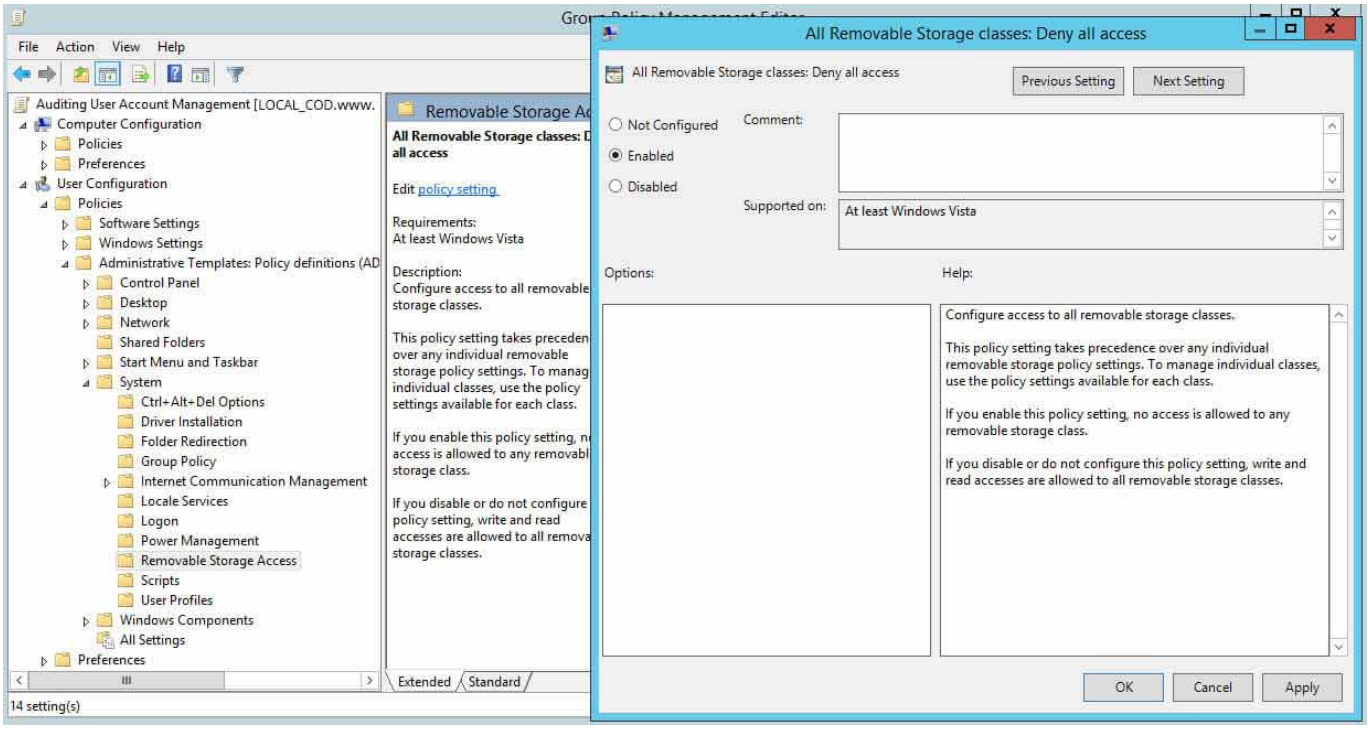


3. Disallow Removable Media Drives, DVDs, CDs, and Floppy Drives

Removable media drives are very prone to infection, and they may also contain a virus or malware. If a user plugs an infected drive to a network computer, it can affect the entire network. Similarly, DVDs, CDs and Floppy Drives are prone to infection.

It is therefore best to disable all these drives entirely. Perform the following steps to do so:

1. In Group Policy Management Editor window (opened for a custom GPO), go to “User Configuration” “Policies” “Administrative Templates” “System” “Removable Storage Access”.
2. In the right pane, double-click “All removable storage classes: Deny all accesses” policy
3. Click “Enabled” to enable the policy.
4. Click “Apply” and “OK”.

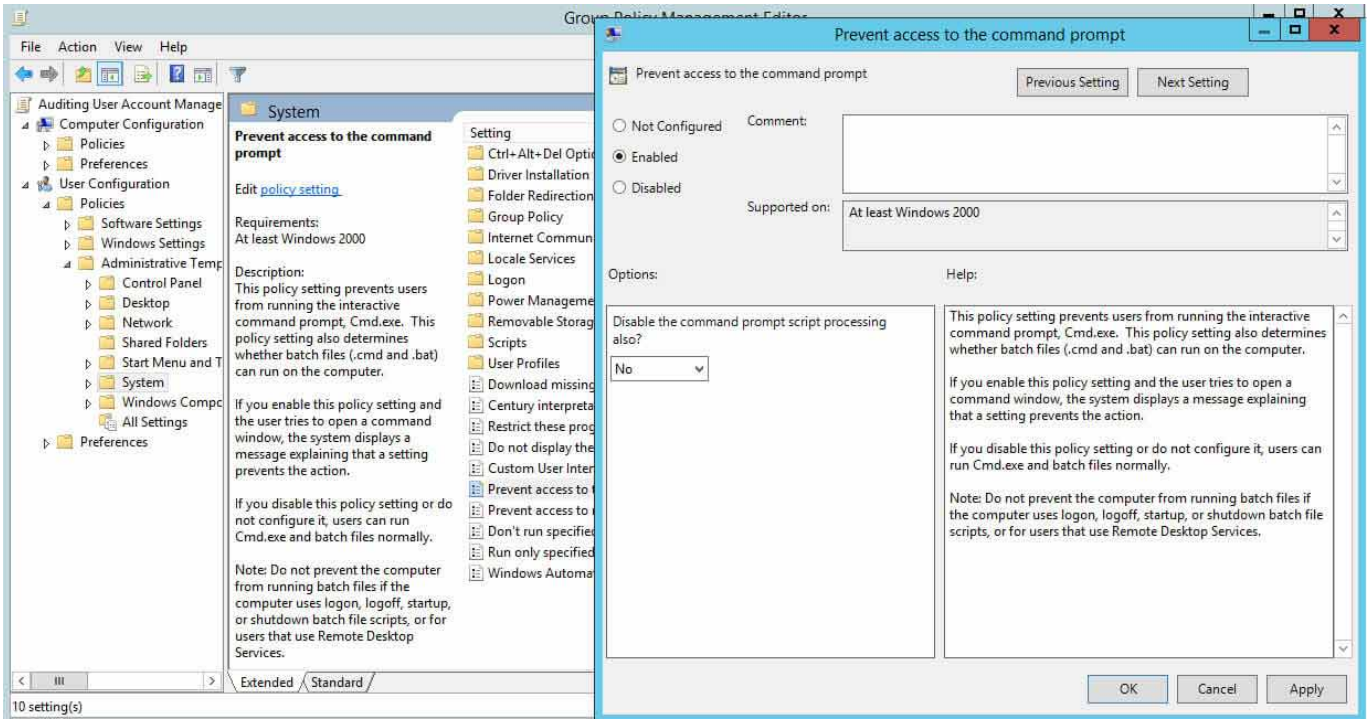


4. Control Access to Command Prompt

Command Prompts can be used to run commands that give high-level access to users and evade other restrictions on the system. So, to ensure system resources' security, it's wise to disable Command Prompt.

After you have disabled Command Prompt and someone tries to open a command window, the system will display a message stating that some settings are preventing this action. Perform the following steps:

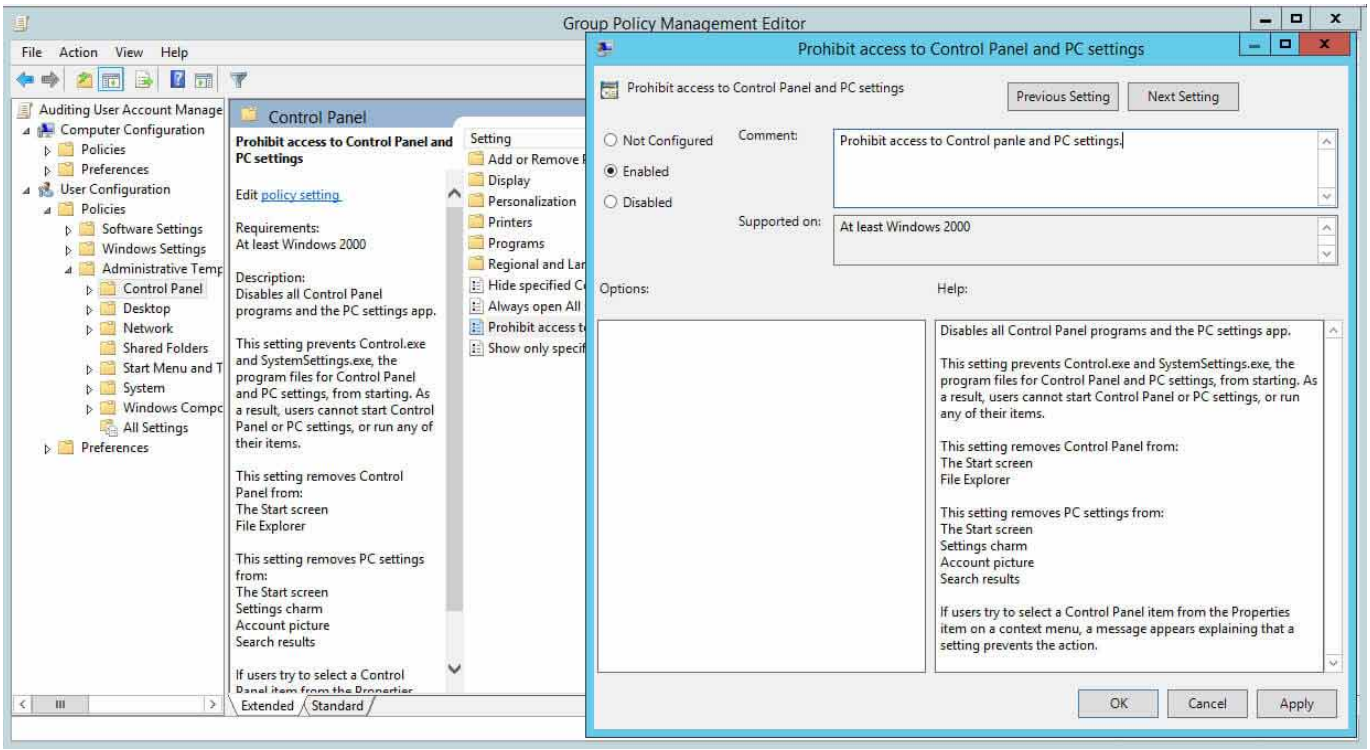
1. In the window of Group Policy Management Editor (opened for a custom GPO), go to "User Configuration" "Windows Settings" "Policies" "Administrative Templates" "System".
2. In the right pane, double-click "Prevent access to the command prompt" policy.
3. Click "Enabled" to apply the policy.
4. Click "Apply" and "OK".



5. Moderating Access to Control Panel

Setting limits on a computers' Control Panel creates a safer business environment. Through Control Panel, you can control all aspects of your computer. So, by moderating who has access to the computer, you can keep data and other resources safe. Perform the following steps:

1. In Group Policy Management Editor (opened for a user-created GPO), navigate to "User Configuration" "Administrative Templates" "Control Panel".
2. In the right pane, double-click "Prohibit access to Control Panel and PC settings" policy in to open its properties.
3. Select "Enabled" from the three options.
4. Click "Apply" and "OK".


Group Policy Management Editor
File Action View Help
Auditing User Account Manage
Computer Configuration
Policies
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Administrative Temp
Control Panel
Desktop
Network
Shared Folders
Start Menu and T
System
Windows Compc
All Settings
Preferences
Control Panel
Prohibit access to Control Panel and PC settings
Edit policy setting
Requirements:
At least Windows 2000
Description:
Disables all Control Panel programs and the PC settings app.
This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.
This setting removes Control Panel from:
The Start screen
File Explorer
This setting removes PC settings from:
The Start screen
Settings charm
Account picture
Search results
If users try to select a Control
Extended
Standard
Setting
Add or Remove
Display
Personalization
Printers
Programs
Regional and Lar
Hide specified C
Always open All
Prohibit access t
Show only specif
Prohibit access to Control Panel and PC settings
Prohibit access to Control Panel and PC settings
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Prohibit access to Control panle and PC settings.
Supported on:
At least Windows 2000
Options:
Help:
Disables all Control Panel programs and the PC settings app.
This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.
This setting removes Control Panel from:
The Start screen
File Explorer
This setting removes PC settings from:
The Start screen
Settings charm
Account picture
Search results
If users try to select a Control Panel item from the Properties item on a context menu, a message appears explaining that a setting prevents the action.
OK
Cancel
Apply