**1. Restricting 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. Open Server Manager, click on tools tab, then Open Group Policy Management.
2. Right click on the Engineering OU, click create a GPO in this domain, and link it here. Notes that the GPO will be applied only to the Engineering group
3. In the name, type Restrict Control Panel and click Ok.
4. Right click the newly created GPO, and click edit.
5. In Group Policy Management Editor (opened for a user-created GPO), navigate to “User Configuration” “Administrative Templates” “Control Panel”.
6. In the right pane, double-click “Prohibit access to Control Panel and PC settings” policy in to open its properties.
7. Select “Enabled” from the three options.
8. Click “Apply” and “OK”.

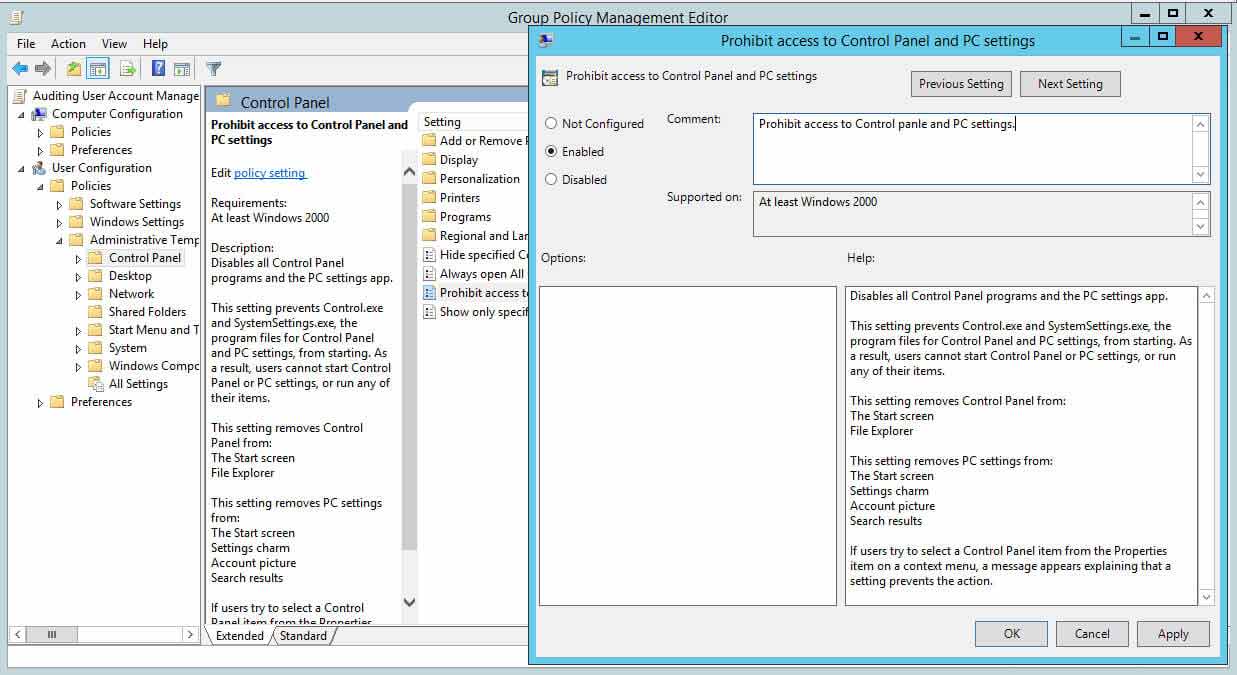
[](https://www.lepide.com/blog/wp-content/uploads/2017/12/Fig-1-Moderating-control-panel-access.jpg)

Figure 1: Configuring Control panel settings through GPO

9. Login to Windows 10 client as an Administrator, open cmd, then type **gpupdate /Force** and hit enter.

10. Sign out and sign in as user from the Engineering department, then verify that the users from the Engineering department can’t open Control Panel.

11. try another user from IT, IT users should have access to Control Panel.

**3. 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:

Step 1 to 4 are the same, except the name of GPO.

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”.

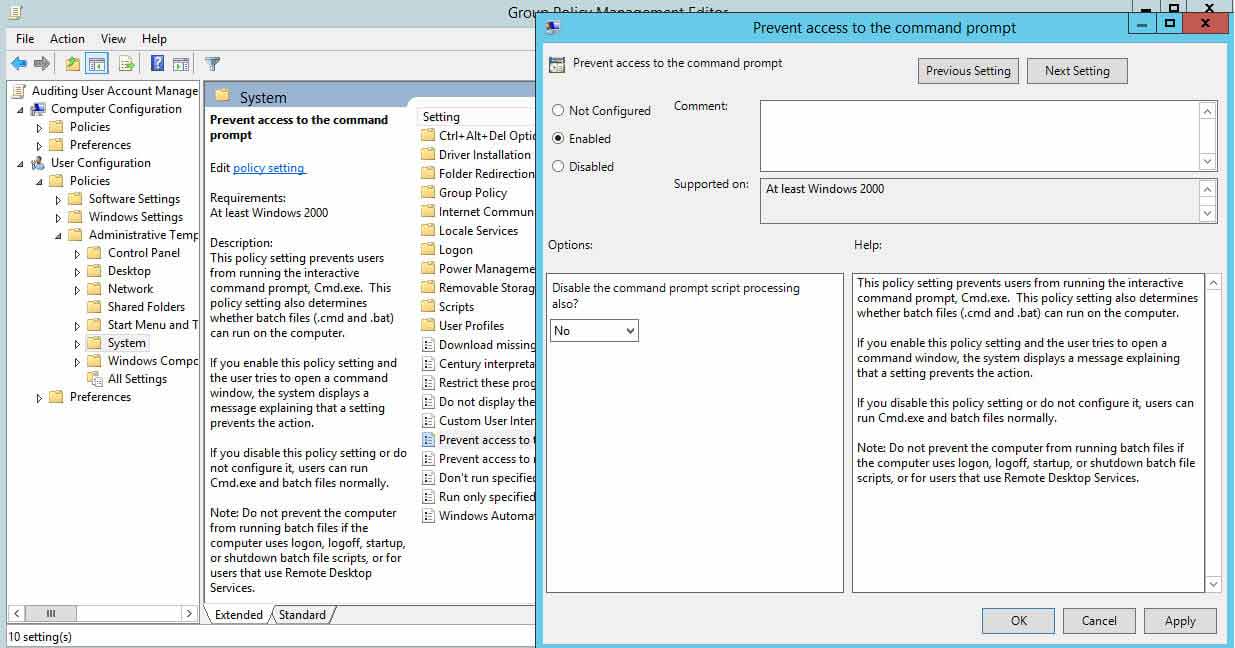
[](https://www.lepide.com/blog/wp-content/uploads/2017/12/Fig-3-Control-access-to-Command-Prompt-1.jpg)

Figure 3: Prevent access to the command prompt window

1. Repeat step 9 to 11 and make sure the Engineering users can’t access Command Prompt.

**5. 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:

Step 1 to 4 are the same, except the name of GPO.

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”.

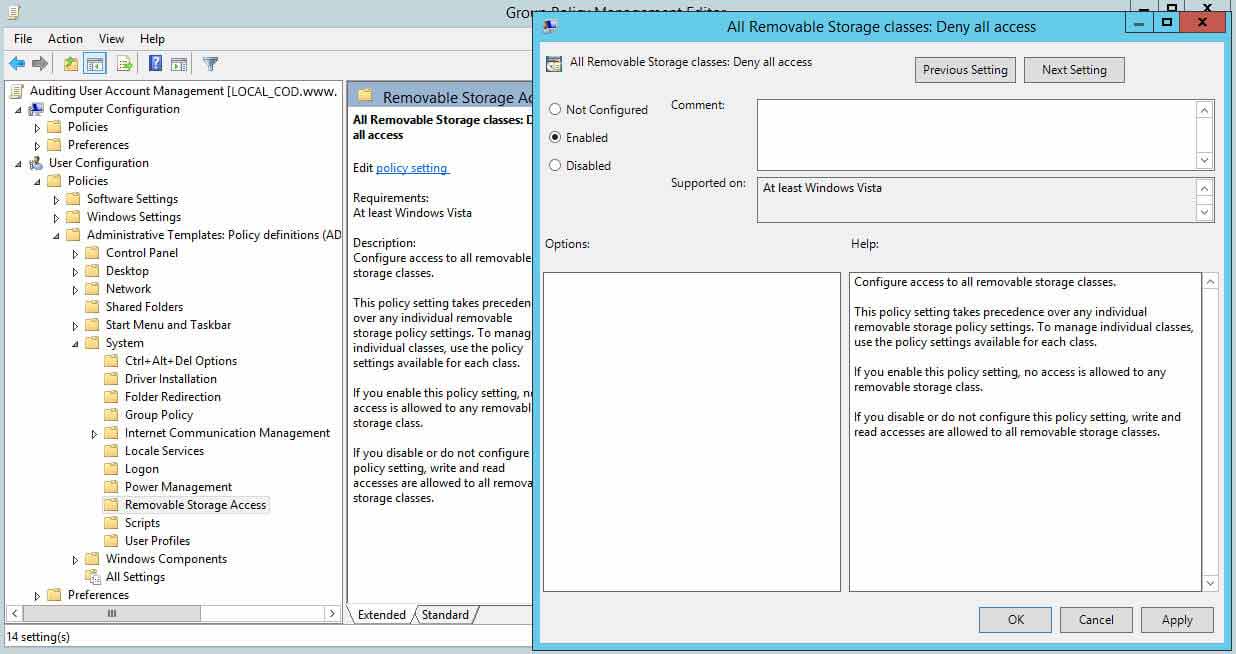
[](https://www.lepide.com/blog/wp-content/uploads/2017/12/Fig-5-Disallow-removable-media-drives.jpg)

Figure 5: Deny access to all removable storage classes

9. Repeat step 9 and 10 and make sure the Engineering users can’t access removable media.

**6. Restrict Software Installations**

When you give users the freedom to install software, they may install unwanted apps that compromise your system. System admins will usually have to routinely do maintenance and cleaning of such systems. To be on the safe side, it’s advisable to prevent software installations through Group Policy:

Step 1 to 4 are the same, except the name of GPO.

1. In Group Policy Management Editor (opened for a custom GPO), go to “Computer Configuration” “Administrative Templates” “Windows Component” “Windows Installer”.
2. In the right pane, double-click “Prohibit User Install” policy.
3. Click “Enabled” to enable the policy
4. Click “Apply” and “OK”.

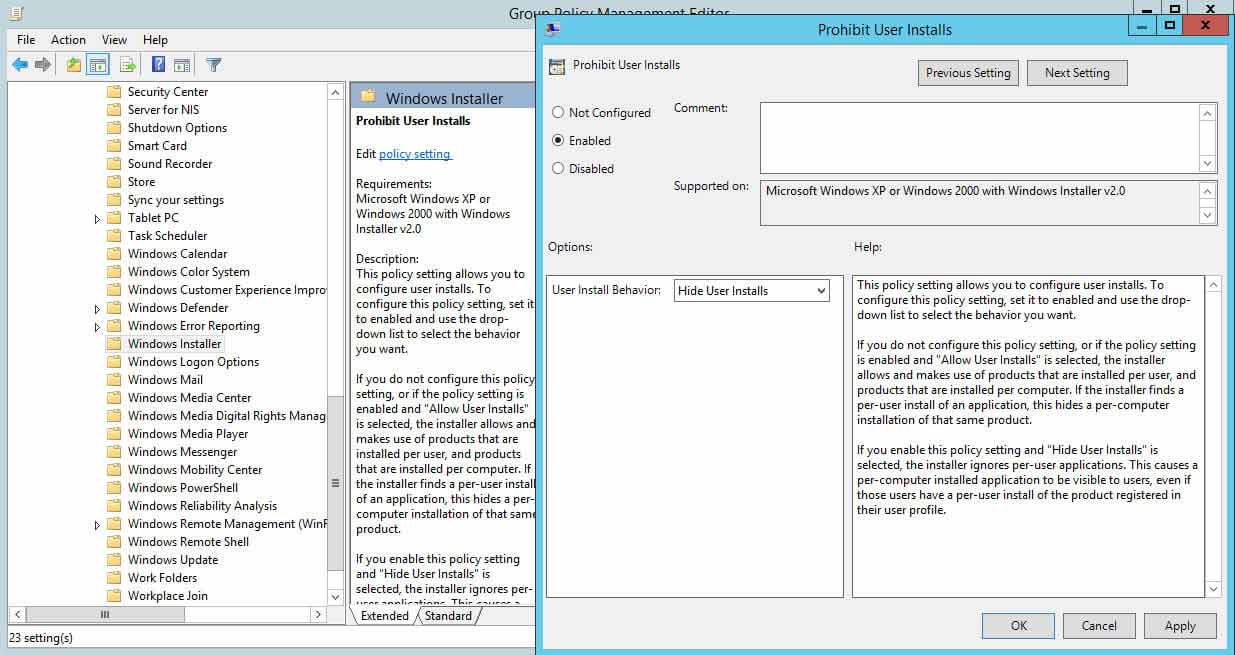
[](https://www.lepide.com/blog/wp-content/uploads/2017/12/Fig-6-Restrict-software-installations.jpg)

Figure 6: Restricting software installations

1. Repeat step 9, 10 and make sure the Engineering users can’t install software on the Windows 10 client.

**7. 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”.

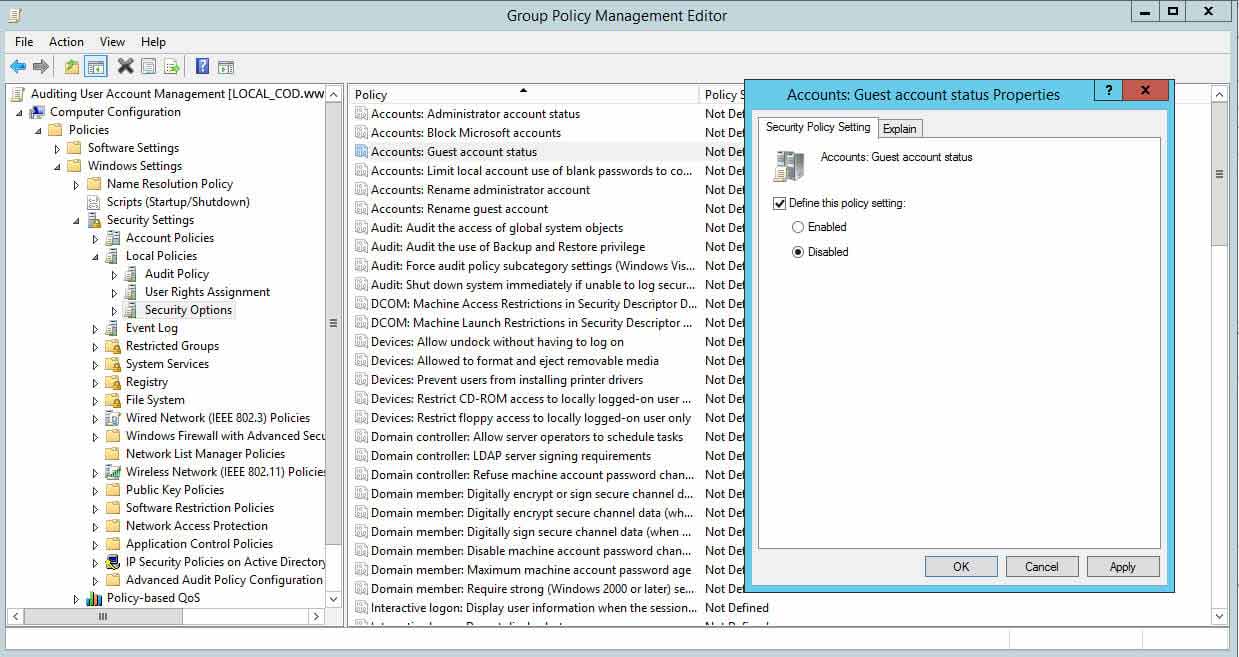
[](https://www.lepide.com/blog/wp-content/uploads/2017/12/Fig-7-Disbale-guest-account.jpg)

Figure 7: Disabling guest account

**8. Set Minimum Password Length to Higher Limits**

Set the minimum password length to higher limits. For example, for elevated accounts, passwords should be set to at least 15 characters, and for regular accounts at least 12 characters. Setting a lower value for minimum password length creates unnecessary risk. The default setting is “zero” characters, so you will have to specify a number:

Step 1 to 4 are the same, except the name of GPO.

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 “Minimum password length” policy, select “Define this policy setting” checkbox.
3. Specify a value for the password length.
4. Click “Apply” and “OK”.

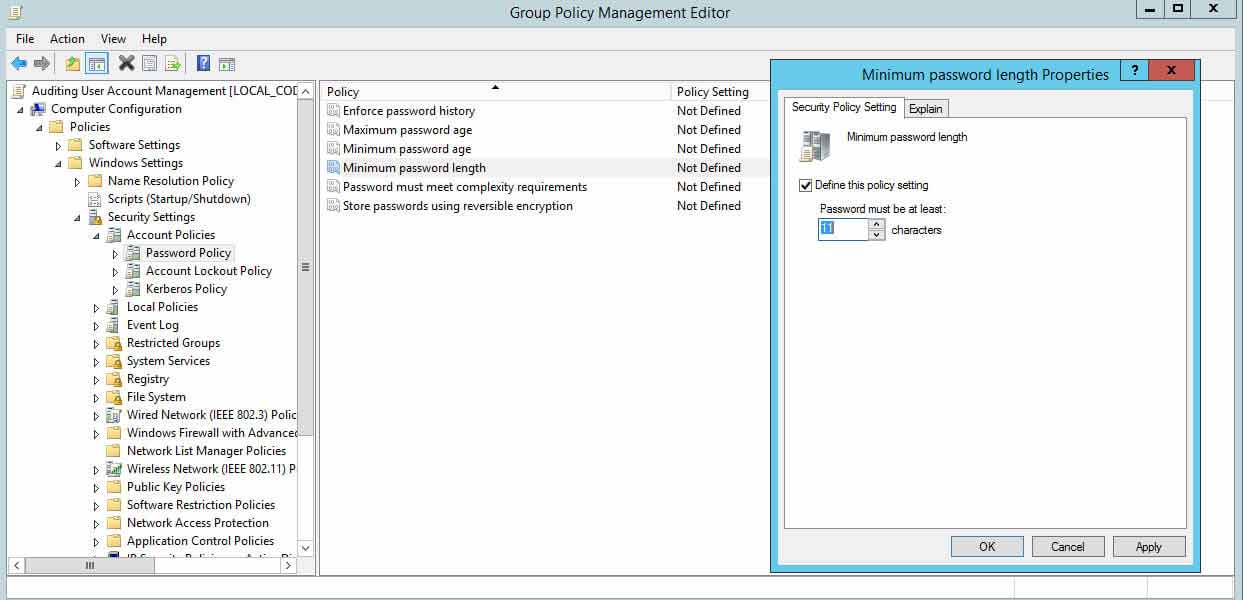
[](https://www.lepide.com/blog/wp-content/uploads/2017/12/Fig-8-Minimum-password-length.jpg)

Figure 8: Configuring minimum password age policy setting

Repeat step 9, 10 and create a new user called user1. In the password try 2019Pass as password.

**9. 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”.

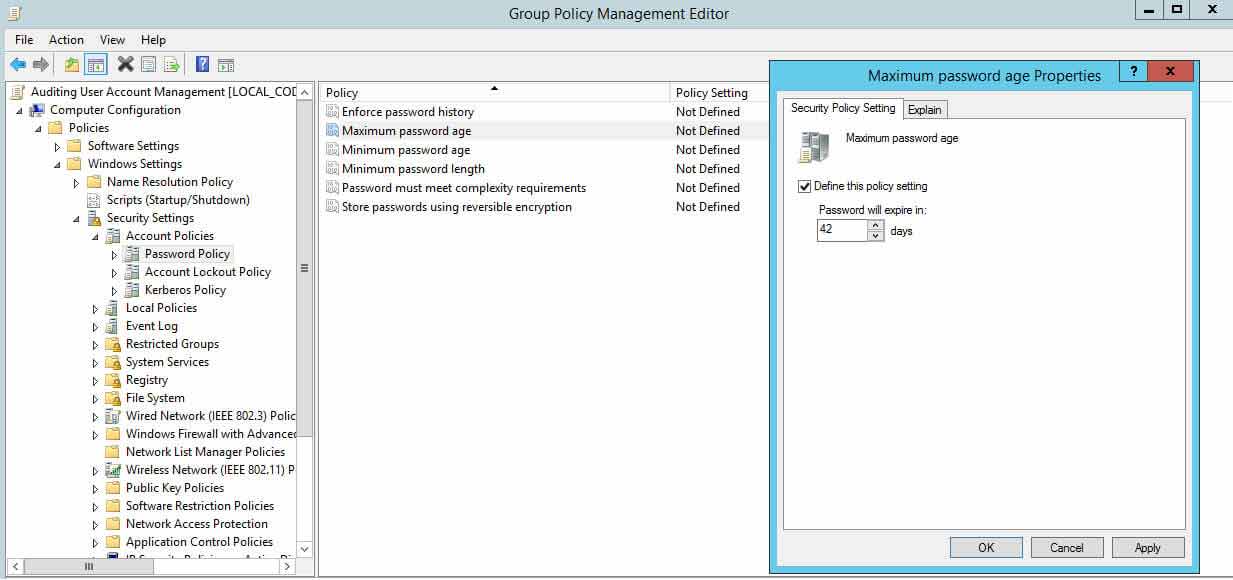
[](https://www.lepide.com/blog/wp-content/uploads/2017/12/Fig-9-Maximum-password-age.jpg)

Figure 9: Configuring maximum password age policy setting