

# **Windows Server 2022**






## **Standard**

**Operating System**

**Installation Guide**

Notices
<ul style="list-style-type: none"> <li>● The reproduction, transmission or use of this document or its contents is not permitted without express written authority.</li> <li>● Information and specifications in this document are subject to change without notice.</li> <li>● While information in this document is well edited and checked, mistake or omission may exist. Please don't hesitate to contact SUPCON if you have any question about this document.</li> <li>● Please contact SUPCON via email "<a href="mailto:SMS@supcon.com">SMS@supcon.com</a>" if you have any question.</li> </ul>

Trademarks
<p>Trademarks or marks SUPCON, SPlant, Webfield, ESP-iSYS, MultiF, InScan, SupField are all registered, registering or using by Zhejiang SUPCON Technology Co., Ltd., which owns the properties of all trademarks or marks above. Without the written authority from Zhejiang SUPCON Technology Co., Ltd, no individual or company shall use any trademarks or marks above. We reserve the right to take legal action for any individual or company using trademarks or marks above illegally.</p>

Symbol Definition	
	<b>WARNING:</b> Indicates information that a potentially hazardous situation which, if not avoided, could result in serious injury or death.
	<b>RISK OF ELECTRICAL SHOCK:</b> Indicates information that Potential shock hazard where HAZARDOUS LIVE voltages greater than 30V RMS, 42.4V peak, or 60V DC may be accessible.
	<b>ESD HAZARD:</b> Indicates information that Danger of an electro-static discharge to which equipment may be sensitive. Observe precautions for handling electrostatic sensitive devices
	<b>ATTENTION:</b> Identifies information that requires special consideration.
	<b>TIP:</b> Identifies advice or hints for the user.

# Table of Contents

<b>Windows Server 2022 Standard .....</b>	<b>1</b>
<b>Section 1 Flow for Installation of Windows 2022 .....</b>	<b>1</b>
<b>Section 2 Installation of Windows 2022.....</b>	<b>2</b>
<b>Section 3 Create Logic Partitions for Hard Disk .....</b>	<b>4</b>
<b>Section 4 Install Drivers .....</b>	<b>5</b>
<b>Section 5 System Optimization and Properties Settings .....</b>	<b>7</b>
5.1 User Accounts Settings .....	7
5.1.1 Change Password Policy .....	7
5.1.2 Administrator Account Setting.....	8
5.1.3 Set Password for Administrator .....	10
5.1.4 Set Automatic Logon .....	11
5.2 Display Properties Settings .....	12
5.2.1 Set Windows Themes .....	12
5.2.2 Change Desktop Icons .....	13
5.2.3 Set Screen Saver .....	14
5.2.4 Set Screen Resolution and Refresh Rate.....	15
5.2.5 Turn off Clear Type Text Tuner .....	16
5.2.6 Turn off Aero Shake Window Minimizing Mouse Gesture.....	17
5.3 Turn off Sticky Keys and Toggle Keys.....	19
5.4 Turn off Hot Keys of Rotating Screen .....	21
5.5 Taskbar Properties.....	22
5.6 Time Settings.....	23
5.7 System and Security Settings.....	24
5.7.1 Set Power Options .....	24
5.7.2 Turn off Windows defender firewall .....	26
5.7.3 User Accounts Control Settings.....	28
5.7.4 Performance options settings.....	31
5.7.5 Turn off auto-update .....	37
5.7.6 Turn off Microsoft Defender Antivirus.....	40
5.7.7 System Anti Virus Settings .....	43
5.8 Background Service Settings .....	46

5.9 Turn off Flow Control of Network Adapter .....	48
5.10 Network Properties Settings .....	50
5.10.1 Network Properties Configuration.....	50
5.10.2 Advanced Sharing Settings .....	52
5.10.3 Network Power Management Configuration .....	54
5.10.4 Disable IPv6 .....	56
5.11 Startup and Recovery Settings .....	57
<b>Section 6 Checklist.....</b>	<b>60</b>
<b>Section 7 Revision.....</b>	<b>63</b>

# Windows Server 2022 Standard



---

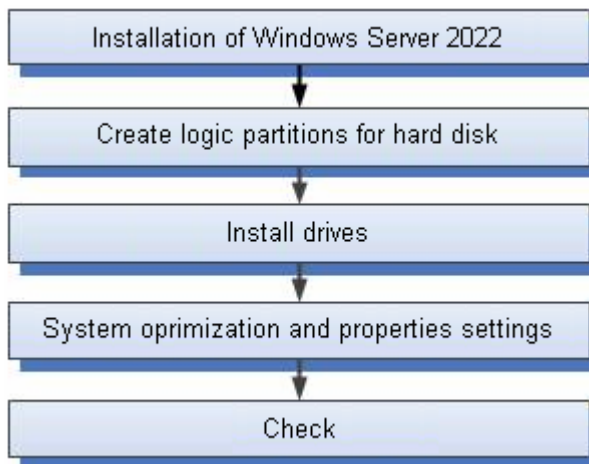
**Attentions:**

- This guideline is only applicable to closed network node operating system.
  - Before installation, please read relevant user manual and observe safety notices.
  - Please refer to the computer user manual for specific instructions or log on the website of the computer supplier to obtain relevant information.
- 

## Section 1 Flow for Installation of Windows 2022

---

The operation system is named Windows Server 2022 in this guide; the flow for installation is shown in Figure 1-1.



**Figure 1-1 Flow for installation of Windows**

## Section 2 Installation of Windows 2022

---

Applicable operating system of this guide is Windows Server 2022 Standard-English-64Bit OS, the installation steps are as follows.

1. Boot up the PC with the installation disk of Windows Server 2022.

Boot up the PC and set disc as boot disc. Insert the installation disk of Windows Server 2022 into CD-ROM, and then enter into the Windows Server 2022 setting interface.

2. Choose the installation language.
  - Language to install: English(United States)
  - Time and currency format: English(United States)
  - Keyboard or input method: US

3. Activation of operation system.

If you have product key, input the key in pop-up interface to finish the activation of operation system.

4. Choose installation operation system.

Windows Server 2022 Standard (Desktop Experience).

5. Accept the license terms.
6. Choose installation mode.

Select "Custom: Install Microsoft Server Operating System Only (advanced)".

7. Create system disk partition.

- 1) Click delete on disk partition interface to delete all the original system disk partition on disk partition interface.
  - 2) Click Driver options (advanced), select the disk partition then click New on disk partition interface to create a new system disk partition of 100G, the conditions of other system disk partition are shown in Table 3-1.
  - 3) Then it starts to install Windows Server 2022 up to end.
8. Set password of system administrator.

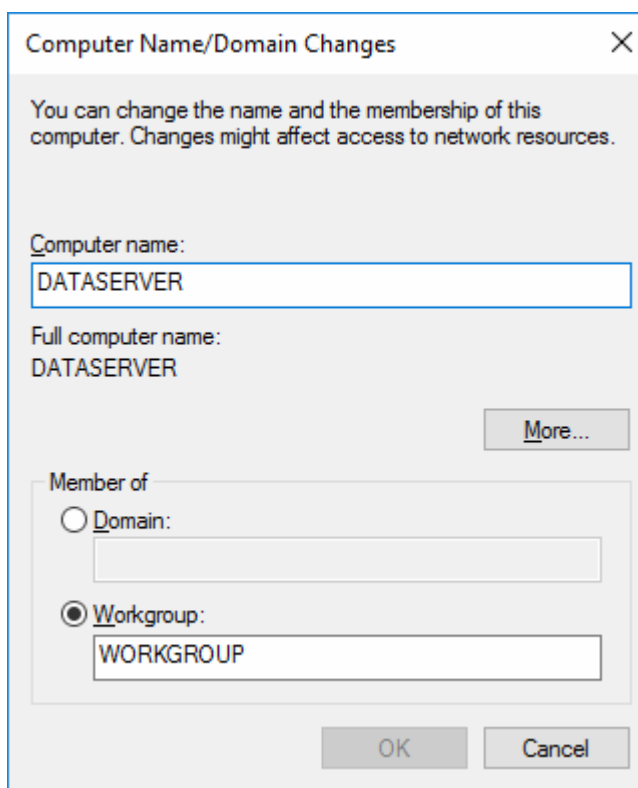
After installing Windows Server 2022 operation system, the system will pop up the dialog box of custom settings, in which you can set password of Administrator account and get the tip "Your password has been changed successfully". Then, you can enter Windows

Server 2022 operation system. The password should contain a mix of uppercase and lowercase letters, along with at least one number, otherwise the operation of changing password will be failed.

9. Change the name of computer.

After opening operation system, please select [Start\ Control Panel\ System and Security\ System] and click “Rename this PC (advanced)” in the “Related setting” interface to open the interface of system property.

Click “Change” in the tab “Computer Name” to pop up the interface shown as Figure 2-1 and input “DATASERVER” as computer name. The click “OK” and restart the computer according to the tip information.



**Figure 2-1 Computer name**

## Section 3 Create Logic Partitions for Hard Disk

---

Select [Start \ Windows Administrative Tools \ Computer Management] and Computer Management interface will pop up, in which click Disk Management below Storage, and then the condition of system disk partition will be shown in the right column.

Firstly, change CD-ROM to Disk G. Secondly, then select right-click menu “New Simple Volume...” at the unallocated disk to divide the disk into disk D, disk E and disk F. Partition standards are as follows.

**Table 3-1 List of disk partitions**

Hard disk space	Disk icon	Local Disk C (system disk)	Local Disk D (data disk)	Local Disk E (backup disk)	Local Disk F (own disk)	Local Disk G
≥160G	Format	NTFS	NTFS	NTFS	NTFS	CD-ROM
	Capacity	102400MB	The rest	20480MB	20480MB	

Application guideline of each partition is as follows:

- Operating system and Supervision software are to be installed on Disk C.
- Disk D is to be used to store supervision running data.
- Disk E is to be used to backup setup programs, engineering configurations and drivers .etc.
- Disk F is to be used to store process database file (history trend, alarm record, report etc.) which is created by supervision software or other working files.



---

### Tips:

- If you want to re-install the operation system, you just need to format Disk C directly and it is no necessary for logic partitions for hard disk over again.
  - If the overall hard disk has rich spare capacity, the capacity of C disk could be expanded at discretion.
-

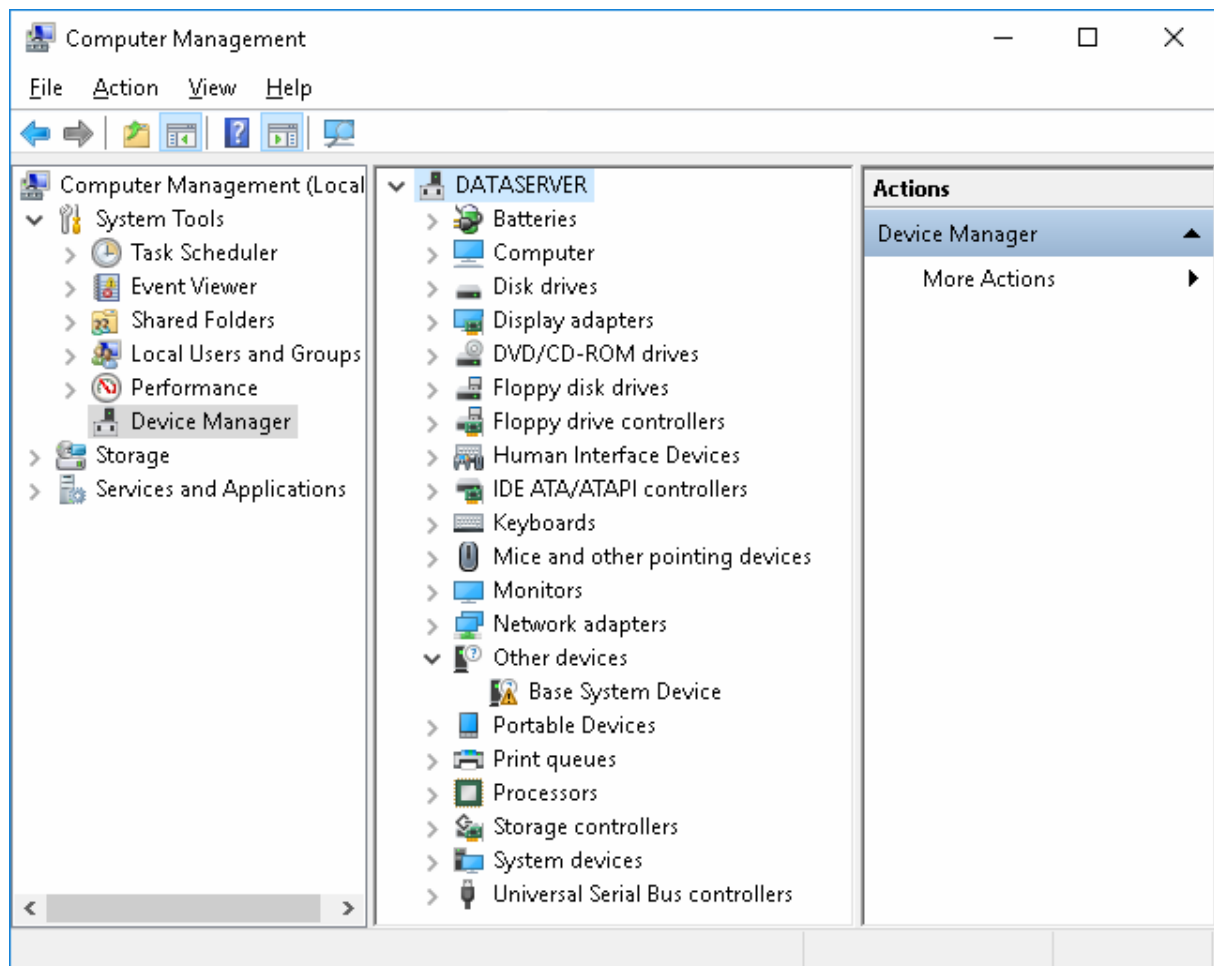


## Section 4 Install Drivers

### Installation

In the light of host configuration, run the main board driver disc and the integrated components driver disc provided by the host manufacturer, and install every component following hints of installation wizard. Restart computer after finishing installation.

However, if you don't know which drivers should be installed by referencing the wizard, please select [Start\ Windows Administrative Tools\ Computer Management] and open the Device Manager in Computer Management interface, it is shown as Figure 4-1, in which those components without finding drive (marked with a yellow interrogation mark or exclamation mark) need to be installed.



**Figure 4-1 Device Manager Interface**

### Backup

Backup the corresponding drivers to disk E.

### **Check**

There should be no item marked with yellow interrogation mark or exclamation mark in interface Device manager after finishing the installation successfully.

## Section 5 System Optimization and Properties Settings



### Attention:

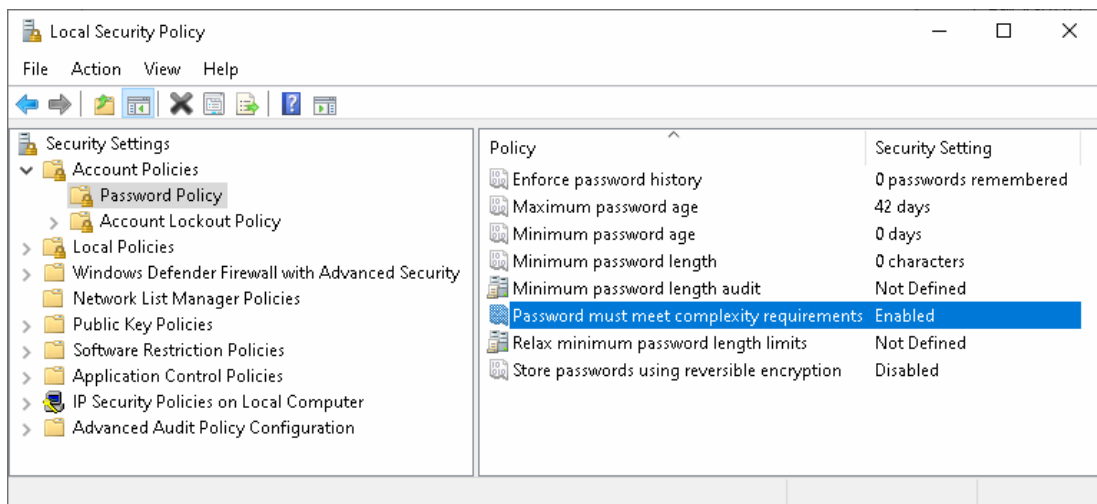
The properties which are not mentioned remain default.

This chapter introduces how to set user accounts, display properties, taskbar and start menu, time, language, system properties, firewall, services, network properties and so on.

## 5.1 User Accounts Settings

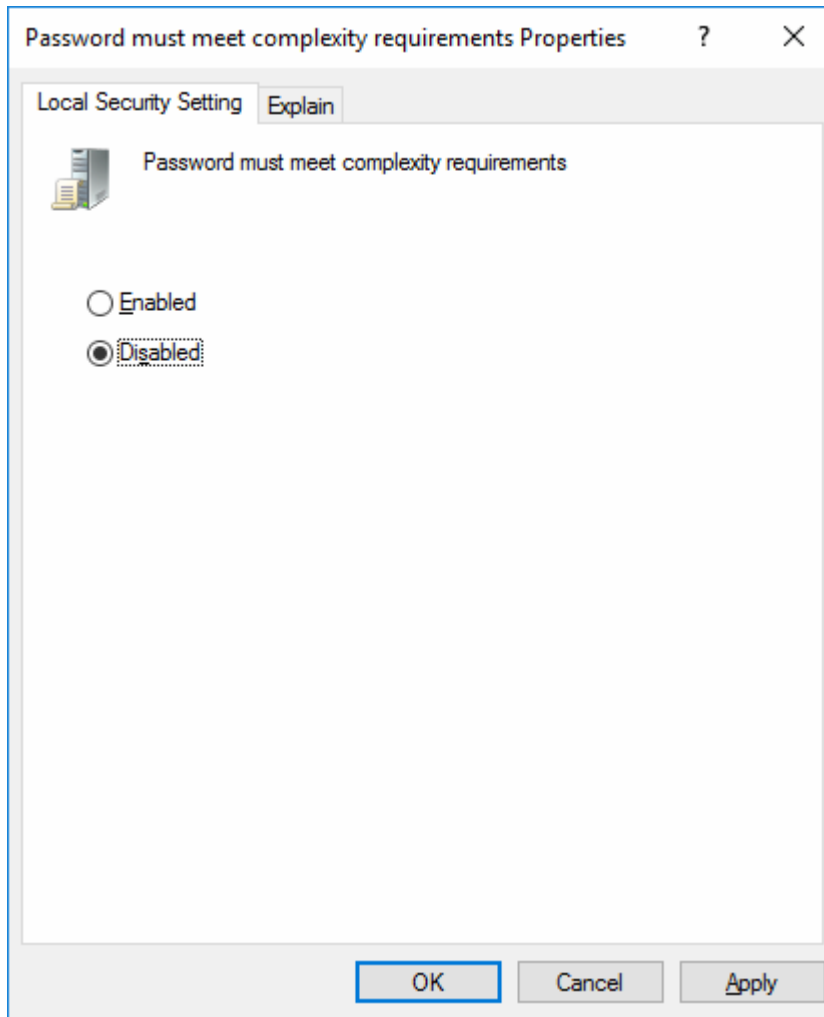
### 5.1.1 Change Password Policy

1. Select [Start\ Windows Administrative Tools\ Local Security Policy] to open the interface of “Local Security Policy”, as shown in Figure 5-1.



**Figure 5-1 Local security policy interface**

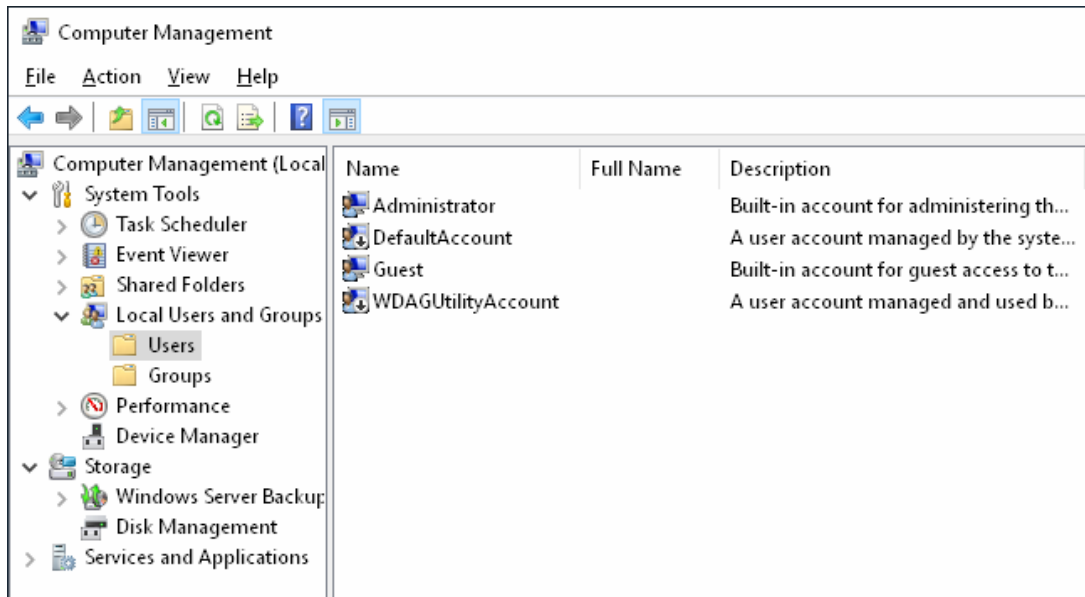
2. Click “Password Policy” below “Account Policies” and double-click “Password must meet complexity requirements” on the right side of the interface to pop up the interface as shown in Figure 5-2. Select “Disabled” in the tab “Local Security Setting”, then click “Apply” and “OK”.



*Figure 5-2 Password must meet complexity requirements interface*

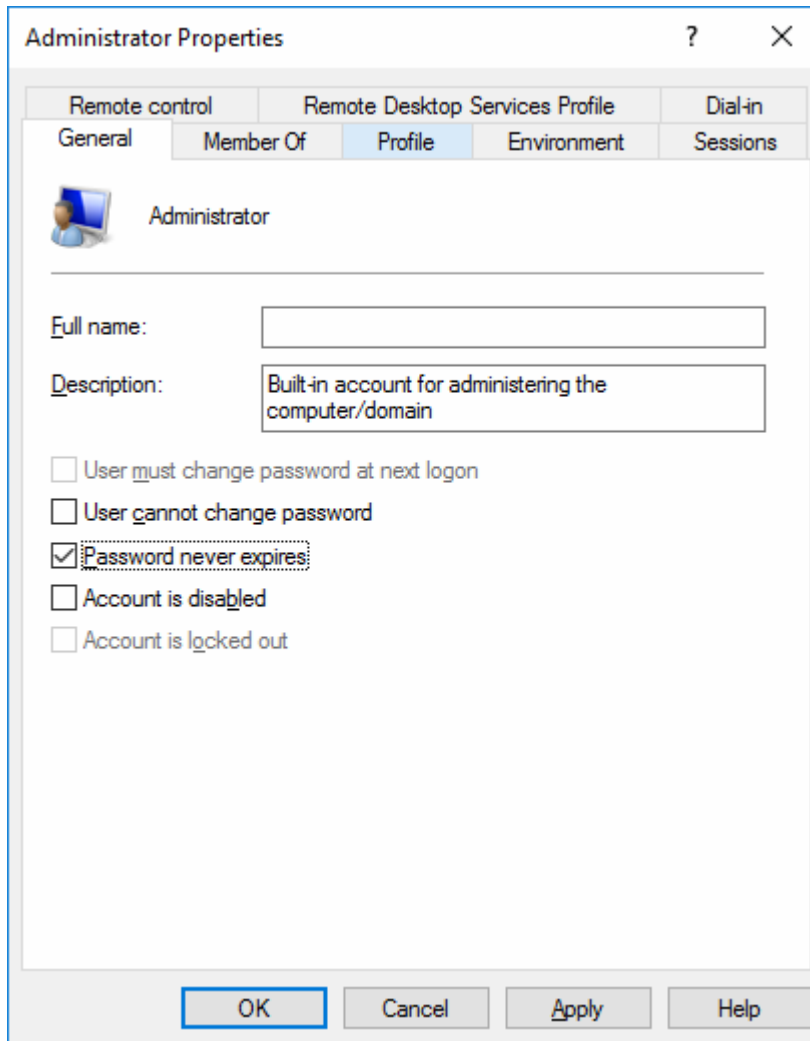
### 5.1.2 Administrator Account Setting

1. Select [Start\ Windows Administrative Tools\ Computer Management] to open the interface of computer management. Select "Users" below "Local Users and Groups", the user interface shown as Figure 5-3.



**Figure 5-3 User interface**

2. Double-click "Administrator", pop up "Administrator Properties" interface. Select "Password never expires" in "General" option page, and click "Apply" and "OK".



**Figure 5-4 Deselect "Account is disabled"**



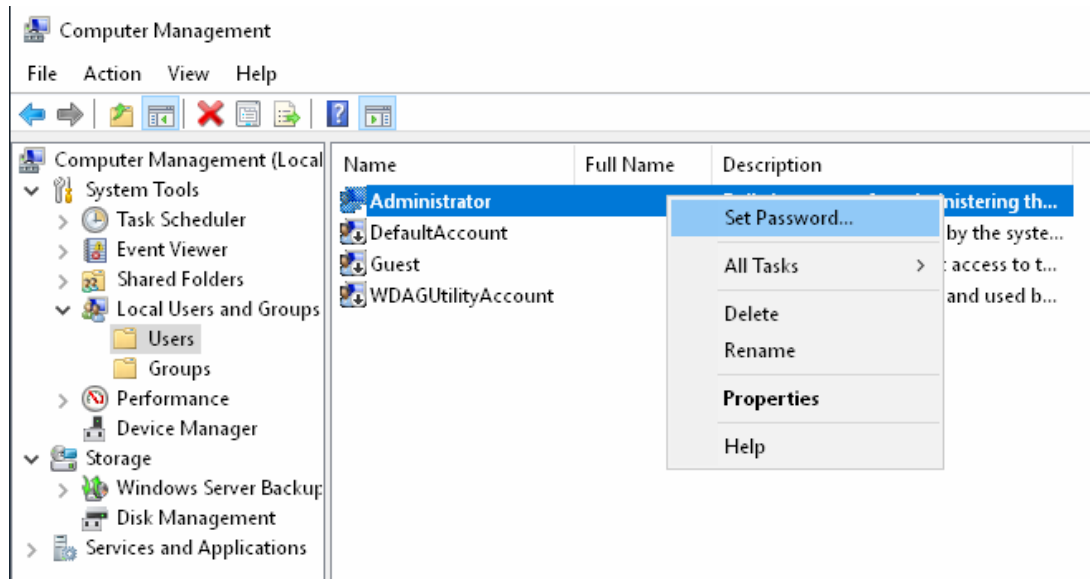
**Attentions:**

- After deleting the user named Temp you must restart the computer (login as Administrator) and then set all the properties as follows.
- As for the built-in users, which can't be deleted such as DefaultAccount, WDAGUtilityAccount and Guest, please check "The user has been forbidden" in the properties interface and click "OK".

---

### 5.1.3 Set Password for Administrator

1. Right-click the account "Administrator" in User interface of Computer Management and select "Set Password" in right-click menu, as shown in Figure 5-5.

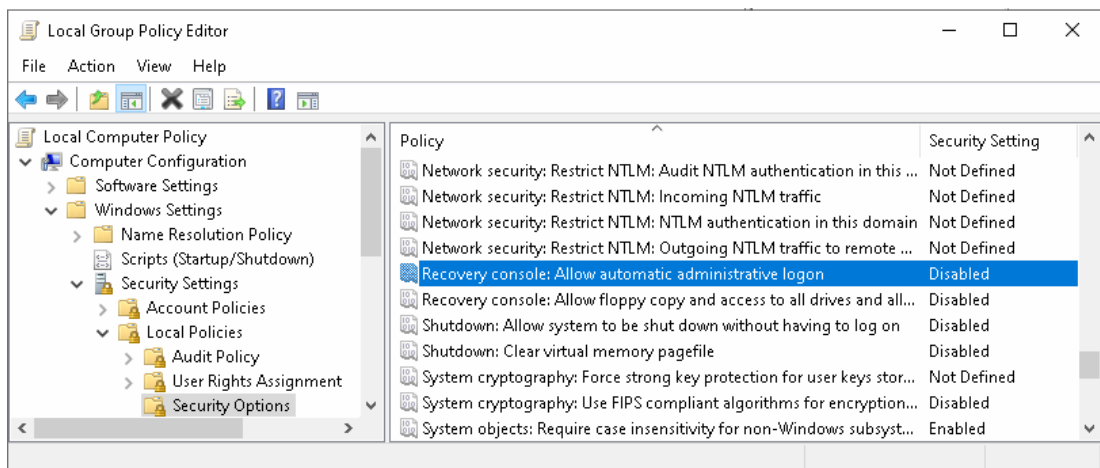


**Figure 5-5 Set password**

2. Click "Proceed" in pop-up tip interface, input the new password "supcondcs" in the interface of "Set Password for Administrator" and click "OK".

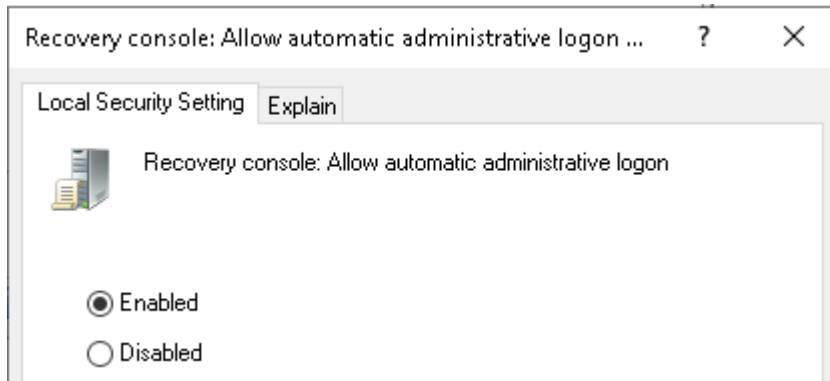
#### 5.1.4 Set Automatic Logon

1. Open "Run" interface by shortcut key "Windows + R", then type command "gpedit.msc" and click "OK", "Local Group Policy Editor" dialog box will pop up. Select "Computer Configuration / Windows Settings / Security Settings / Local Policy / Security Options" on the left.



**Figure 5-6 Local Group Policy Editor**

2. Double-click "Recovery console: Allow automatic administrative logon" on the right, select "Enabled" in the pop-up dialog box and click "OK" to save the change.



**Figure 5-7 Set automatic logon**



---

**Tip:**

Click “OK” or “Save” after modification every time.

---

## 5.2 Display Properties Settings



---

**Tip:**

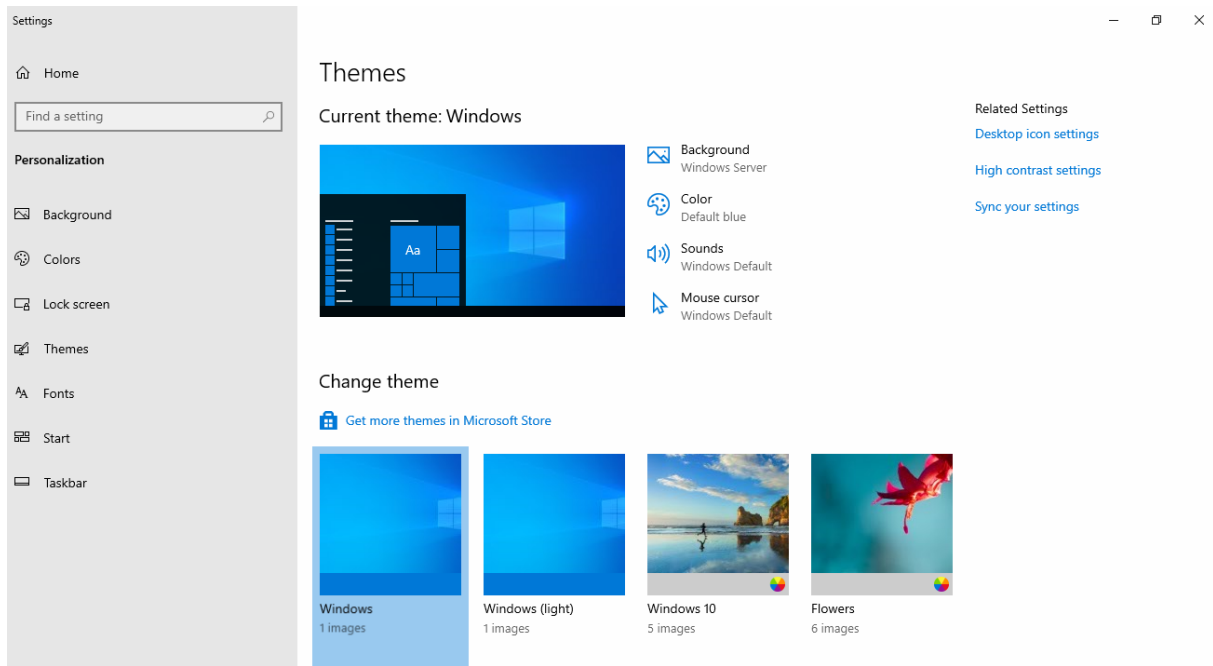
The view mode of control panel is “Type”. If you choose other mode, the path of settings may be different.

---

### 5.2.1 Set Windows Themes

Right click desktop, select “Personalize” in the right-click menu and pop up the interface shown as Figure 5-8.then click “Themes” and choose the theme “Windows”.

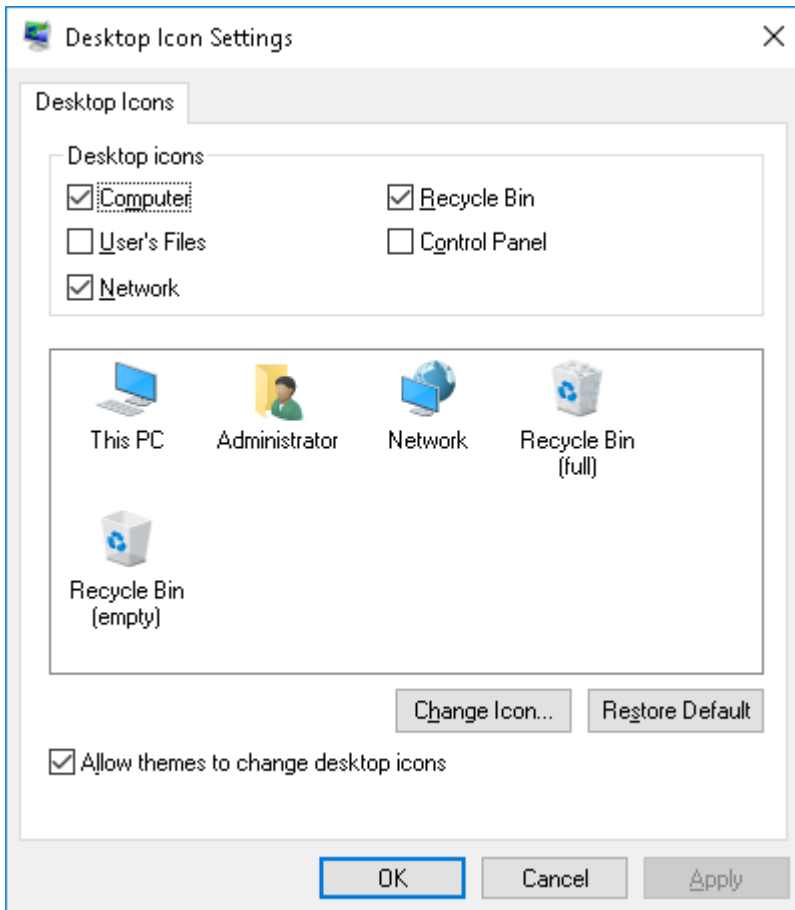




**Figure 5-8 Set Windows themes**

## 5.2.2 Change Desktop Icons

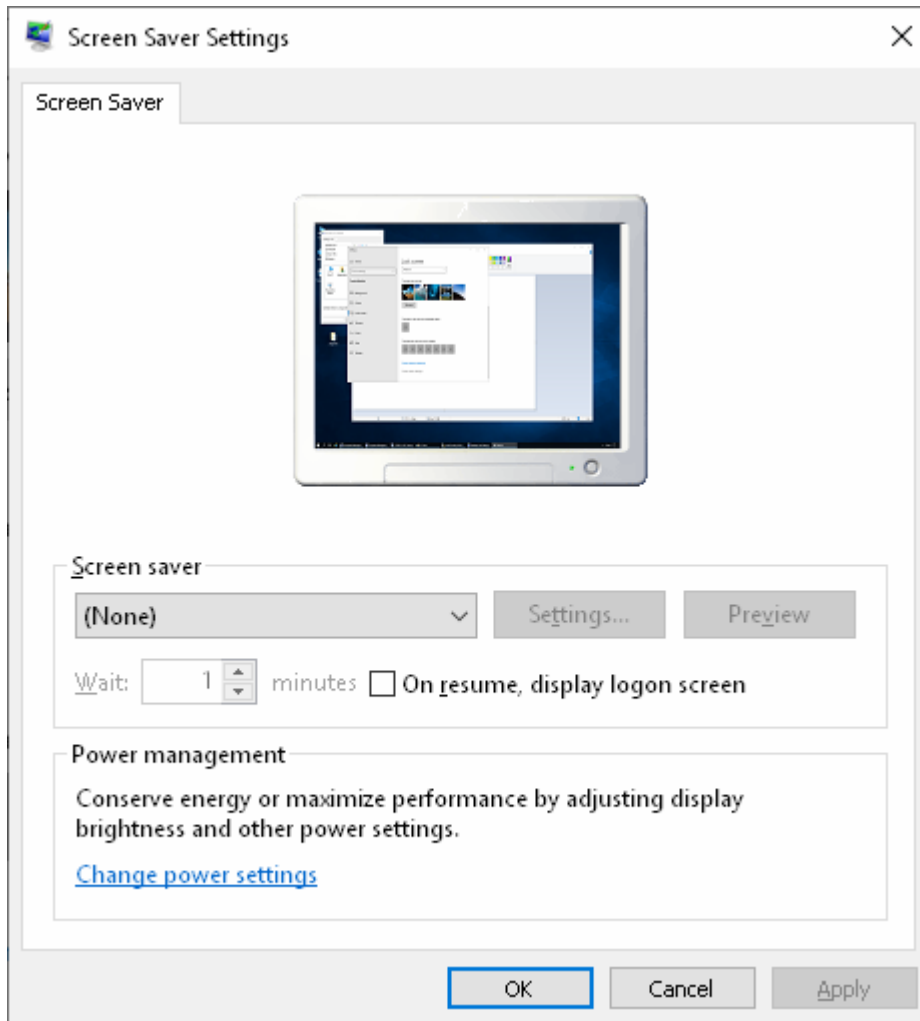
Click “Desktop icon settings” in the “Related Settings” list in the interface as Figure 5-8, pop up the dialog box shown as Figure 5-9, select “Computer” and “Network” and click “OK”(“Recycle Bin” is selected by default).



**Figure 5-9 Set desktop icons**

### 5.2.3 Set Screen Saver

Click “Lock screen” in the left interface of Figure 5-8, click “Screen saver settings” in personalization interface to pop up the interface as shown in Figure 5-10, set “Screen saver” to “None” (default) and click “OK”.



**Figure 5-10 Set Screen Saver**

### 5.2.4 Set Screen Resolution and Refresh Rate

Right click desktop, select “Display Settings” in the right-click menu and pop up the interface shown as Figure 5-11. Set “Change the size of text, apps, and other items” as “100% (Recommended)”, set “Display resolution” as “1920×1080(Recommended)” and set “Display orientation” as “Landscape”.

Generally, screen resolution could be set as recommended.

- 19” monitor: 1280 × 1024 pixels (recommended)
- 20” monitor: 1600 × 1200 pixels (recommended)
- 22” widescreen monitor: 1920 × 1080 pixels (recommended)
- 24” widescreen monitor: 1920 × 1080 pixels (recommended)

# Display

## Scale and layout

Change the size of text, apps, and other items

100% (Recommended) ▼

[Advanced scaling settings](#)

Display resolution

1920 × 1080 ▼

Display orientation

Landscape ▼

## Multiple displays

Older displays might not always connect automatically. Select Detect to try to connect to them.

Detect

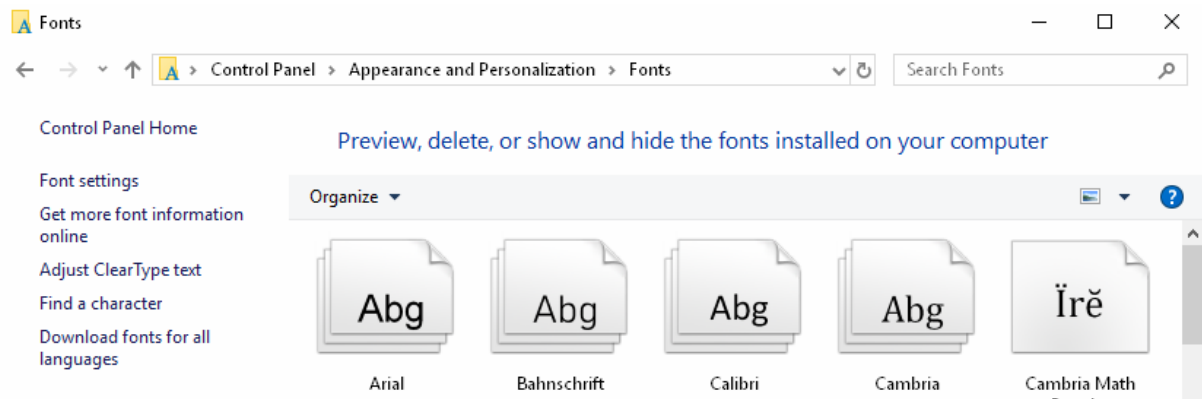
[Advanced display settings](#)

[Graphics settings](#)

**Figure 5-11 Set screen resolution**

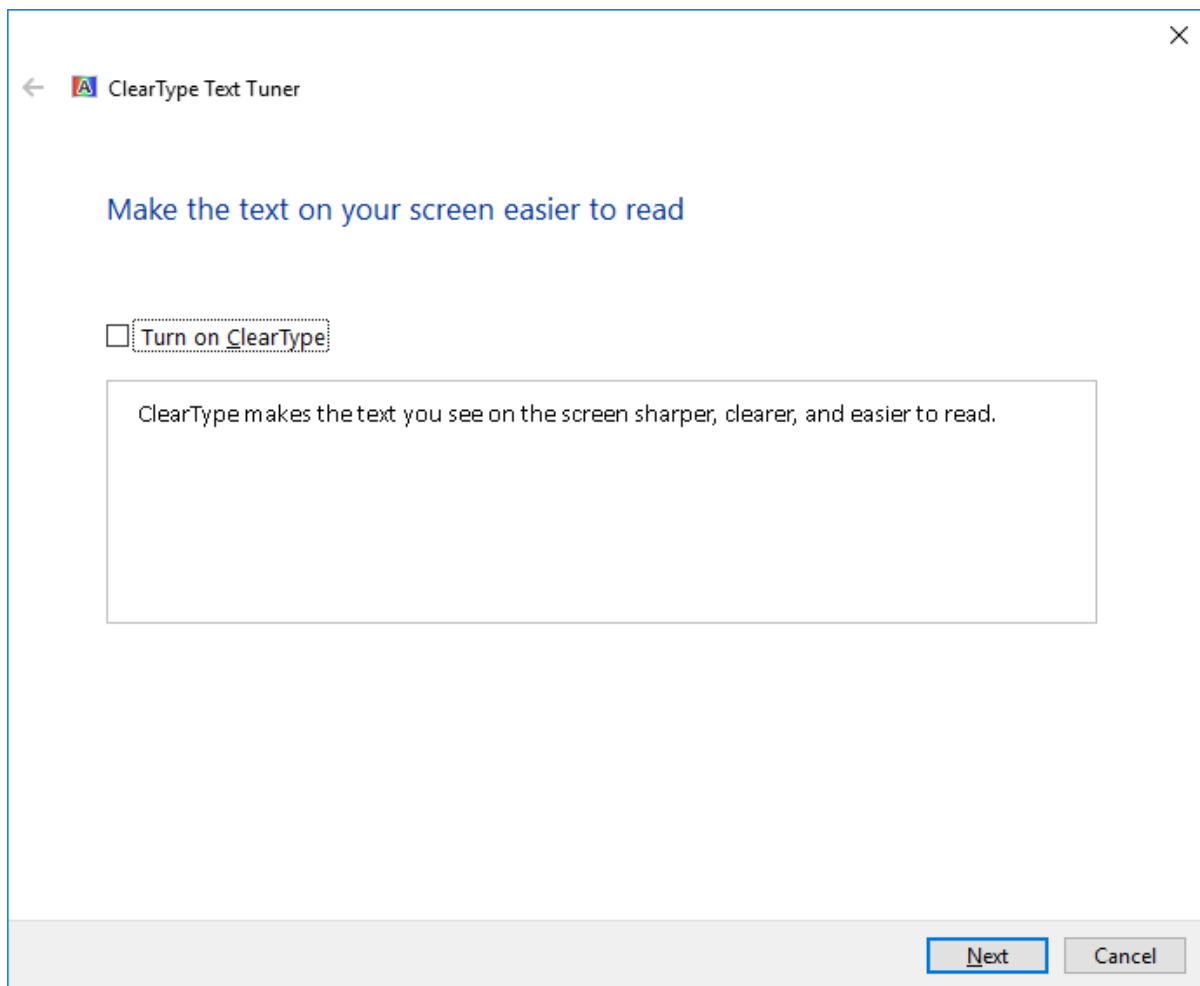
### 5.2.5 Turn off Clear Type Text Tuner

Select [Start\Control Panel\Appearance and Personalization\Fronts], the Figure 5-12 shown as follows.



**Figure 5-12 Fonts**

Click "Adjust ClearType Text" in the left interface of Figure 5-12 interface as to open the interface as shown in Figure 5-13. Unselect "Turn on ClearType", and click "Next" until "Finish".

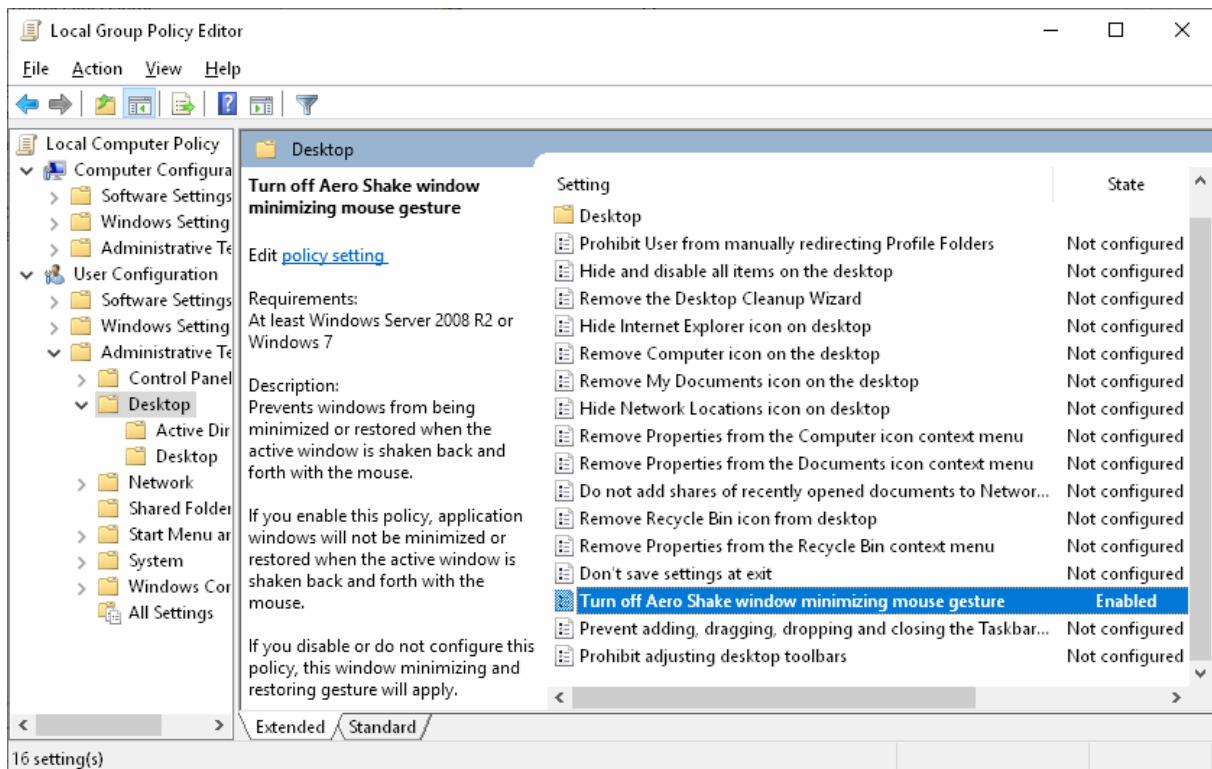


**Figure 5-13 Turn off Clear Type**

### 5.2.6 Turn off Aero Shake Window Minimizing Mouse Gesture

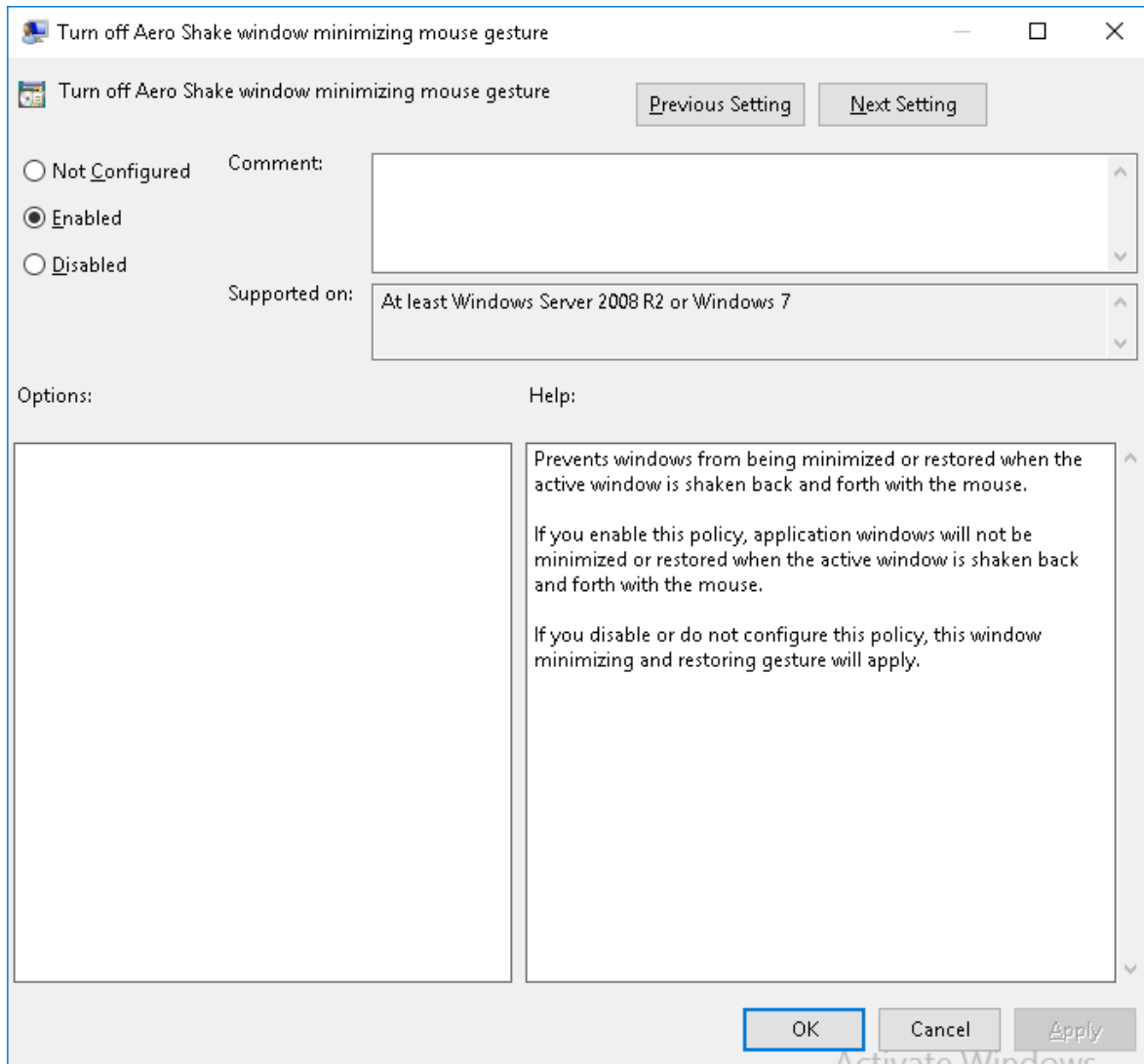
Open "Run" interface by shortcut key "Windows + R", then type command "gpedit.msc" in Run

dialog box and click “OK” to open the interface “Local Group Policy Editor”, as shown in Figure 5-14. Click [User Configuration/Administrative Templates/Desktop] in left structure tree and double-click “Turn off Aero Shake window minimizing mouse gesture” in the right interface.



**Figure 5-14 Local group policy editor**

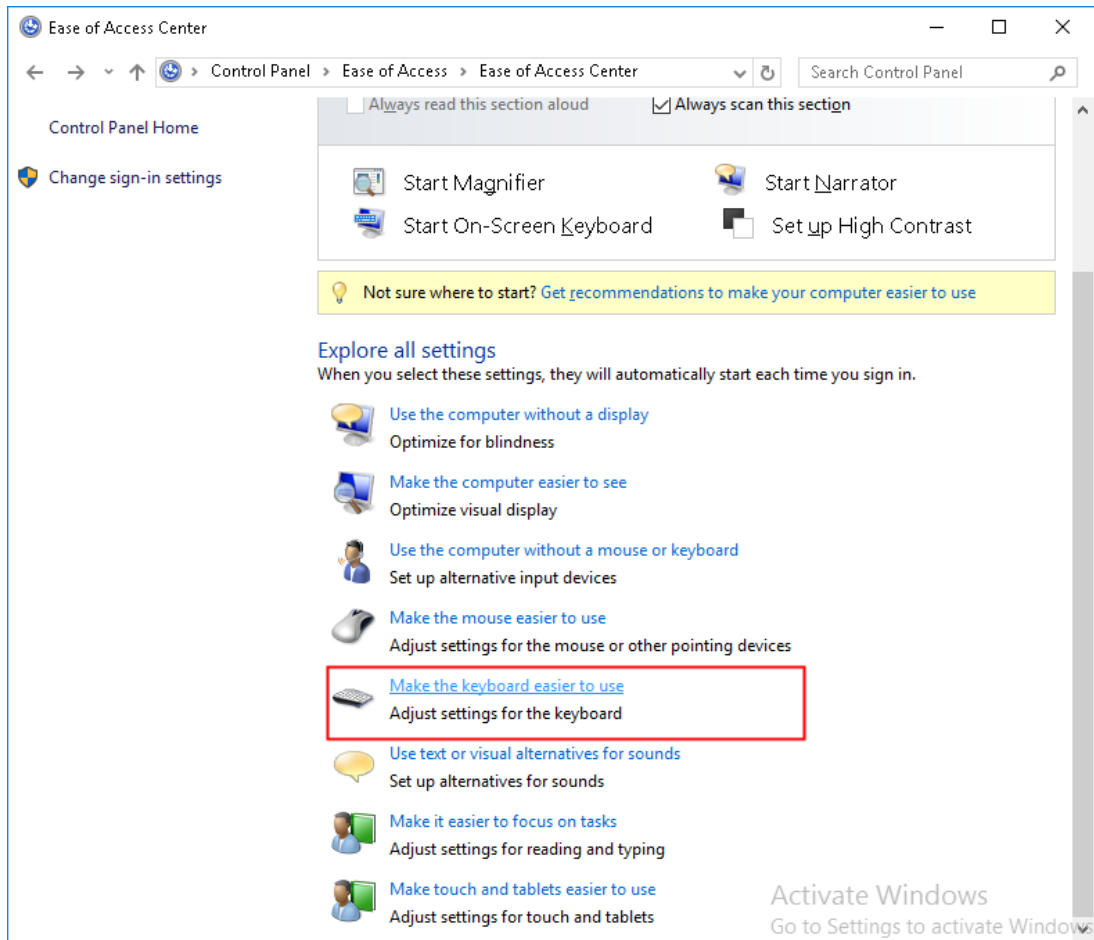
Pop up the dialog box as shown in Figure 5-15, select “Enabled” and click “OK” to end.



**Figure 5-15** Turn off Aero Shake window minimizing mouse gesture

## 5.3 Turn off Sticky Keys and Toggle Keys

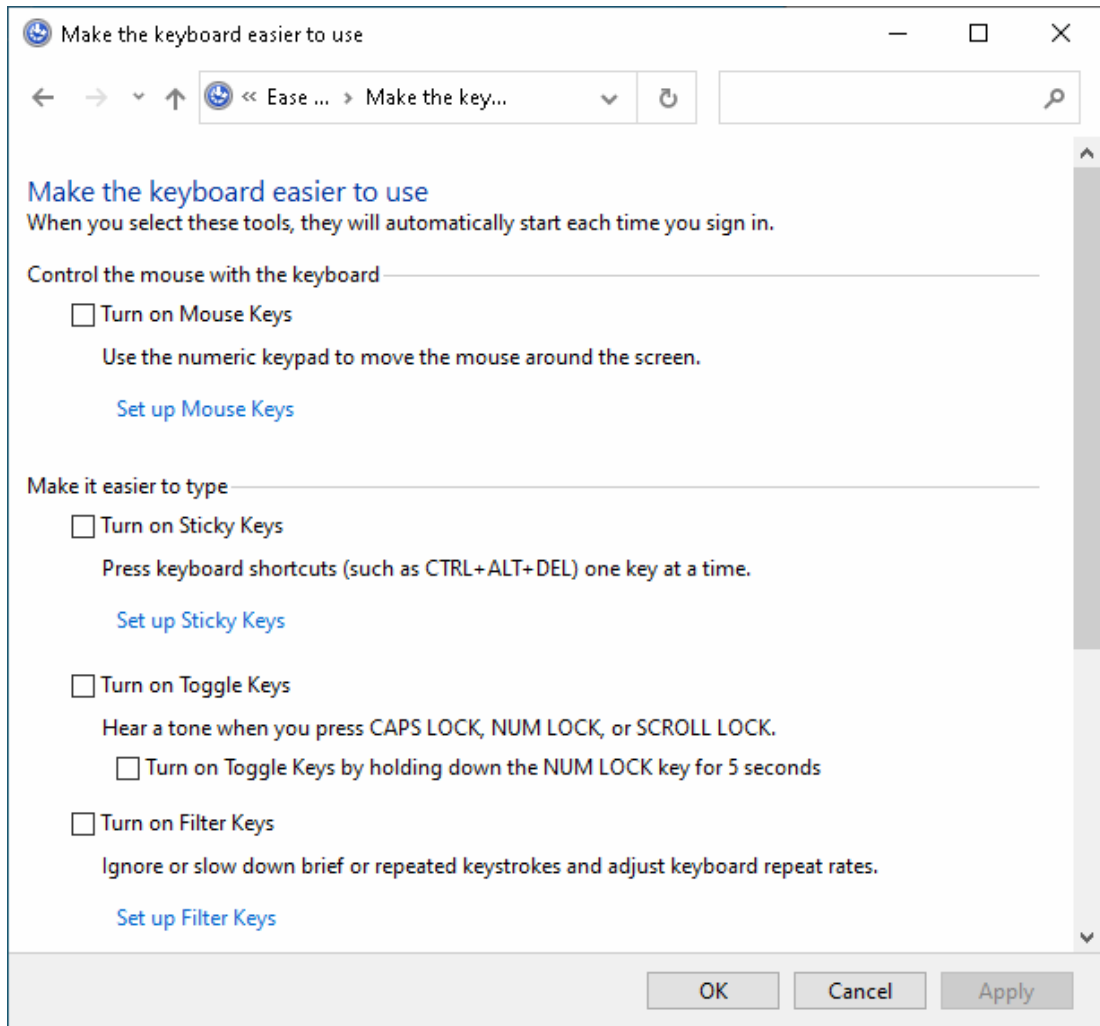
1. Select [Start\Control Panel\Ease of Access\Ease of Access Center], click "Make the keyboard easier to use", the figure shown as follows.



**Figure 5-16 Ease of access center**

2. Unselect “Turn on Sticky Keys”, “Turn on Toggle Keys” and “Turn on Toggle Keys by holding down the NUM LOCK key for 5 seconds”, as shown in Figure 5-17.





**Figure 5-17 Turn off sticky keys and toggle keys**

3. Click "Set up Sticky Keys" in the interface shown above and set as shown in Figure 5-18.

### Set up Sticky Keys

☐ Turn on Sticky Keys

Press keyboard shortcuts (such as CTRL+ALT+DEL) one key at a time.

Keyboard shortcut

☐ Turn on Sticky Key when SHIFT is pressed five times

When using keyboard shortcuts to turn Ease of Access settings on:

☐ Display a warning message when turning a setting on

☐ Make a sound when turning a setting on or off

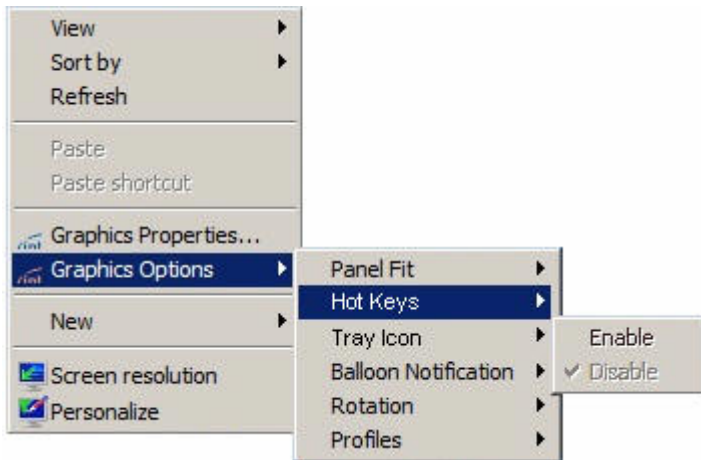
**Figure 5-18 Turn off keyboard shortcut**

## 5.4 Turn off Hot Keys of Rotating Screen

If integrated display card is used in computer (such as Lenovo TS140), and the hot keys of rotating

screen should be disabled, operation: right click any blank in desktop, and pop up the menu as shown in Figure 5-19, select [Graphics Options/Hot Keys/Disable].

If there is not menu as shown in Figure 5-19, and jump over this setting.



**Figure 5-19** Turn off hot keys of rotating screen

## 5.5 Taskbar Properties

Right click taskbar, and select “Taskbar settings” in the right-click menu, set “Lock the taskbar” as “On”, as shown in Figure 5-20. For other settings, please keep their default options.

## Taskbar

Lock the taskbar



Automatically hide the taskbar in desktop mode



Automatically hide the taskbar in tablet mode



Use small taskbar buttons



Use Peek to preview the desktop when you move your mouse to the Show desktop button at the end of the taskbar



Replace Command Prompt with Windows PowerShell in the menu when I right-click the start button or press Windows key+X



Show badges on taskbar buttons



Taskbar location on screen



Combine taskbar buttons



[How do I customize taskbars?](#)

*Figure 5-20 System icons settings*

## 5.6 Time Settings

Select [Start\ Control Panel\ Clock and Region\ Region], pup up the figure shown in Figure 5-21.  
Set as follow introduction:

- Short data: M/d/yyyy
- Long data: dddd, MMMM d, yyyy
- Short time: HH:mm
- Long time: HH:mm:ss

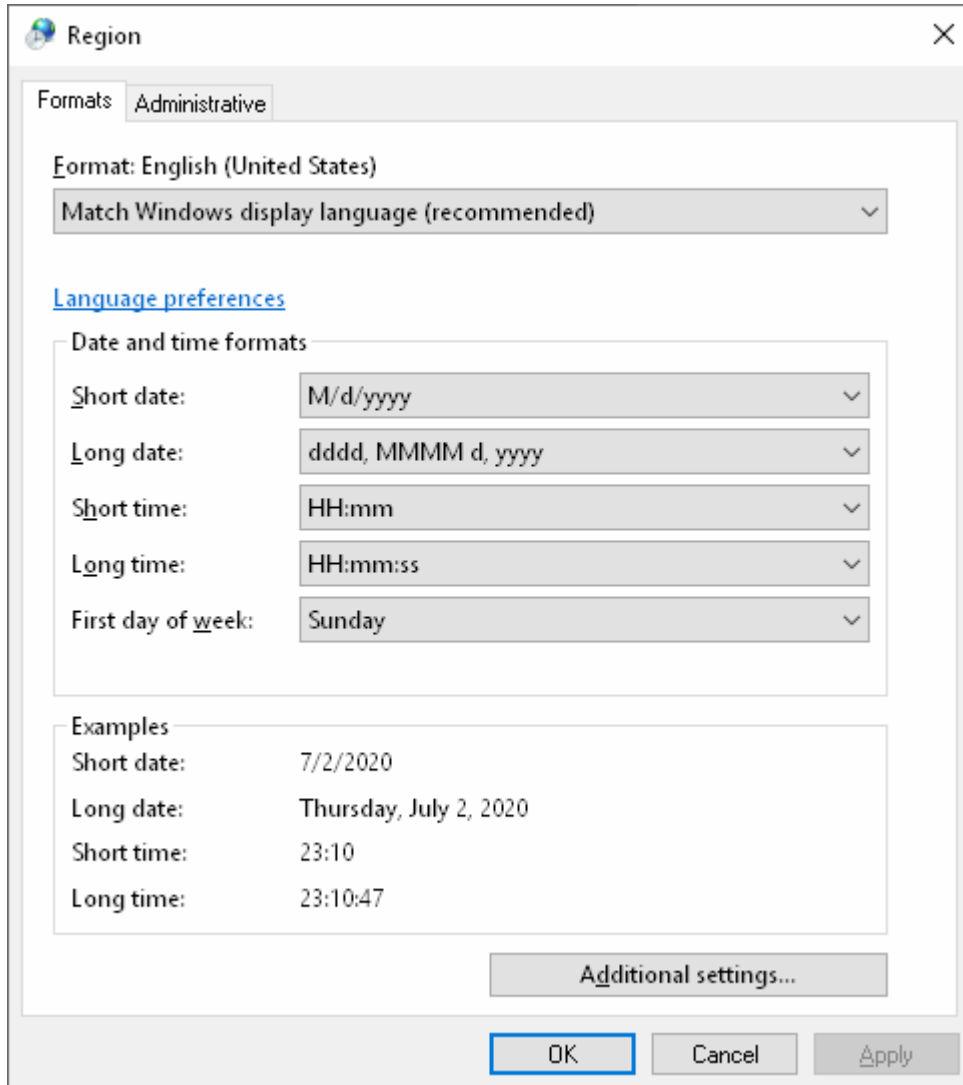
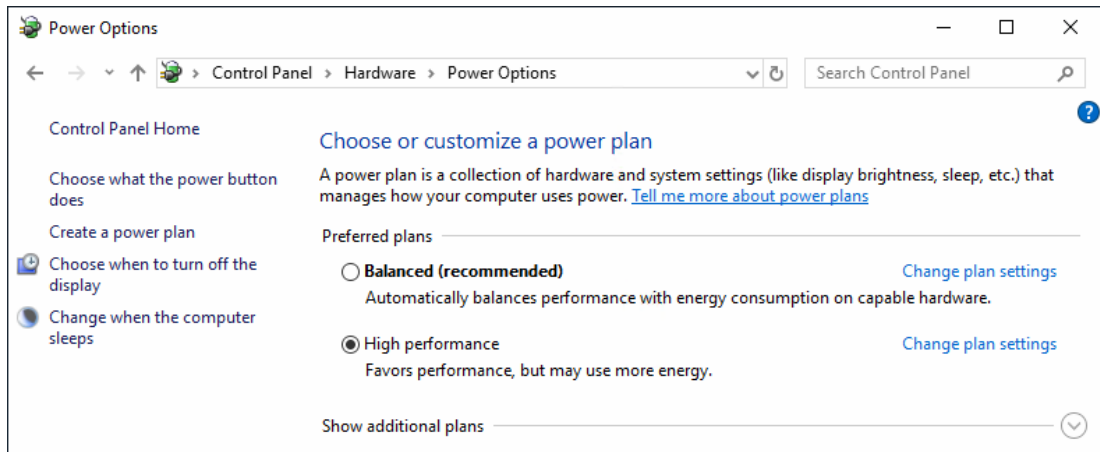


Figure 5-21 Region and language options

## 5.7 System and Security Settings

### 5.7.1 Set Power Options

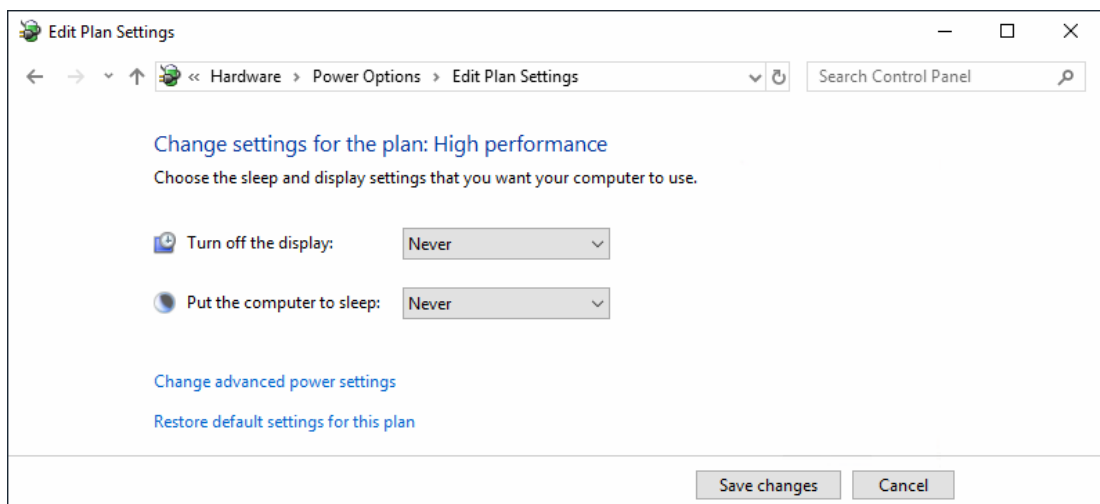
1. Select [Start\ Control Panel\ System and Security\ Power Options] to pop up the interface shown as the following figure. Click "Show additional plans" and select "High performance" plan, which is balanced plan by default. Then, click "Change plan settings" in the "High performance" plan,



**Figure 5-22 Power Options**

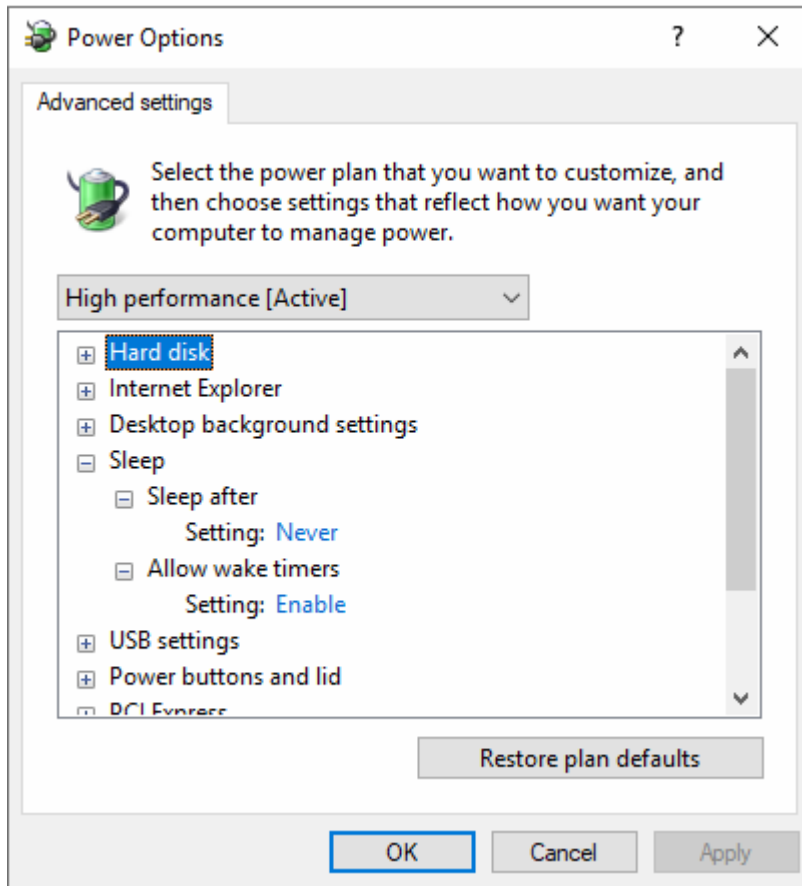
2. Click “Change plan settings” in the default “High performance” plan, pop up the “Edit Plan Settings” interface, set “Turn off the display” as “Never”, then click “Save changes” in the bottom. As shown in the following figure.

“Put the computer to sleep” may be displayed in the interface of different computer, it should also be set to “Never”.



**Figure 5-23 Set power plan**

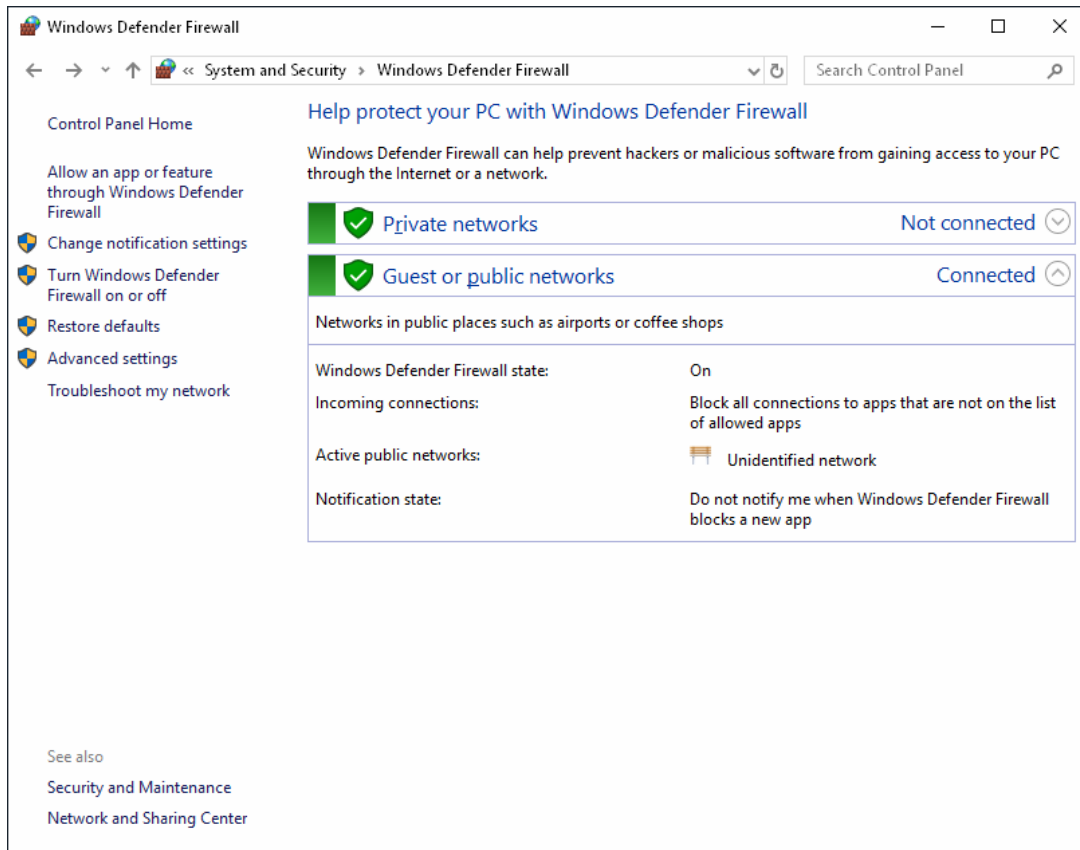
3. Click “Change advanced power settings” in the figure above, pop up “Power Options” dialog box as shown in the following figure. Set “Allow wake timers” as “Enable” and click “OK”.



*Figure 5-24 Set sleep options*

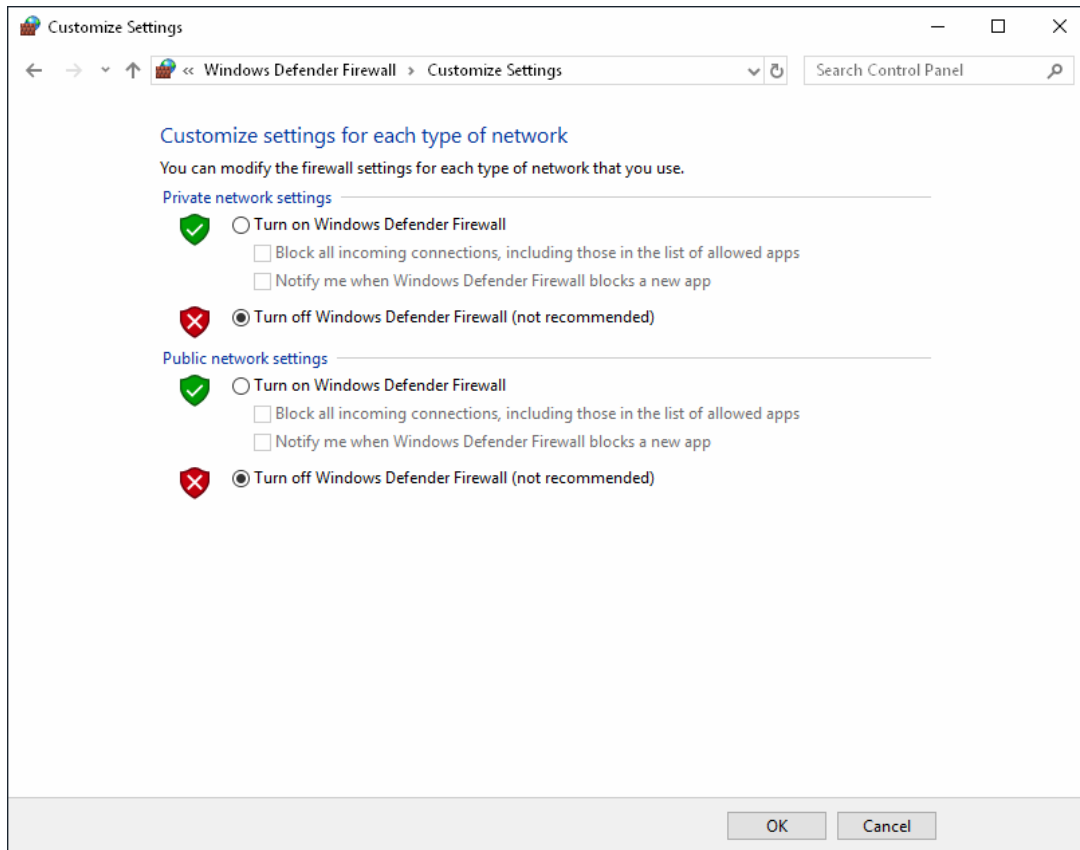
### 5.7.2 Turn off Windows defender firewall

1. Select [Start\ Control Panel\ System and Security \Windows Defender Firewall], pop up the interface as shown in Figure 5-25.



**Figure 5-25 Windows Defender Firewall interface**

2. Click "Turn Windows Firewall on or off" in the left to pop up the interface as shown in Figure 5-26, turn off all Windows firewalls and click "OK".

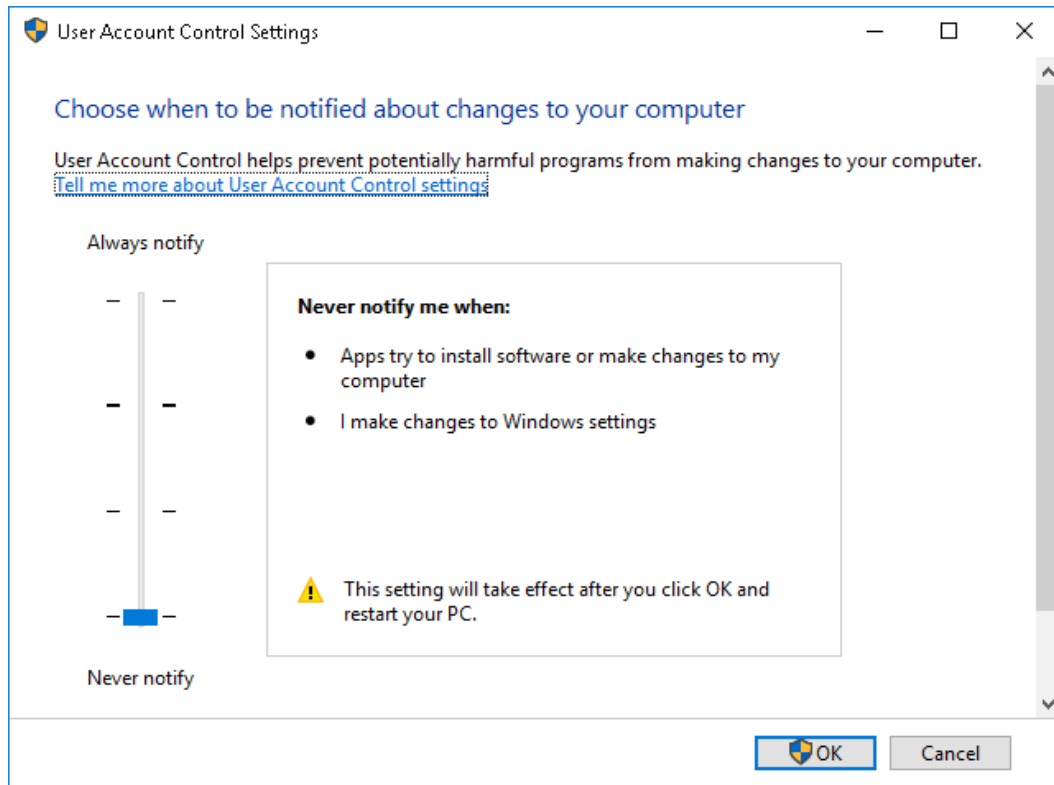


**Figure 5-26 Windows Defender Firewall settings**

### 5.7.3 User Accounts Control Settings

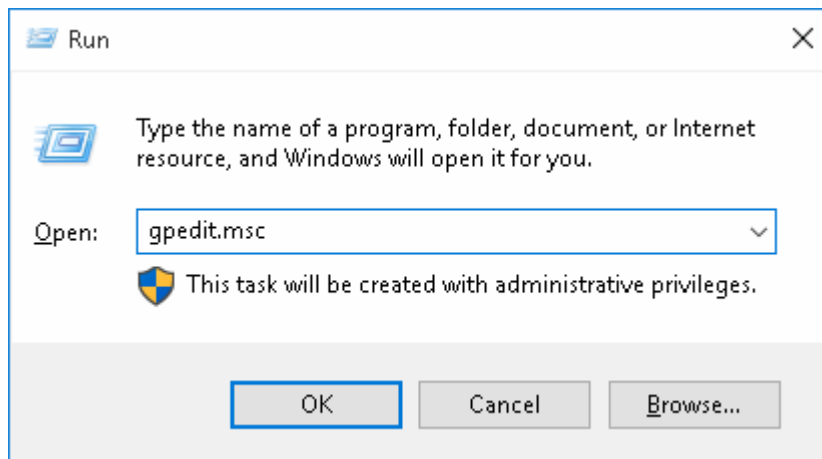
1. Select [Start\ Control Panel\ System and Security\ Security and Maintenance\ Change User Account Control Settings], pop up the interface shown as Figure 5-27 Set “Allow notify” to “Never notify” by pulling down the scroll button to the bottom and click “OK”.





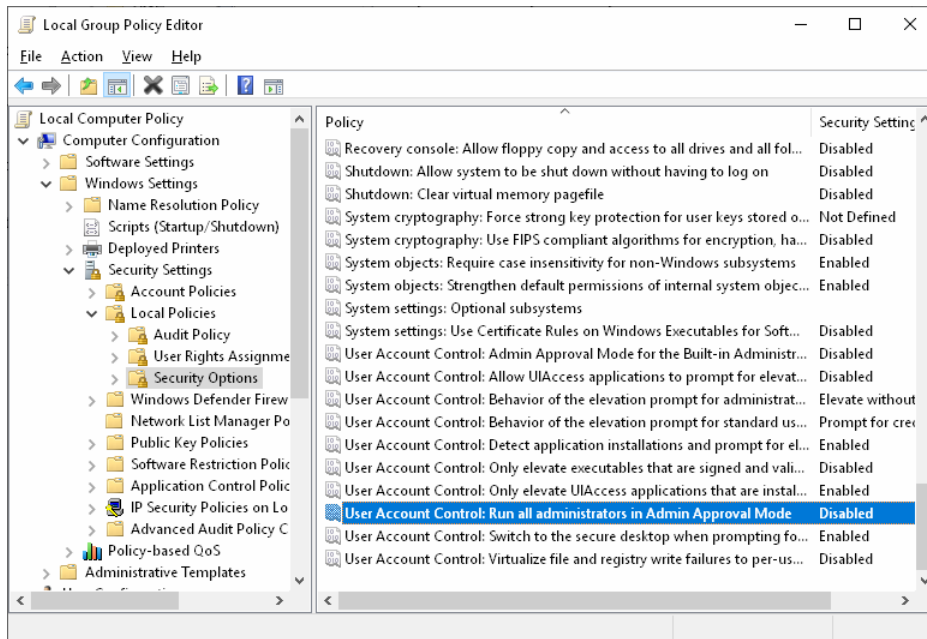
**Figure 5-27 User account control settings**

2. Open "Run" interface by shortcut key "Windows + R", then type command "gpedit.msc" in Run dialog box, as shown in the following figure.



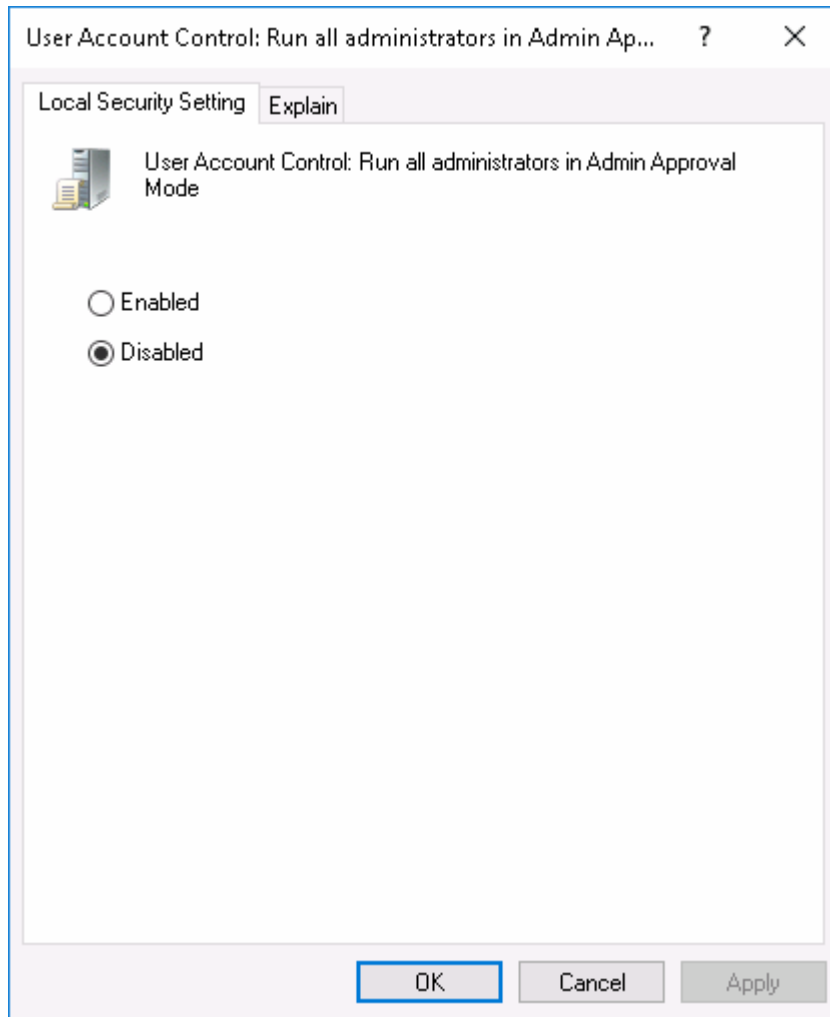
**Figure 5-28 Run dialog box**

3. Click "OK" to pop up the "Local Group Policy Editor" interface, extend "Computer Configuration", select "Computer Configuration> Windows Settings > Security Settings > Local Policies > Security Options", as shown in the Figure 5-29.



**Figure 5-29 Change setting in Local Group Policy Editor**

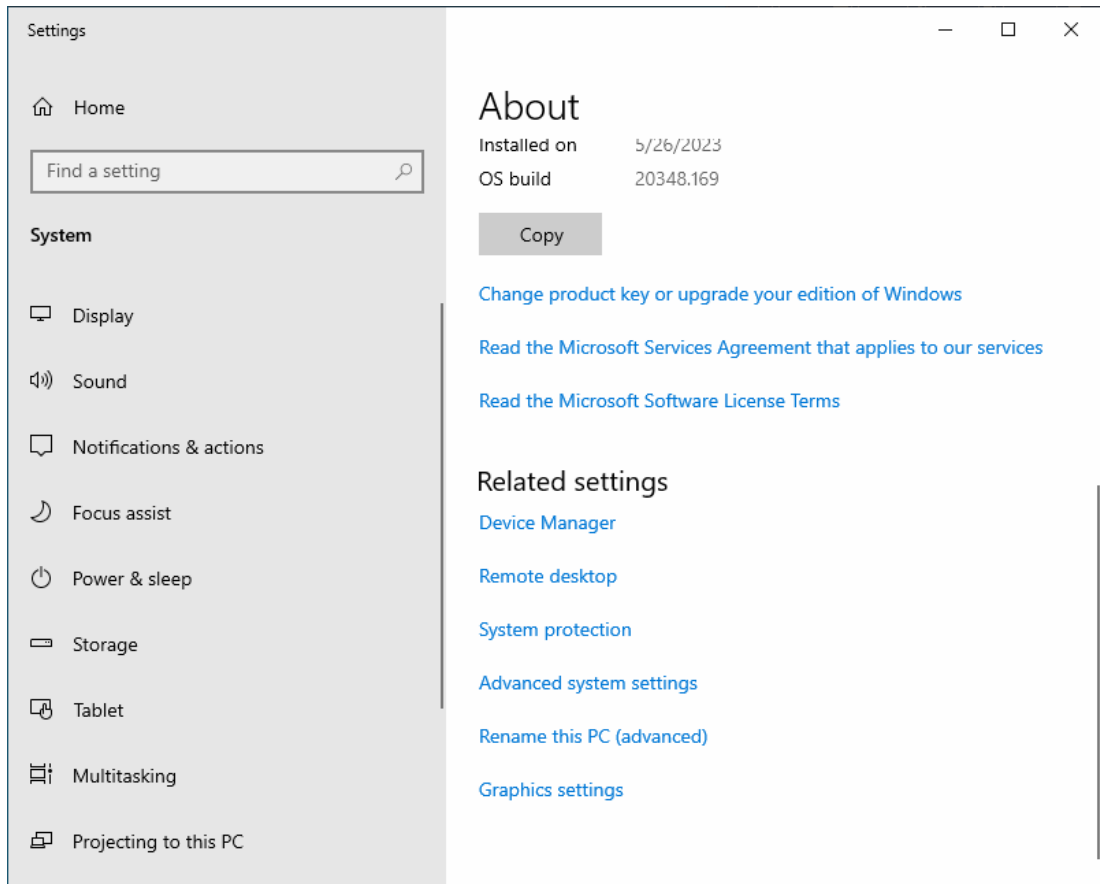
4. Double-click “User Account Control: Run all administrators in Admin Approval Mode” in the right interface to open the dialog box, and set as “Disabled”, as shown below. Then click “Apply” and “OK”, the change will take effect after restarting the computer.



*Figure 5-30 Disable the user account control property*

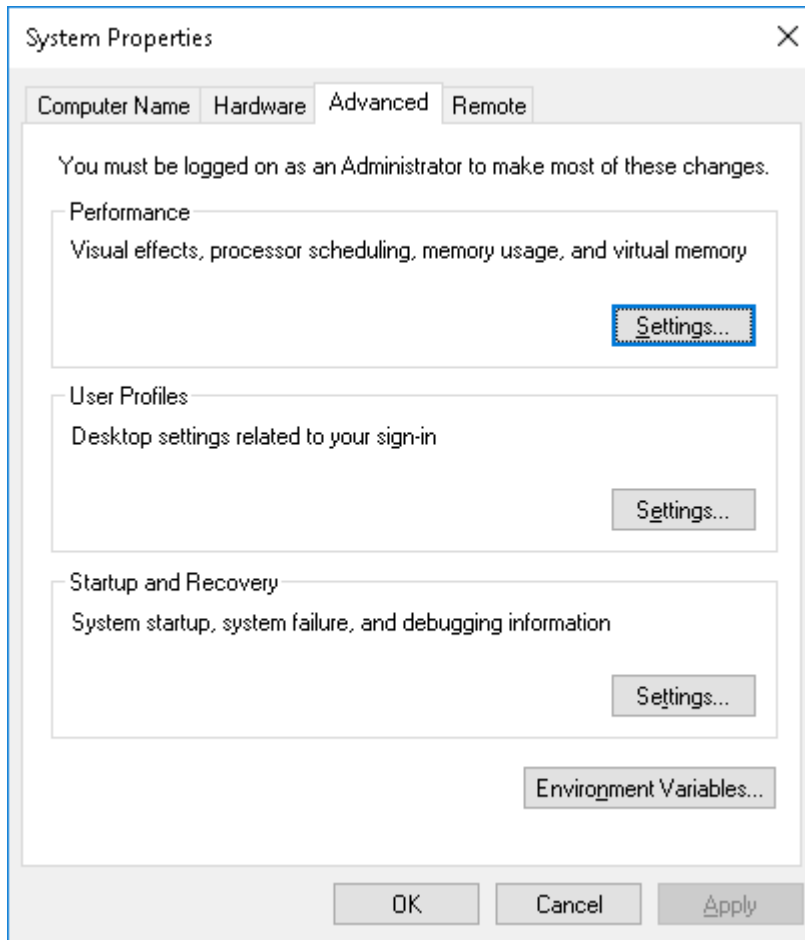
#### **5.7.4 Performance options settings**

1. Select [Start\ Control Panel\ System and Security\ System] to pop up the interface shown as Figure 5-31.



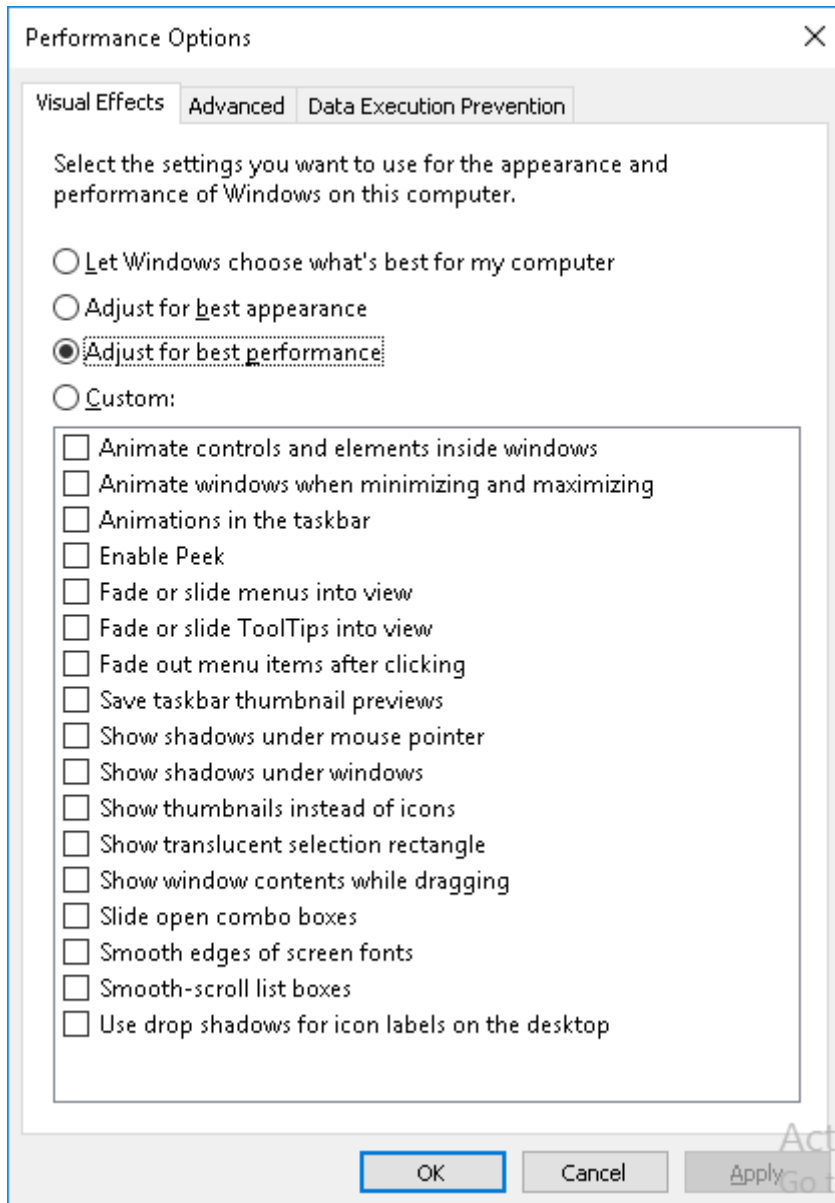
**Figure 5-31 System interface**

2. Select “Advanced system settings” option page in the Related Settings list of system properties interface, as shown in Figure 5-32.



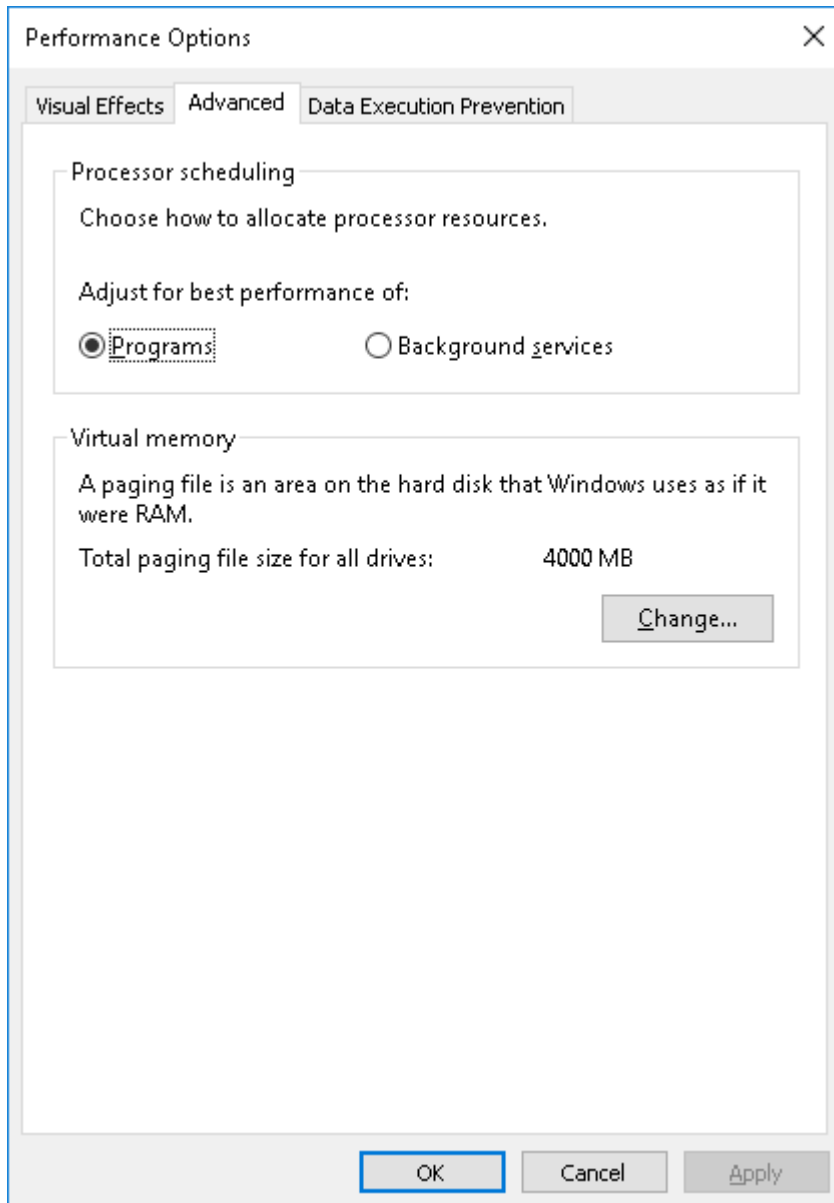
**Figure 5-32** Dialog box of Advanced settings of system properties

3. Click “Settings” in “Performance” window, pop up “Performance Options” interface, as shown in Figure 5-33. Select “Adjust for best performance” in “Visual Effects” option page.



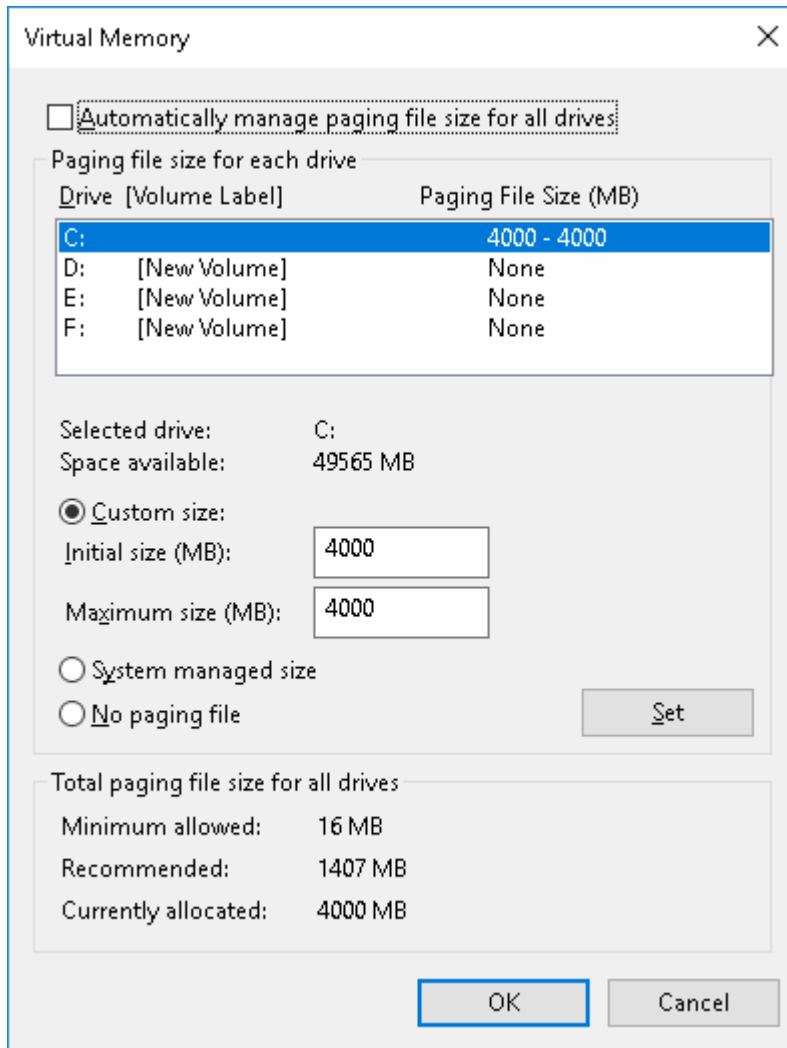
**Figure 5-33 Select “Adjust for best performance”**

4. Select “Advanced” option page, advanced properties interface is shown in Figure 5-34.



**Figure 5-34** Dialog box of advanced settings of performance options

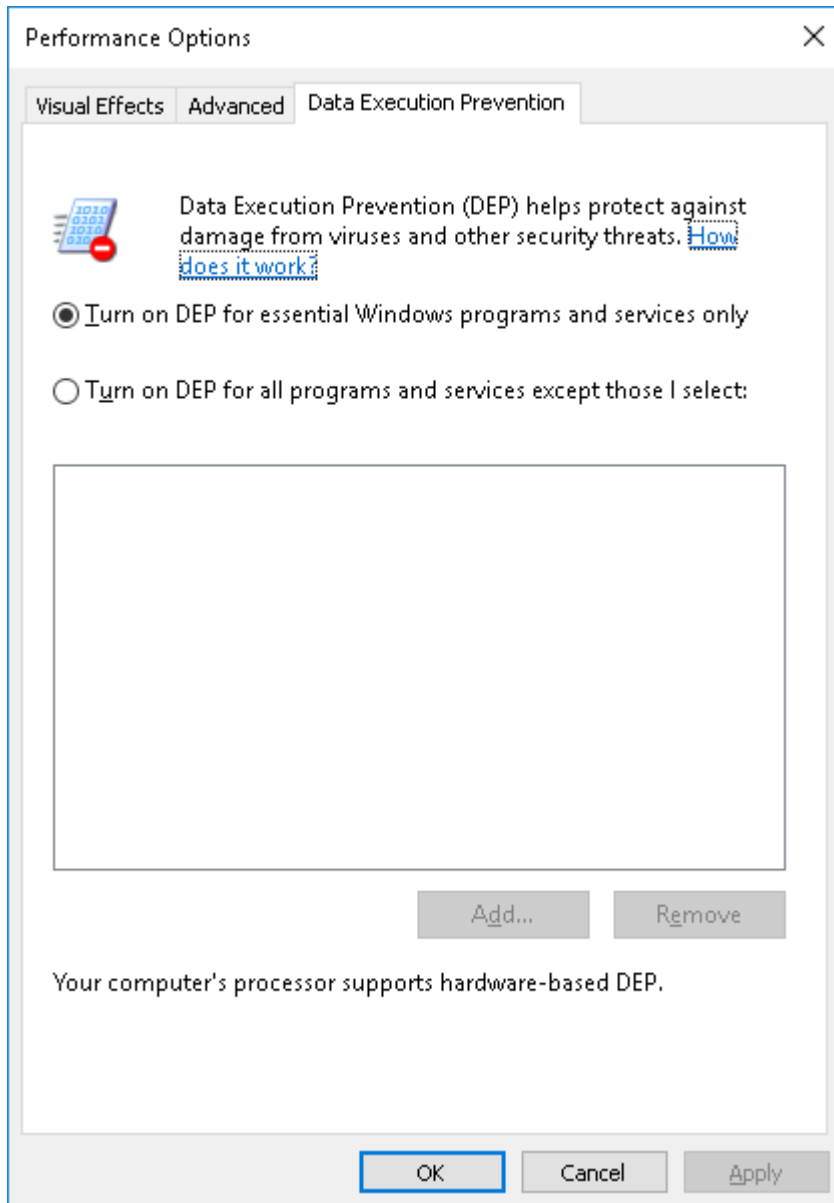
5. Click "Change" in "Virtual memory" window, pop up virtual memory setting interface. Deselect "Automatically manage paging file size for all drives", and select "Custom size", set the value of "Initial size" and "Maximum size" to 3000MB (4000MB when the RAM is larger than 2GB), as shown in Figure 5-35. Then set "OK" to save the change.



**Figure 5-35 Set virtual memory**

- Back to "Performance Options" interface as Figure 5-34, click "Data Execution Prevention" tab and select "Turn on DEP for essential Windows programs and services only", as shown in Figure 5-36, then click "Apply" to save the change.



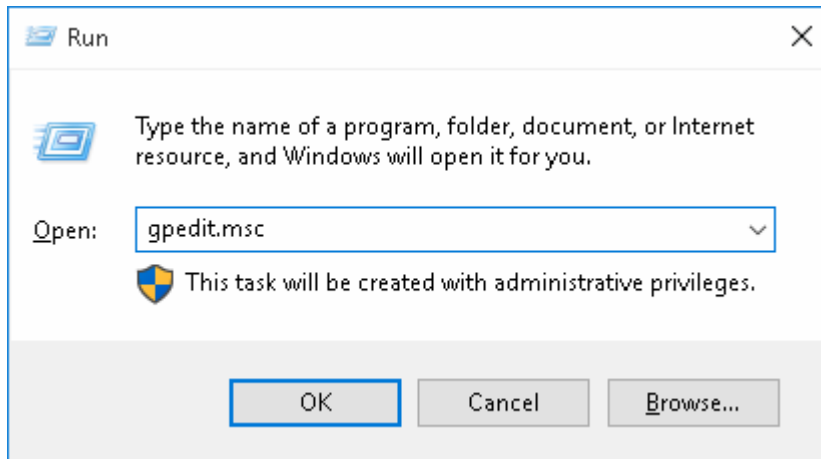


**Figure 5-36 Close data execution prevention**

7. Click “OK” and restart the computer following the tips.

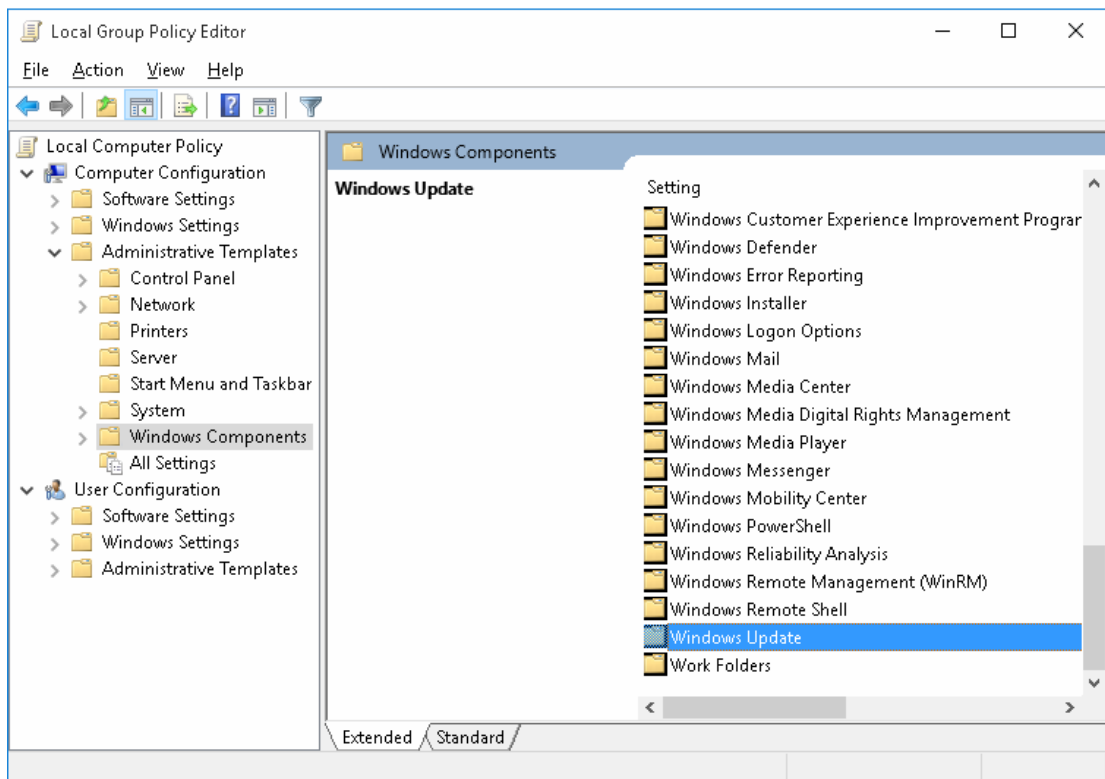
### 5.7.5 Turn off auto-update

1. Open “Run” interface by shortcut key “Windows + R”, then type command “gpedit.msc” in Run dialog box and click “OK”, as shown in Figure 5-37.



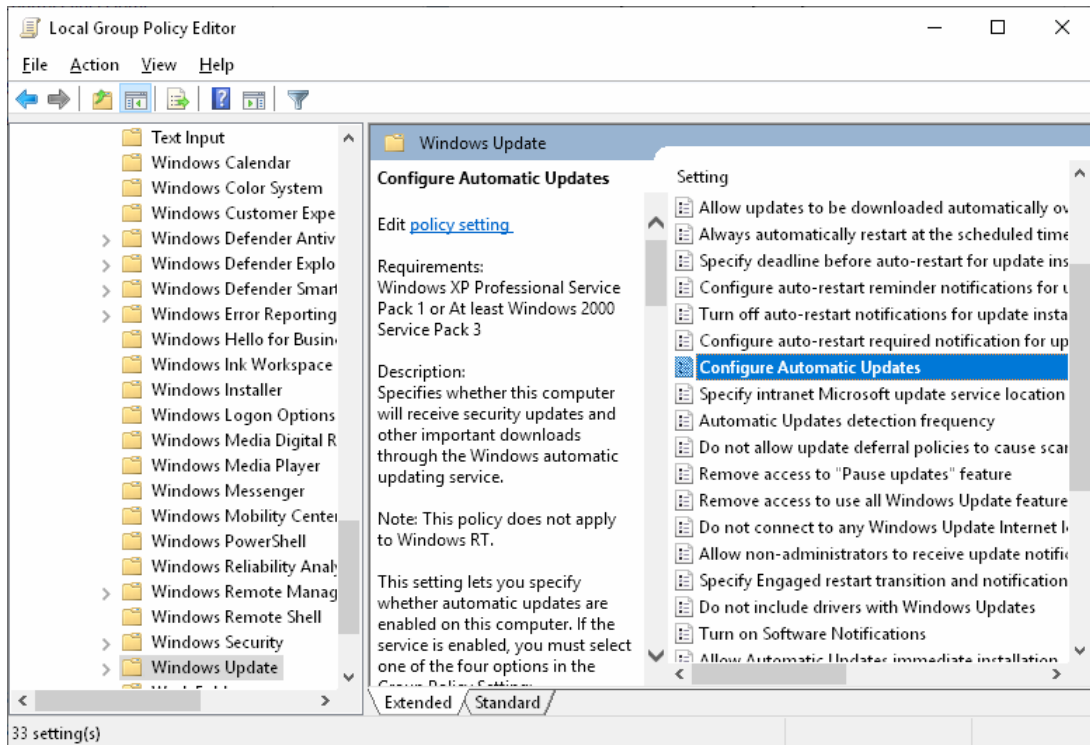
**Figure 5-37 Run command**

2. Click “OK” to pop up the interface of Local Group Policy Editor. Extend “Computer Configuration”, select “Windows Component” below “Administrative Templates”, as shown in Figure 5-38.



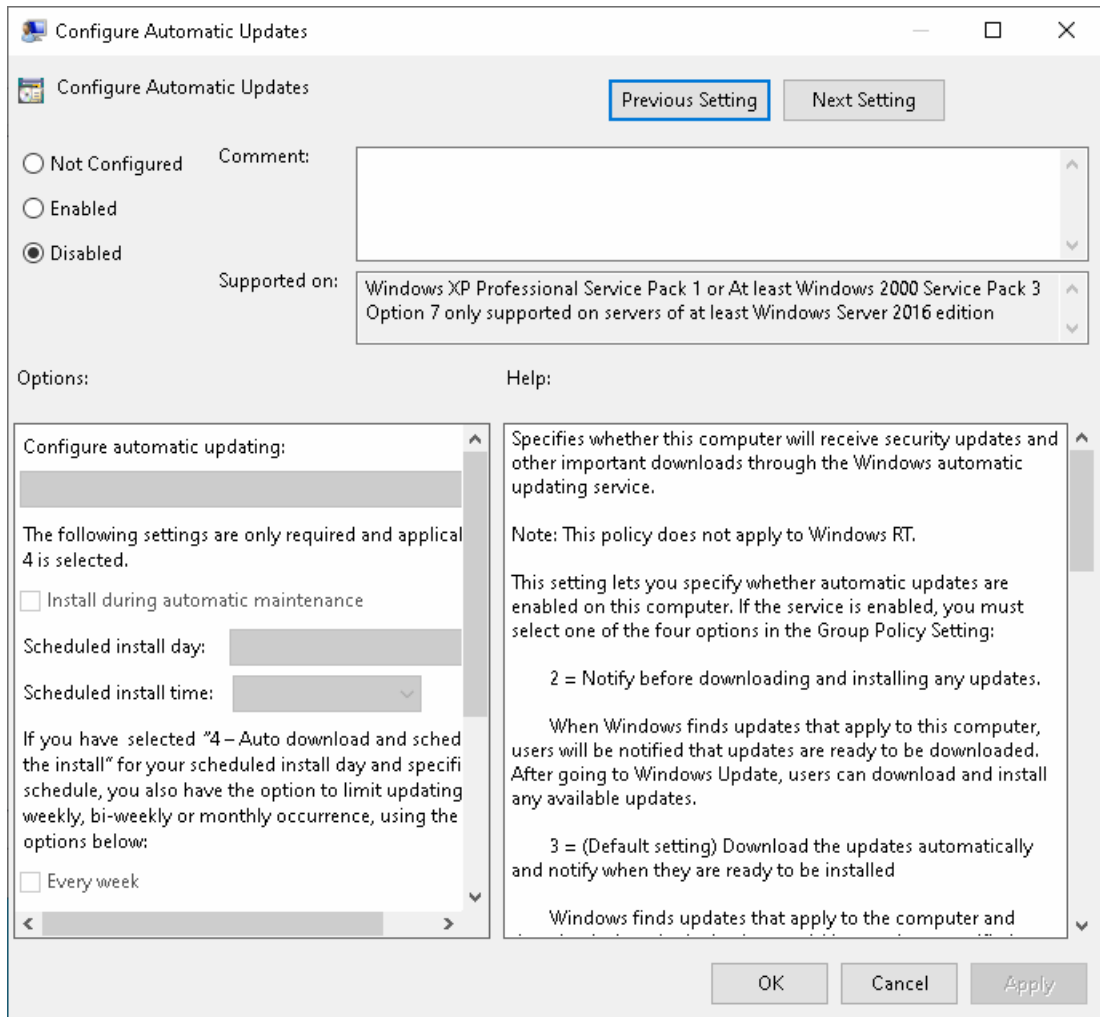
**Figure 5-38 Local group policy editor interface**

3. Double-click “Windows Update” in “Windows Components” list and pop up the interface shown as Figure 5-39.



**Figure 5-39 Windows update interface**

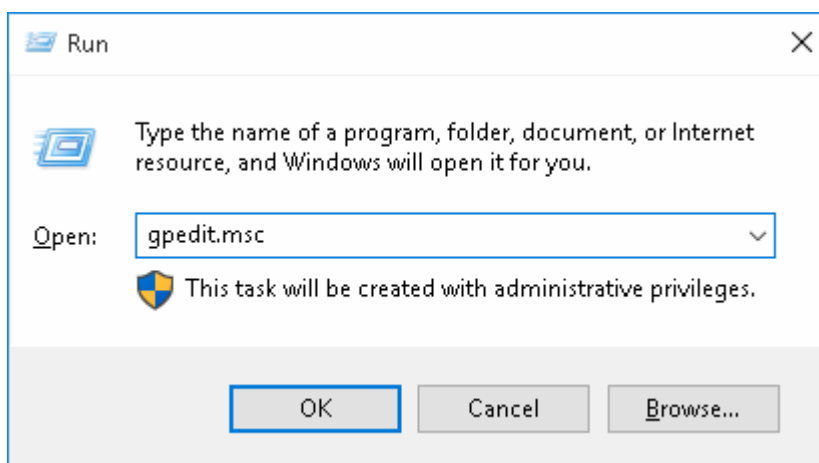
4. Double-click “Configure Automatic Updates” in “Windows Update” interface and pop up the interface shown as Figure 5-40. Select “Disabled”, click “Apply” and “OK”, the change will take effect after restarting the computer.



**Figure 5-40 Turn off auto-update**

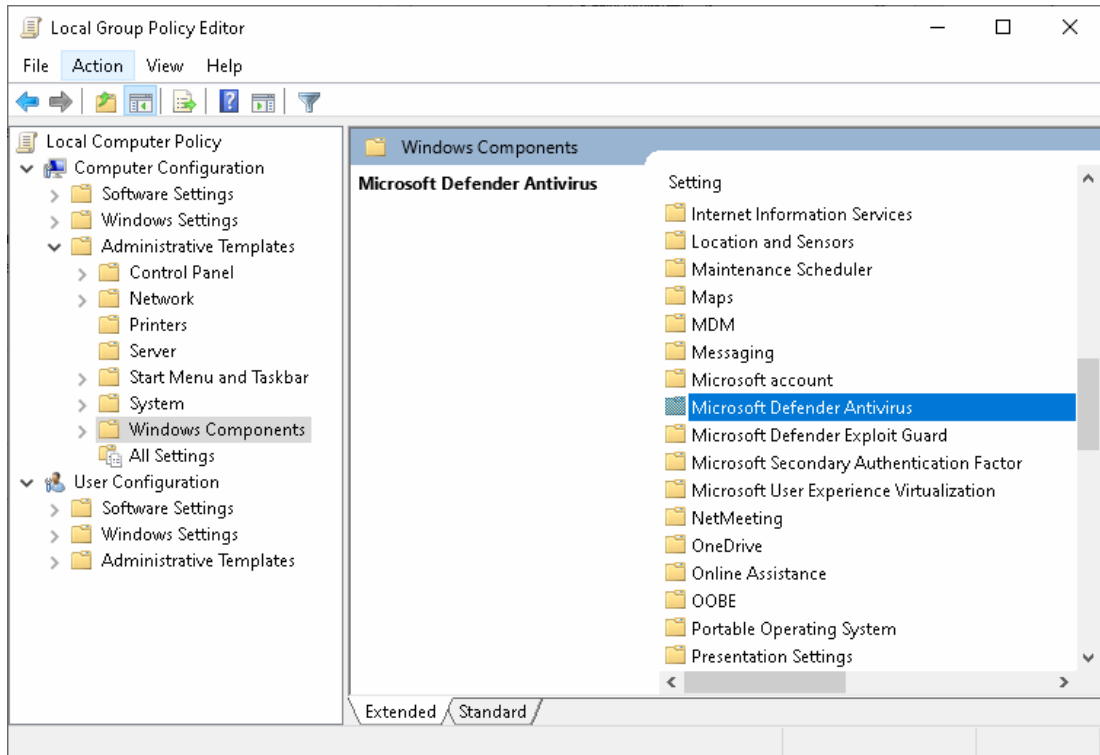
### 5.7.6 Turn off Microsoft Defender Antivirus

1. Open "Run" interface by shortcut key "Windows + R", then type command "gpedit.msc" in Run dialog box and click "OK", as shown in Figure 5-41.



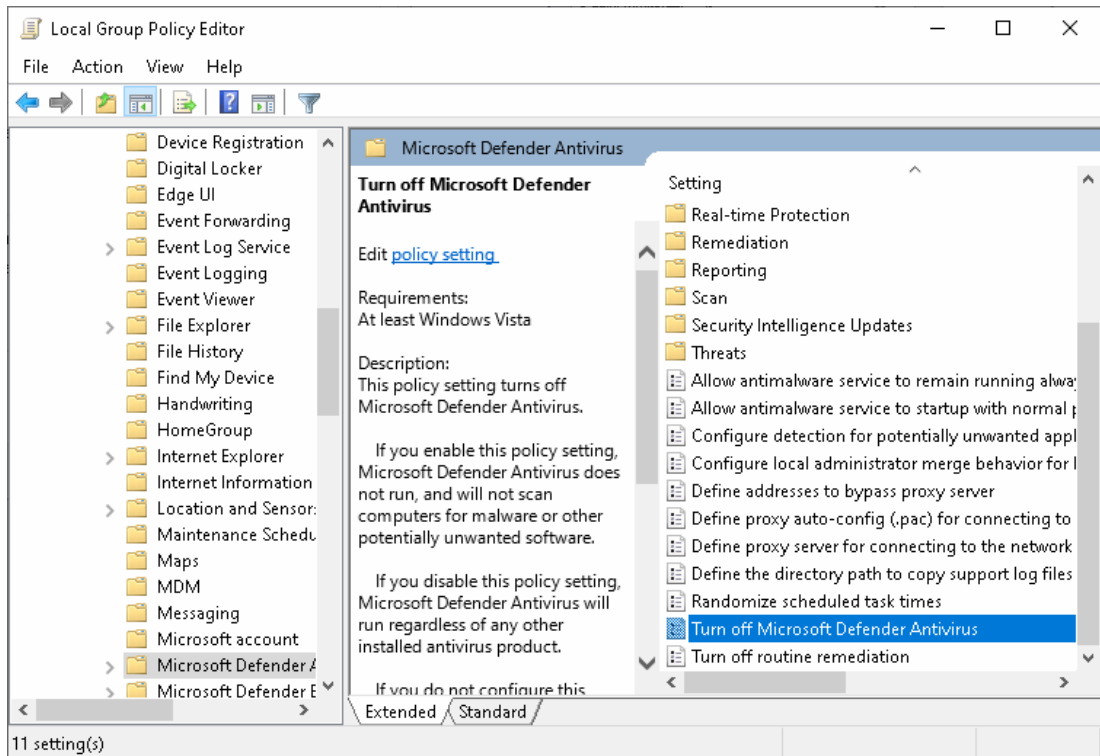
**Figure 5-41 Run command**

- Click “OK” to pop up the interface of Local Group Policy Editor. Extend “Computer Configuration”, select “Windows Component” below “Administrative Templates”, as shown in Figure 5-42.



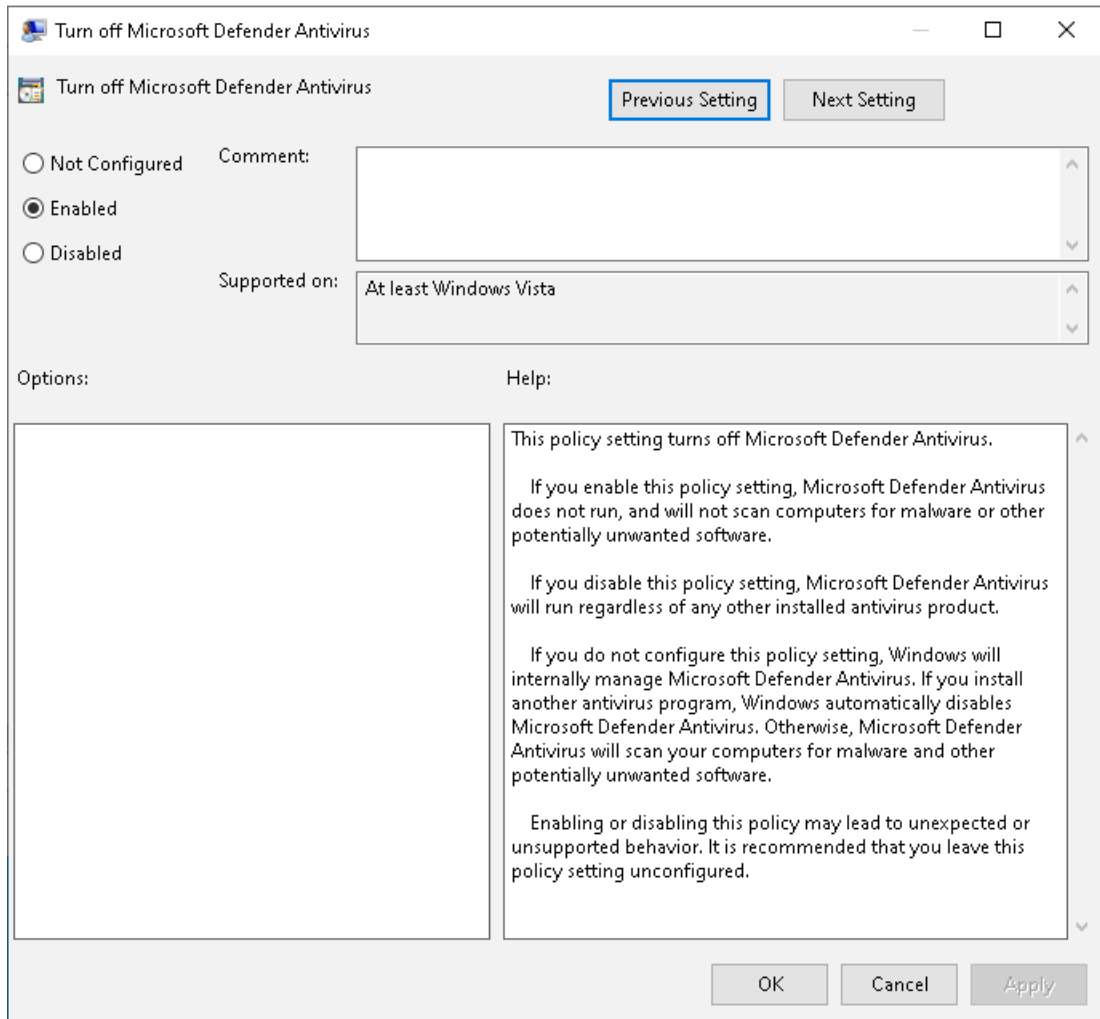
**Figure 5-42 Local group policy editor interface**

- Double-click “Microsoft Defender Antivirus” in the list of “Windows Components” and pop up the interface shown as Figure 5-43.



**Figure 5-43 Microsoft Defender Antivirus interface**

4. Double-click “Turn off Microsoft Defender Antivirus” and pop up the interface shown as Figure 5-44. Select “Enabled” and click “OK”.



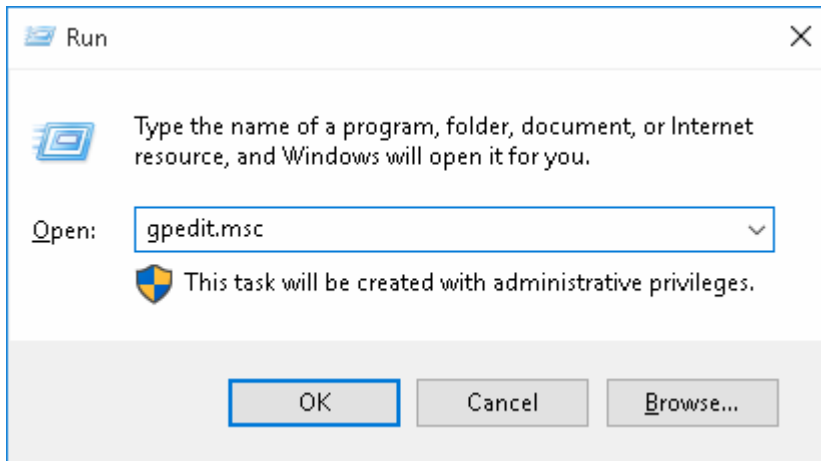
**Figure 5-44 Turn off Microsoft Defender Antivirus interface**

### 5.7.7 System Anti Virus Settings

#### 1. Turn off Autoplay

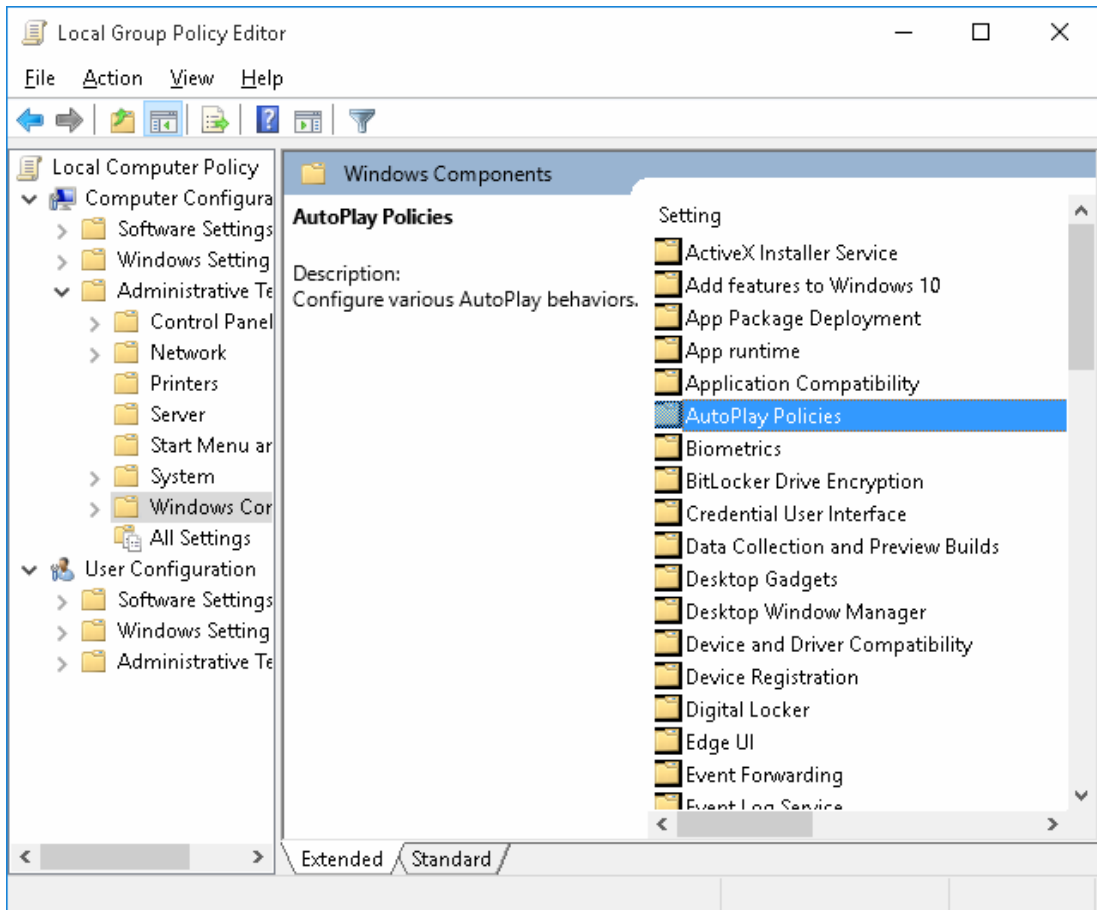
In order to prevent the computer from attacking by the virus carried in mobile storage devices and endangering the DCS supervision software, it is necessary to enable “Turn off Autoplay” function.

1. Open “Run” interface by shortcut key “Windows + R”, then type command “gpedit.msc” in Run dialog box, as shown in Figure 5-45.



**Figure 5-45 Run dialog box**

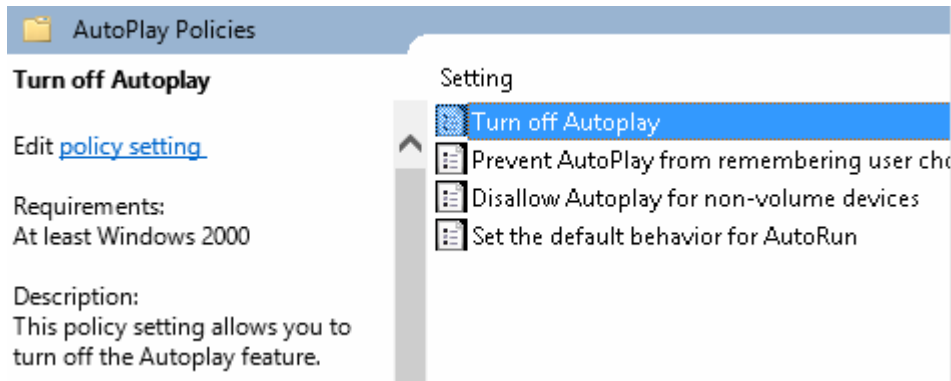
2. Click “OK” to pop up the “Local Group Policy Editor” interface, extend “Computer Configuration”, select “Windows Components” below “Administrative Templates”, as shown in Figure 5-46.



**Figure 5-46 “Windows Components” window**

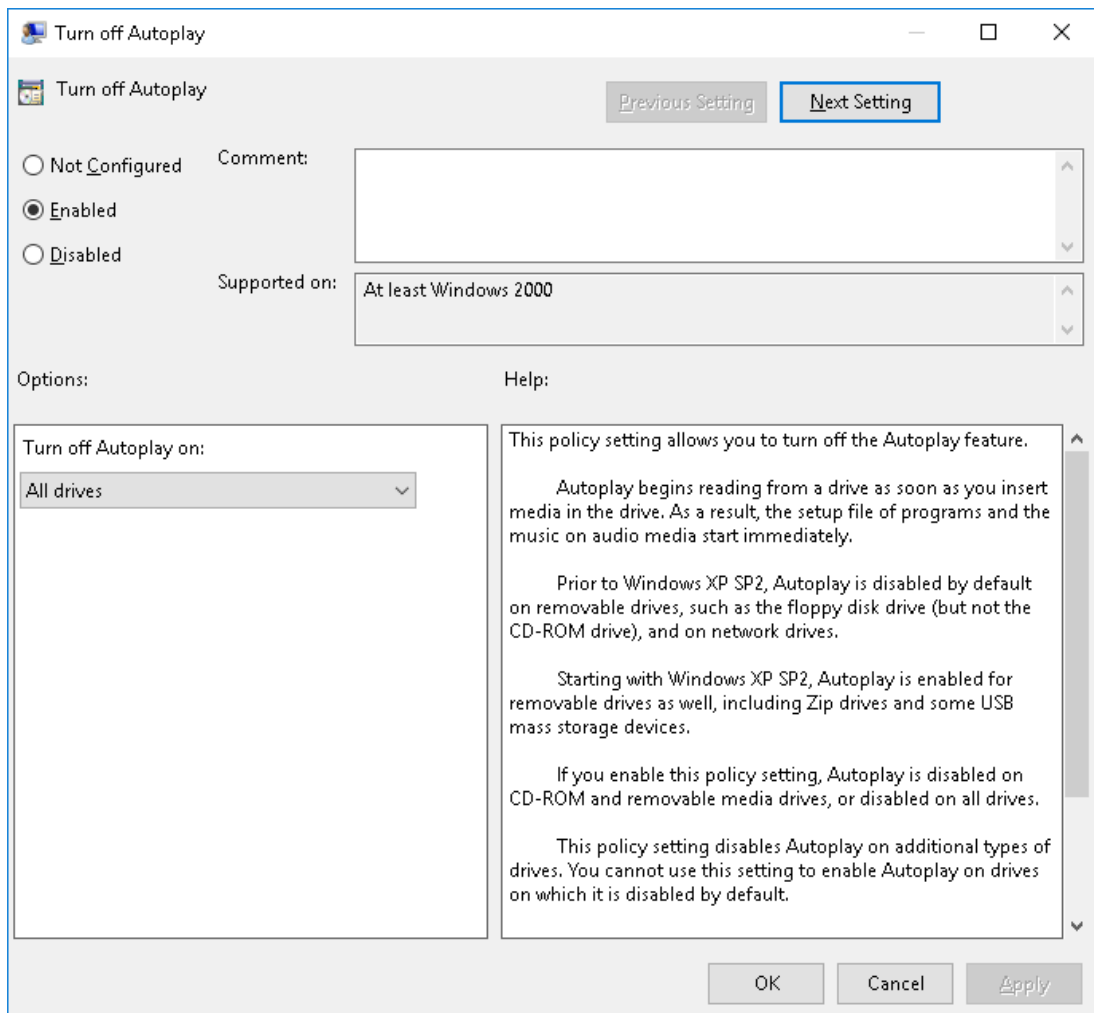
3. Double click “AutoPlay Policies”, pop up the following interface.





**Figure 5-47 Close “AutoPlay Policies”**

4. Double click “Turn off Autoplay” in “AutoPlay Policies” window, pop up “Turn off Autoplay” interface, select “Enabled” and choose “All drives” in the drop-down menu of the “Turn off Autoplay on”, as shown in Figure 5-48.



**Figure 5-48 “Turn off Autoplay” settings**

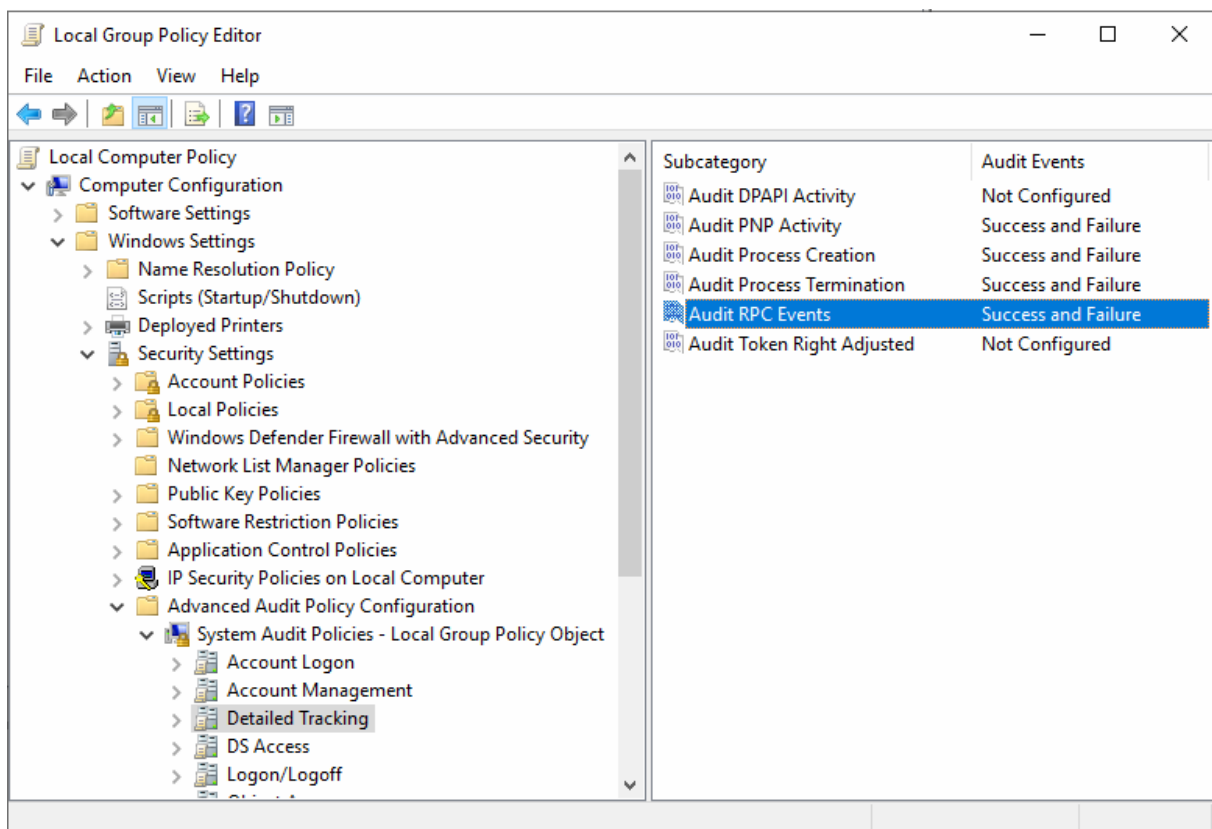
5. Click “OK” to finish the settings. Restart your computer, then the mobile storage devices will not automatically play when be inserted.

## 2. Enabling Security Audit Policy

To facilitate efficient tracking of the virus source, it is necessary to enable the security audit policy. The specific steps are as follows:

1. In the "Local Group Policy Editor" interface shown in Figure 5-46, select "Local Computer Policy/Computer Configuration/Windows Settings/Security Settings/Advanced Audit Policy Configuration/System Audit Policies - Local Group Policy Object/Detailed Tracking" to enter the configuration interface.
2. Double-click "Audit Process Creation", check "Configure the following audit events" in the pop-up dialog box, and select "Success" and "Failure".
3. Repeat the operation of step 2, and configure "Audit PNP Activity", "Audit Process Termination", and "Audit RPC Events" respectively.

The configuration results are shown in Figure 5-49.



**Figure 5-49 Security Audit Policy settings**

## 5.8 Background Service Settings

Set the following services to "Disabled". This chapter takes windows update as an example to illustrate.

- Internet Connection Sharing (ICS)
- Remote Desktop Services
- Windows Update
- Windows Time
- Windows Defender Firewall
- Touch Keyboard and Handwriting Panel Service

## Disable Windows Update

1. Select [Start\ Windows Administrative Tools\ Service] to pop up the interface of background service configuration, as shown in Figure 5-50.

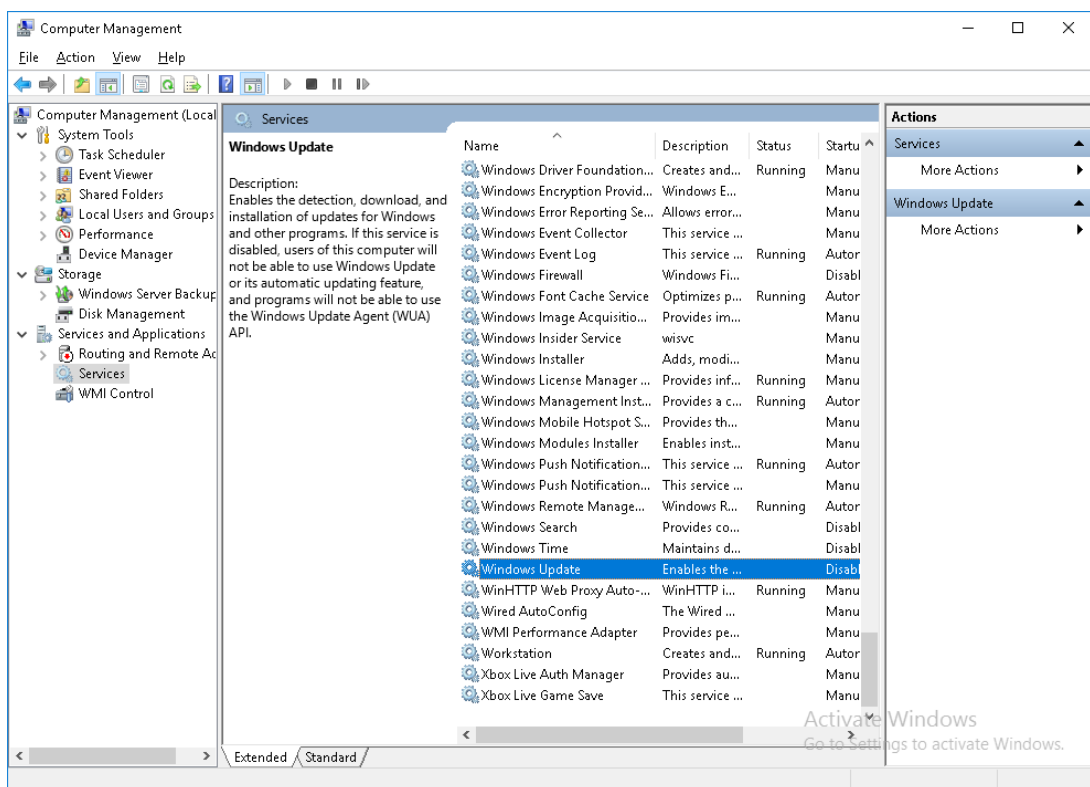
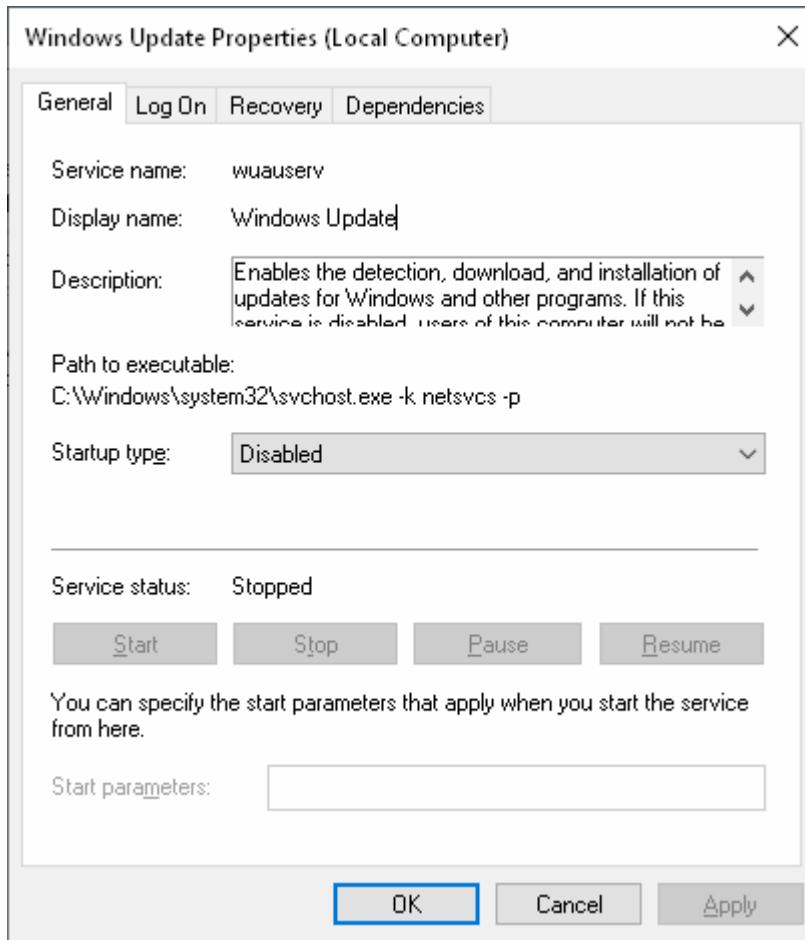


Figure 5-50 Services list window

2. Double-click "Windows Update" in the services list, pop up the corresponding properties setting interface, select "Disabled" in the pull-down list of "Startup type", as shown in Figure 5-51.



**Figure 5-51 Disable the service of “Windows Update”**

3. Click “Stop” to stop this service, then click “OK” to disable this service.

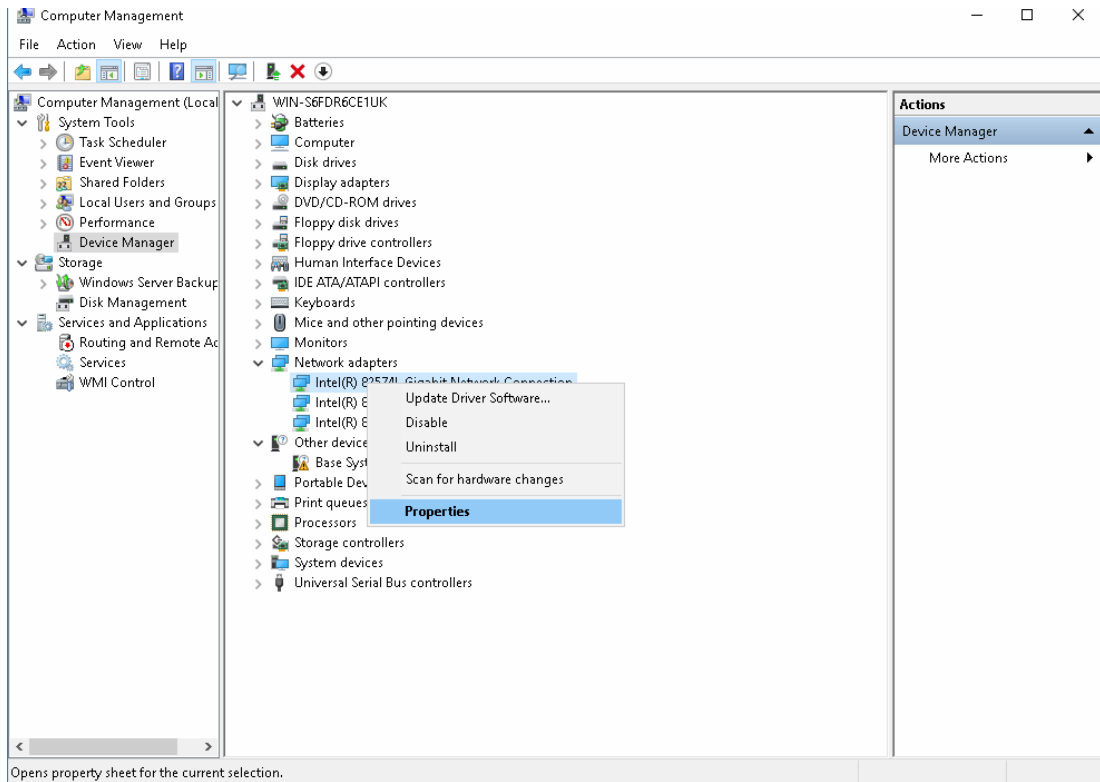


**Warning:**

All network connections on the operation nodes should be disabled after setting background services.

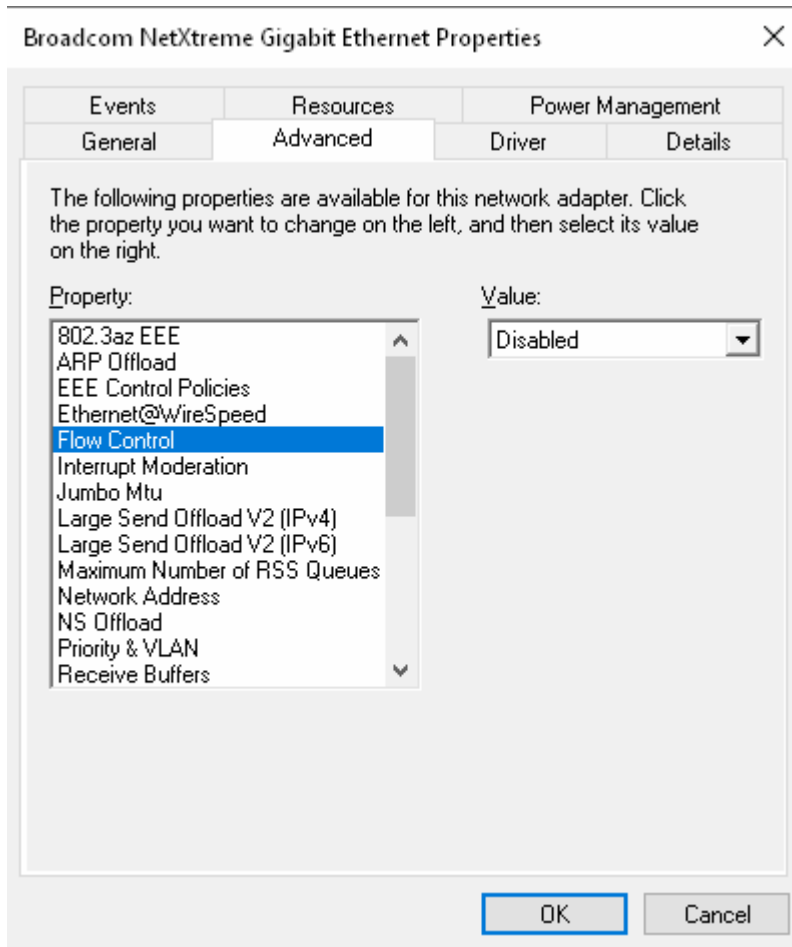
## 5.9 Turn off Flow Control of Network Adapter

1. Select [Start\ Windows Administrative Tools\ Computer Management], select Device Manager in left structure tree, as shown in Figure 5-52.



**Figure 5-52 Device Management interface**

2. Right click a network adapter in device manager window, select “Properties” in right-click menu to open its properties interface and select “Advanced” tab, as shown in Figure 5-53.



**Figure 5-53** Disable flow control of network adapter

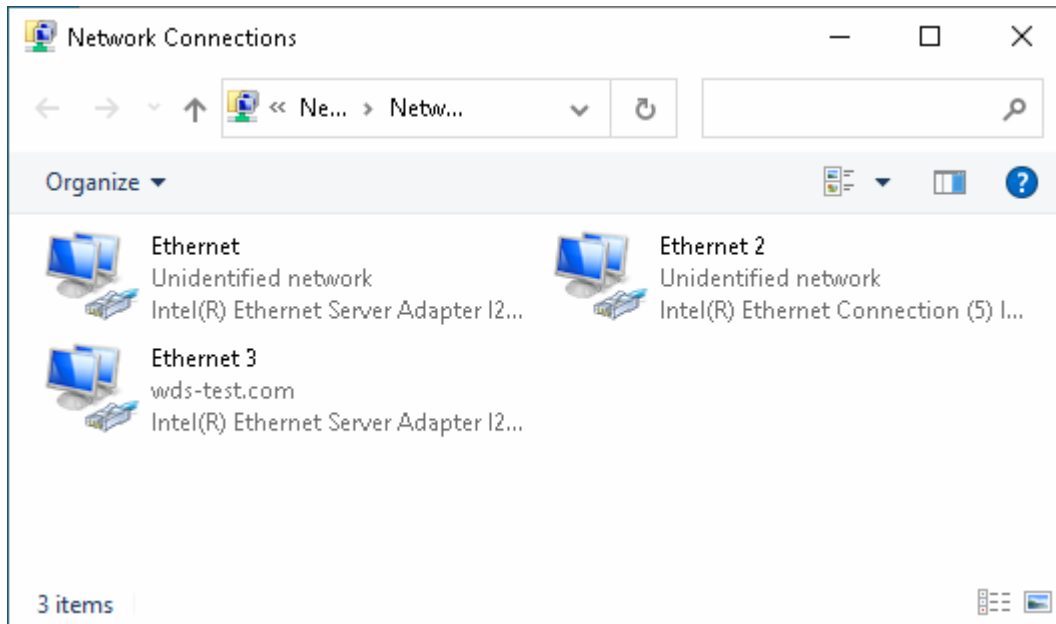
3. Set "Flow Control" to "Disable" in "Advanced" option page in properties interface and click "OK" to finish a network adapter setting.
4. Set other network adapters like this.

## 5.10 Network Properties Settings

Set the Network Connections Settings as follows after finishing the network hardware connections settings, this chapter includes connection properties settings and advanced sharing settings.

### 5.10.1 Network Properties Configuration

Select [Control Panel/Network and Internet/Network and Sharing Center], then click "Change adapter settings", pop up network connection settings interface.



**Figure 5-54 Network connections setting interface**

The “Local Connection” as shown in above figure utilizes integrated network adapter of the system, and “Local Connection 2” and “Local Connection 3” utilize the two network adapters inserted.

1. If VisualField is installed in the control system, the properties of network adapters should be set as follows:
  - 1) Change the “Local Connection 2” to “Network A” that is to connect process control network-A. Properties setting of “Network A” is as follows:
    - IP address: 172.20.X.Y (X indicates the domain address; Y indicates the station address. Both of them should be in the value range of operation node addresses.)
    - Subnet mask: 255.255.0.0
    - Other items such as DNS, WINS etc shall remain default.
  - 2) Change the “Local Connection 3” to “Network B” that is to connect process control network-B. Properties setting of “Network B” is as follows:
    - IP address: 172.21.X.Y (X indicates the domain address; Y indicates the station address. Both of them should be in the value range of operation node addresses.)
    - Subnet mask: 255.255.0.0
    - Other items such as DNS, WINS etc shall remain default.
  - 3) Change the “Local Connection” to “Information Network” that is to connect information network, Properties setting of “Information Network” is as follows:
    - IP address: 172.30. X.Y (X indicates the domain address; Y indicates the station address. Both of them should be in the value range of operation node addresses.)
    - Subnet mask: 255.255.0.0

- Other items such as DNS, WINS and etc shall remain default.
2. If AdvanTrol-Pro is installed in the control system, the properties of network adapter should be set as follows:
    - 1) Change the “Local Connection 2” to “Network A”, that is to connect process control network- A, Properties setting of “Network A” is as follows:
      - IP address: 128.128.1.X (X is should be in the value range of operation node addresses.)
      - Subnet mask: 255.255.255.0
      - Other items such as DNS, WINS etc shall remain default.
    - 2) Change the “Local Connection 3” to “Network B”, that is to connect process control network-B, Properties setting of “Network B” is as follows :
      - IP address: 128.128.2. X ((X should be in the value range of operation node addresses.)
      - Subnet mask: 255.255.255.0
      - Other items such as DNS, WINS and etc shall remain default.
    - 3) Change the “Local Connection” to “Operation Network”, that is to connect with operation network, Properties setting of “Operation Network” is as follows:
      - IP address: 128.128.5. X (X should be in the value range of operation node addresses.)
      - Subnet mask: 255.255.255.0
      - Other items such as DNS, WINS etc shall remain default.

Check whether the network adapter functions well or not after setting.



---

**Attention:**

**Please refer to the related User Manual for Network Properties Settings.**

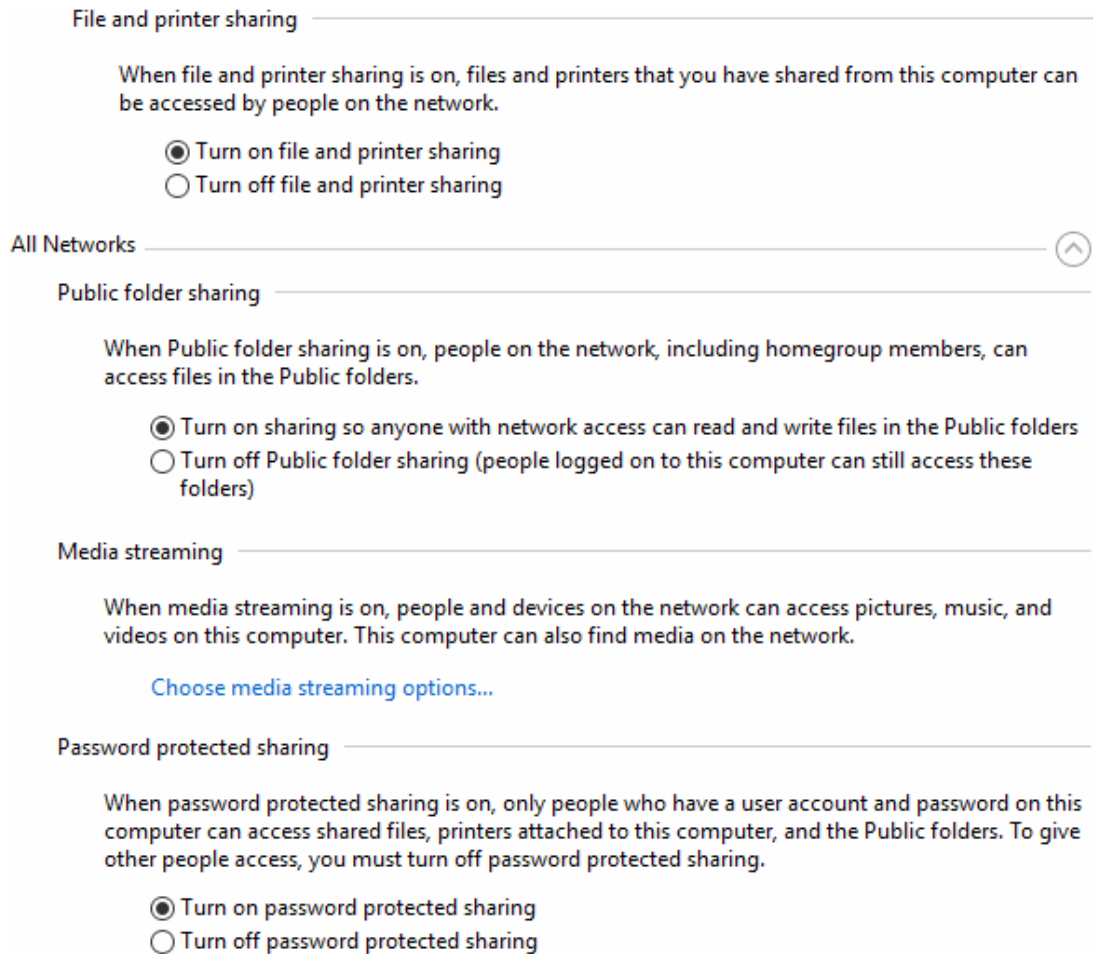
---

### 5.10.2 Advanced Sharing Settings

After finishing network hardware connection, network connection should be set by following steps.

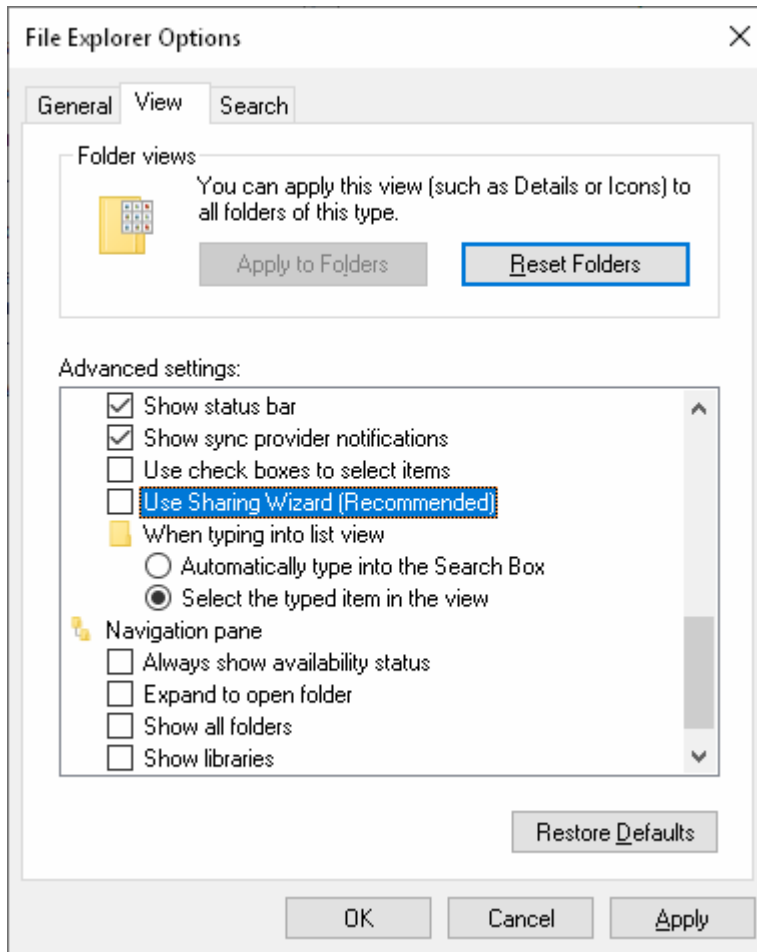
1. Select [Control Panel/Network and Internet/Network and Sharing Center], then click “Change advanced sharing settings”, pop up “Advanced sharing settings” interface. Turn on “File and printer sharing”, “Public folder sharing” and “Password Protected Sharing”, as shown in Figure 5-55. Other settings are in default.





**Figure 5-55 Advanced sharing settings**

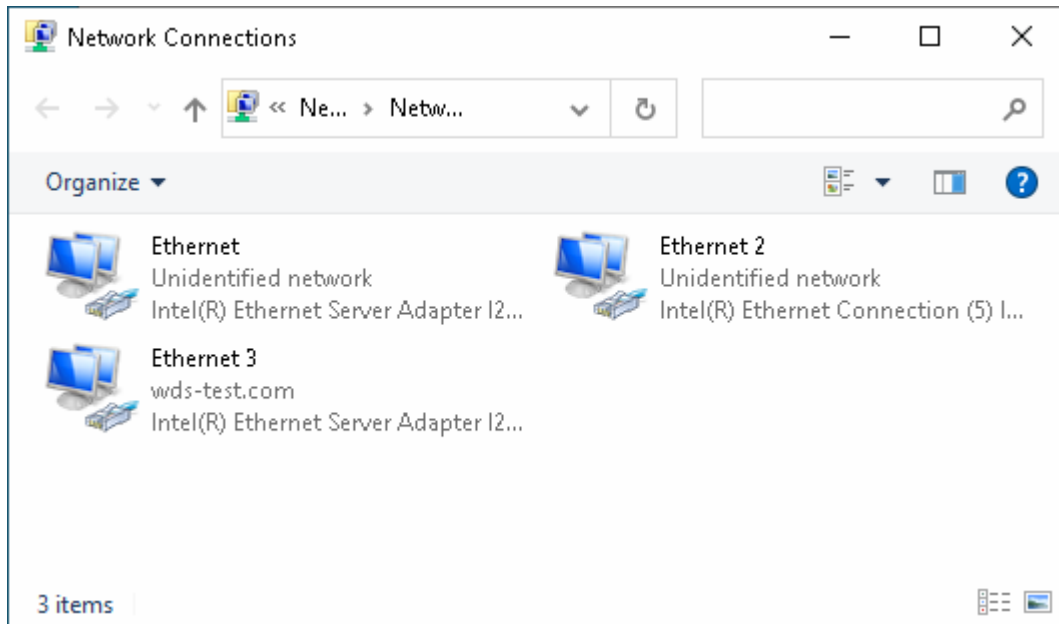
2. Select [Start\Control Panel\ Appearance and Personalization\ File Explorer Option], deselect "Use Sharing Wizard (Recommended)" in pop-up interface, as shown in Figure 5-56.



**Figure 5-56 Folder options setting interface**

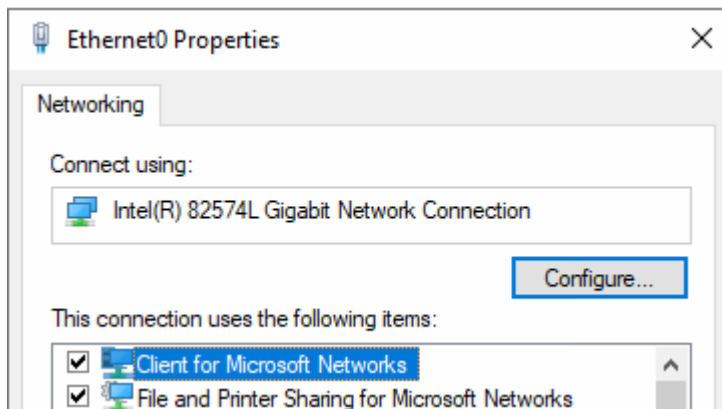
### 5.10.3 Network Power Management Configuration

1. Select [Control Panel/Network and Internet/Network and Sharing Center], then click “Change adapter settings”, the network connection settings interface pops up.



**Figure 5-57 Network connections setting interface**

2. Right-click an adapter and select "Properties" in the right-click menu to pop up the properties interface, as shown below.



**Figure 5-58 Properties of network connections**

3. Click "Configure" button in the Networking tab to pop up the properties interface of network adapter. Then, select the "Power Management" tab and unselect the item "Allow the computer to turn off this device to save power".



**Figure 5-59 Properties of network adapter**



---

**Tips:**

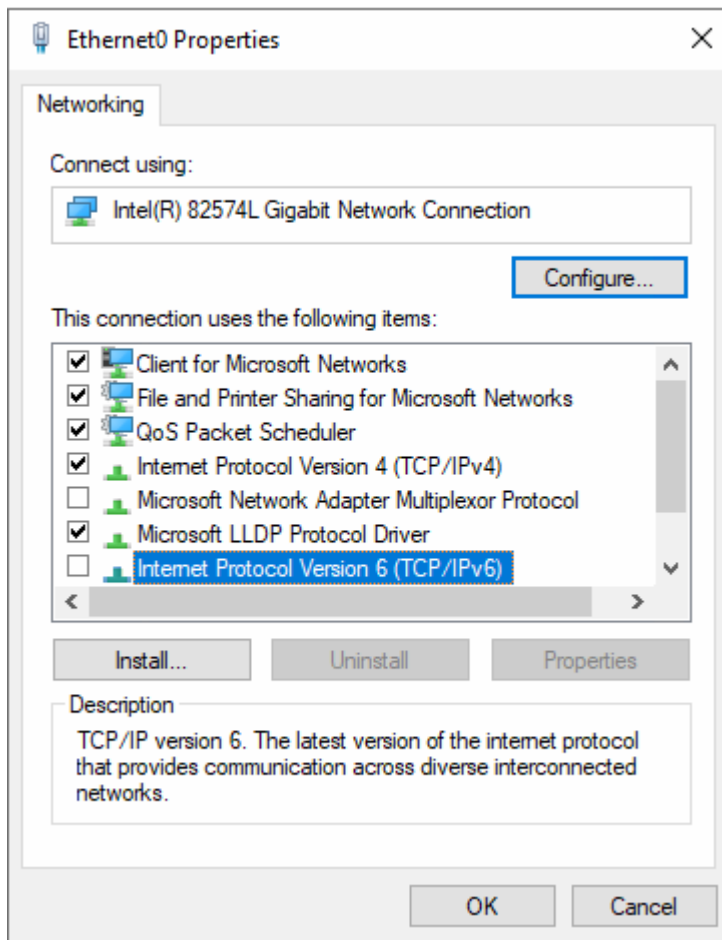
By following steps, you can also open the setting interface of network adapter properties: (The interfaces opened in the two ways may not be exactly the same, please refer to the actual interface.)

1. Right-click on the "Computer" icon on the desktop and select "Manage" in the right-click menu.
  2. In the "Computer Management" window, select "Device Manager" from the left tree-list under "Computer Management/System Tools".
  3. Select a network adapter from the list of hardware devices on the right-hand side, and select "Properties" in the right-click menu.
- 

4. Save the changes of settings.
5. Repeat the steps above to change the corresponding properties of each network adapter.

#### **5.10.4 Disable IPv6**

1. Select [Control Panel\Network and Internet\Network and Sharing Center\Change adapter settings] to open the setting interface of network connection, as shown in Figure 5-57.
2. Right click a adapter and select "Property" in the right-click menu to open the property interface of network connection, as shown in Figure 5-60, unselect the item "Internet Protocol Version 6 (TCP/IPv6)".



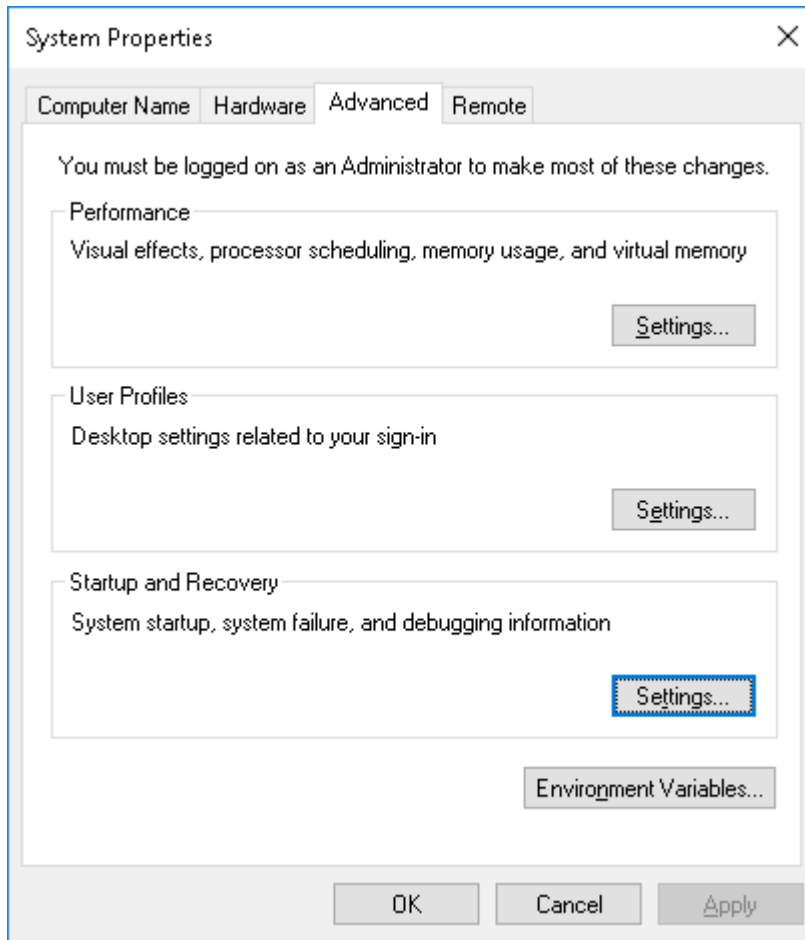
**Figure 5-60 Network connection properties**

3. Click OK to save the setting.
4. Repeat the steps above to change the property of each adapter.

## 5.11 Startup and Recovery Settings

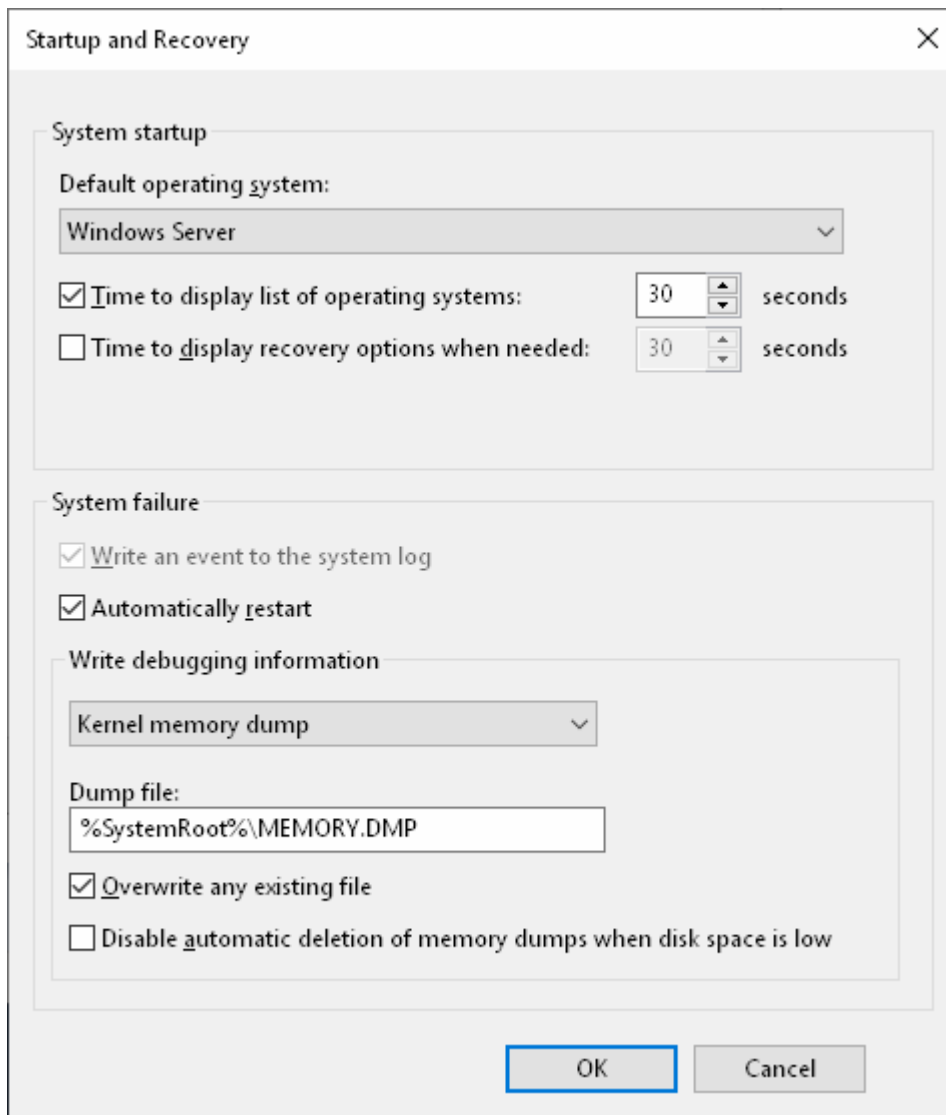
In order to save full information about abnormal situation immediately when the Windows operating system appears blue screen in the application process, write debugging information mode of Startup and Recovery setting should be selected as “Kernel memory dump” in the settings of System Properties. The detailed operating steps are shown below:

1. Open “Run” interface by shortcut key “Windows + R”, then type command “systempropertiesadvanced.exe” to pop up “User Properties” dialog box and switch to the tab Advanced, as shown in Figure 5-61.



**Figure 5-61 Advanced system property settings**

2. Click the button "Settings" in "Startup and Recovery" window to pop up the interface as shown in Figure 5-62, then select "Kernel memory dump" from the drop-down list of "Write debugging information" window below "System failure".



**Figure 5-62** Setting interface of *Startup and Recovery*

3. After setting, click “OK”.

## Section 6 Checklist

After Windows Server 2022 has been installed completely, you can check each of the proprieties settings according to the items in the following table.

**Table 6-1 Check list**

Setting items		Setting result	Notes
Driver programs	Main broad driver and integrated components drivers	All of them has been installed	-
	Drivers for other components		-
User accounts	Change password policy	Turn off the complexity requirements of password	-
	Enable Administrator account settings	The password of administrator account never expires	-
	Set automatic logon		-
Display properties	Theme setting	Default theme Windows	-
	Desktop icons	Computer, Network and Recycle Bin	-
	Screen saver setting	None	-
	Screen resolution	19" monitor: 1280 × 1024 pixels(recommended) 20" monitor: 1600 × 1200 pixels(recommended) 22" widescreen monitor: 1920 × 1080 pixels(recommended) 24" widescreen monitor: 1920 × 1080 pixels (recommended)	-
	ClearType Text Tuner	Turn off ClearType	-
	Aero Shake window minimizing mouse gesture	Turn off	-
StickyKeys and ToggleKeys	Keyboard Shortcut	Turn off	-
Taskbar and start menu properties setting	Taskbar appearance	Select: Lock the taskbar	-
Time Settings	Time	Short time: HH:mm Long time: HH:mm:ss	-
	Data	Short data: M/d/yyyy Long data: dddd, MMMM d, yyyy	
System and Security	Power plan	High performance	
	Turn off the display	Never	
	Put the computer to sleep	Never	Skip this item if there is no such setting.
	Power Options – Advanced settings	High performance	-
	Allow wake timers	Enable	-



Setting items		Setting result	Notes
	Windows Defender Firewall	Turn off	-
	User Accounts Control Settings	Never	-
	User Accounts Control: Run all administrators in Admin Approval Mode	Disabled	-
	Visual effects	Adjust for best performance	-
	Virtual memory	Set sizes of Initial size and Maximum size both as 3000MB (4000MB when the RAM is larger than 2GB)	-
	Data Execution Prevention	Turn on DEP for essential Windows programs and services only	
	Auto-update	Never check for updates	-
	Microsoft Defender Antivirus	Turn off	-
	Turn off Autoplay	Enabled	-
	Security Audit Policy Settings: Audit PNP Activity, Audit Process Creation, Audit Process Termination, Audit RPC Events	Enable these subcategories and set their audit events as "Success" and "Failure"	-
Service	Windows Update	Disabled	-
	Internet Connection Sharing		-
	Remote Desktop Services		-
	Windows Defender Firewall		-
	Windows time		-
	Touch Keyboard and Handwriting Panel Service		-
Network properties setting	Flow Control	Disabled	-
	Local Connection	Rename: Information Network IP: 172.30.X.Y	Fit for VisualField software packets
		Rename: Operation Network IP: 128.128.5.X	Fit for AdvanTrol-Pro software packets
	Local Connection 2	Rename: Network A IP: 172.20.X.Y	Fit for VisualField software packets
		Rename: Network A IP: 128.128.1.X	Fit for AdvanTrol-Pro software packets
	Local Connection 3	Rename: Network B IP: 172.21.X.Y	Fit for VisualField software packets
		Rename: Network B IP: 128.128.2.X	Fit for AdvanTrol-Pro software packets
Network Properties Settings	Advanced Sharing Settings	Turn on "File and printer sharing", "Public folder sharing" and "Password Protected Sharing",	-
	File Explorer Option	Unselect "Use Sharing Wizard (Recommended)"	
Network Adapter Property	Power Management	Unselect "Allow the computer to turn off this device to save power"	-

Setting items		Setting result	Notes
	Network Property	Unselect "Internet Protocol Version 6 (TCP/IPv6)"	-
Startup and Recovery	Write debugging information	Select "Kernel memory dump"	-

## Section 7 Revision

---

*Table 7-1 Retrofit list of the version*

Document Version	Applicable Product Version	Remarks
V1.0 (20230619)	Windows Server 2022 Standard (64-bit)	The first version