Lab Assignment & Solution

Cybersecurity Professional Program

Microsoft Security

Group Policy

MS-05-L1
Basic GPO Configuration

Lab Objective

Learn to secure an environment by applying basic policies to users using GPOs.

Lab Mission

Configure group policy objects to secure client machines and prevent unauthorized users from making changes.

Lab Duration

20–40 minutes

Requirements

- Knowledge of the ADUC structure
- Familiarity with the Windows Server environment

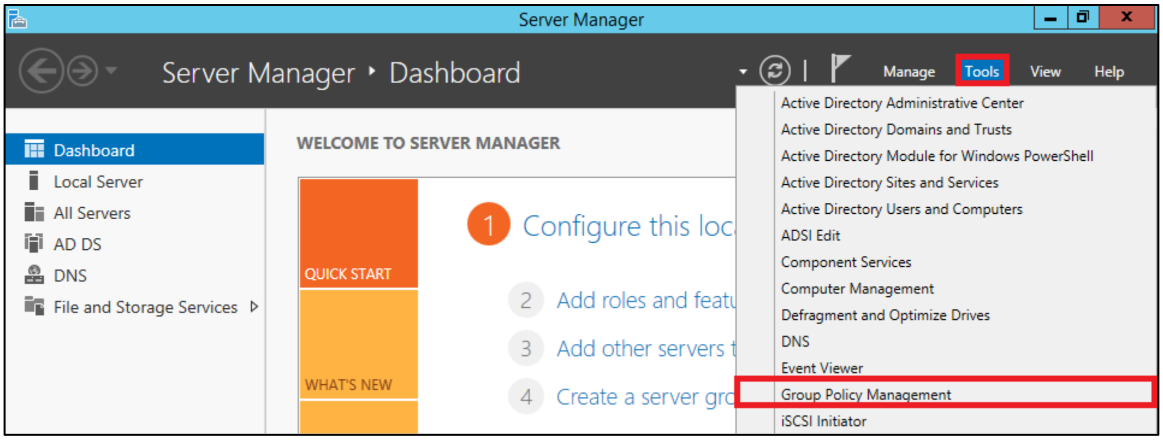
Resources

- Environment & Tools
  - VirtualBox
    - Windows Server 2016
    - Windows 10

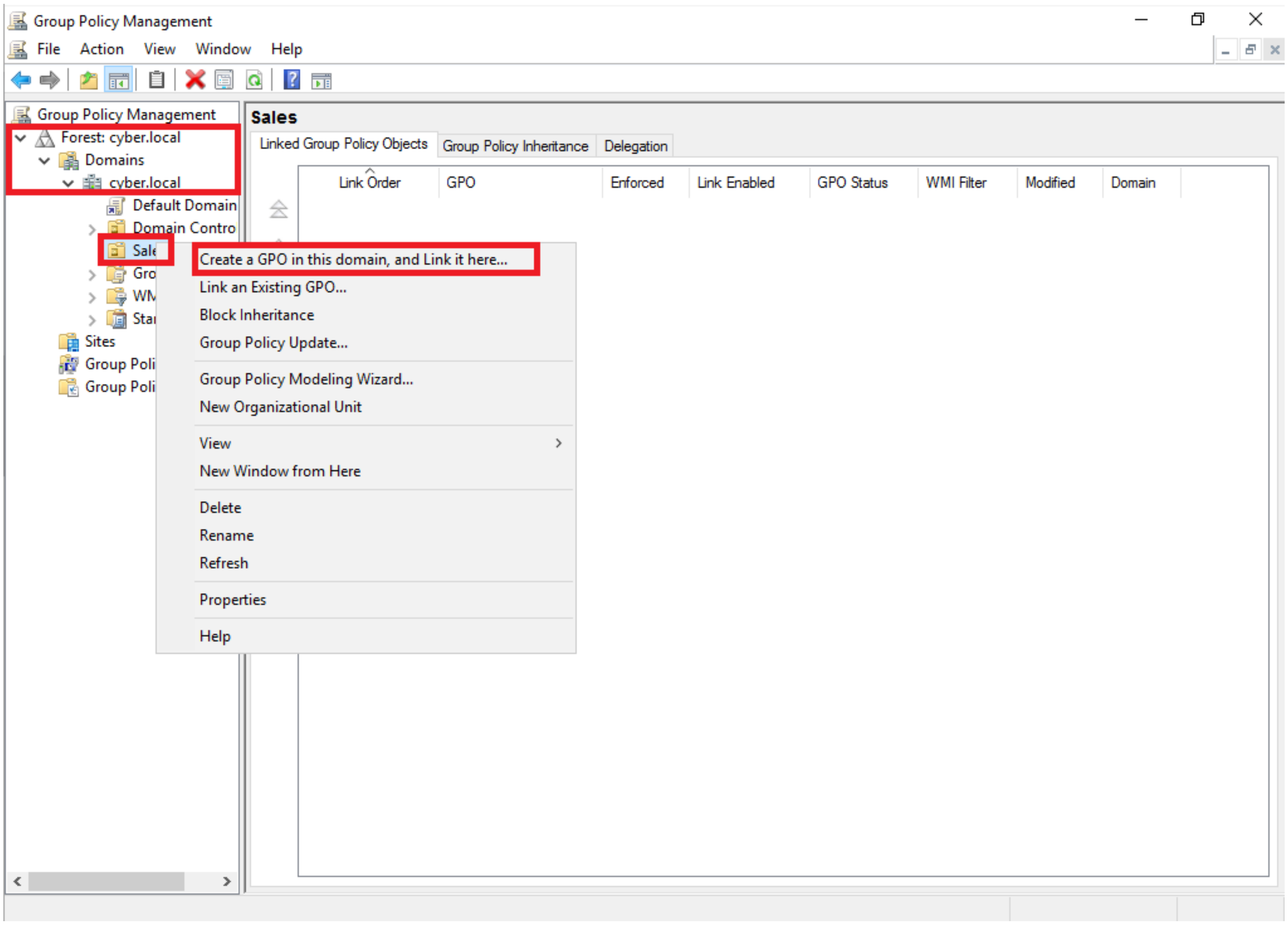
Lab Task 1: Create Organization Units & Group Policy Objects

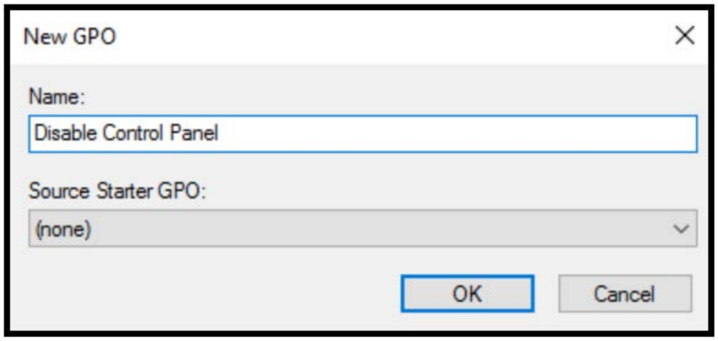
Practice Group Policy configuration on the domain controller via Group Policy Management by creating four new GPOs.

1 Access the **Group Policy Management Console (GPMC)** by clicking the **Tools** tab and selecting ***Group Policy Management***.


Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
1 Configure this loc
2 Add roles and featu
3 Add other servers t
4 Create a server gro
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DNS
Event Viewer
Group Policy Management
iSCSI Initiator

2 Expand ***Forest: cyber.local*** > ***Domains*** > ***cyber.local*** and right-click ***Sales OU***. Select ***Create a GPO in this domain, and Link it here...*** Name the new GPO **Disable Control Panel**.

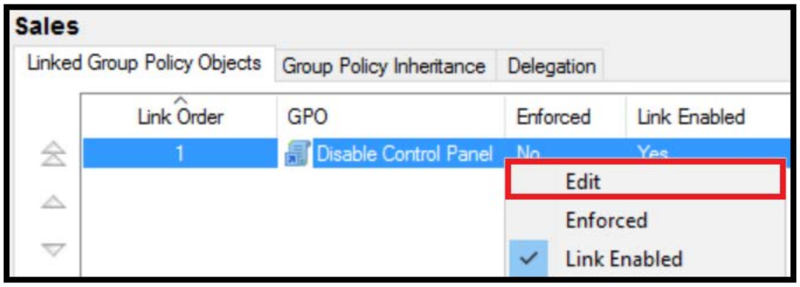




Name: Disable Control Panel

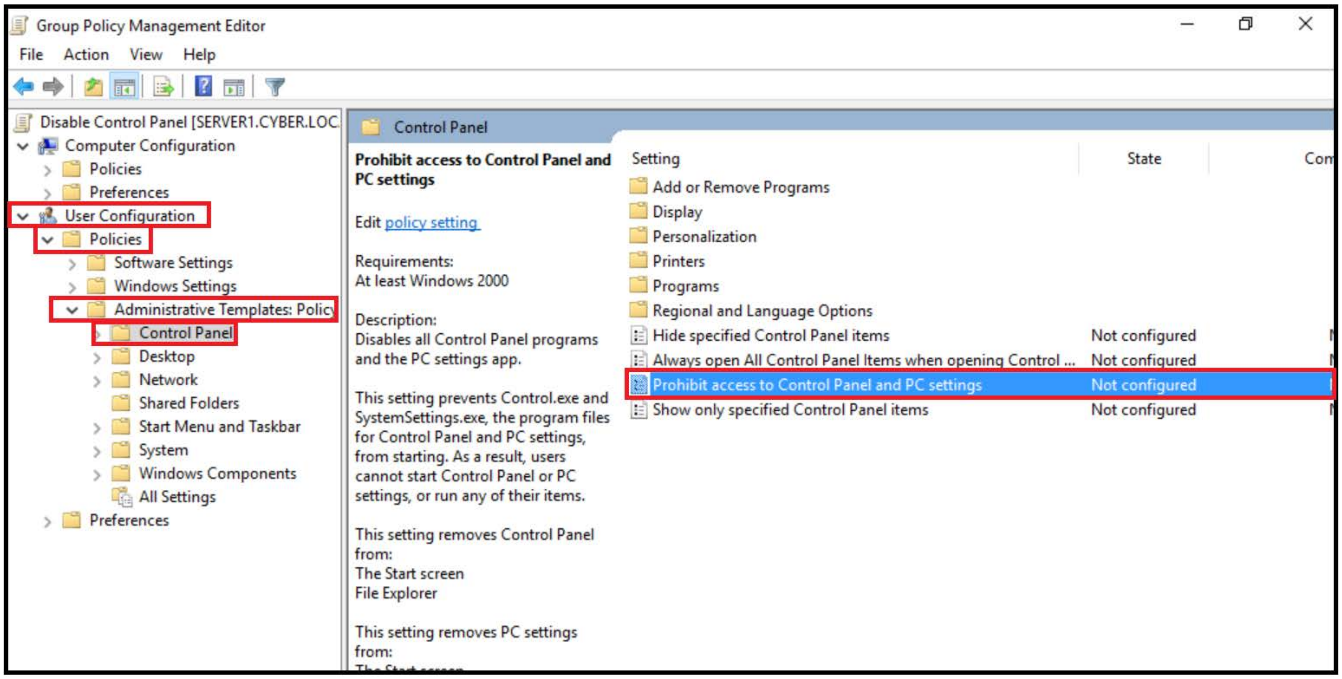
Source Starter GPO: (none)

3 Right-click the GPO and click ***Edit.***



Link Order	GPO	Enforced	Link Enabled
1	Disable Control Panel	No	Yes

4 In the **Group Policy Management Editor** window, in the left pane, navigate to ***User Configuration*** > ***Policies*** > ***Administrative Templates*** > ***Control Panel*** and click it. On the right side of the screen, right-click ***Prohibit access to Control Panel and PC settings*** and choose ***Edit***.



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.

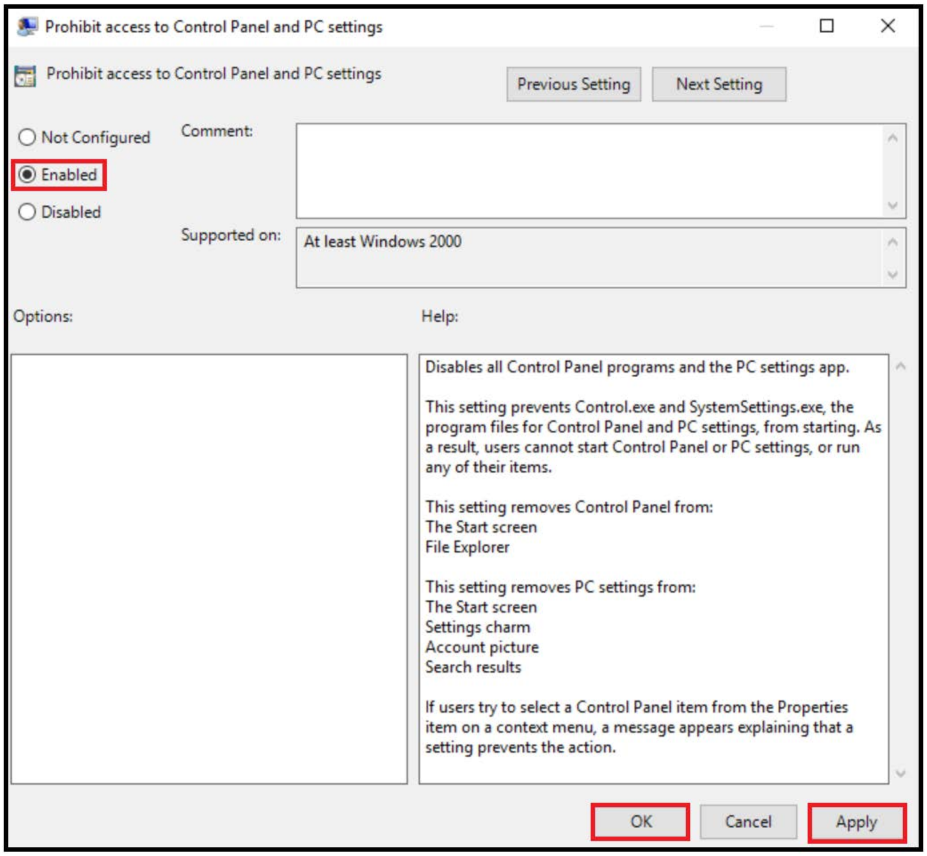
This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.

This setting removes Control Panel from:
The Start screen
File Explorer

This setting removes PC settings from:

Setting	State	Com
Add or Remove Programs		
Display		
Personalization		
Printers		
Programs		
Regional and Language Options		
Hide specified Control Panel items	Not configured	
Always open All Control Panel Items when opening Control ...	Not configured	
Prohibit access to Control Panel and PC settings	Not configured	
Show only specified Control Panel items	Not configured	

5 On the next window, select ***Enabled*** and click **Apply,** then **OK**.



Prohibit access to Control Panel and PC settings

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 2000

Options:

Help:

Disables all Control Panel programs and the PC settings app.

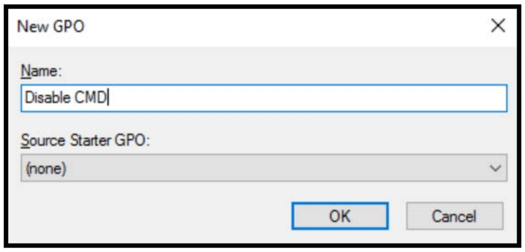
This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.

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.

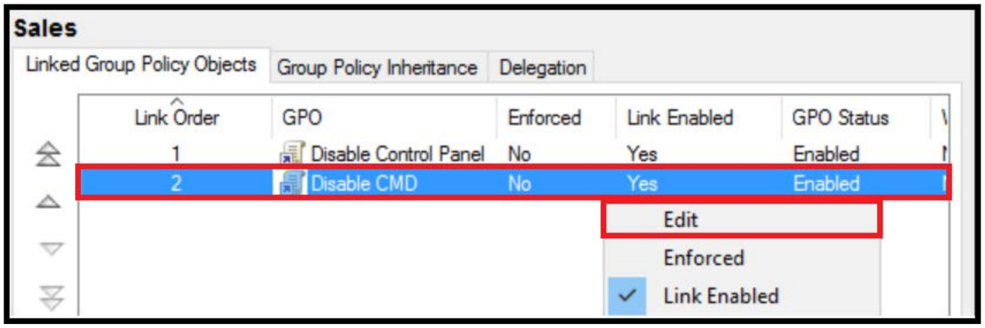
6 Exit the window and create another GPO under **Sales OU** called **Disable CMD**. Once created, right-click the new GPO and choose ***Edit***.



New GPO

Name: Disable CMD

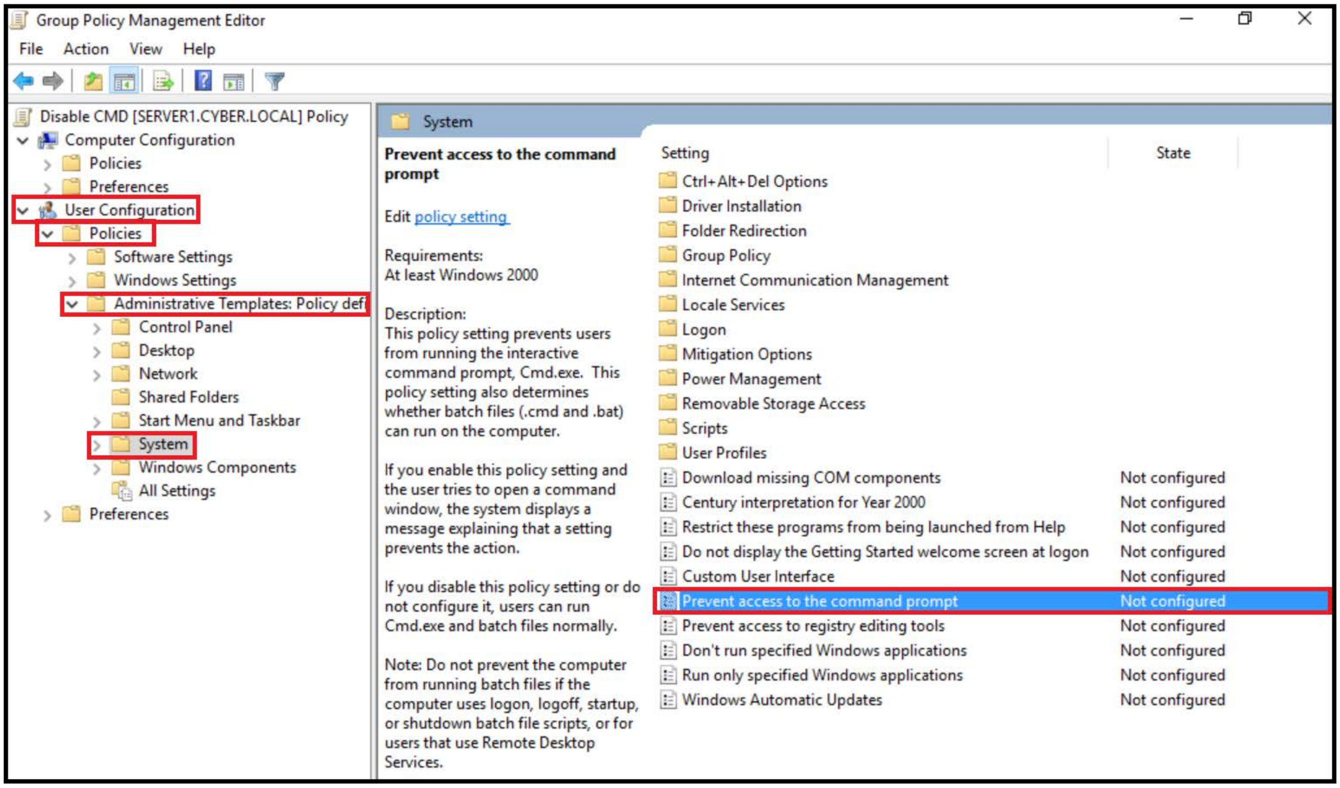
Source Starter GPO: (none)



Sales

Link Order	GPO	Enforced	Link Enabled	GPO Status
1	Disable Control Panel	No	Yes	Enabled
2	Disable CMD	No	Yes	Enabled

7 Navigate to ***User Configuration*** > ***Policies*** > ***Administrative Templates*** > ***System*** and click it. On the right side, right-click ***Prevent access to the command prompt*** and choose ***Edit***.



Prevent access to the command prompt

Edit policy setting

Requirements:
At least Windows 2000

Description:
This policy setting prevents users from running the interactive command prompt, Cmd.exe. This policy setting also determines whether batch files (.cmd and .bat) can run on the computer.

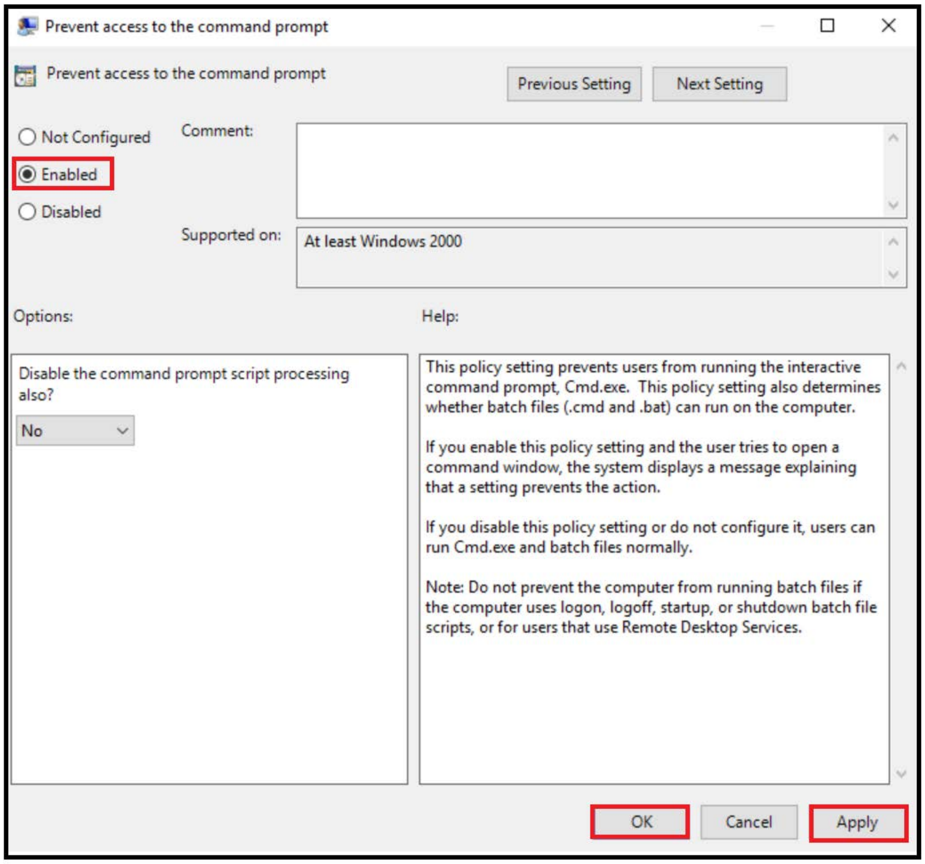
If you enable this policy setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.

If you disable this policy setting or do not configure it, users can run Cmd.exe and batch files normally.

Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Remote Desktop Services.

Setting	State
Ctrl+Alt+Del Options	
Driver Installation	
Folder Redirection	
Group Policy	
Internet Communication Management	
Locale Services	
Logon	
Mitigation Options	
Power Management	
Removable Storage Access	
Scripts	
User Profiles	
Download missing COM components	Not configured
Century interpretation for Year 2000	Not configured
Restrict these programs from being launched from Help	Not configured
Do not display the Getting Started welcome screen at logon	Not configured
Custom User Interface	Not configured
Prevent access to the command prompt	Not configured
Prevent access to registry editing tools	Not configured
Don't run specified Windows applications	Not configured
Run only specified Windows applications	Not configured
Windows Automatic Updates	Not configured

8 On the next window, check ***Enabled*** and click **Apply,** then **OK**.



Prevent access to the command prompt

Prevent access to the command prompt

○ Not Configured

● Enabled

○ Disabled

Comment:

Supported on: At least Windows 2000

Options:

Disable the command prompt script processing also?

No

Help:

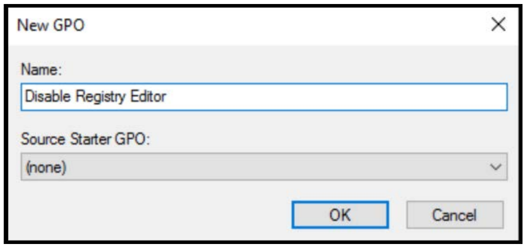
This policy setting prevents users from running the interactive command prompt, Cmd.exe. This policy setting also determines whether batch files (.cmd and .bat) can run on the computer.

If you enable this policy setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.

If you disable this policy setting or do not configure it, users can run Cmd.exe and batch files normally.

Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Remote Desktop Services.

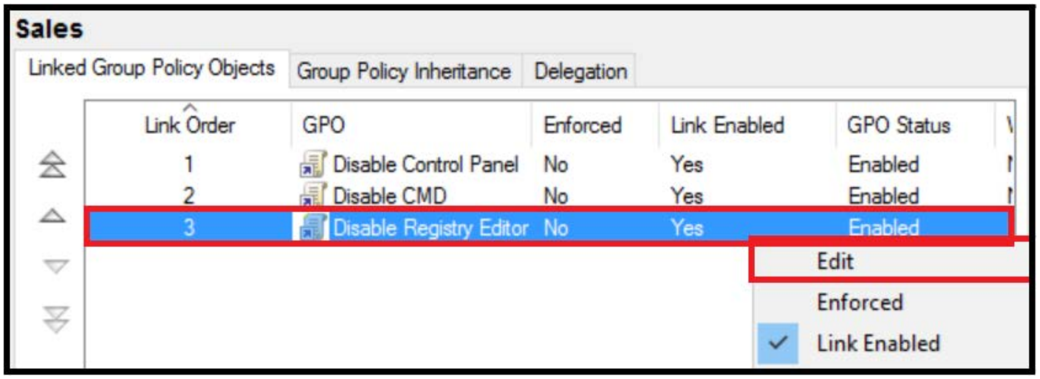
9 Exit the window and create another GPO under **Sales OU** called **Disable Registry Editor**. Once created, right-click the new GPO and choose ***Edit***.



New GPO

Name: Disable Registry Editor

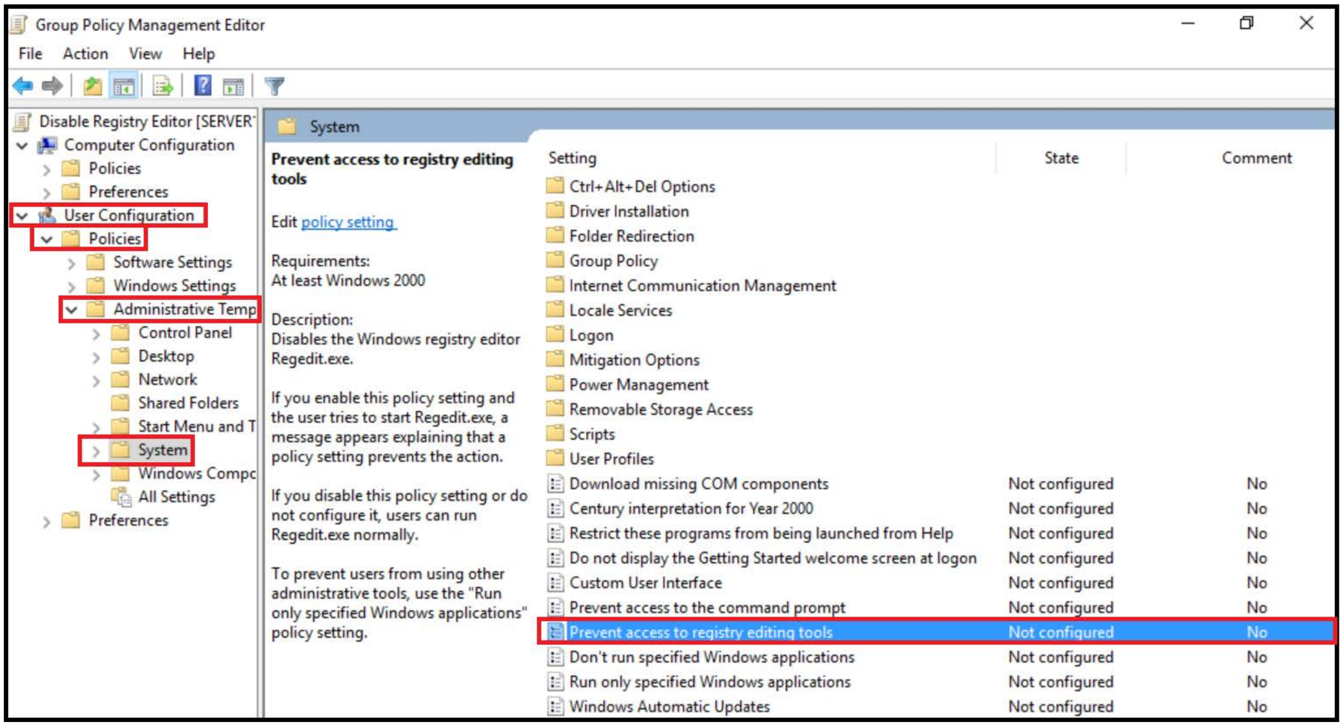
Source Starter GPO: (none)



Sales

Link Order	GPO	Enforced	Link Enabled	GPO Status
1	Disable Control Panel	No	Yes	Enabled
2	Disable CMD	No	Yes	Enabled
3	Disable Registry Editor	No	Yes	Enabled

10 Navigate to ***User Configuration*** > ***Policies*** > ***Administrative Templates*** > ***System*** and click it. On the right side, right-click ***Prevent access to registry editing tools*** and choose ***Edit***.



Prevent access to registry editing tools

Edit policy setting

Requirements:
At least Windows 2000

Description:
Disables the Windows registry editor Regedit.exe.

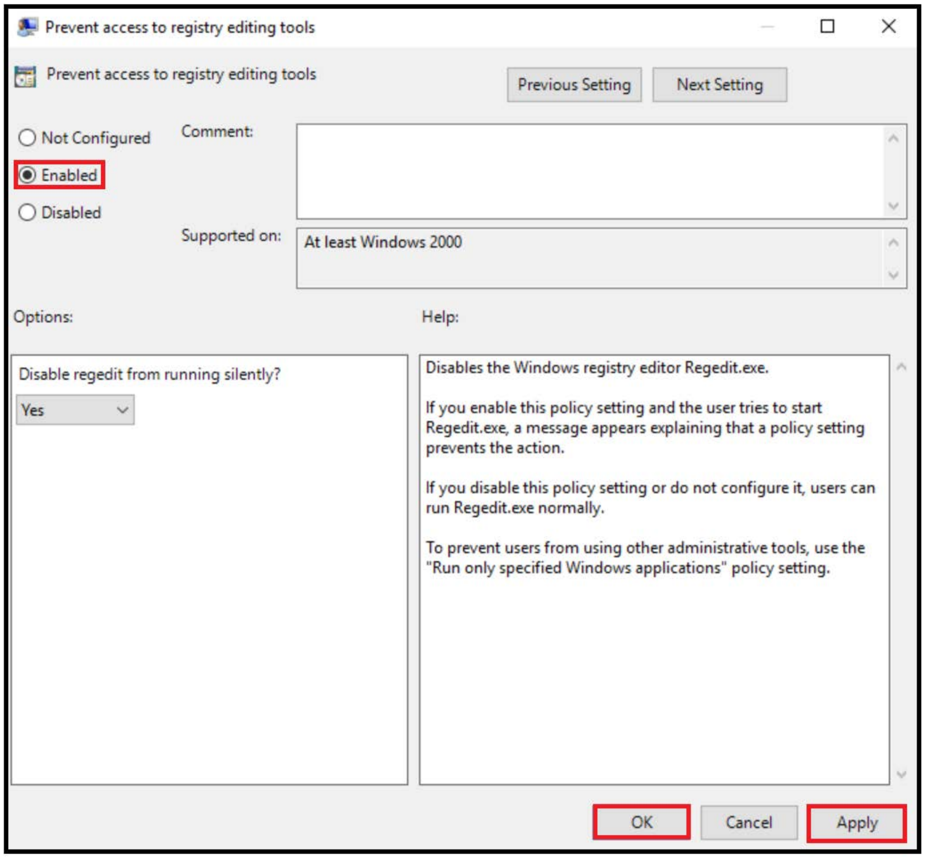
If you enable this policy setting and the user tries to start Regedit.exe, a message appears explaining that a policy setting prevents the action.

If you disable this policy setting or do not configure it, users can run Regedit.exe normally.

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

Setting	State	Comment
Ctrl+Alt+Del Options		
Driver Installation		
Folder Redirection		
Group Policy		
Internet Communication Management		
Locale Services		
Logon		
Mitigation Options		
Power Management		
Removable Storage Access		
Scripts		
User Profiles		
Download missing COM components	Not configured	No
Century interpretation for Year 2000	Not configured	No
Restrict these programs from being launched from Help	Not configured	No
Do not display the Getting Started welcome screen at logon	Not configured	No
Custom User Interface	Not configured	No
Prevent access to the command prompt	Not configured	No
Prevent access to registry editing tools	Not configured	No
Don't run specified Windows applications	Not configured	No
Run only specified Windows applications	Not configured	No
Windows Automatic Updates	Not configured	No

11 On the next window, check ***Enabled*** and click **Apply,** then **OK**. Close the window.



Prevent access to registry editing tools
Prevent access to registry editing tools
Previous Setting
Next Setting

○ Not Configured

● Enabled

○ Disabled

Comment:

Supported on: At least Windows 2000

Options:

Disable regedit from running silently? Yes

Help:

Disables the Windows registry editor Regedit.exe.

If you enable this policy setting and the user tries to start Regedit.exe, a message appears explaining that a policy setting prevents the action.

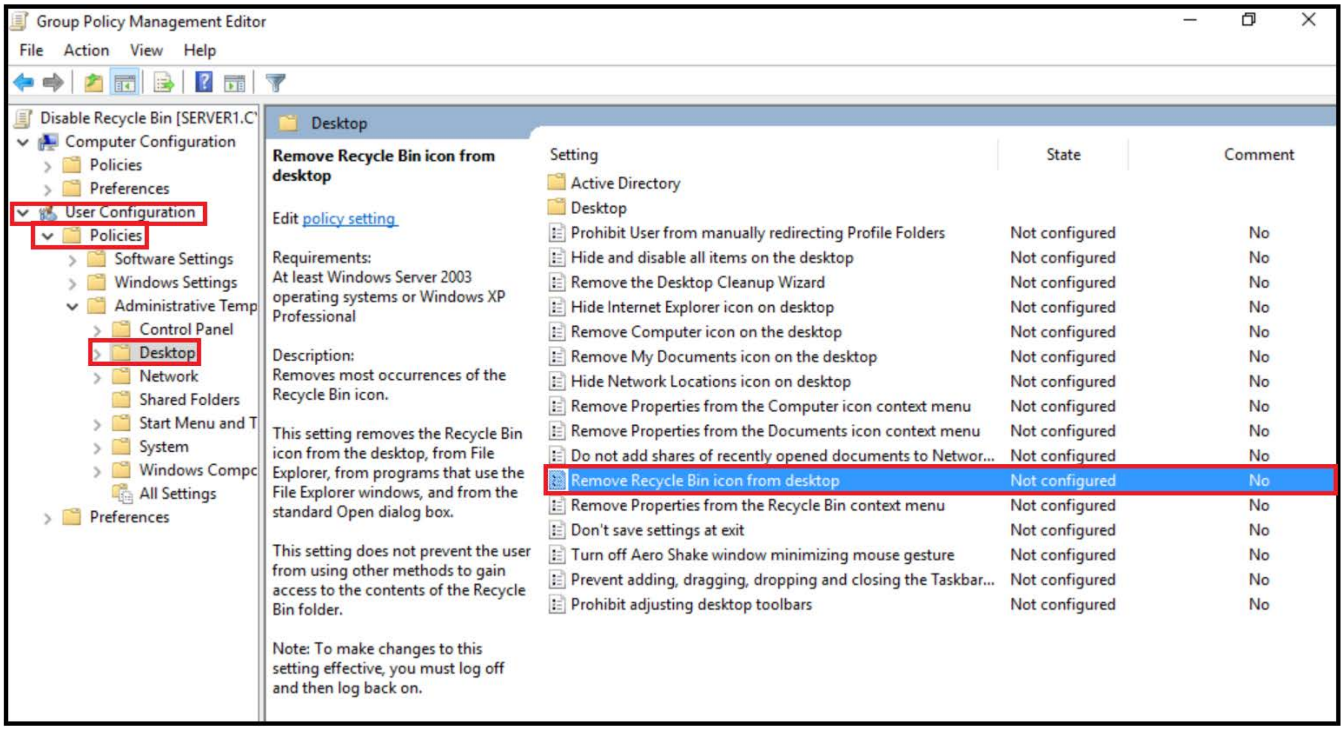
If you disable this policy setting or do not configure it, users can run Regedit.exe normally.

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

12 On the left pane, right-click the ***cyber.local*** domain and choose ***Create a GPO in this domain, and Link it here…*** Refer to Step 2 if you need to recall how to perform this step, but make sure you select the ***cyber.local*** domain.

13 Create a new GPO called **Disable Recycle Bin**. Then right-click the new GPO and select ***Edit***.

14 Navigate to ***User Configuration*** > ***Policies*** > ***Administrative Templates*** > ***Desktop*** and click it. On the right side, right-click ***Remove Recycle Bin icon from desktop*** and choose ***Edit***.



Remove Recycle Bin icon from desktop

Edit policy setting

Requirements:
At least Windows Server 2003 operating systems or Windows XP Professional

Description:
Removes most occurrences of the Recycle Bin icon.

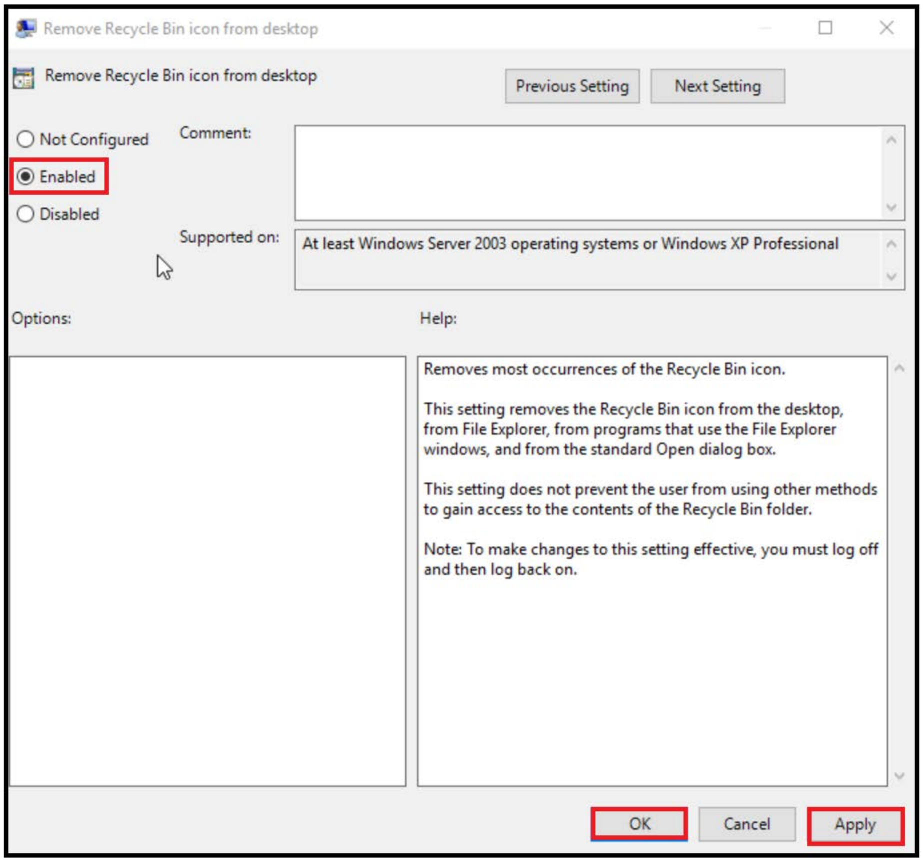
This setting removes the Recycle Bin icon from the desktop, from File Explorer, from programs that use the File Explorer windows, and from the standard Open dialog box.

This setting does not prevent the user from using other methods to gain access to the contents of the Recycle Bin folder.

Note: To make changes to this setting effective, you must log off and then log back on.

Setting	State	Comment
Active Directory		
Desktop		
Prohibit User from manually redirecting Profile Folders	Not configured	No
Hide and disable all items on the desktop	Not configured	No
Remove the Desktop Cleanup Wizard	Not configured	No
Hide Internet Explorer icon on desktop	Not configured	No
Remove Computer icon on the desktop	Not configured	No
Remove My Documents icon on the desktop	Not configured	No
Hide Network Locations icon on desktop	Not configured	No
Remove Properties from the Computer icon context menu	Not configured	No
Remove Properties from the Documents icon context menu	Not configured	No
Do not add shares of recently opened documents to Networ...	Not configured	No
Remove Recycle Bin icon from desktop	Not configured	No
Remove Properties from the Recycle Bin context menu	Not configured	No
Don't save settings at exit	Not configured	No
Turn off Aero Shake window minimizing mouse gesture	Not configured	No
Prevent adding, dragging, dropping and closing the Taskbar...	Not configured	No
Prohibit adjusting desktop toolbars	Not configured	No

15 On the next window, select ***Enabled*** and click **Apply,** then **OK**. Close the window.



Remove Recycle Bin icon from desktop

Remove Recycle Bin icon from desktop

○ Not Configured

● Enabled

○ Disabled

Comment:

Supported on: At least Windows Server 2003 operating systems or Windows XP Professional

Options:

Help:

Removes most occurrences of the Recycle Bin icon.

This setting removes the Recycle Bin icon from the desktop, from File Explorer, from programs that use the File Explorer windows, and from the standard Open dialog box.

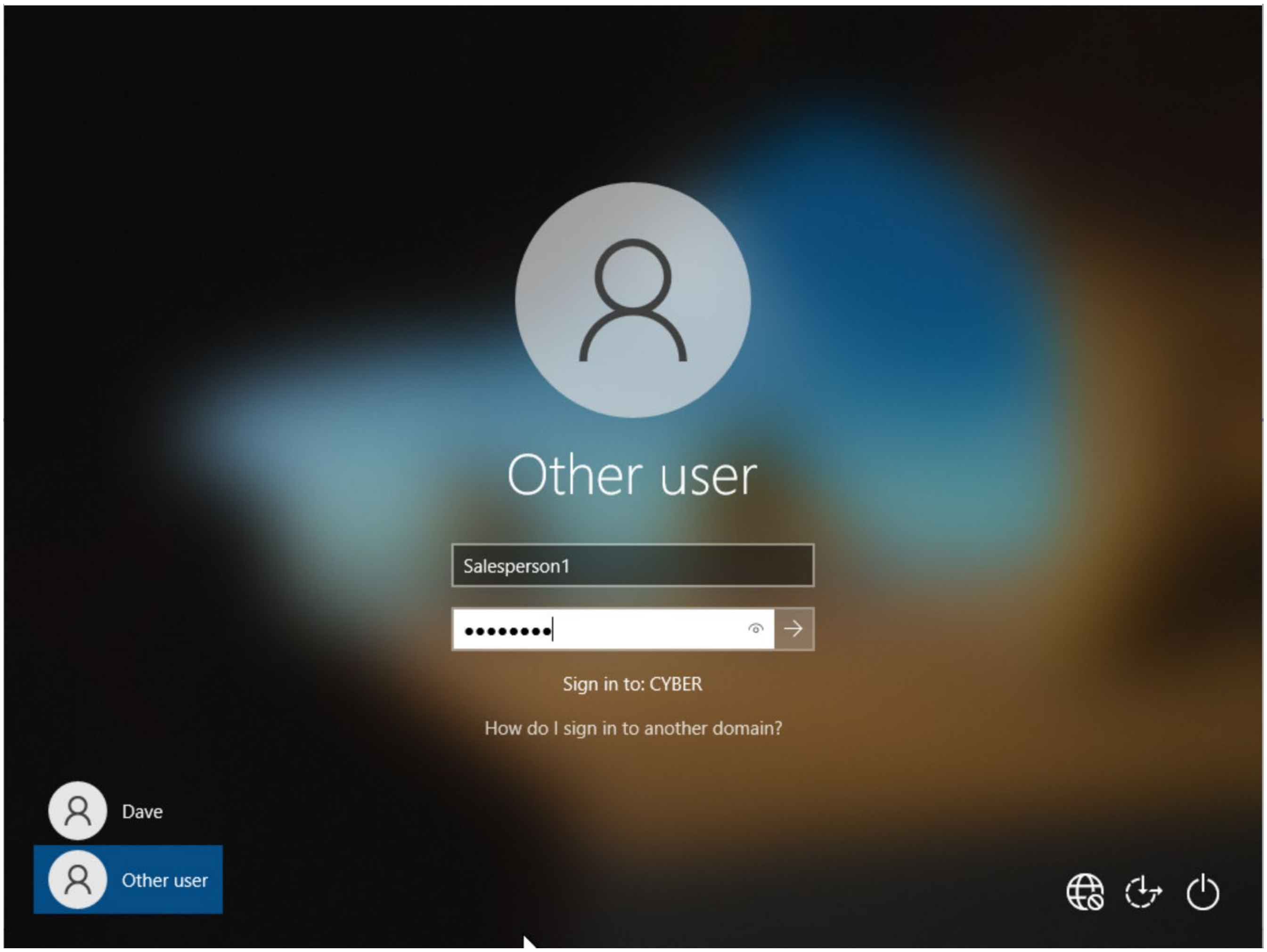
This setting does not prevent the user from using other methods to gain access to the contents of the Recycle Bin folder.

Note: To make changes to this setting effective, you must log off and then log back on.

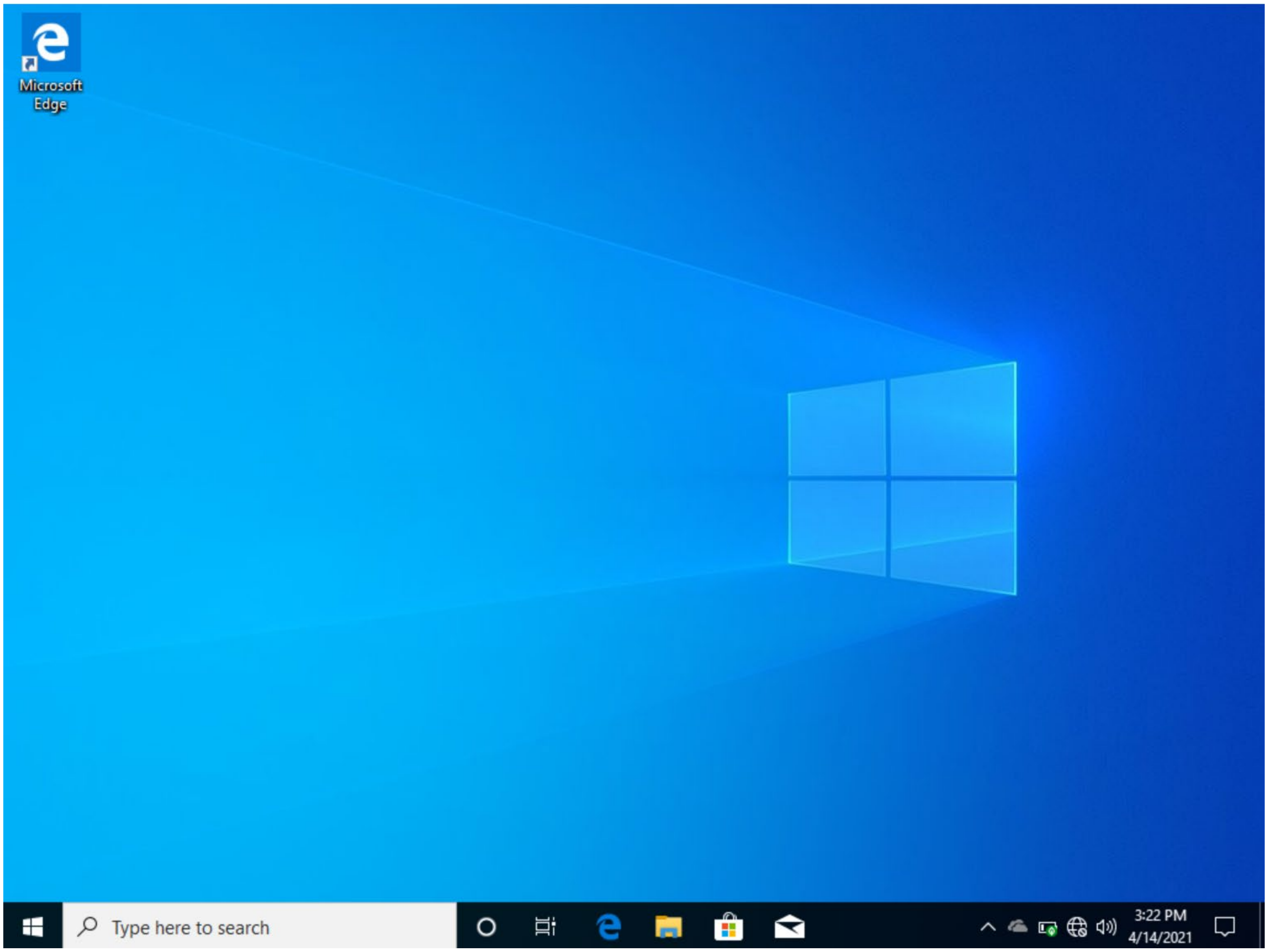
Lab Task 2: Verify GPO Configuration

Run the policy update command and verify that the settings were applied.

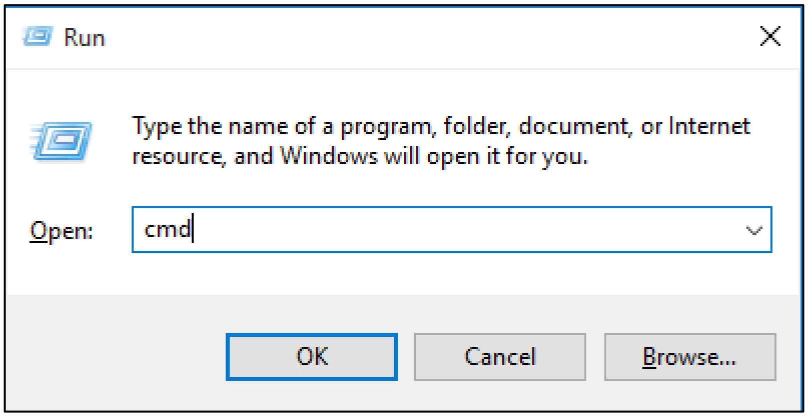
1 Log onto the client VM using Salesperson1.
Note: Because Salesperson1 was not previously used, the new policies are automatically applied upon logon.
If the policies are not applied, run the following command in the CMD:
gpupdate /force



2 Note that the *Recycle Bin* icon does not appear on the desktop.

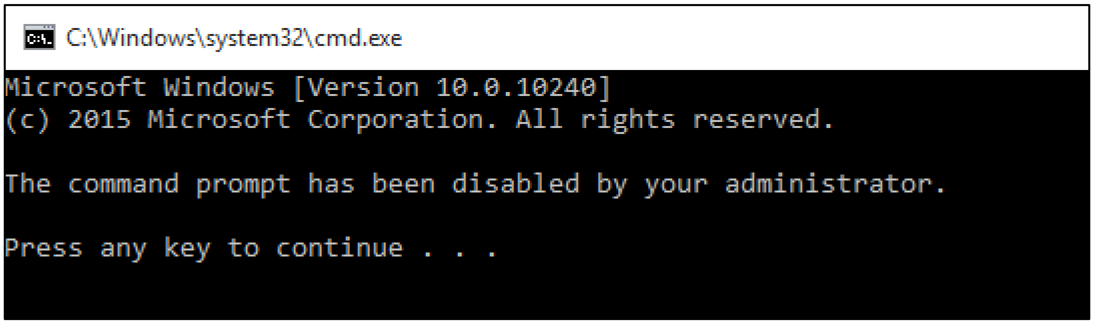


3 Try to open the CMD.
Hint: Press ***WINKEY + R***, type **cmd**, and press ***Enter***.



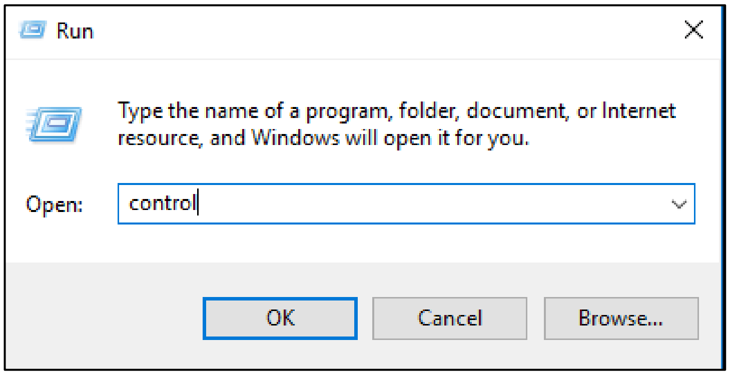
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd



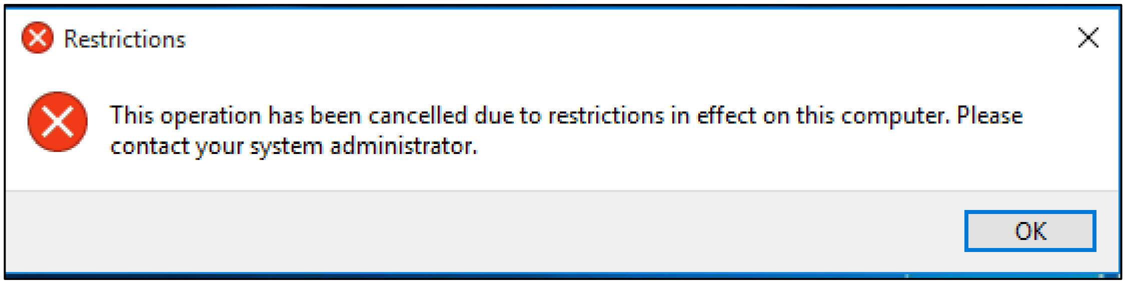
```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

The command prompt has been disabled by your administrator.

Press any key to continue . . .
```

4 Try to access the Control Panel. An error message should appear.
Hint: Press ***WINKEY + R***, type **control**, and press ***Enter***.



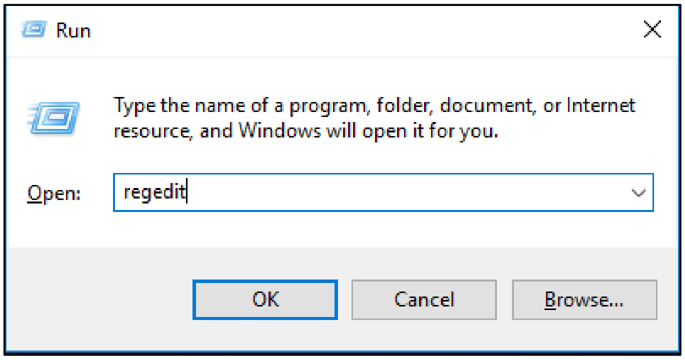
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: control



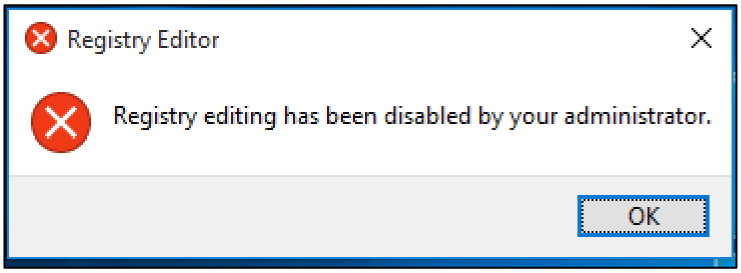
This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.

5 Try to access the registry. An error message should appear.
Hint: Press ***WINKEY + R***, type **regedit**, and press ***Enter***.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit



Registry editing has been disabled by your administrator.