

Lab Assignment 2 (Part 1) – GPO

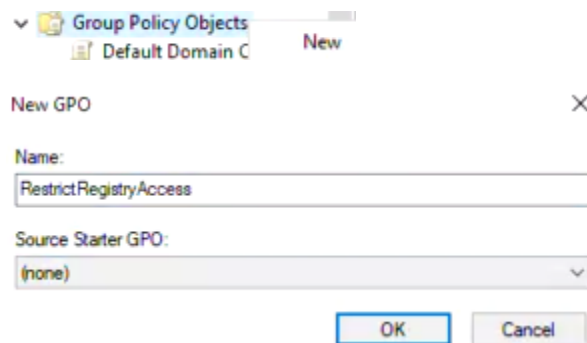
Task 1: Configuring Group Policy using GUI

1. Objective: Prevent users from opening the Windows Registry using a Group Policy Object (GPO).

2. GPO Name: RestrictRegistryAccess

3. Steps:

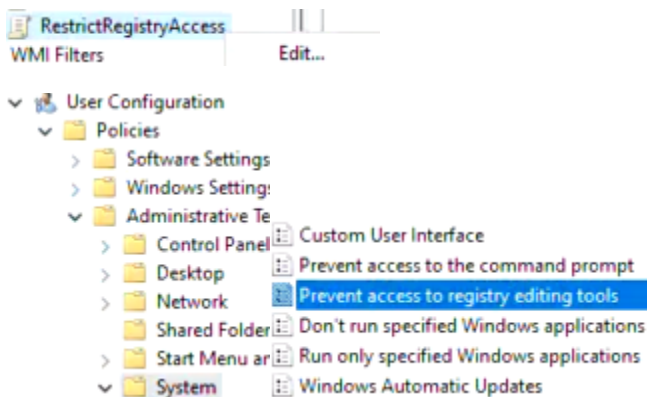
- Create a new GPO named RestrictRegistryAccess.





Group Policy Objects in viabs10.com



- Configure the required setting to block access to the registry editing tools.



 Prevent access to registry editing tools

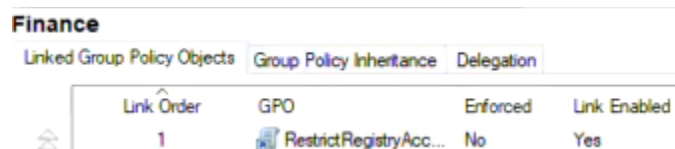
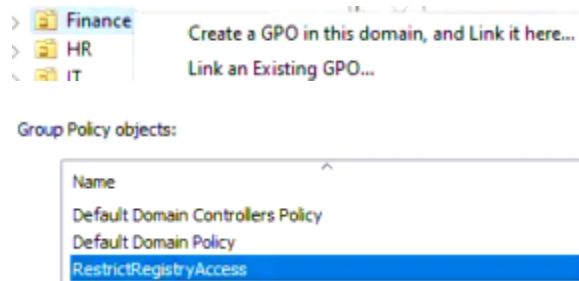
 Prevent access to registry editing tools

☐ Not Configured Comment:

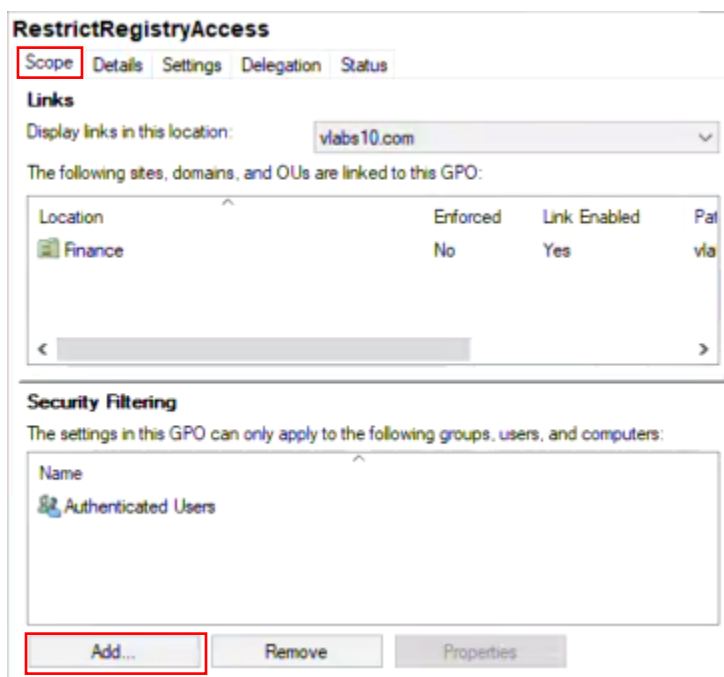
☒ Enabled

☐ Disabled

- Link the GPO to the Finance OU.



- Use Security Filtering to ensure that Ava Mercier from Finance is not affected by this GPO.



Select User, Computer, or Group

Select this object type:

From this location:

Enter the object name to select (examples):

Security Filtering

The settings in this GPO can only apply to the

Name

- Authenticated Users
- Ava.Mercier (VLABS10\Ava.Mercier)

RestrictRegistryAccess

Scope Details Settings **Delegation** Status

These groups and users have the specified permission for this GPO

Groups and users:

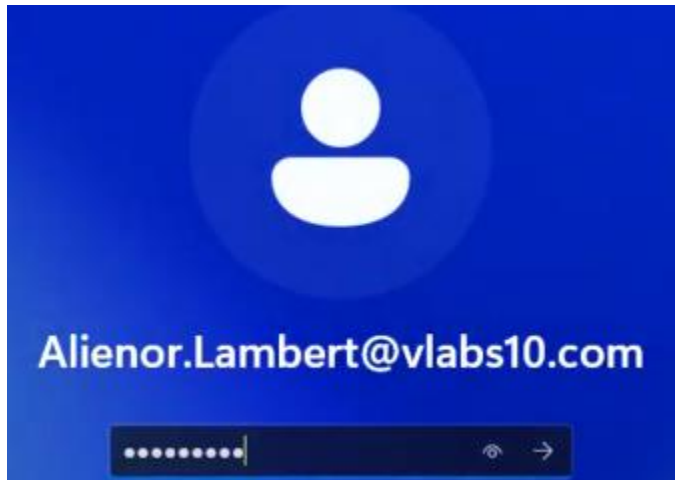
Name	Allowed Permissions	Inherited
Authenticated Users	Read (from Security Filtering)	No
Ava.Mercier (VLABS10\Ava.Mercier)	Read (from Security Filtering)	No
Domain Admins (VLAB...	Edit settings, delete, modify security	No
Enterprise Admins (VL...	Edit settings, delete, modify security	No
ENTERPRISE DOMAI...	Read	No
SYSTEM	Edit settings, delete, modify security	No

Permissions for Ava.Mercier

	Allow	Deny
Read	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Create all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Delete all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Apply group policy	<input type="checkbox"/>	<input checked="" type="checkbox"/>

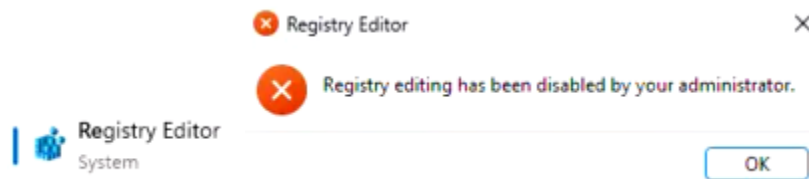
4. Testing:

- Log in to ClientXX with any Finance user and verify that the registry editing tools are blocked.

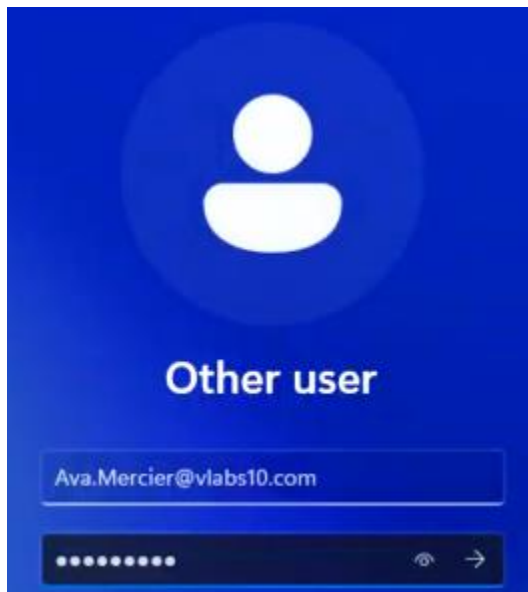


```
PS C:\Users\Alienor.Lambert> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```



- Log in as Ava Mercier and confirm that the GPO does not apply.

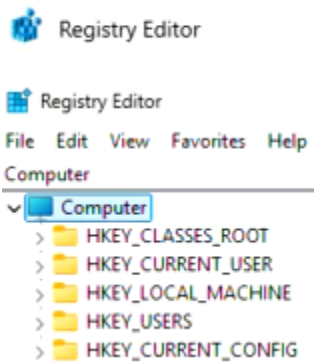


```
PS C:\Users\Ava.Mercier> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

```
PS C:\Users\Ava.Mercier> gpresult /r
```

```
The following GPOs were not applied because they were filtered out
-----
RestrictRegistryAccess
Filtering: Denied (Security)
```



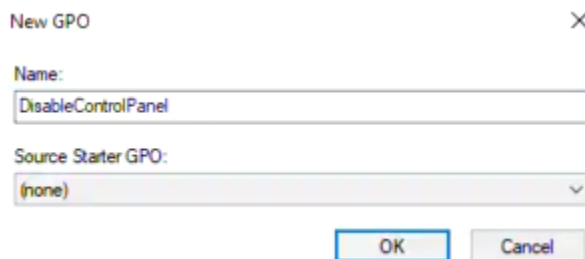
Task 2: Configuring Group Policy using PowerShell

1. Objective: Disable access to the Control Panel using PowerShell.

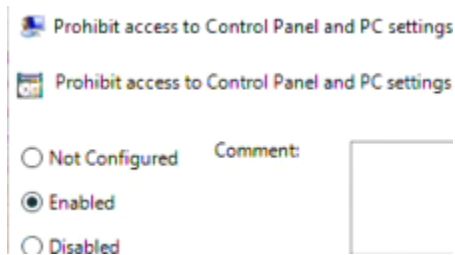
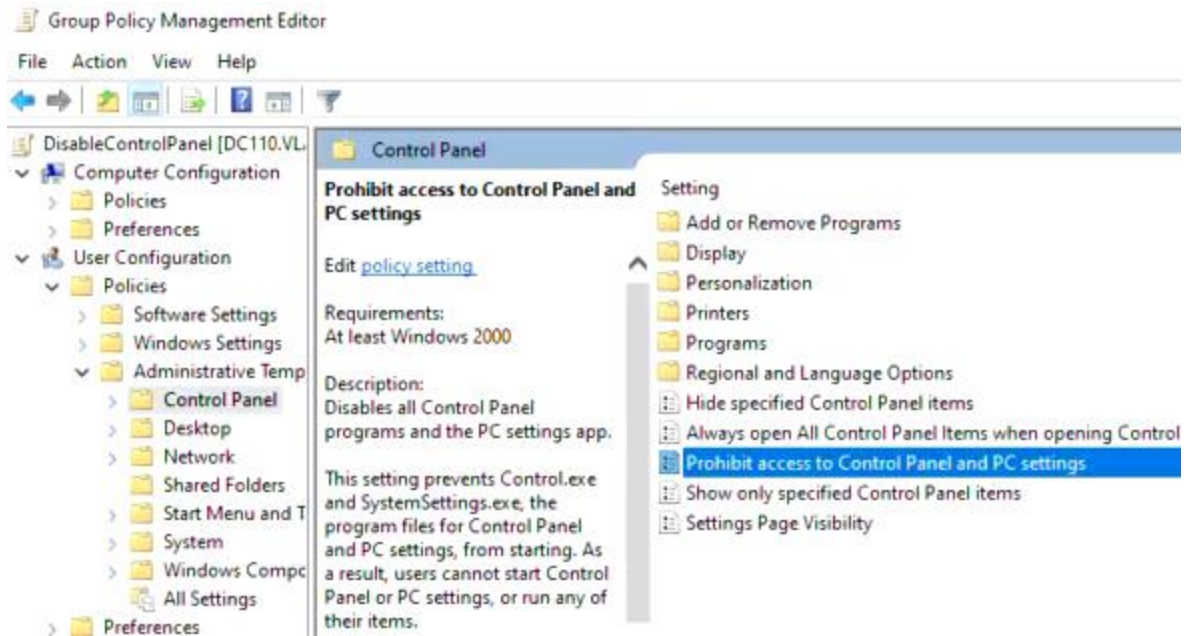
2. GPO Name: DisableControlPanel

3. Steps (using PowerShell):

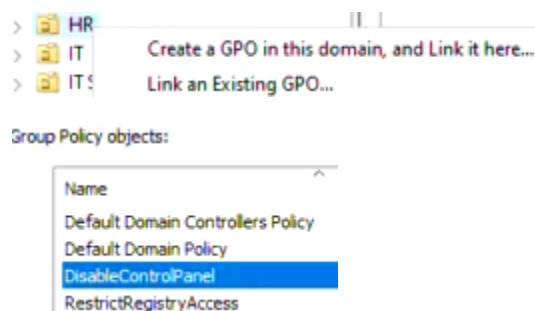
- Create a new GPO named DisableControlPanel



- Configure the necessary settings to disable access to the Control Panel.



- Link the GPO to the OU HR.



- Use Security Filtering to ensure that Emma Petit from HR is not affected by this GPO.

Select User, Computer, or Group

Select this object type:
 Object Types...

From this location:
 Locations...

Enter the object name to select (examples):
 Check Names

Advanced... OK Cancel

DisableControlPanel

Scope Details Settings Delegation Status

These groups and users have the specified permission for this GPO

Groups and users:

Name	Allowed Permissions	Inherited
Authenticated Users	Read (from Security Filtering)	No
Domain Admins (VLAB...	Edit settings, delete, modify security	No
Emma Pett (VLABS10...	Read (from Security Filtering)	No
Enterprise Admins (VL...	Edit settings, delete, modify security	No
ENTERPRISE DOMAI...	Read	No
SYSTEM	Edit settings, delete, modify security	No

Add... Remove Properties Advanced...

DisableControlPanel Security Settings

Security

Group or user names:

- CREATOR OWNER
- Authenticated Users
- SYSTEM
- Emma Pett (Emma.Pett@vlabs10.com)
- Domain Admins (VLABS10\Domain Admins)

Add...

Remove

Permissions for Emma Pett

	Allow	Deny
Read	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Create all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Delete all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Apply group policy	<input type="checkbox"/>	<input checked="" type="checkbox"/>

For special permissions or advanced settings, click Advanced.

Advanced

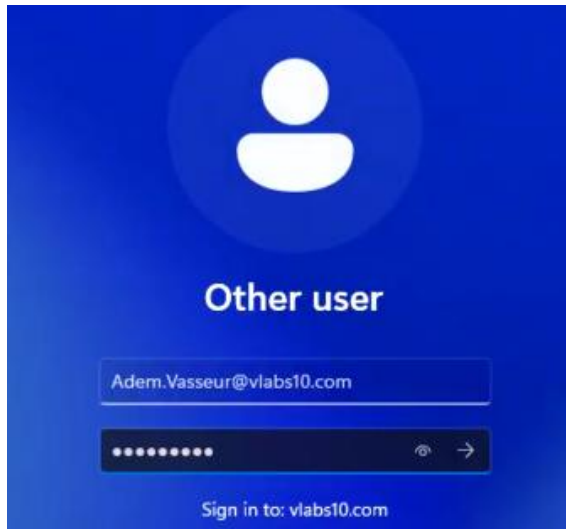
OK

Cancel

Apply

4. Testing: (Don't forget to run gpupdate /force on the client before each test)

- Log in to ClientXX with any HR user and verify that the Control Panel is disabled.



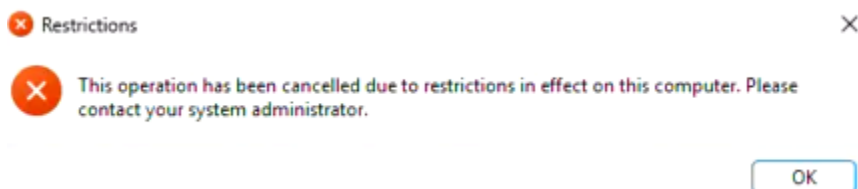
```
PS C:\Users\Adem.Vasseur> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

```
PS C:\Users\Adem.Vasseur> gpresult /r
```

```
Applied Group Policy Objects
-----
DisableControlPanel
```

 Control Panel

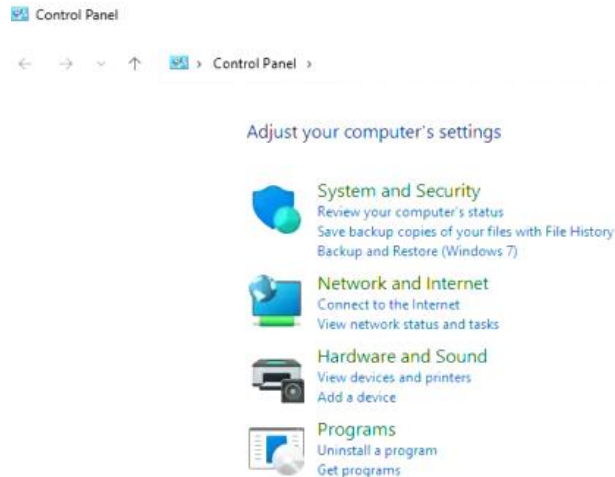


- Log in as Emma Petit and confirm that the GPO does not apply.

```
PS C:\Users\Emma.Petit> gpresult /r
```

```
The following GPOs were not applied because they were filtered out
-----
DisableControlPanel
Filtering: Denied (Security)
```

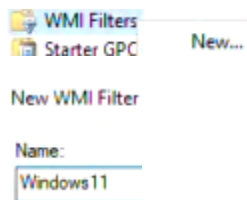
 Control Panel



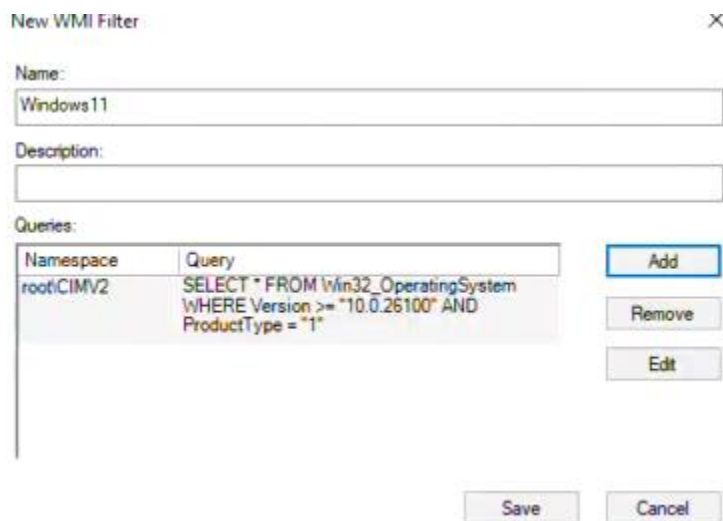
Task 3: Creating and Testing a WMI Filter for Windows 11 using GUI

1. Objective: Create a WMI filter that applies only to Windows 11 devices.
2. GPO Name: NoRecycleBin
3. Steps:

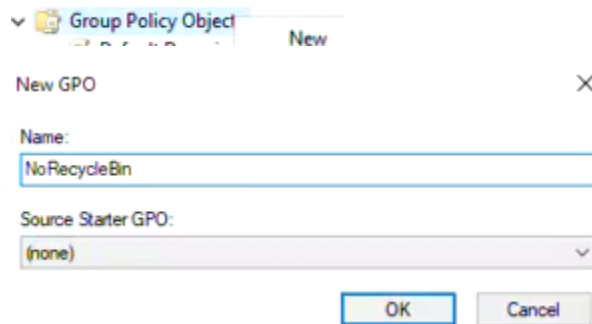
- Create a new WMI filter and named Windows11



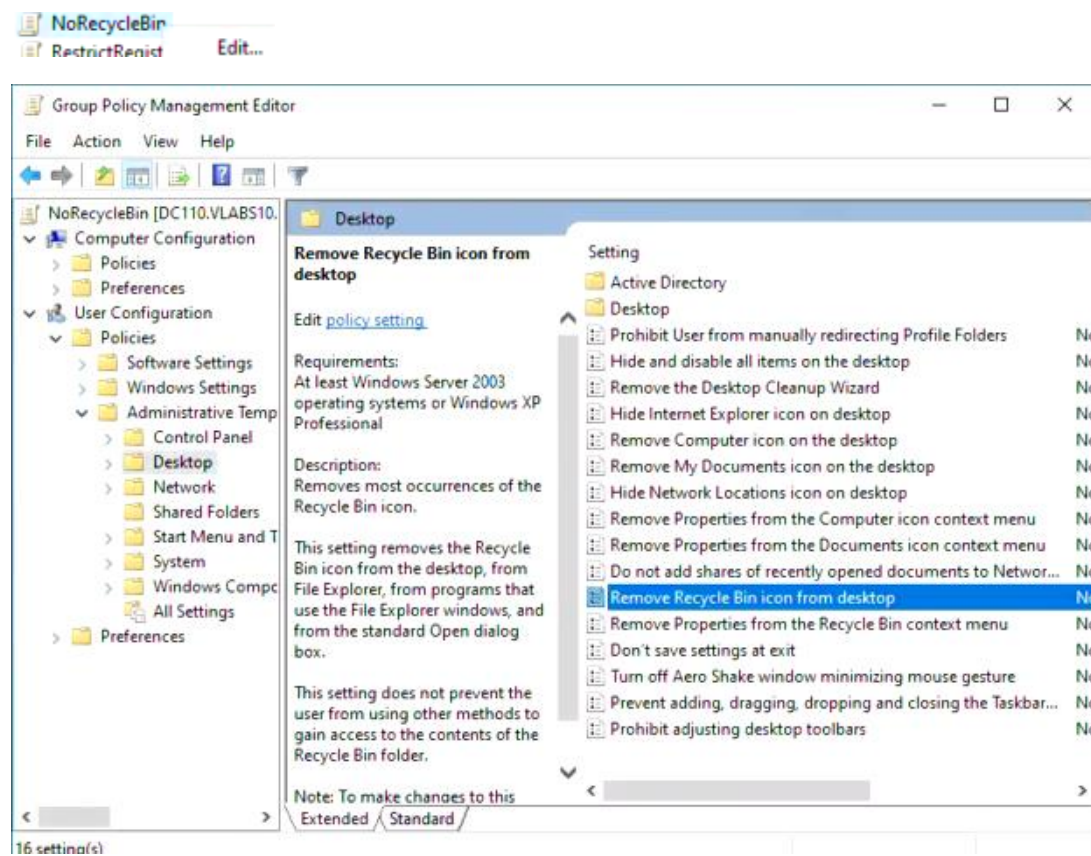
- Define the appropriate query to target Windows 11 machines.



- Create a new GPO named NoRecycleBin.



- Configure the necessary settings to Remove the Recycle Bin from the Desktop.

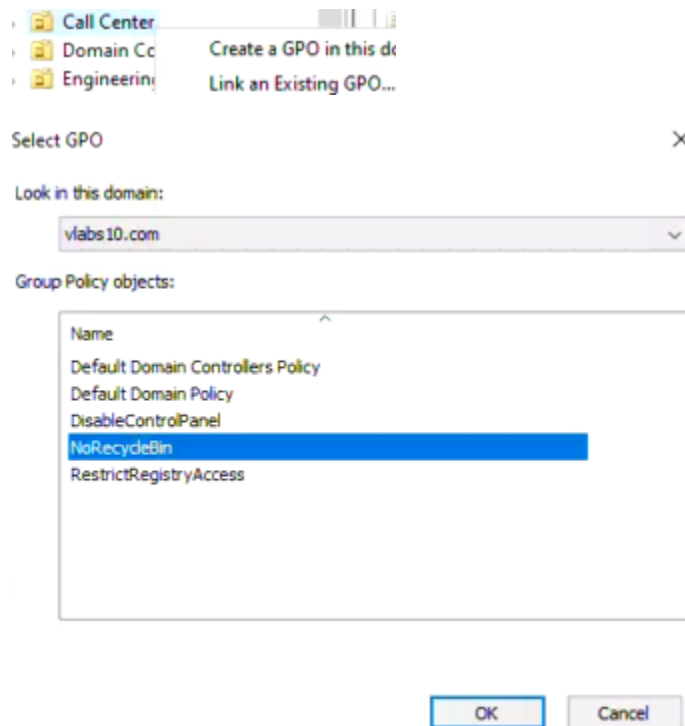


Remove Recycle Bin icon from desktop

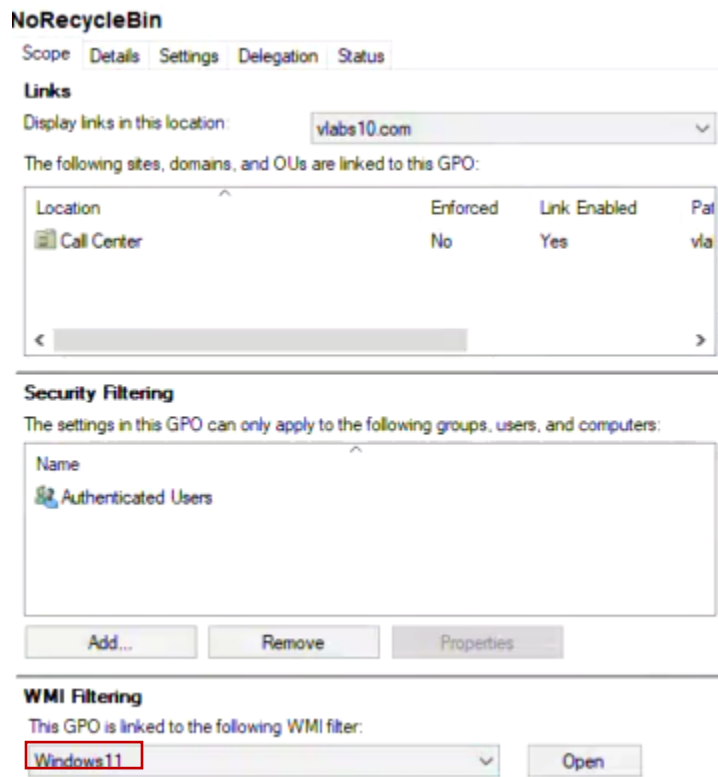
Remove Recycle Bin icon from desktop

☐ Not Configured Comment:
☒ Enabled
☐ Disabled

- Link this GPO to the Call Center OU.

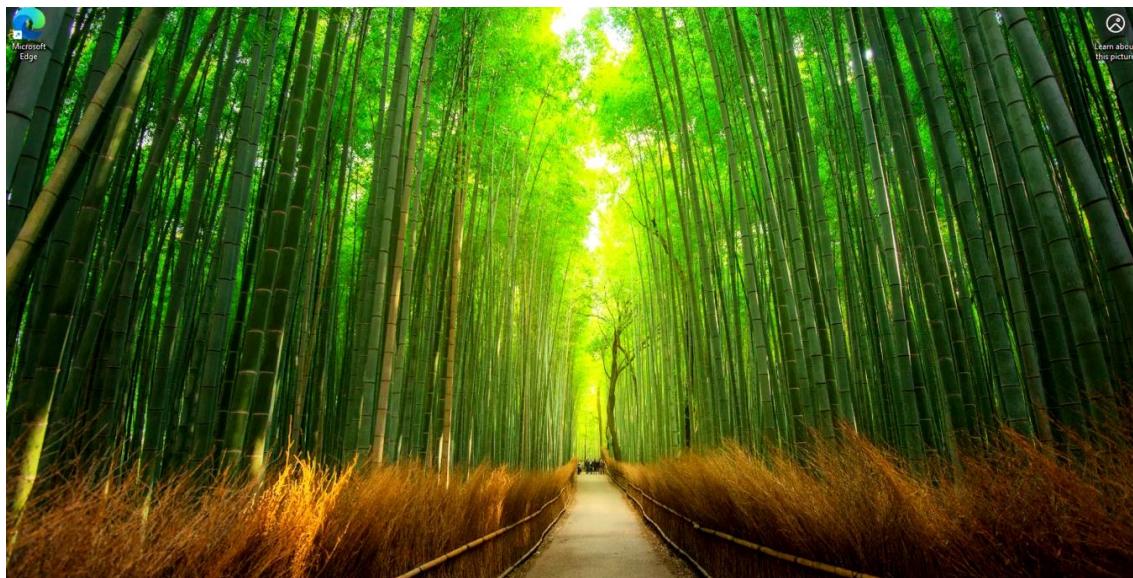
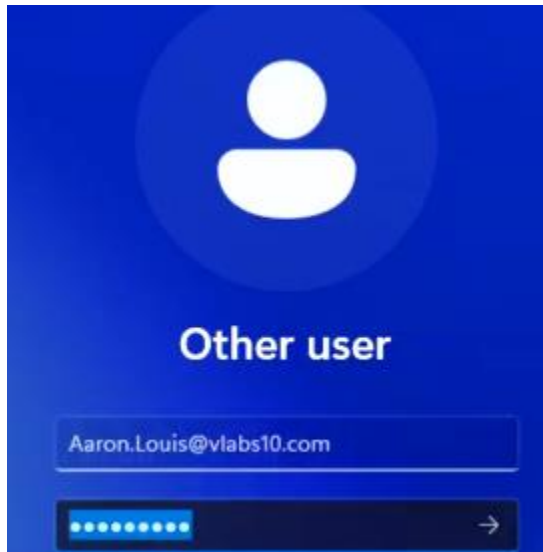


- Link to this GPO to the WMI filter Windows 11.



4. Testing: (Don't forget to run `gpupdate /force` on the client before each test)

- Log in to ClientXX with any user from Call Center user and verify that the Recycle Bin doesn't appear on the Desktop.

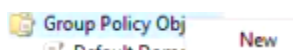


Task 4: Practicing GPO Processing Order using GUI

1. Objective: Understand the impact of multiple GPOs.

2. Steps:

- Link Order: (Don't forget to run `gpupdate /force` on the client before each test)
 - o Create a new GPO named AllowRegistryAccess that grants access to the registry editing tools.



New GPO

Name:

Source Starter GPO:

OK Cancel

Group Policy Management Editor

File Action View Help

AllowRegistryAccess [DC110.VL]

- Computer Configuration
 - Policies
 - Preferences
- User Configuration
 - Policies
 - Software Settings
 - Windows Settings
 - Administrative Templates
 - Control Panel
 - Desktop
 - Network
 - Shared Folders
 - Start Menu and Taskbar
 - System
 - Windows Components
 - All Settings
 - Preferences

System

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

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

Prevent access to registry editing tools

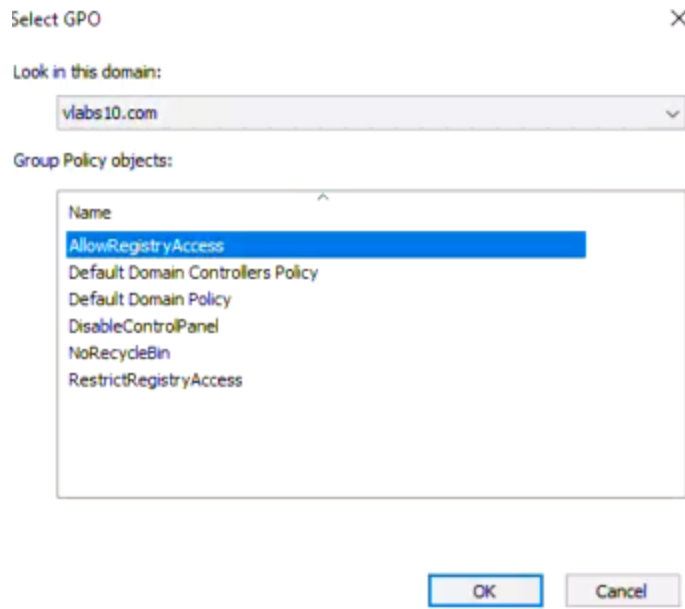
Prevent access to registry editing tools

Not Configured Enabled Disabled

Comment:

o Link it to OU Finance as Order 1.

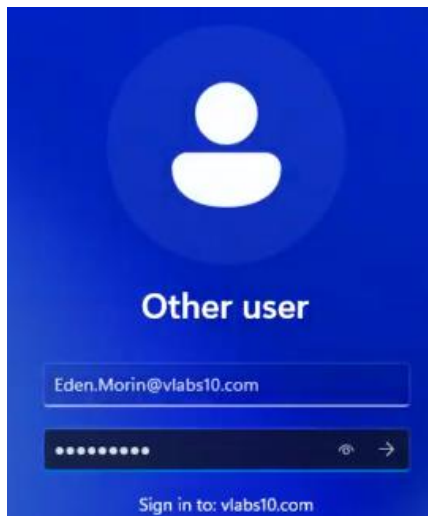
- Finance
 - HR
 - IT
- Create a GPO in this dc
- Link an Existing GPO...



Finance

Linked Group Policy Objects				
Group Policy Inheritance				
Delegation				
Link	Order	GPO	Enforced	Link Enabled
	1	AllowRegistryAccess	No	Yes
	2	RestrictRegistryAcc...	No	Yes

o Test using Eden Morin to ensure he now has access to the registry.



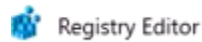
```
PS C:\Users\Eden.Morin> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

```
PS C:\Users\Eden.Morin> gpresult /r
```

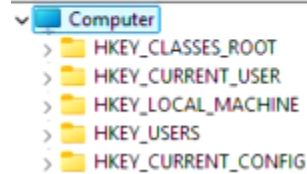

Applied Group Policy Objects

RestrictRegistryAccess



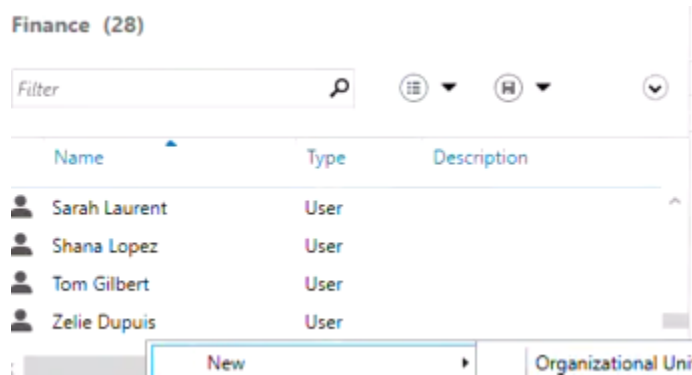
File Edit View Favorites Help

Computer

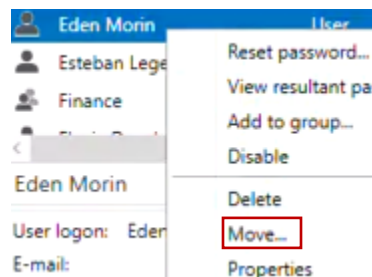
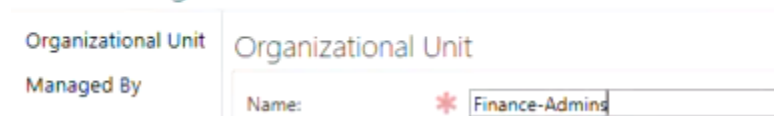


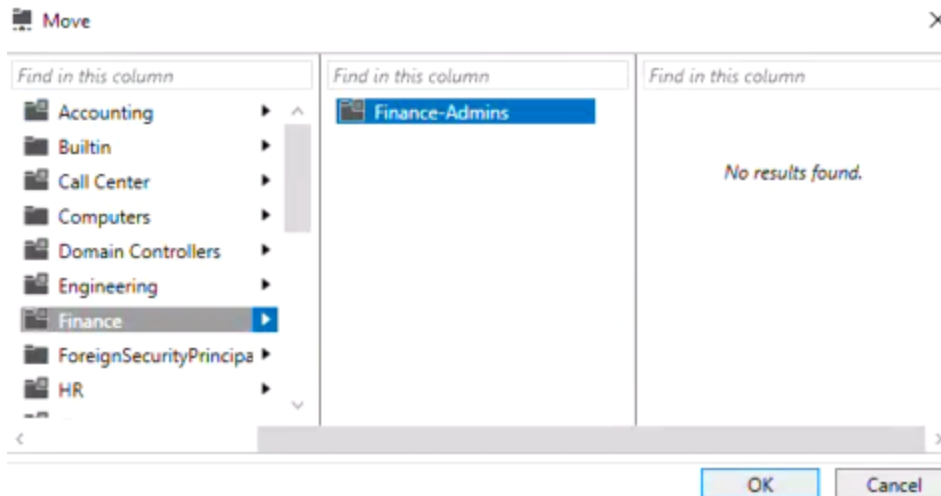
- Precedence Rules: (Don't forget to run gpupdate /force on the client before each test)

o Create OU Finance-Admins and move Eden Morin to it.

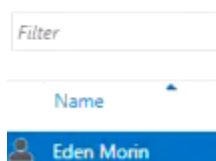


Create Organizational Unit: Finance-Admins



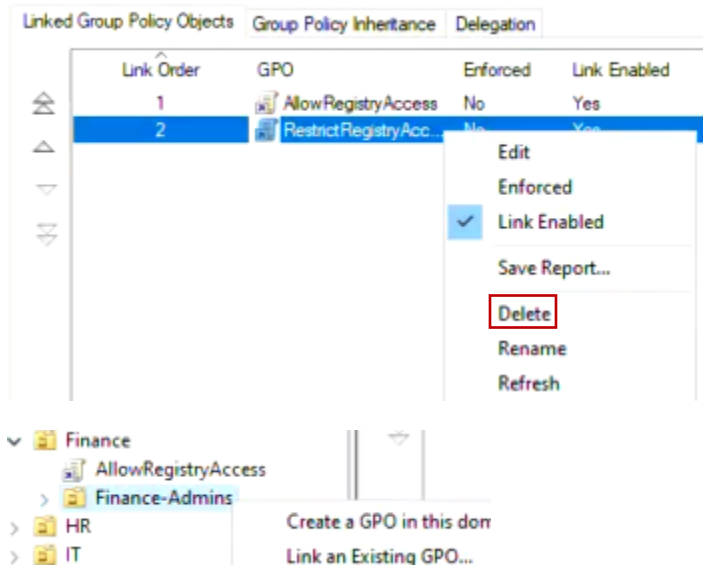


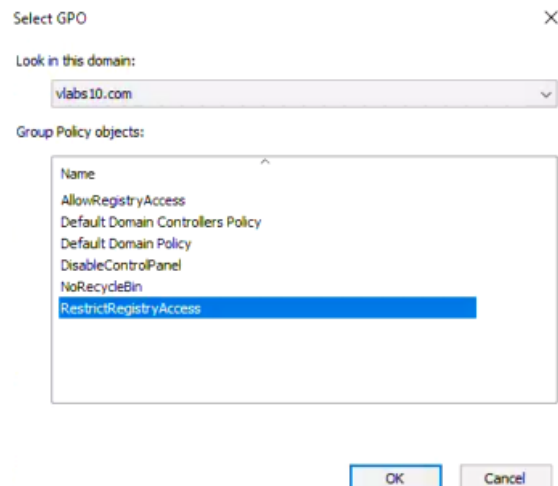
Finance-Admins (1)



o Unlink the GPO RestrictRegistryAccess from OU Finance and link it to OU Finance-Admins.

Finance

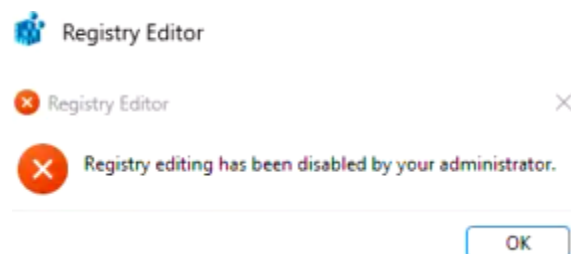




o Test using Eden Morin to verify that the registry editing tools are now blocked.

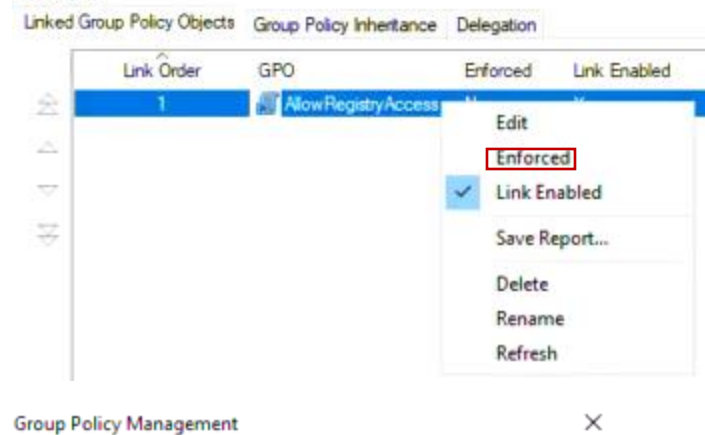
```
PS C:\Users\Eden.Morin> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```



- Enforced GPO: (Don't forget to run gpupdate /force on the client before each test)
- o Enforce the AllowRegistryAccess GPO on OU Finance.

Finance

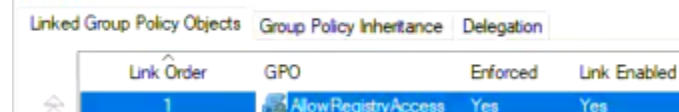


Do you want to change the Enforced setting for this GPO Link(s)?

OK

Cancel

Finance



o Test using Eden Morin to confirm he has access to the registry editing tools.

```
PS C:\Users\Eden.Morin> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
```



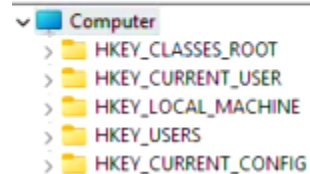
Registry Editor



Registry Editor

File Edit View Favorites Help

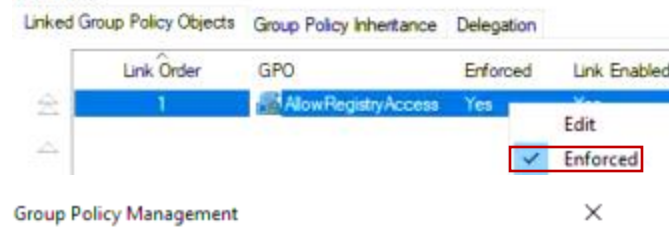
Computer



- Block Inheritance: (Don't forget to run gpupdate /force on the client before each test)

o Remove Enforce the AllowRegistryAccess GPO on OU Finance.

Finance



Do you want to change the Enforced setting for this GPO Link(s)?

OK

Cancel

1

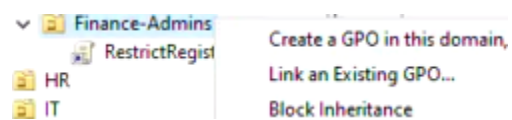


AllowRegistryAccess

No

Yes

o Block inheritance on OU Finance-Admins.



o Test using Eden Morin to ensure the registry editing tools are now blocked.

```
PS C:\Users\Eden.Morin> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```



Registry Editor



Registry Editor



Registry editing has been disabled by your administrator.

OK

• Link Enabled: (Don't forget to run gpupdate /force on the client before each test)

o Uncheck Link Enabled on the RestrictRegistryAccess GPO on OU Finance Admins

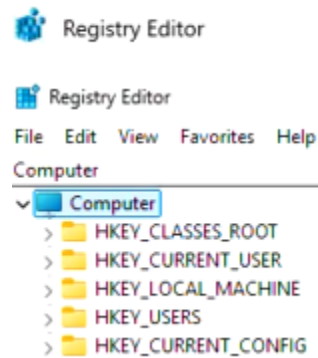
Finance-Admins



o Test using Eden Morin to confirm he has access to the registry editing tools.

```
PS C:\Users\Eden.Morin> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
```



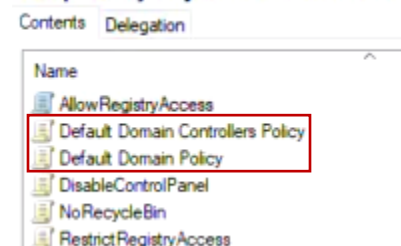
Task 5: Exploring Default Group Policy Objects using GUI

1. Objective: Understand and analyze the impact of Default Domain Policy and Default Domain Controllers Policy.

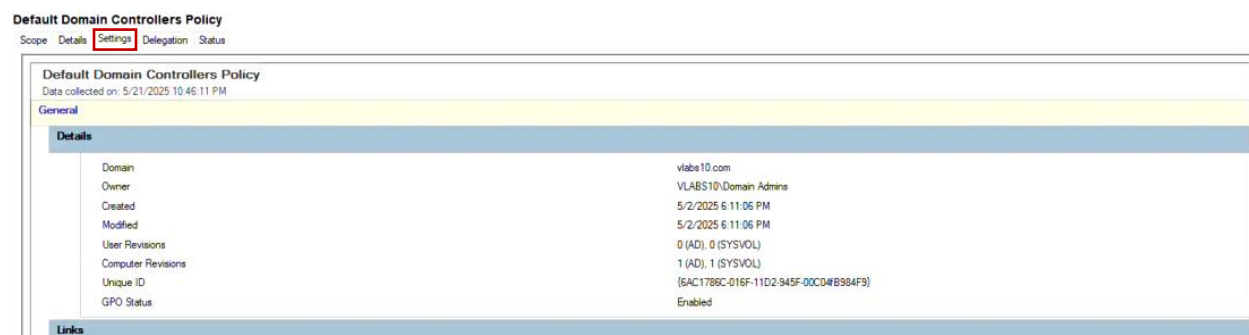
2. Steps:

- Identify and review the two default GPOs in the domain.

Group Policy Objects in vlabs10.com



- Generate a Settings Report for both policies.



Default Domain Policy

Scope Details **Settings** Delegation Status

Default Domain Policy	
Data collected on: 5/21/2025 10:48:04 PM	
General	
Details	
Domain	vlabs10.com
Owner	VLABS10\Domain Admins
Created	5/2/2025 6:11:06 PM
Modified	5/2/2025 6:15:32 PM
User Revisions	0 (AD), 0 (SYSVOL)
Computer Revisions	3 (AD), 3 (SYSVOL)
Unique ID	{31B2F340-016D-11D2-945F-00C04FB984F9}
GPO Status	Enabled
Links	

- Analyze the impact of these GPOs without making any modifications or testing at this stage.

Default Domain Controller Policy

Policies	
Windows Settings	
Security Settings	
Local Policies/User Rights Assignment	
Policy	Setting
Access this computer from the network	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, Everyone
Add workstations to domain	NT AUTHORITY\Authenticated Users
Adjust memory quotas for a process	BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Allow log on locally	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Account Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Back up files and directories	BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Bypass traverse checking	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, Everyone
Change the system time	BUILTIN\Server Operators, BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE
Create a pagefile	BUILTIN\Administrators
Debug programs	BUILTIN\Administrators
Enable computer and user accounts to be trusted for delegation	BUILTIN\Administrators
Force shutdown from a remote system	BUILTIN\Server Operators, BUILTIN\Administrators
Generate security audits	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Increase scheduling priority	Window Manager\Window Manager Group, BUILTIN\Administrators
Load and unload device drivers	BUILTIN\Print Operators, BUILTIN\Administrators
Log on as a batch job	BUILTIN\Performance Log Users, BUILTIN\Backup Operators, BUILTIN\Administrators
Manage auditing and security log	BUILTIN\Administrators
Modify firmware environment values	BUILTIN\Administrators
Profile single process	BUILTIN\Administrators
Profile system performance	NT SERVICE\WdServiceHost, BUILTIN\Administrators
Remove computer from docking station	BUILTIN\Administrators
Replace a process level token	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Restore files and directories	BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Shut down the system	BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Take ownership of files or other objects	BUILTIN\Administrators

Go to Settings to activate

Local Policies/Security Options	
Domain Controller	
Policy	Setting
Domain controller: LDAP server signing requirements	None
Domain Member	
Policy	Setting
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Microsoft Network Server	
Policy	Setting
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled

Default Domain Policy

Windows Settings	
Security Settings	
Account Policies/Password Policy	
Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled
Account Policies/Account Lockout Policy	
Policy	Setting
Account lockout threshold	0 invalid logon attempts
Account Policies/Kerberos Policy	
Policy	Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes
Local Policies/Security Options	
Network Access	
Policy	Setting
Network access: Allow anonymous SID/Name translation	Disabled
Network Security	
Policy	Setting
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Disabled