Table of Contents

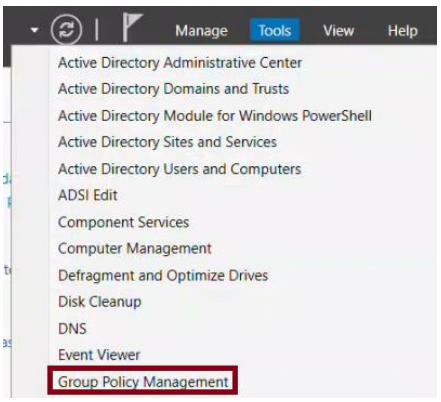
Lab Assignment 2 (Part I) – GPO

Task 1: Configuring Group Policy using GUI

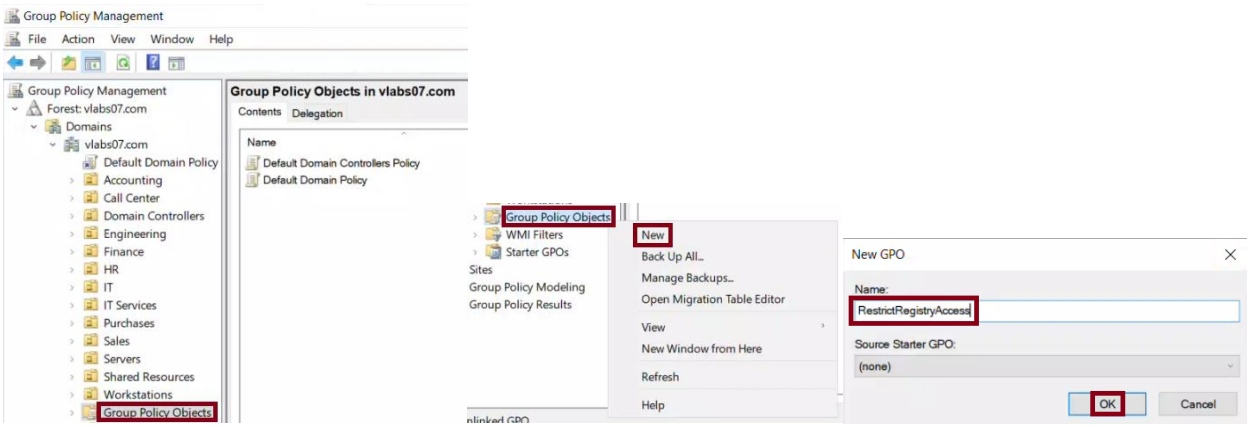
System: DC107

Objective:
Create a GPO to prevent access to Registry Editor for all users in the Finance OU,
except Ava Mercier. This task is performed using Group Policy Management Console (GPMC).

Step 1 – Open Group Policy Management Console (GPMC)
Click Tools → Search for "Group Policy Management" and open it.
Alternatively, press Windows + R, type gpmc.msc, and hit Enter.

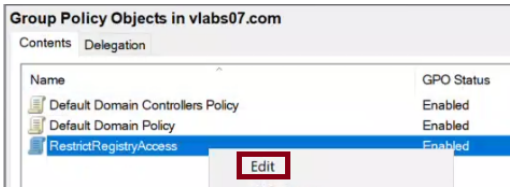


Step 2 – Create a new GPO
In the left pane, expand the Forest and Domain until you see the "Group Policy Objects" container.
Right-click on "Group Policy Objects" → Click "New".
For the name, enter: RestrictRegistryAccess.
Click OK. The GPO will now appear in the list.



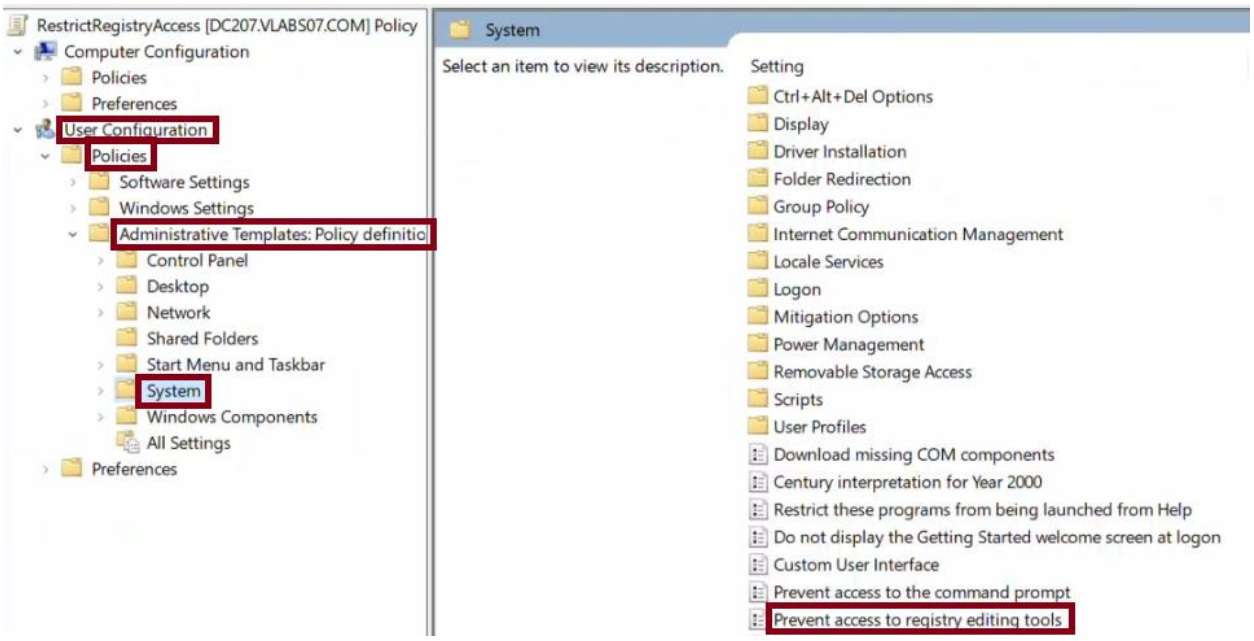
Step 3 – Edit the new GPO

Right-click on the GPO named RestrictRegistryAccess → Click "Edit".
This opens the Group Policy Management Editor window.

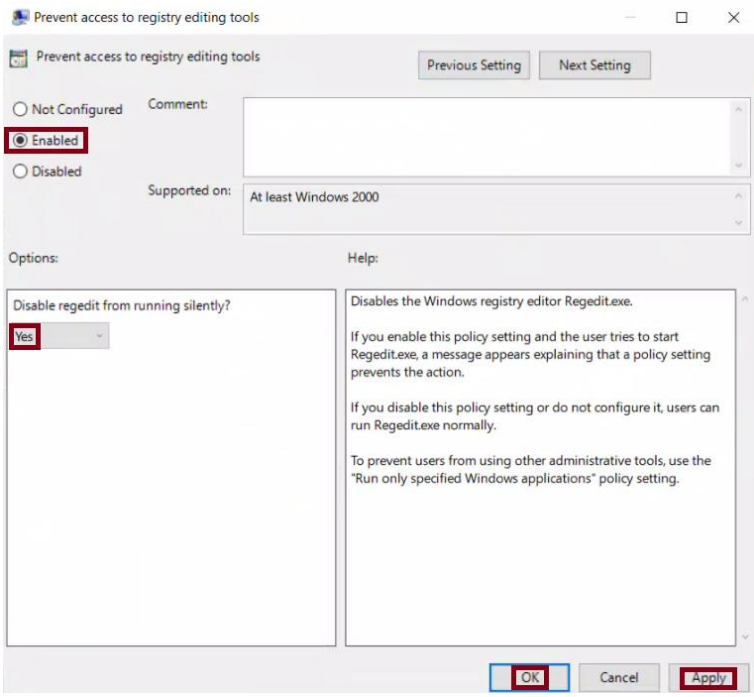


In the GPM editor, navigate to:
User Configuration → Policies → Administrative Templates → System

On the right-hand side, double-click on:
Prevent access to registry editing tools

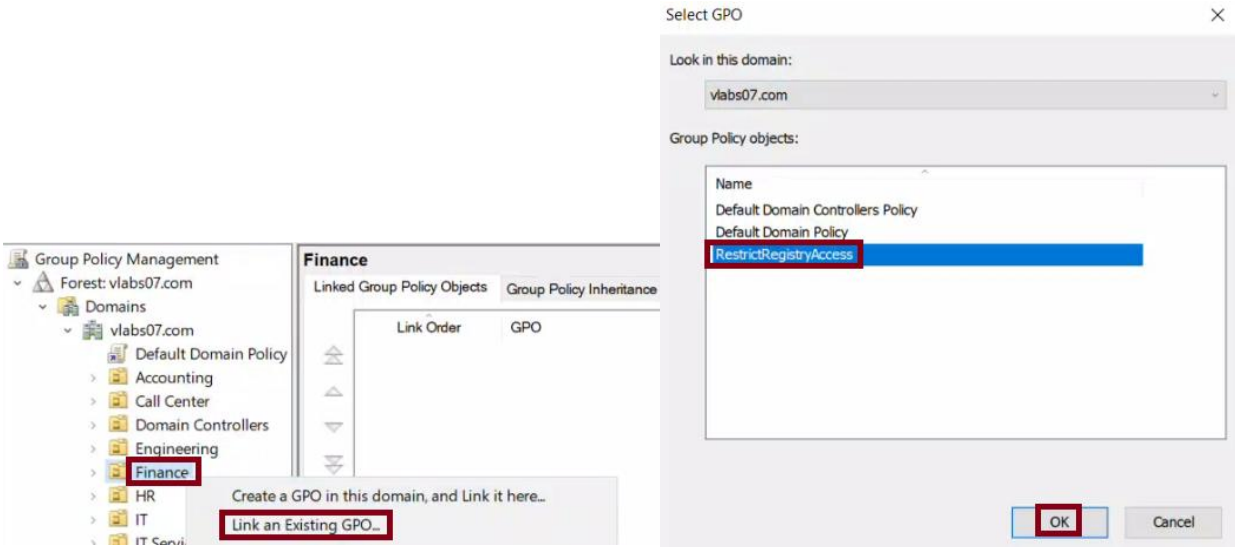


In the window that opens:
Select: Enabled
From the Options at the bottom, Yes: Disable regedit from running silently
Click Apply, then OK.
Close the Group Policy Management Editor window.



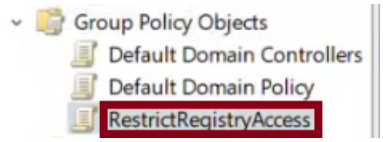
Step 4 – Link the GPO to the Finance OU

Back in GPMC, locate the "Finance" Organizational Unit under your domain.
Right-click on Finance → Click "Link an Existing GPO".
From the list, select: RestrictRegistryAccess → Click OK.



Step 5 – Configure Security Filtering (to exclude Ava Mercier)

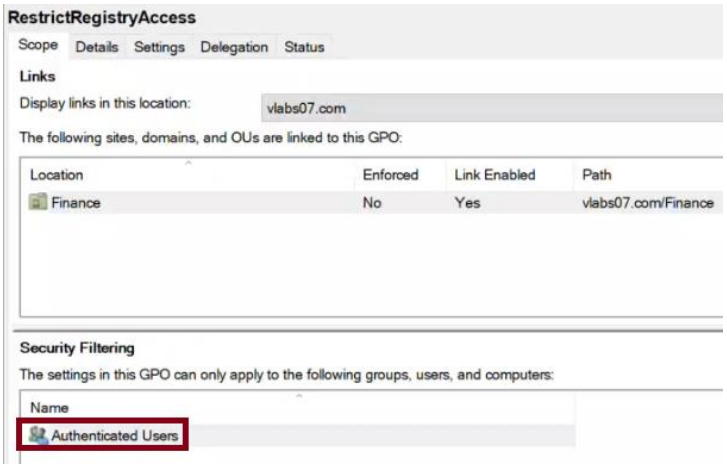
In the left pane of GPMC, expand your domain and click on "Group Policy Objects".
Click once on the GPO named "RestrictRegistryAccess" to highlight it.



In the right-hand pane, click the "Scope" tab.

Initial Setup: Use "Authenticated Users" for testing
Ensure "Authenticated Users" is listed under Security Filtering.

This allows the GPO to apply to all domain users in the Finance OU without any filtering issues during the initial setup.



****Test the GPO****
Log in to Client07 as any Finance user except Ava Mercier. Run gpupdate /force and attempt to open regedit. Confirm that the Registry Editor is blocked.

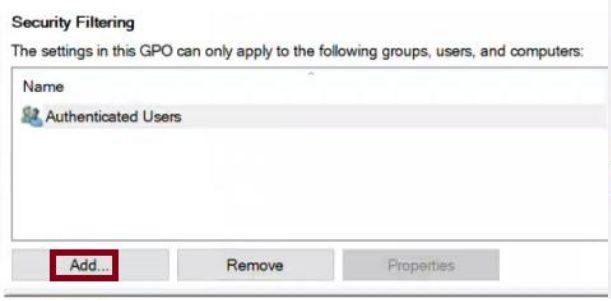

```
C:\Users\Carla.Chevalier>gpupdate /force
Updating policy...

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

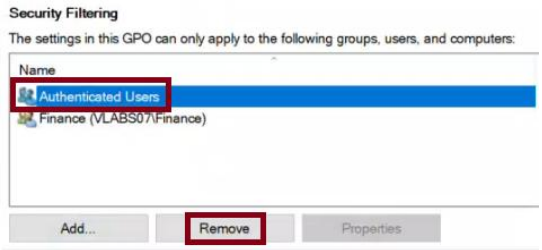
```
C:\Users\Carla.Chevalier>gpresult /r
```

```
RSOP data for VLABS07\Carla.Chevalier on CLIENT07 : Logging Mode
-----------------------------------------------------------------

OS Configuration:            Member Workstation
OS Version:                  10.0.26100
Site Name:                   N/A
Roaming Profile:             N/A
Local Profile:               C:\Users\Carla.Chevalier
Connected over a slow link?: No


USER SETTINGS
-------------
    CN=Carla Chevalier,OU=Finance,DC=vlabs07,DC=com
    Last time Group Policy was applied: 5/21/2025 at 11:54:09 AM
    Group Policy was applied from:      DC207.vlabs07.com
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        VLABS07
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    ----------------------------
        RestrictRegistryAccess
```

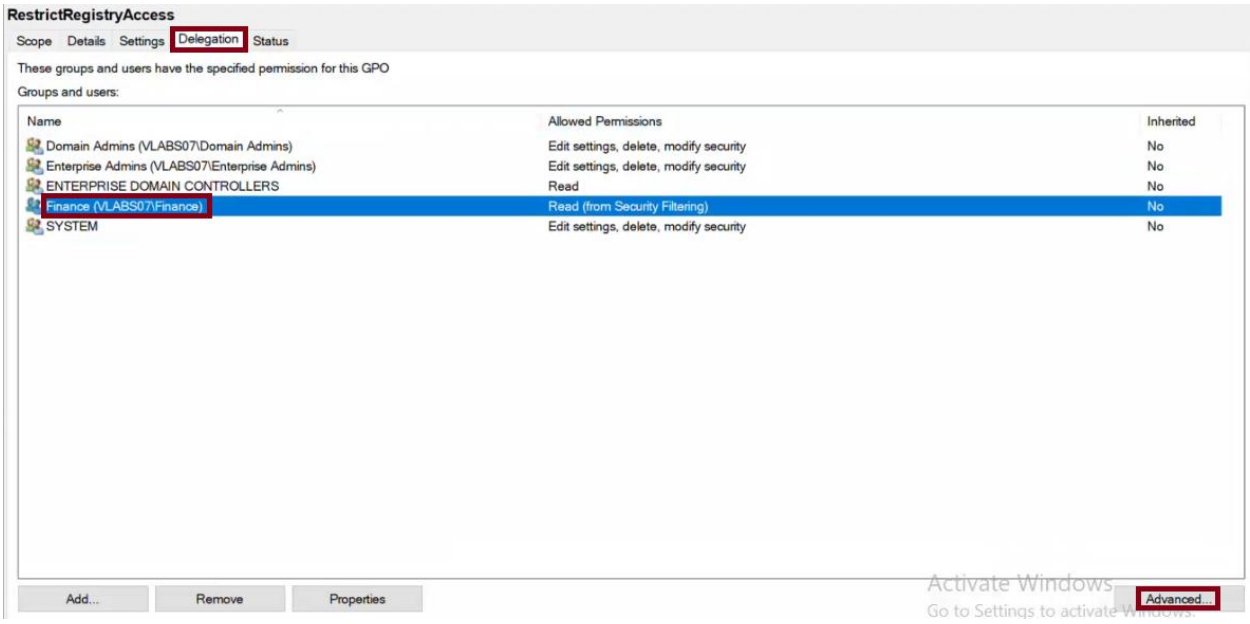
Refine Filtering: Replace Authenticated Users with the Finance group
Once the GPO is confirmed to be working:

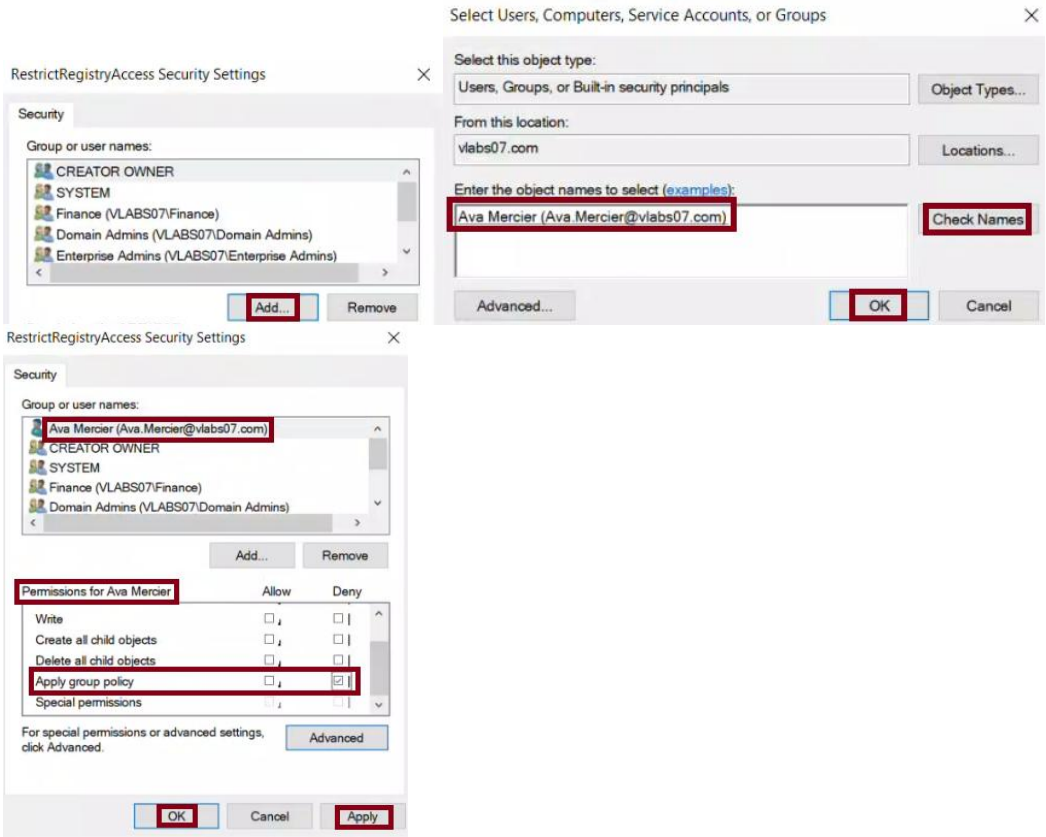
1. **In** the **Scope** tab under Security Filtering:
   - Click **Add** → Add the group **Finance**.
   - Remove **Authenticated Users** from the list.

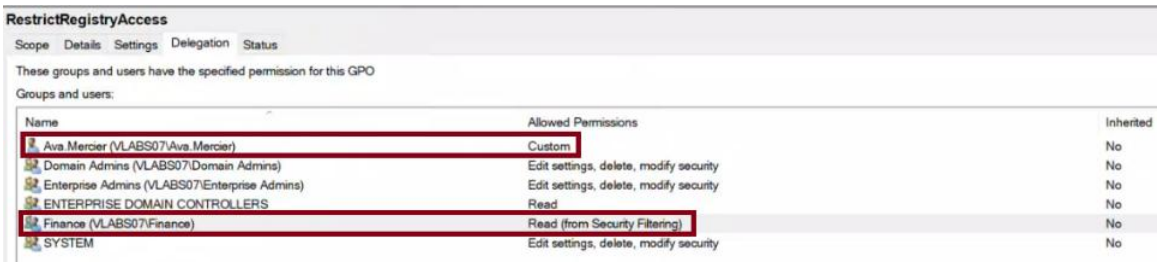




2. In the **Delegation** tab → Click **Advanced**.
   - Click **Add** → Type: Ava Mercier → Click OK.
   - In the permission entries, find Ava Mercier → Check **Deny** under **Apply group policy**.
   - Click OK to close the window.







This setup ensures the GPO applies to all members of the Finance group, except Ava Mercier, without needing to create a separate group.

Optional Alternative – Group-Based Filtering Without Delegation

Instead of **using** the Delegation tab, you can:
- Create a new group (e.g., Finance-ExcptAva)
- Add all Finance users *except* Ava Mercier to this group
- Add only this group to the Security Filtering list

Pros and Cons:

Delegation + Deny
- Fast and doesn't require creating extra groups
- Useful **for** quickly excluding individual users
- Clear override **using** built-in permissions

Downside:
- "Deny" entries can cause confusion **if** misused or stacked

Group-based filtering
- More scalable and visible **in** enterprise environments

Downside:
- Requires group management **in** AD (create + maintain additional group)

Either method is valid. **In** this lab, I used Delegation **for** simplicity and to avoid creating unnecessary AD groups.

Step 6 – Testing the GPO from Client07

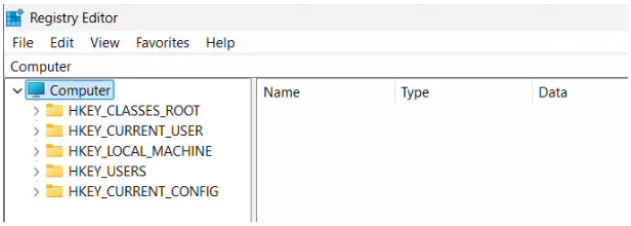
Log in to **Client07** as **Ava Mercier**.
Open Command Prompt → run: `gpupdate /force`
Press Windows + R → type: **regedit** → Press Enter
Registry Editor should open normally, as the GPO is denied for her.

```
OS Configuration:            Member Workstation
OS Version:                  10.0.26100
Site Name:                   N/A
Roaming Profile:             N/A
Local Profile:               C:\Users\Ava.Mercier
Connected over a slow link?: No


USER SETTINGS
-------------
    CN=Ava Mercier,OU=Finance,DC=vlabs07,DC=com
    Last time Group Policy was applied: 5/21/2025 at 12:34:37 PM
    Group Policy was applied from:      DC207.vlabs07.com
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        VLABS07
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    ----------------------------
        N/A

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

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

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

Note: If changes are not applied, use `gpupdate /force` on **DC207** to ensure replication from DC107 is up to date.

```
PS C:\Users\Administrator.VLABS07> gpupdate /force
Updating policy...

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



Final Note – Why Using "Authenticated Users" Initially Matters

When a new GPO is created, **"Authenticated Users"** is included by default in the Security Filtering.
This ensures the GPO can apply to any domain-authenticated user in the linked OU.
Using it during initial testing helps validate the GPO works, before narrowing the scope.
If group filtering fails due to replication issues or missing permissions, reverting to "Authenticated Users" can help confirm functionality.

Task 2: Configuring Group Policy using PowerShell

System: DC107

Objective:
Disable access to the Control Panel for all users in the HR OU, except Emma Petit.
This task is performed using PowerShell cmdlets with final exclusions done in GPMC.

Step 1 – Open PowerShell as Administrator
Open PowerShell on DC107 with elevated privileges (right-click → Run as Administrator)

Step 2 – Create the GPO
This command creates a new GPO named DisableControlPanel:

```
New-GPO -Name "DisableControlPanel" -Comment "GPO to restrict access to Control Panel"
```

```
PS C:\Users\Administrator> New-GPO -Name "DisableControlPanel" -Comment "GPO to restrict access to Cont
rol Panel"


DisplayName      : DisableControlPanel
DomainName       : vlabs07.com
Owner            : VLABS07\Domain Admins
Id               : f052abe1-472d-4151-b8c4-4edda7a5562b
GpoStatus        : AllSettingsEnabled
Description      : GPO to restrict access to Control Panel
CreationTime     : 5/21/2025 9:18:59 PM
ModificationTime : 5/21/2025 9:18:59 PM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        :
```

Step 3 – Configure the GPO to Disable Control Panel
This command sets a user-level registry policy that disables the Control Panel:

```
Set-GPRegistryValue -Name "DisableControlPanel" `
-Key "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" `
-ValueName "NoControlPanel" -Type DWord -Value 1
```

```
PS C:\Users\Administrator> Set-GPRegistryValue -Name "DisableControlPanel" -Key "HKCU\Software\Microsof
t\Windows\CurrentVersion\Policies\Explorer" -ValueName "NoControlPanel" -Type DWord -Value 1


DisplayName      : DisableControlPanel
DomainName       : vlabs07.com
Owner            : VLABS07\Domain Admins
Id               : f052abe1-472d-4151-b8c4-4edda7a5562b
GpoStatus        : AllSettingsEnabled
Description      : GPO to restrict access to Control Panel
CreationTime     : 5/21/2025 9:18:59 PM
ModificationTime : 5/21/2025 9:23:48 PM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        :
```

Explanation:
- This sets NoControlPanel = 1 under the Current User registry hive
- HKCU = HKEY_CURRENT_USER → affects user-level settings
- A value of 1 disables Control Panel access

Step 4 – Link the GPO to the HR OU
This links the GPO to the HR OU **in** Active Directory:

```
New-GPLink -Name "DisableControlPanel" -Target "OU=HR,DC=vlabs07,DC=com"
```

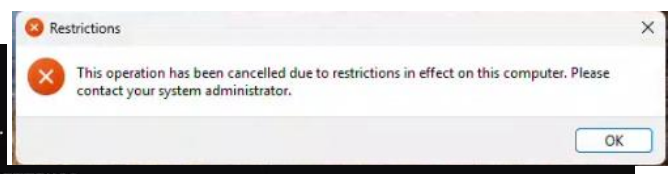
```
PS C:\Users\Administrator> New-GPLink -Name "DisableControlPanel" -Target "OU=HR,DC=vlabs07,DC=com"


GpoId       : f052abe1-472d-4151-b8c4-4edda7a5562b
DisplayName : DisableControlPanel
Enabled     : True
Enforced    : False
Target      : OU=HR,DC=vlabs07,DC=com
Order       : 1
```

Note:
Replace the domain portion (DC=vlabs07,DC=com) **if** your domain name differs.

Step 5 – Initial Testing (Keep Authenticated Users)
Leave "Authenticated Users" **in** the GPO's Security Filtering **for** now.
This ensures the GPO applies broadly **for** testing and is easier to troubleshoot.

Step 6 – Test the GPO
Log **in** as a regular HR user (not Emma Petit)
Run: gpupdate /force
Open the Control Panel → It should be blocked
Run: gpresult /r → Confirm the GPO is listed under Applied Group Policies

```
C:\Users\Tess.Dupuy>gpupdate /force
Updating policy...

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




```
C:\Users\Tess.Dupuy>gpresult /r
```

```
USER SETTINGS
-------------
    CN=Tess Dupuy,OU=HR,DC=vlabs07,DC=com
    Last time Group Policy was applied: 5/21/2025 at 6:42:50 PM
    Group Policy was applied from:      DC207.vlabs07.com
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        VLABS07
    Domain Type:                        Windows 2008 or later

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

Step 7 – Add HR Group (Keep Authenticated Users for Now)
Add the HR group to the GPO's permissions so they are authorized to receive it:

```
Set-GPPermission -Name "DisableControlPanel" -TargetName "HR" `
-TargetType Group -PermissionLevel GpoApply
```

```
PS C:\Users\Administrator> Set-GPPermission -Name "DisableControlPanel" -TargetName "HR" -TargetType Gr
oup -PermissionLevel GpoApply


DisplayName      : DisableControlPanel
DomainName       : vlabs07.com
Owner            : VLABS07\Domain Admins
Id               : f052abe1-472d-4151-b8c4-4edda7a5562b
GpoStatus        : AllSettingsEnabled
Description      : GPO to restrict access to Control Panel
CreationTime     : 5/21/2025 9:18:59 PM
ModificationTime : 5/21/2025 9:23:48 PM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        :
```

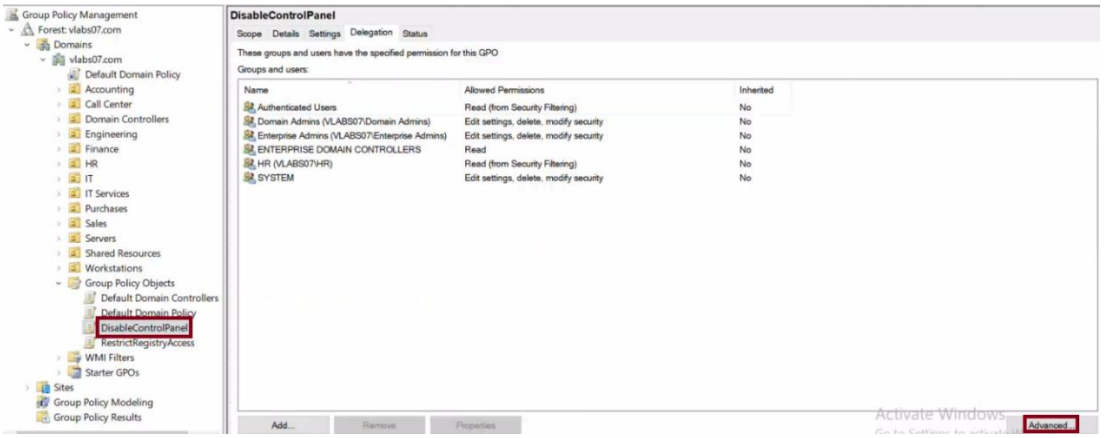
Step 8 – Exclude Emma Petit **Using** Delegation **(**GUI Required**)**

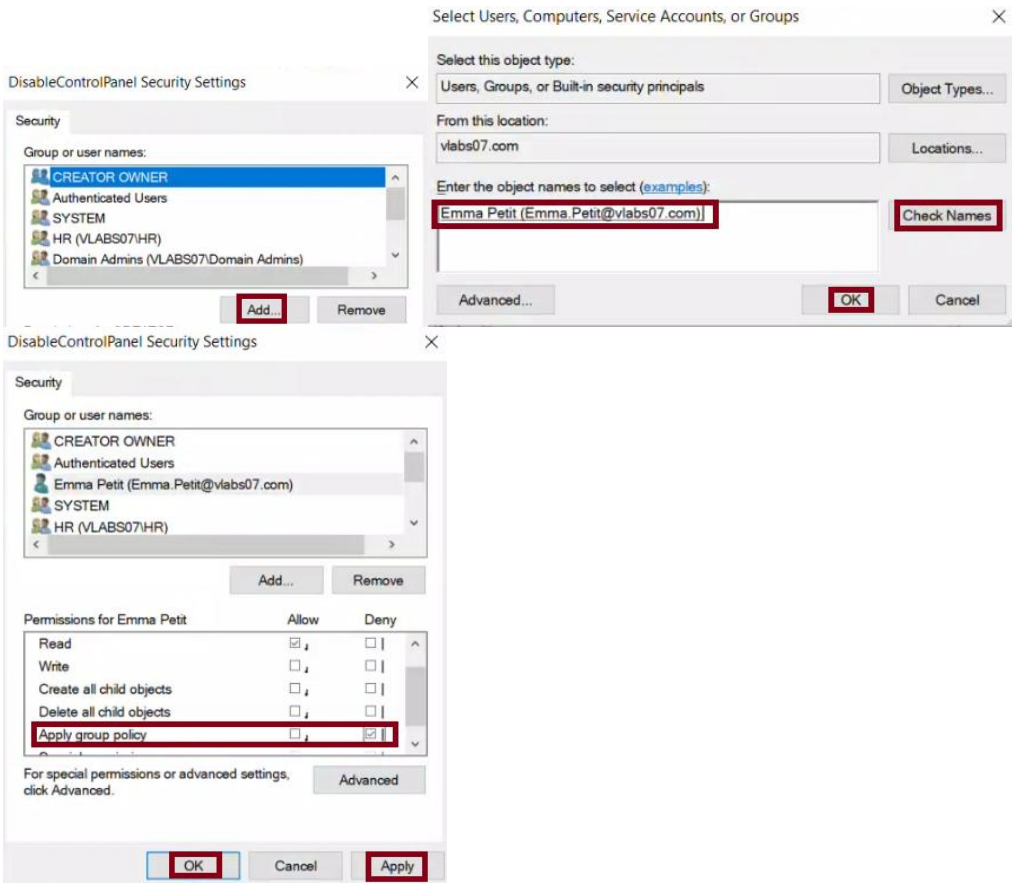
Note: PowerShell does not support applying explicit **"Deny Apply Group Policy"** permissions on GPOs.
This action must be done through the **Group Policy Management Console (GPMC)** **using** the Delegation tab.

PowerShell's `Set-GPPermission -PermissionLevel None` only removes existing Allow entries,
but does **not create a Deny**, so it cannot guarantee exclusion from the GPO.

To exclude Emma properly, follow these steps **in** the GUI:

1. Open **GPMC** → Select the **DisableControlPanel** GPO
2. Go to the **Delegation tab** → Click **Advanced**
3. Click **Add** → Enter: Emma Petit → Click OK
4. **In** the permission list, select **Emma Petit**
5. Check **Deny** **for** **Apply group policy**
6. Click OK to save



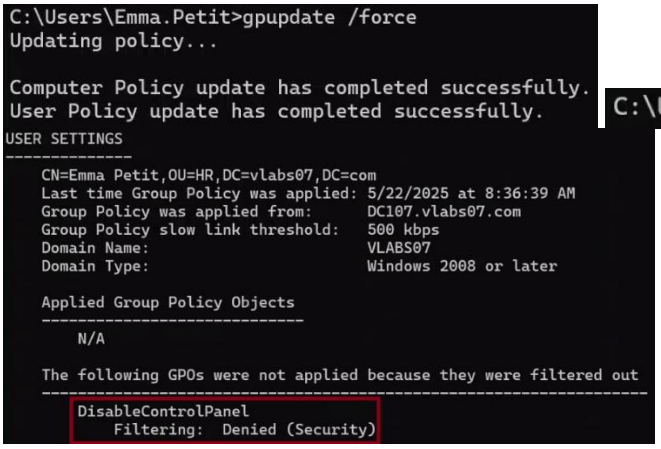


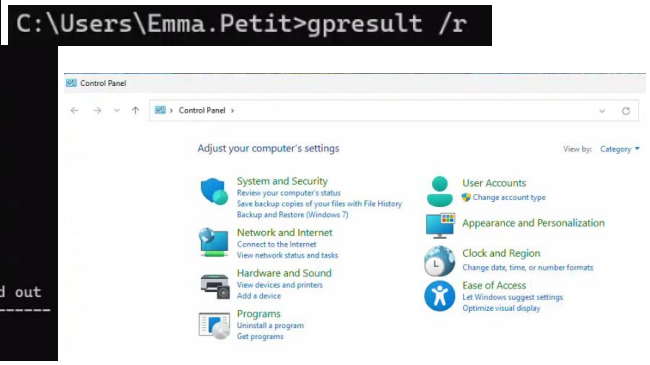
This ensures the GPO will **not apply to Emma Petit**, even though she is part of the HR group.

Note: Advanced PowerShell methods **using** ADSI and raw ACLs can technically apply Deny permissions, but they are complex and not beginner friendly.

Step 9 – Final Testing

Log **in** as Emma Petit
Run: gpupdate **/**force
Open Control Panel → It should open normally
Run: gpresult **/**r → GPO should NOT appear under Applied Group Policies





Step 10 - Finalize Security Filtering (Remove Authenticated Users)
==========

Objective:

Now that testing is successful and the GPO works correctly **for** the HR group **(**with Emma Petit excluded via Deny**),**
we remove "Authenticated Users" from the GPOs permission list **using** PowerShell**.**

Explanation:

The command below uses Set-GPPermission to remove any permissions that "Authenticated Users" has on the GPO**.**
This finalizes the GPO so it only applies to the HR group**,** not to all domain users**.**

```
PS C:\Users\Administrator> Set-GPPermission -Name "DisableControlPanel" -TargetName "Authenticated User
s" -TargetType Group -PermissionLevel None
```

```
Set-GPPermission -Name "DisableControlPanel" `
                 -TargetName "Authenticated Users" `
                 -TargetType Group `
                 -PermissionLevel None
```

Command Breakdown:

- Set-GPPermission **:** Cmdlet used to change security filtering or delegation permissions on a GPO
- **-**Name "DisableControlPanel" **:** Specifies the name of the GPO
- **-**TargetName "Authenticated Users" **:** The security principal **(**group**)** to remove
- **-**TargetType Group **:** Specifies that the target is a group
- **-**PermissionLevel None **:** Removes existing permission **(**Read**/**Apply**)** without assigning any new ones

Result:

"Authenticated Users" will no longer be able to read or apply the GPO**.**
The policy will now apply only to members of the HR group **(**excluding Emma Petit via explicit Deny**).**

Step 11 - Verification (Confirm Removal of "Authenticated Users")
==========

Objective:

Ensure that "Authenticated Users" no longer has permission to apply the GPO named "DisableControlPanel".

This script checks the GPOs permissions (ACL) **using** its LDAP path and filters **for** any remaining access entries **for** "Authenticated Users".

Get the GPO object
```
$gpo = Get-GPO -Name "DisableControlPanel"
```

```
PS C:\Users\Administrator> $gpo = Get-GPO -Name "DisableControlPanel"
```

Build the LDAP path to the GPO object
```
$path = "LDAP://$($gpo.Path)"
```

```
PS C:\Users\Administrator> $path = "LDAP://$($gpo.Path)"
```

Check for any permission entries assigned to Authenticated Users
```
([ADSI]$path).psbase.ObjectSecurity.Access |
    Where-Object { $_.IdentityReference -match "Authenticated Users" }
```

```
PS C:\Users\Administrator> ([ADSI]$path).psbase.ObjectSecurity.Access | Where-Object { $_.IdentityRefer
ence -match "Authenticated Users" }
PS C:\Users\Administrator>
```

Command Breakdown:

$gpo = Get-GPO -Name "DisableControlPanel"
- Retrieves the GPO object by name.

$path = "LDAP://$($gpo.Path)"
- Constructs the LDAP path to the GPO object so we can access it via ADSI.

([ADSI]$path)
- Connects to the GPO object **in** Active Directory **using** ADSI (Active Directory Service Interfaces).

.psbase.ObjectSecurity.Access
- Accesses the list of ACEs (Access Control Entries) associated with the GPO object.

Where-Object { $_.IdentityReference -match "Authenticated Users" }
- Filters the ACE list to check **if** any entry is assigned to "Authenticated Users".

Expected Output:

- **If** no result is returned: "Authenticated Users" was successfully removed.
- **If** an ACE is shown: They still have permissions, and Step 10 needs to be repeated.

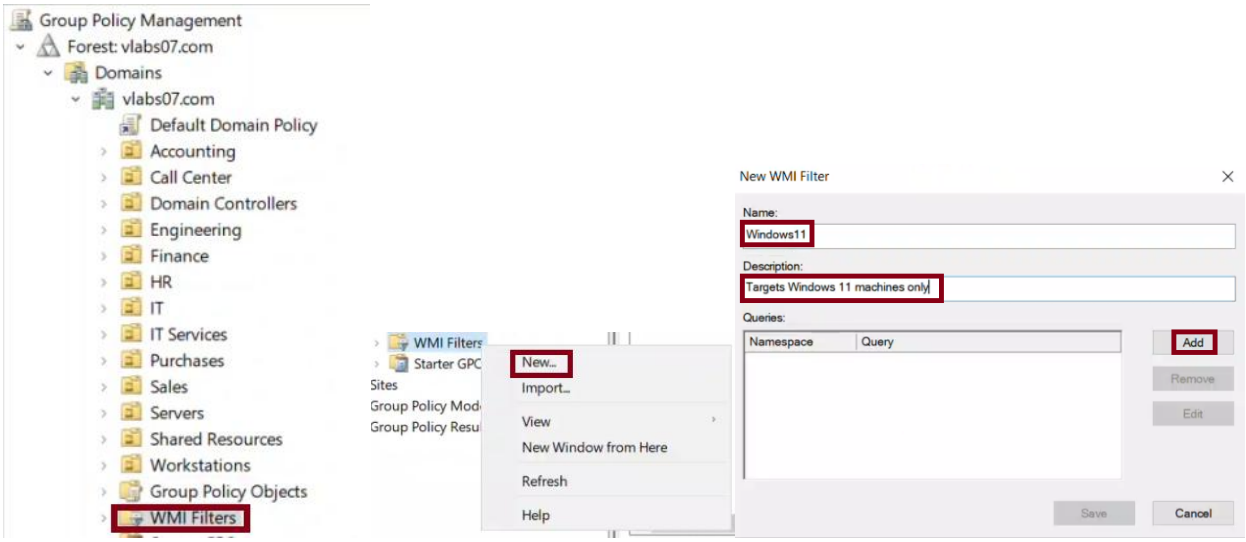
Task 3 – Creating and Testing a WMI **Filter for** Windows 11 **(GUI)**

System: DC107

Objective:

Create a WMI **filter** that targets only Windows 11 systems, attach it to a new GPO called "NoRecycleBin",
and configure this GPO to remove the Recycle Bin from the desktop. The GPO should only apply to computers
in the Call Center OU running Windows 11.

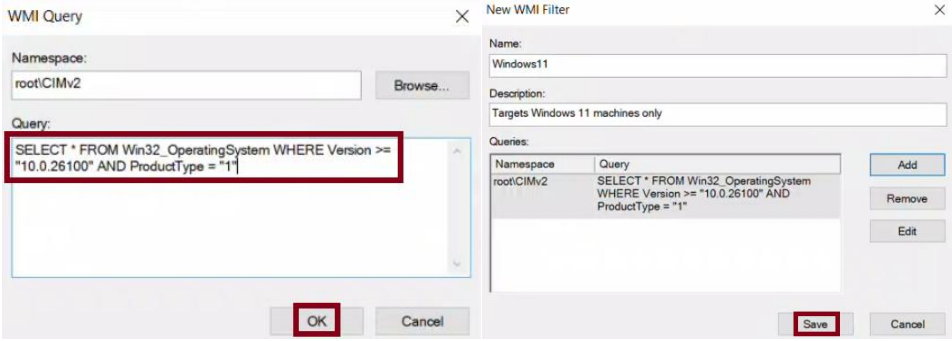
Step 1 – Create WMI Filter (GUI Only)
Open GPMC on DC107:
1. **In** the left pane, right-click on "WMI Filters" → Click "New..."
2. Name: Windows11
3. Description: Targets Windows 11 machines only
4. Click "Add" to define a query:



WMI Query:
SELECT * FROM Win32_OperatingSystem WHERE Version >= "10.0.26100" AND ProductType = "1"

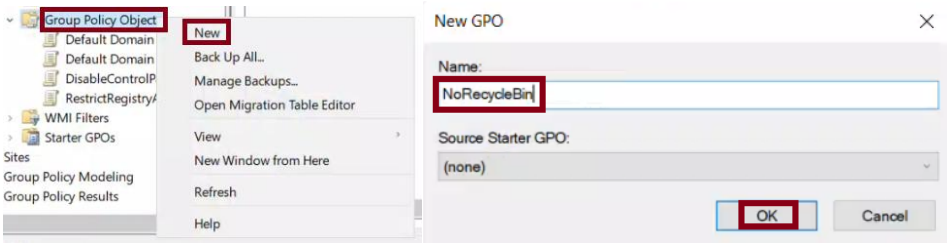
- Version >= "10.0.26100" → Targets Windows 11 and newer
- ProductType = "1" → Ensures its a client OS (not server)

Click OK → Save the **filter**



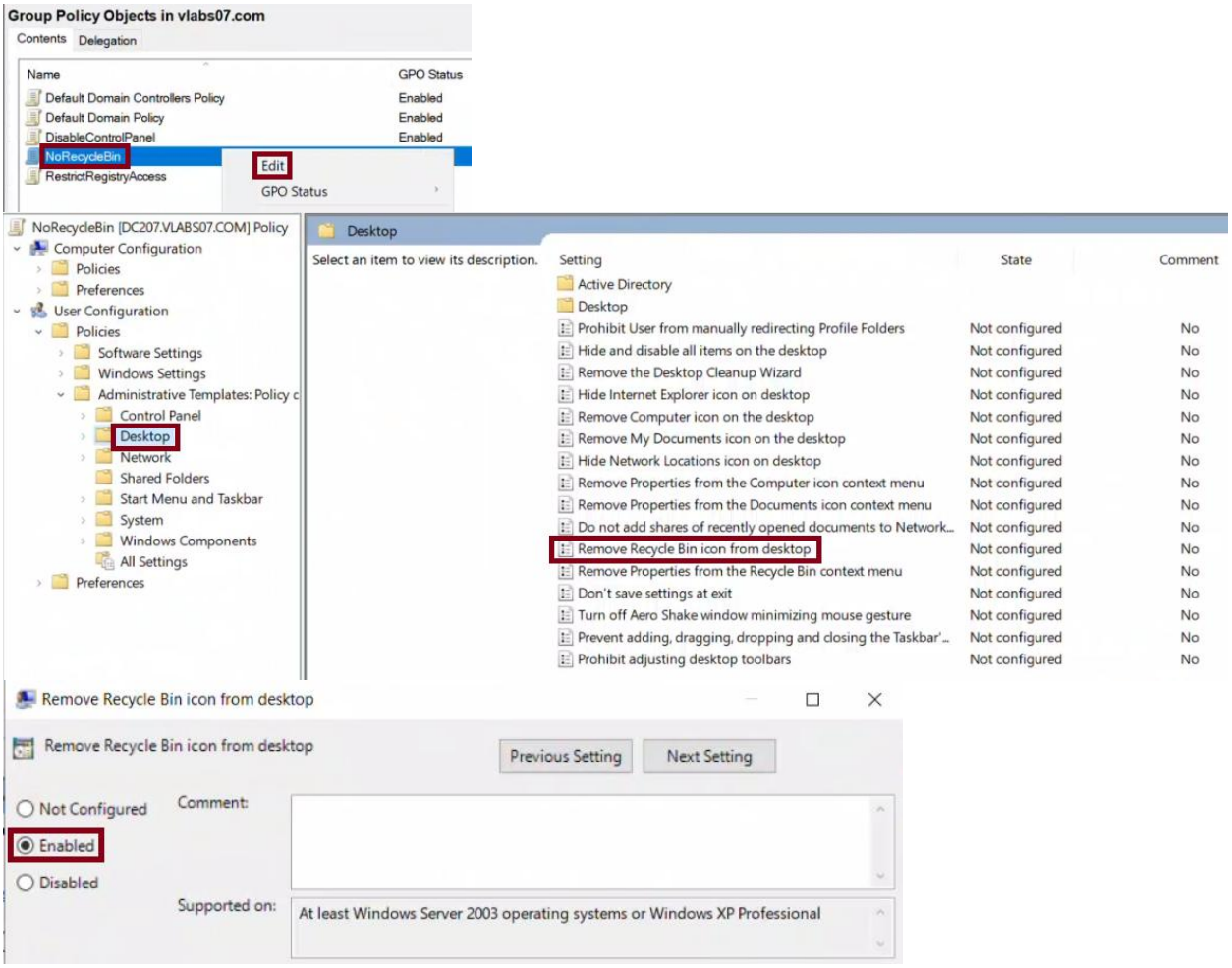
Step 2 – Create GPO named "NoRecycleBin"

1. **In** GPMC → Right-click "Group Policy Objects" → New
2. Name: NoRecycleBin → Click OK



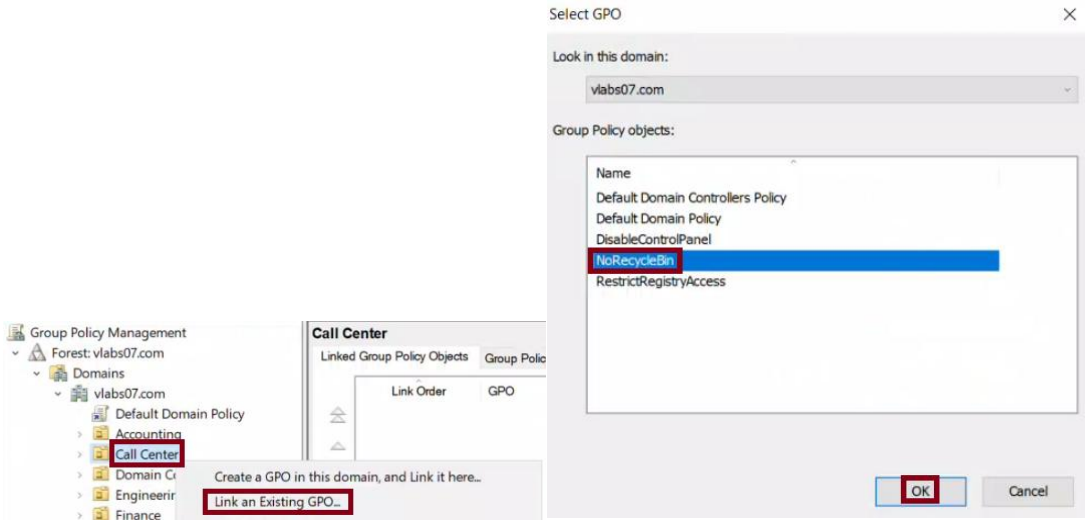
Step 3 – Edit the GPO to remove Recycle Bin from desktop

1. Right-click the "NoRecycleBin" GPO → Click "Edit"
2. Navigate to:
   User Configuration → Administrative Templates → Desktop
3. Double-click: Remove Recycle Bin icon from desktop
4. Set to: Enabled → Click Apply → OK
5. Close the Group Policy Editor



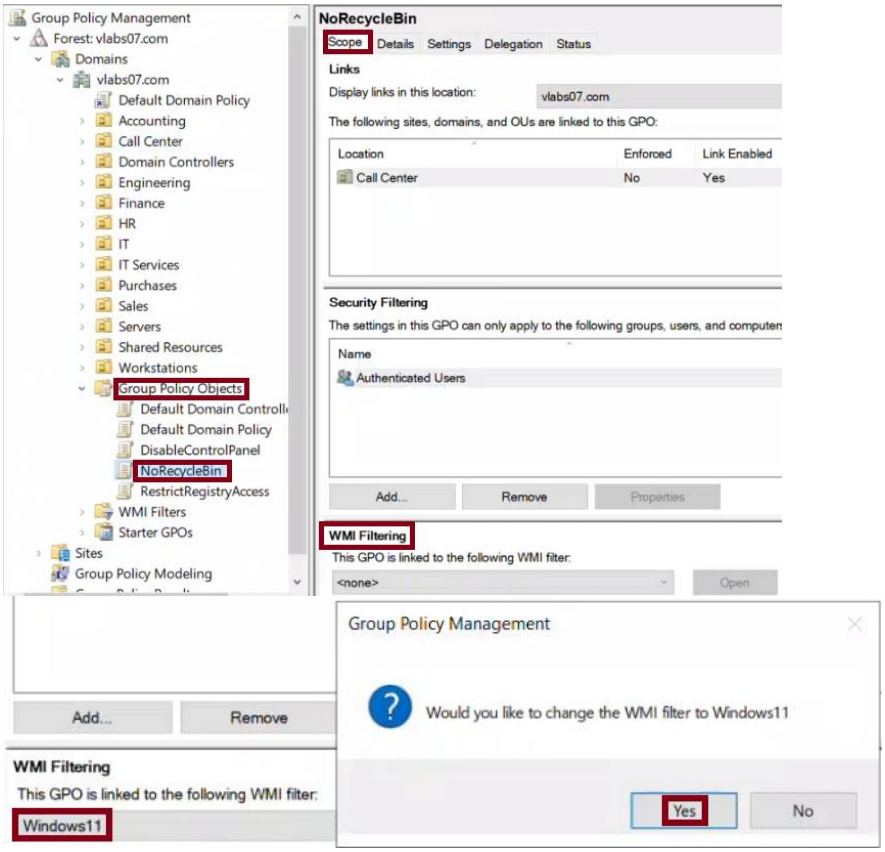
Step 4 – Link GPO to the Call Center OU

1. **In** GPMC, locate the "Call Center" OU
2. Right-click → Link an Existing GPO → Choose: NoRecycleBin → Click OK



Step 5 – Link the WMI Filter to the GPO

1. **In** GPMC, click once on the "NoRecycleBin" GPO under Group Policy Objects
2. **In** the right pane, look at the bottom section labeled "WMI Filtering"
3. Click "None" → Select the WMI **Filter:** Windows11 → Click Yes to confirm



Step 6 – Testing from Client07

On Client07 (must be running Windows 11):

1. Log in with any user from the Call Center OU
2. Open Command Prompt → Run:
   gpupdate /force

```
C:\Users\Leo.Barre>gpupdate /force
Updating policy...

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

```
C:\Users\Leo.Barre>gpresult /r

USER SETTINGS
--------------
    CN=Leo Barre,OU=Call Center,DC=vlabs07,DC=com
    Last time Group Policy was applied: 5/22/2025 at 9:59:19 AM
    Group Policy was applied from:      DC207.vlabs07.com
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        VLABS07
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    ----------------------------
        NoRecycleBin

    The following GPOs were not applied because they were filtered out
    ------------------------------------------------------------------
        Local Group Policy
            Filtering:  Not Applied (Empty)
```

3. Log off and log back in
4. Verify that the Recycle Bin icon is removed from the desktop

Note: If testing on non-Windows 11 systems, the GPO should NOT apply due to the WMI filter.

Task 4 – Practicing GPO Processing Order (GUI)

System: DC107

Objective:

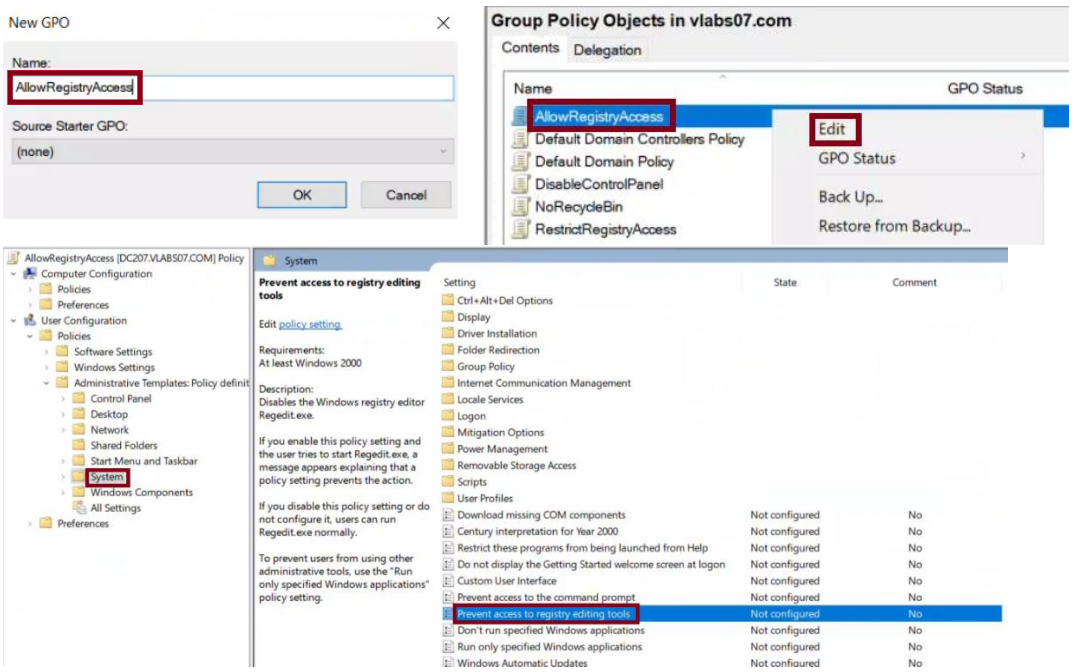
Understand how GPO link order, precedence, enforcement, and inheritance affect GPO application
by applying different configurations step-by-step and observing their effects on a test user.

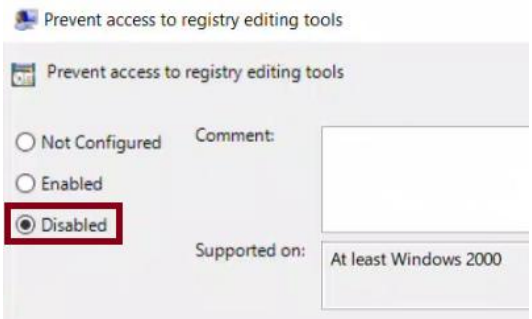
Test user: Eden Morin (used in all steps for consistent observation)
OUs involved:
- Finance
- Finance-Admins (child OU of Finance)

GPOs involved:
- RestrictRegistryAccess (blocks access to regedit)
- AllowRegistryAccess (grants access to regedit)

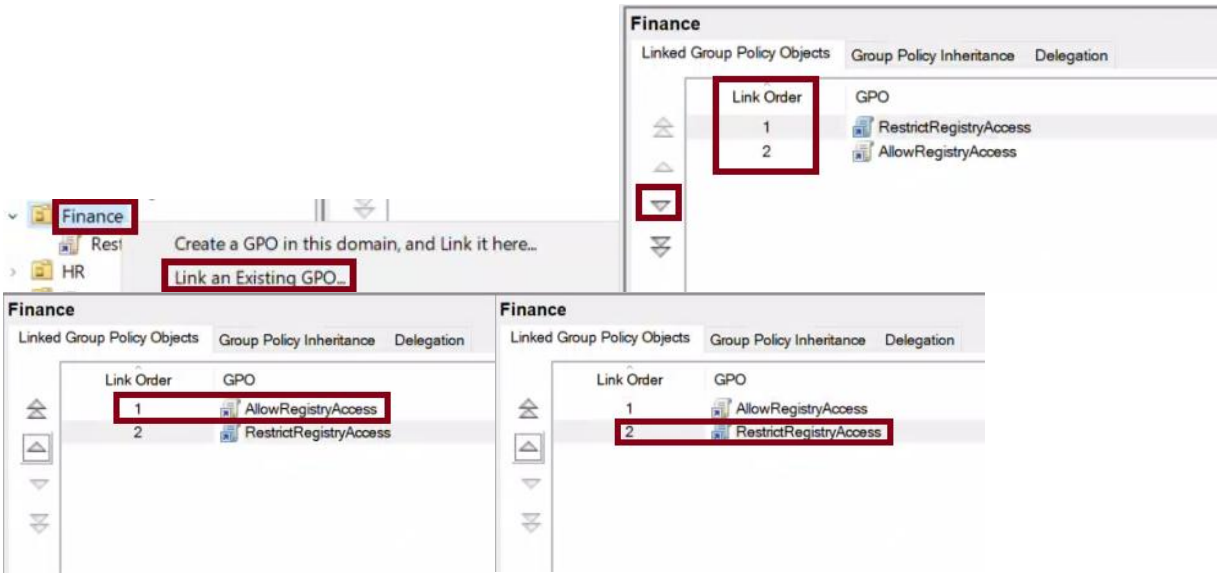
Part A – Link Order (Lower Number = Higher Priority)

1. Create a new GPO named: AllowRegistryAccess
2. Edit the GPO:
   - Go to: User Configuration → Administrative Templates → System
   - Enable: Prevent access to registry editing tools → Set to "Not Configured" or "Disabled"
     (This grants access to regedit)

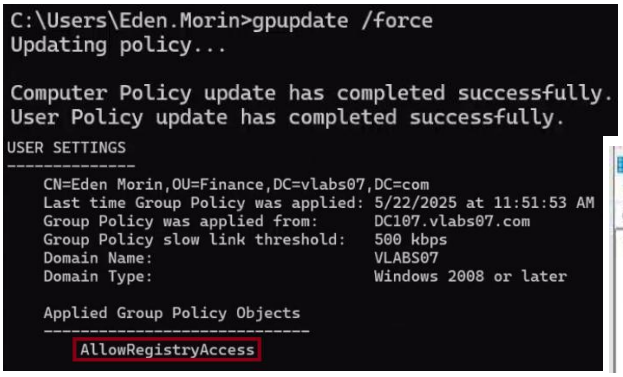


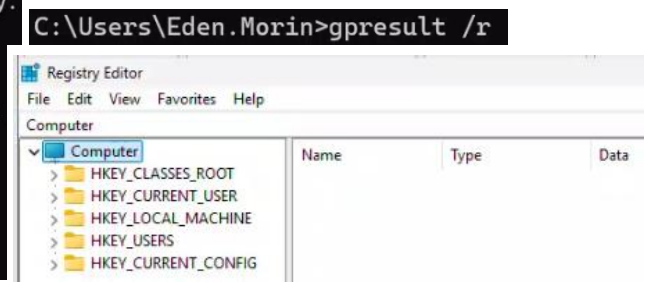


3. Link AllowRegistryAccess to the "Finance" OU
4. **In** GPMC, go to the Finance OU → Under Linked GPOs, make sure AllowRegistryAccess has **Link Order 1**
5. Confirm that RestrictRegistryAccess is still linked with order 2 **(if** it exists**)**



Test:
- Log **in** to Client07 as Eden Morin **(**a user **in** the Finance OU**)**
- Run: gpupdate **/**force
- Press Win**+**R → type**:** regedit → You should be able to open the registry



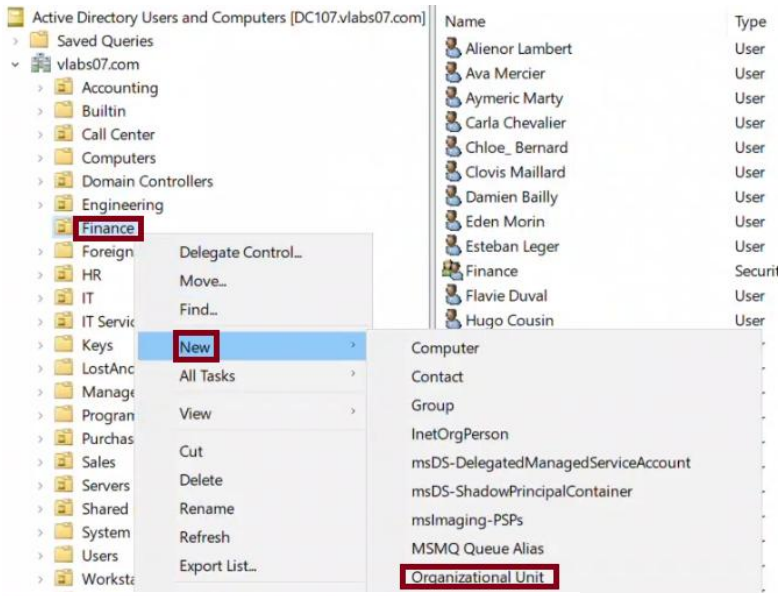


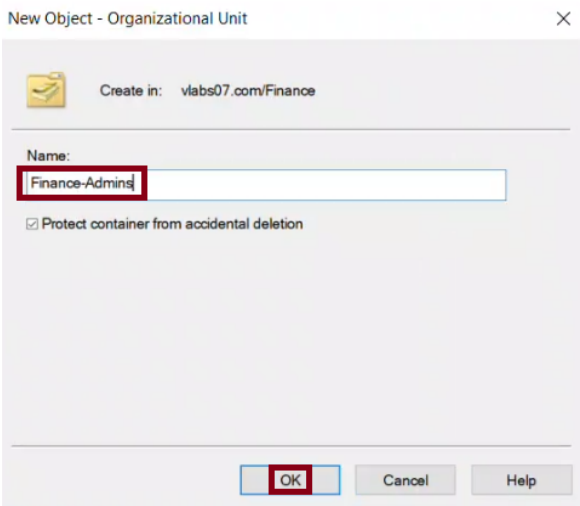
Part B – Precedence Rules (Child OU GPOs override Parent GPOs)

Goal:
Move Eden Morin to a sub-OU (Finance-Admins) and apply a conflicting GPO (RestrictRegistryAccess)
directly to the child OU to observe how child-level GPOs take precedence.

Step 1 – Create the child OU:

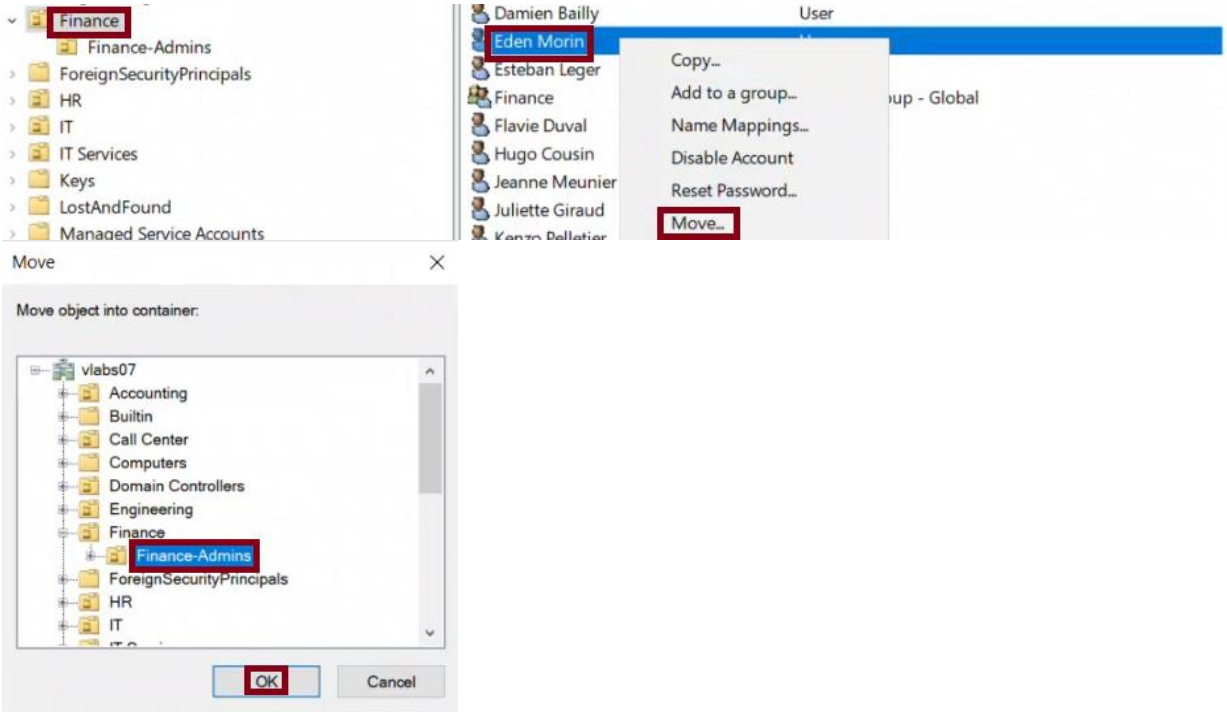
1. Open Active Directory Users and Computers (ADUC)
2. Navigate to your domain > OU: Finance
3. Right-click Finance → New → Organizational Unit → Name it: Finance-Admins → Click OK





Step 2 – Move Eden Morin to Finance-Admins:

1. In ADUC, locate user Eden Morin
2. Right-click Eden Morin → Click "Move"
3. Browse to: Finance → Finance-Admins → Click OK

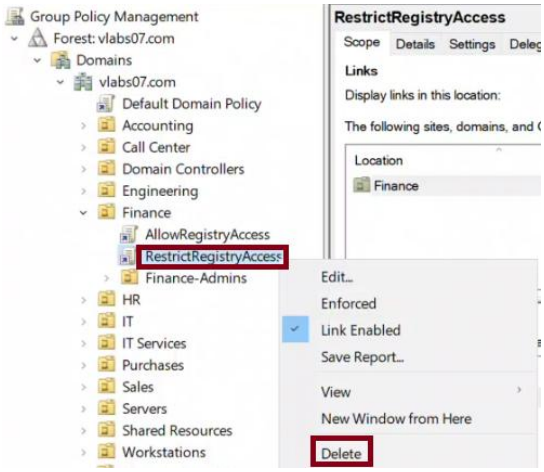


Step 3 – Unlink the RestrictRegistryAccess GPO from Finance

Objective:

To remove the RestrictRegistryAccess GPO from the Finance OU completely (not just disable it), so it no longer applies to users in that OU.

Instructions:
---
1. Open Group Policy Management Console (GPMC) on DC107
2. In the left pane, expand:
   Domains → vlabs07.com → Finance
3. In the right pane under "Linked Group Policy Objects":
   - Locate the GPO: RestrictRegistryAccess
   - Right-click it → Click **Remove**
   - Click **Yes** to confirm the removal of the link



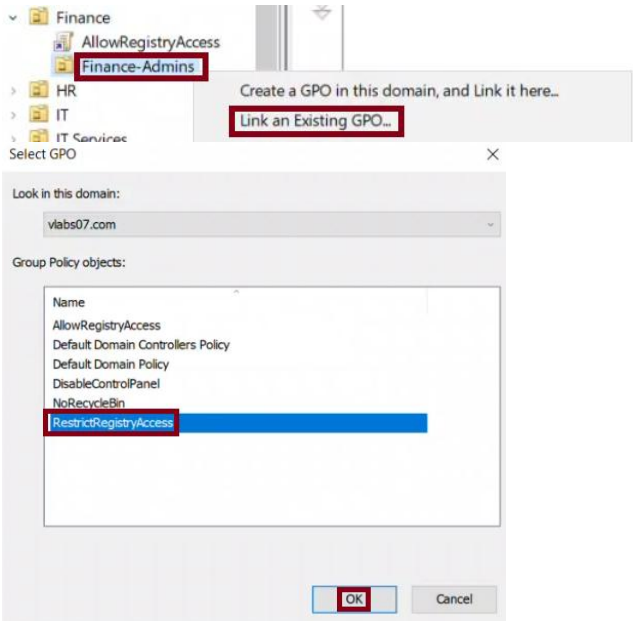
Note:

This does NOT delete the GPO itself. It only removes its link from the Finance OU.

You will still be able to link the same GPO later to another OU (e.g., Finance-Admins).

Step 4 – Link RestrictRegistryAccess to Finance-Admins:

1. In GPMC, expand Finance → Select Finance-Admins
2. Right-click → Click "Link an Existing GPO"
3. Choose: RestrictRegistryAccess → Click OK



Step 5 – Test from Client:

1. Log in to Client07 as Eden Morin
2. Open CMD and run:
   gpupdate /force
3. Try opening regedit (Win+R → regedit)

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

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

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

```
USER SETTINGS
--------------
    CN=Eden Morin,OU=Finance-Admins,OU=Finance,DC=vlabs07,DC=com
    Last time Group Policy was applied: 5/22/2025 at 4:38:50 PM
    Group Policy was applied from:      DC207.vlabs07.com
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        VLABS07
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    ----------------------------
        RestrictRegistryAccess
        AllowRegistryAccess
```

Expected Result:
Access should be blocked (child GPO overrides parent)

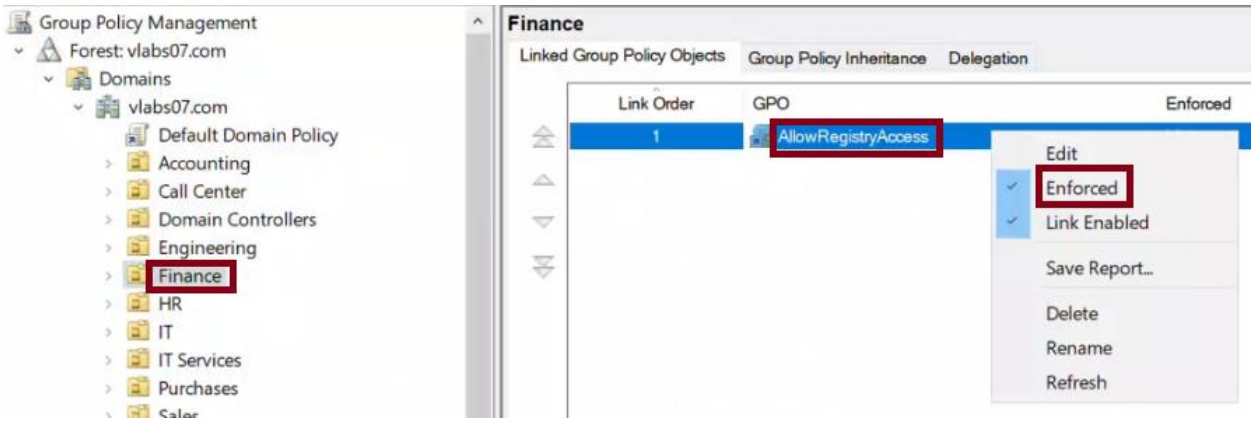
Part C – Enforced GPO (Parent GPO overrides child-level GPOs)

Goal:
Enforce the parent GPO AllowRegistryAccess so it applies to all child OUs, even if a conflicting GPO exists.

Step 1 – In GPMC, go to:
Domain > Finance → In the right pane, locate AllowRegistryAccess

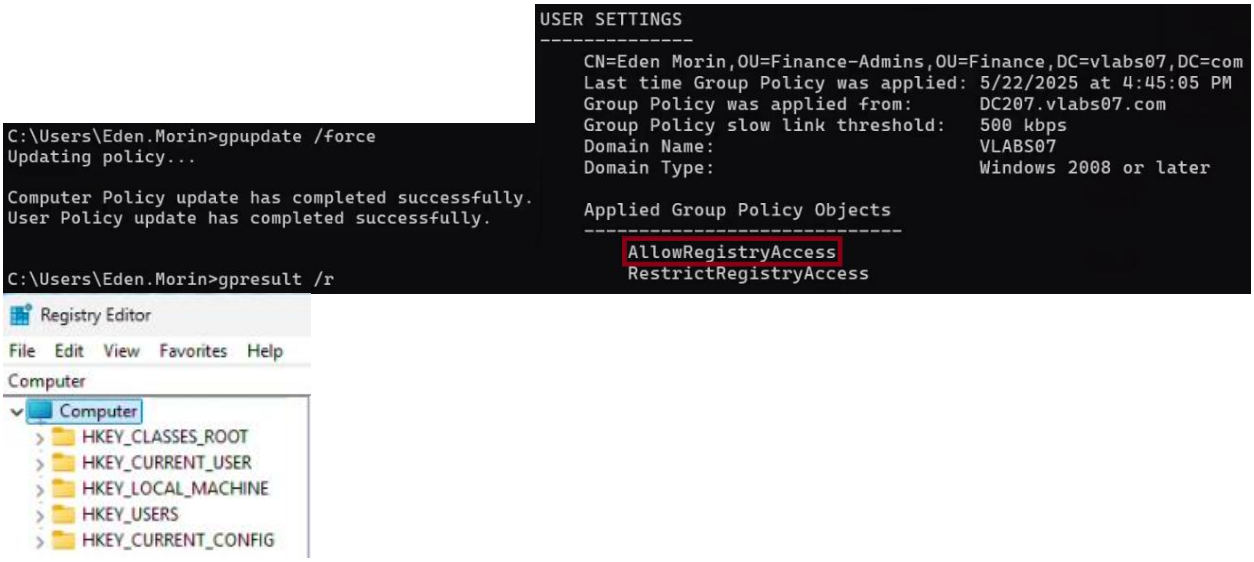
Step 2 – Enforce the GPO:

1. Right-click AllowRegistryAccess → Click "Enforced"
2. Confirm the small lock icon appears next to it



Step 3 – Test from Client:

1. Log in to Client07 as Eden Morin
2. Run: gpupdate /force
3. Launch regedit



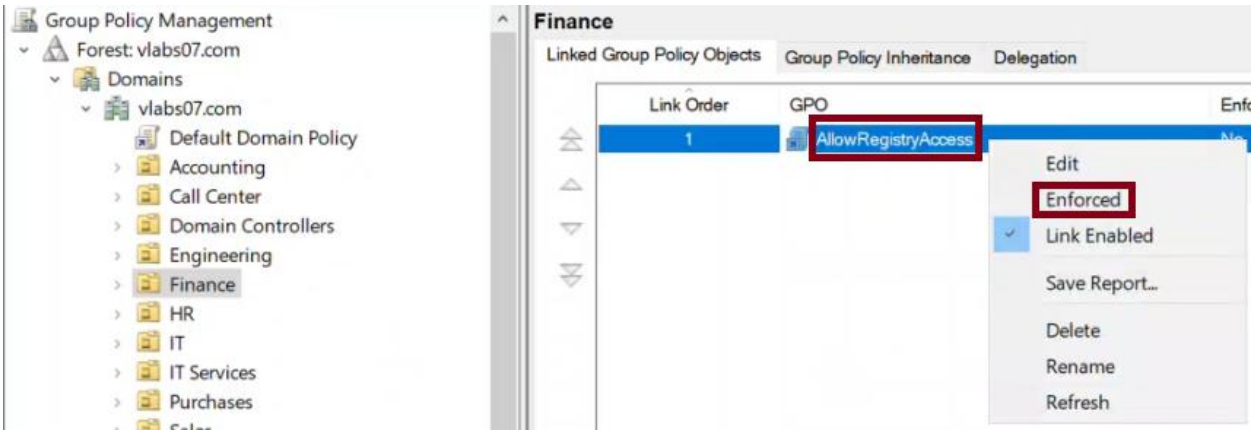
Expected Result:
Access should now be allowed due to the Enforced parent GPO taking precedence

Part D – Block Inheritance (Child OU blocks parent GPOs)

Goal:
Undo enforcement and block GPO inheritance in the Finance-Admins OU.

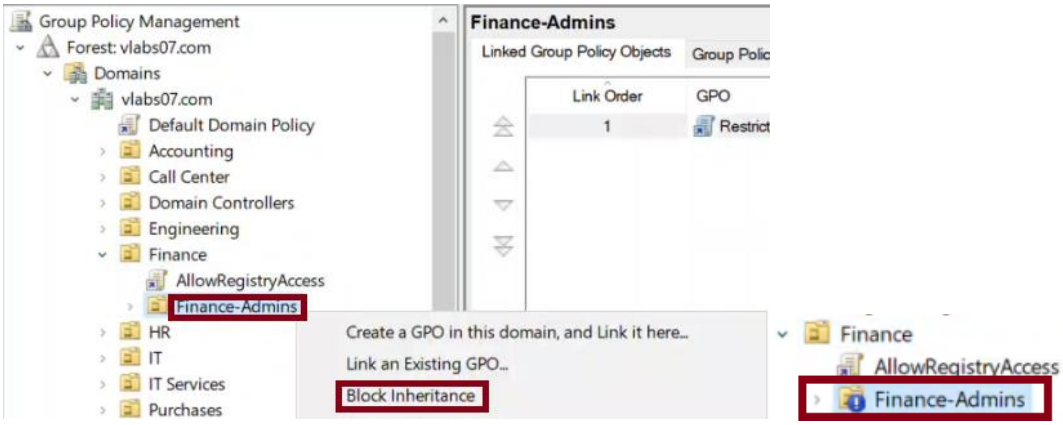
Step 1 – Remove enforcement from AllowRegistryAccess:

1. In GPMC, go to Domain > Finance
2. Right-click AllowRegistryAccess → Uncheck "Enforced"



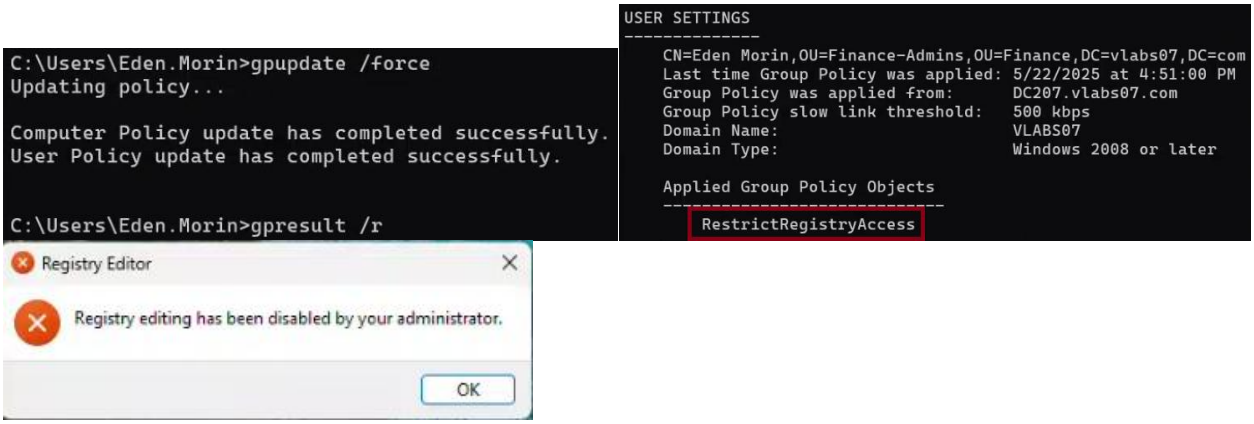
Step 2 – Block inheritance in Finance-Admins:

1. In GPMC, go to Domain > Finance > Finance-Admins
2. Right-click Finance-Admins → Click "Block Inheritance"
3. A blue arrow should appear on the OU icon



Step 3 – Test from Client:

1. Log in to Client07 as Eden Morin
2. Run: gpupdate /force
3. Launch regedit



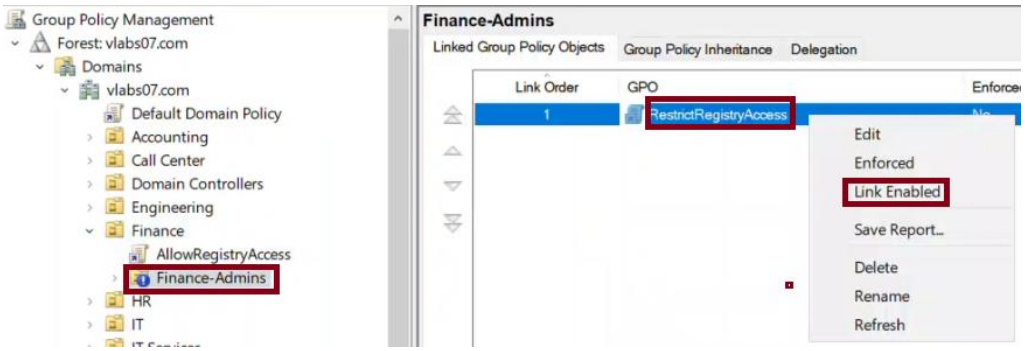
Expected Result:
Access should be blocked (child OU blocked inheritance from Finance and RestrictRegistryAccess remains linked)

Part E – Link Enabled (Temporarily disable a GPO without removing it)

Goal:
Disable the RestrictRegistryAccess GPO temporarily without removing the link.

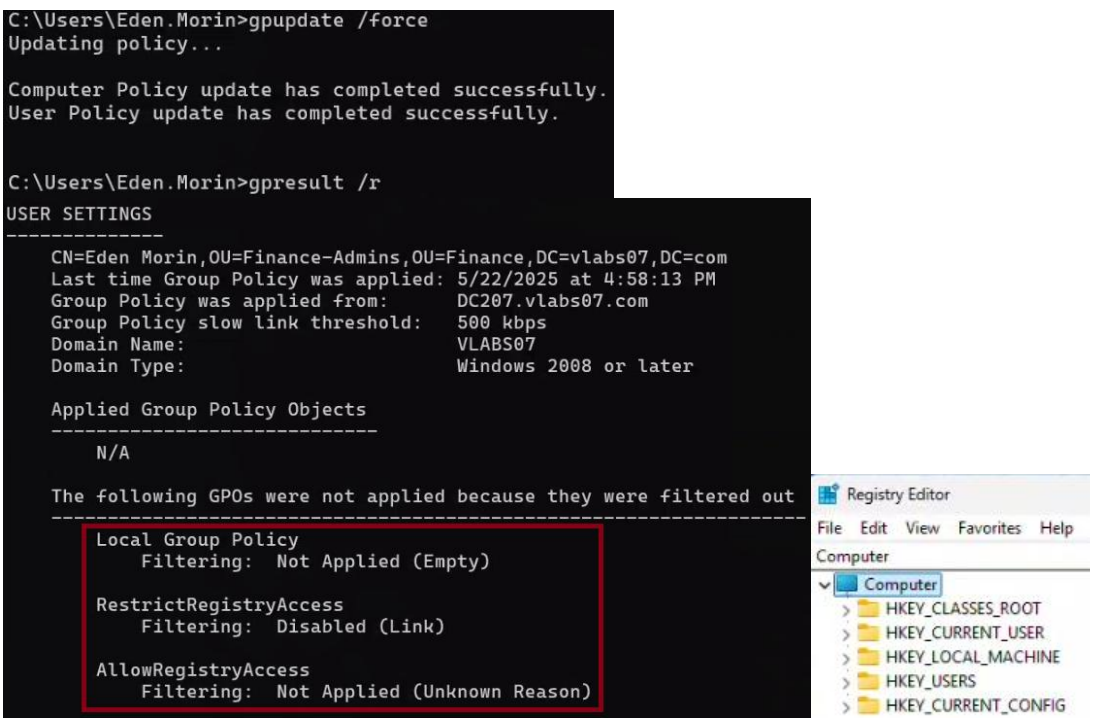
Step 1 – Disable the link:

1. In GPMC, go to Domain > Finance > Finance-Admins
2. Under "Linked Group Policy Objects", find RestrictRegistryAccess
3. Right-click it → Uncheck "Link Enabled"



Step 2 – Test from Client:

1. Log in to Client07 as Eden Morin
2. Run: gpupdate /force
3. Launch regedit



Expected Result:
Access should now be allowed (RestrictRegistryAccess is disabled and no other GPO blocks regedit)

Task 5 – Exploring Default Group Policy Objects (GUI)

System: DC107

Objective:

To review and analyze the configuration and intended purpose of the two default GPOs:
- Default Domain Policy
- Default Domain Controllers Policy

This task helps understand their role in security and domain-wide behavior,

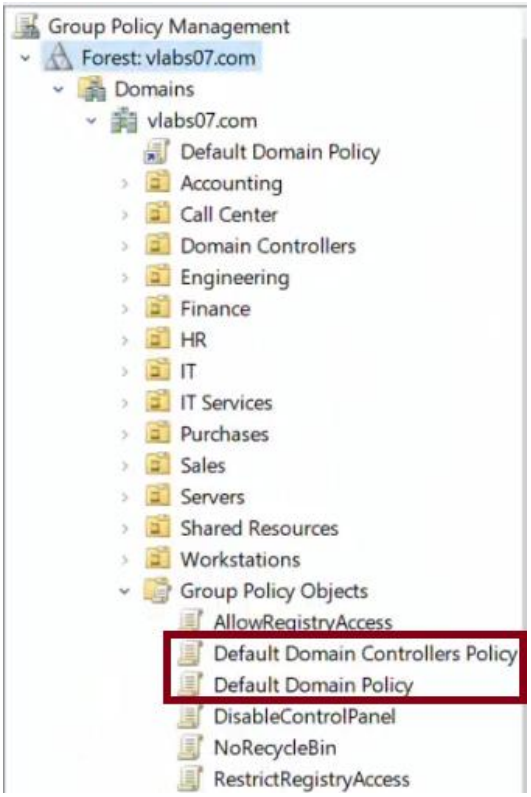
Step 1 – Identify the Two Default GPOs

1. Open Group Policy Management Console (GPMC):
   - Tools → Group Policy Management
   - Or press Win+R → type `gpmc.msc` → Press Enter

2. In the left pane, expand:
   - Forest: vlabs07.com
   - Domains → vlabs07.com

3. Scroll down and expand the container named: **Group Policy Objects**

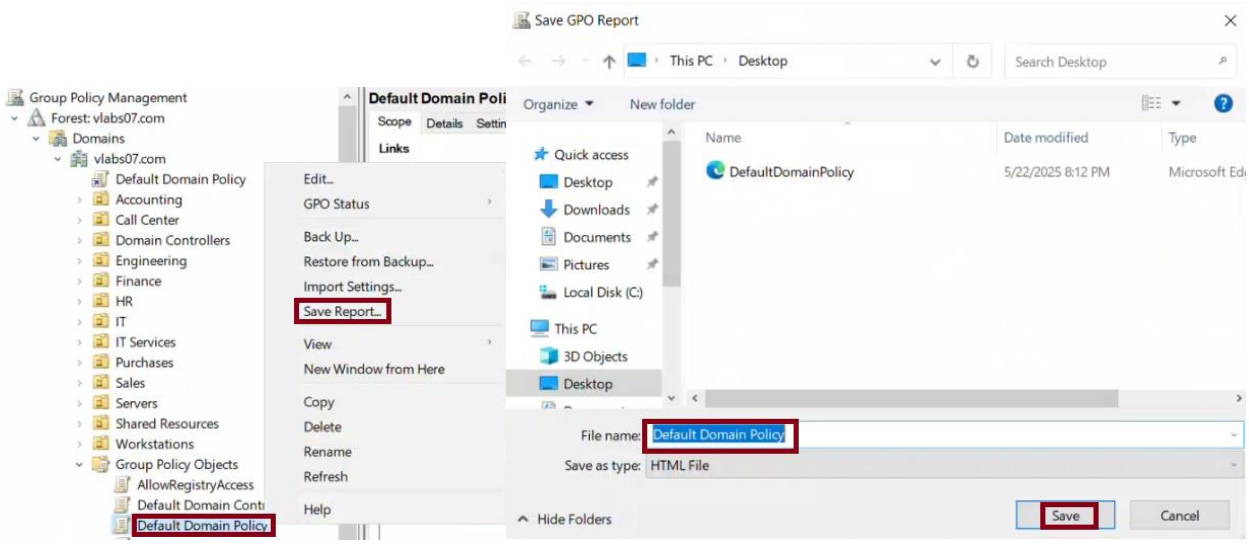
4. Locate the two default policies:
   - **Default Domain Policy**
   - **Default Domain Controllers Policy**



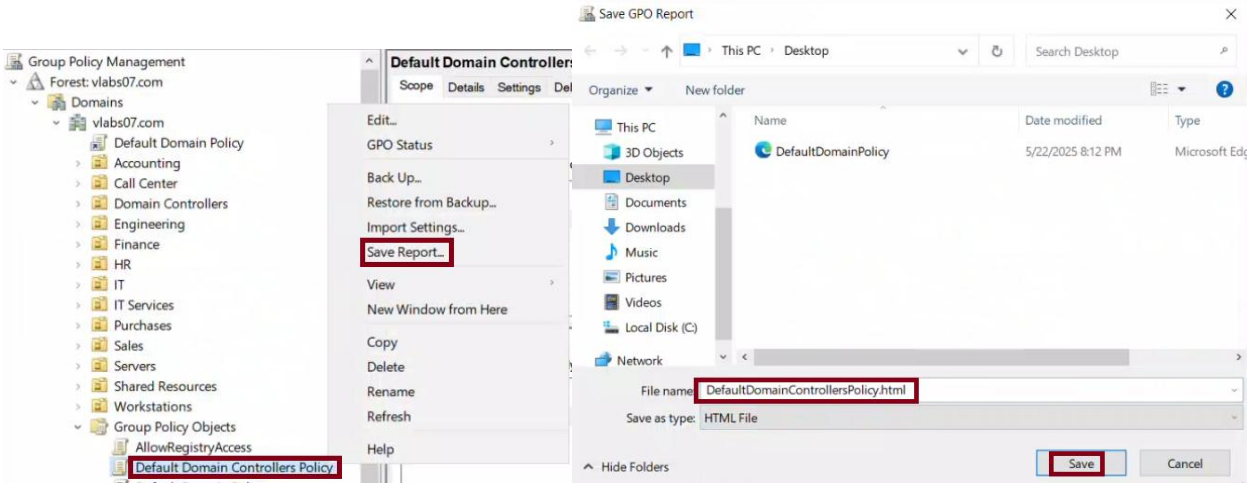
Step 2 – Generate a Settings Report for Both GPOs

Purpose:
Generate HTML reports to review the configured settings.

Procedure:
1. **In** GPMC:
   - Expand "Group Policy Objects"
   - Right-click on **Default Domain Policy** → Click **Save Report**
   - Save it as: DefaultDomainPolicy.html (e.g., on Desktop or Lab Reports folder)



2. Repeat the same **for**:
   - **Default Domain Controllers Policy**
   - Save as: DefaultDomainControllersPolicy.html



Step 3 – Analyze the Purpose and Scope

Default Domain Policy:

- Applies to all users and computers in the domain
- Includes settings like:
  - Password policies (minimum length, complexity)
  - Account lockout policies
  - Kerberos settings
  - Default logon restrictions

Default Domain Policy

Data collected on: 5/22/2025 8:11:59 PM

General

Details

Links

Location	Enforced	Link Status	Path
vlabs07	No	Enabled	vlabs07.com

This list only includes links in the domain of the GPO.

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
NT AUTHORITY\Authenticated Users

Computer Configuration (Enabled)

Policies

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

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

Account Policies/Account Lockout Policy

Account Policies/Kerberos Policy

Local Policies/Security Options

Public Key Policies/Encrypting File System

Default Domain Controllers Policy:

- Applies only to Domain Controllers
- Includes settings like:
  - User rights assignments for DC roles
  - Security options
  - Audit policy
  - Network access restrictions

Default Domain Controllers Policy

Data collected on: 5/22/2025 8:15:10 PM

General

Details

Links

Location	Enforced	Link Status	Path
Domain Controllers	No	Enabled	vlabs07.com/Domain Controllers

This list only includes links in the domain of the GPO.

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
NT AUTHORITY\Authenticated Users

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Local Policies/User Rights Assignment

Local Policies/Security Options

Domain Controller

Domain Member

Microsoft Network Server

Local Policies/User Rights Assignment

hide

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

Important:

- **These policies should **not be deleted or unlinked****
- **You can **modify them**, but it is **best practice** to create new GPOs for additional settings to avoid misconfiguration**