This lab is designed to understand and apply Group Policy Objects (GPOs) in a domain environment.

Lab Assignment 2 (Part I) - GPO

420-636-AB-Network Installation and Administration II

Teacher: Antoine Tohme
Student: Monica Perez Mata
Student id : 2498056

Table of Contents

Lab Assignment 2 (Part I) – GPO

1 Lab Objective

This lab is designed to **understand and apply Group Policy Objects (GPOs)** in a domain environment.

You will **create, configure, and manage GPOs using both the GUI and PowerShell**, apply security filtering, implement WMI filters, and test GPO processing order, enforcement, and inheritance rules.

By the end of this lab, you should be able to effectively deploy and troubleshoot GPOs within an enterprise environment.

The following tasks are to be executed:

- Task 1: Configuring Group Policy using GUI
- Task 2: Configuring Group Policy using PowerShell
- Task 3: Creating and Testing a WMI Filter for Windows 11 using GUI
- Task 4: Practicing GPO Processing Order using GUI
- Task 5: Exploring Default Group Policy Objects using GUI

2 Lab Environment Requirements

- **DC101**: Domain Controller with Active Directory, DNS, and Group Policy Management installed.
- **Client1**: Windows 11 client machine joined the domain.

3 Task 1: Configuring Group Policy using GUI

3.1 Objective

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

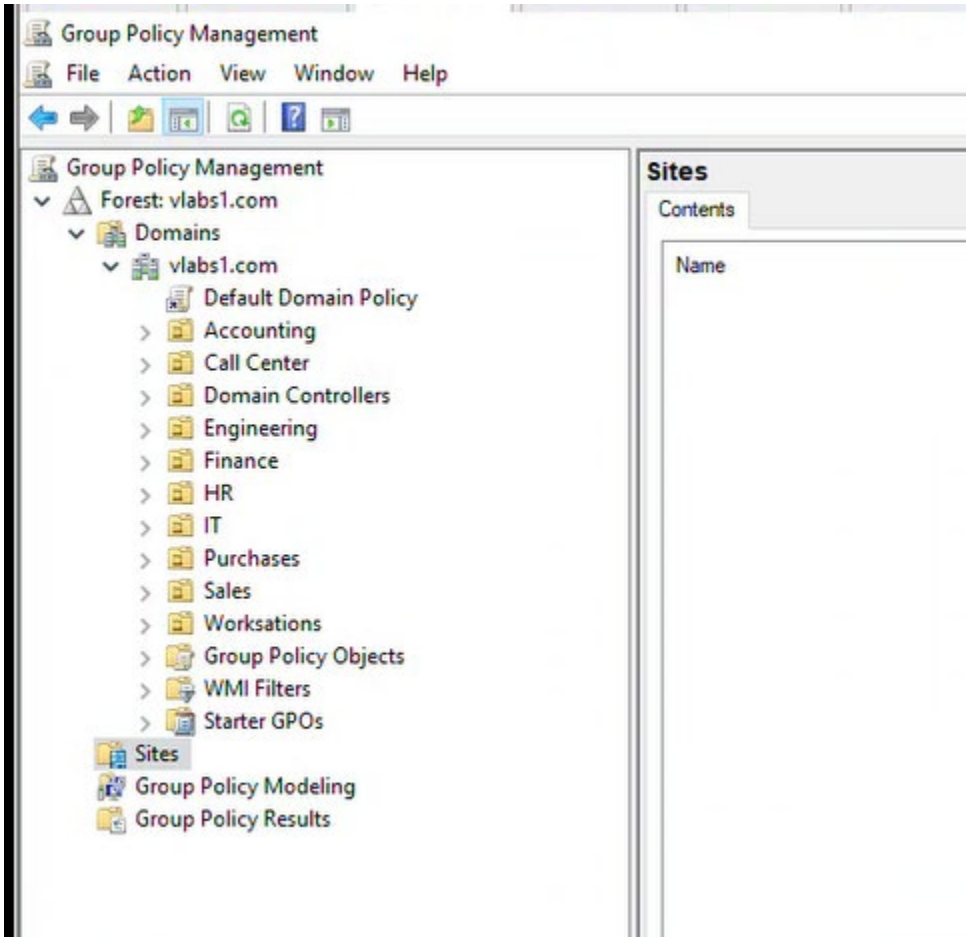
GPO Name: RestrictRegistryAccess

3.2 Steps

1. Create a new GPO named **RestrictRegistryAccess.**

a) Open Group Policy Management Console (GPMC)

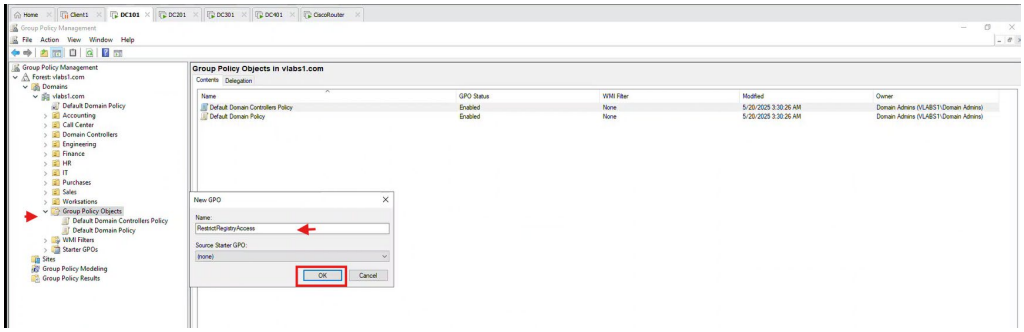
On DC101, open Server Manager → Tools → Group Policy Management.

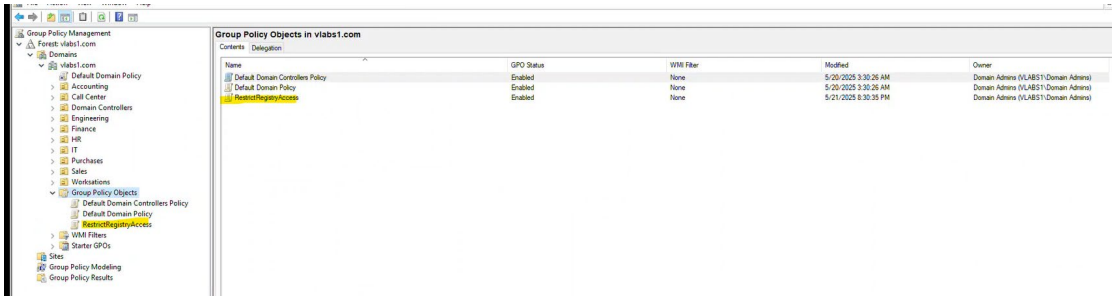


b) Create a New GPO

Right-click Group Policy Objects → New.

Name: RestrictRegistryAccess → Click OK.





2. Configure the required setting to **block access to the registry editing tools.**

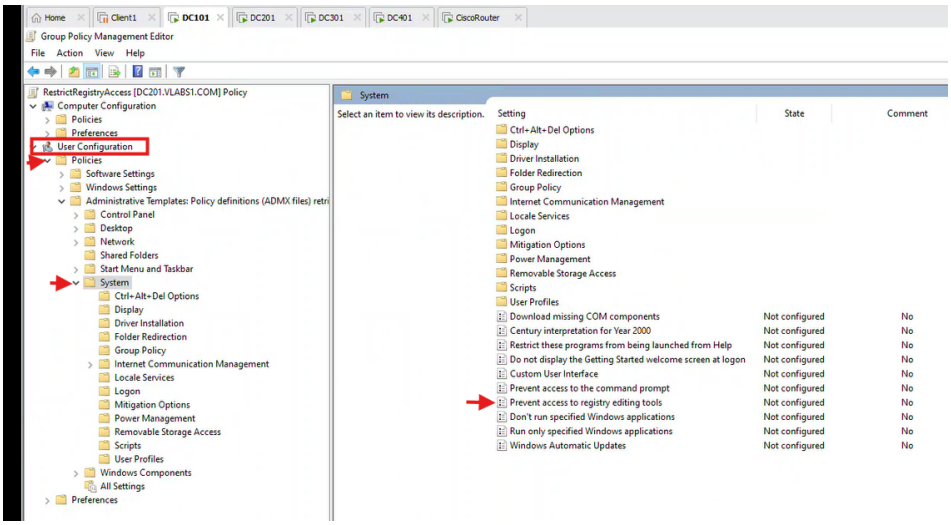
a) **Edit the GPO**

Right-click **RestrictRegistryAccess** → **Edit**.

b) **Navigate to the Registry Restriction Setting**

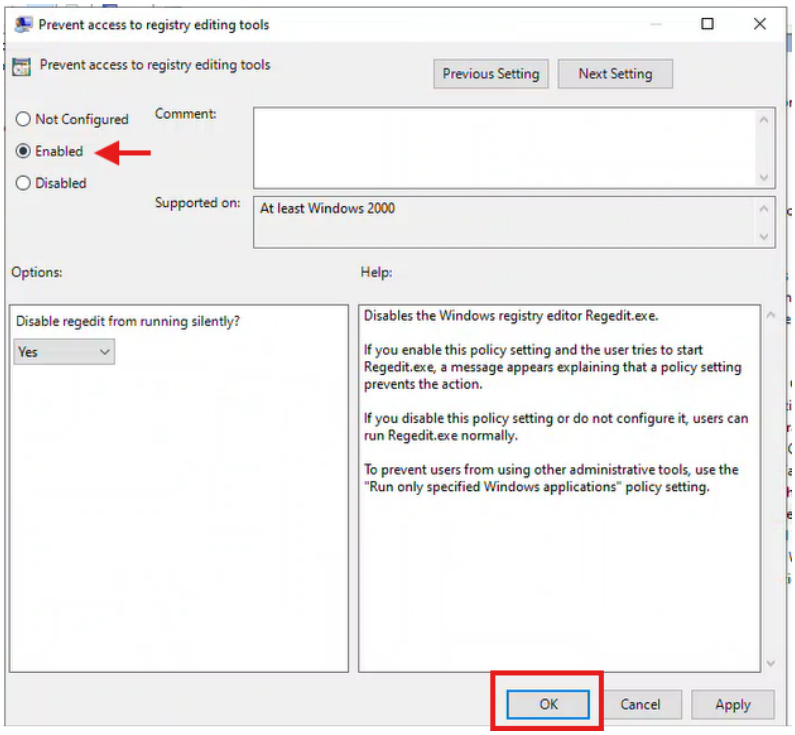
Go to: User Configuration → Policies → Administrative Templates → System

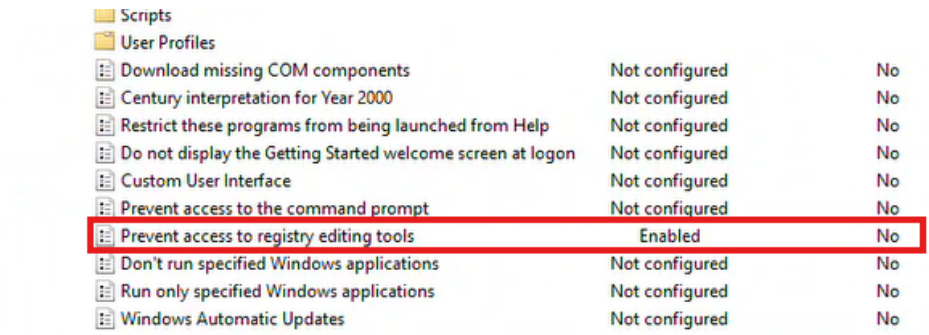
Find and double-click **"Prevent access to registry editing tools"**.



c) **Enable the Policy**

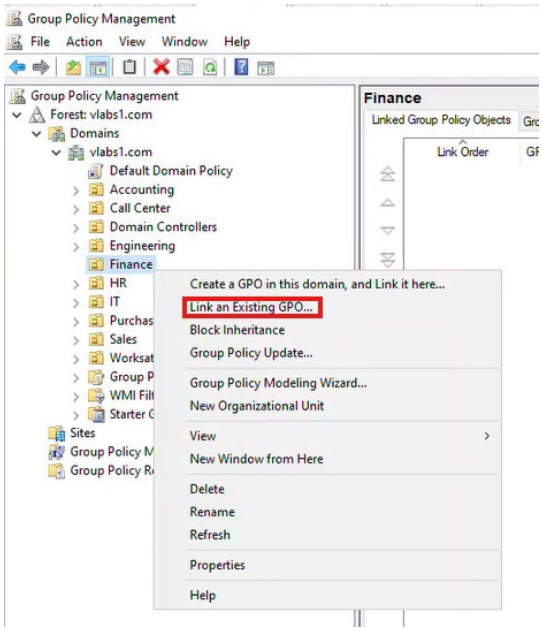
Select **Enabled** → Click **OK**.



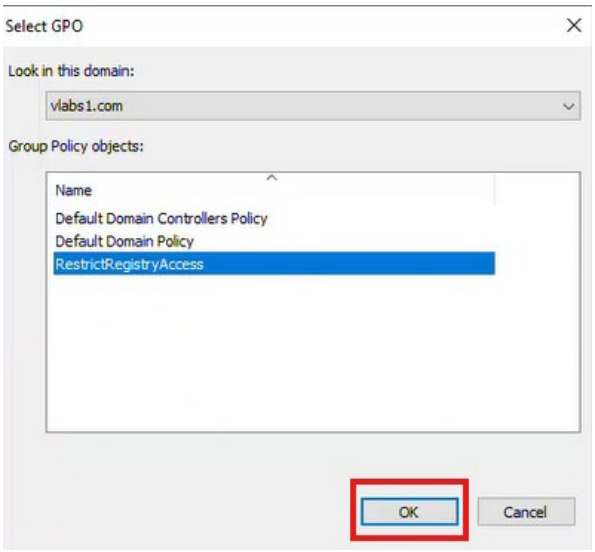


3. Link the GPO to the **Finance OU**.

1. **Locate the Finance OU**
    - In **Group Policy Management**, expand:
      Forest: vlabs1.com → Domains → vlabs1.com → Finance OU
2. **Link the GPO**
    - Right-click **Finance OU** → **Link an Existing GPO**.



- Select **RestrictRegistryAccess** → **OK**.

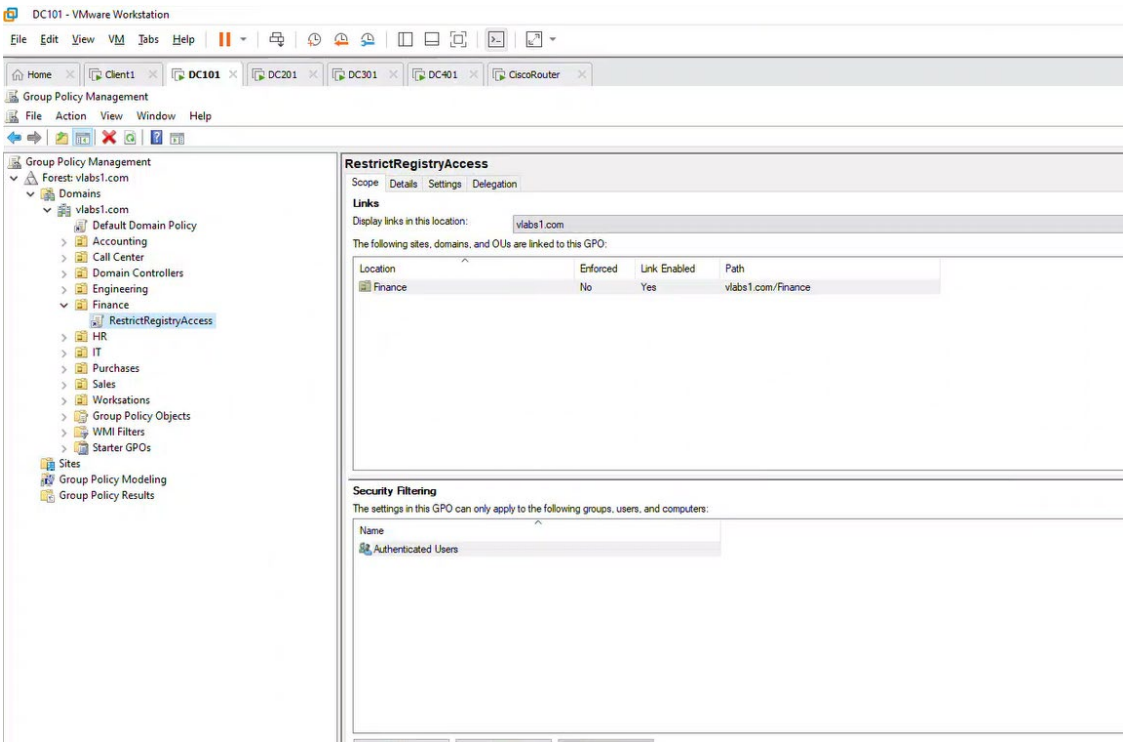


4. Use **Security Filtering** to ensure that **Ava Mercier** from **Finance** is not affected by this GPO.

Proper Security Filtering (Using Deny Permissions)

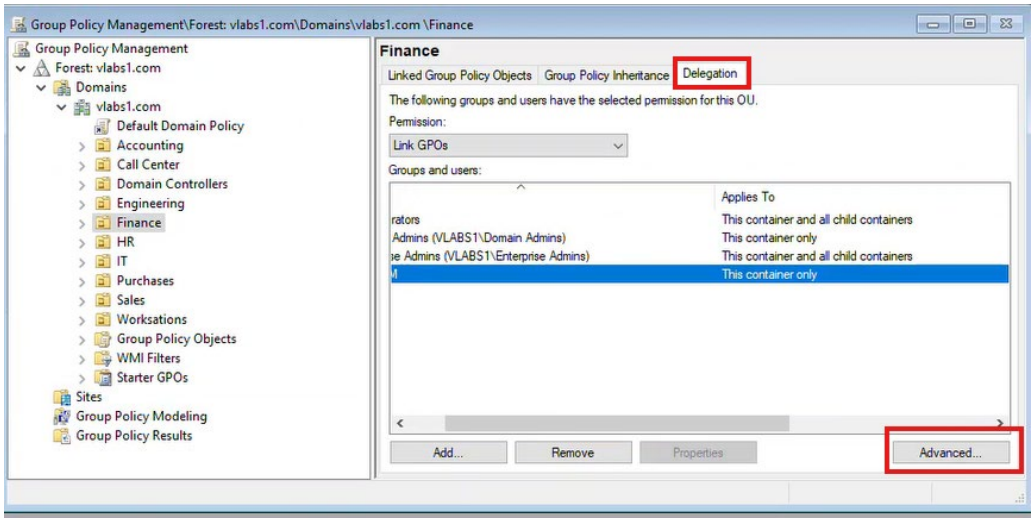
a) **Keep Authenticated Users**

- Under **Security Filtering**, ensure **Authenticated Users** remains (critical for proper processing).

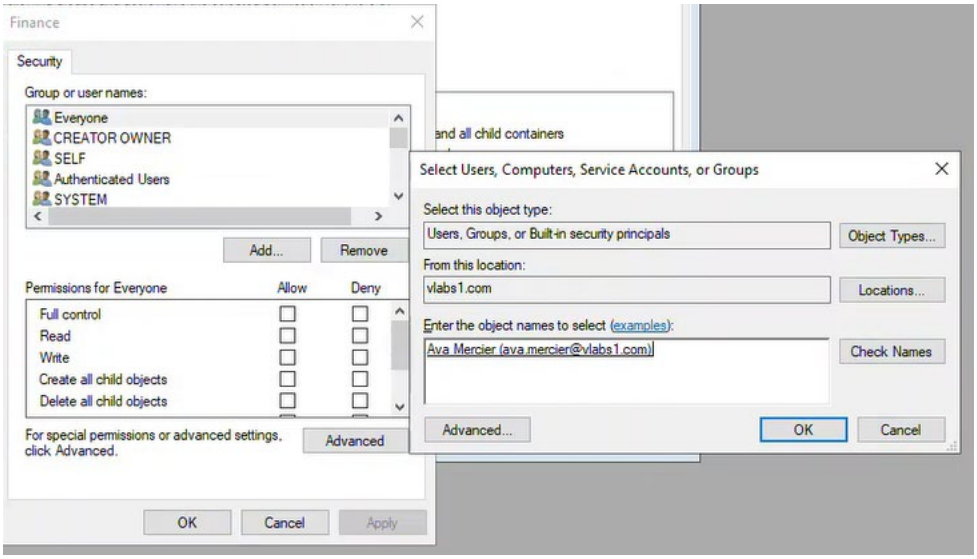


b) **Add Deny Permission for Ava Mercier**

- Go to the **Delegation** tab → Click **Advanced**.

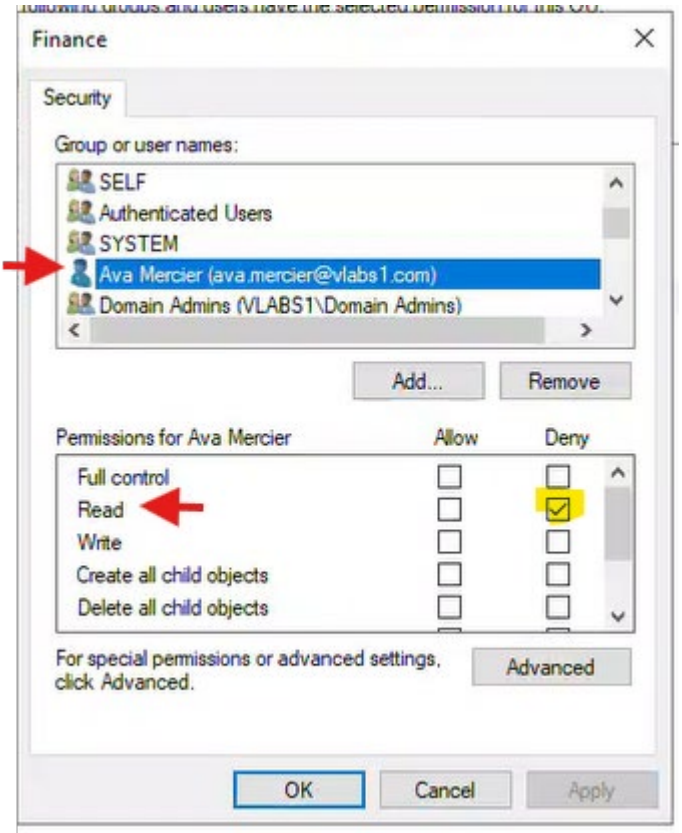


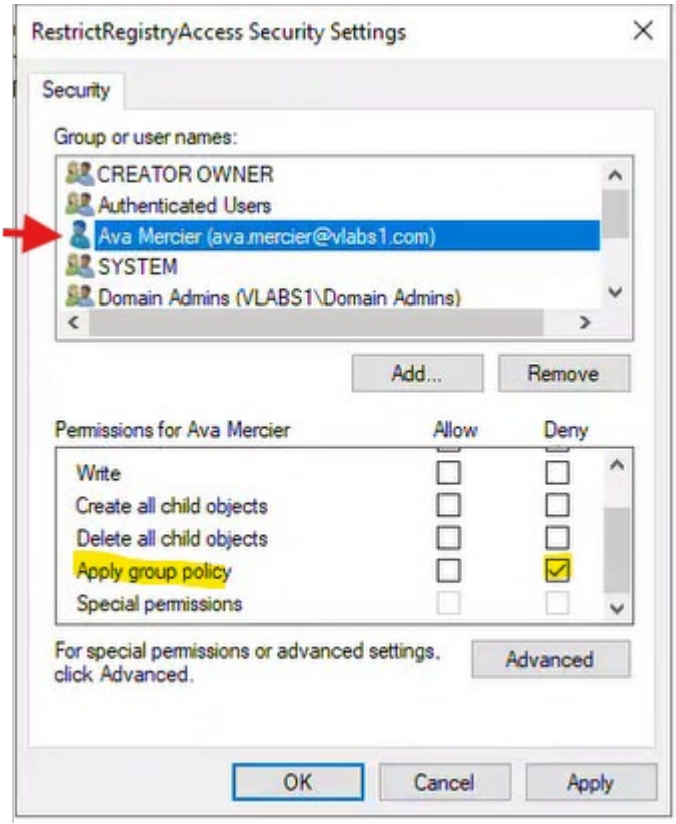
- Click **Add** → Type **Ava Mercier** → **OK**.



- Set the following permissions to **Deny**:
  - **Read**

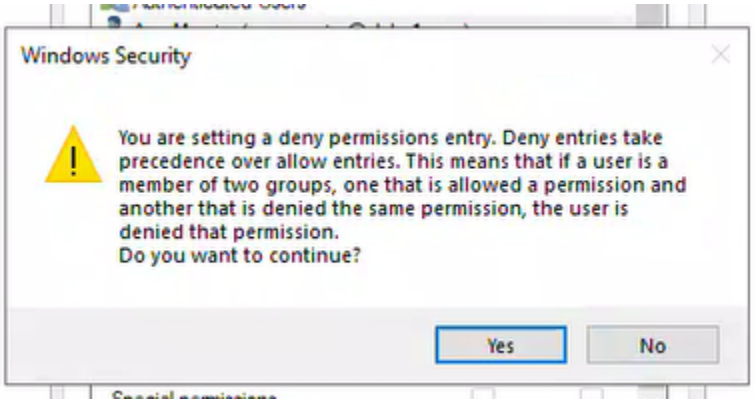
  Click Apply group policy

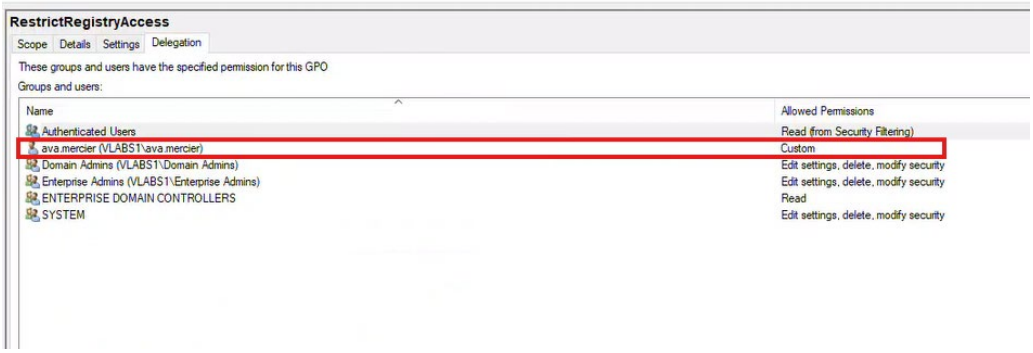




- *Leave all other permissions unchanged*

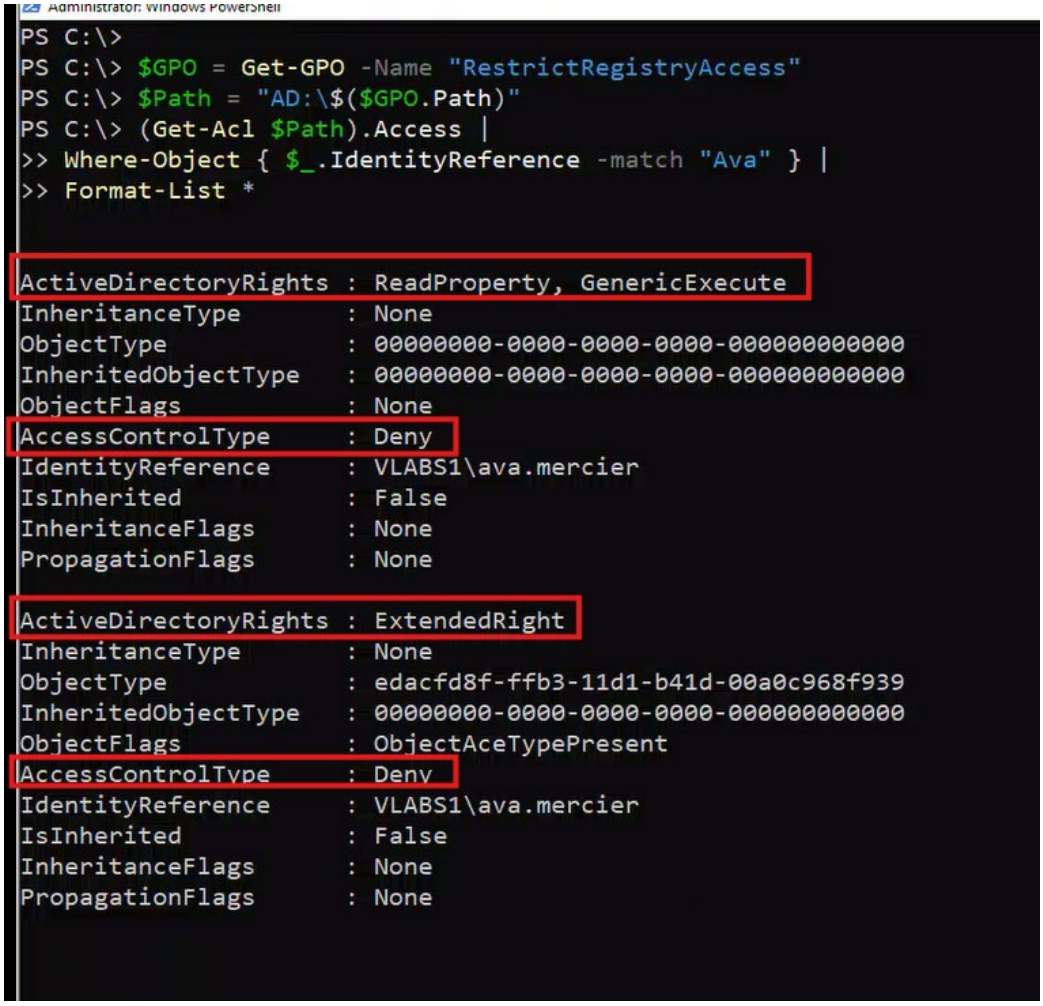
Click **OK** → Confirm the security warning ("Deny entries take precedence...")





Verify in powershell

```
$GPO = Get-GPO -Name "RestrictRegistryAccess"
$Path = "AD:\$($GPO.Path)"
(Get-Acl $Path).Access |
Where-Object { $_.IdentityReference -match "Ava" } |
Format-List *
```

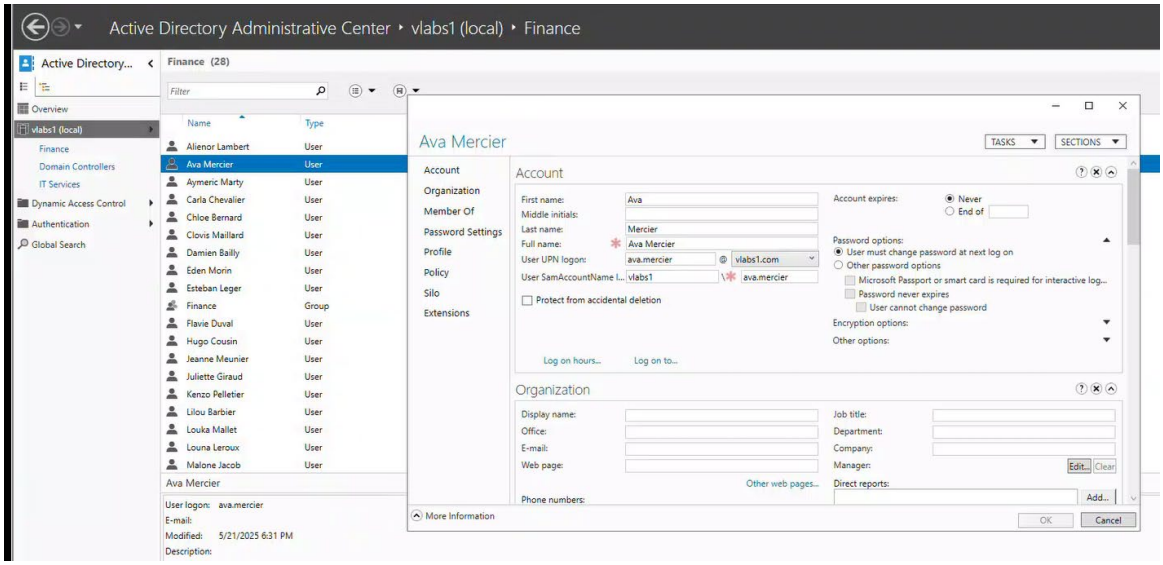


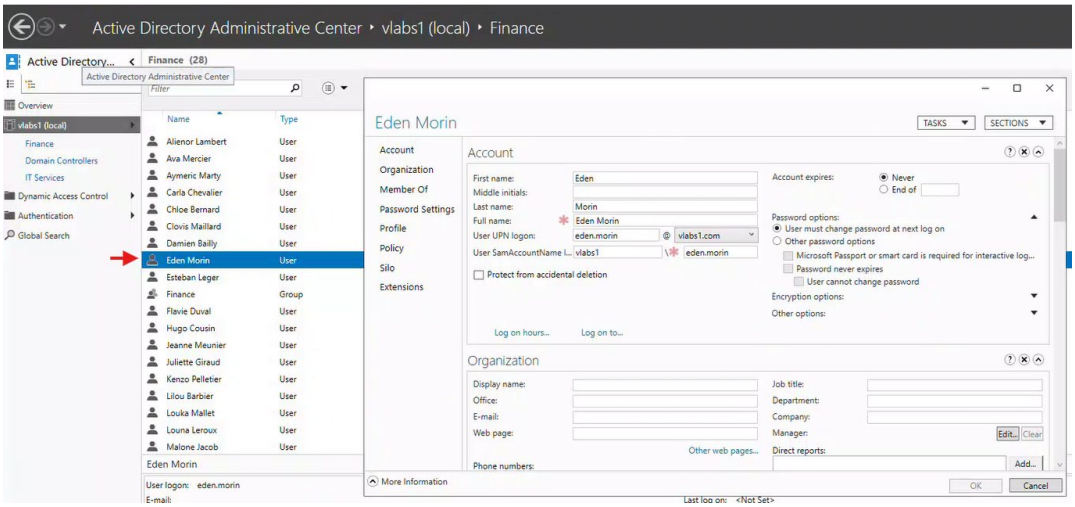
NOTE - Permissions are not inherited (IsInherited: False), meaning they were manually set (as intended)

3.3 Testing:

- Log in to **Client1** with any **Finance user** and verify that the **registry editing tools are blocked.**
- Log in as **Ava Mercier** and confirm that the **GPO does not apply.**

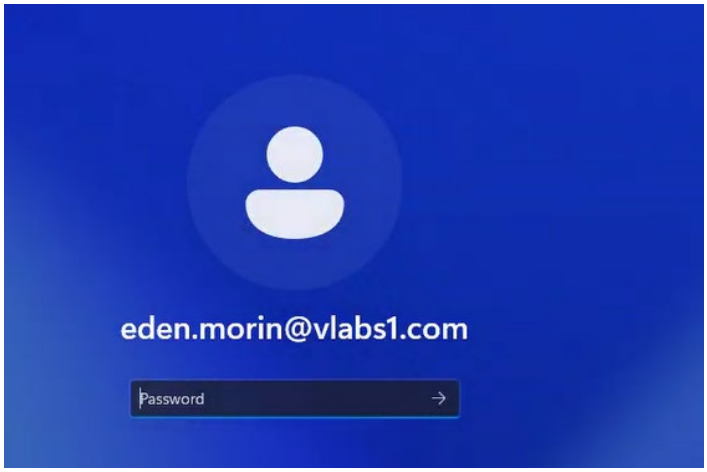
1. In DC101 identify users in Finance using Active directory Administrative Center





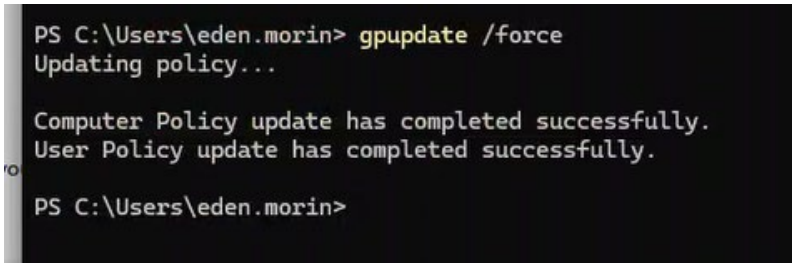
2. Test 1 : Regular Finance User (Policy Should Apply)

a) Log in to Client1 as any Finance user (not Ava Mercier).



b) Force policy update on Client1

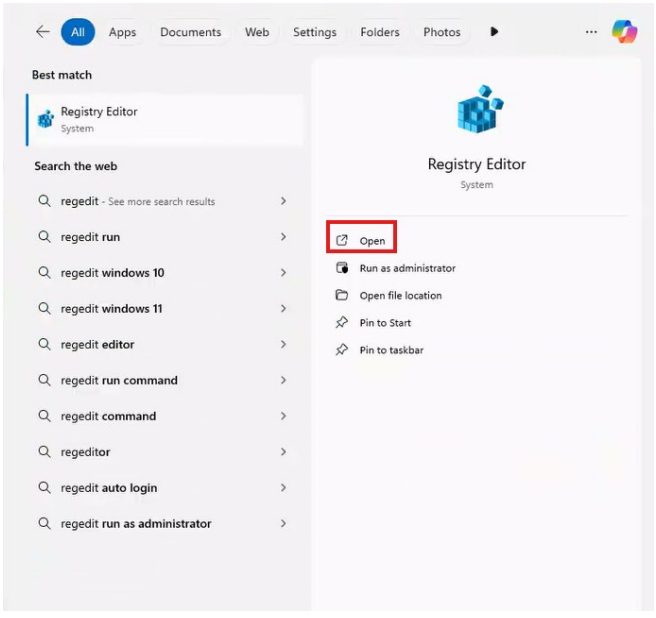
gpupdate /force

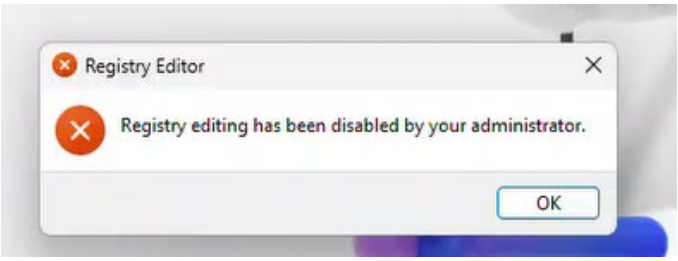


c) Try opening Registry Editor (regedit).

Expected Result:

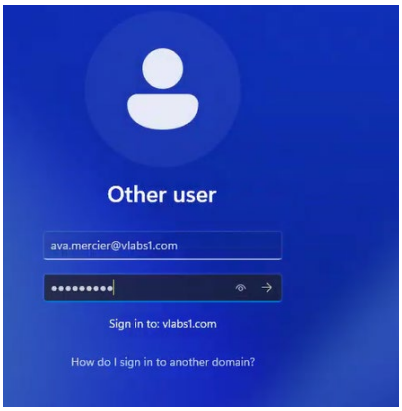
- **Error: *"Registry editing has been disabled by your administrator."***



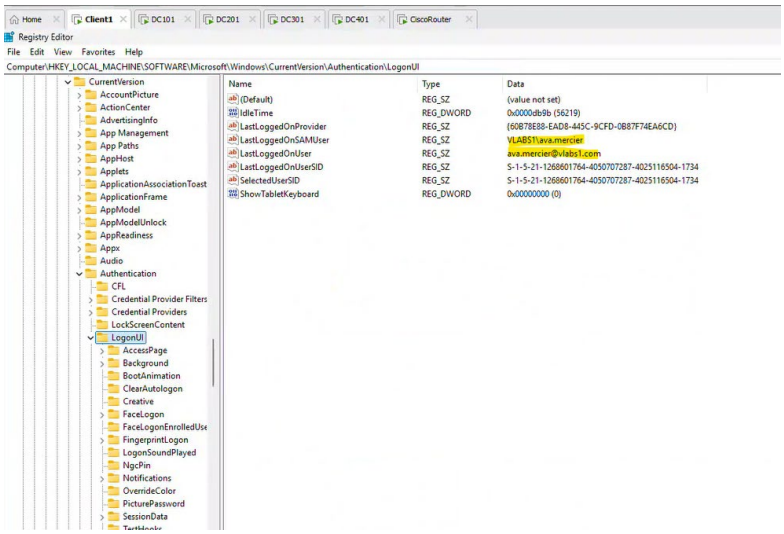


2. **Test 2: Ava Mercier (Policy Should NOT Apply)**

a) **Log in to Client1 as vlabs1\ava.mercier.**



b) **Try opening Registry Editor (regedit).**
   - **Expected Result:**
     - **Registry Editor opens normally (no restriction).**



4 Task 2: Configuring Group Policy using PowerShell

4.1 Objective

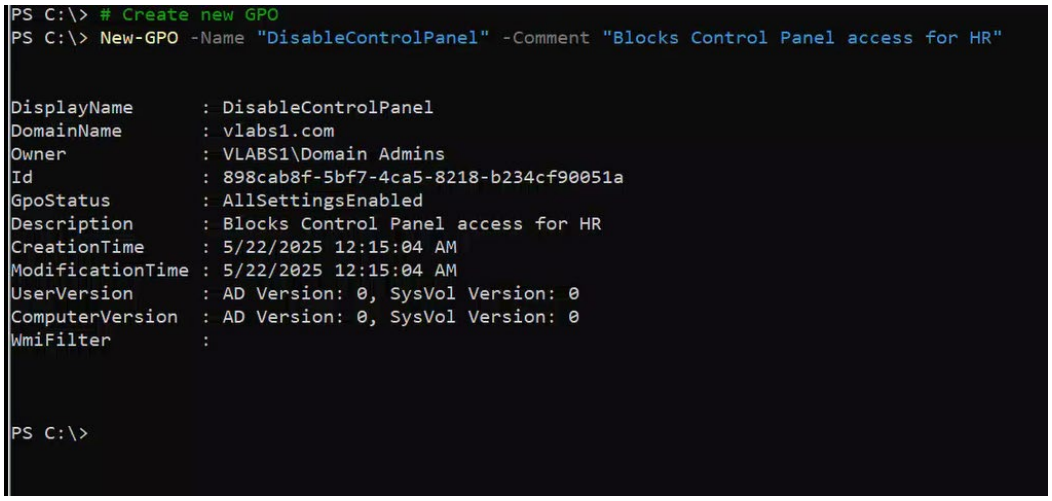
Disable access to the Control Panel using PowerShell.
GPO Name: DisableControlPanel

4.2 Steps (using PowerShell)

a) Create a new GPO named **DisableControlPanel**

 # Create new GPO

```
New-GPO -Name "DisableControlPanel" -Comment "Blocks Control Panel access for HR"
```



b) Configure the necessary settings to **disable access to the Control Panel**.

```
Configure Control Panel restriction (User Configuration)
Set-GPRegistryValue -Name "DisableControlPanel" -Key
"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" `
  -ValueName "NoControlPanel" -Type DWord -Value 1
```

```
PS C:\> # Configure Control Panel restriction (User Configuration)
PS C:\> Set-GPRegistryValue -Name "DisableControlPanel" -Key "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" `
>>      -ValueName "NoControlPanel" -Type DWord -Value 1


DisplayName      : DisableControlPanel
DomainName       : vlabs1.com
Owner            : VLABS1\Domain Admins
Id               : 898cab8f-5bf7-4ca5-8218-b234cf90051a
GpoStatus        : AllSettingsEnabled
Description      : Blocks Control Panel access for HR
CreationTime     : 5/22/2025 12:15:04 AM
ModificationTime : 5/22/2025 12:17:50 AM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        :
```

c) Link the GPO to the OU **HR**.

```
#  Link to HR OU
New-GPLink -Name "DisableControlPanel" -Target "OU=HR,DC=vlabs1,DC=com"
```

```
PS C:\> # Link to HR OU
PS C:\> New-GPLink -Name "DisableControlPanel" -Target "OU=HR,DC=vlabs1,DC=com"


GpoId       : 898cab8f-5bf7-4ca5-8218-b234cf90051a
DisplayName : DisableControlPanel
Enabled     : True
Enforced    : False
Target      : OU=HR,DC=vlabs1,DC=com
Order       : 1
```

d) Verify Authenticated Users Permissions

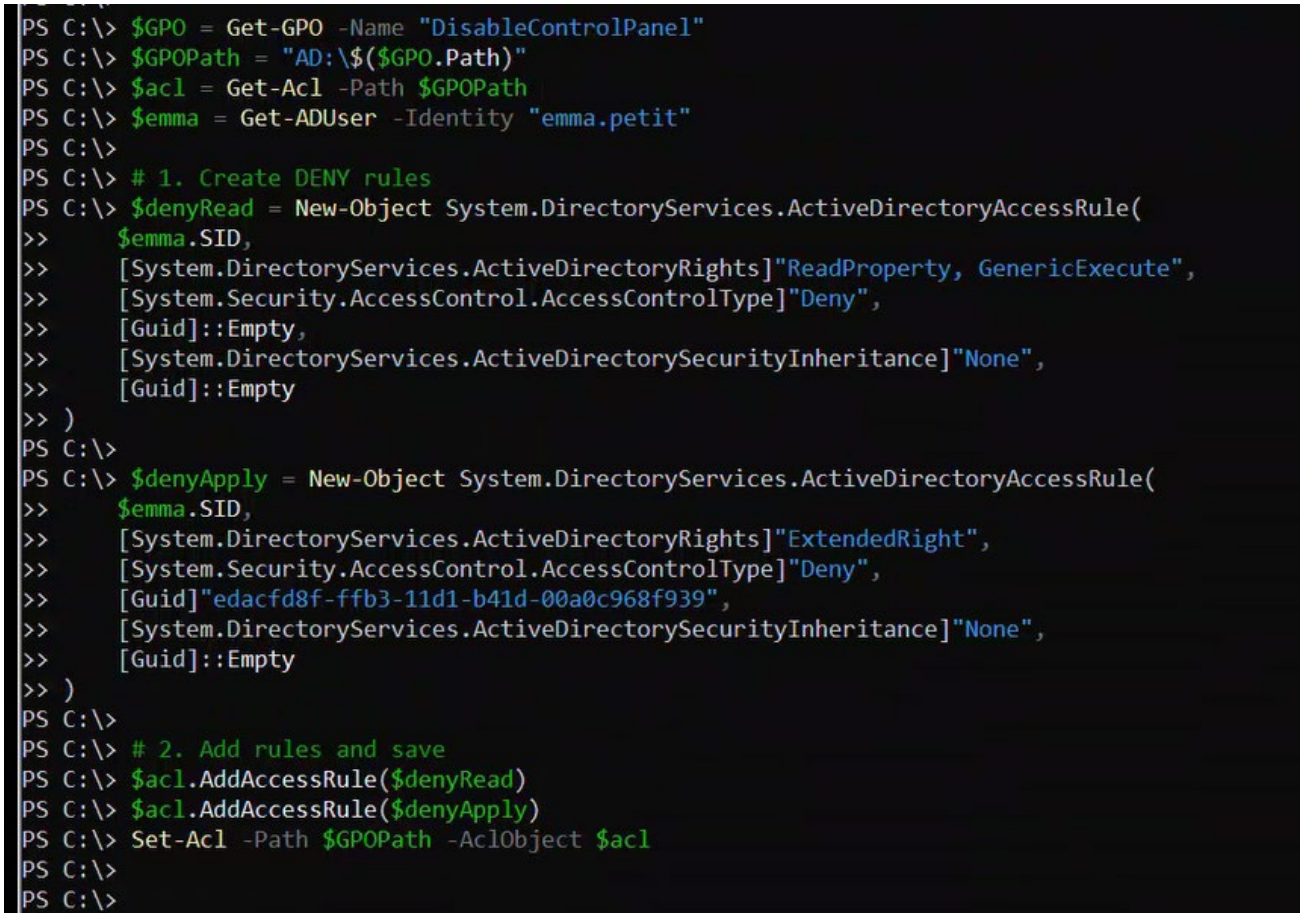
```
# First get the GPO path (must run this first)
$GPO = Get-GPO -Name "DisableControlPanel"
 $GPOPath = "AD:\$($GPO.Path)"
 # Now run verification
Write-Host "`n[Authenticated Users Permissions]" -ForegroundColor Cyan
(Get-Acl $GPOPath).Access |
  Where-Object { $_.IdentityReference -eq "NT AUTHORITY\Authenticated Users" }
|
  Format-List *
```

```
PS C:\> # First get the GPO path (must run this first)
PS C:\> $GPO = Get-GPO -Name "DisableControlPanel"
PS C:\> $GPOPath = "AD:\$($GPO.Path)"
PS C:\>
PS C:\> # Now run verification
PS C:\> Write-Host "`n[Authenticated Users Permissions]" -ForegroundColor Cyan

[Authenticated Users Permissions]
PS C:\> (Get-Acl $GPOPath).Access |
>>     Where-Object { $_.IdentityReference -eq "NT AUTHORITY\Authenticated Users" } |
>>     Format-List *


ActiveDirectoryRights : GenericRead
InheritanceType       : All
ObjectType            : 00000000-0000-0000-0000-000000000000
InheritedObjectType   : 00000000-0000-0000-0000-000000000000
ObjectFlags           : None
AccessControlType     : Allow
IdentityReference     : NT AUTHORITY\Authenticated Users
IsInherited           : False
InheritanceFlags      : ContainerInherit
PropagationFlags      : None

ActiveDirectoryRights : ExtendedRight
InheritanceType       : All
ObjectType            : edacfd8f-ffb3-11d1-b41d-00a0c968f939
InheritedObjectType   : 00000000-0000-0000-0000-000000000000
ObjectFlags           : ObjectAceTypePresent
AccessControlType     : Allow
IdentityReference     : NT AUTHORITY\Authenticated Users
IsInherited           : False
InheritanceFlags      : ContainerInherit
PropagationFlags      : None
```

e) Use a security group HR and remove a user (e.g., Emma Petit) from that group does not work as expected.

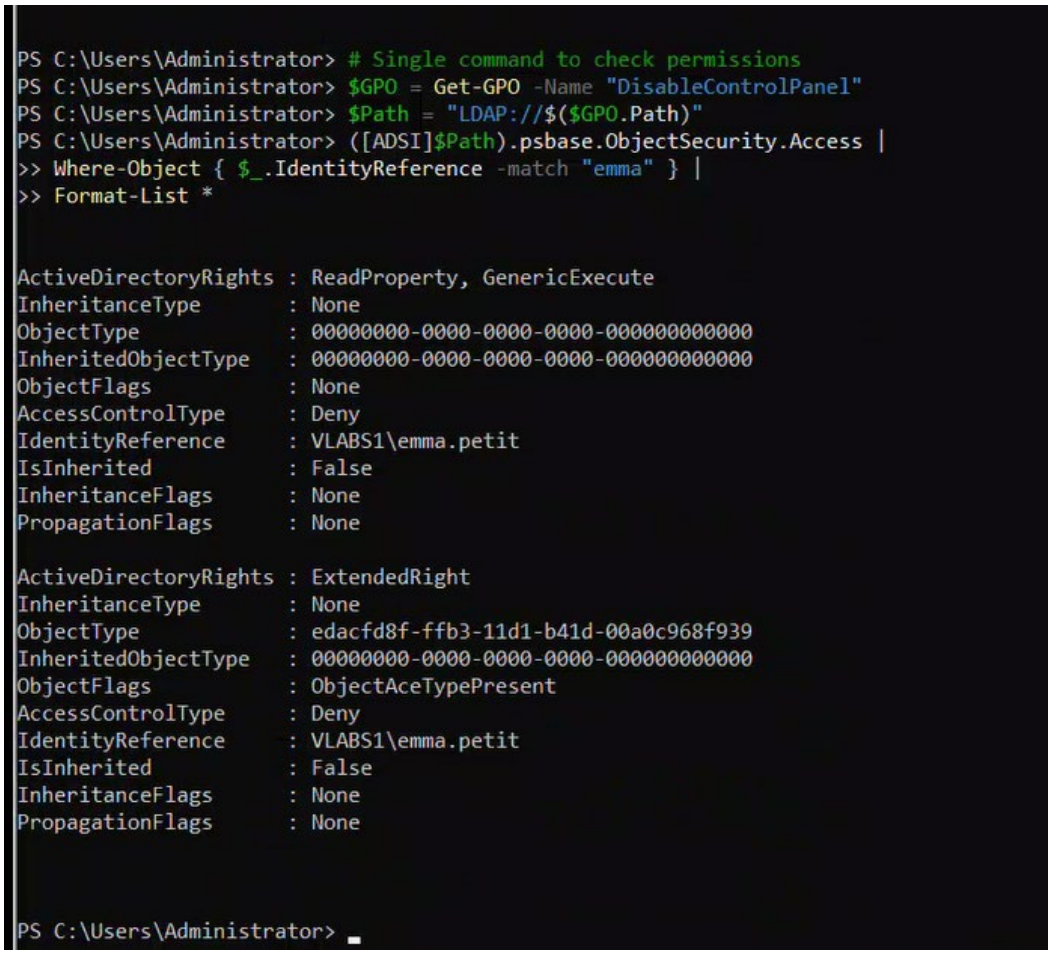
```
# Add Emma Petit with EXPLICIT DENY (matches GUI Advanced Security)
$GPOPath = "AD:\$($GPO.Path)"
$acl = Get-Acl -Path $GPOPath
$emma = Get-ADUser -Identity "emma.petit"
# 1. Create DENY rules
$denyRead = New-Object System.DirectoryServices.ActiveDirectoryAccessRule(
  $emma.SID,
  [System.DirectoryServices.ActiveDirectoryRights]"ReadProperty, GenericExecute",
  [System.Security.AccessControl.AccessControlType]"Deny",
  [Guid]::Empty,
  [System.DirectoryServices.ActiveDirectorySecurityInheritance]"None",
```

```
  [Guid]::Empty
)

$denyApply = New-Object System.DirectoryServices.ActiveDirectoryAccessRule(
  $emma.SID,
  [System.DirectoryServices.ActiveDirectoryRights]"ExtendedRight",
  [System.Security.AccessControl.AccessControlType]"Deny",
  [Guid]"edacfd8f-ffb3-11d1-b41d-00a0c968f939",
  [System.DirectoryServices.ActiveDirectorySecurityInheritance]"None",
  [Guid]::Empty
)

# 2. Add rules and save
$acl.AddAccessRule($denyRead)
$acl.AddAccessRule($denyApply)
Set-Acl -Path $GPOPath -AclObject $acl
```



f) Verification

```
# Single command to check permissions
$GPO = Get-GPO -Name "DisableControlPanel"
$Path = "LDAP://$($GPO.Path)"
([ADSI]$Path).psbase.ObjectSecurity.Access |
Where-Object { $_.IdentityReference -match "emma" } |
Format-List *
```



4.3 Testing

Don't forget to run **gpupdate /force** on the client before each test

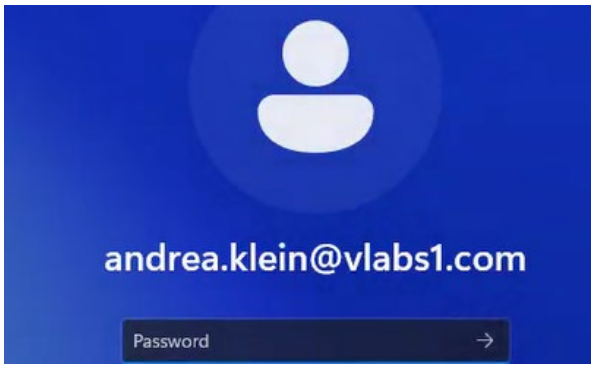
- Log in to **Client1** with any **HR user** and verify that the **Control Panel is disabled.**
- Log in as **Emma Petit** and confirm that the **GPO does not apply.**

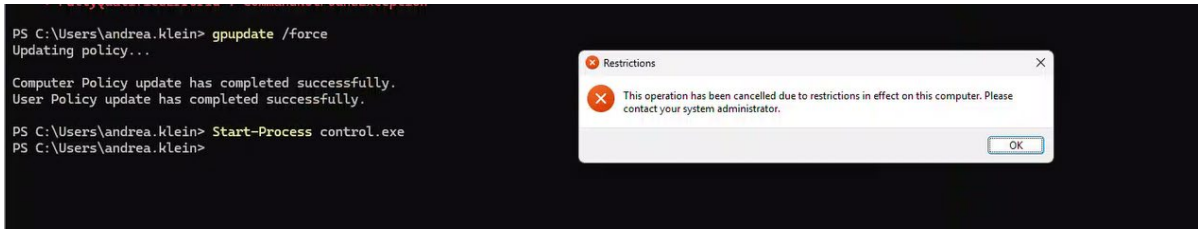
a) In DC101 Verify users in HR

```
# Get all users in the HR OUemma
$HRUsers = Get-ADUser -Filter * -SearchBase "OU=HR,DC=vlabs1,DC=com" -Properties Name, SamAccountName, Enabled

# Display HR users in three columns: Name, SamAccountName, Enabled
Write-Host "`n--- All Users in HR OU ---" -ForegroundColor Cyan
$HRUsers | Select-Object Name, SamAccountName, Enabled | Format-Table -Property Name, SamAccountName, Enabled -AutoSize
```

```
PS C:\> # Get all users in the HR OU
PS C:\> $HRUsers = Get-ADUser -Filter * -SearchBase "OU=HR,DC=vlabs1,DC=com" -Properties Name, SamAccountName, Enabled
PS C:\>
PS C:\> # Display HR users in three columns: Name, SamAccountName, Enabled
PS C:\> Write-Host "`n--- All Users in HR OU ---" -ForegroundColor Cyan

--- All Users in HR OU ---
PS C:\> $HRUsers | Select-Object Name, SamAccountName, Enabled | Format-Table -Property Name, SamAccountName, Enabled -AutoSize

Name              SamAccountName    Enabled
----              --------------    -------
Adem Vasseur      adem.vasseur         True
Ambre Rousseau    ambre.rousseau       True
Andrea Klein      andrea.klein         True
Benjamin Guyot    benjamin.guyot       True
Blanche Guerin    blanche.guerin       True
Charlie Legrand   charlie.legrand      True
Dylan Schneider   dylan.schneider      True
elise Henry       elise.henry          True
Emma Petit        emma.petit           True
Ethan Michel      ethan.michel         True
Evan Julien       evan.julien          True
Giulia Dumont     giulia.dumont        True
Ilian Breton      ilian.breton         True
Killian Perrier   killian.perrier      True
Lina Rivière      lina.rivière         True
Livia Martinez    livia.martinez       True
Madeline Vidal    madeline.vidal       True
Marvin Michaud    marvin.michaud       True
Ombeline Pierre   ombeline.pierre      True
Oscar DaSilva     oscar.dasilva        True
Raphael Girard    raphael.girard       True
Tanguy Perret     tanguy.perret        True
Tess Dupuy        tess.dupuy           True
Valentin Delaunay valentin.delaunay    True
```

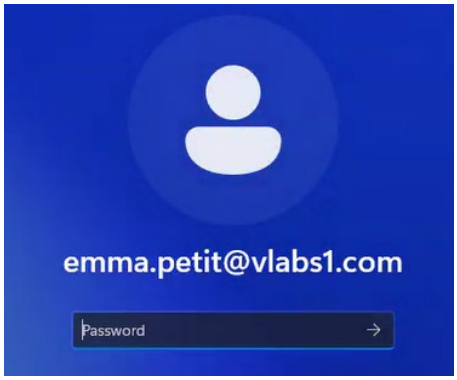
b) Login as Andrea Klein



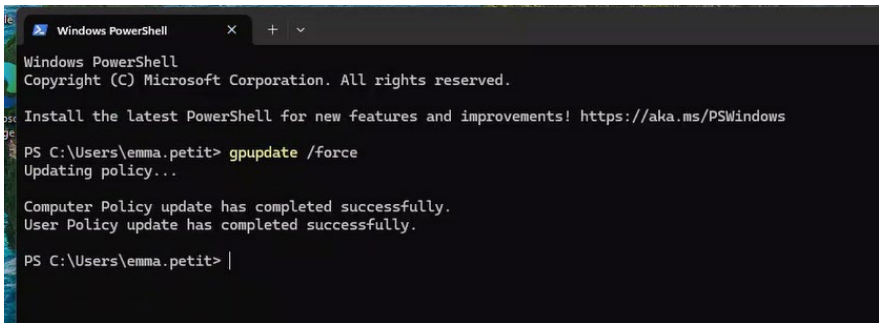


c) Log in as Emma Petit

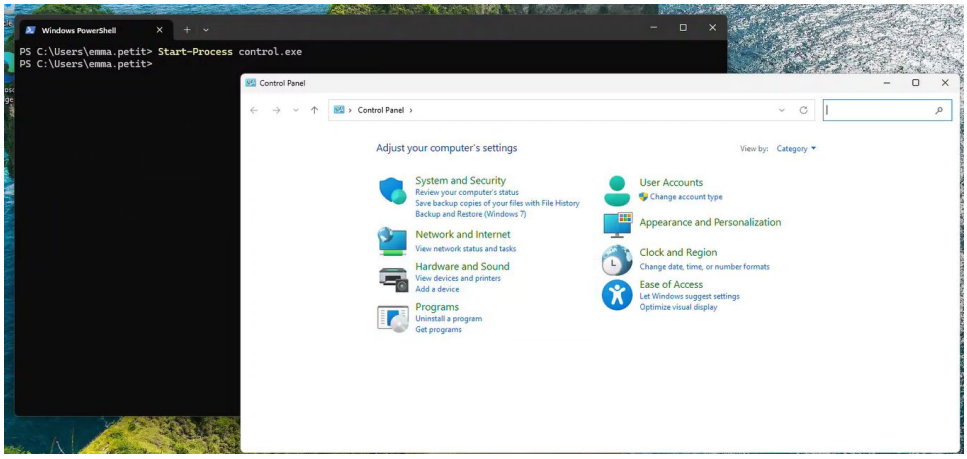
Log in as **Emma Petit** and confirm that the **GPO does not apply.**



- **Force policy update**



Open control panel



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

5.1 Objective

Create a **WMI filter** that applies only to **Windows 11** devices.

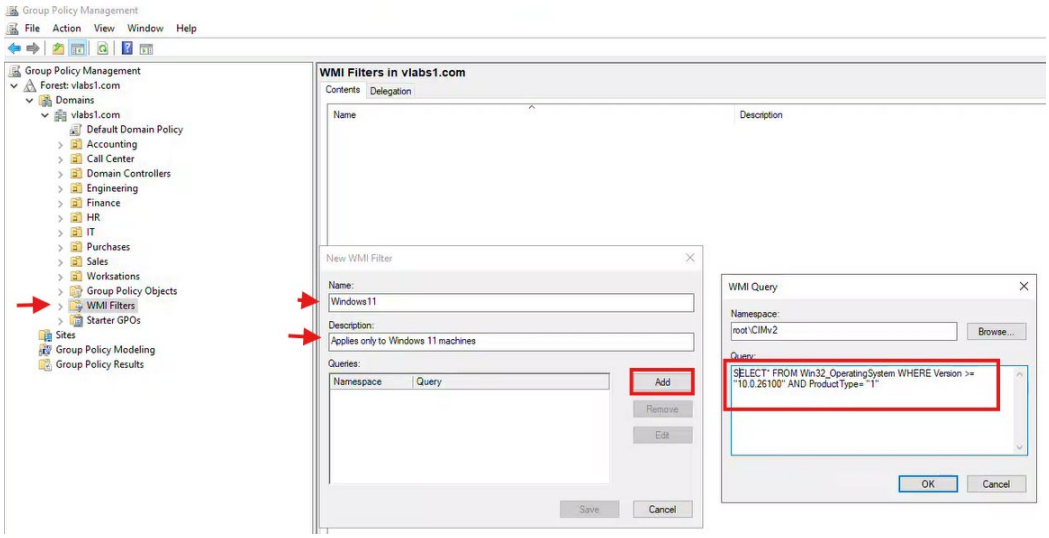
GPO Name: NoRecycleBin

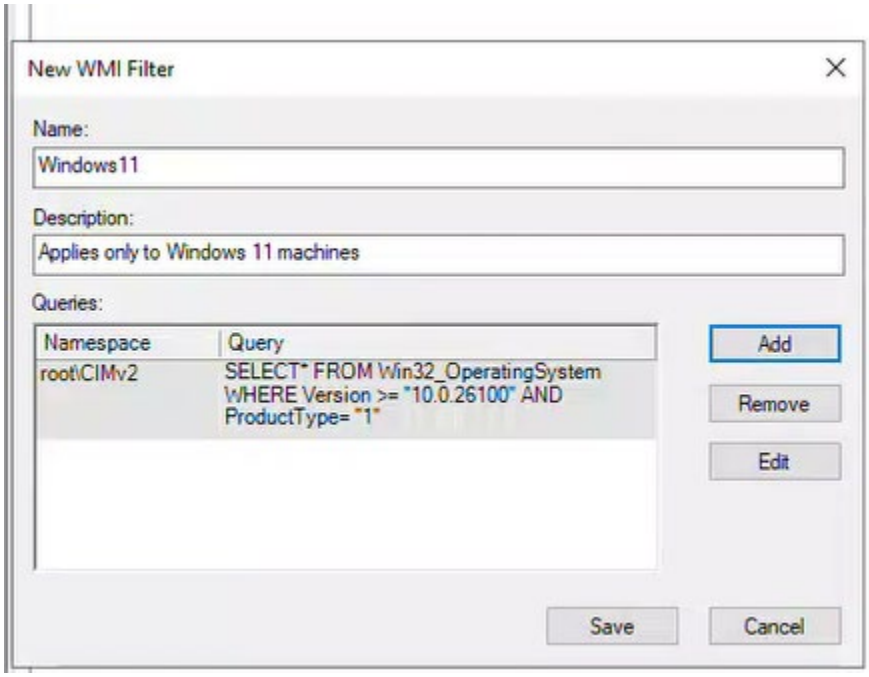
5.2 Steps

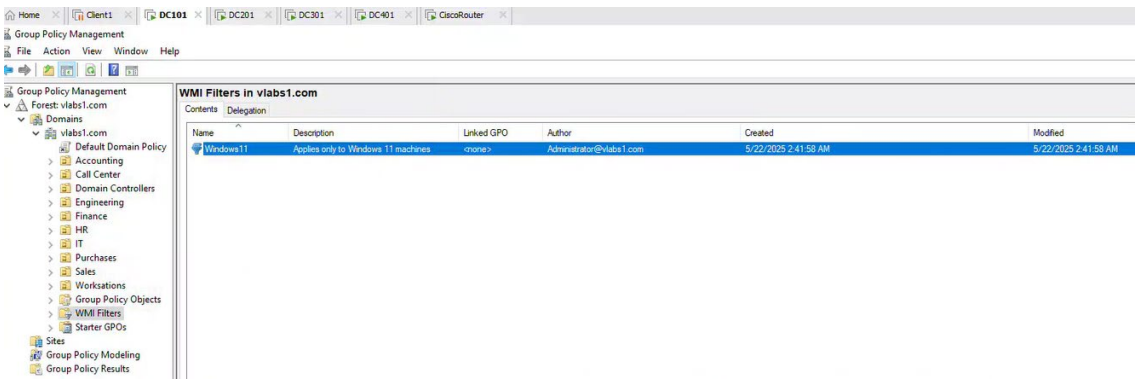
On DC101

1. Create a new **WMI filter** and named **Windows11**
2. Define the appropriate **query** to target **Windows 11 machines.**

a) Open Group Policy Management
b) Expand Forest → Domains → vlabs1.com
c) Right-click WMI Filters → New
Enter: Name: Windows11
Description: "Applies only to Windows 11 machines"
d) Click Add → Enter the WMI query:
SELECT* FROM Win32_OperatingSystem WHERE Version >= "10.0.26100" AND ProductType= "1"
e) Click OK → Save





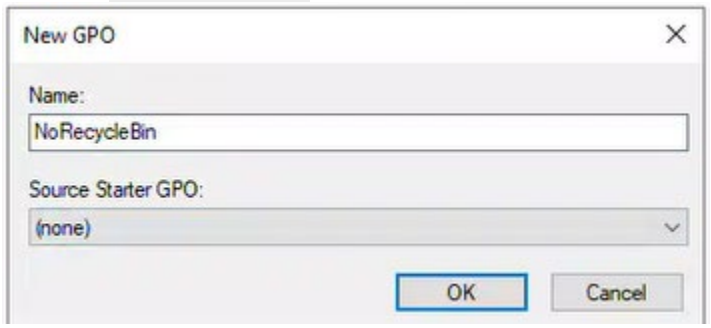


3. Create a new GPO named **NoRecycleBin** and Configure the necessary settings to

Remove the Recycle Bin from the Desktop.

a) Right-click **Group Policy Objects → New**

   a. **Name:** `NoRecycleBin`

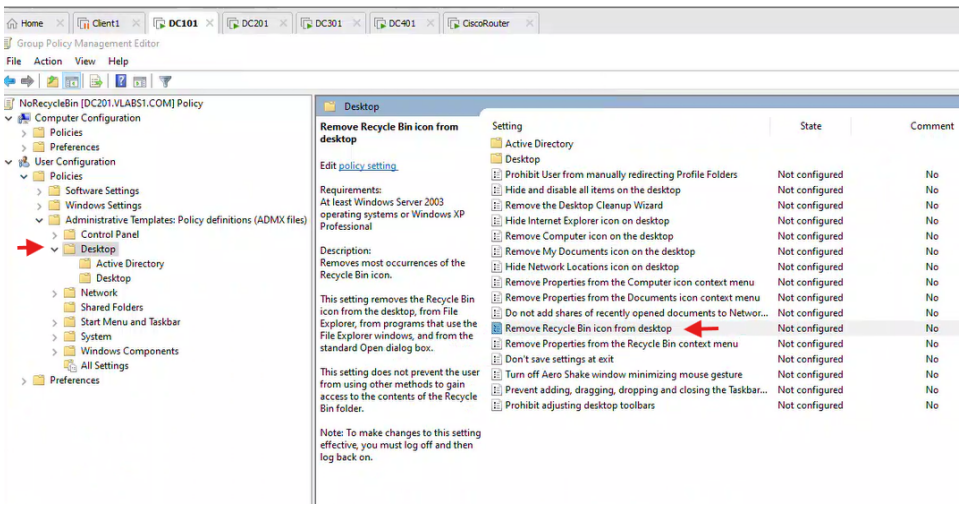


   b. **Description:** "Removes Recycle Bin from Desktop (Windows 11 only)"

b) Right-click the new GPO → **Edit**

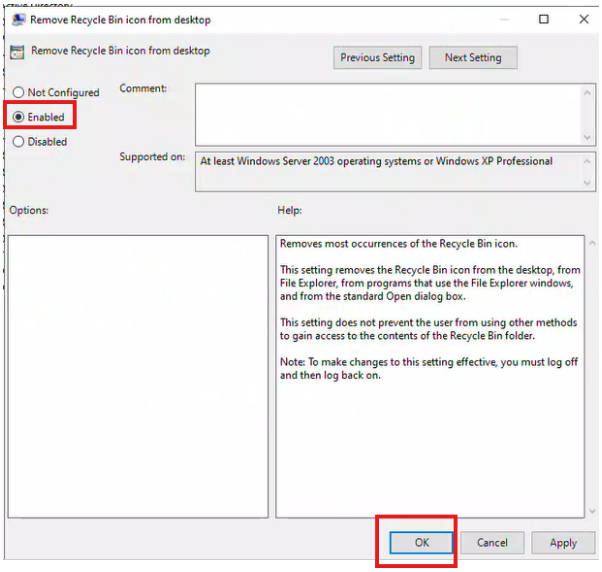
c) Navigate to: `User Configuration → Policies → Administrative Templates → Desktop`

d) Double-click **"Remove Recycle Bin icon from desktop"**



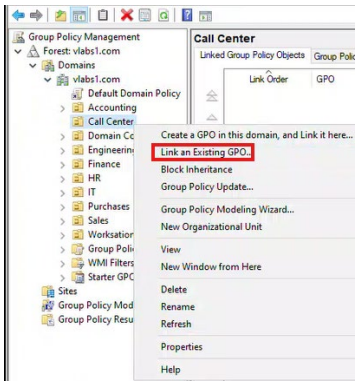
e) Set to **Enabled → OK**

f) Close the GPO Editor.

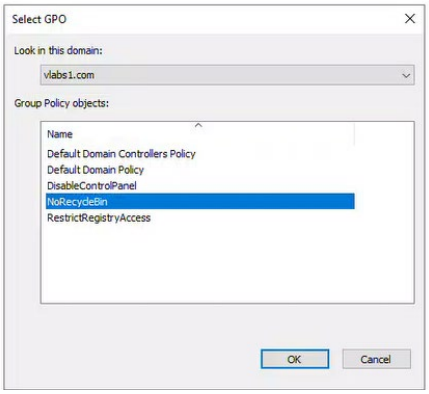


4. Link this GPO to the **Call Center OU**.

a) Expand **vlabs1.com** → Locate the **Call Center OU**



b) Right-click **Call Center OU** → **Link an Existing GPO**
Select NoRecycleBin → OK

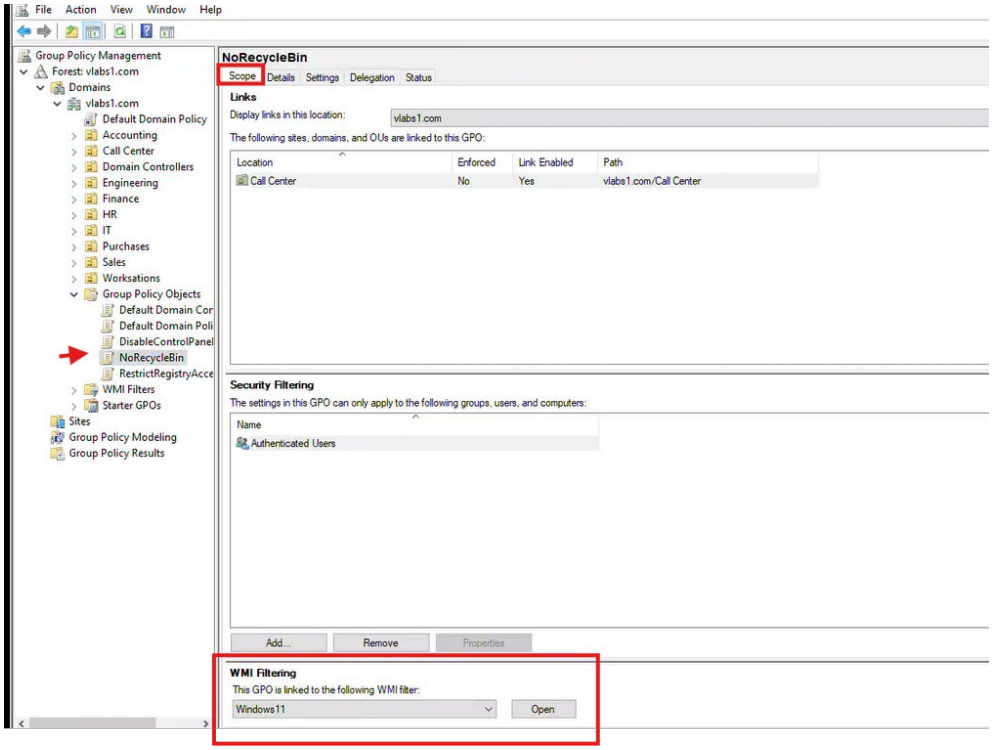


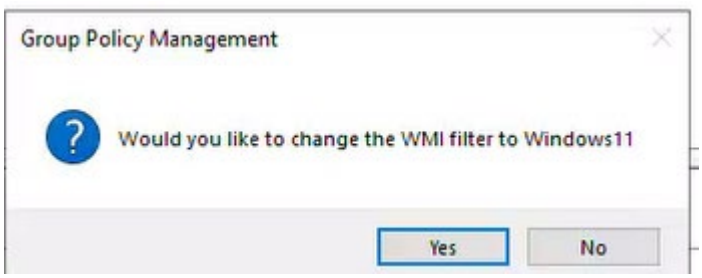
c) Click the **NoRecycleBin** link → Go to **Scope** tab

d) Under **WMI Filtering**, select **Windows11** from the dropdown
e) Click **OK**

5. Link to this **GPO** to the **WMI filter Windows 11.**

1. Open **Group Policy Management Console (GPMC)**.
2. In the left pane, expand **Group Policy Objects**.
3. Click on **NoRecycleBin**.
4. In the right pane, click the **Scope** tab.
5. Look at the bottom where it says **WMI Filtering**.
    - If it says **None**, you need to attach the **Windows11** WMI filter.
6. To attach the WMI filter:
    - Click the dropdown arrow next to **WMI Filtering**.
    - Select **Windows11** filter.
    - Click **Yes** to confirm.



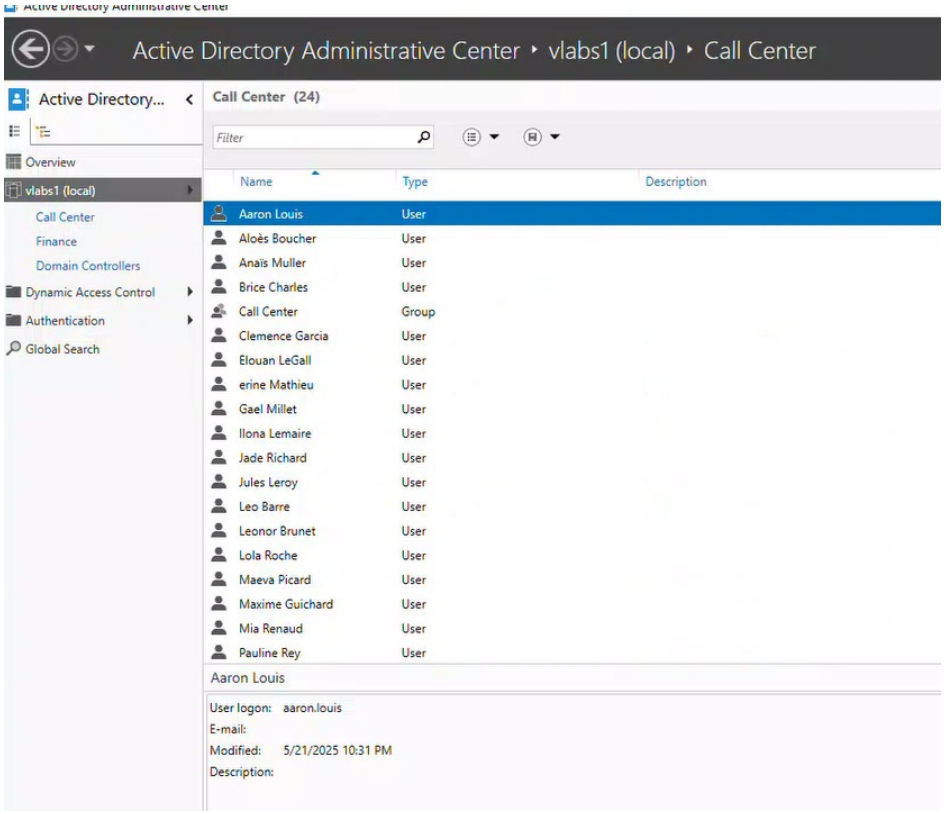


5.3 Testing

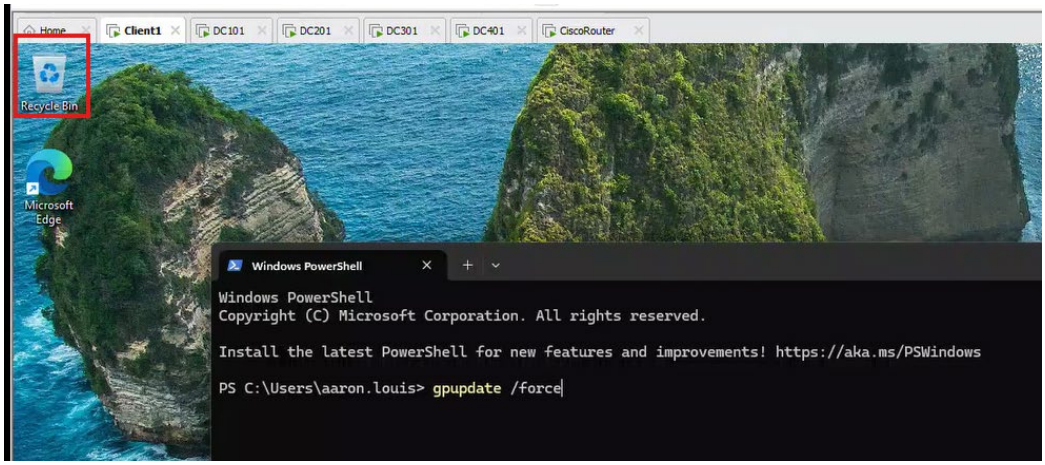
(Don't forget to run **gpupdate /force** on the client before each test)

- Log in to **Client1** with any user from **Call Center** user and verify that the **Recycle Bin** doesn't appear on the **Desktop**.

Verify users from Call centre (run in DC101)

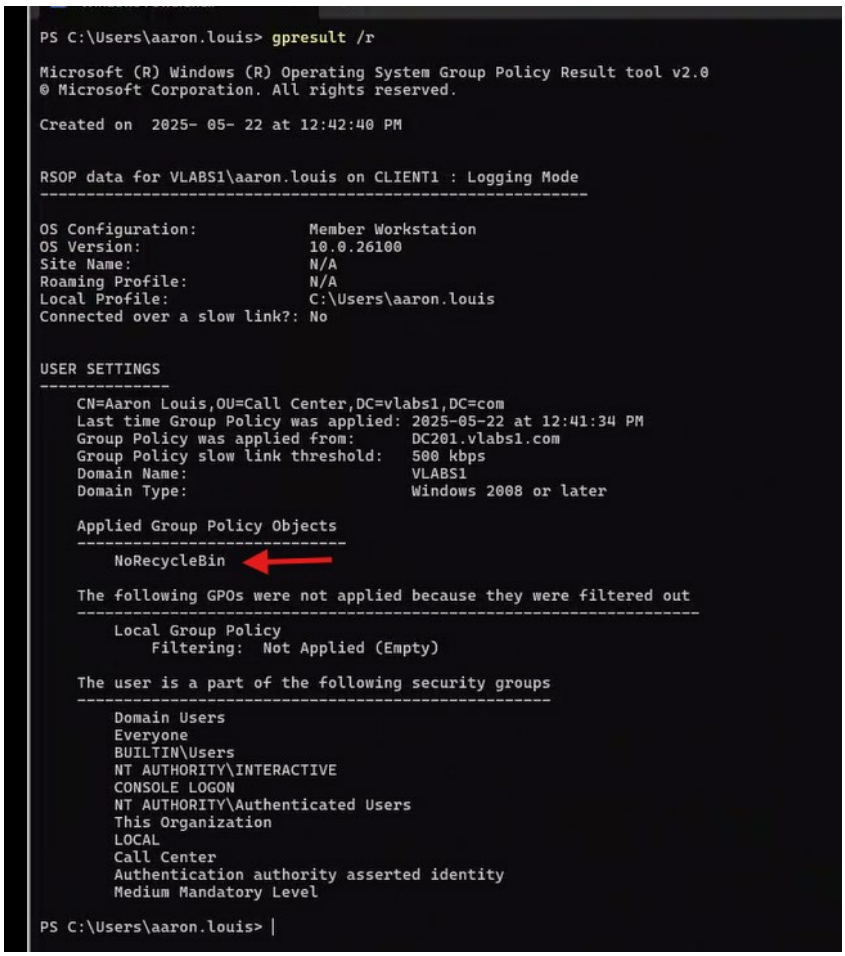


Before policy update



```
PS C:\Users\aaron.louis> gpupdate /force
Updating policy...

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

PS C:\Users\aaron.louis>
```

Verify the policy is updated
gpresult /r

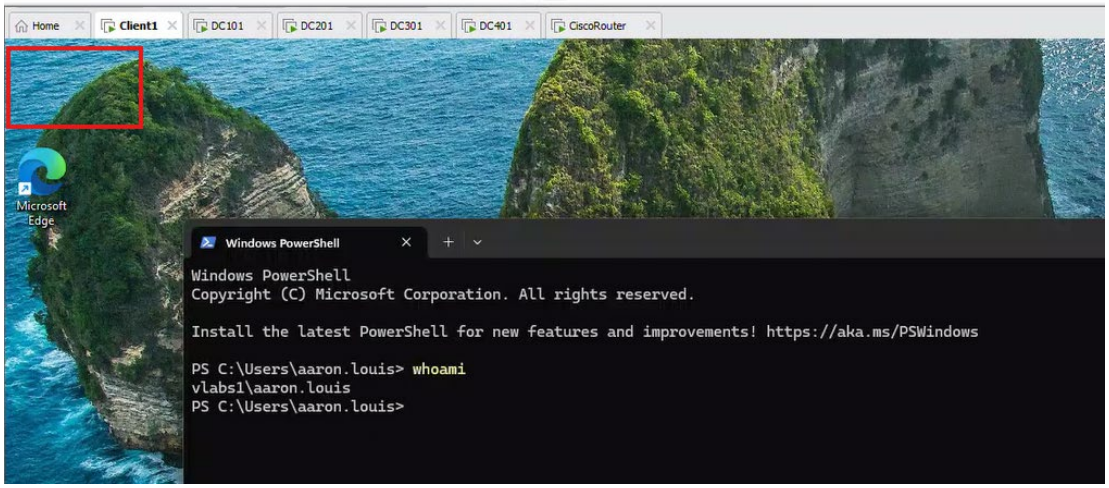


Even though `gpresult /r` shows the GPO is applied, the visual refresh of the desktop might not have happened automatically.

Solution:

1. **Restart the Explorer.exe Process:** This is often the quickest way to refresh desktop icons and settings.
    - Press `Ctrl + Shift + Esc` to open Task Manager.
    - Go to the "Processes" tab.
    - Find "Windows Explorer" (or "explorer.exe").
    - Right-click on it and select "Restart."
2. **Log Off and Log On Again:** A full log off and log on often ensures all user-specific policies are re-applied and the desktop is properly refreshed.

After that the recycle bin is not seen in the Desktop



6 Task 4: Practicing GPO Processing Order using GUI

6.1 Objective

Understand the impact of multiple GPOs.

6.2 Steps

6.2.1 Link order

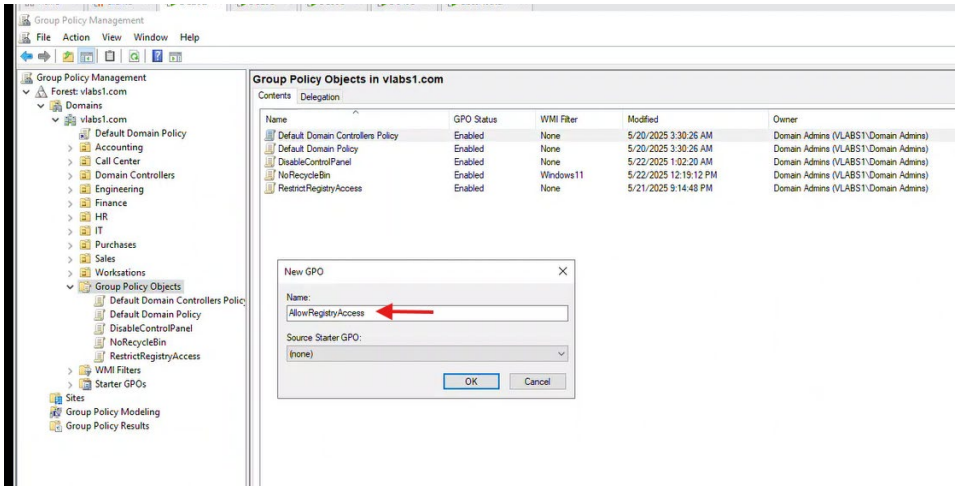
1. **Link Order**: (Don't forget to run **gpupdate /force** on the client before each test)

a) Create a new GPO named AllowRegistryAccess that grants access to the registry editing tools.

6.2.1.1 On your Domain Controller DC101

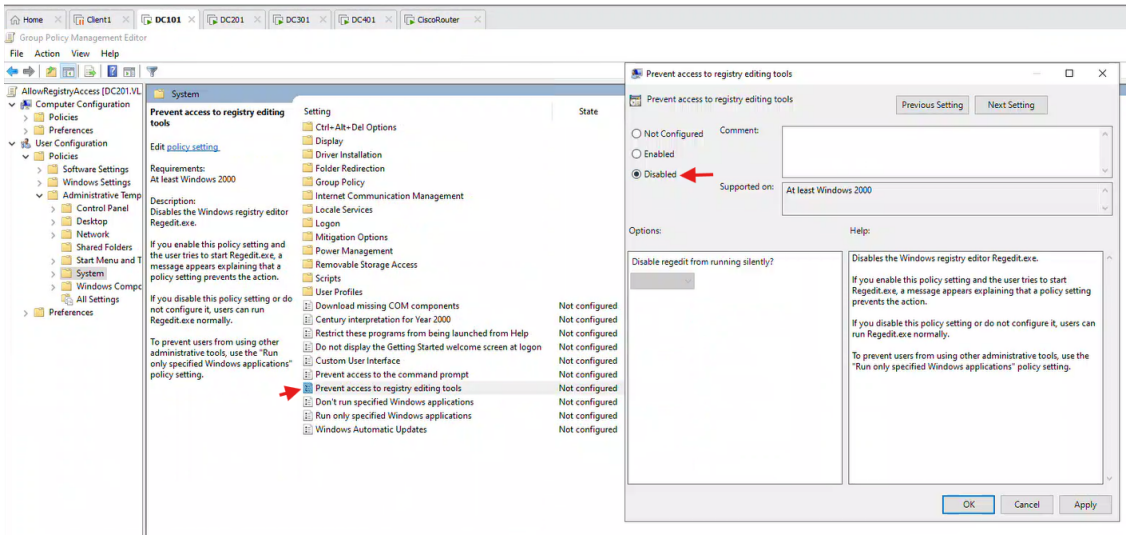
1. **Open Group Policy Management Console (GPMC):**
    - Press `Win + R`, type `gpmc.msc`, and hit **Enter**.

2. **Create a New GPO:**
    - Right-click **Group Policy Objects** → **New**.
    - Name it `AllowRegistryAccess` → Click **OK**.



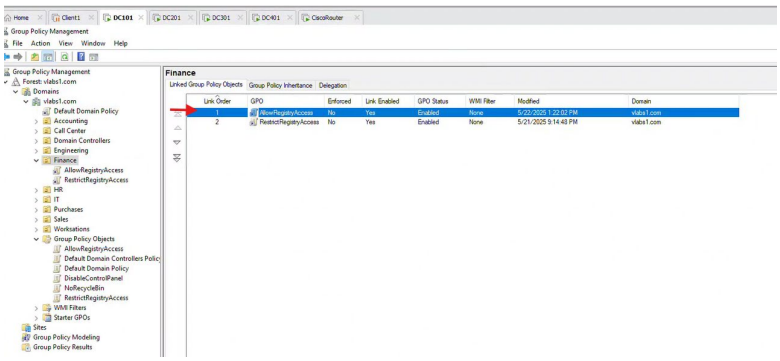
3. **Configure the GPO to Enable Registry Tools:**

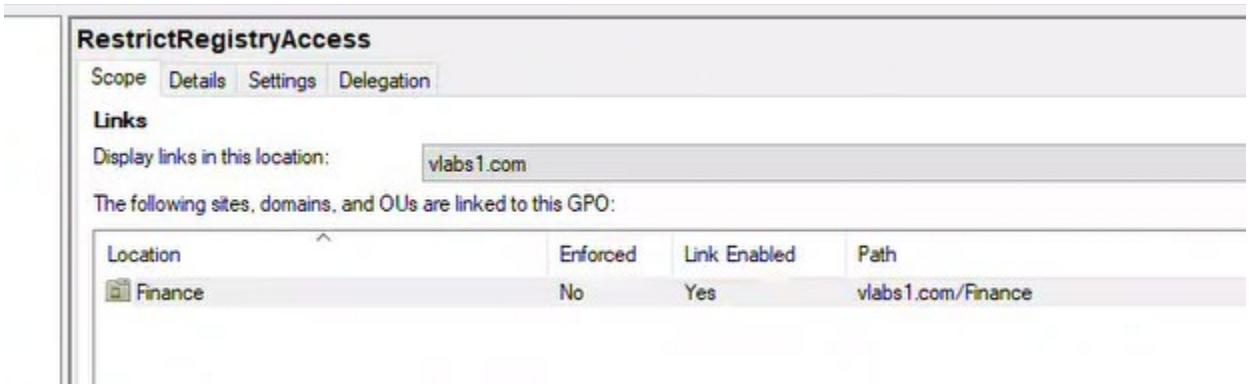
- Right-click `AllowRegistryAccess` → **Edit**.
- Navigate to: `User Configuration` → `Policies` → `Administrative Templates` → `System`
- Find **"Prevent access to registry editing tools"** → Double-click it.
- Set it to **Disabled** (this allows registry access) → Click **OK**.
- Close the **Group Policy Editor**.



b) Link it to OU **Finance** as **Order 1**.

1. In the Group Policy Management console, select **OU Finance**. In the "Link and existing GPO" tab, ensure AllowRegistryAccess is listed and move it to **Order 1** if there are other GPOs linked.

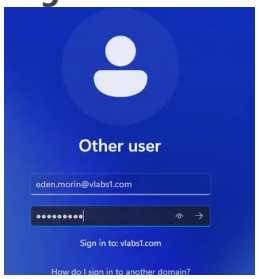




6.2.1.2 On Client1

Test using **Eden Morin** to ensure he now has access to the registry.
Force a Group Policy Update on Eden Morin's Machine

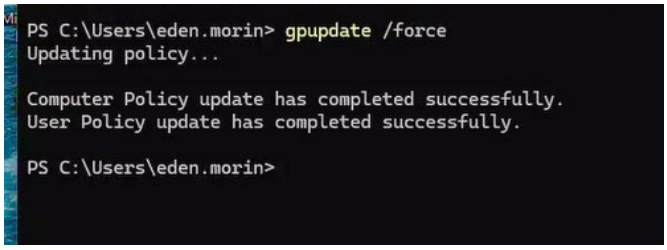
1. **Log in as Eden Morin**



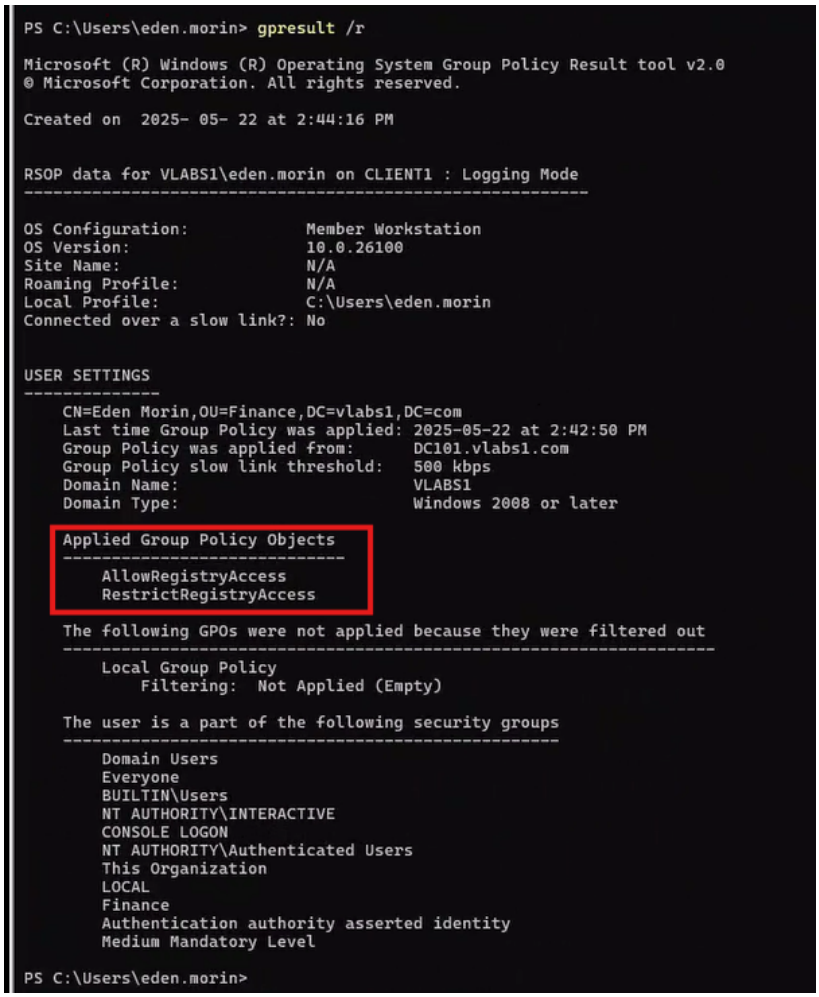
2. **Open Command Prompt as Administrator** and run:

```
gpupdate /force
```

3. Wait for the policy to apply (should see **"Computer Policy update has completed successfully"**).

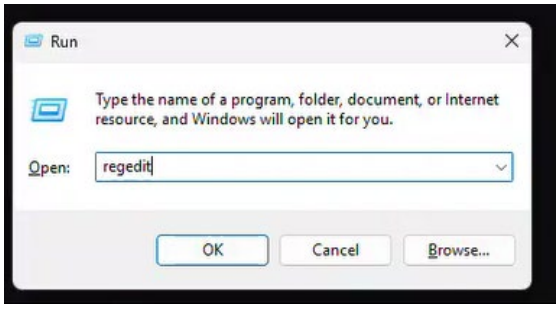


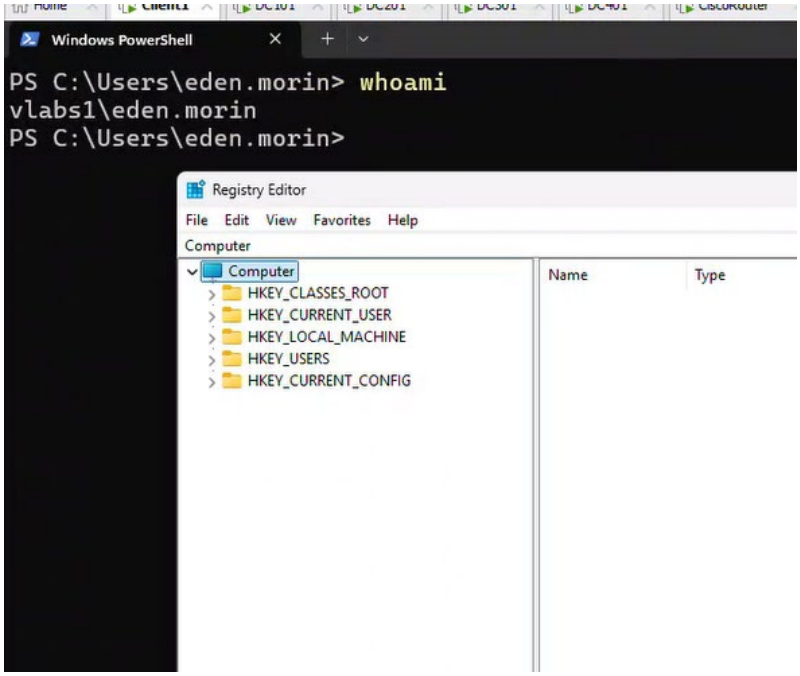
4. Verify the policy is updated
   gpresult /r



5. Test Registry Access

1. **Open Registry Editor:**
    - Press `Win + R`, type `regedit`, and hit **Enter**.
2. **Expected Result:**
    - **Registry Editor should open successfully** because the `AllowRegistryAccess` GPO (set to **Disabled**) overrides any restrictions.





AllowRegistryAccess (Order 1) → Allows Registry Access (since it's set to Disabled, meaning it explicitly allows regedit).

GPOs apply in reverse order (higher priority = processed last, so it wins).

Eden Morin now has access to regedit because the allowing policy takes precedence.

6.2.2 Precedence rules

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

6.2.2.1 On DC101

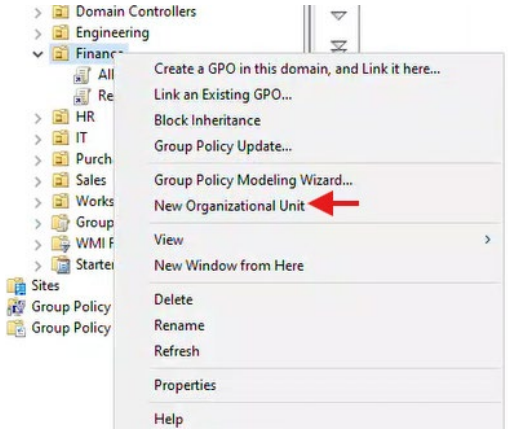
1. Create OU **Finance-Admins** inside the OU **Finance** and move **Eden Morin** to it.

a) **Open Active Directory Users and Computers (ADUC):**

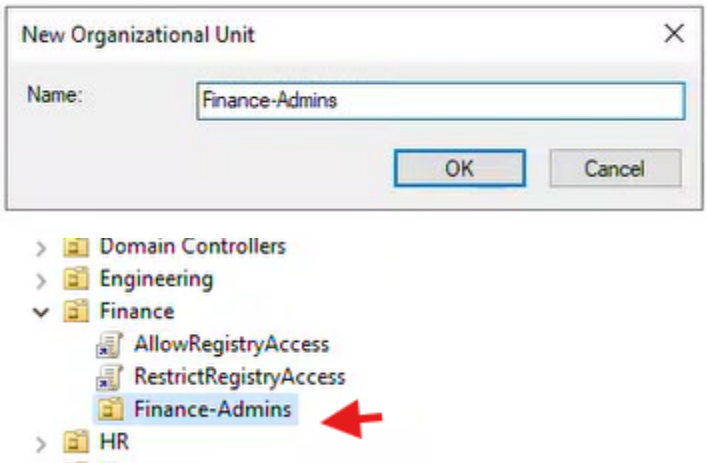
- Press Win + R, type dsa.msc, and hit **Enter**.

b) **Create a New OU Inside Finance:**

- Right-click **Finance OU** → **New** → **Organizational Unit**.

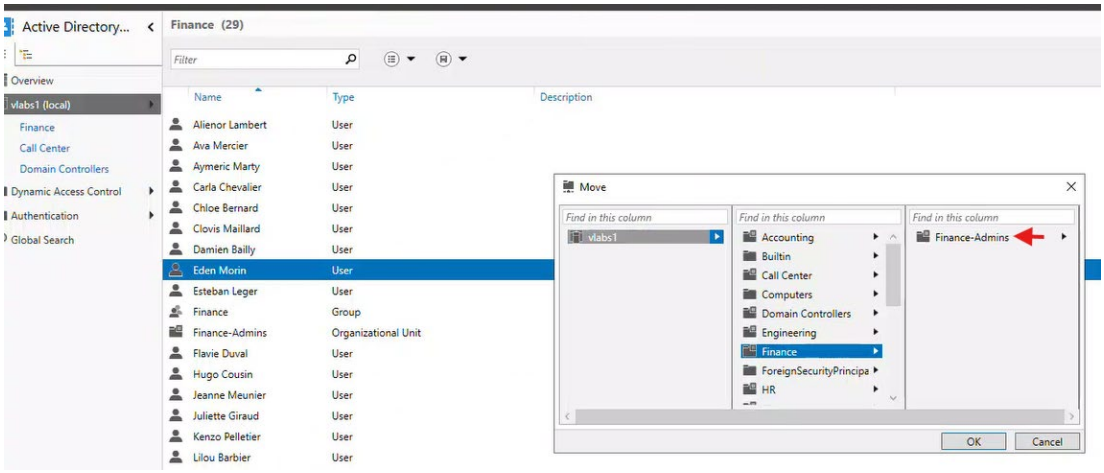


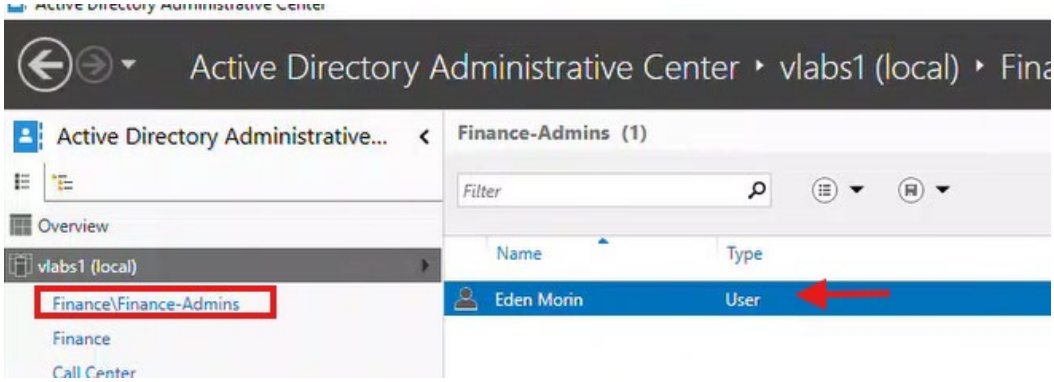
- Name it **Finance-Admins** → Click **OK**.



c) **Move Eden Morin to Finance-Admins OU:**

- Locate **Eden Morin's user account** (under **Finance** or another OU).
- Right-click **Eden Morin** → **Move**.
- Select **Finance-Admins OU** → Click **OK**.



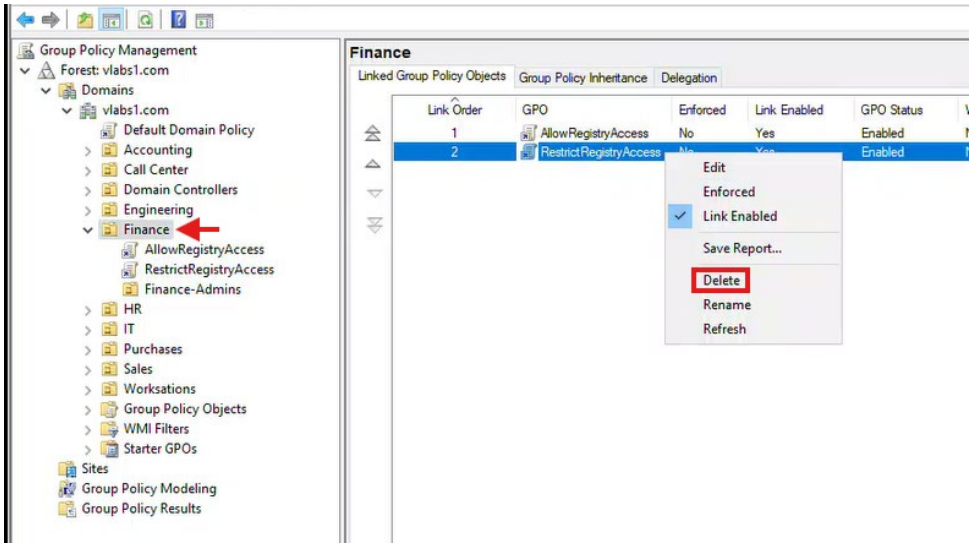


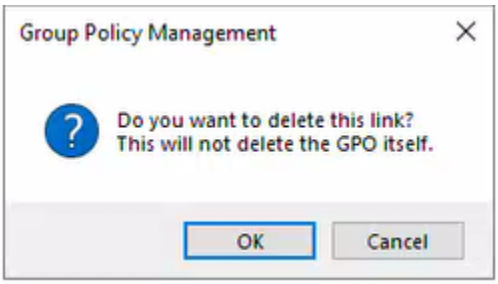
2. Unlink the GPO **RestrictRegistryAccess** from OU **Finance** and link it to OU Finance-Admins.

Move the RestrictRegistryAccess GPO to Finance-Admins OU

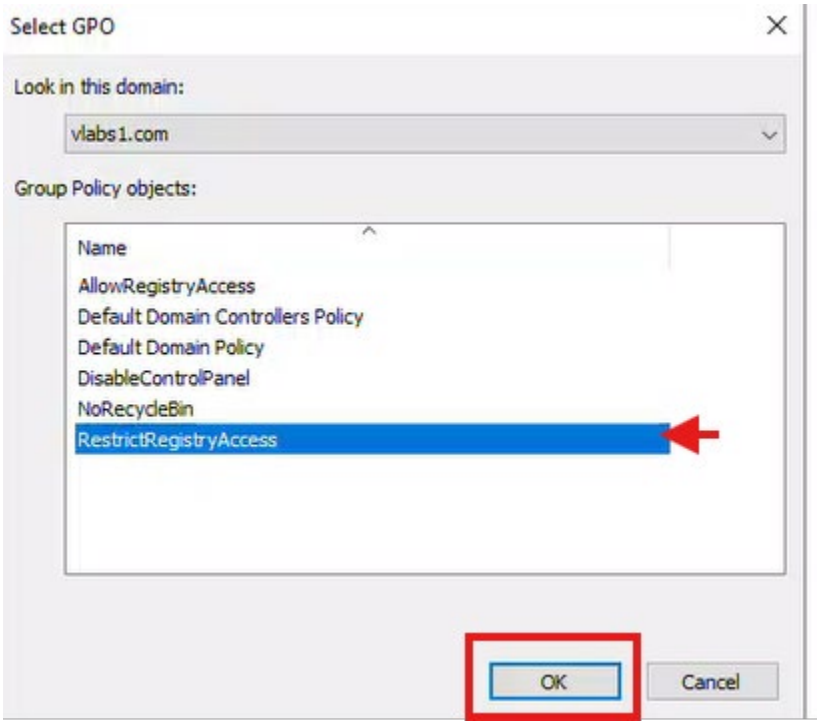
a) **Open Group Policy Management Console (GPMC):**
   - Press Win + R, type gpmc.msc, and hit **Enter**.

b) **Unlink RestrictRegistryAccess from Finance OU:**
   - Go to: Forest → Domains → vlabs1.com → Organizational Units → Finance
   - Under **Linked Group Policy Objects**, right-click **RestrictRegistryAccess** → **Delete**.

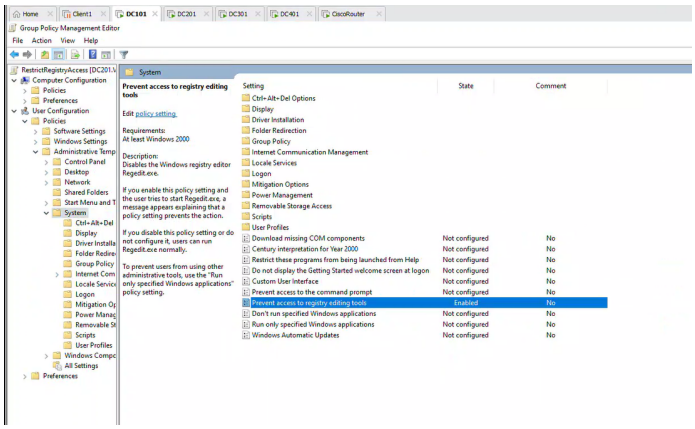




c) **Link RestrictRegistryAccess to Finance-Admins OU:**
   - Right-click **Finance-Admins OU** → **Link an Existing GPO**.
   - Select **RestrictRegistryAccess** → Click **OK**.



Check is enabled



6.2.2.2 On client1

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

a. Update policy

```
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>
```

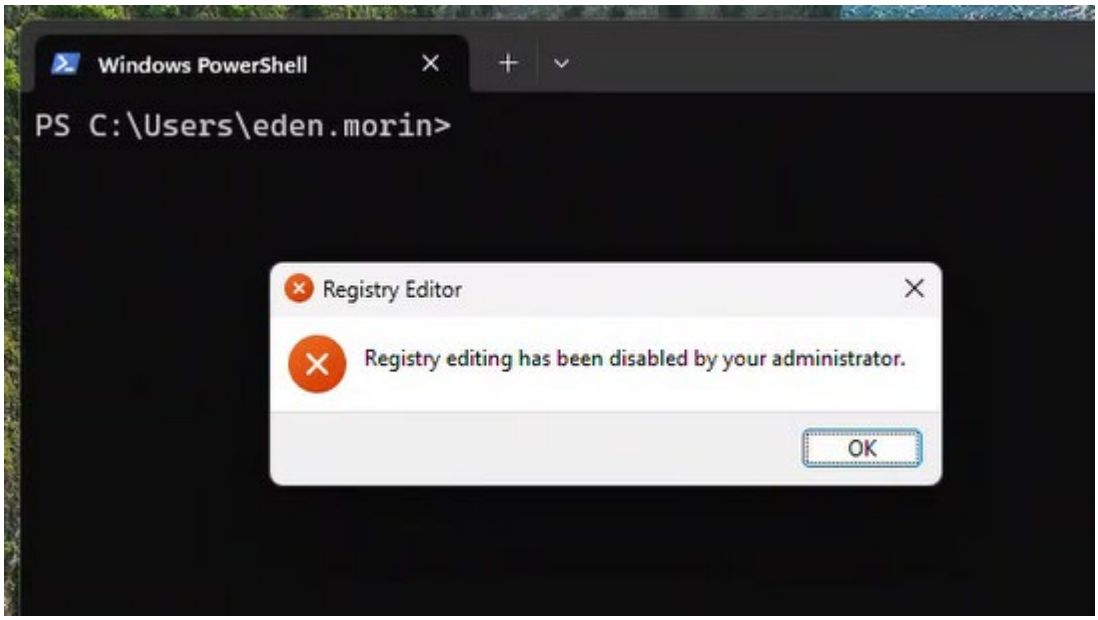
b. Verify policies

```
PS C:\Users\eden.morin> gpresult /r

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© Microsoft Corporation. All rights reserved.

Created on  2025- 05- 22 at 6:49:40 PM


RSOP data for VLABS1\eden.morin on CLIENT1 : Logging Mode
-------------------------------------------------------

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


USER SETTINGS
--------------
    CN=Eden Morin,OU=Finance-Admins,OU=Finance,DC=vlabs1,DC=com
    Last time Group Policy was applied: 2025-05-22 at 5:06:38 PM
    Group Policy was applied from:      DC201.vlabs1.com
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        VLABS1
    Domain Type:                        Windows 2008 or later

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

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

    The user is a part of the following security groups
    ---------------------------------------------------
        Domain Users
        Everyone
        BUILTIN\Users
        NT AUTHORITY\INTERACTIVE
        CONSOLE LOGON
        NT AUTHORITY\Authenticated Users
        This Organization
        LOCAL
        Finance
        Authentication authority asserted identity
        Medium Mandatory Level

PS C:\Users\eden.morin>
```

c. Test Registry Access

1. **Open Registry Editor:**
    - Press Win + R, type regedit, and hit **Enter**.
2. **Expected Result:**
    - **Registry Editor should be blocked** because:
        - The **RestrictRegistryAccess** GPO is now linked **directly to Finance-Admins OU** (where Eden is located).
        - **Child OU policies take precedence over parent OU policies** (even if AllowRegistryAccess is still linked to Finance OU).

RestrictRegistryAccess **(Linked to Finance-Admins OU)** → **Blocks Registry Access** (wins because it's applied to the child OU).
AllowRegistryAccess **(Linked to Finance OU)** → **Still exists but is overridden** by the more specific policy.
GPOs apply from child OUs first, meaning policies closest to the user/computer take precedence.



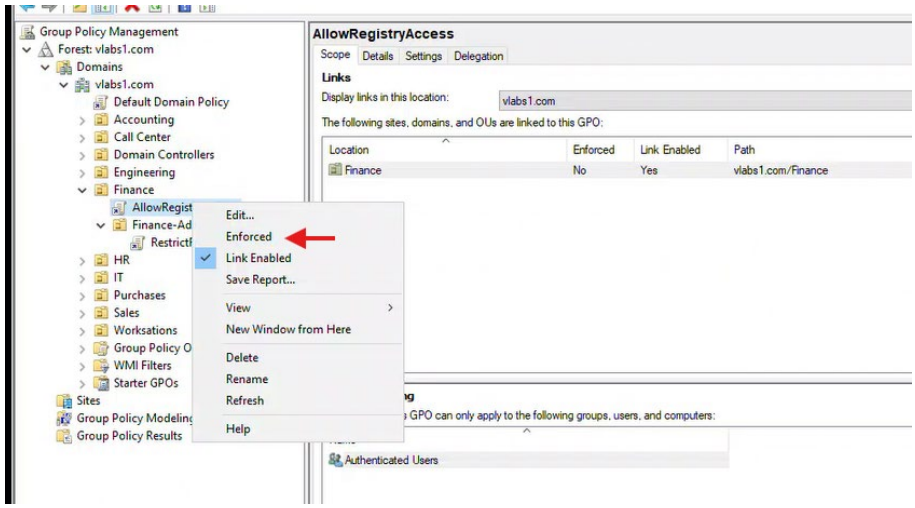
6.2.3 Enforced GPO

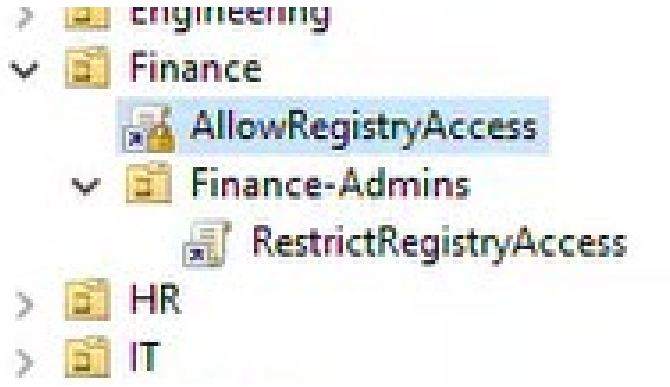
Enforced GPO: (Don't forget to run **gpupdate /force** on the client before each test)

6.2.3.1 On DC101

Enforce the AllowRegistryAccess GPO on OU Finance.

1. **Open Group Policy Management Console (GPMC):**
    - Press Win + R, type gpmc.msc, and hit **Enter**.
2. **Locate the GPO Link in Finance OU:**
    - Go to: Forest → Domains → vlabs1.com → Organizational Units → Finance
    - Under **Linked Group Policy Objects**, right-click **AllowRegistryAccess**.
3. **Enable Enforced (No Override):**
    - Select **Enforced** (this ensures the policy applies even if child OUs block inheritance).
    - The GPO link should now show a **lock icon** indicating it is enforced.

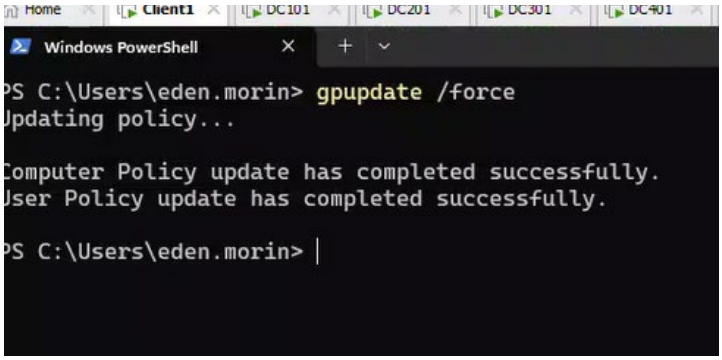




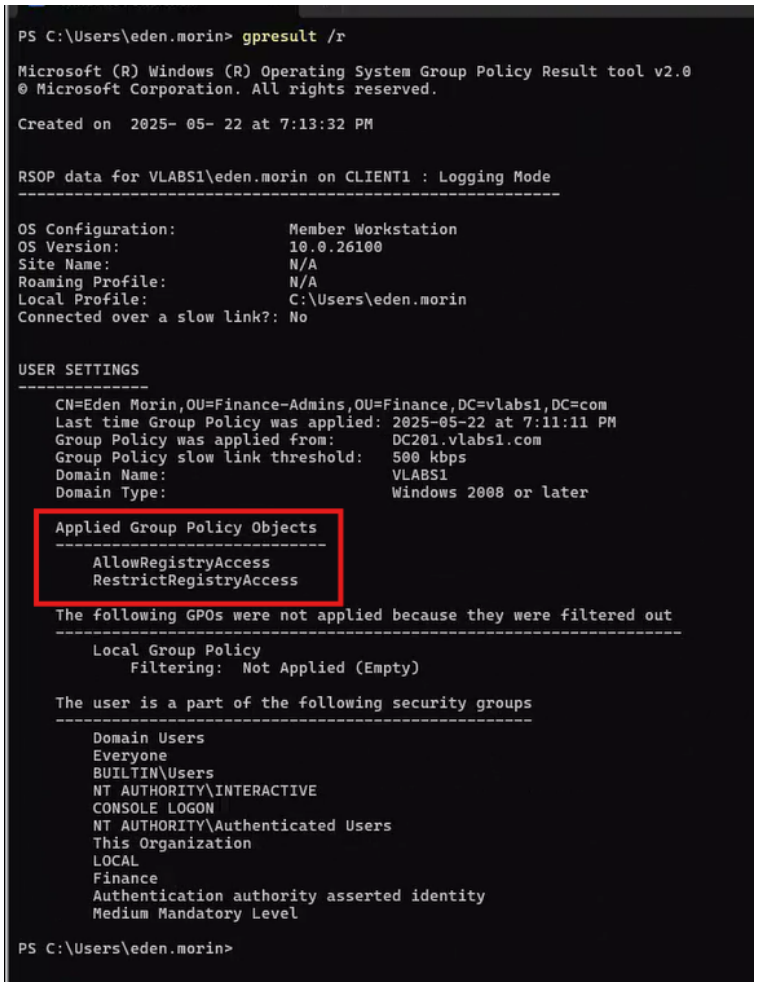
6.2.3.2 On Client1

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

a. Update policy



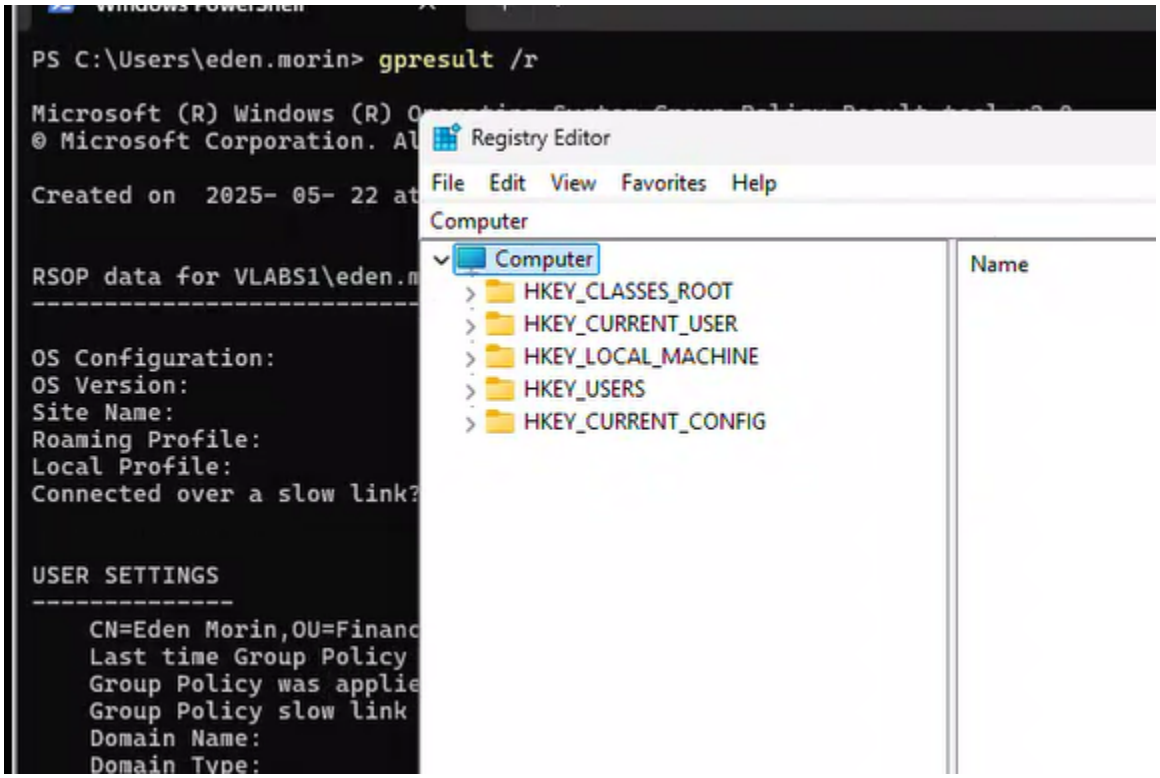
b. Verify policy



c. Test **Registry Access**

1. **Open Registry Editor:**
    - Press Win + R, type regedit, and hit **Enter**.
2. **Expected Result:**
    - **Registry Editor should open successfully** because:
        - The **Enforced** setting on AllowRegistryAccess overrides the RestrictRegistryAccess policy in the child OU.
        - **Enforced GPOs cannot be blocked by Block Inheritance.**

AllowRegistryAccess (Enforced on Finance OU) → Overrides all conflicting policies, even in child OUs.
RestrictRegistryAccess (Linked to Finance-Admins OU) → Normally blocks access, but is bypassed due to Enforced setting.
Enforced GPOs take highest priority (even above Block Inheritance).



6.2.4 Block inheritance

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

- Remove Enforce the **AllowRegistryAccess** GPO on OU **Finance**.
- Block inheritance on OU **Finance-Admins**.
- Test using **Eden Morin** to ensure the registry **editing tools** are now blocked.

6.2.5 Link enabled

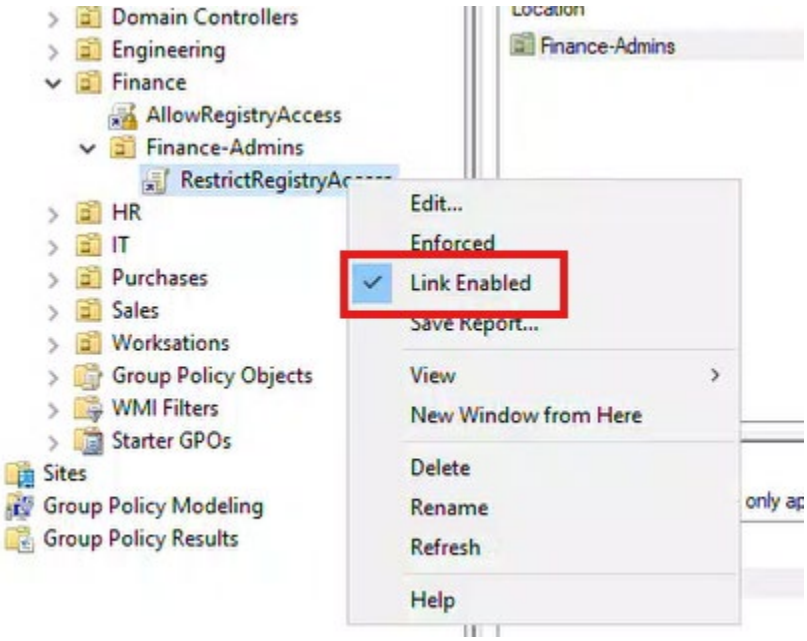
Link Enabled: (Don't forget to run **gpupdate /force** on the client before each test)

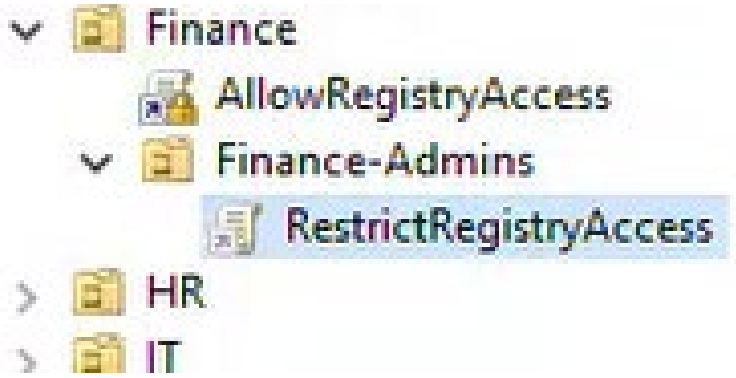
Verify how disabling a GPO link affects policy application by testing registry access for Eden Morin.

6.2.5.1 DC101

Uncheck **Link Enabled** on the **RestrictRegistryAccess** GPO on OU **Finance-Admins**

1. **Open Group Policy Management Console (GPMC):**
    - Press Win + R, type gpmc.msc, and hit **Enter**
2. **Navigate to the Finance-Admins OU:**
    - Expand: Forest → Domains → vlabs1.com → Organizational Units → Finance → Finance-Admins
3. **Disable the RestrictRegistryAccess GPO Link:**
    - In the **Linked Group Policy Objects** list:
        - Right-click **RestrictRegistryAccess**
        - Uncheck **Link Enabled** (this disables the GPO link while keeping it in place)
    - The GPO will now appear with a grayed-out icon





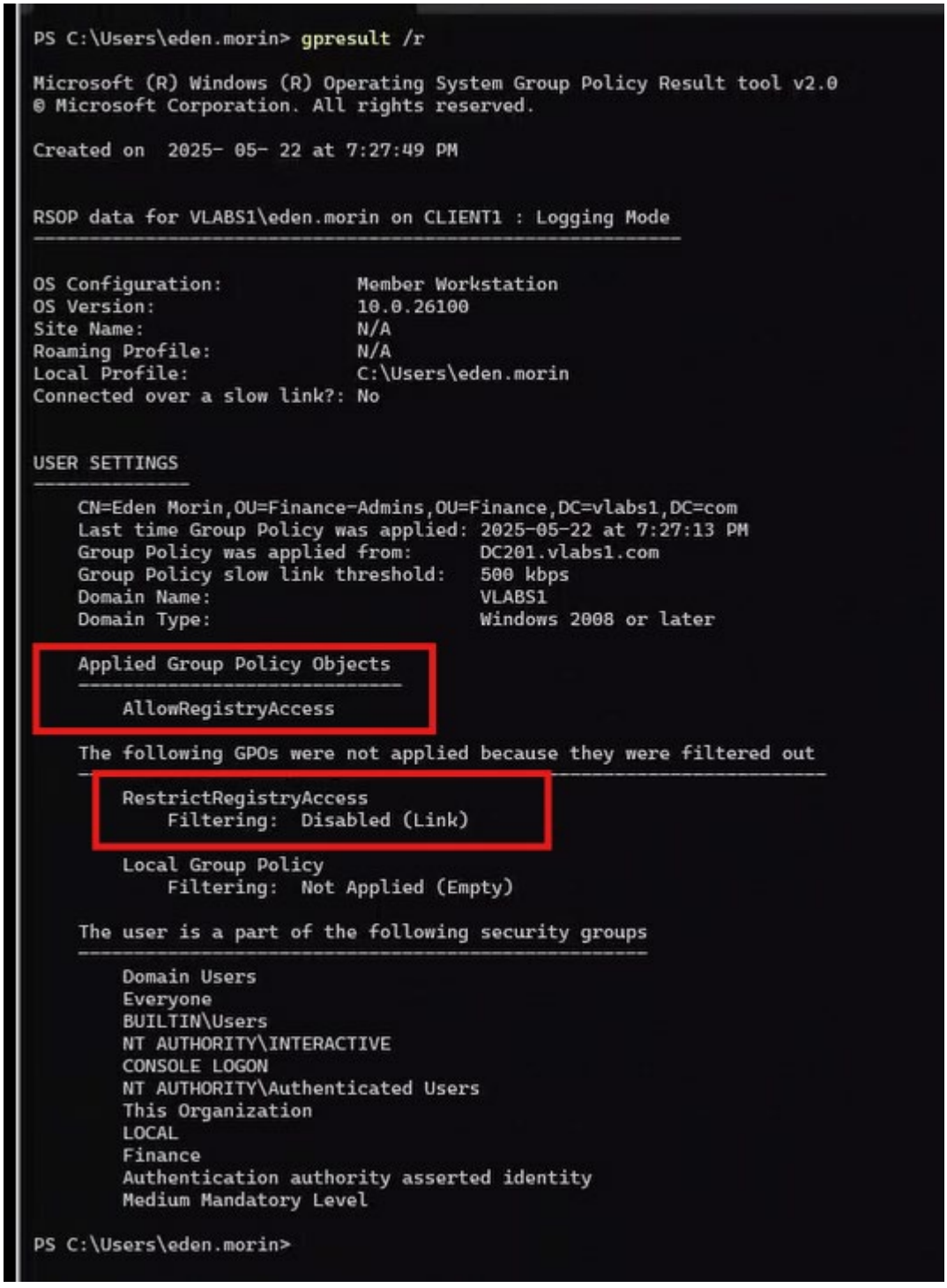
6.2.5.2 Client1

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

a. Update policy

```
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>
```

b. Update policy

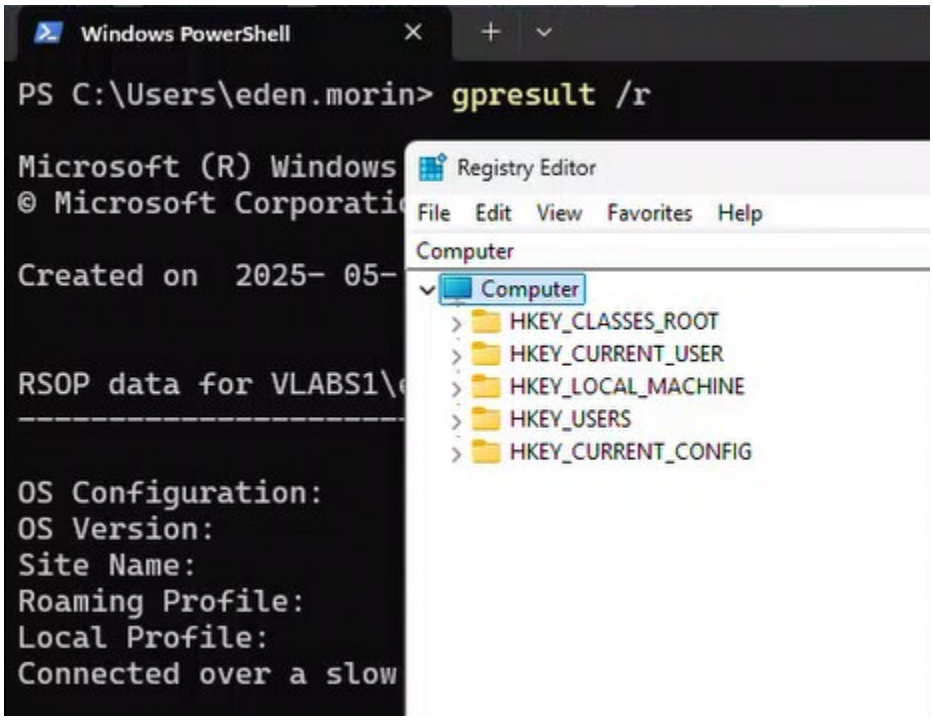


c. Test regedit

1. **Attempt to open Registry Editor:**
    - Press Win + R, type regedit, hit **Enter**
2. **Expected Result:**

- **Registry Editor opens successfully** because:
  - The RestrictRegistryAccess GPO is effectively disabled (link disabled)
  - Only the AllowRegistryAccess GPO (from parent Finance OU) applies

Setting	Effect	Current Status
Link Enabled	When unchecked, the GPO does not apply to the OU	Disabled for RestrictRegistryAccess
AllowRegistryAccess	Still linked and enforced at parent OU	Active
Result	Registry access allowed because restrictive policy is not applied	Eden can use regedit



7 Task 5: Exploring Default Group Policy Objects using GUI

Analyze the Default Domain Policy and Default Domain Controllers Policy without making modifications.

7.1 Objective

Understand and analyze the impact of Default Domain Policy and Default Domain Controllers Policy.

7.2 Steps

7.2.1 Identify and review the **two default GPOs** in the domain.

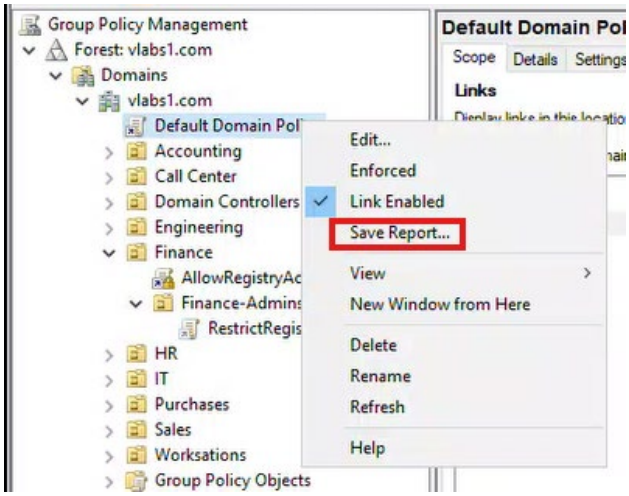
a. **Open Group Policy Management Console (GPMC):**
   - Press Win + R, type gpmc.msc, and hit **Enter**.

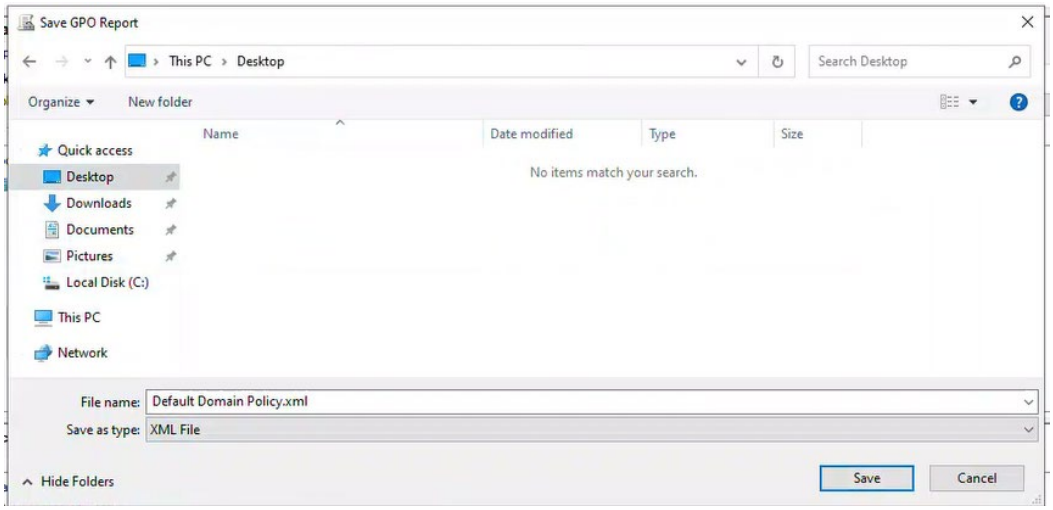
b. **Locate Default GPOs:**
   - Under your domain, you will see two default GPOs:
     - **Default Domain Policy** (applies to all domain-joined computers & users)
     - **Default Domain Controllers Policy** (applies only to Domain Controllers)

7.2.2 Generate a **Settings Report** for both policies.

7.2.2.1 For Default Domain Policy:

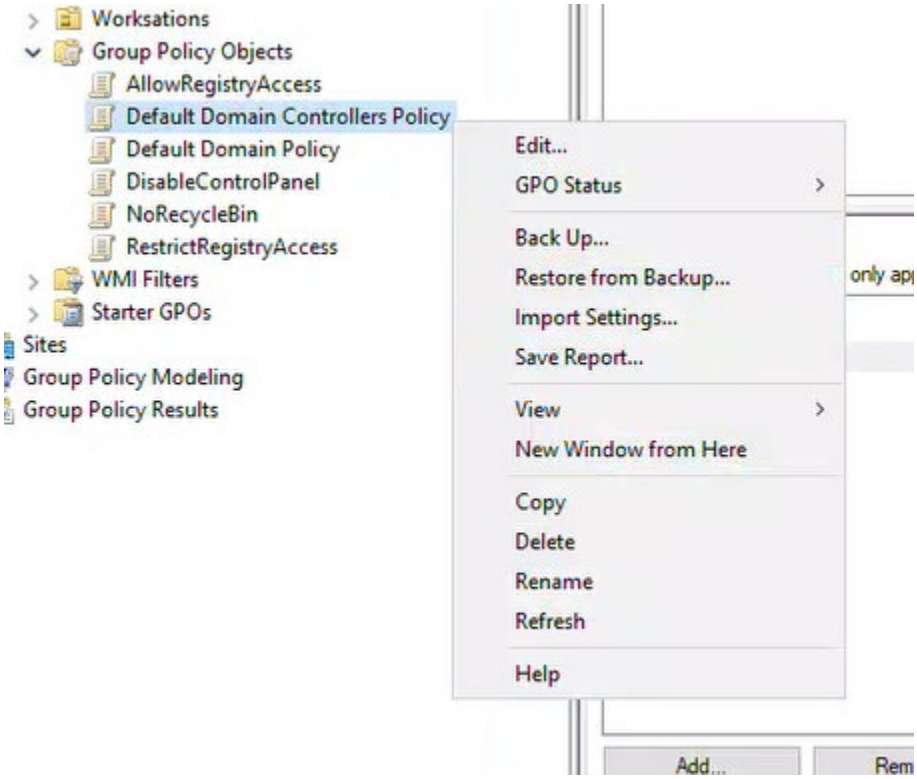
1. Right-click **Default Domain Policy** → **Save Report**.
2. Choose a location (e.g., Desktop) and save as **HTML** or **XML**.
3. Open the report and review key settings:
   - **Password Policy** (minimum length, complexity)
   - **Account Lockout Policy**
   - **Kerberos Policy**
   - **User Rights Assignments**

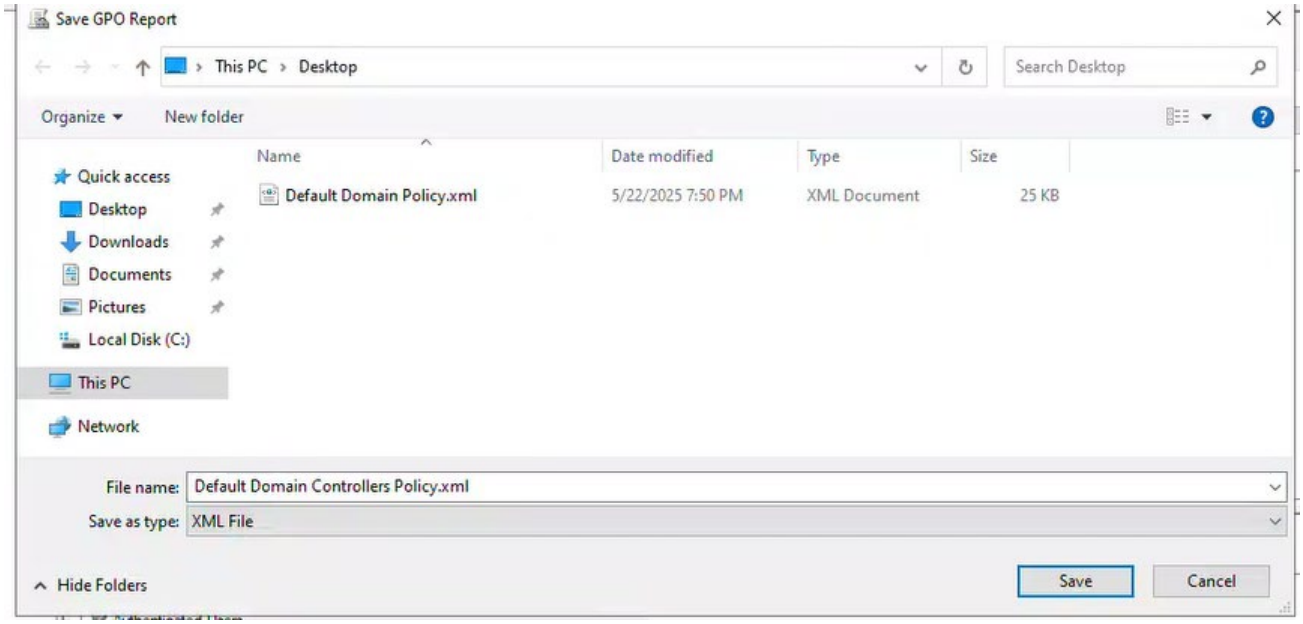




7.2.2.2 For Default Domain Controllers Policy:

1. Right-click **Default Domain Controllers Policy** → **Save Report**.
2. Save the report and analyze:
    - **Logon Rights** (e.g., "Allow log on locally" for Admins)
    - **Audit Policies** (security logging)
    - **User Rights** (restrictions on DCs)

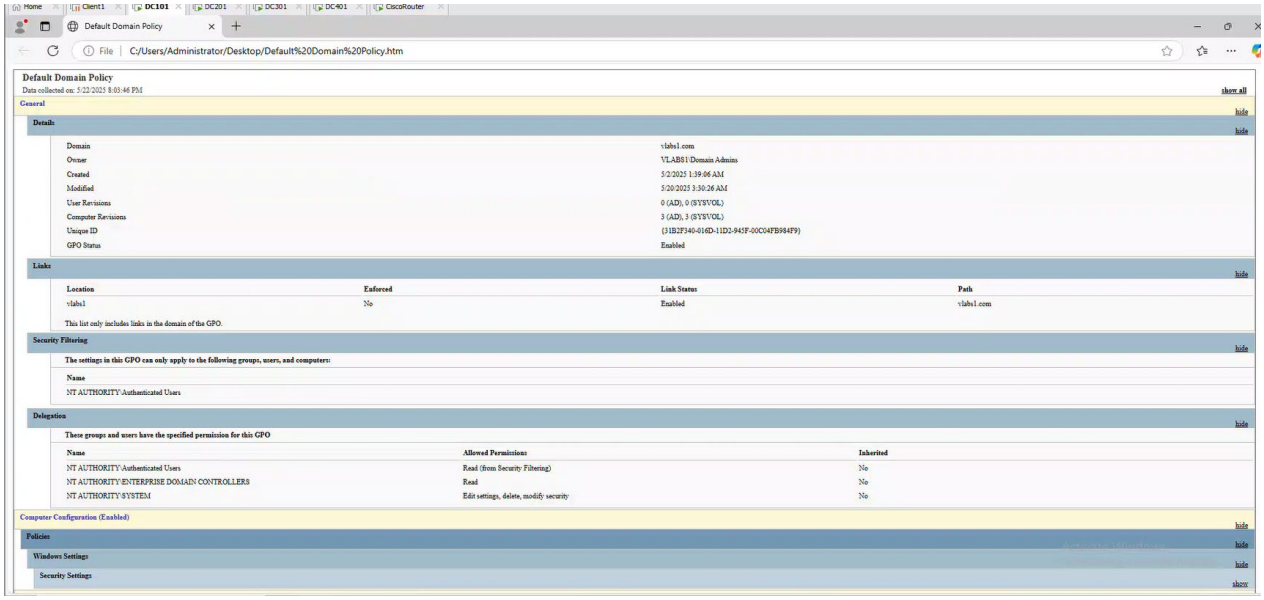




7.2.3 Analyze the impact of these GPOs

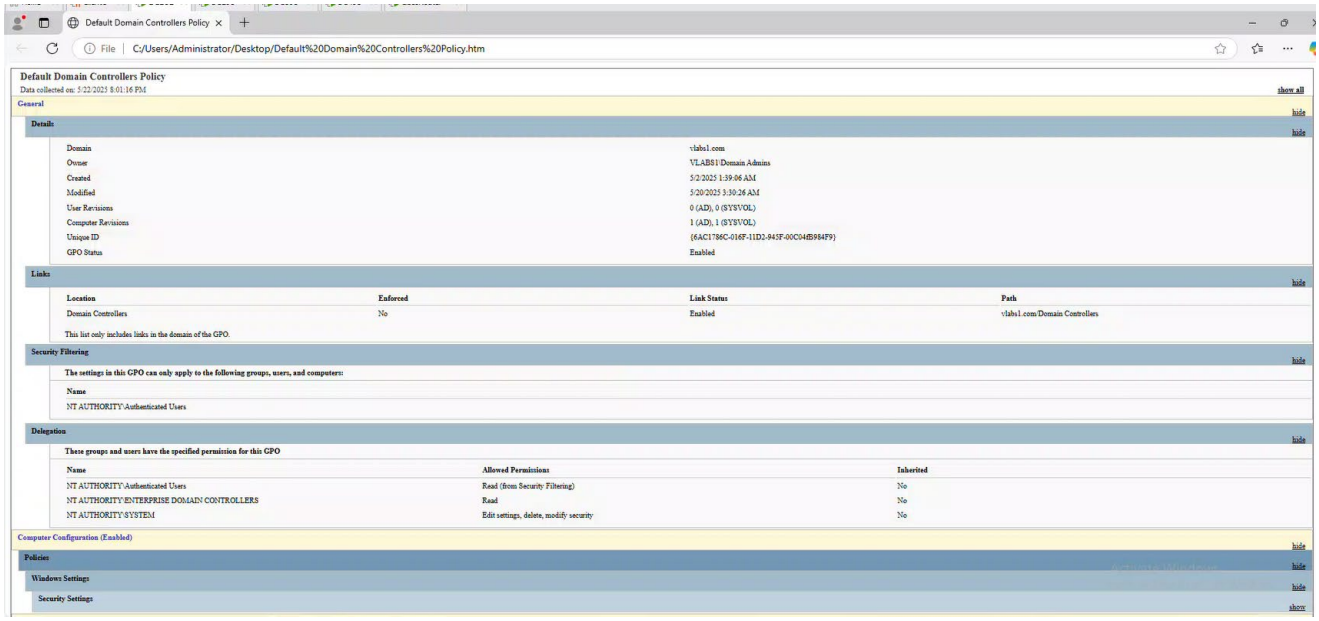
Analyze the impact of these GPOs without making any modifications or testing at this stage.

7.2.3.1 Default Domain Policy



- **Applies to:** All users and computers in the domain.
- **Key Functions:**
  - Sets **domain-wide security policies** (password rules, account lockout).
  - Configures **default user permissions**.
- **Why It Matters:**
  - Changing this can affect **every machine & user in the domain**.

7.2.3.2 Default Domain Controllers Policy:



- **Applies to:** Only **Domain Controllers** (in the "Domain Controllers" OU).
- **Key Functions:**
    - Restricts **who can log on to DCs** (security hardening).
    - Configures **audit policies** (tracks security events).
- **Why It Matters:**
    - Protects **critical servers** from unauthorized access.

GPO	Applies To	Key Settings	Impact if Modified
Default Domain Policy	All domain users & computers	Password policy, account lockout	Affects entire domain security
Default Domain Controllers Policy	Only Domain Controllers	Logon rights, audit policies	Impacts DC security & logging