ASSIGNMENT 2

Part 1

MAY 20, 2025

NETWORK INSTALLATION AND ADMINISTRATION II

Laetitia Mohammed, 0931512

Contents

Task 1: Configuring Group Policy using GUI

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

GPO Name: **RestrictRegistryAccess**

Steps:

Create a new GPO named **RestrictRegistryAccess.**

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

Link the GPO to the Finance OU.

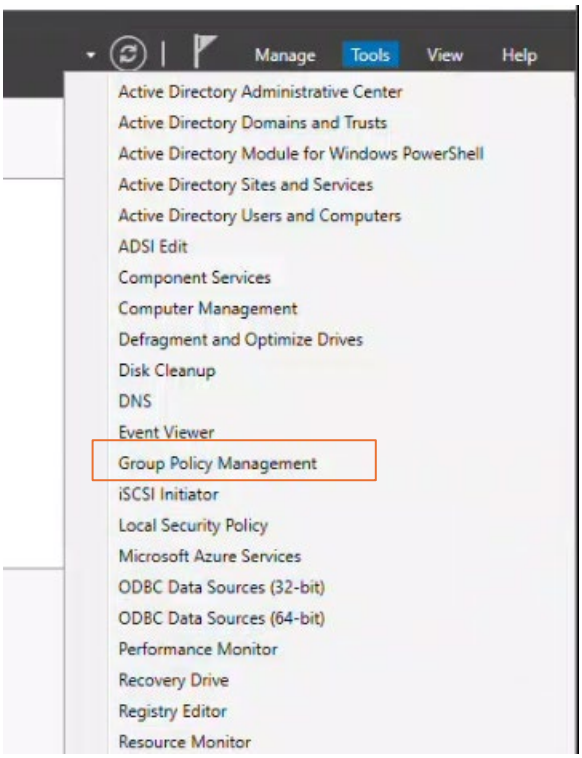
Use Security Filtering to ensure that Ava Mercier from Finance is not affected by this GPO

Testing:

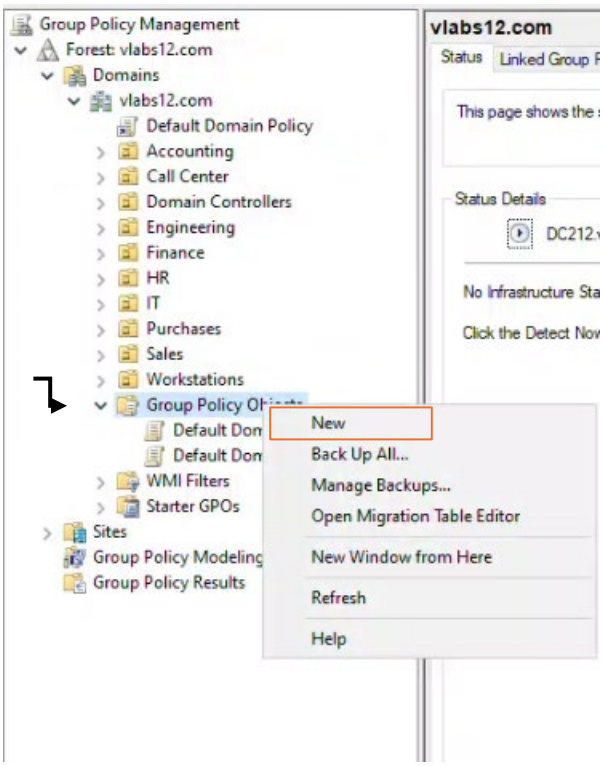
Log in to Client12 with any Finance user and verify that the registry editing tools are blocked

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

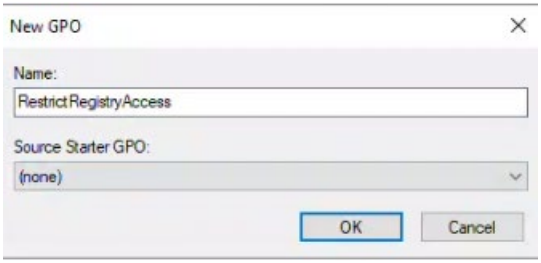
Create a new GPO named **RestrictRegistryAccess.** On DC112, go to Tools → Group Policy Management



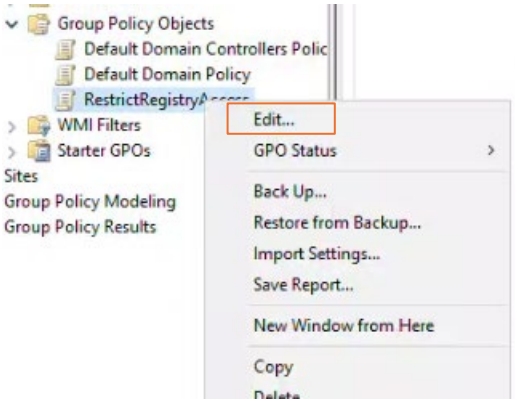
Expand vlab12.com → Group Policy Object. Right click and select New



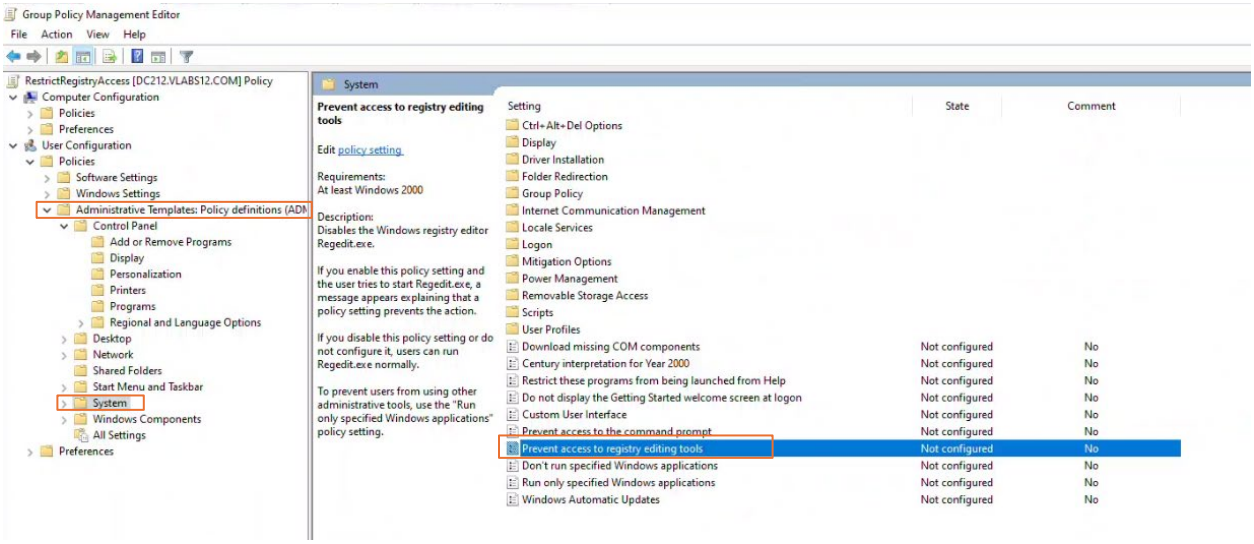
Name it **RestrictRegistryAccess** and click OK.



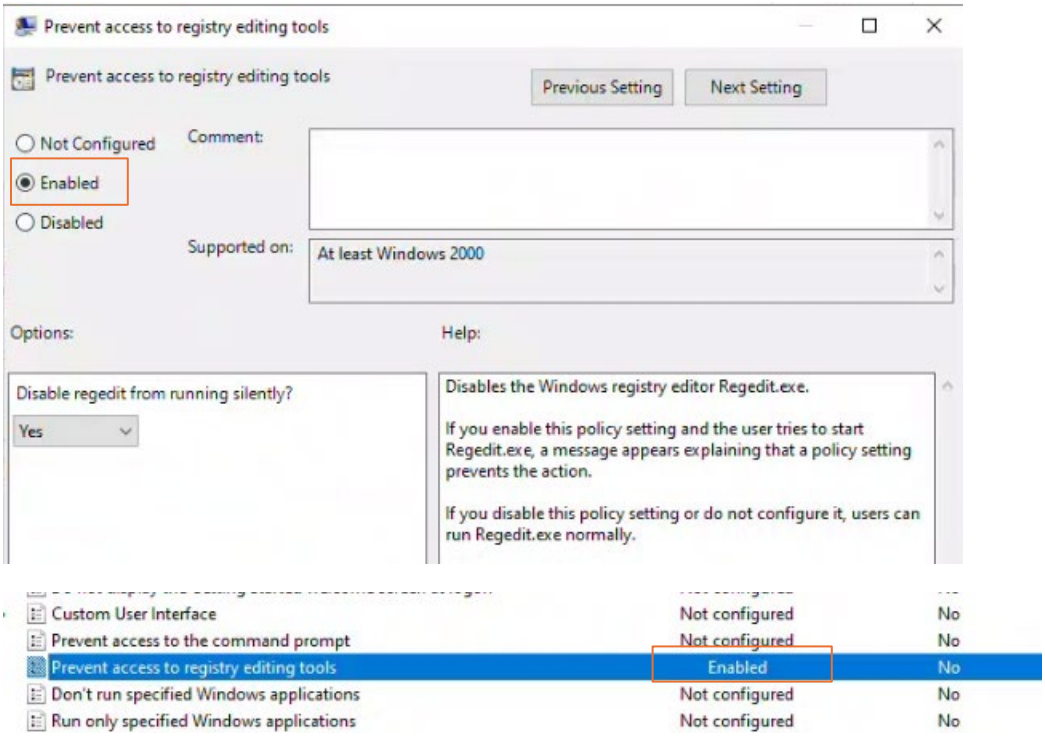
Configure the required setting to block access to the registry editing tools. Right-click on the new GPO and select Edit



Under User Configuration → Policies → Administrative Templates → System, you'll find on the right, in the details section the option to block access to the registry editing tools

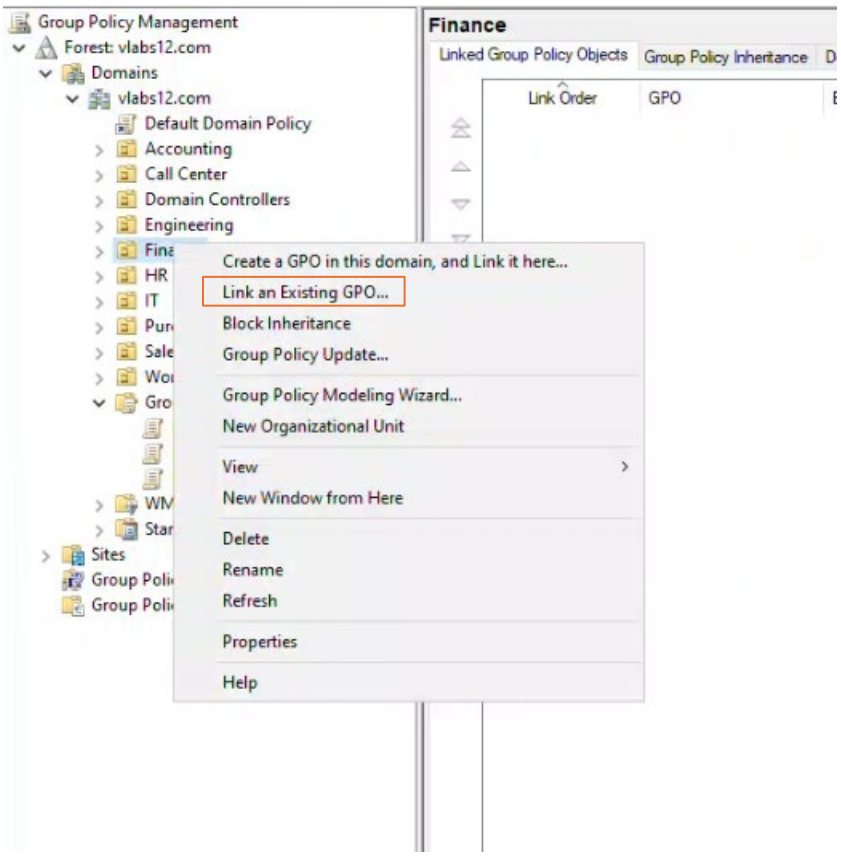


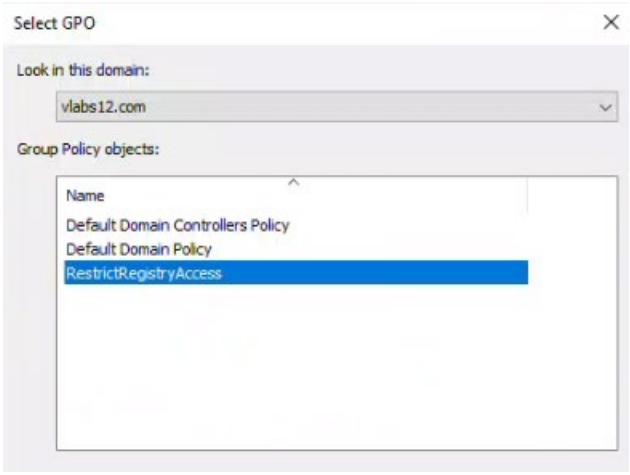
Select "Enabled" and OK

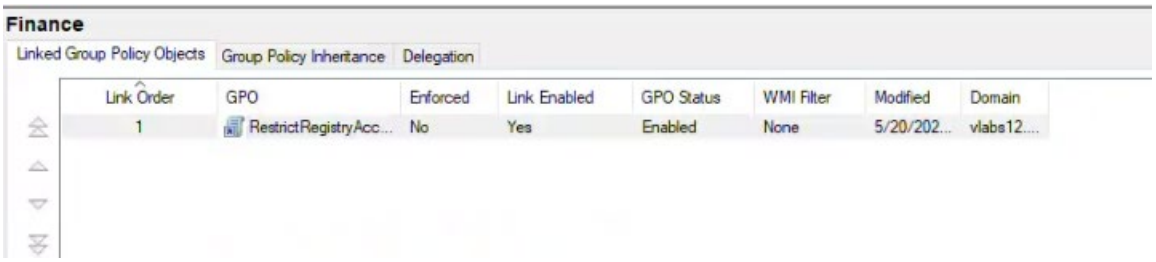


Link the GPO to the Finance OU.

In Group Policy Management, right-click the Finance OU → Link an Existing GPO, and choose RestrictRegistryAccess

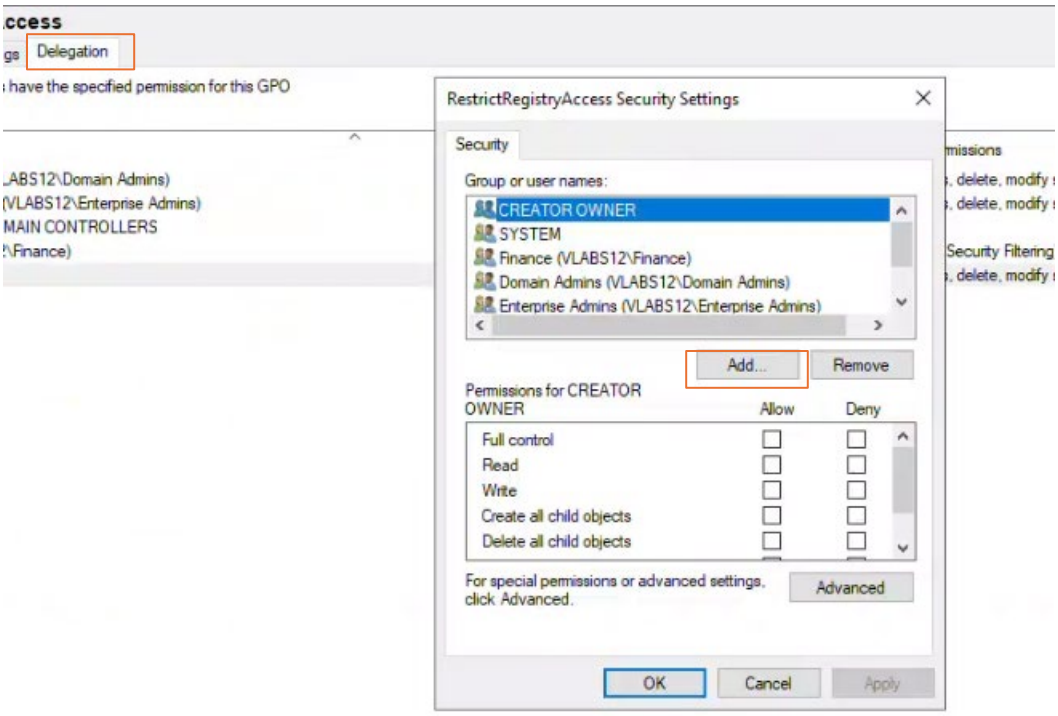

Group Policy Management
Forest: vlabs12.com
Domains
vlabs12.com
Default Domain Policy
Accounting
Call Center
Domain Controllers
Engineering
HR
IT
Sites
Finance
Linked Group Policy Objects
Group Policy Inheritance
Link Order
GPO
Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance
Group Policy Update...
Group Policy Modeling Wizard...
New Organizational Unit
View
New Window from Here
Delete
Rename
Refresh
Properties
Help

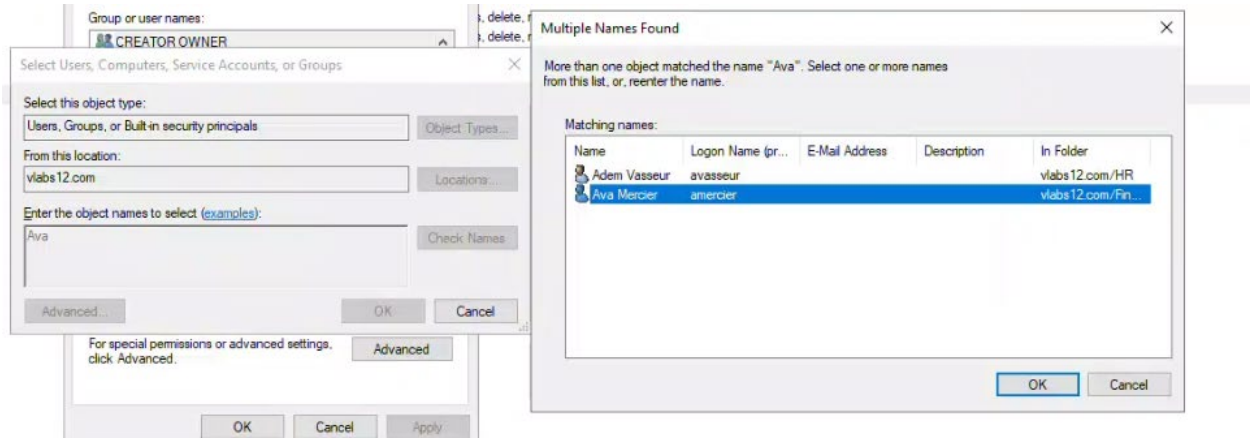

Select GPO
Look in this domain:
vlabs12.com
Group Policy objects:
Name
Default Domain Controllers Policy
Default Domain Policy
RestrictRegistryAccess


Finance
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO Status
WMI Filter
Modified
Domain
1
RestrictRegistryAcc...
No
Yes
Enabled
None
5/20/202...
vlabs12....

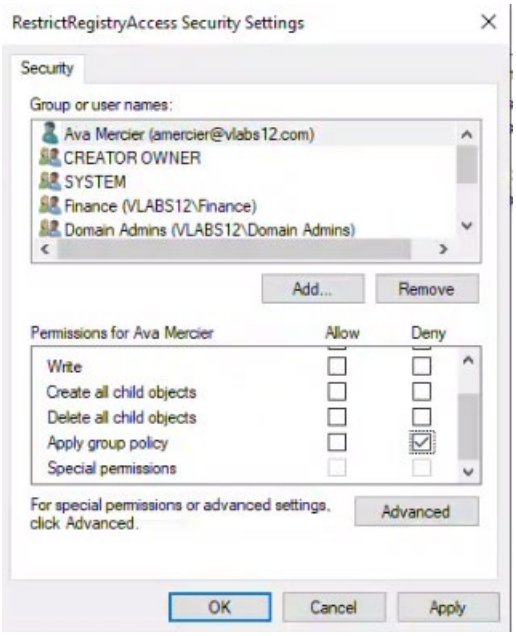
We have to go to the Delegation tab to add the user Ava Mercier and deny the GPO for her

Delegation → Advanced → Add

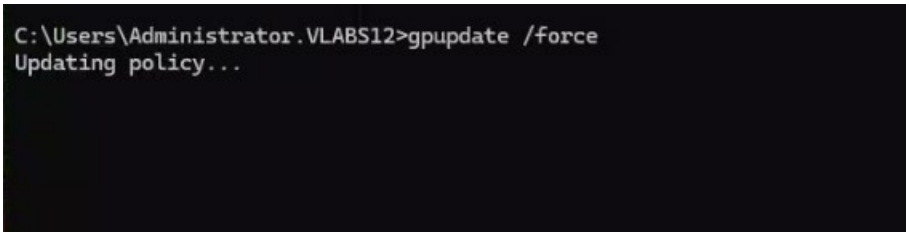




Once she's added, check the box "Deny" for Apply group policy



On Client12, log in as administrator and run cmd with administrator privileges. Do a "gpupdate /force"



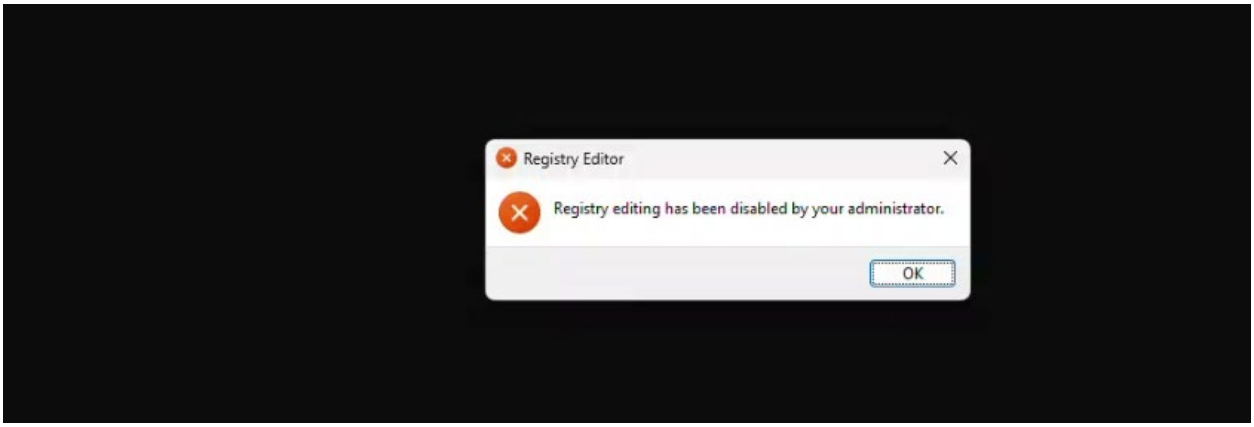
Sign out and log in as a user from the Finance group that the GPO applies to

Example: Alienor Lambert

Do a “gpupdate /force”

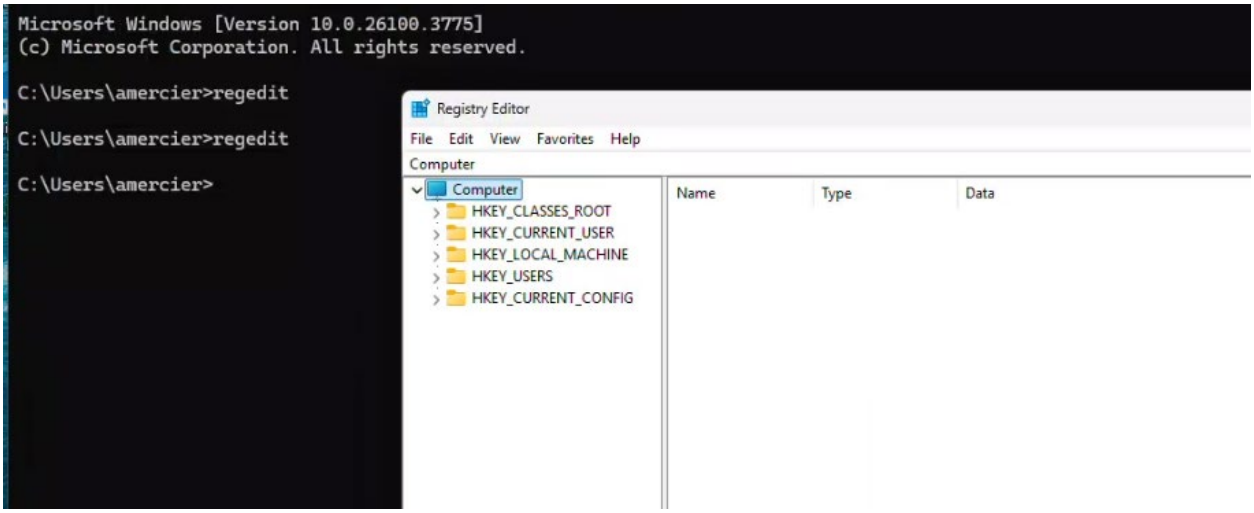
```
C:\Users\alambert>gpupdate
Updating policy...

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

Try to access registry tools. Access will be denied.



Sign out and sign back in with Ava Mercier and repeat the process. Registry Tools will work for her.

```
C:\Users\amercier>regedit

C:\Users\amercier>
```



Task 2: Configuring Group Policy using PowerShell

Objective: Disable access to the Control Panel using PowerShell

GPO Name: **DisableControlPanel**

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

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

Log in to Client12 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.

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

```
PS C:\Users\Administrator.DC112> New-GPO -Name "DisableControlPanel" -Comment "GPO to restrict access to Control Panel"


DisplayName      : DisableControlPanel
DomainName       : vlabs12.com
Owner            : VLABS12\Domain Admins
Id               : bf22a630-be15-4de8-b03e-b7d0ed246908
GpoStatus        : AllSettingsEnabled
Description      : GPO to restrict access to Control Panel
CreationTime     : 5/21/2025 2:52:57 PM
ModificationTime : 5/21/2025 2:52:58 PM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        :


PS C:\Users\Administrator.DC112>
```

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

```
PS C:\Users\Administrator.DC112> Set-GPRegistryValue -Name "DisableControlPanel" -Key "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" -ValueName "NoContr
olPanel" -Type DWord -Value 1


DisplayName      : DisableControlPanel
DomainName       : vlabs12.com
Owner            : VLABS12\Domain Admins
Id               : bf22a630-be15-4de8-b03e-b7d0ed246908
GpoStatus        : AllSettingsEnabled
Description      : GPO to restrict access to Control Panel
CreationTime     : 5/21/2025 2:52:57 PM
```

New-GPLink-Name "DisableControlPanel" -Target "OU=HR,DC=vlabs12,DC=com"

```
PS C:\Users\Administrator.DC112> New-GPLink -Name "DisableControlPanel" -Target "OU=HR,DC=vlabs12,DC=com"


GpoId       : bf22a630-be15-4de8-b03e-b7d0ed246908
DisplayName : DisableControlPanel
Enabled     : True
Enforced    : False
Target      : OU=HR,DC=vlabs12,DC=com
Order       : 1



PS C:\Users\Administrator.DC112>
```

Set-GPPermission -Name "DisableControlPanel" -TargetName "Authenticated Users" -TargetType Group -PermissionLevel GpoApply -ErrorAction Stop

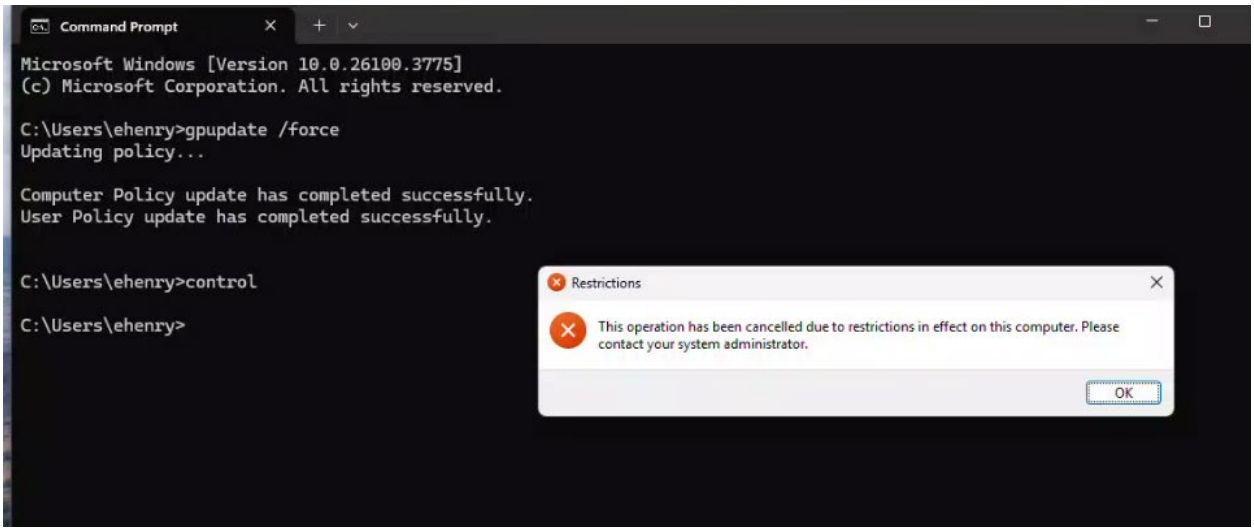
```
PS C:\Users\Administrator.DC112> Set-GPPermission -Name "DisableControlPanel" -TargetName "Authenticated Users" -TargetT
ype Group -PermissionLevel GpoApply -ErrorAction Stop


DisplayName      : DisableControlPanel
DomainName       : vlabs12.com
Owner            : VLABS12\Domain Admins
Id               : bf22a630-be15-4de8-b03e-b7d0ed246908
GpoStatus        : AllSettingsEnabled
Description      : GPO to restrict access to Control Panel
CreationTime     : 5/21/2025 2:52:57 PM
ModificationTime : 5/22/2025 8:54:10 AM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        :



PS C:\Users\Administrator.DC112>
```

Remove Emma Petit from HR (only worked if I used her SID)

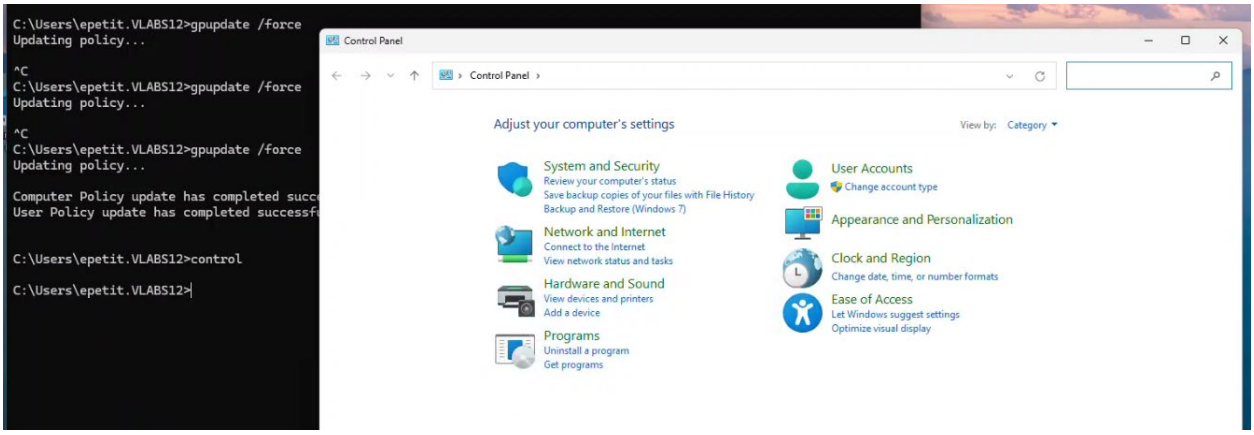
```
PS C:\Users\Administrator.DC112> $EmmaPetitSID = "S-1-5-21-1463046243-3978224867-743297864-1760"
PS C:\Users\Administrator.DC112> $EmmaPetitIdentity = New-Object System.Security.Principal.SecurityIdentifier($EmmaPetitSID)
PS C:\Users\Administrator.DC112> Remove-ADGroupMember -Identity "HR" -Members $EmmaPetitIdentity -Confirm:$false -ErrorAction Stop
PS C:\Users\Administrator.DC112> Get-ADGroupMember -Identity "HR" -Server "DC112.vlabs12.com" | Where-Object { $_.SID -eq $EmmaPetitSID }
PS C:\Users\Administrator.DC112>
```

On Client12, log in as Elise Henry. In cmd, enter “gpupdate /force”

Once it’s updated, try to open the control panel. It will fail.



Repeat for Emma Petit. It will open control panel.



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

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

GPO Name: **NoRecycleBin**

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

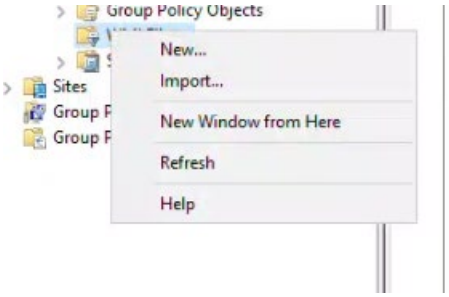
Link this GPO to the Call Center OU

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)

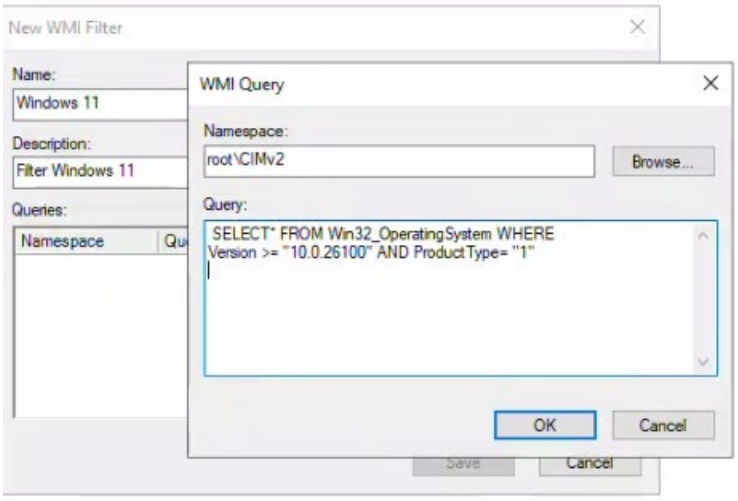
Log in to Client12 with any user from Call Center user and verify that the Recycle Bin doesn't appear on the Desktop

Right-click on WMI Filters and select New

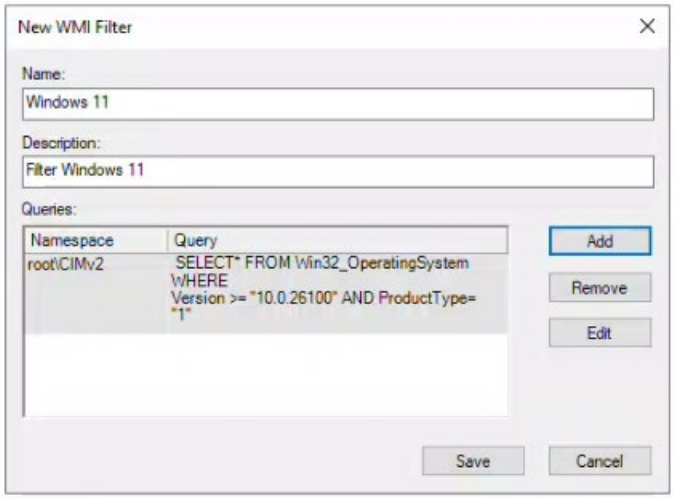


Name it Windows 11 and set a description. Click on Add for queries and use the namespace root\CIMv2. Under “Query”, enter the following to specify Windows version 11

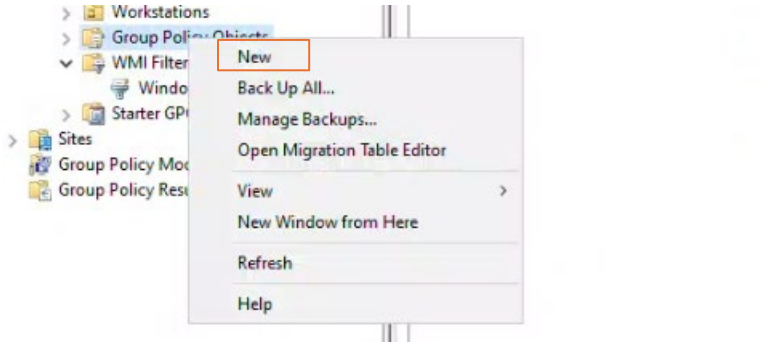
SELECT* FROM Win32_OperatingSystem WHERE Version >= "10.0.26100" AND ProductType= "1"



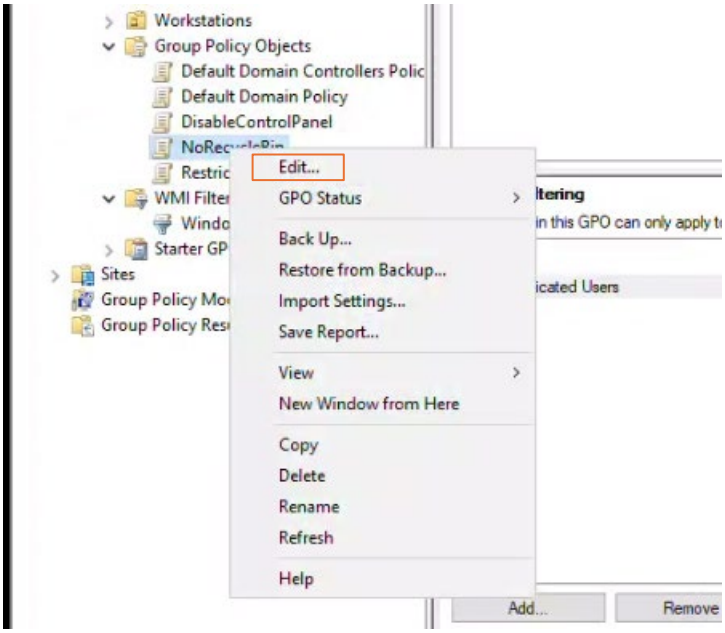
Click OK and Save



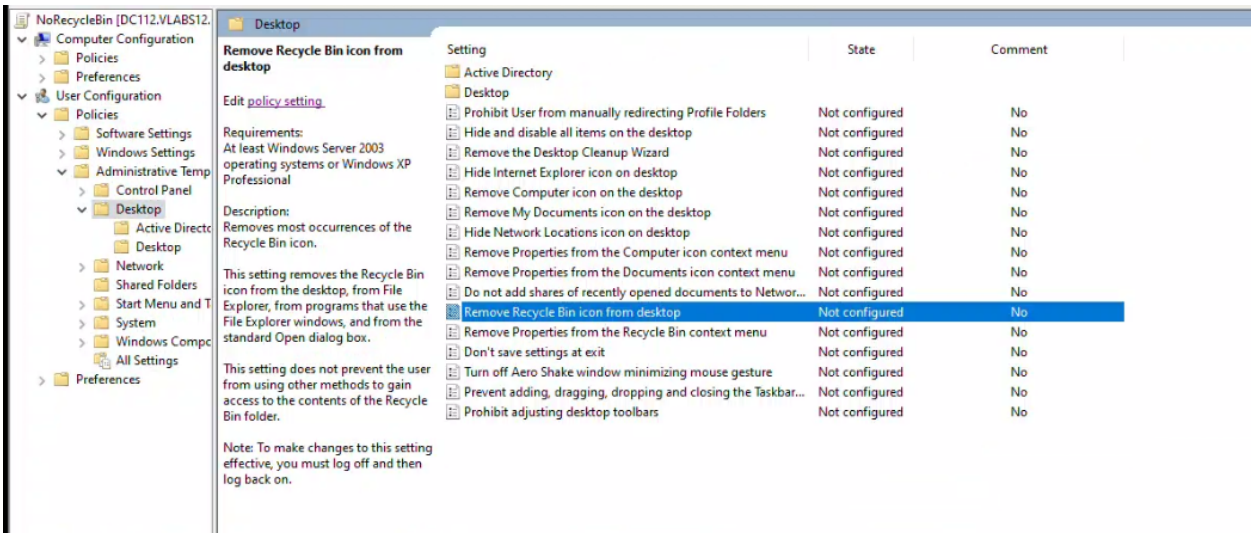
Create a new GPO and name it NoRecycleBin

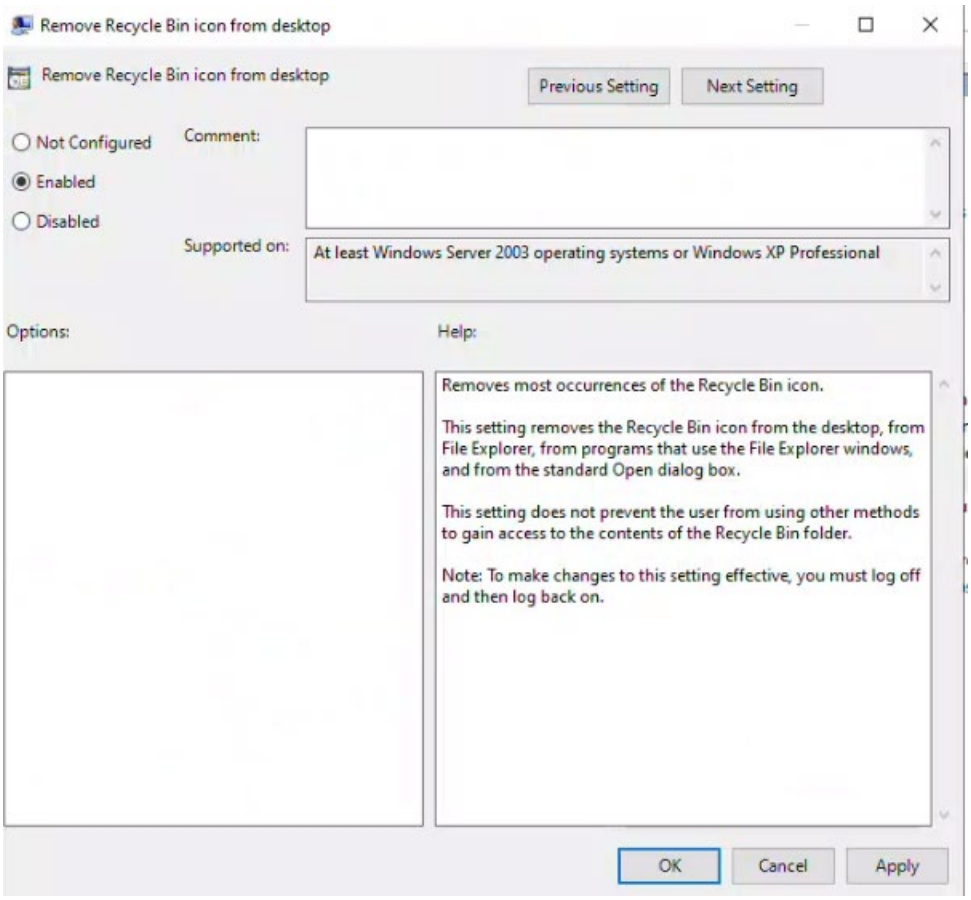


Right click on the new GPO and select Edit

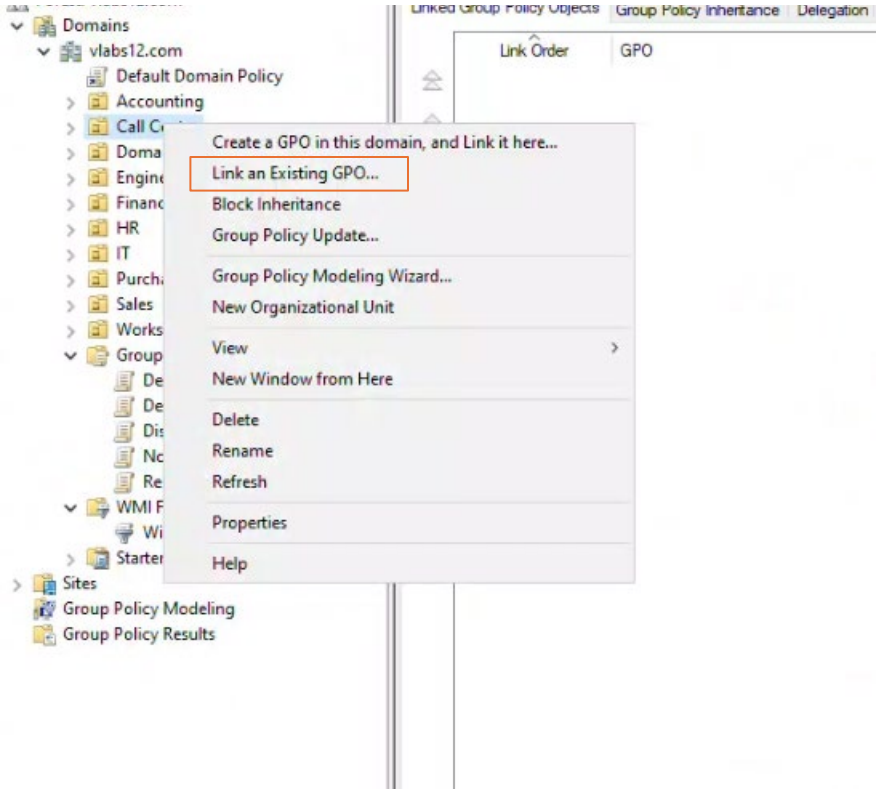


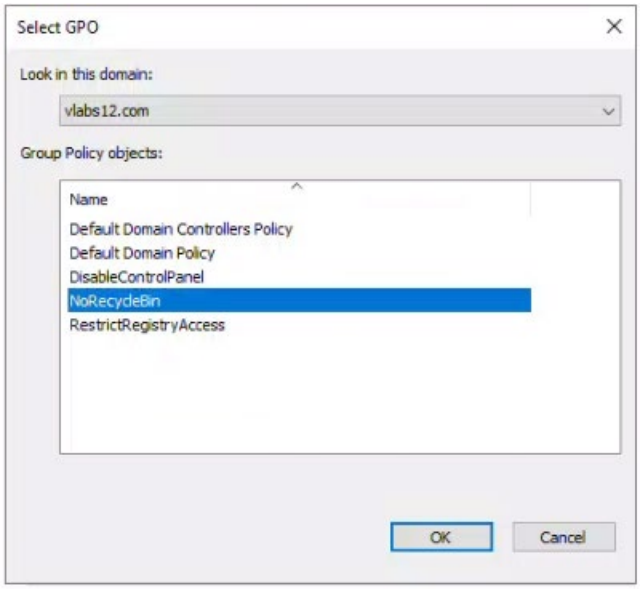
Under User Configuration → Policies → Administrative Template → Desktop, find “Remove Recycle Bin icon from desktop” and enable it.



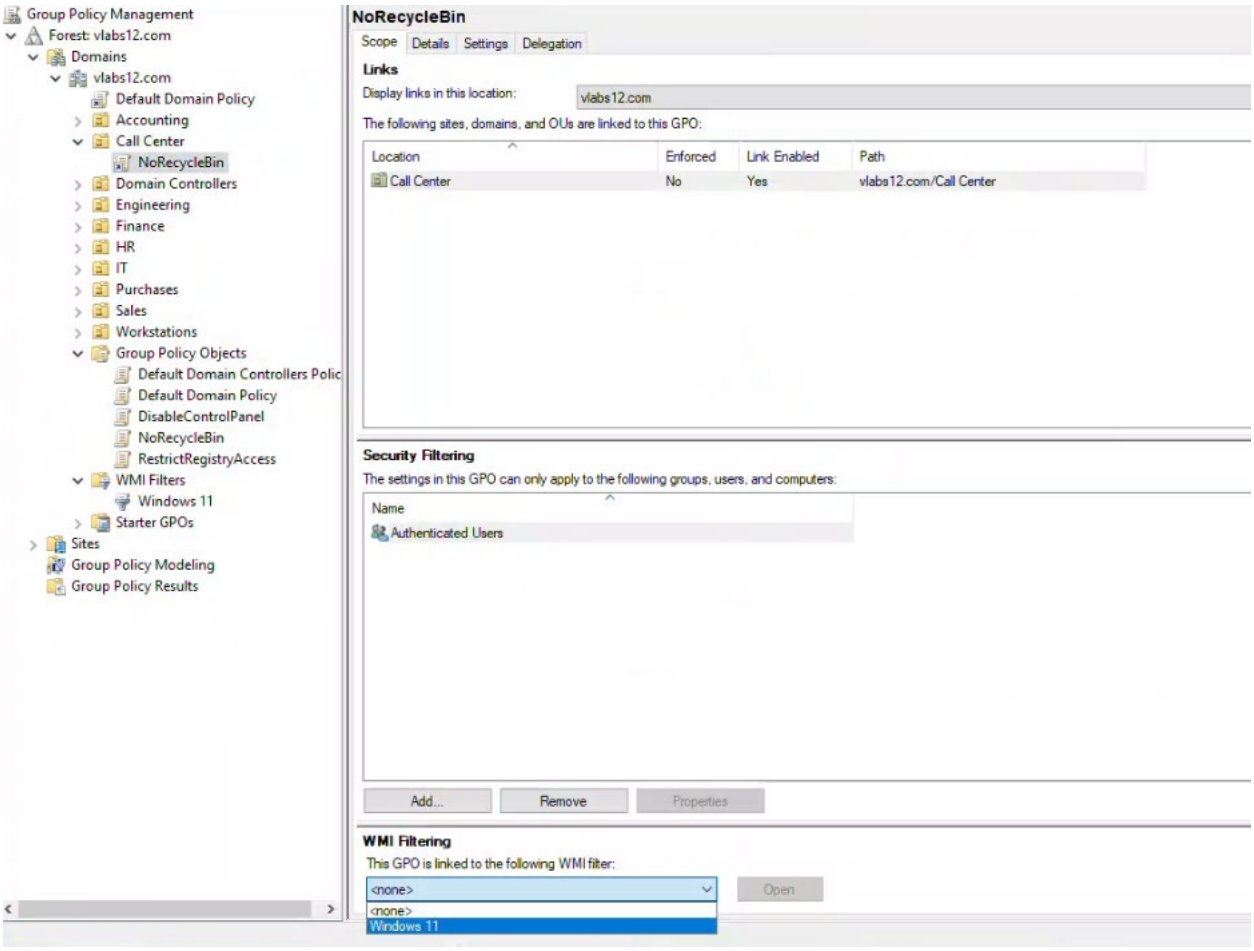


Link the new Recycle Bin GPO to Call Center

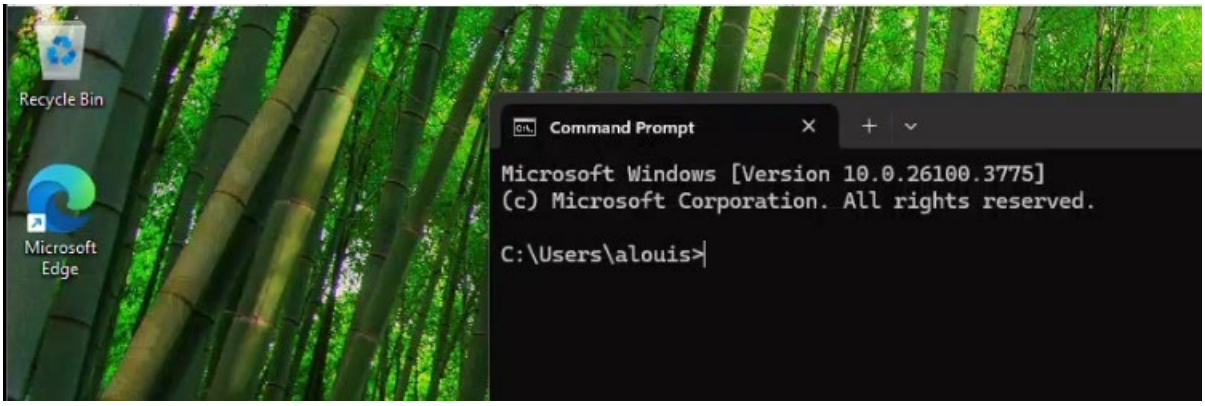




Under WMI Filtering (all the way at the bottom of the page), use the dropdown menu and select Windows 11 we just created.

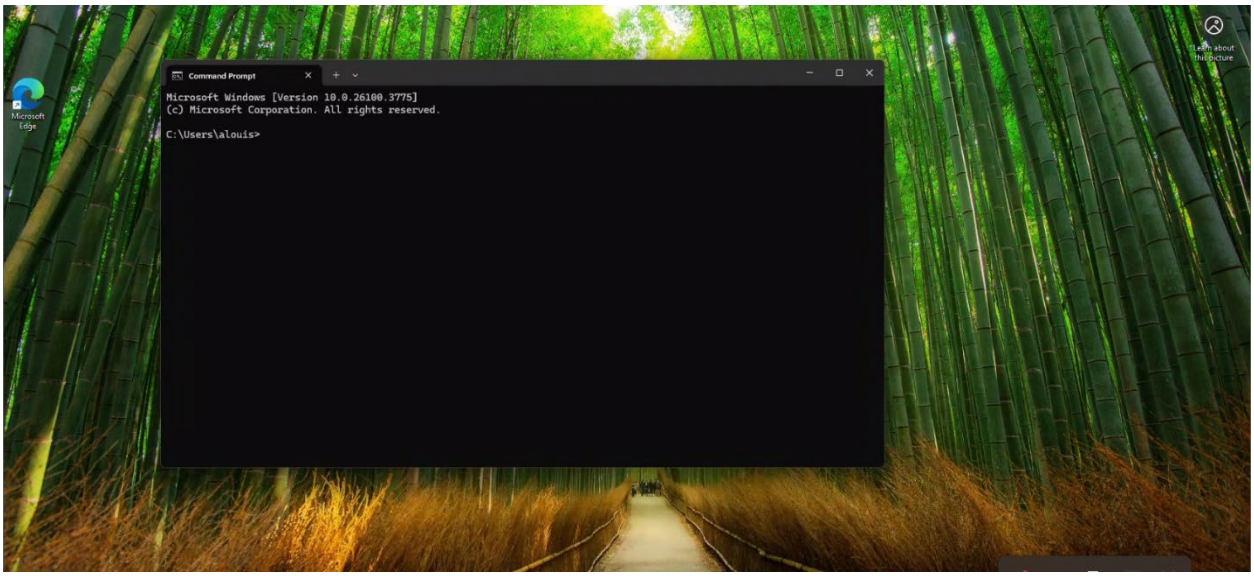


On Client12 (Windows 11), sign in at Aaron Louis, a member of Call Center and verify that the reclycle bin is visible before doing a gpupdate /force



After gpupdate /force:

No recycling bin icon



Task 4: Practicing GPO Processing Order using GUI

Objective: Understand the impact of multiple GPOs

Steps:

- ❖ Link Order: (Don't forget to run gpupdate /force on the client before each test)
- Create a new GPO named AllowRegistryAccess that grants access to the registry editing tools.
- Link it to OU Finance as Order
- Test using Eden Morin to ensure he now has access to the registry

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

- Create OU Finance-Admins and move Ethan Michel to it
- Unlink the GPO RestrictRegistryAccess from OU Finance and link it to OU Finance-Admins
- Test using Eden Morin to verify that the registry editing tools are now blocked

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

- Enforce the AllowRegistryAccess GPO on OU Finance
- Test using Eden Morin to confirm he has access to the registry editing tools

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

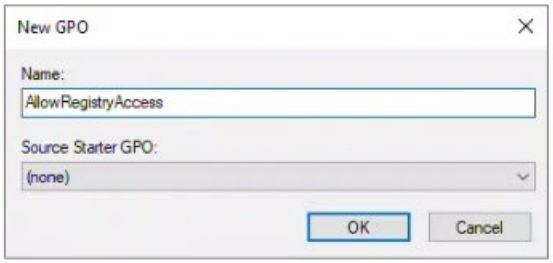
- Remove Enforce the AllowRegistryAccess GPO on OU Finance
- Block inheritance on OU Finance-Admins
- Test using Eden Morin to ensure the registry editing tools are now blocked

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

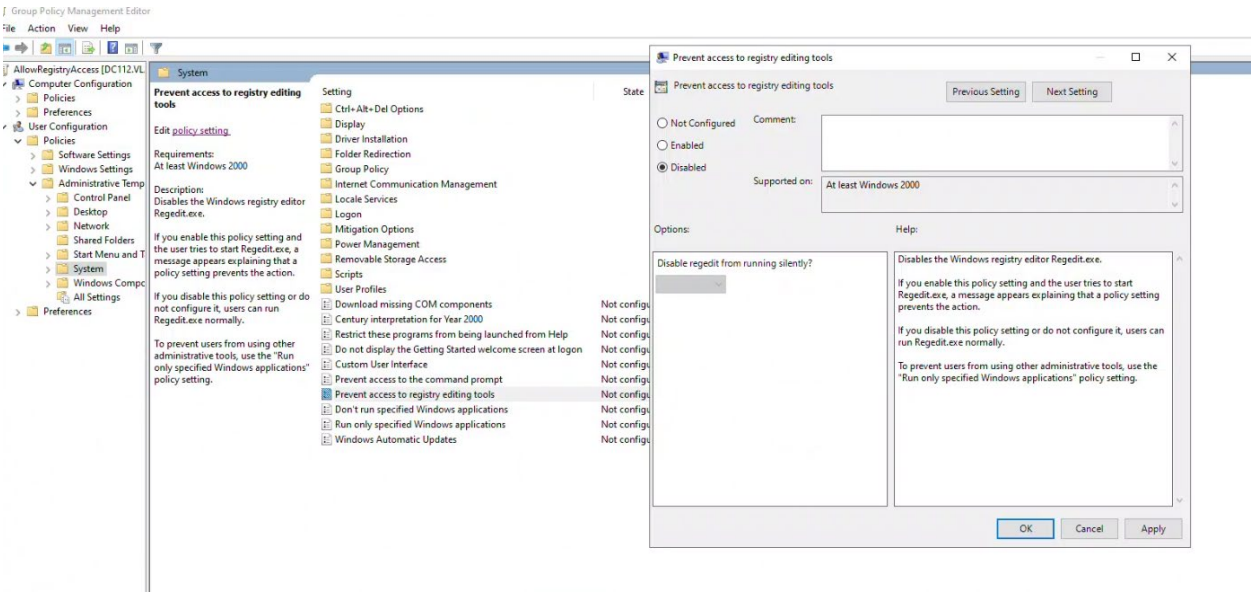
- Uncheck Link Enabled on the RestrictRegistryAccess GPO on OU Finance Admins
- Test using Eden Morin to confirm he has access to the registry editing tools.

- Link Order:
- Create a new GPO named AllowRegistryAccess that grants access to the registry editing tools.
- Link it to OU Finance as Order
- Test using Eden Morin to ensure he now has access to the registry

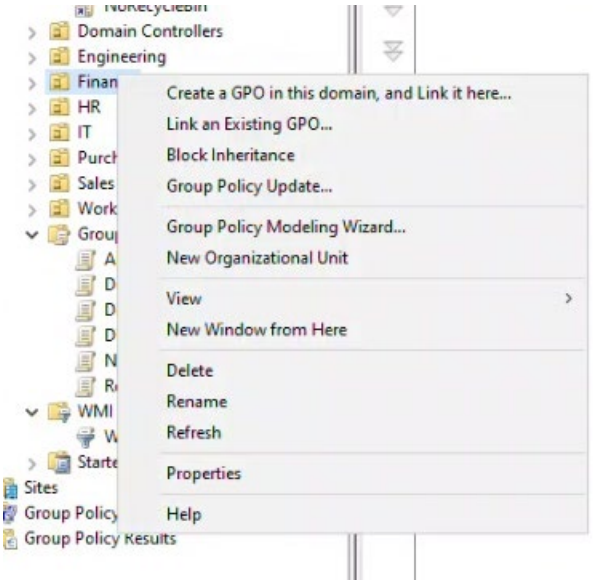
Create the GPO “AllowRegistryAccess”

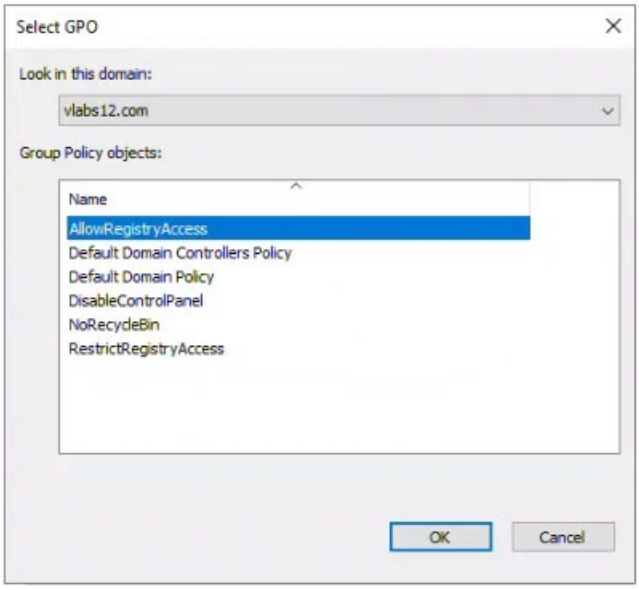


Right-click on the new GPO and select Edit

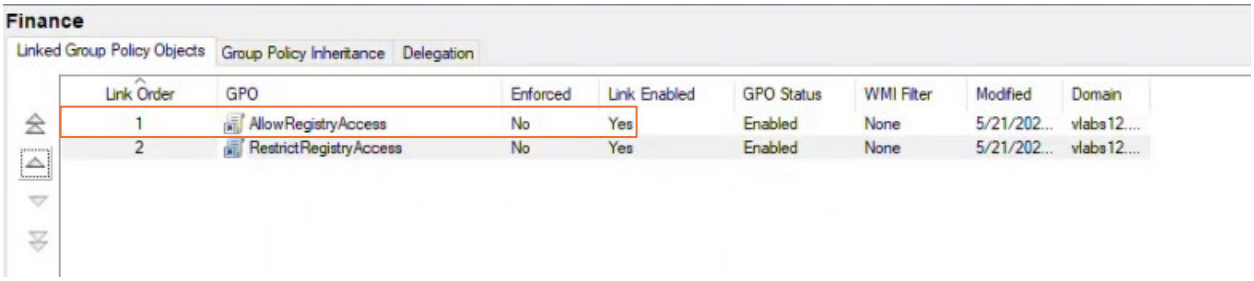


Link the new GPO to Finance, like done earlier.

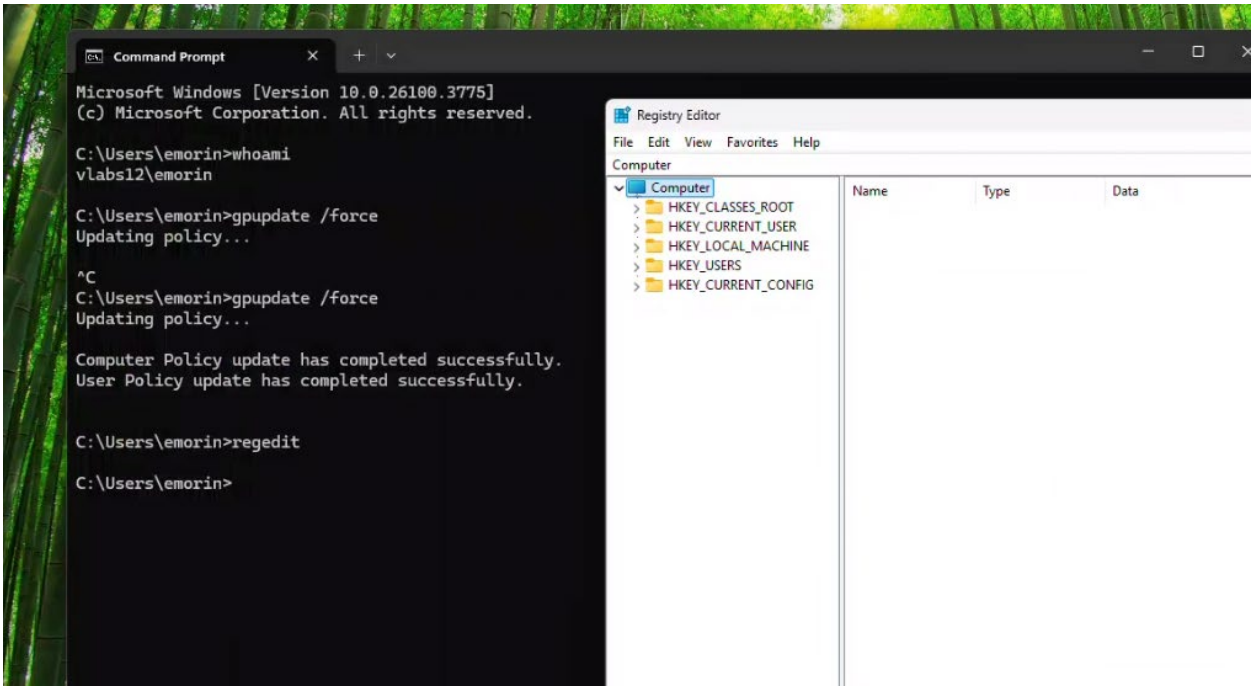




In the “linked group policy objects”, use the arrow to make AllowRegistryAccess order #1, and not RestrictRegistryAccess



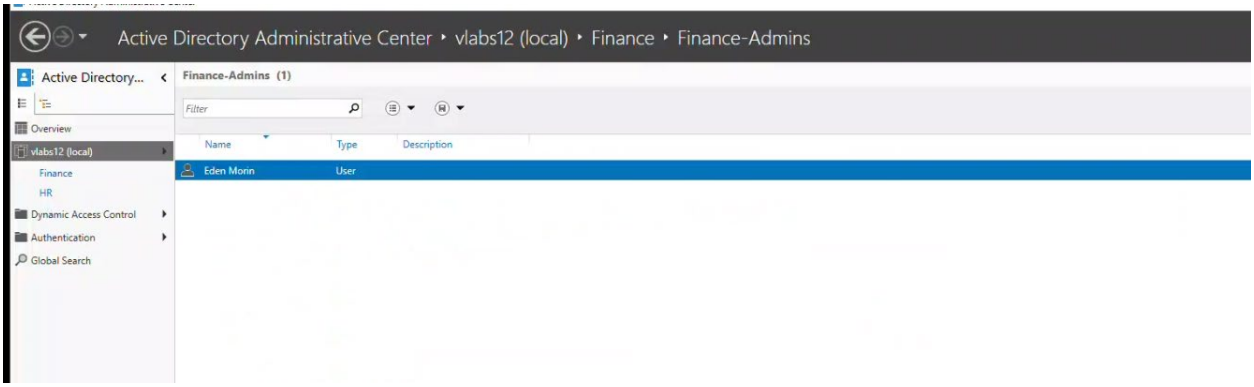
On Client12, log in as Eden Morin to verify that he now has access to the registry tools



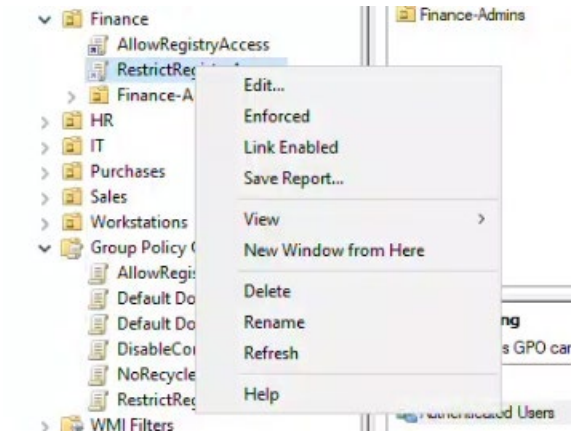
❖ Precedence Rules: (Don't forget to run gpupdate /force on the client before each test)

- Create OU Finance-Admins and move Ethan Michel to it
- Unlink the GPO RestrictRegistryAccess from OU Finance and link it to OU Finance-Admins
- Test using Eden Morin to verify that the registry editing tools are now blocked

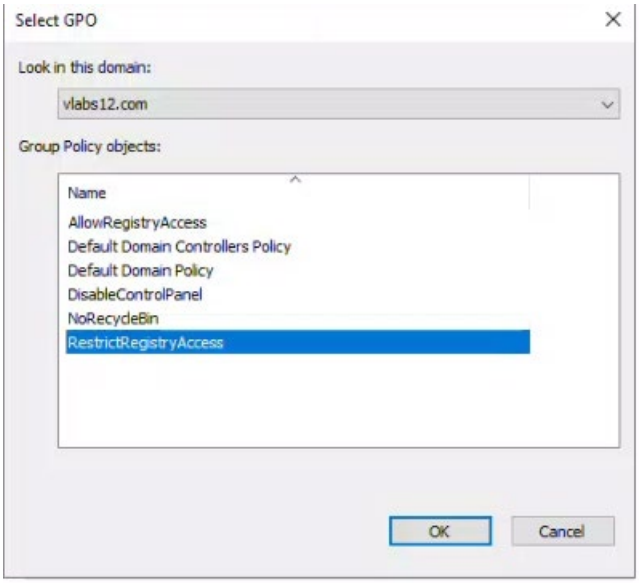
I created the OU Finance-Admins in ADAC and moved Eden Morin to the group

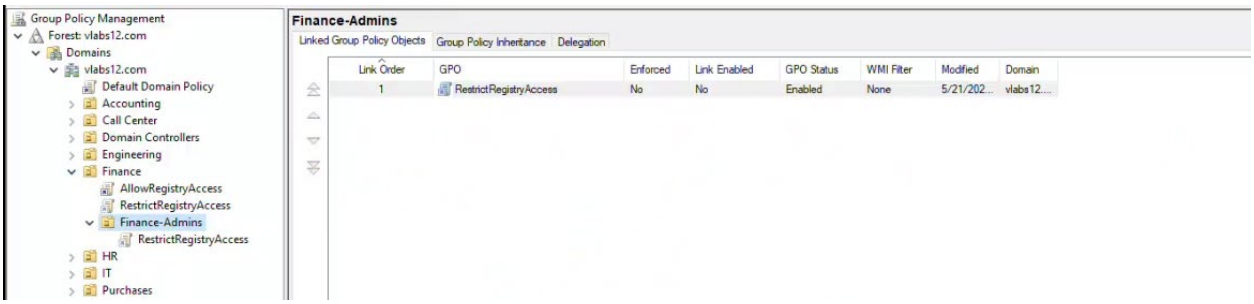


Right-click and uncheck “Link Enabled”

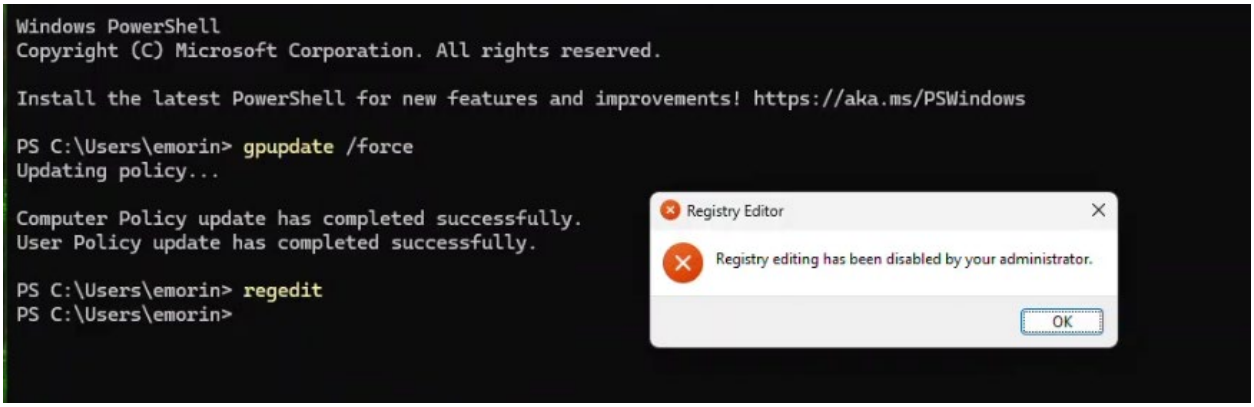


Link the GPO “RestrictRegistryAccess” to Finance-Admins

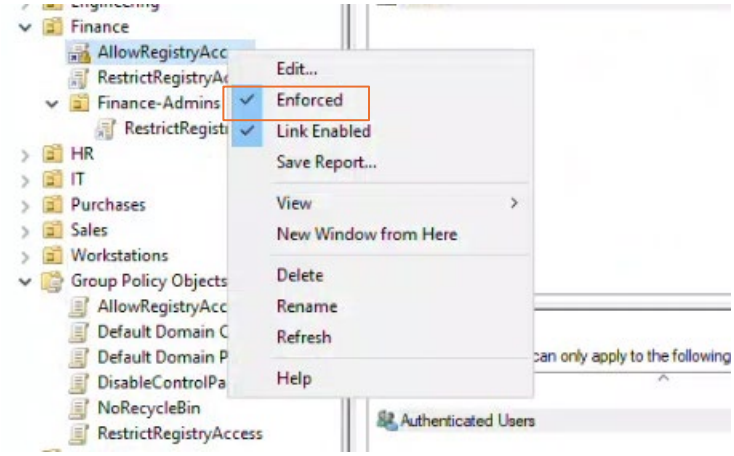


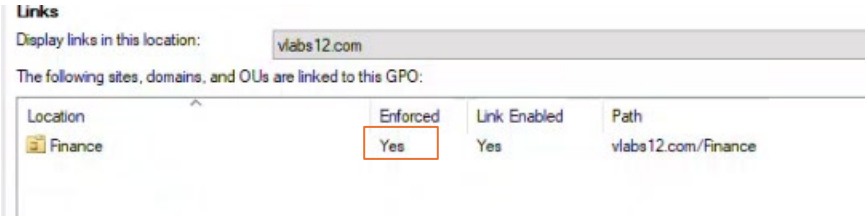


Gpupdate /force as usual and test access to the registry tools.

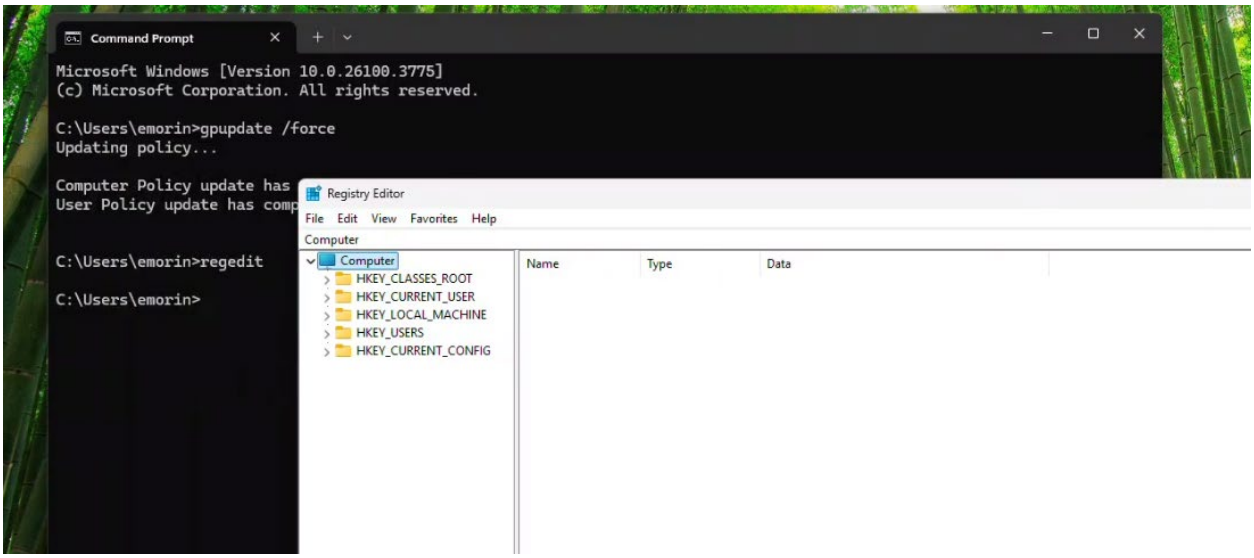


- ❖ Enforced GPO: (Don’t forget to run gpupdate /force on the client before each test)
- Enforce the AllowRegistryAccess GPO on OU Finance
- Test using Eden Morin to confirm he has access to the registry editing tools



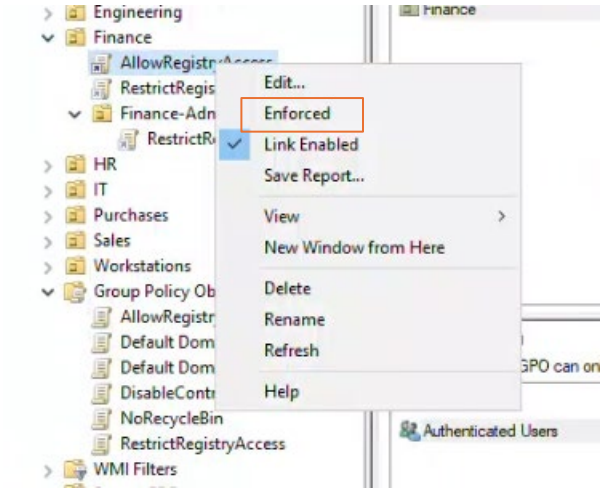


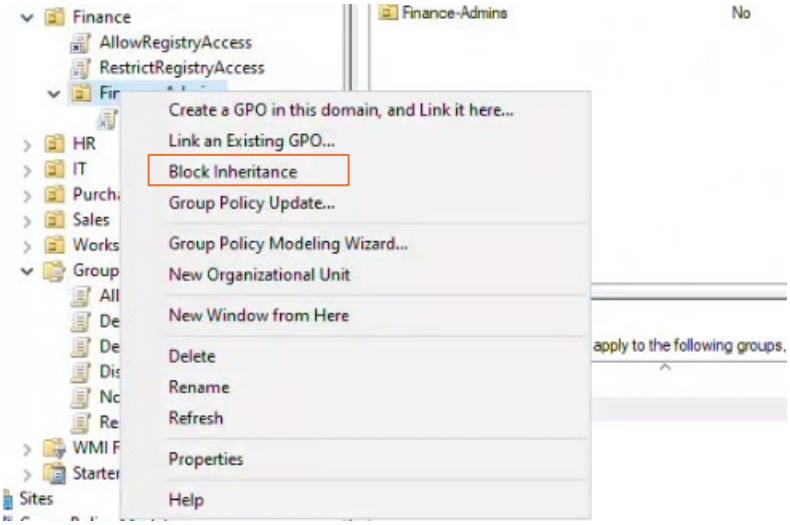
Test again on Client12 with Eden Morin after doing a gpupdate /force

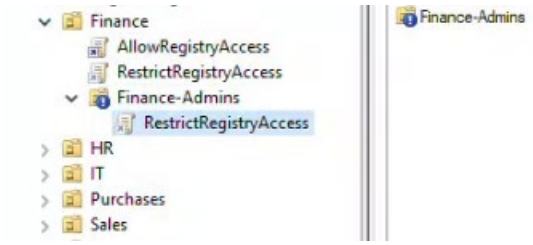


- ❖ Block Inheritance: (Don't forget to run gpupdate /force on the client before each test)
- Remove Enforce the AllowRegistryAccess GPO on OU Finance

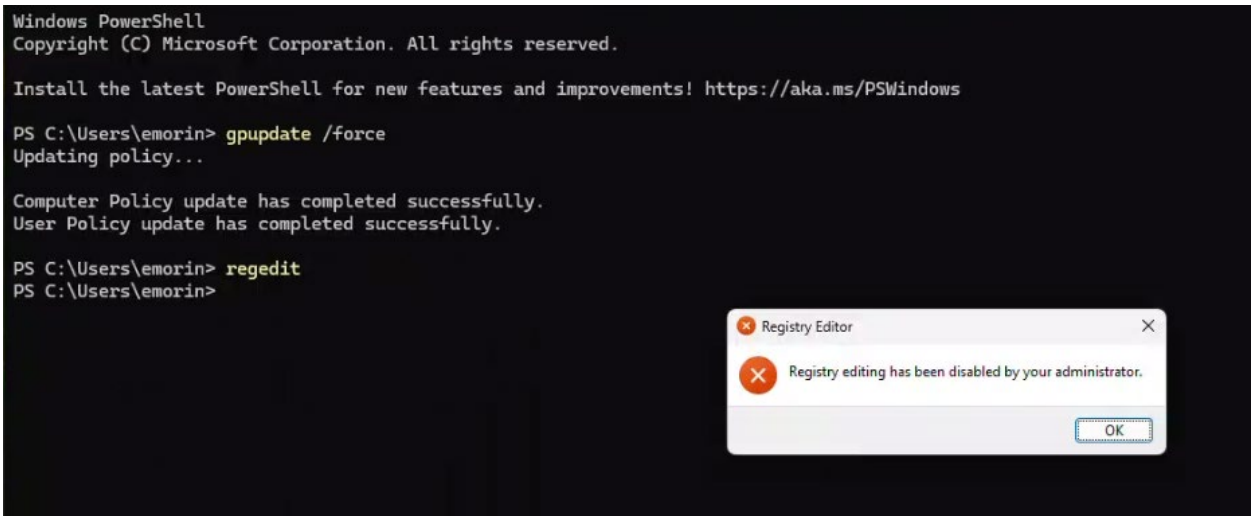
- Block inheritance on OU Finance-Admins
- Test using Eden Morin to ensure the registry editing tools are now blocked





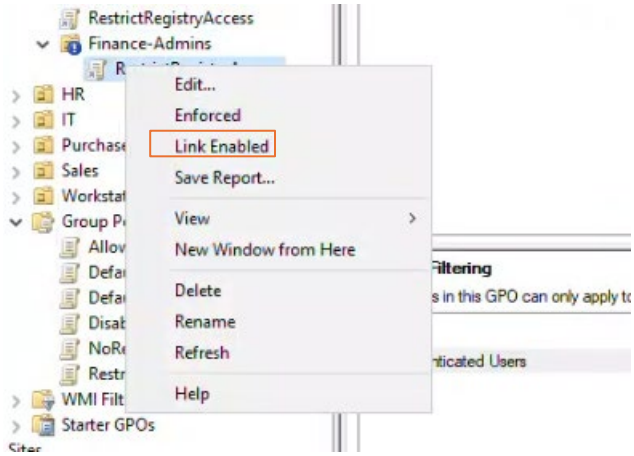


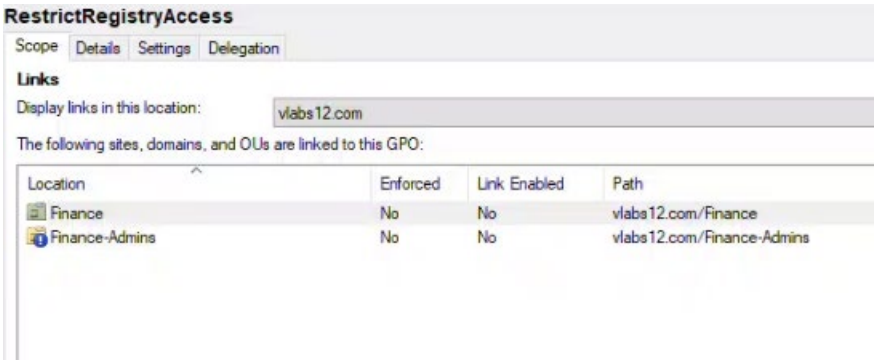
Sign in as Eden Morin to confirm the registry tools are blocked.



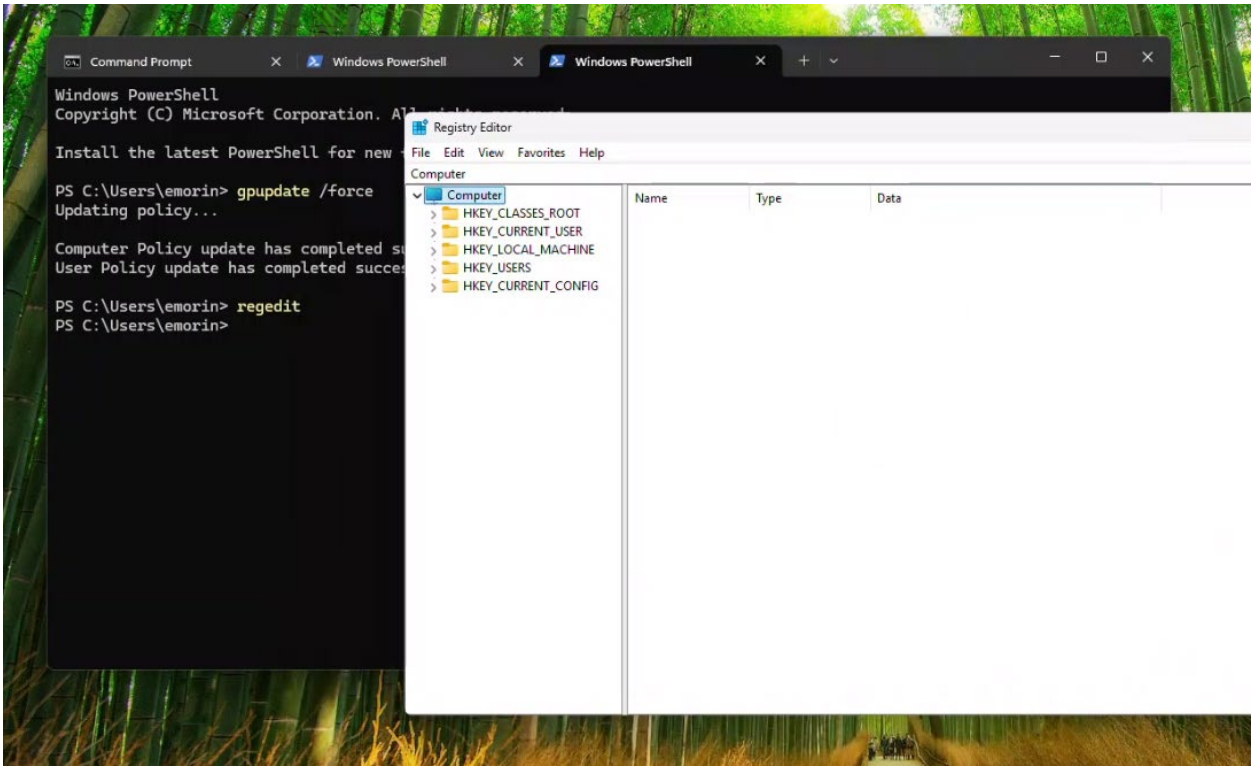
❖ Link Enabled: (Don't forget to run gpupdate /force on the client before each test)

- Uncheck Link Enabled on the RestrictRegistryAccess GPO on OU Finance Admins
- Test using Eden Morin to confirm he has access to the registry editing tools.





Sign in as Eden Morin to make sure he has access.



Task 5: Exploring Default Group Policy Objects using GUI

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

Steps:

Identify and review the two default GPOs in the domain

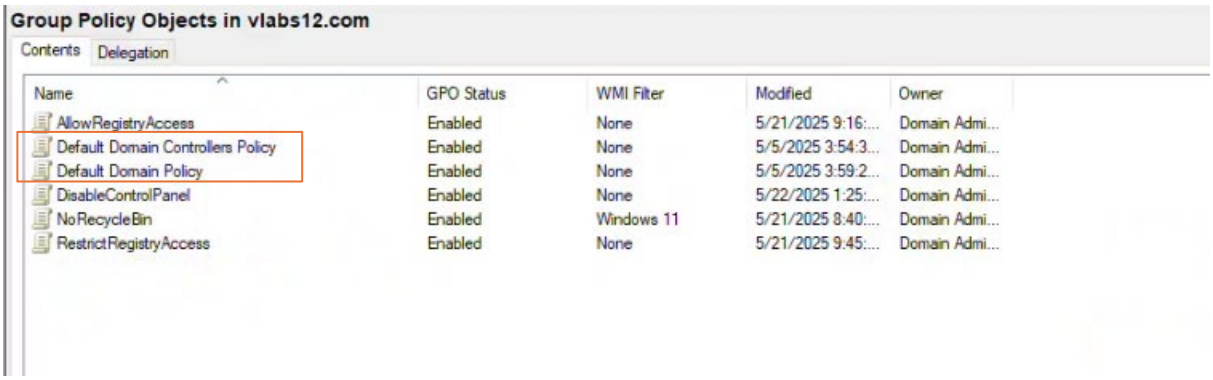
Generate a Settings Report for both policies

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

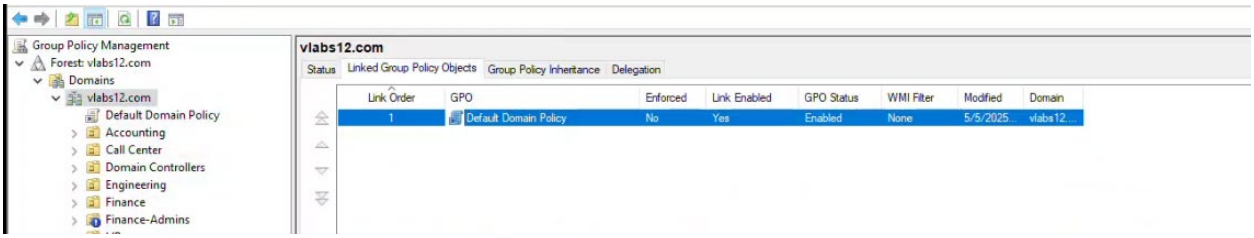
These two are the default GPOs:

Default Domain Controllers Policy

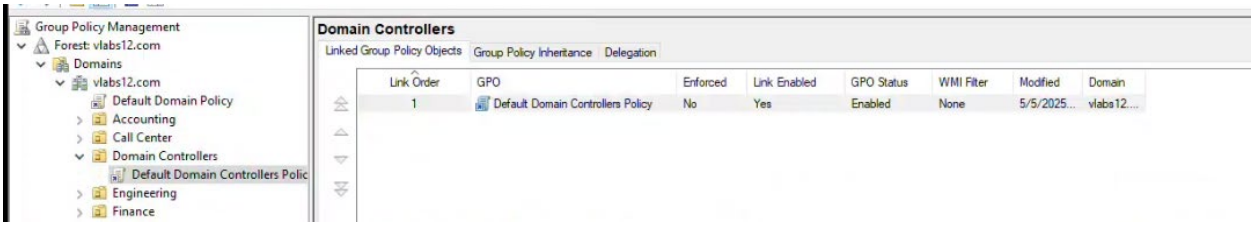
Default Domain Policy



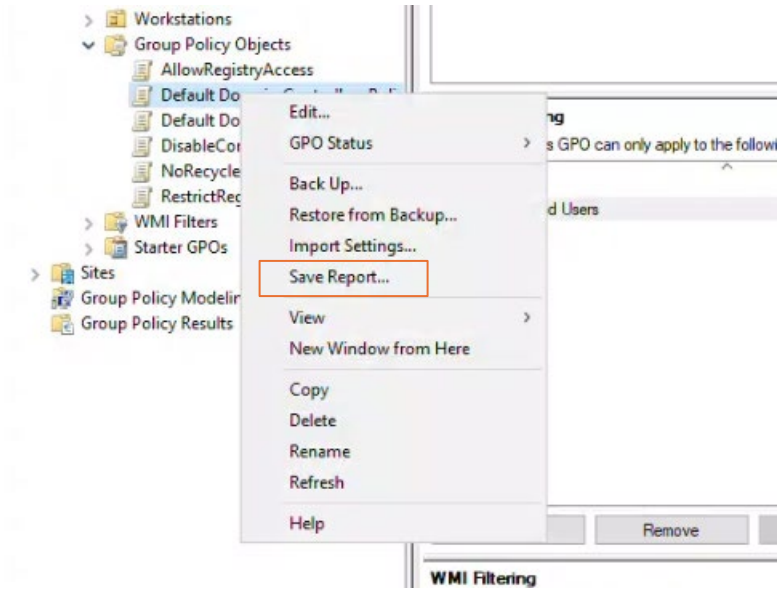
Default Domain policy is linked to the domain root (vlabs12.com)

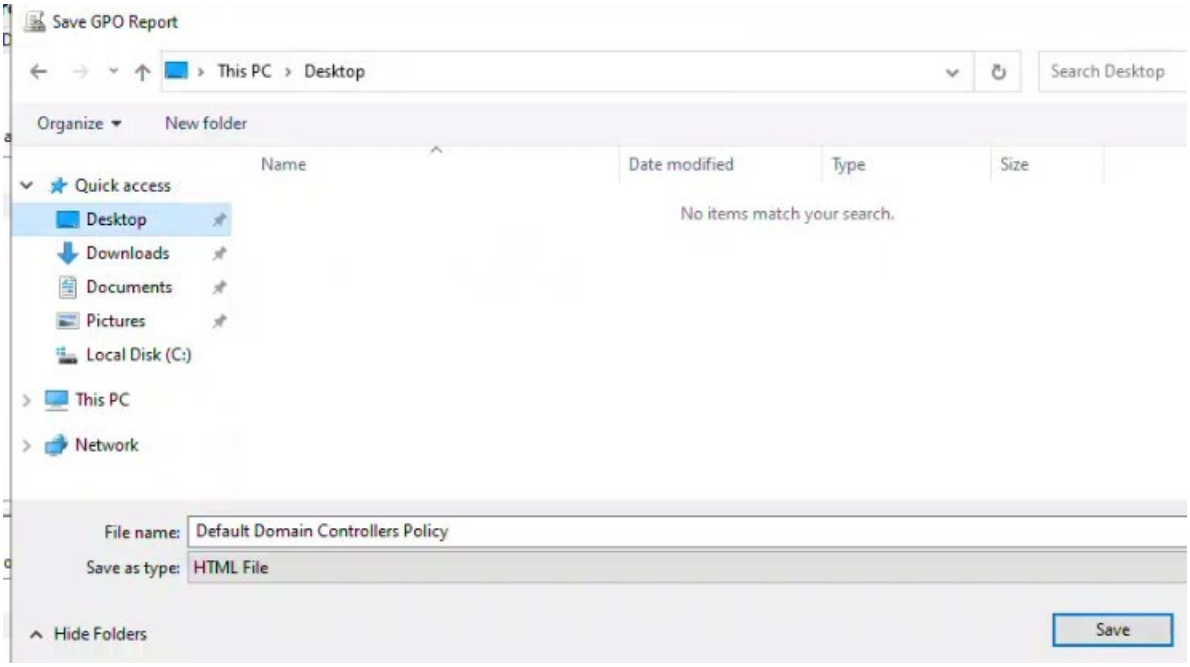


Default Domain Controllers Policy is linked to the Domain Controllers OU



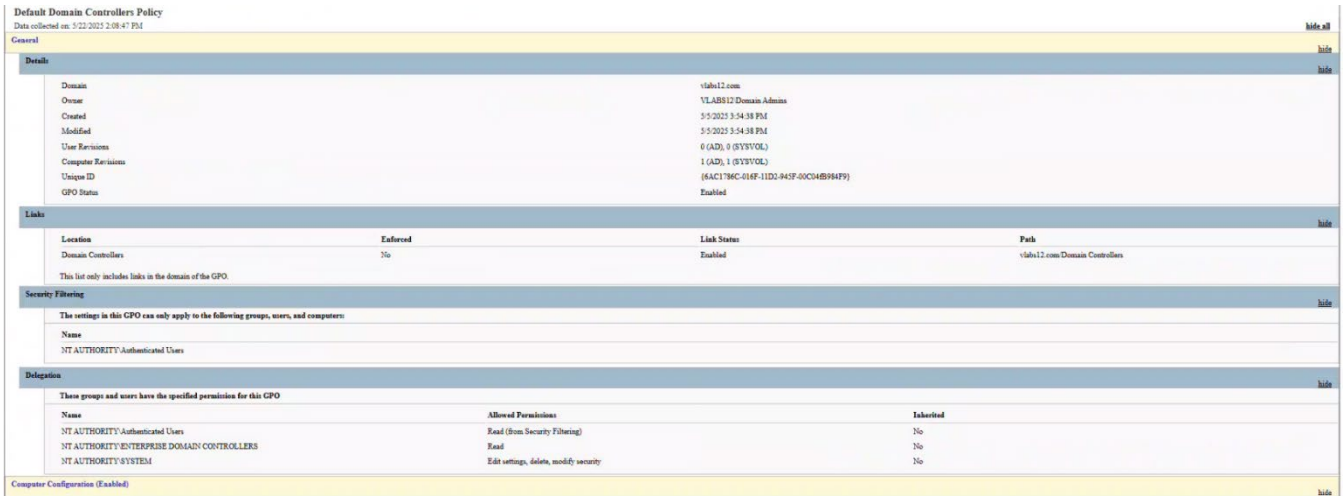
To generate a report for each, right click on the GPO under group policy objects and select “Save Report”





Do so for both to analyze the impact of these GPOs

(very hard to read)



Default Domain Controllers Policy

Data collected on: 5/22/2025 2:08:47 PM

hide all

General hide

Details hide

Domain	vlabs12.com
Owner	VLABS12\Domain Admins
Created	5/5/2025 3:54:38 PM
Modified	5/5/2025 3:54:38 PM
User Revisions	0 (AD), 0 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{6AC1786C-016F-11D2-945F-00C04fB984F9}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Domain Controllers	No	Enabled	vlabs12.com/Domain Controllers

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

Security Filtering hide

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

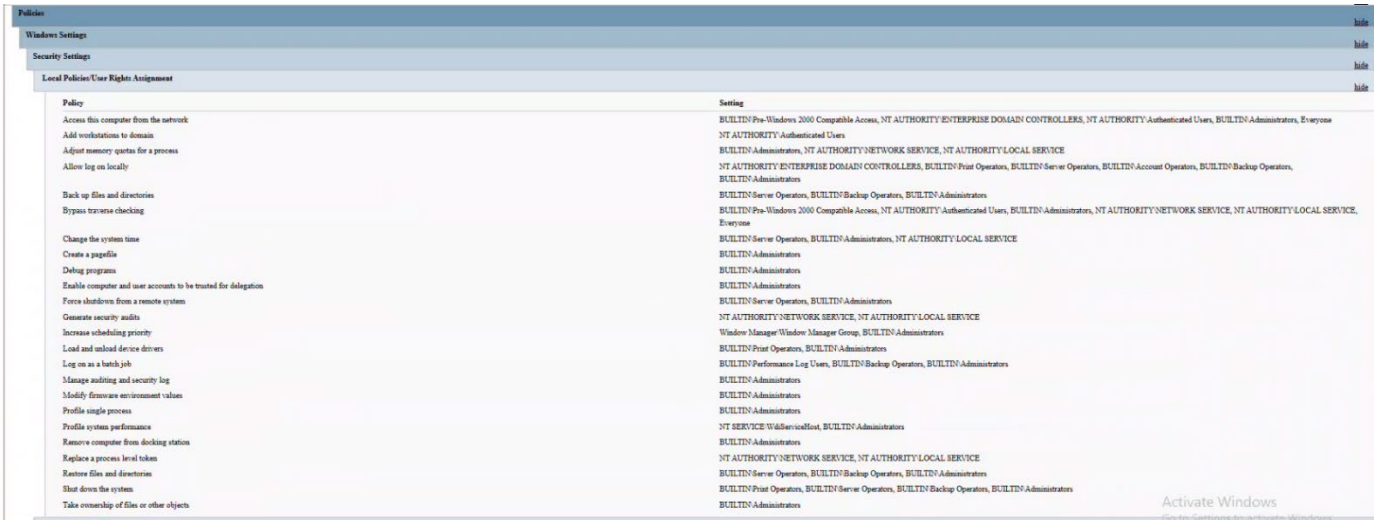
Name
NT AUTHORITY\Authenticated Users

Delegation hide

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Enabled) hide



Policies hide

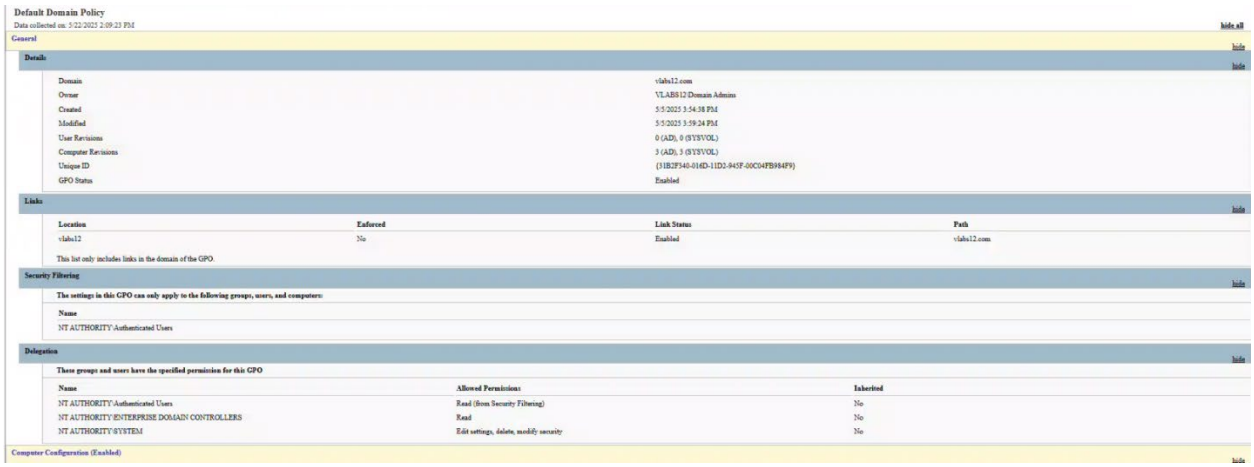
Windows Settings hide

Security Settings hide

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
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\WdiServiceHost, 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

Default Domain Policy



Default Domain Policy
Data collected on: 5/22/2025 2:09:23 PM
hide all

General
hide

Details
hide

Domain	vlabs12.com
Owner	VLAB\12\Domain Admins
Created	5/5/2025 3:54:38 PM
Modified	5/5/2025 3:59:24 PM
User Revisions	0 (AD), 0 (SYSVOL)
Computer Revisions	3 (AD), 3 (SYSVOL)
Unique ID	{31B2F340-016D-11D2-945F-00C04FB984F9}
GPO Status	Enabled

Links
hide

Location	Enforced	Link Status	Path
vlabs12	No	Enabled	vlabs12.com

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

Security Filtering
hide

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

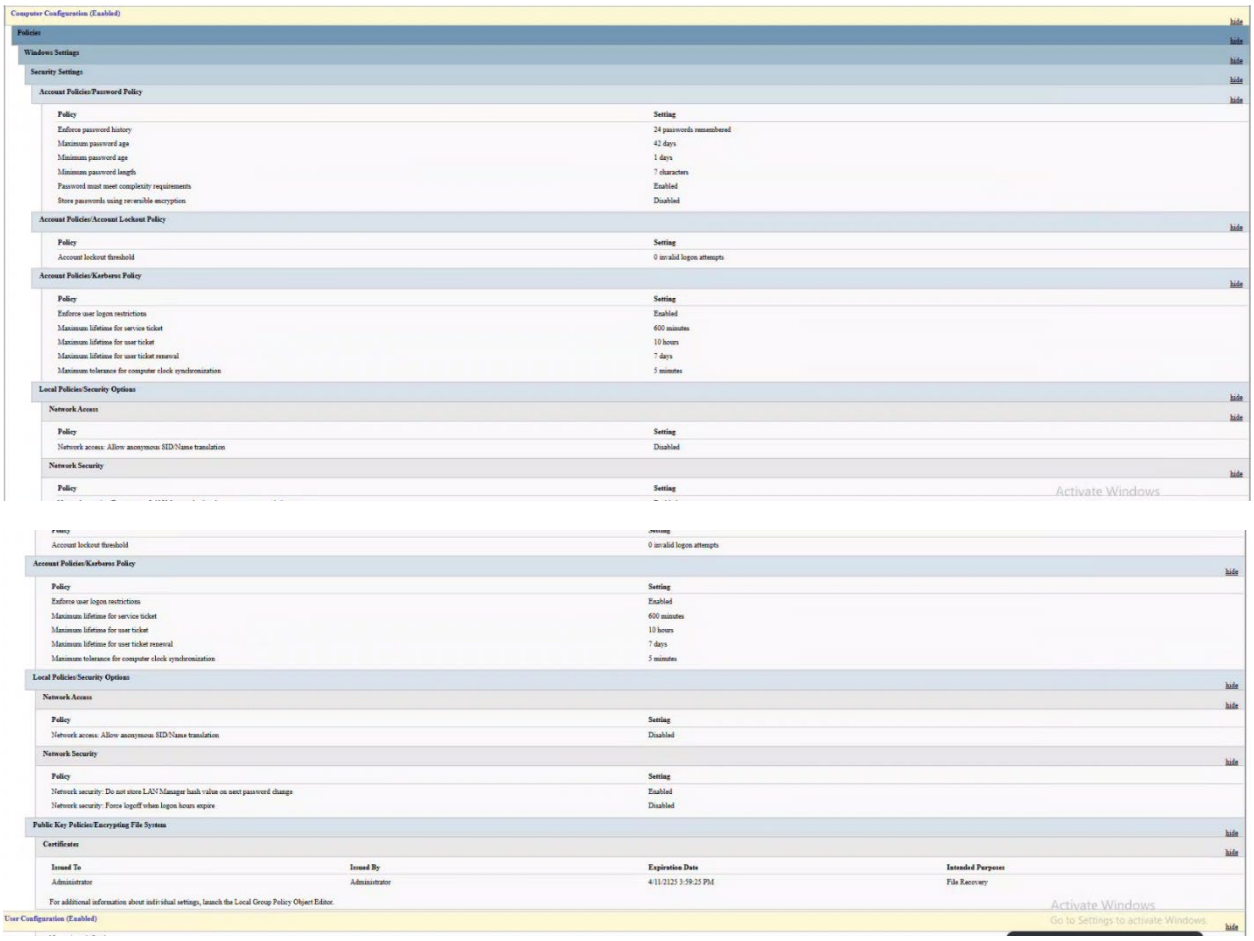
Name
NT AUTHORITY\Authenticated Users

Delegation
hide

These groups and users have the specified permission for this GPO

Name	Allowed Permission	Inherited
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Enabled)
hide



Computer Configuration (Enabled)
hide

Policies
hide

Windows Settings
hide

Security Settings
hide

Account Policies/Password Policy
hide

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
hide

Policy	Setting
Account lockout threshold	0 invalid logon attempts

Account Policies/Kerberos Policy
hide

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
hide

Network Access
hide

Policy	Setting
Network access: Allow anonymous SID/Name translation	Disabled

Network Security
hide

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

Public Key Policies/Encrypting File System
hide

Certificates
hide

Issued To	Issued By	Expiration Date	Intended Purposes
Administrator	Administrator	4/11/2125 3:59:25 PM	File Recovery

For additional information about individual settings, launch the Local Group Policy Object Editor.

User Configuration (Enabled)
hide

The **Default Domain Policy** is set for the vlabs12.com domain, so it affects everyone and every computer, like Client12 and users such as Eden Morin and

Emma Petit. It makes people use more secure passwords (at least 7 characters, with uppercase, lowercase, numbers, and symbols, changing every 42 days) and locks accounts for 30 minutes after 5 wrong password tries. This keeps things safe but might impact users who forget their passwords.

The **Default Domain Controllers Policy** only works on the domain controller computers, like DC112 and DC212, keeping them more secure by only letting admins log in directly, while still allowing everyone to connect over the network for login requests. Together, these rules make sure the domain is safe—strong passwords for everyone and locked-down servers—without getting in each other's way, helping everything run smoothly as of May 22, 2025.

ASSIGNMENT 2

Part 2

MAY 22, 2025

NETWORK INSTALLATION AND ADMINISTRATION II

Laetitia Mohammed, 0931512

Contents

Task 1: Creating a Central Store for Administrative Templates

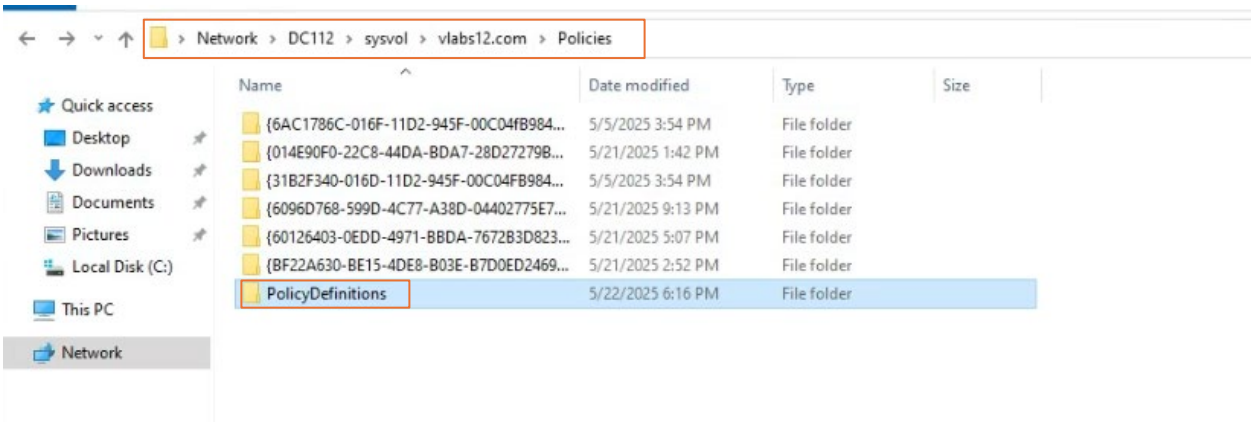
Create a central store for Administrative Templates on DC112

Copy all ADMX and ADML files to this Central store

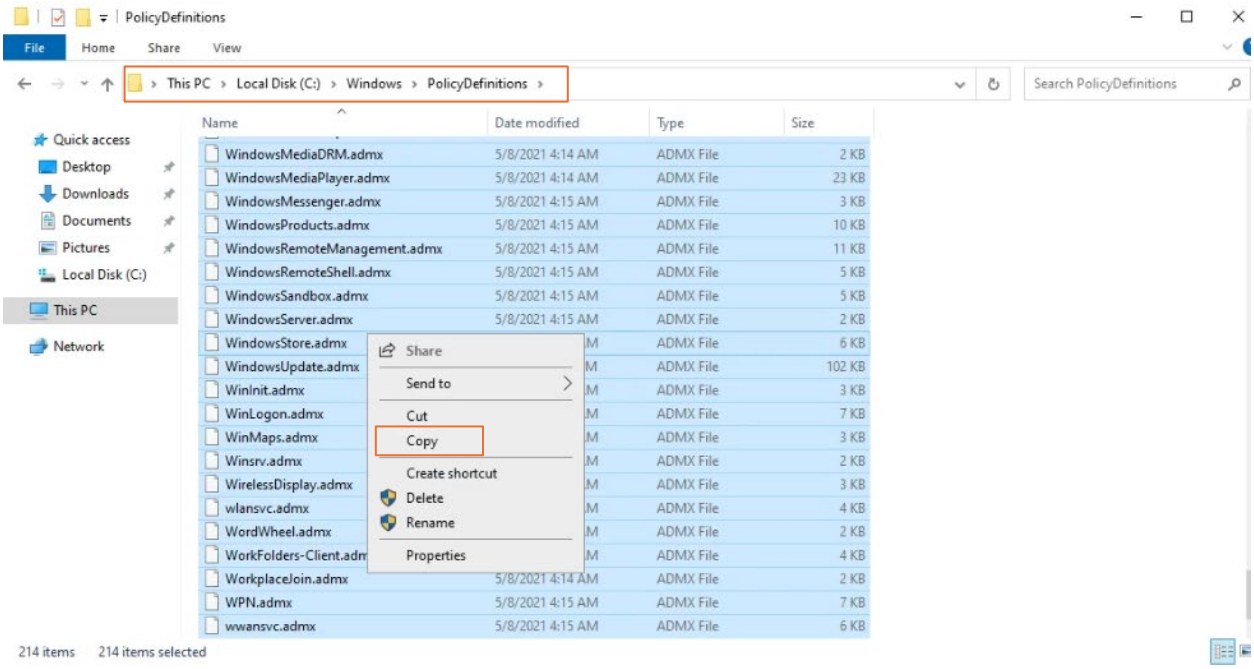
Verify that Group Policy Management Console (GPMC) loads templates from the central store.

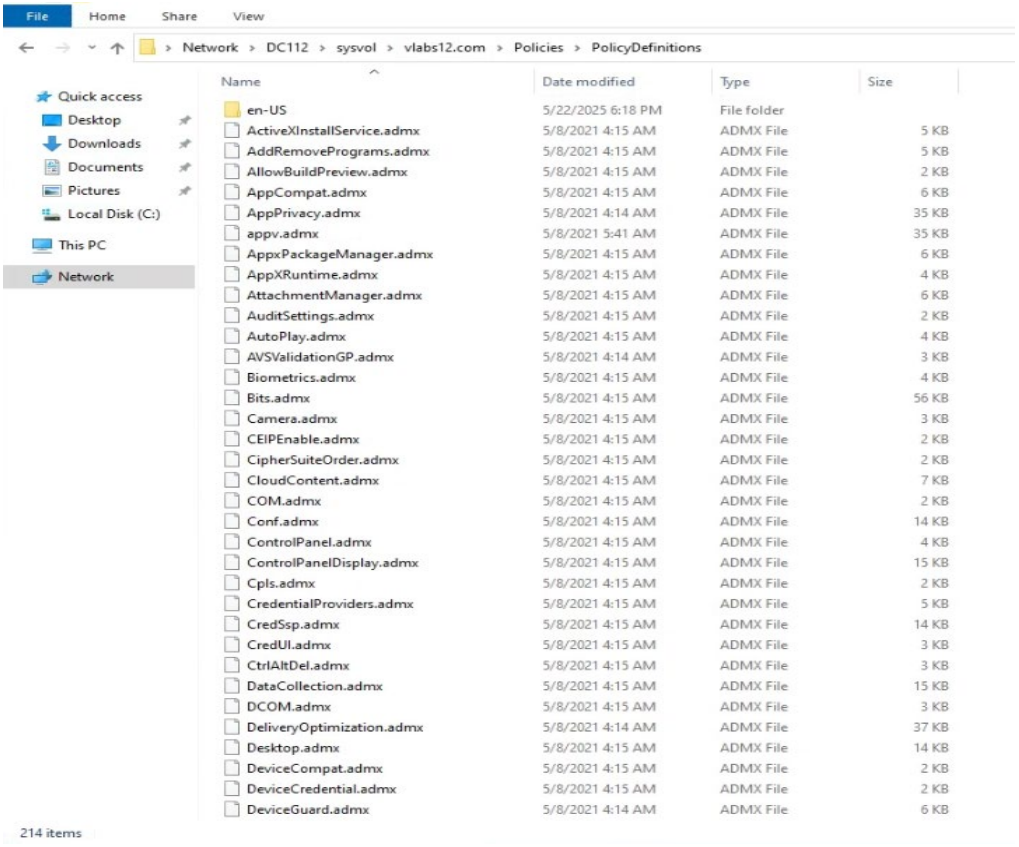
On the C:/ drive, go to \\DC112\SYSVOL\vlabs12.com\Policies

Create the folder “PolicyDefinitions”

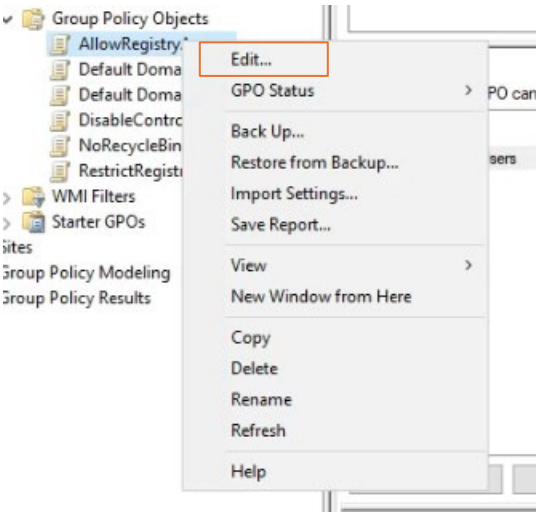


In another page, go to Local Disk (C:) → Windows → PolicyDefinitions. Copy all the ADMX and ADML (en-US folder) and paste it in the new PolicyDefinitions folder we just created in the other location.



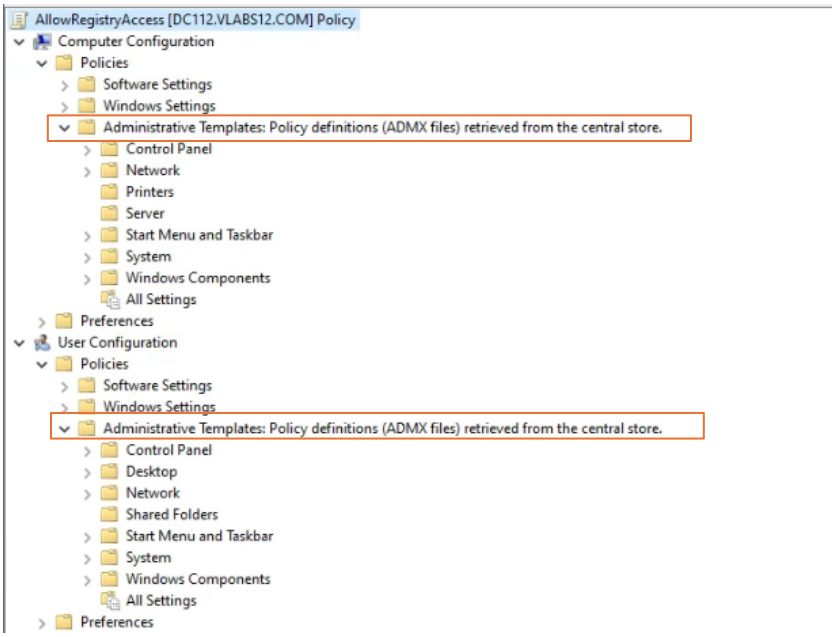


In Group Policy Management, right-click on any GPO and select Edit.



Press the dropdown menu for Policies on both Computer Configuration and User Configuration. You'll see that Administrative Templates now displays that the ADMX

files are retrieved from the central store we just created and not locally on the machine



Task 2: Managing and Configuring Administrative Templates

Download and install **Microsoft Office Administrative Templates** (You will need to add the NAT NIC to download this package. Remove it after completing the download).

Create a new GPO named **RestrictTeamsStarting**

Use Filter Options for User Configuration to locate **Microsoft Teams** settings

Enable Prevent Microsoft Teams from starting automatically after installation

Add a comment to document this setting

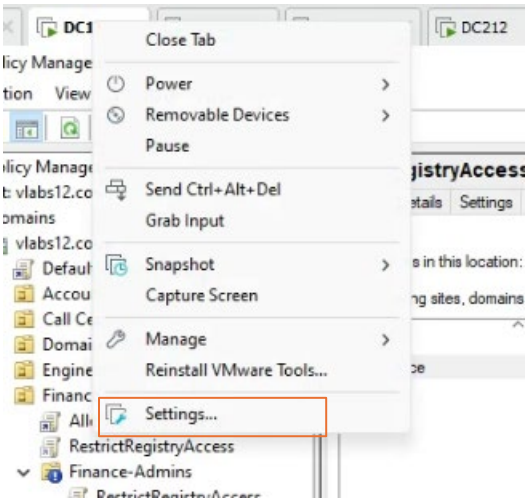
Link to **Engineering OU** (to be tested in Task 8 Managing Software Installation task)

Run gpupdate /force to apply changes.

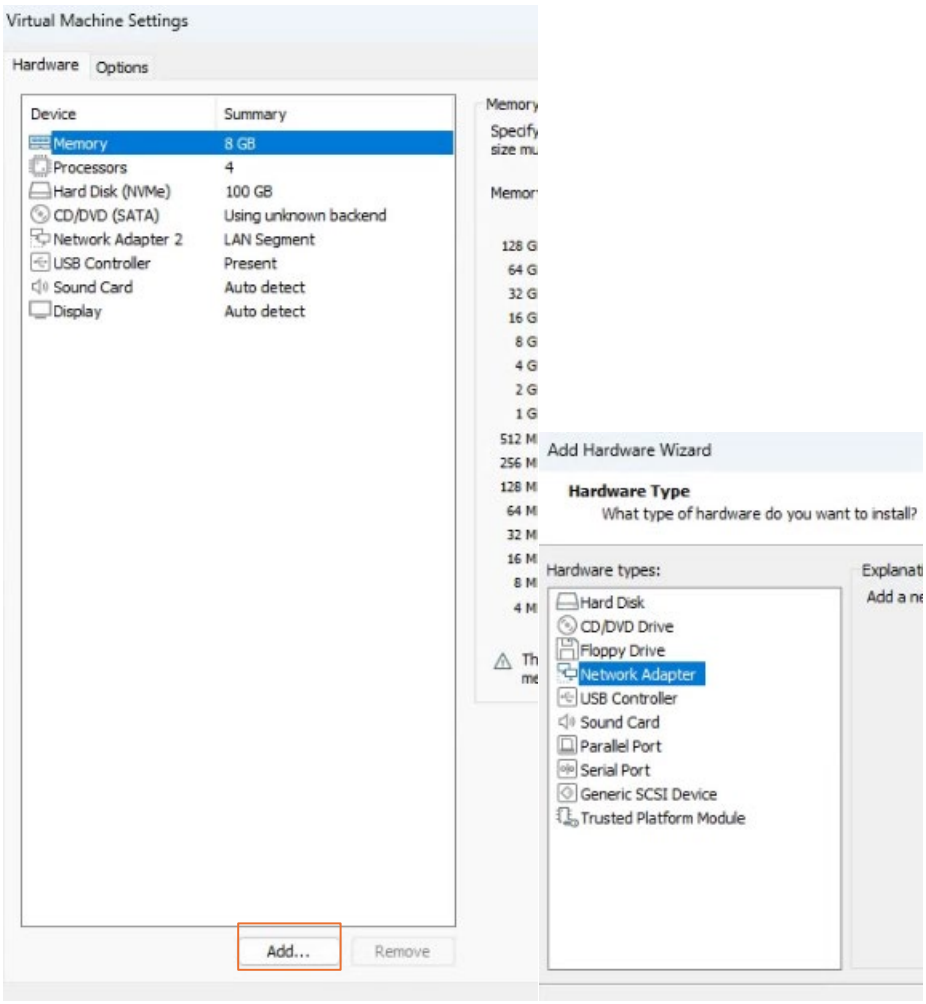
Install Microsoft Office Administrative Templates from this link:
https://www.microsoft.com/en-us/download/details.aspx?id=49030

But first, we have to add a NAT NIC to access the internet and download the package. We'll remove it right after the download.

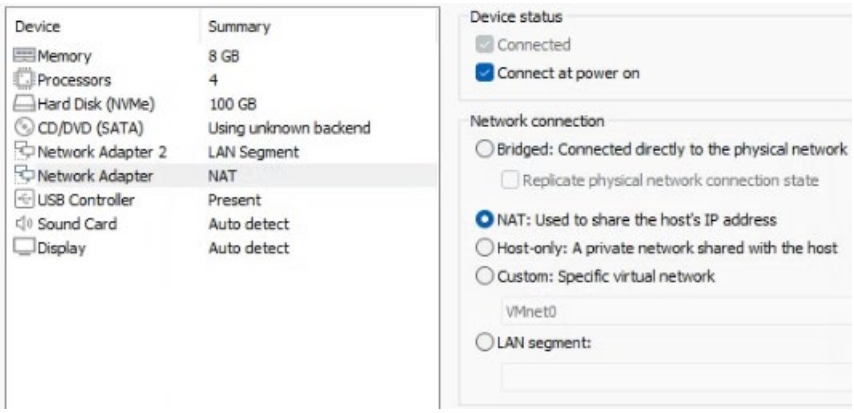
Right-click on DC112 → Settings



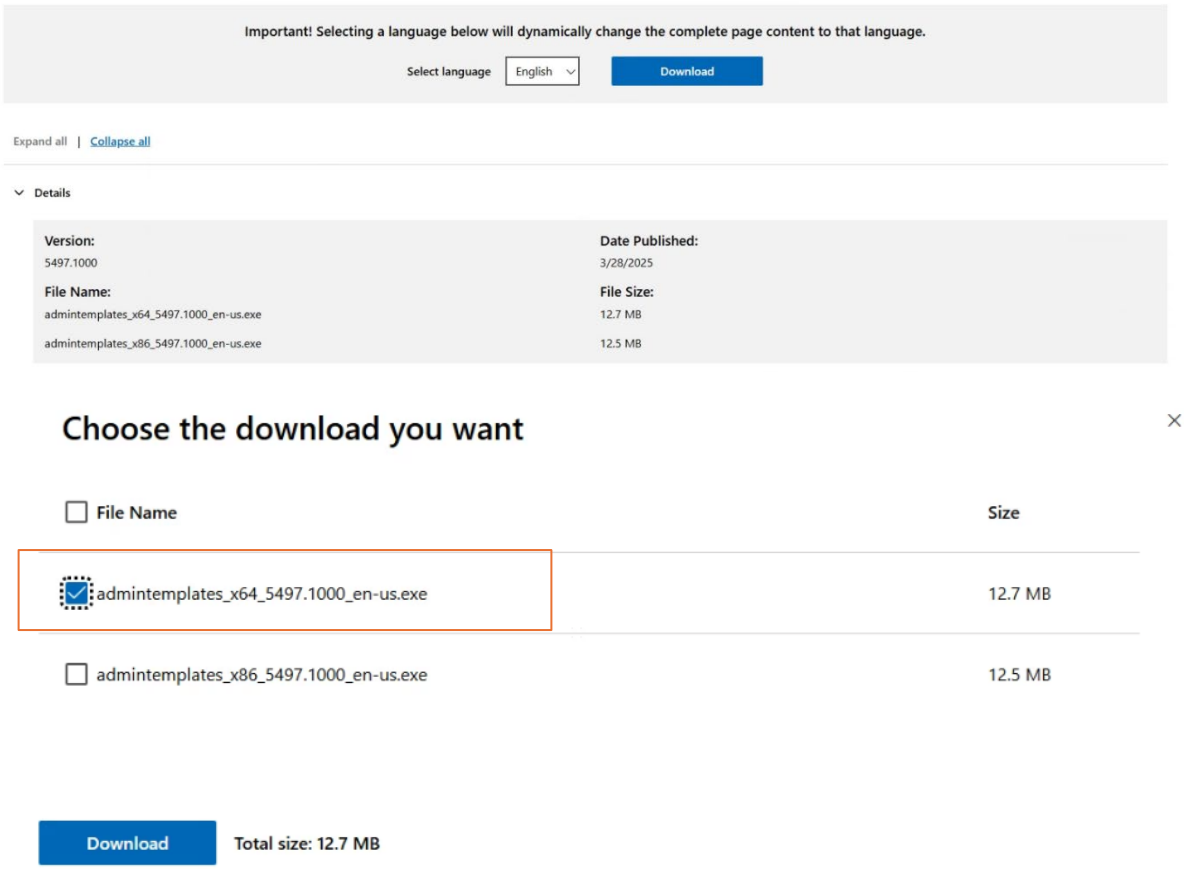
Click on Add and select Network Adapter

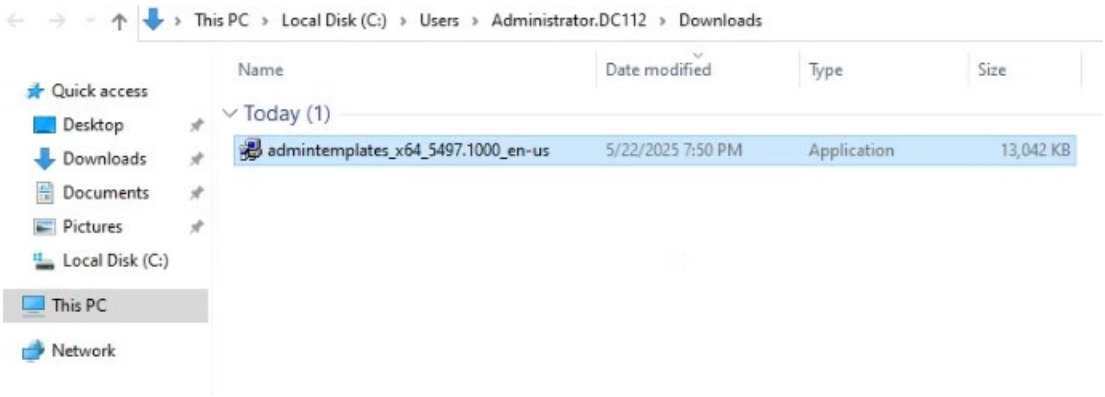


Make sure it's set to NAT and then click on OK

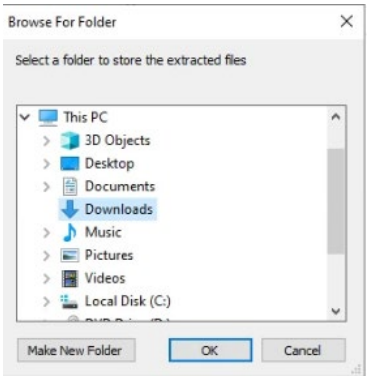


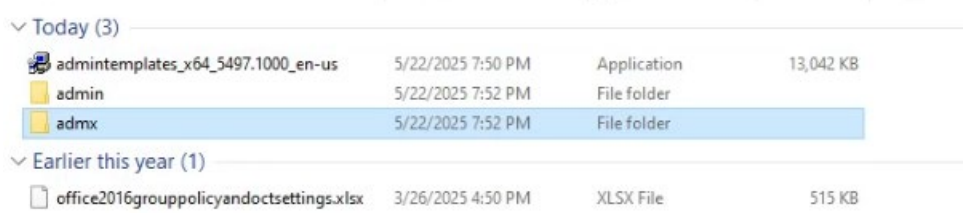
Copy paste the link in Edge



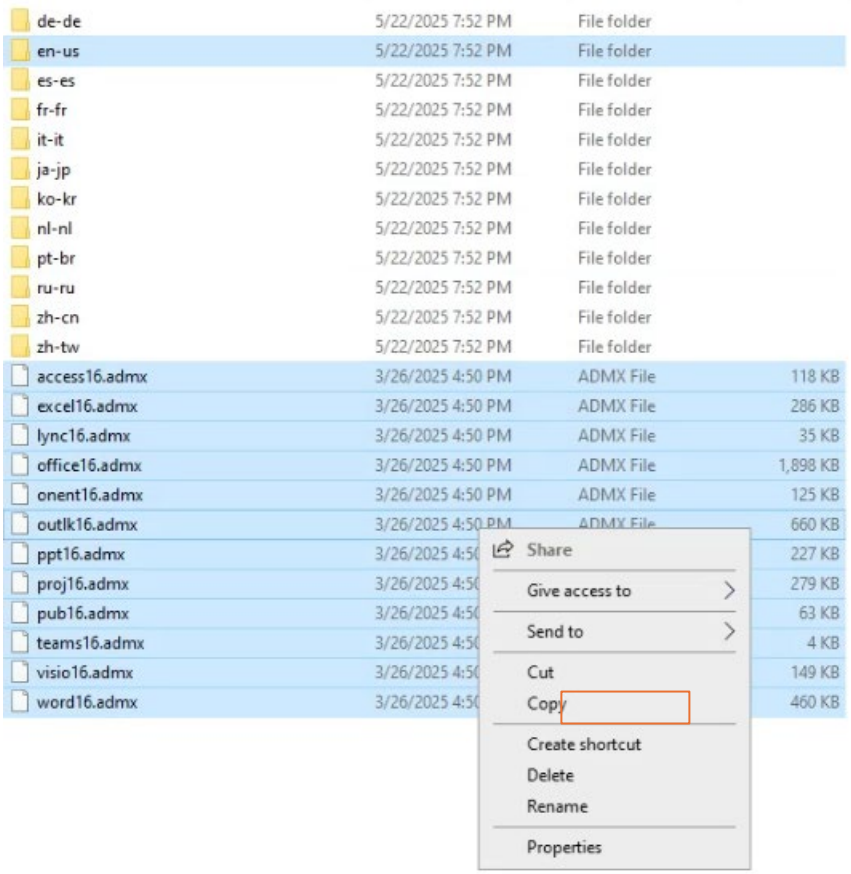


Double-click on the package and extract the files to Downloads

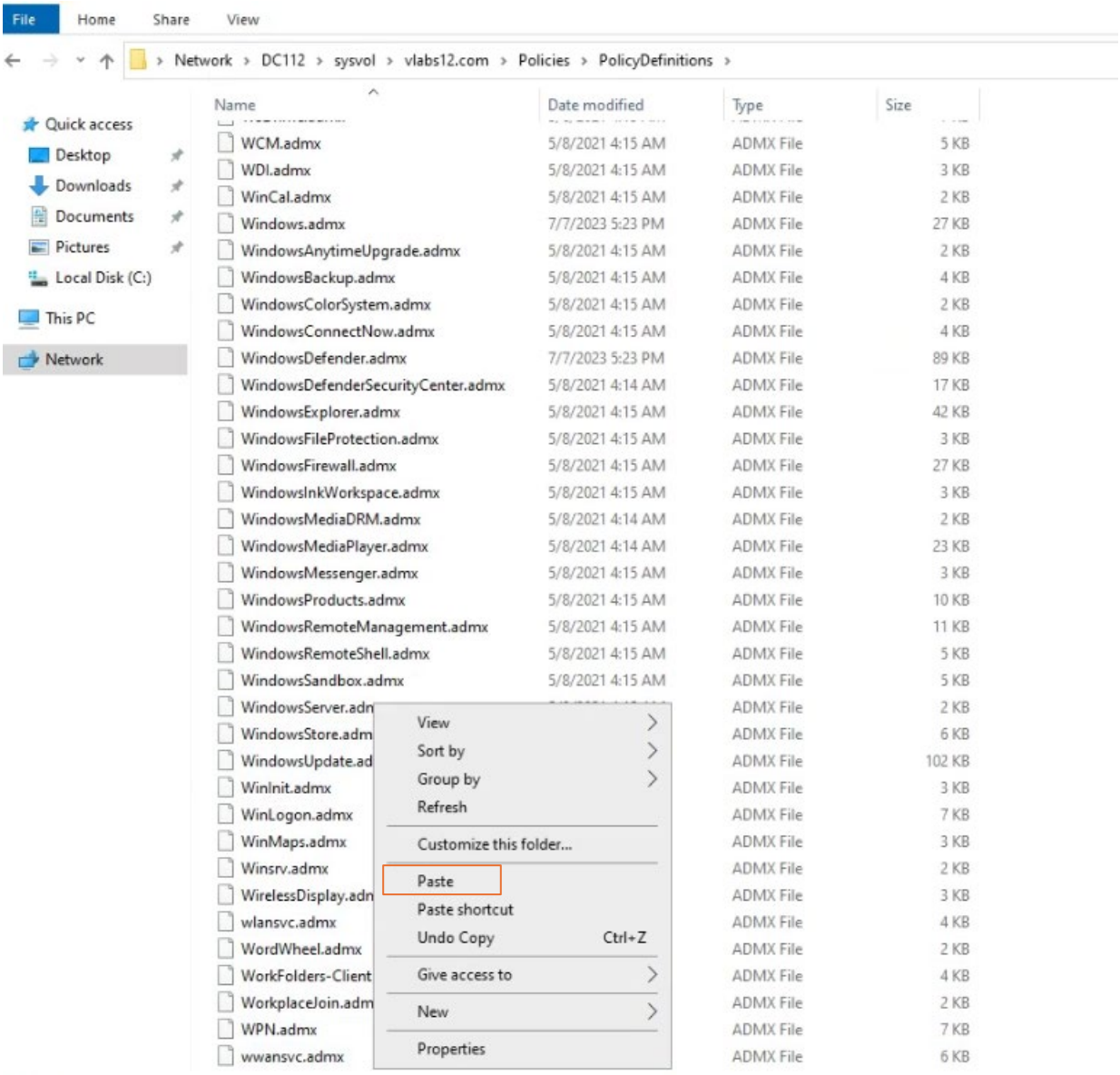


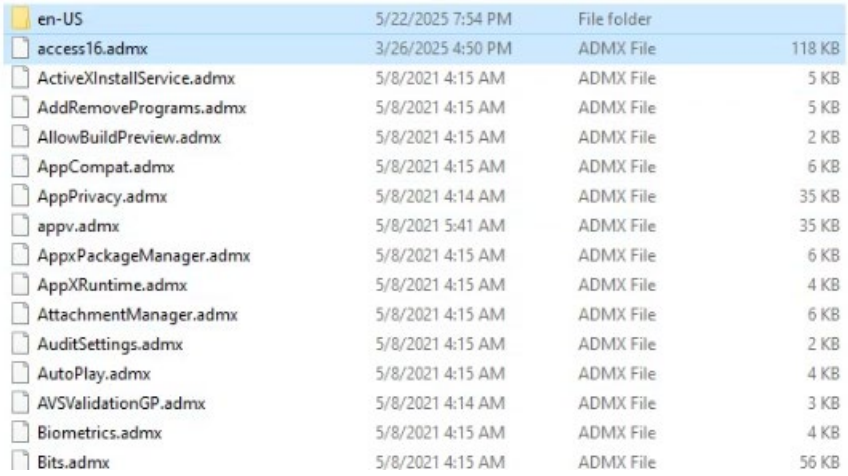


Copy all the admx files and the en-us folder (adml)



Paste them in PolicyDefinitions



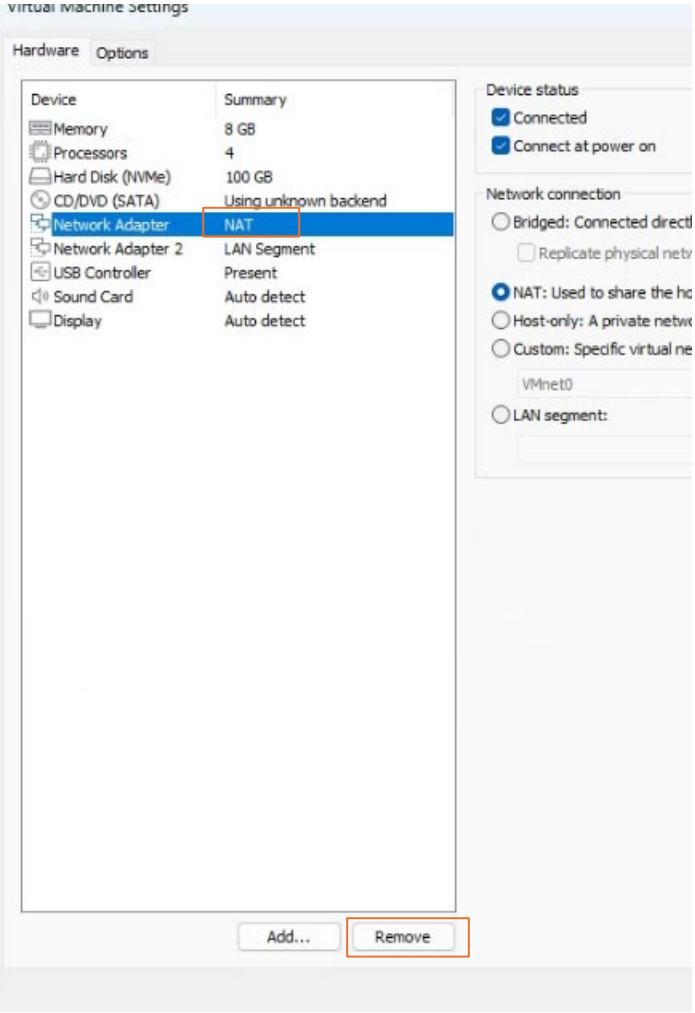


en-US	5/22/2025 7:54 PM	File folder	
access16.admx	3/26/2025 4:50 PM	ADMX File	118 KB
ActiveXInstallService.admx	5/8/2021 4:15 AM	ADMX File	5 KB
AddRemovePrograms.admx	5/8/2021 4:15 AM	ADMX File	5 KB
AllowBuildPreview.admx	5/8/2021 4:15 AM	ADMX File	2 KB
AppCompat.admx	5/8/2021 4:15 AM	ADMX File	6 KB
AppPrivacy.admx	5/8/2021 4:14 AM	ADMX File	35 KB
appv.admx	5/8/2021 5:41 AM	ADMX File	35 KB
AppxPackageManager.admx	5/8/2021 4:15 AM	ADMX File	6 KB
AppXRuntime.admx	5/8/2021 4:15 AM	ADMX File	4 KB
AttachmentManager.admx	5/8/2021 4:15 AM	ADMX File	6 KB
AuditSettings.admx	5/8/2021 4:15 AM	ADMX File	2 KB
AutoPlay.admx	5/8/2021 4:15 AM	ADMX File	4 KB
AVSValidationGP.admx	5/8/2021 4:14 AM	ADMX File	3 KB
Biometrics.admx	5/8/2021 4:15 AM	ADMX File	4 KB
Bits.admx	5/8/2021 4:15 AM	ADMX File	56 KB

Remove the NAT NIC.

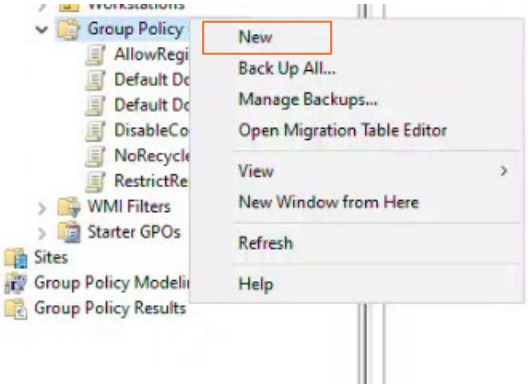
Like before, right click on DC112 → Settings

Select NAT and click Remove

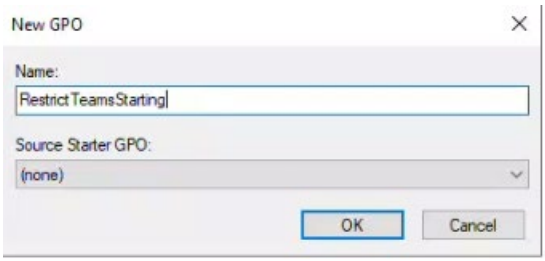


Create a new GPO named **RestrictTeamsStarting**

In Group Policy Management, right-click on GPO → New

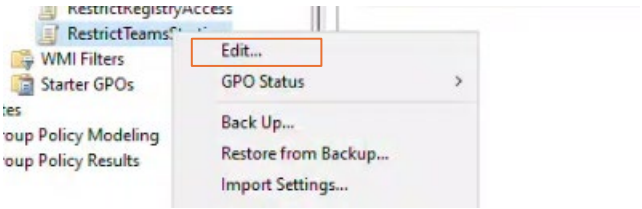


Create the GPO **RestrictTeamsStarting**

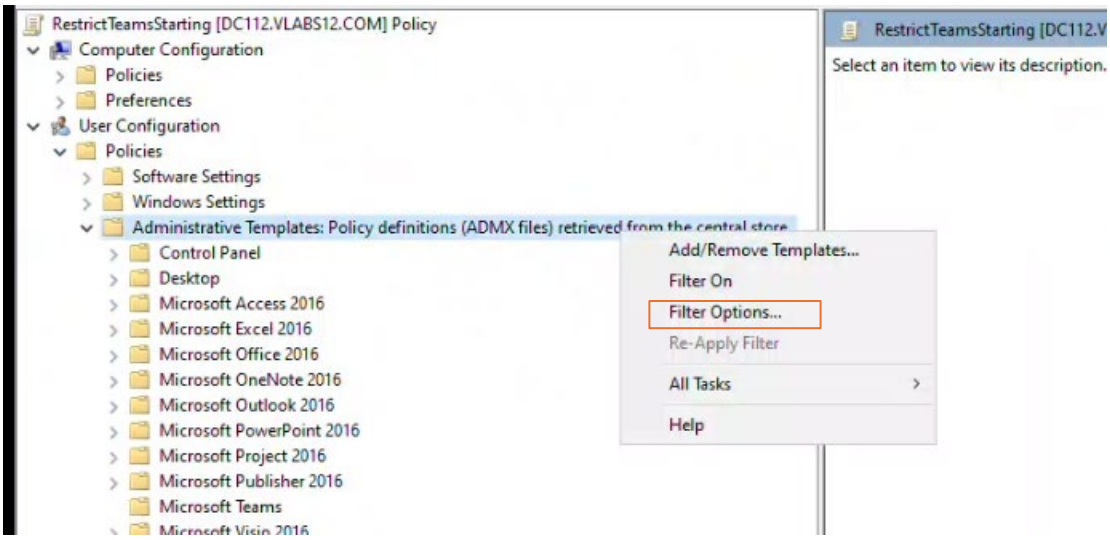


Use Filter Options for User Configuration to locate **Microsoft Teams** settings.

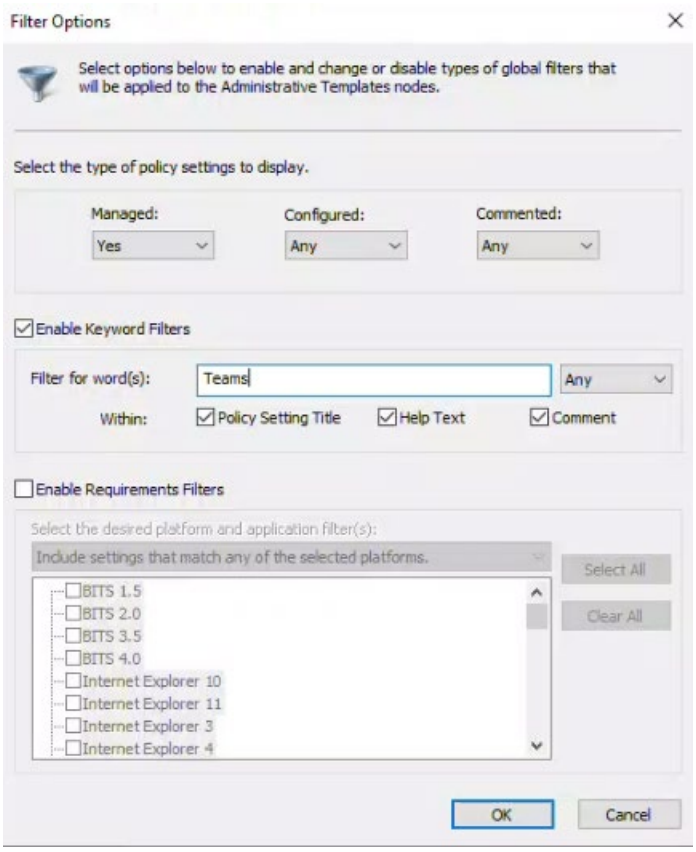
Right-click on the new GPO → Edit



Under User Configuration → Policies, right click on Administrative Templates and select Filter Options

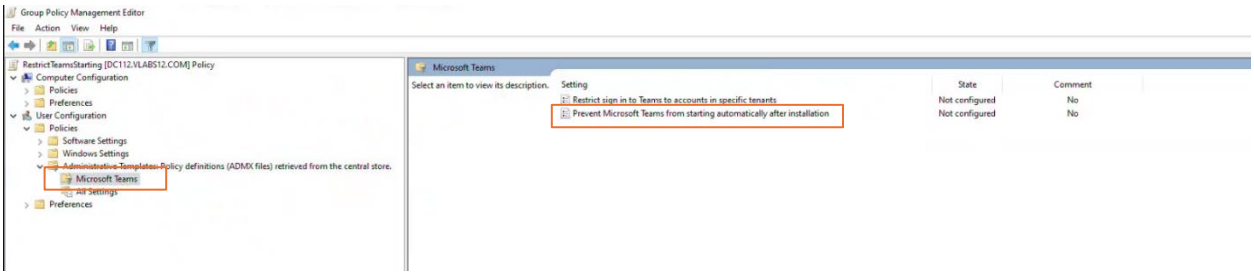


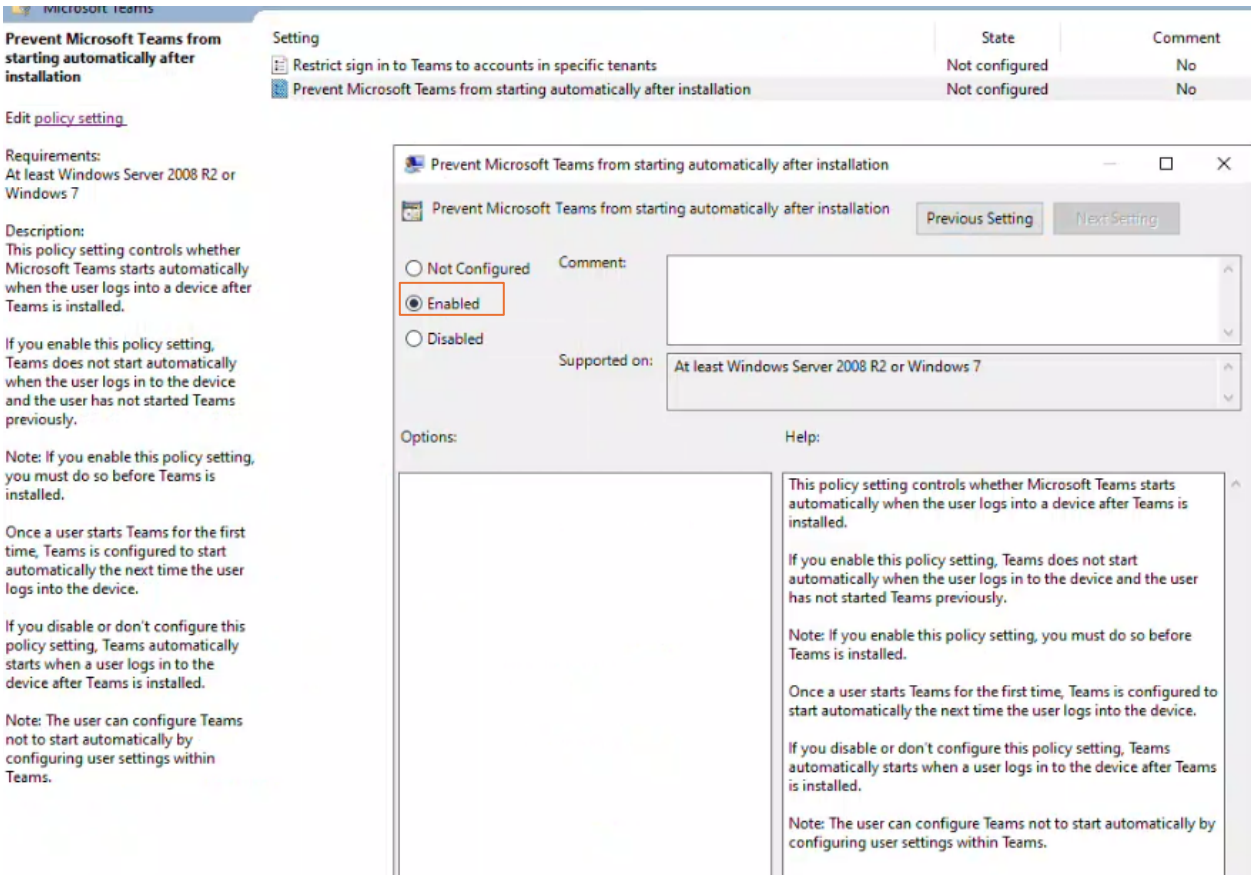
Click on Enable Keyword Filters and filter for the word Teams. Click OK.

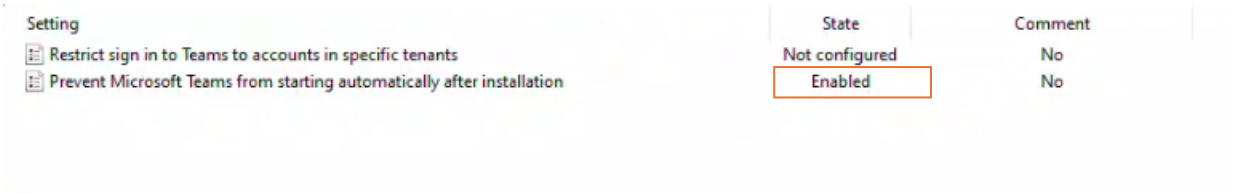


Under Microsoft Teams, find the setting “Prevent Microsoft Teams from starting automatically after installation”

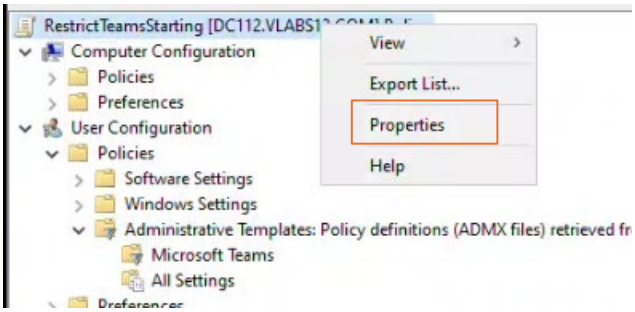
Enable it.



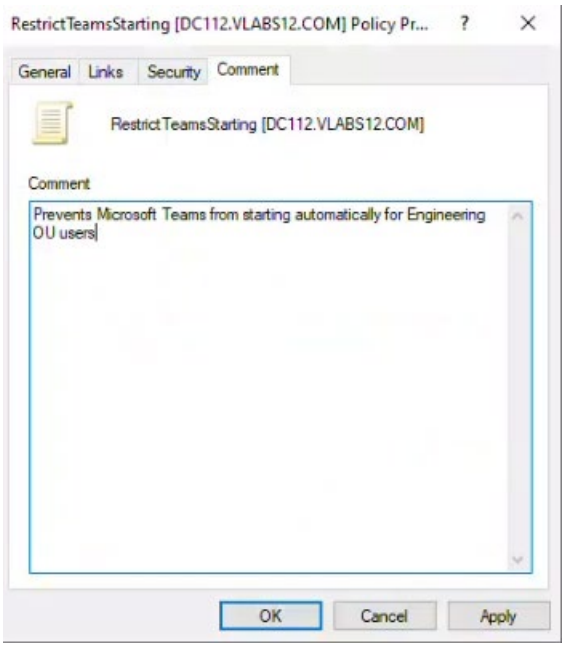




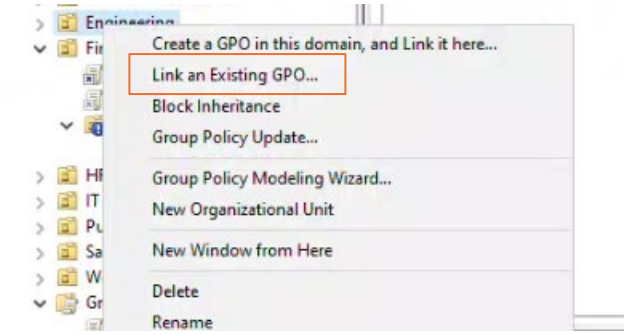
Still in the editor, right-click on the GPO → Properties



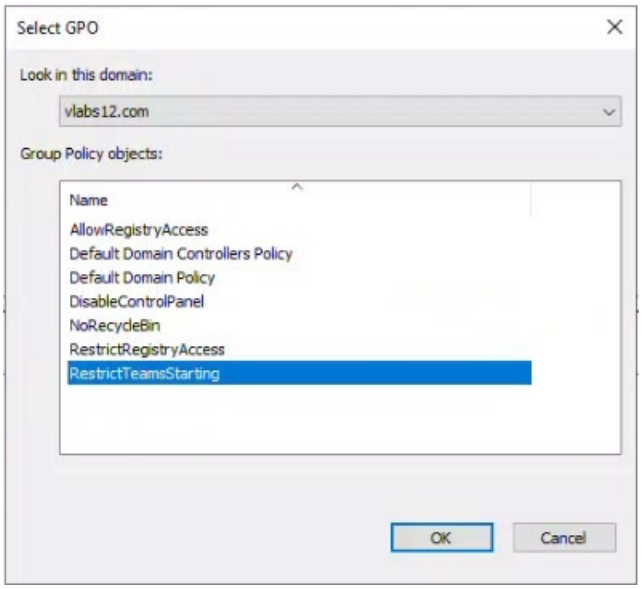
In the Comment section, write a comment related to the purpose of this GPO.



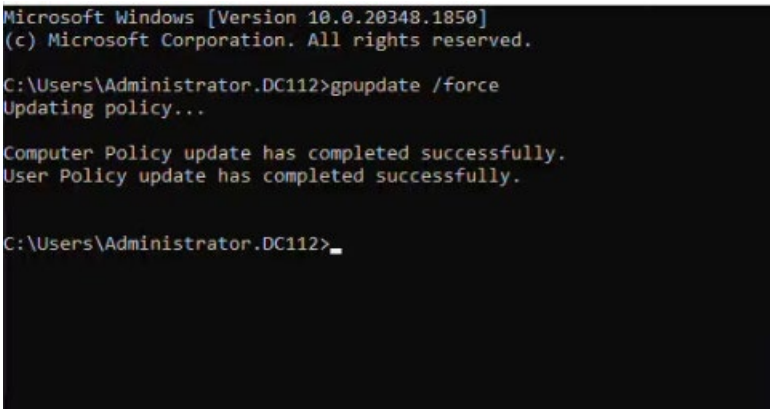
Back in Group Policy Management, right-click on Engineering OU and select Link an Existing GPO



Link **RestrictTeamsStarting**



In CMD, do a **gpupdate /force.**



Task 3: Managing Account Policies

Modify password policies in the Default Domain Policy GPO:

Minimum password length: 12 characters.

Password complexity: Enabled.

Password expiration: 60 days.

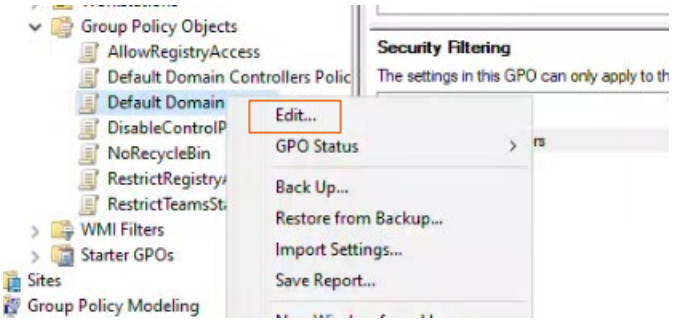
Apply Account Lockout Policy:

Lock account after 2 failed login attempts.

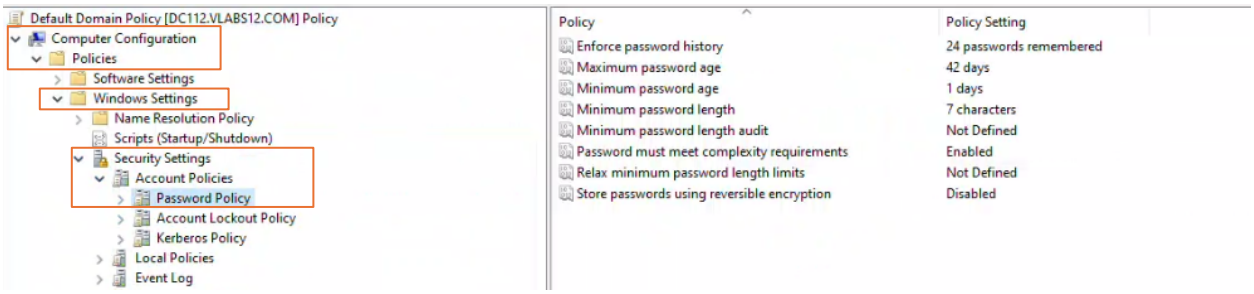
Lockout duration: 2 minutes.

- Run gpupdate /force to apply changes.
- From Client12, test with Emma Petit by attempting password modification and simulating an account lockout.

Under **Group Policy Objects**, right-click **Default Domain Policy** and select **Edit**.



Go to Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy

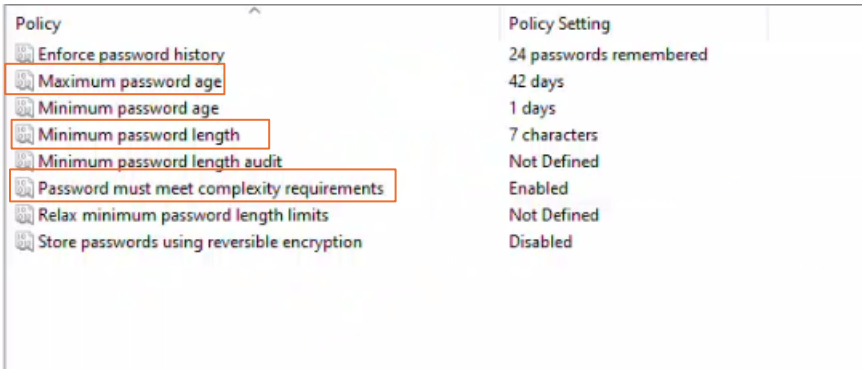


We'll be configuring the Minimum password length, Password complexity and Password expiration

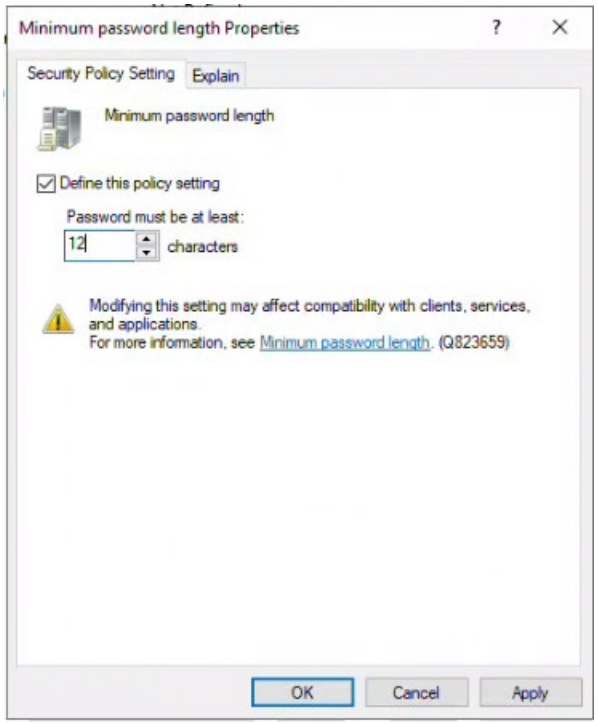
Minimum password length: 12 characters

Password complexity: Enabled.

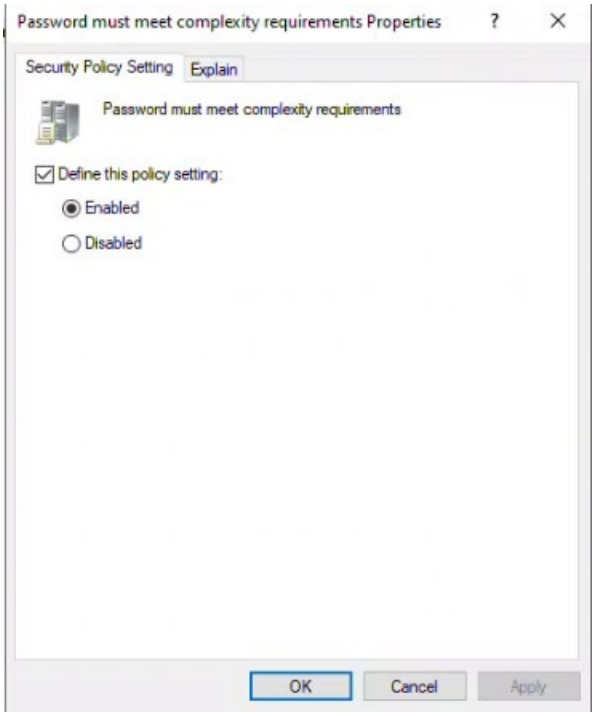
Password expiration: 60 days



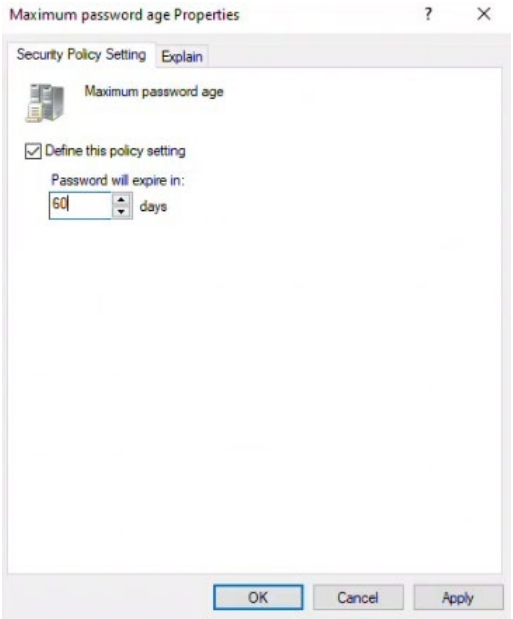
Minimum password length: 12 characters



Password complexity: Enabled.



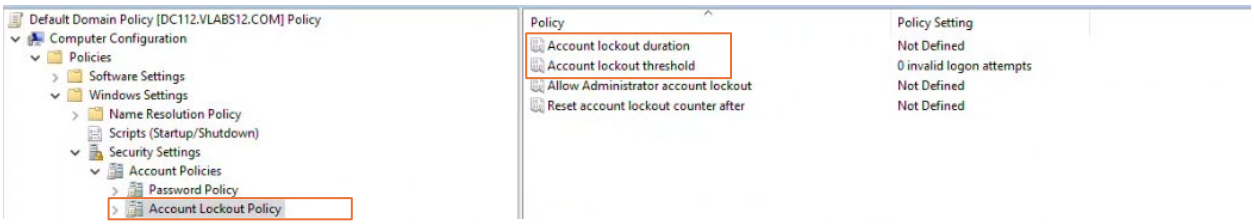
Password expiration: 60 days



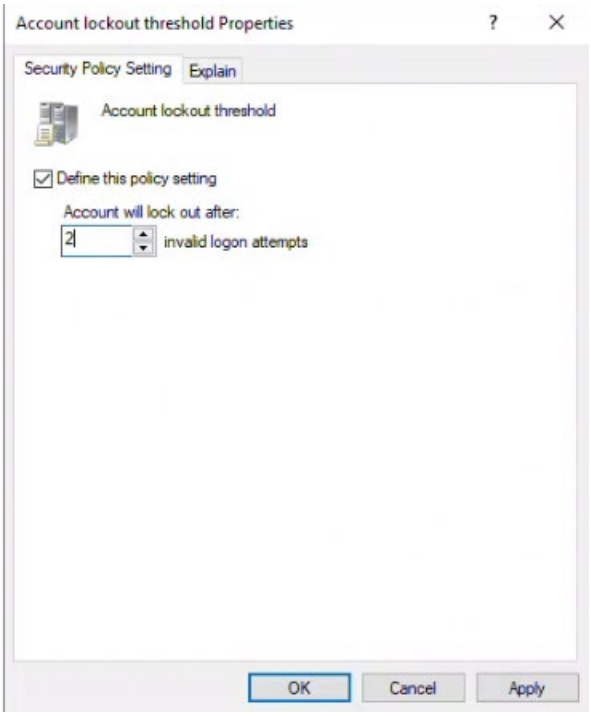
Apply Account Lockout Policy:

Lock account after 2 failed login attempts.

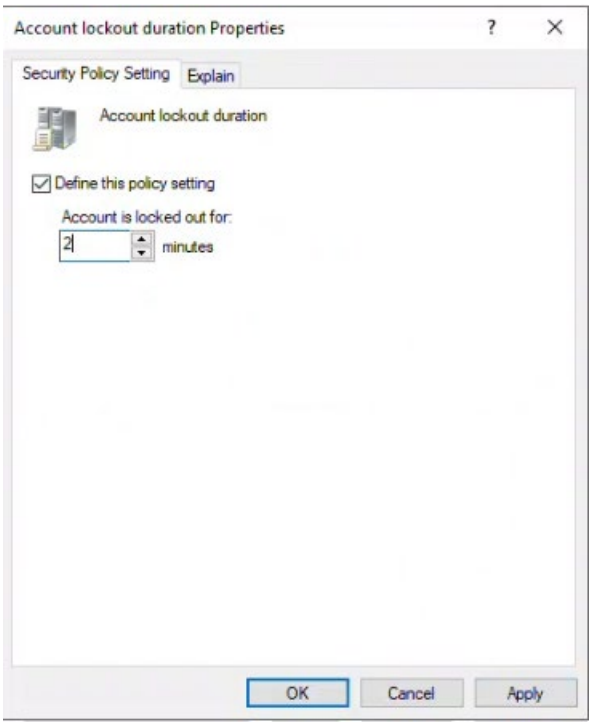
Lockout duration: 2 minutes

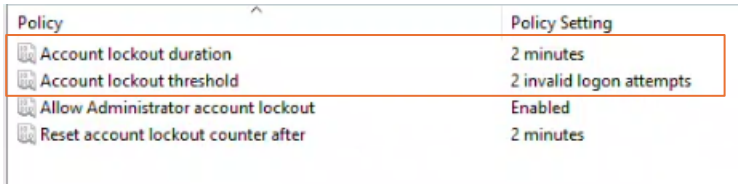


Lock account after 2 failed login attempts.

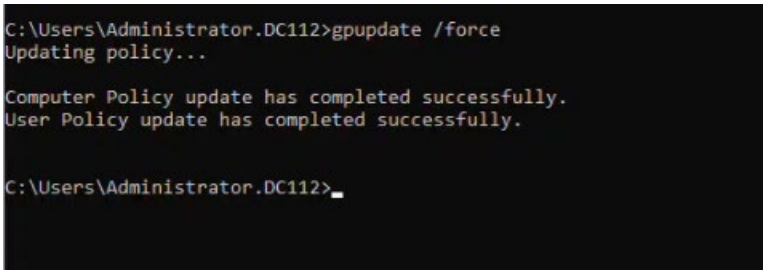


Lockout duration: 2 minutes





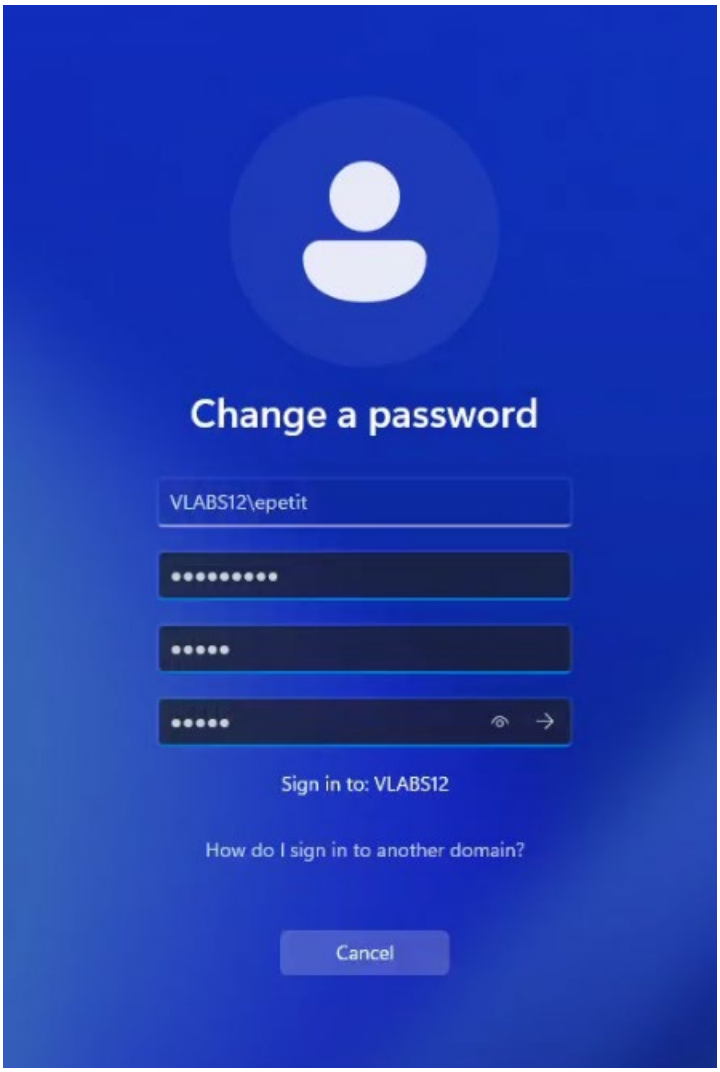
Run **gpupdate /force** to apply the policy changes.

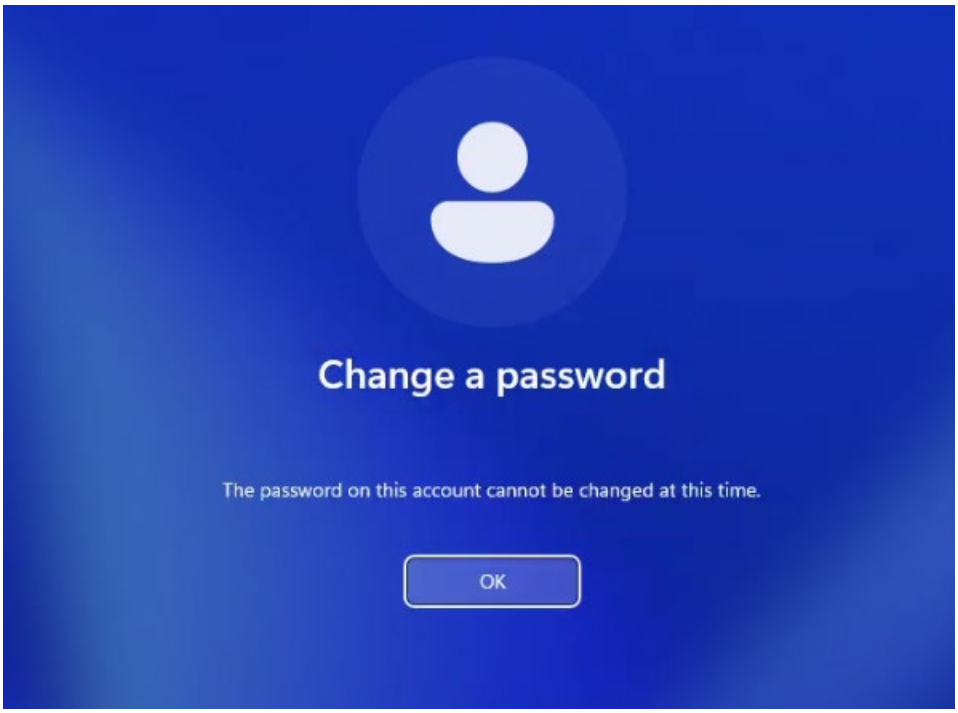


From Client12, test with Emma Petit by attempting password modification and simulating an account lockout

Press Ctrl+Alt+Delete, select **Change a password**.

Try a password shorter than 12 characters (e.g win11). It should fail due to the minimum length requirement.



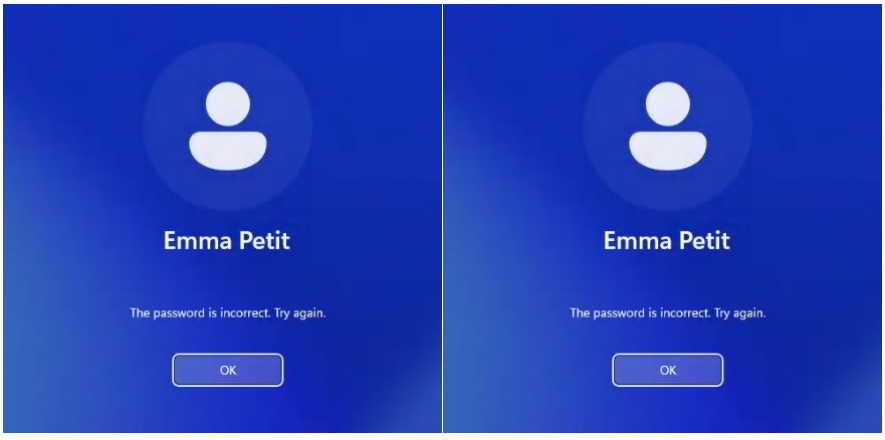


Simulate an account lockout:

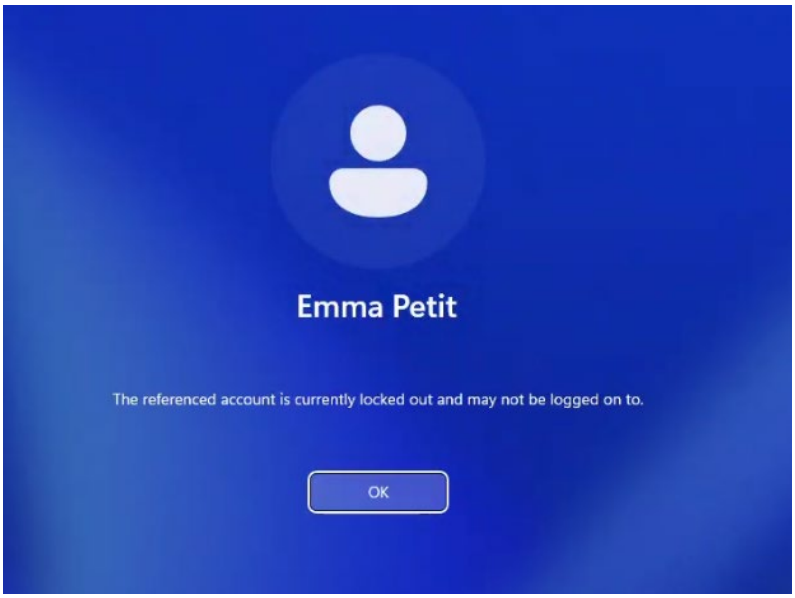
Log out, then attempt to log in with incorrect passwords 3 times (e.g. Pass121)

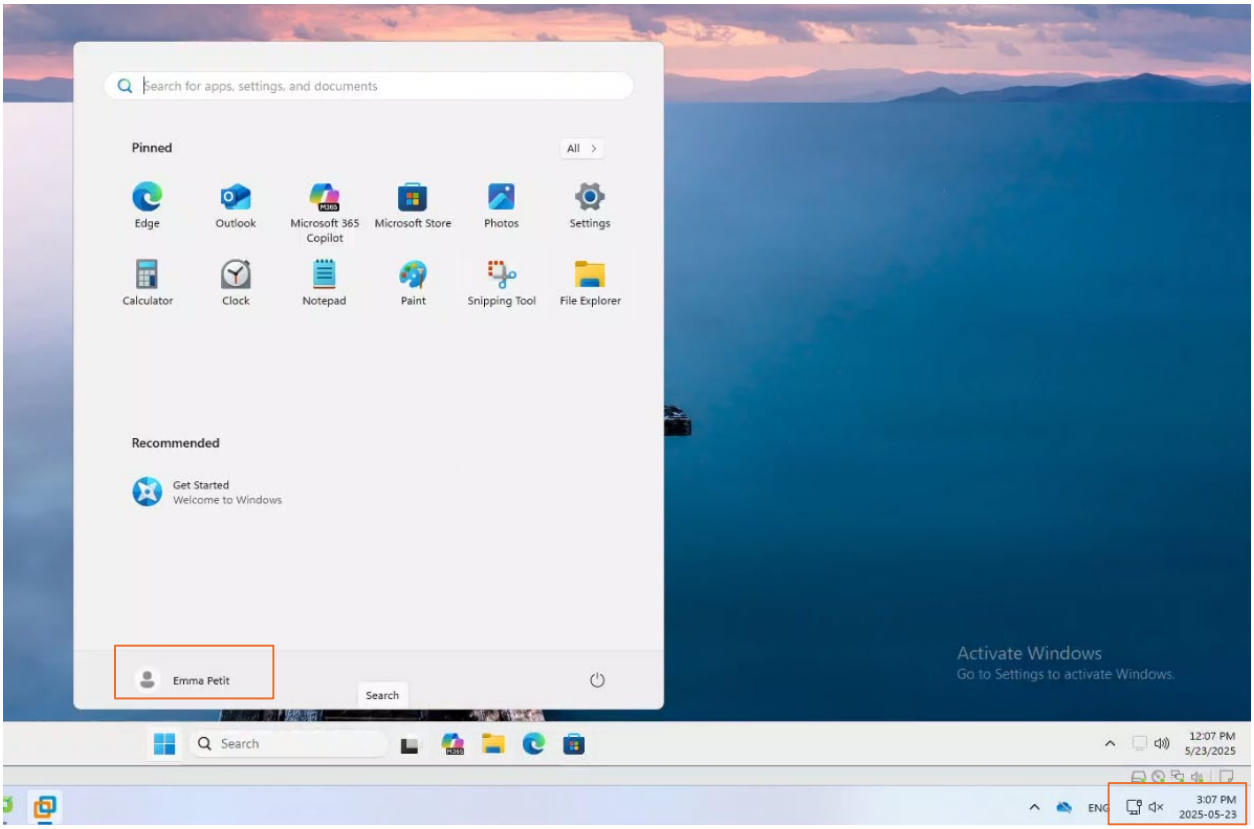
After the 2nd failed attempt, the account should lock for 2 minutes.

Try logging in again after 2 minutes with the correct password to confirm the lockout resets.



Locked out at 3:05 PM. I'll try again with the correct password at 3:07 PM





Lock out works for 2 minutes.

Task 4: Implementing Fine-Grained Password Policies

Create a new Fine-Grained Password Policy named **IT_FGPPolicy**

Modify password settings:

Minimum password length: **10 characters**.

Password complexity: **Disabled**.

Password expiration: **Never.**

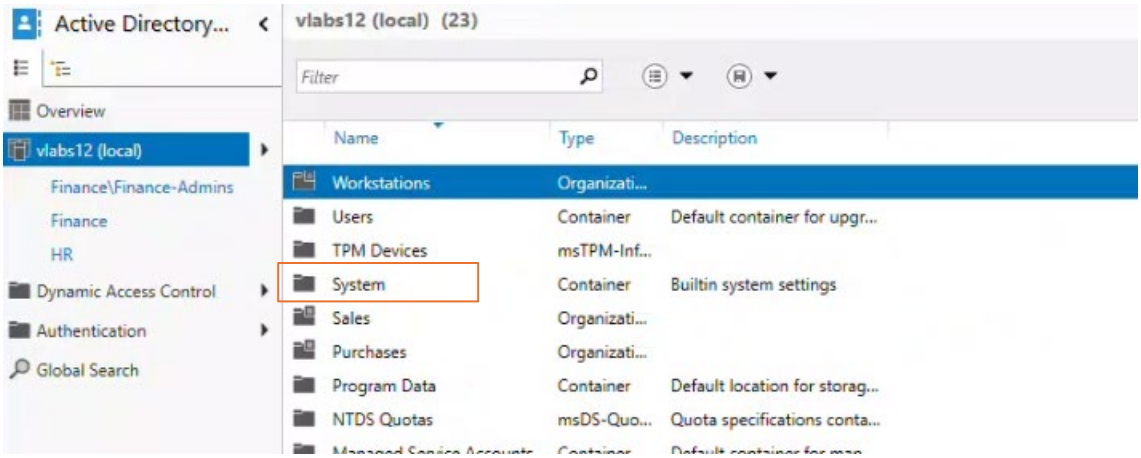
Directly apply it to the **IT Group.**

Run **gpupdate /force** to apply changes.

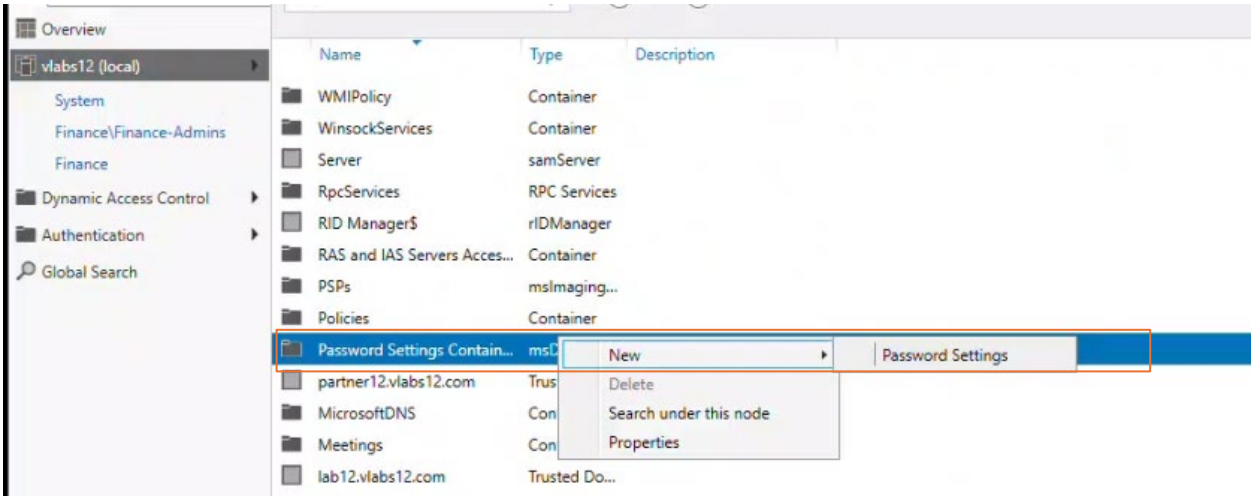
From Client12, test with a user from the IT group by attempting password modification.

Open ADAC (active directory administrative center)

Go to System → Password settings container

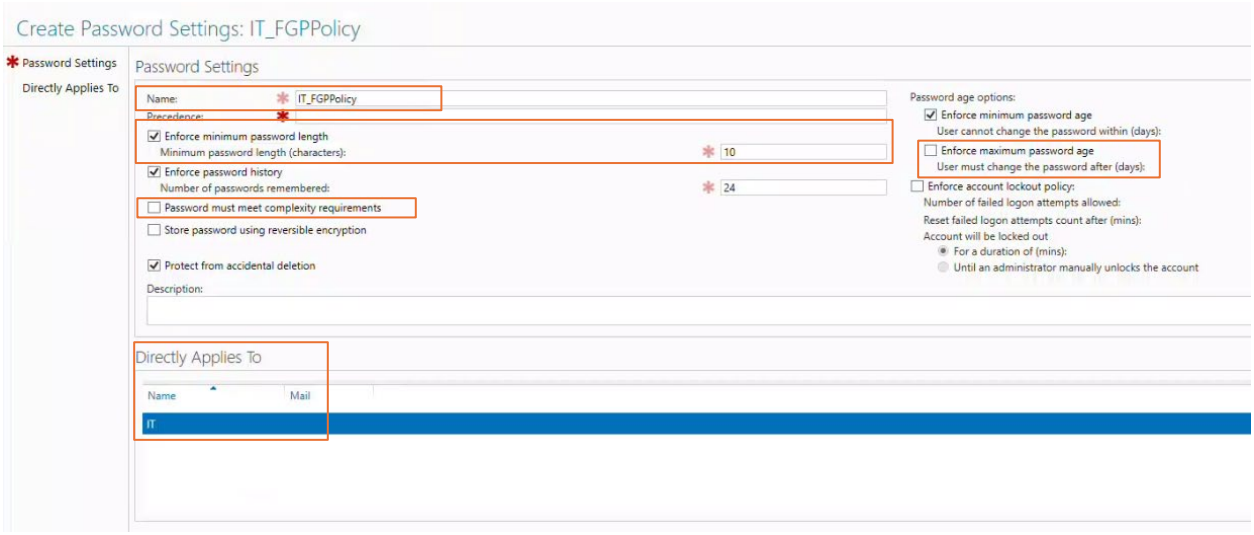


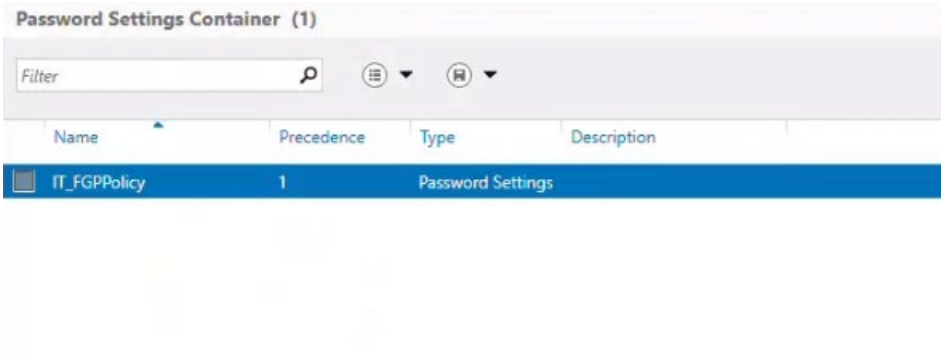
Right-click → New → Password settings



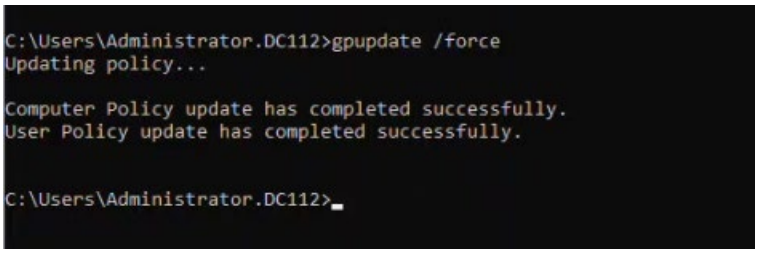
Enter IT_FGPPolicy,

Set the minimum password length to 10 characters, uncheck the box for enforce maximum password age and password must meet complexity requirements



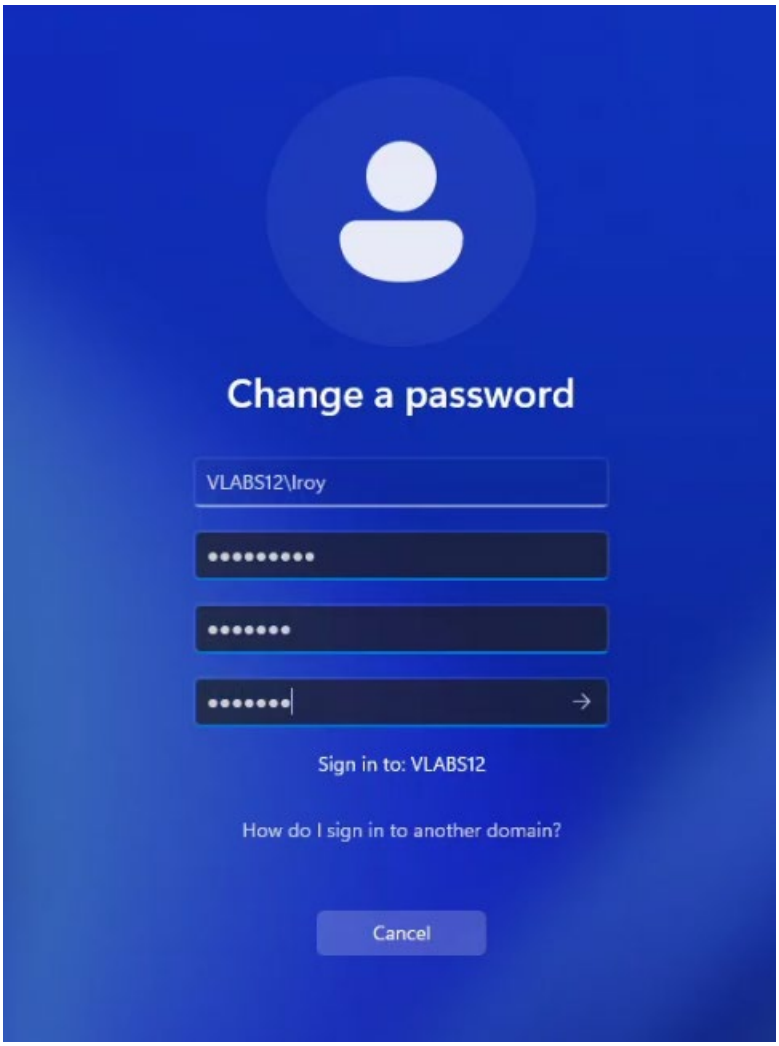


Do a gpupdate /force

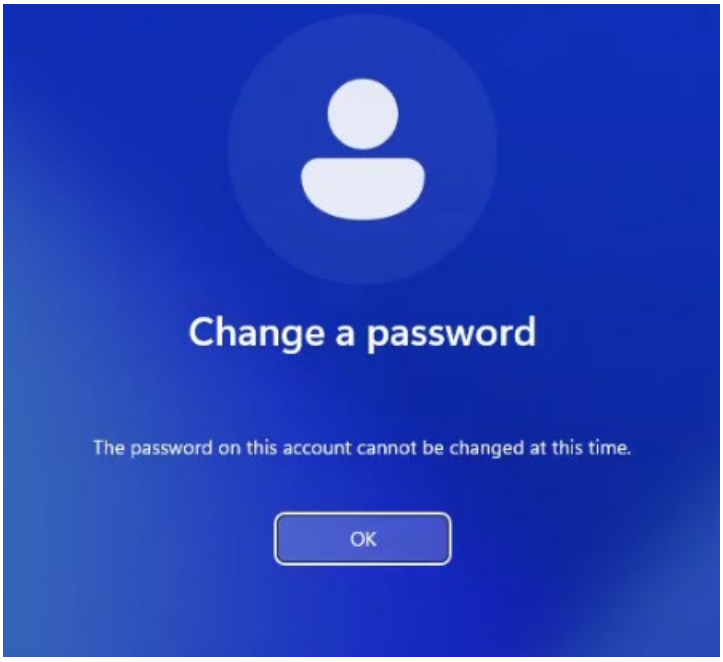


Sign in to Client12 with and IT user (Louise Roy)

Try to change the password to something 9 characters or less (e.g, pass123)

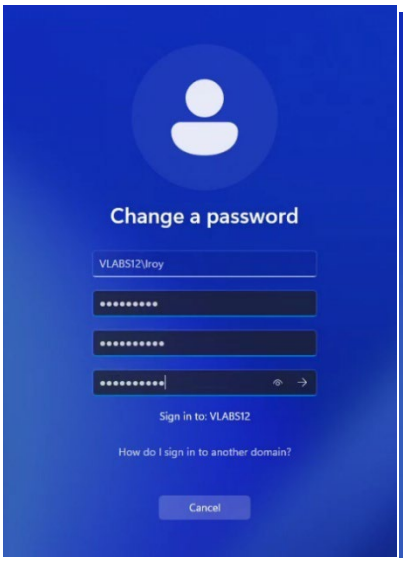


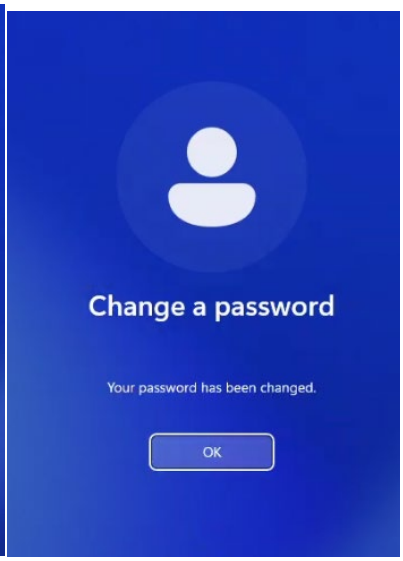
Can’t change it to pass123 because it’s 7 characters long.



I'll change it to something not complex that's 10 characters long (pass123456)

Note: I had to go back to the password policy we just created and disable "enforce minimum password age" in order to prove that the other settings worked. Since this was the first time signing in as Louise Roy, it had not been 1 day, which was the minimum password age requirement. I went back afterwards to re-enable the setting since it was not part of the requirements.





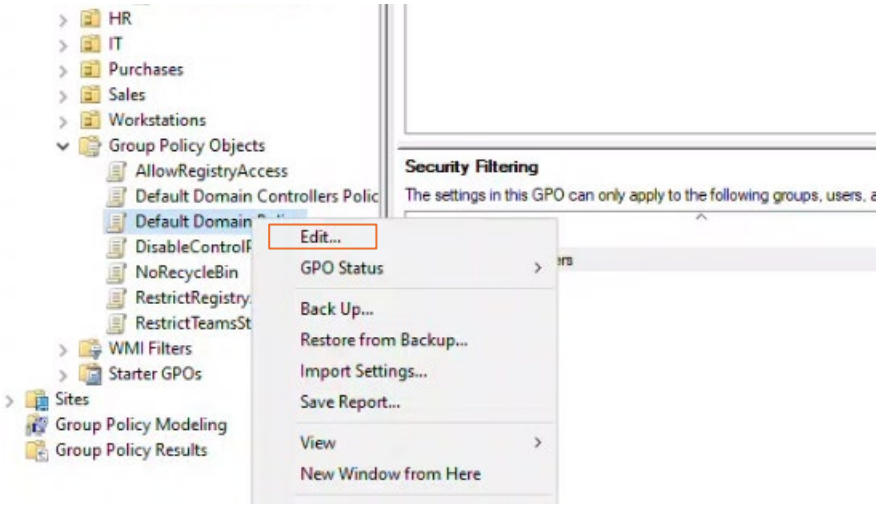
Task 5: Managing Audit Authentication

Modify Default Domain Policy GPO to enable Audit Logon Events (Success and Failure)

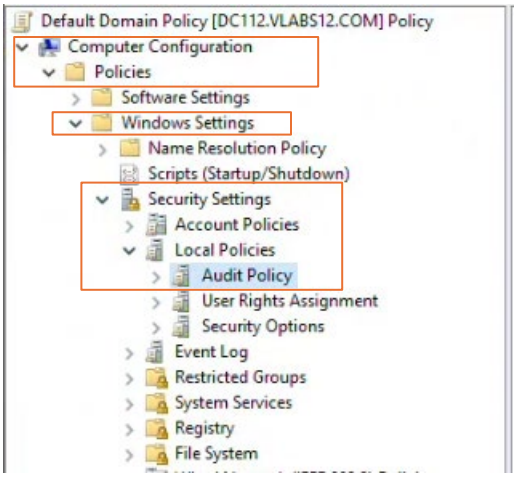
Restart the Client12

Test by failing and successfully logging in with any user on Client12

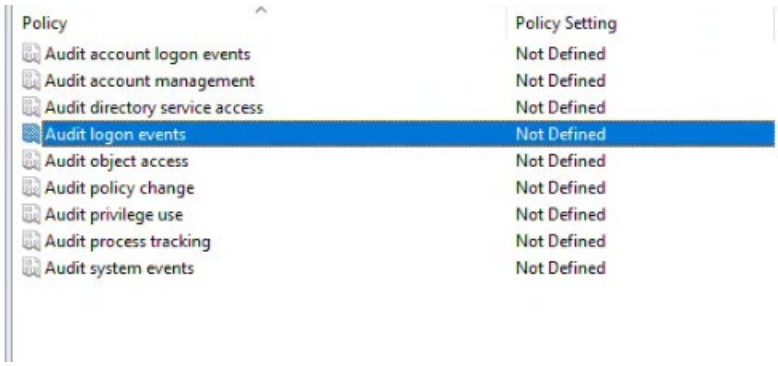
Open Event Viewer on DC112 and verify Security Logs.

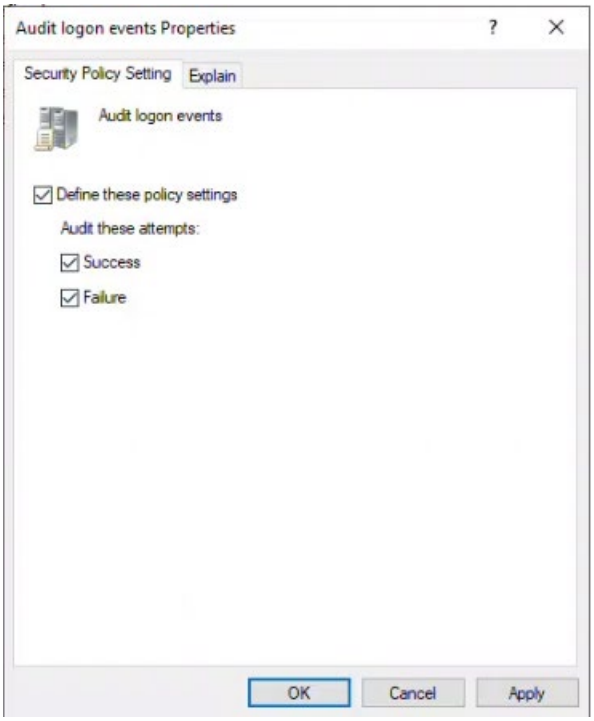


Go to Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Audit Policy



Set “Audit logon events” to success and failure

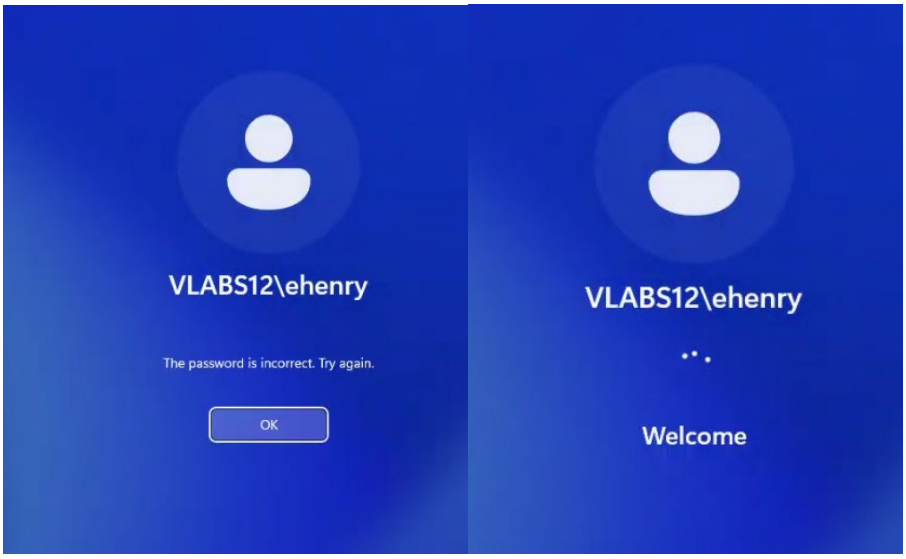




Policy	Policy Setting
Audit account logon events	Not Defined
Audit account management	Not Defined
Audit directory service access	Not Defined
Audit logon events	Success, Failure
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined

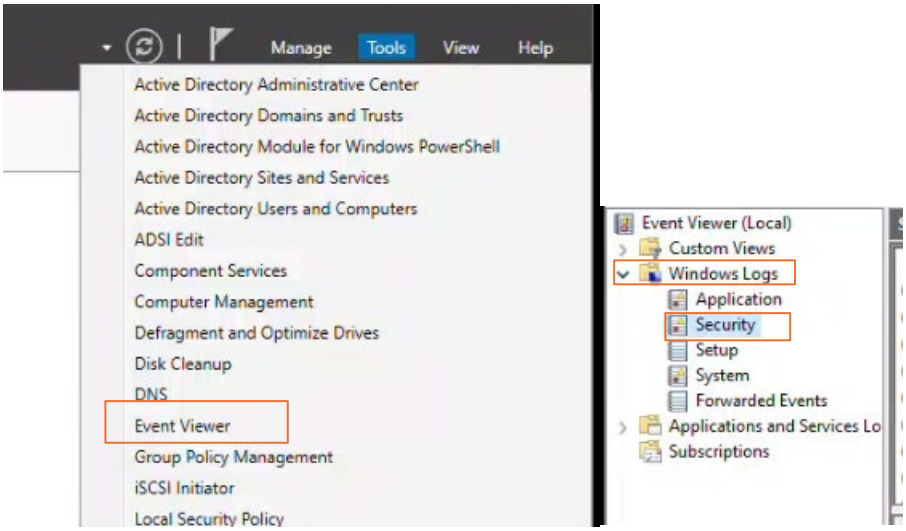
Reboot Client12

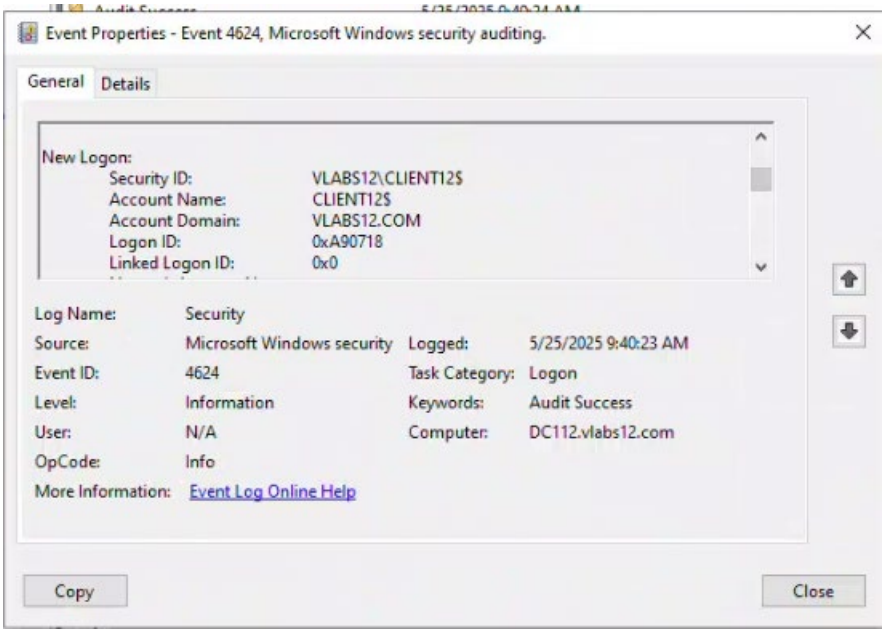
Test the changes by failing to log in and then logging in successfully.

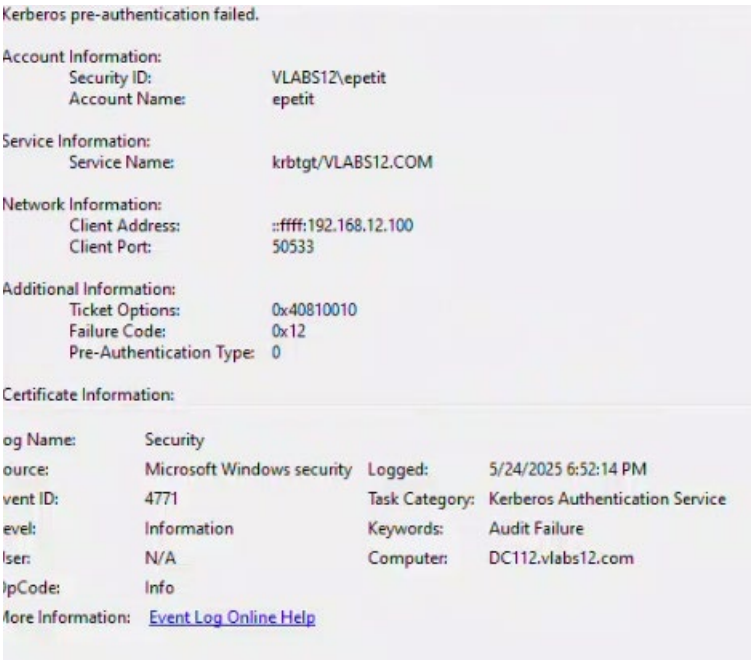


Open Event Viewer on DC112 and verify Security Logs

On DC112, go to Tools → Event Viewer. In Event Viewer, go to Windows Logs → Security







Task 6: Managing Security Templates

Create a security template named OpenSSH_Auth.

In this template, modify OpenSSH Authentication Agent under System Services to start automatically.

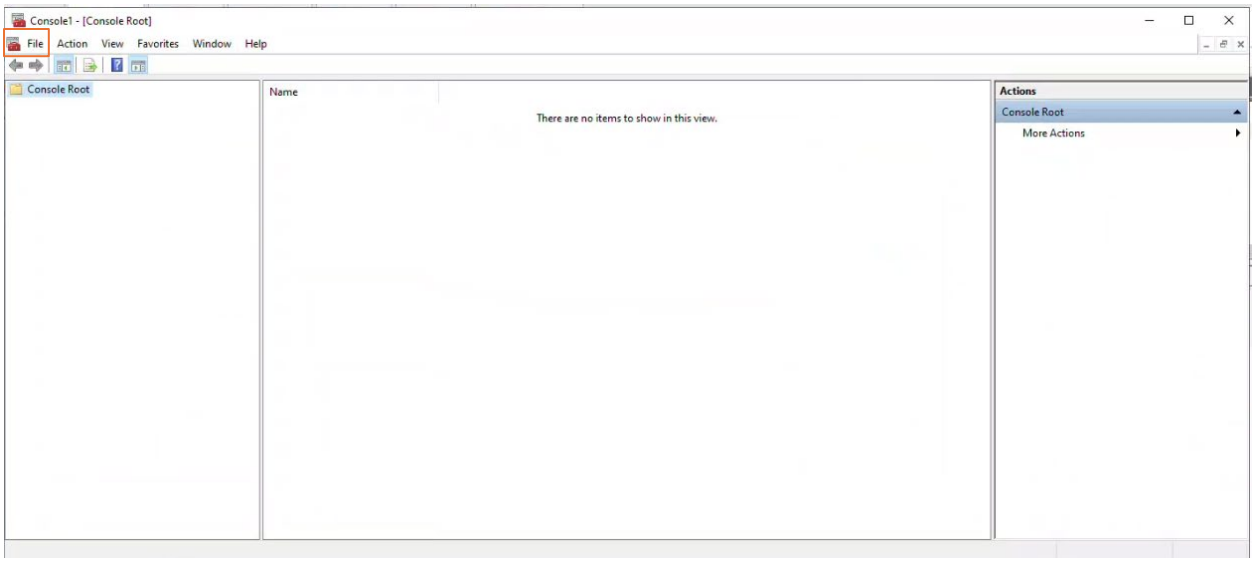
Import this new template into a new GPO named OpenSSHAuth.

Link the GPO to DomainControllers OU.

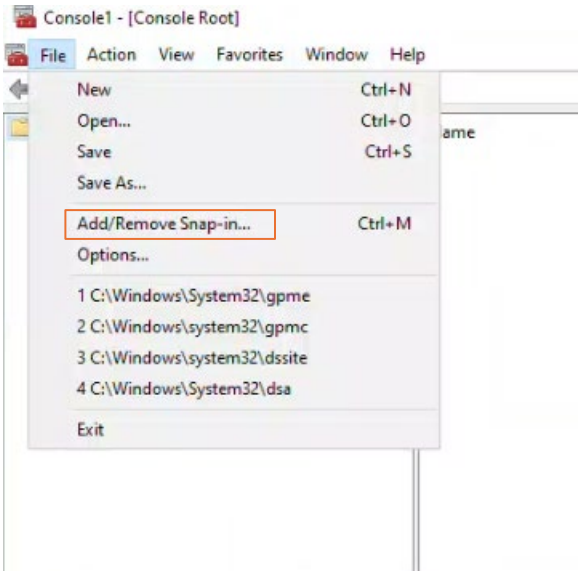
Run gpupdate /force on DC112 to apply changes.

Restart DC112 and verify in Services that OpenSSH Authentication Agent has started.

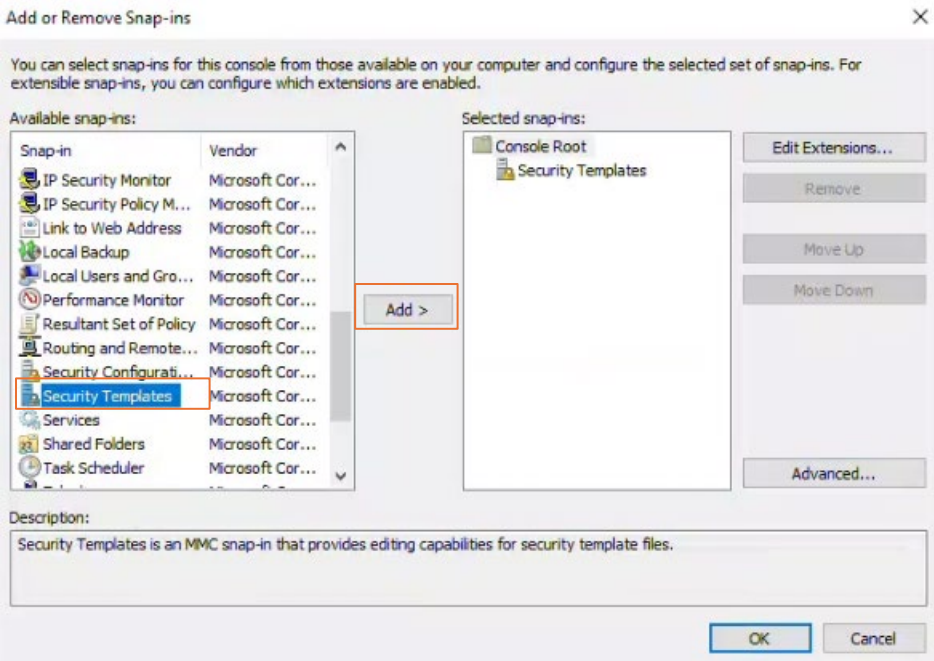
On DC112, go to run (Win+r) and type in “mmc”



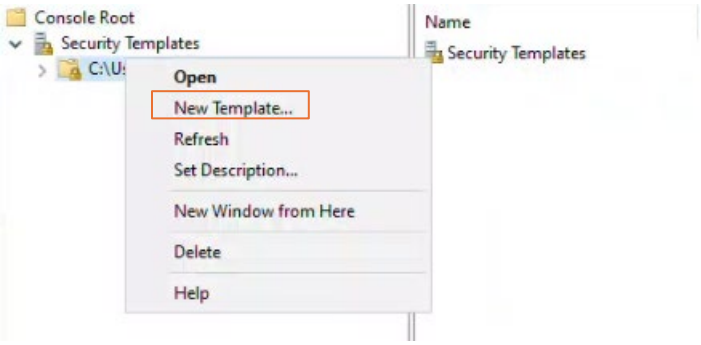
Go to File → Add/remove snap-in..



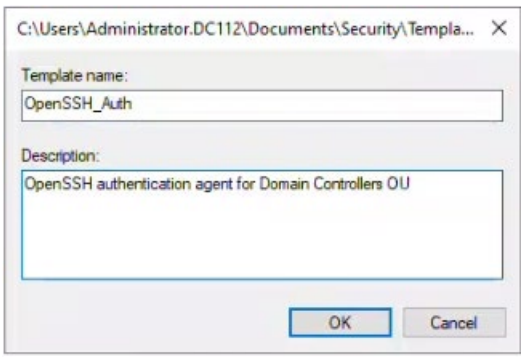
Scroll down to Security Templates and click Add



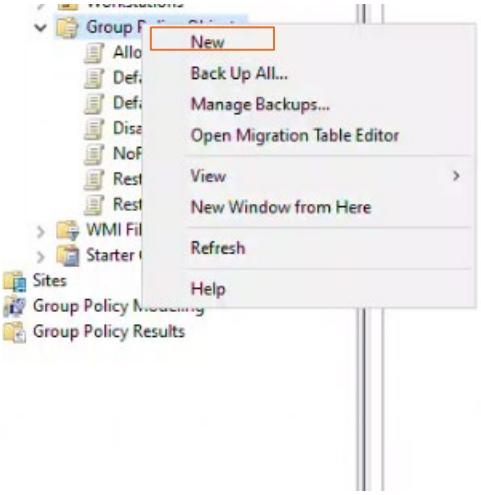
Expand security templates and right click on the default path. Select New Template

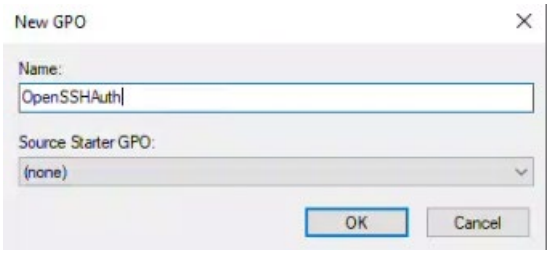


Name it OpenSSH_Auth and set a description

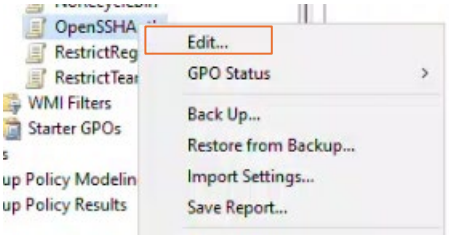


Create the new GPO OpenSSHAuth



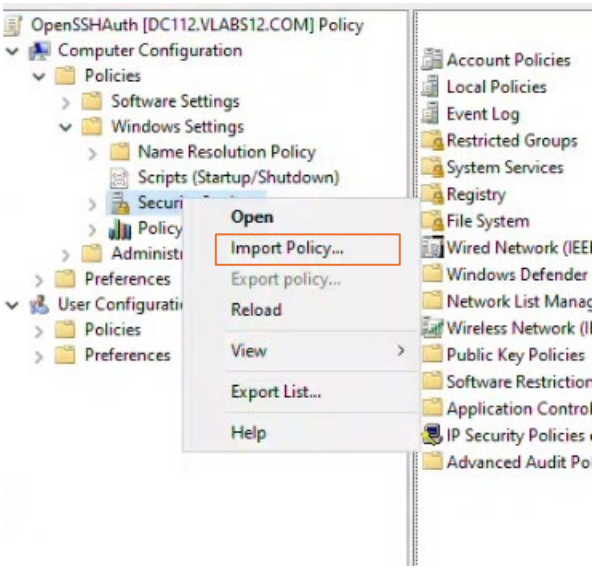


Right-click and go to Edit

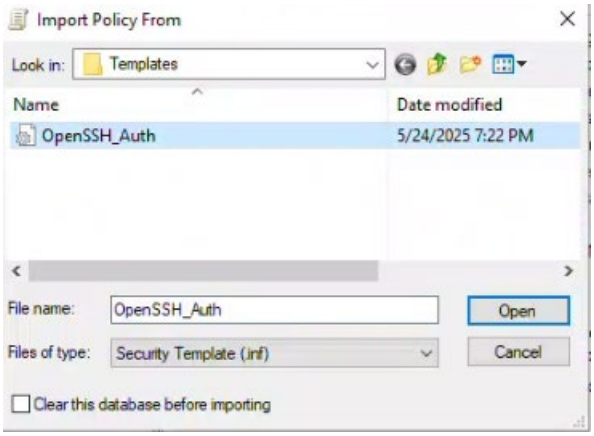


Go to Computer Configuration → Policies → Windows Settings → Security Settings.

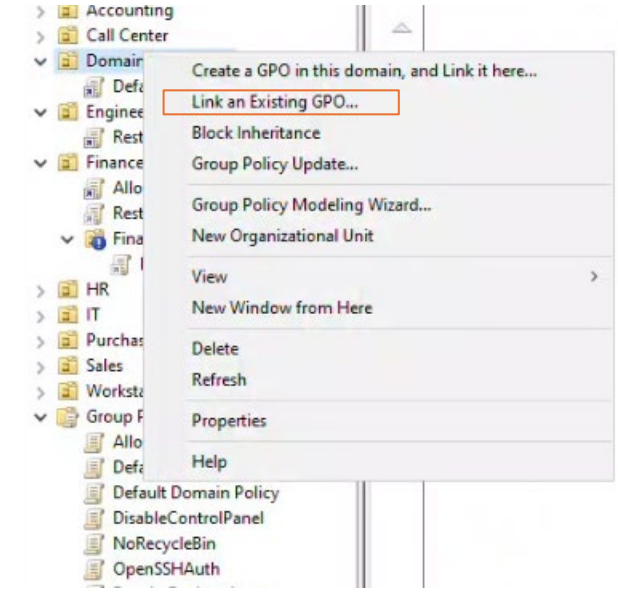
Right-click on Security Settings and select Import Policy

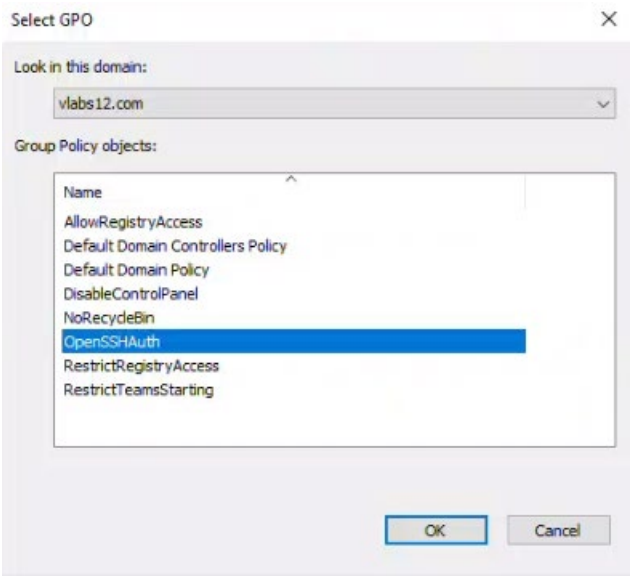


Select the template we created



Link the GPO to Domain Controllers OU





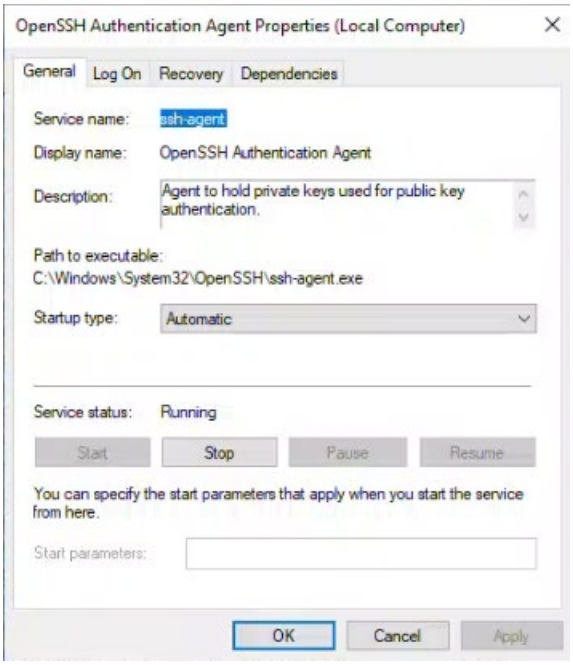
Use the arrow to set the link order to 1 (not shown here)

Apply the policy with gpupdate /force and then restart the server

```
C:\Users\Administrator.DC112>gpupdate /force
Updating policy...

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


C:\Users\Administrator.DC112>
```

Go to Services and find OpenSSH Authentication Agent

Make sure it's automatic and running



Task 7: Configuring Folder Redirection

Use DC312 as the file server.

Create a shared folder: \\DC312\UserData to the HR Group (r & w).

Create a new GPO named SharedUserData

Use Basic redirection to Create a Folder for Each User Under the Root Path

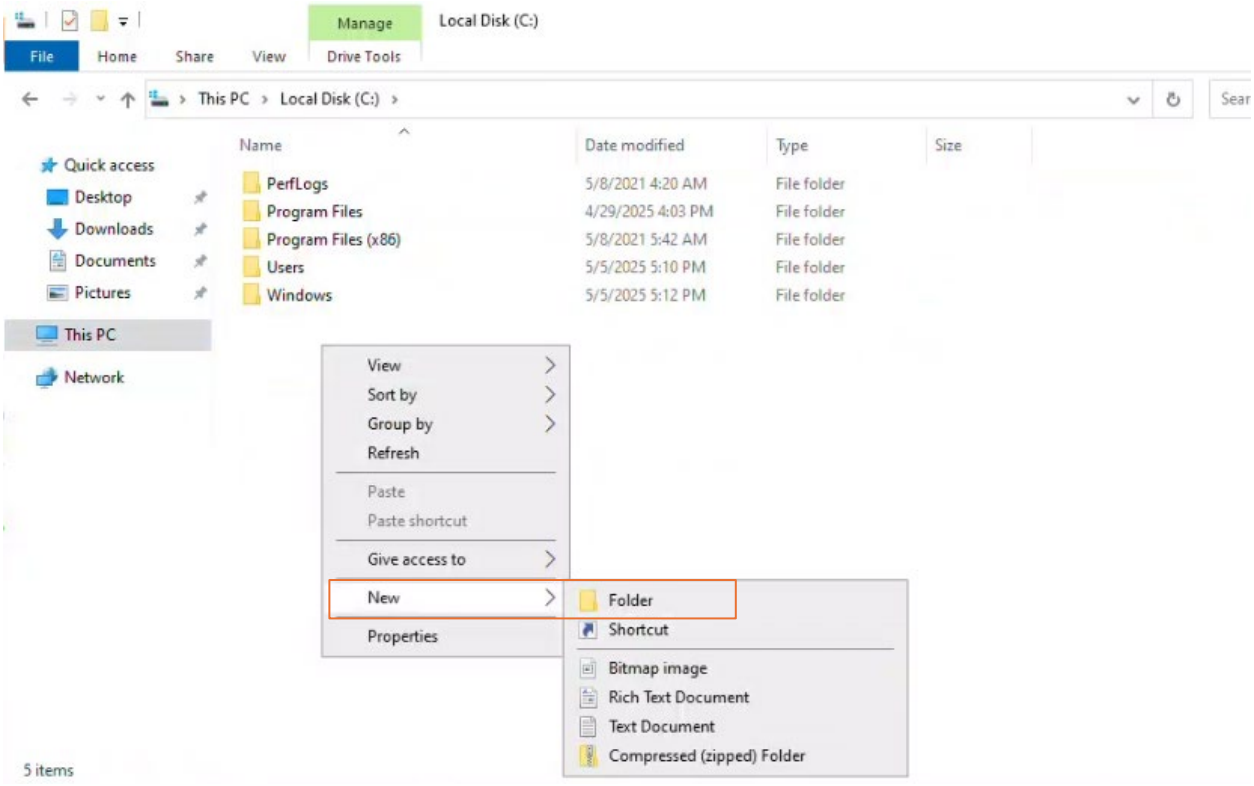
Redirect Documents and Desktop to the user's respective folder under \\DC312\UserData

Link GPO to HR OU

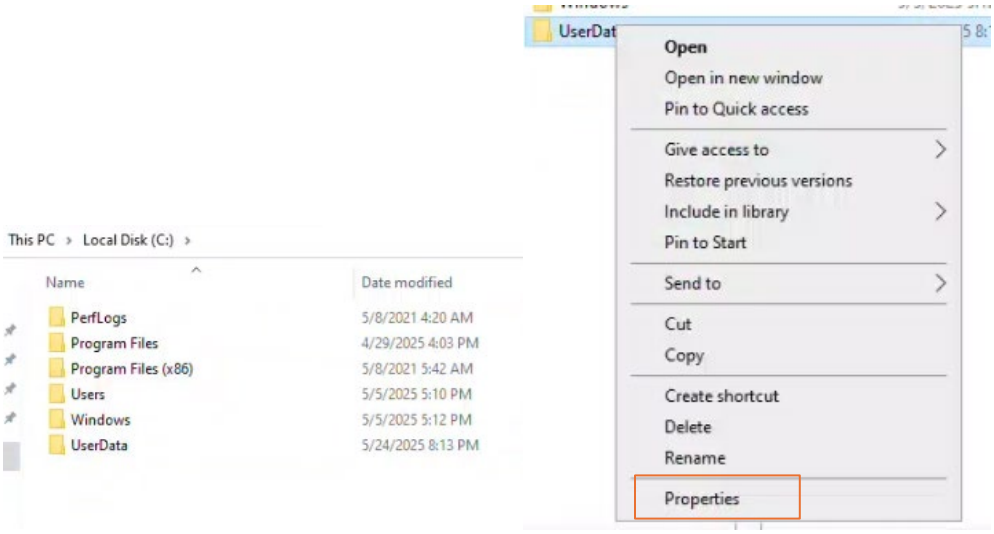
Run gpupdate /force to apply changes

Test with a user from the HR OU.

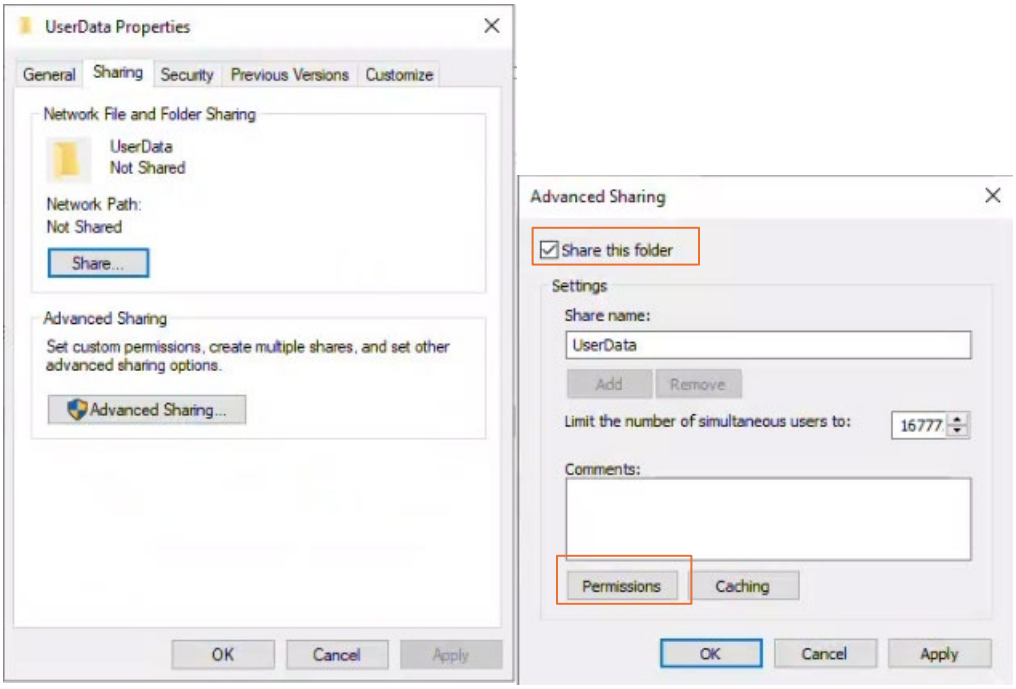
On DC312, create the folder UserData on the C: drive



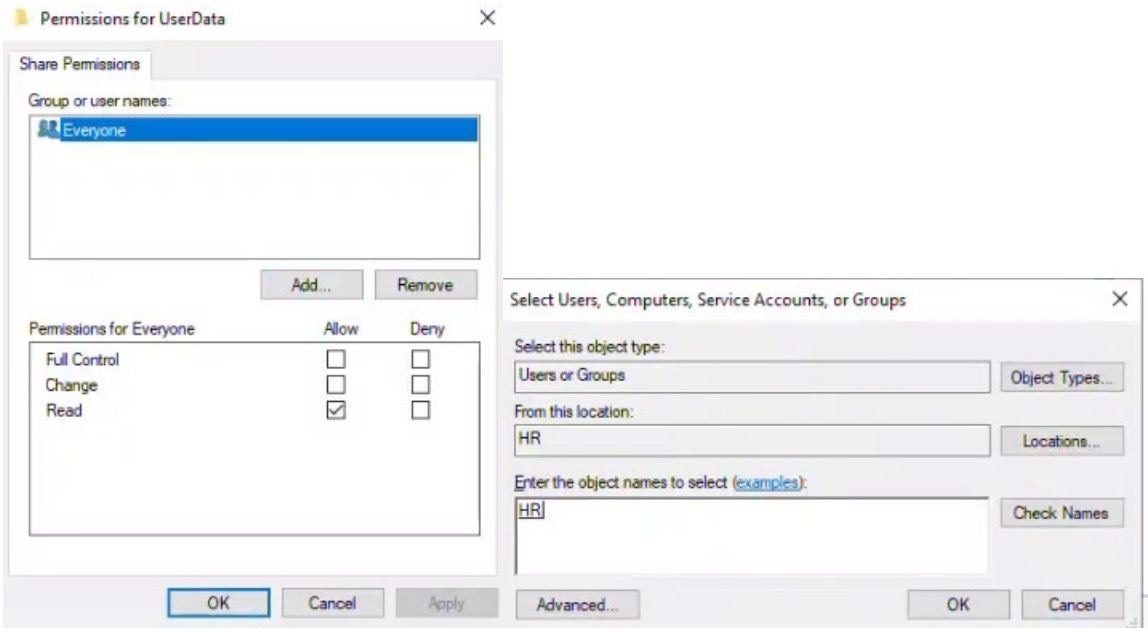
Right-click and go to Properties



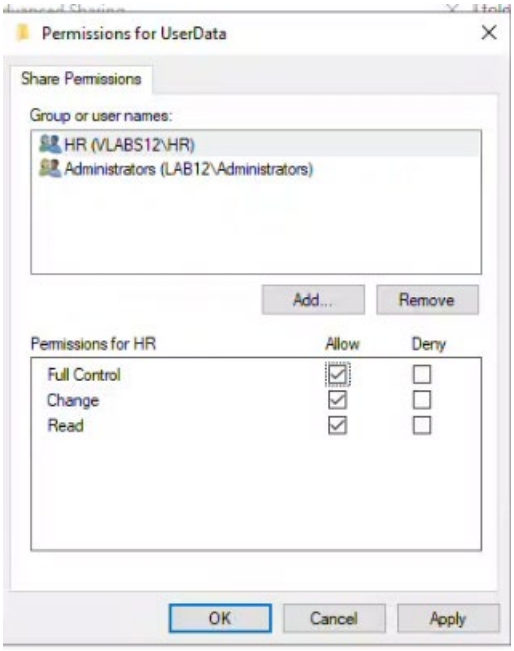
Go to Advanced Sharing → tick the box Share this folder. Next, go to Permissions



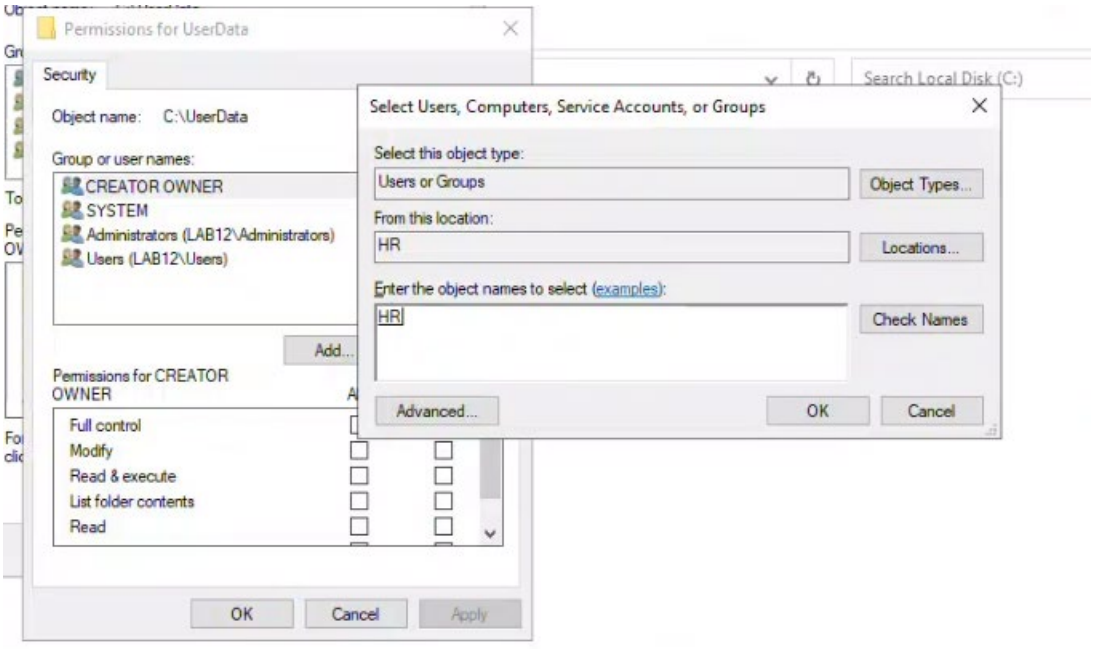
Remove “Everyone” and click on Add, add HR



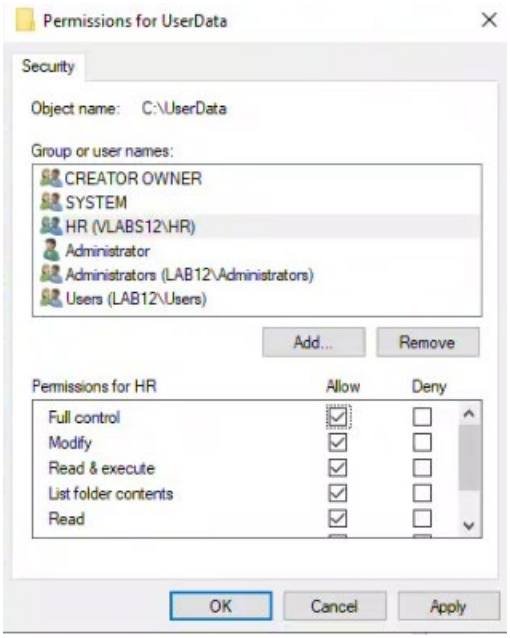
Grant them full control



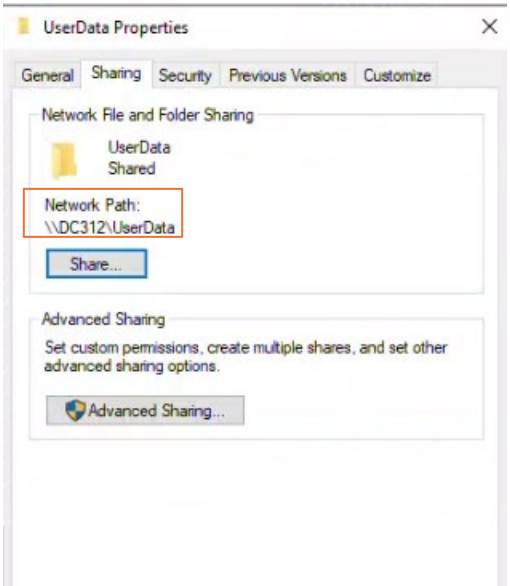
Next, go to Security to set the NTFS permissions



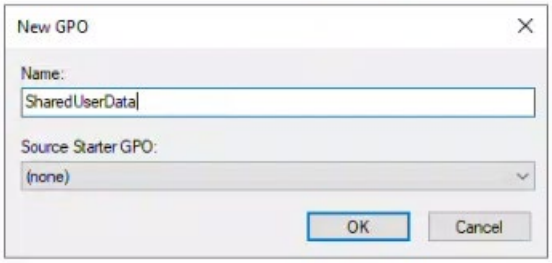
Ensure that HR has full control permissions



Verify the path



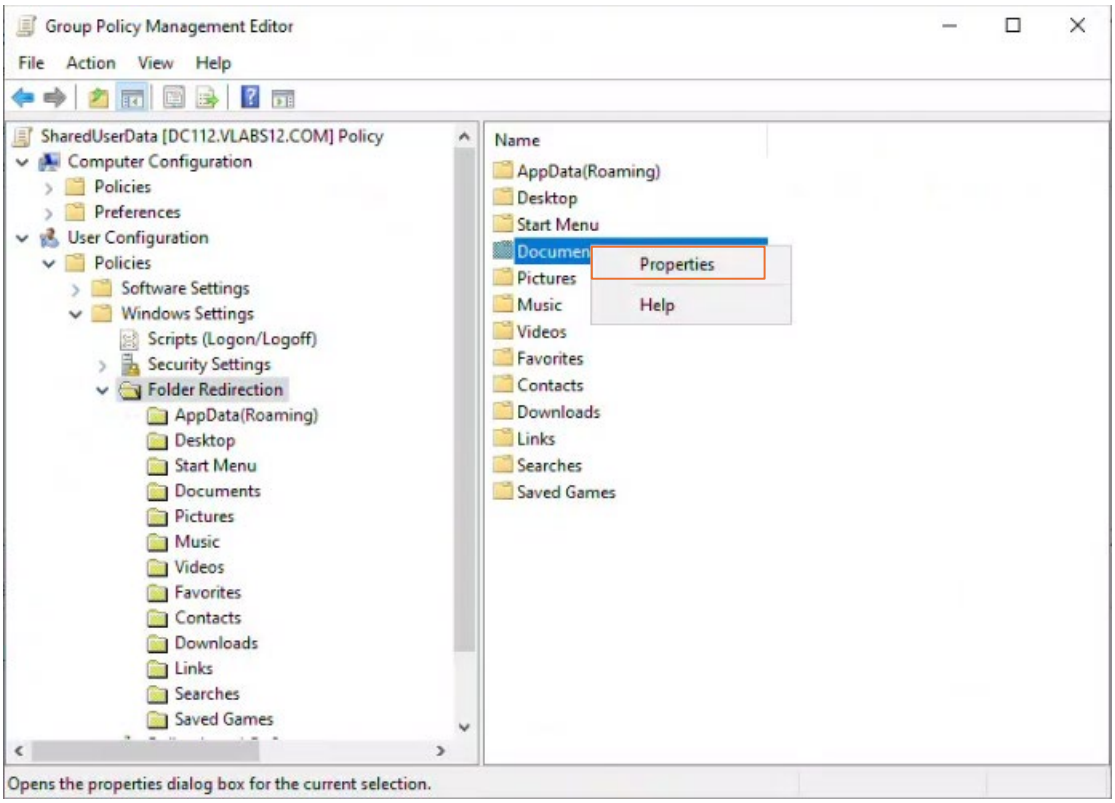
Next, create the GPO on DC112 and name it SharedUserData



Right click on the GPO → Edit

Go to User Configuration → Policies → Windows Settings → Folder Redirection

Right click on Document → Properties

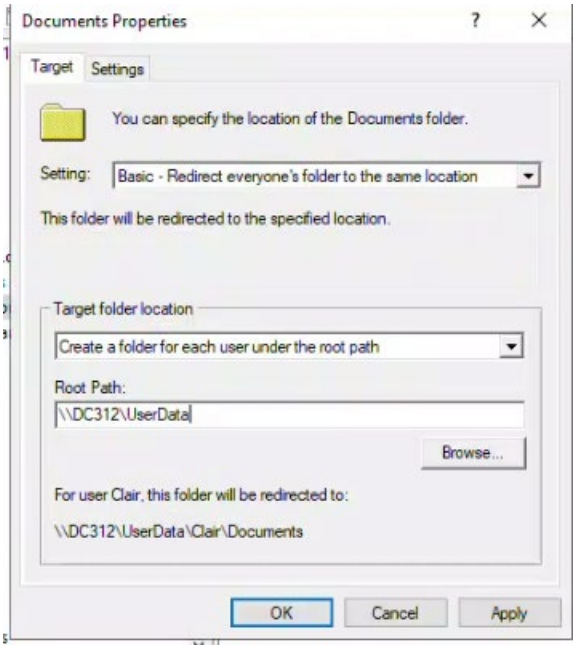


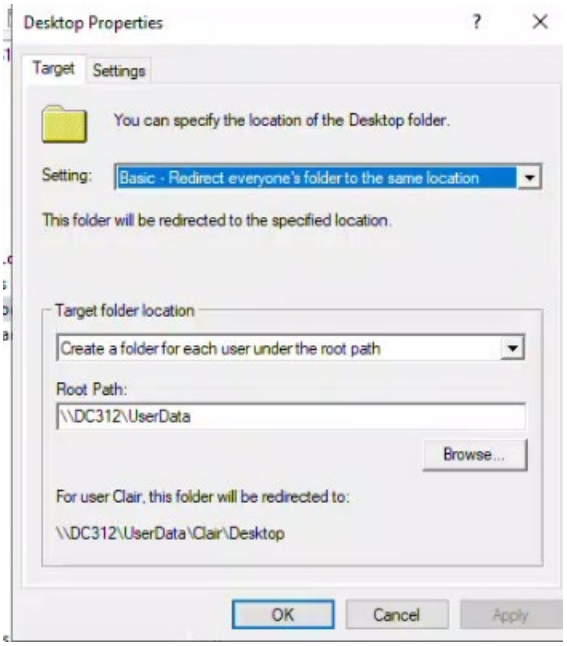
Setting: Basic

Target folder location: create a folder for each user under the root path

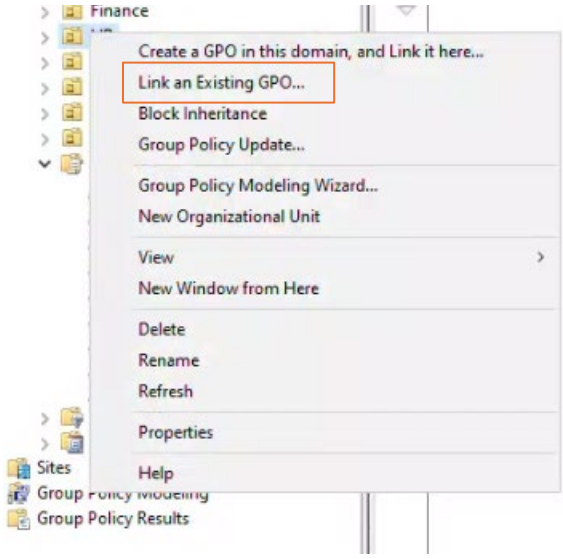
Root path: \\DC312\UserData

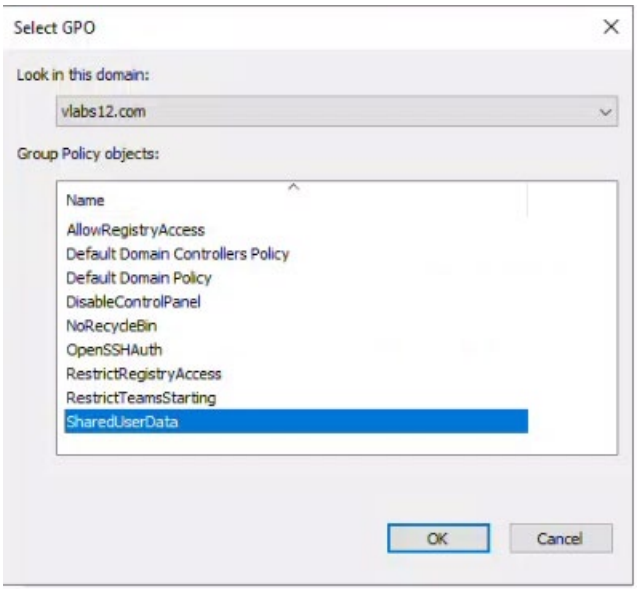
Repeat for Desktop





Link the GPO to HR OU

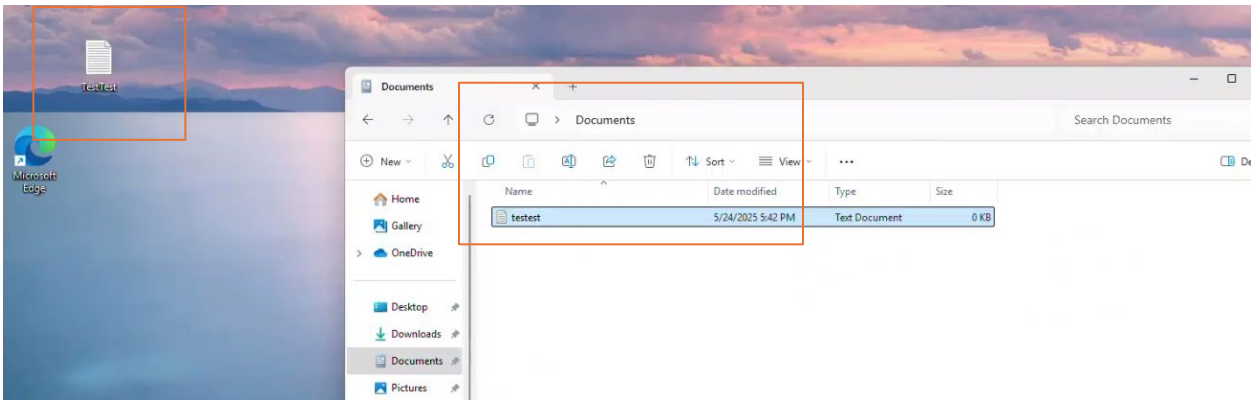




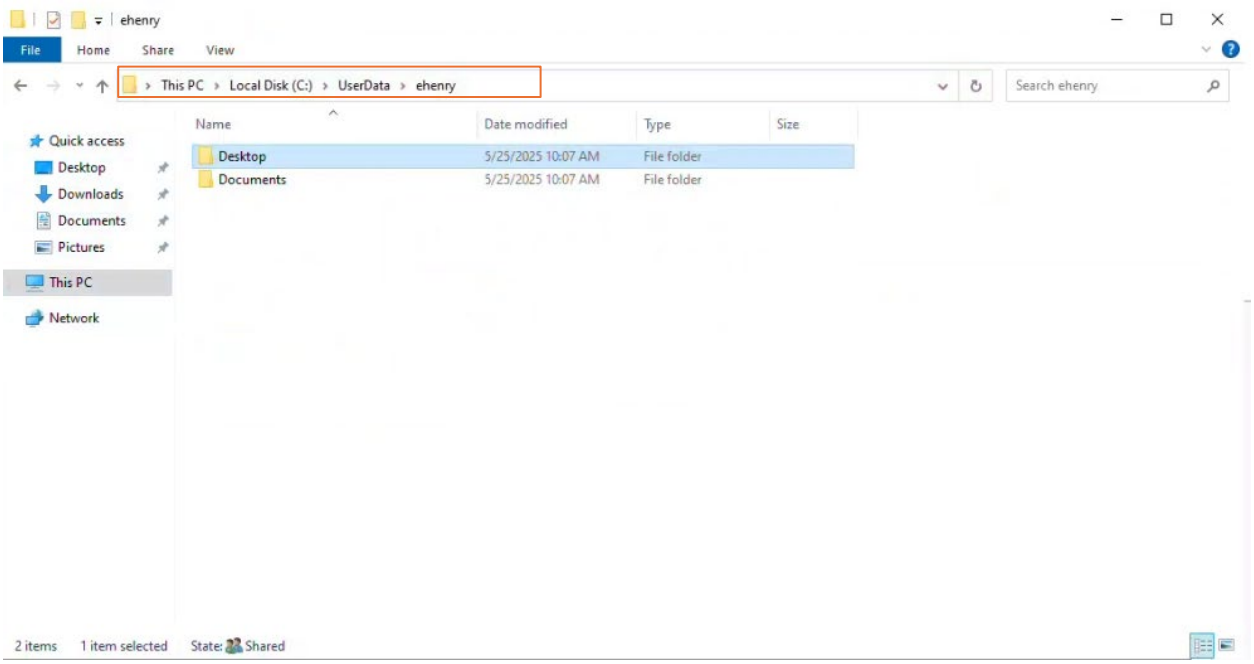
Do gpupdate /force on both DC112 and client12

```
PS C:\Users\Administrator.DC112> gpupdate /force
Updating policy...

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

PS C:\Users\Administrator.DC112>
```

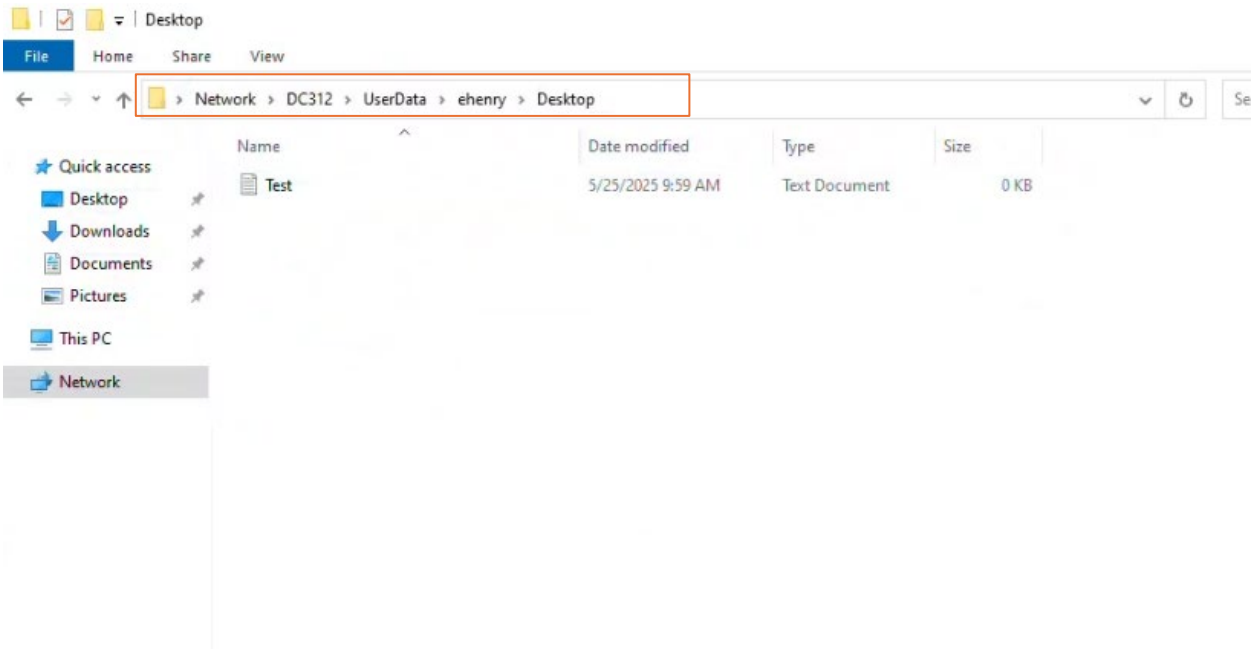
Create files in Desktop and Documents signed in to Client12 as a HR user

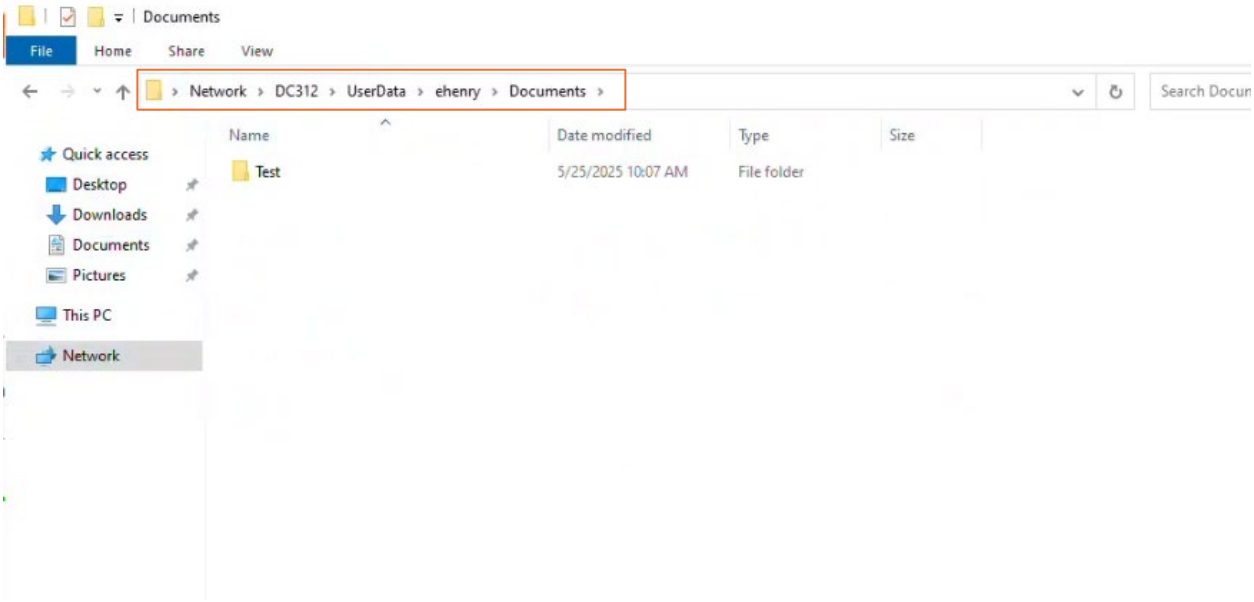


On DC312, verify that the user Elise Henry's folder has been created



Verify that you can see the files





Task 8: Managing Software Installation

Create a network share: \\DC312\Software.

Download the Microsoft Teams MSI package (You will need to add the NAT NIC to download this package. Remove it after completing the download).
https://learn.microsoft.com/en-us/microsoftteams/msi deployment#msi-files

Create a new GPO named **DC312_Teams_Installation.**

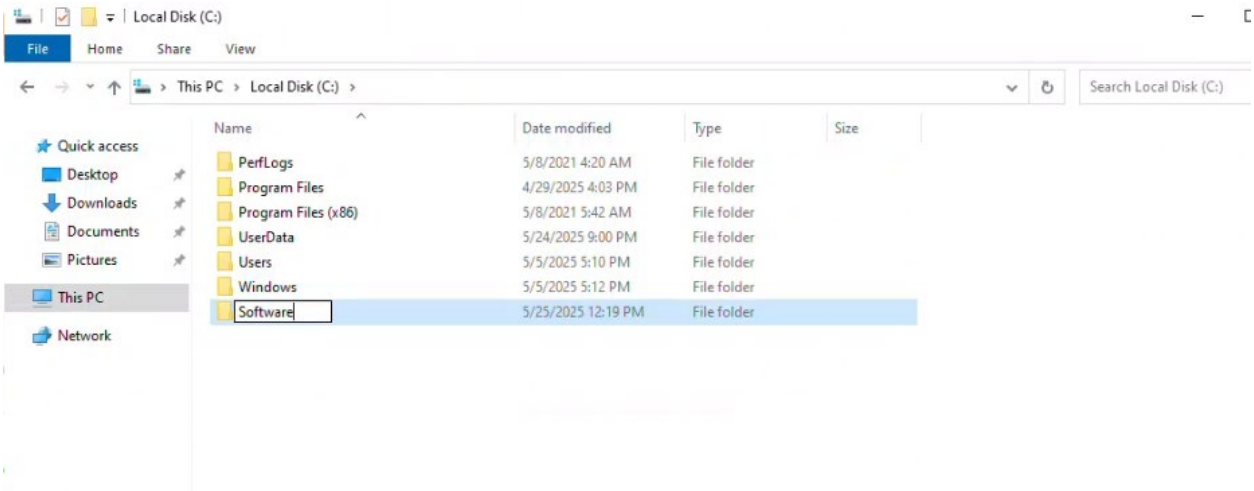
Assign the Teams MSI package installation to the **Engineering OU.**

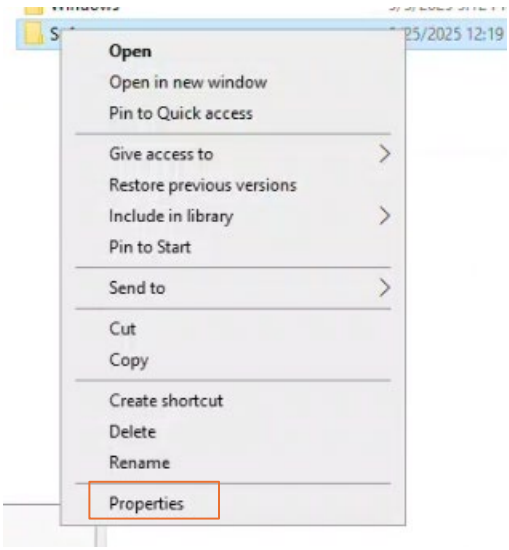
Run gpupdate /force to apply changes.

Restart Client12, log in with a user from Engineering OU, and verify that Microsoft Teams is installed.

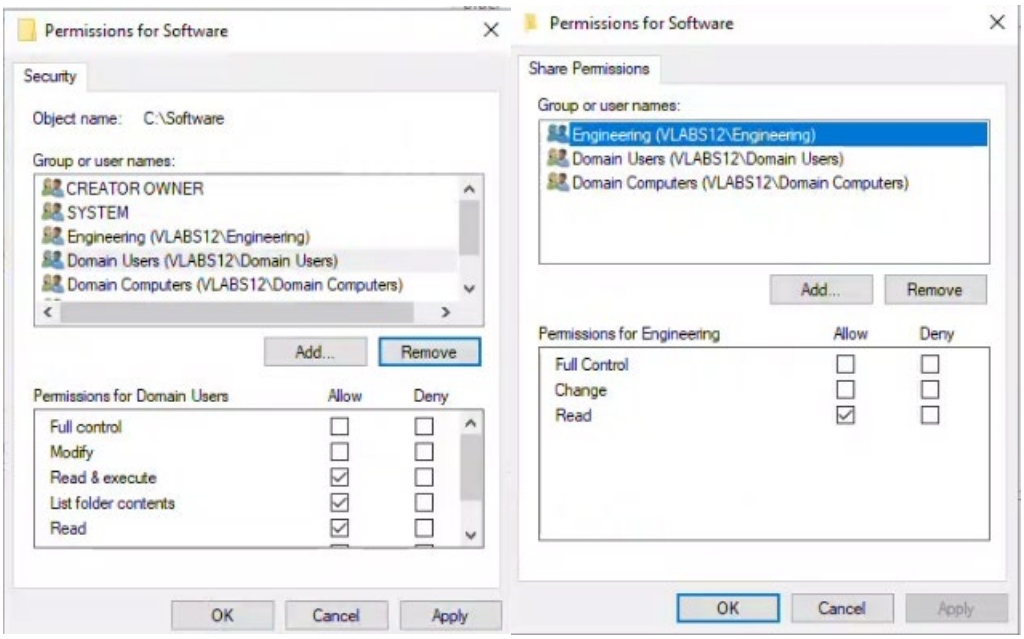
Confirm that Teams do not start automatically after installation (to test GPO RestrictTeamsStarting, created in Task 2).

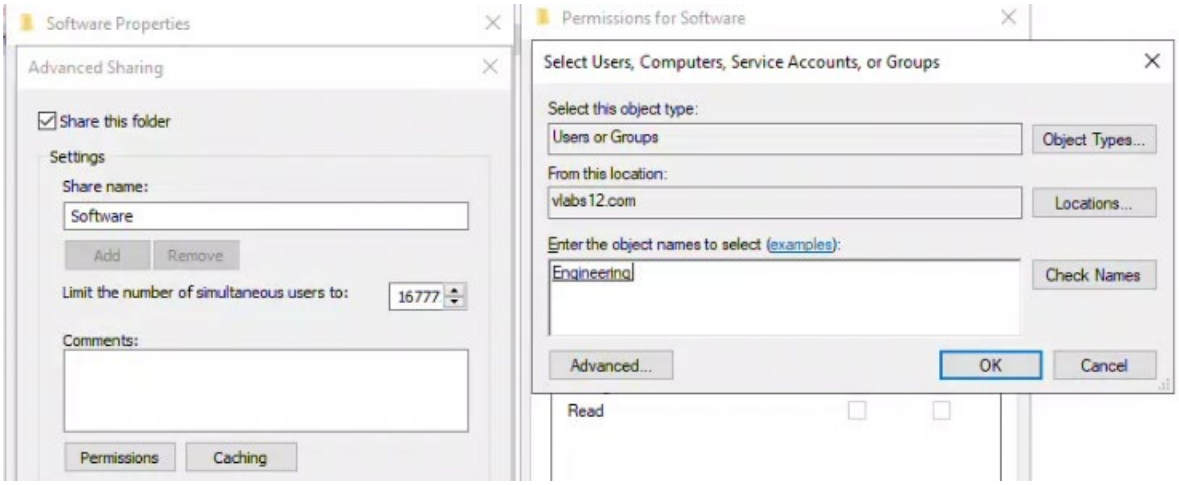
On DC312, create the shared folder Software



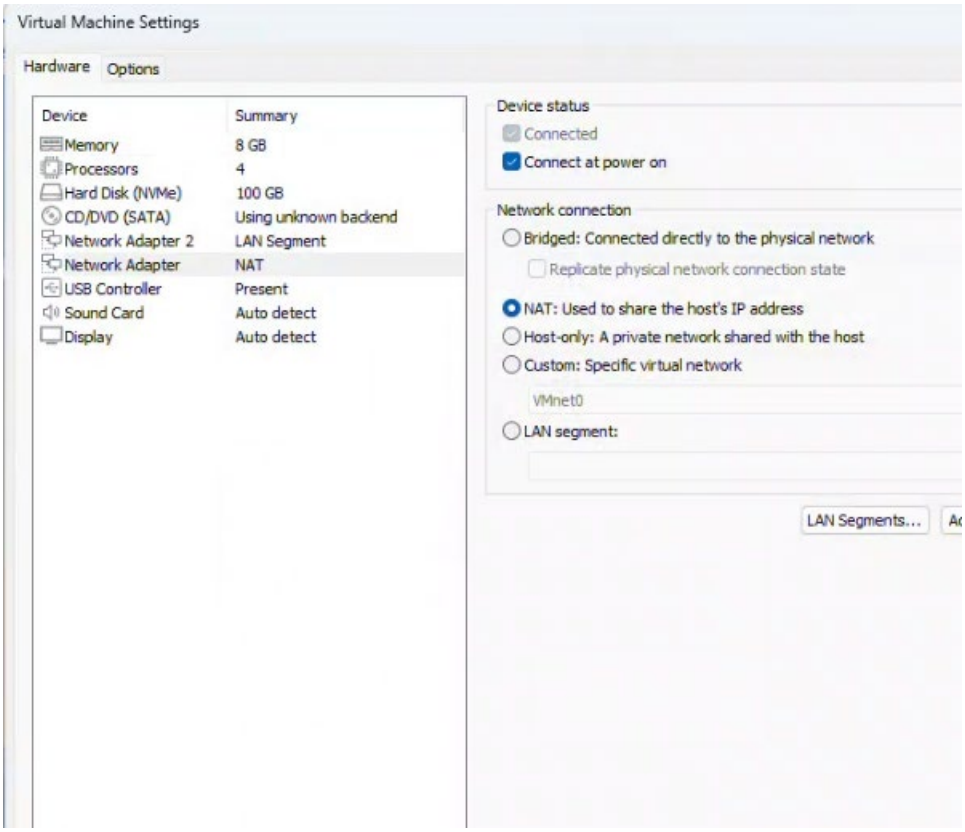


Set it to share and set the appropriate permissions for both share and NTFS

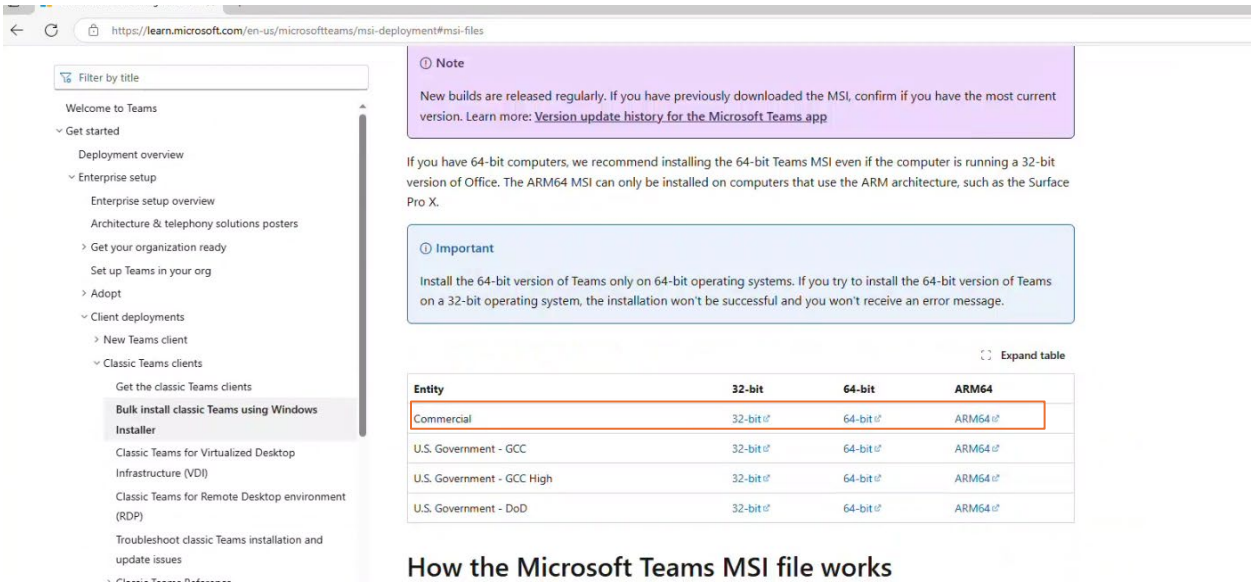




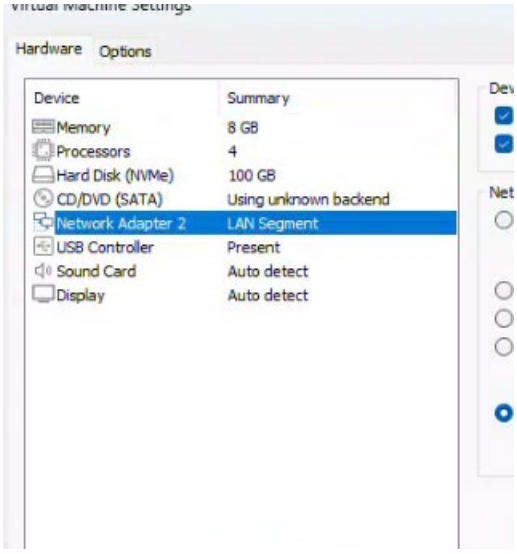
Install a network adapter temporarily (NAT) so that we can download the Teams MSI package



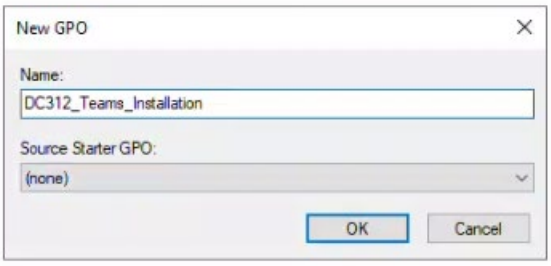
Go to the link and download the Teams MSI package (64-bit)



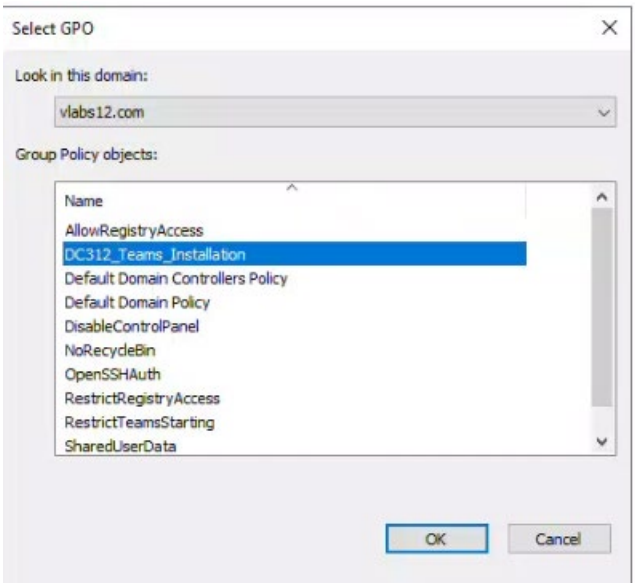
Once downloaded, remove the network adapter.



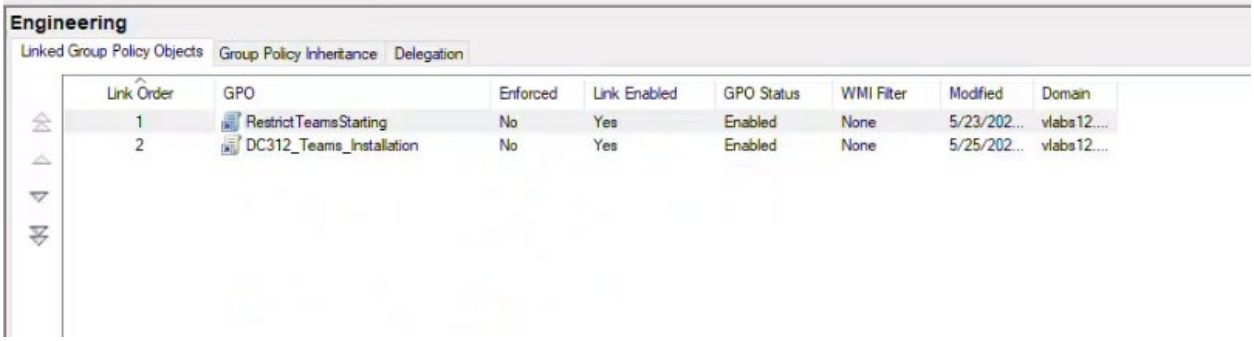
Create the GPO “DC312_Teams_Installation”



Link it to Engineering OU

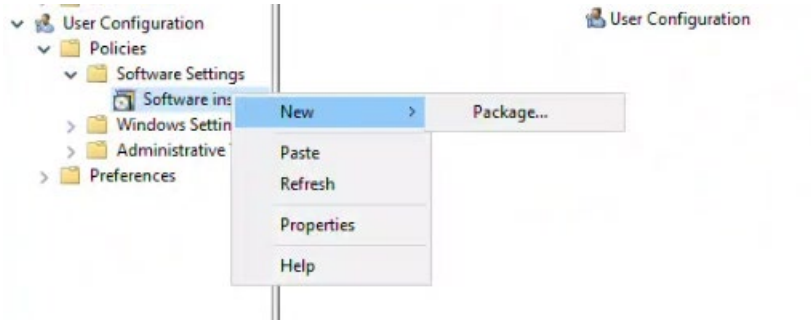


Below you see the two GPOs that go hand in hand. RestrictTeamsStarting is configured to prevent Teams from starting automatically at sign-on and Teams_Installation installs Teams automatically in the background without prompt.

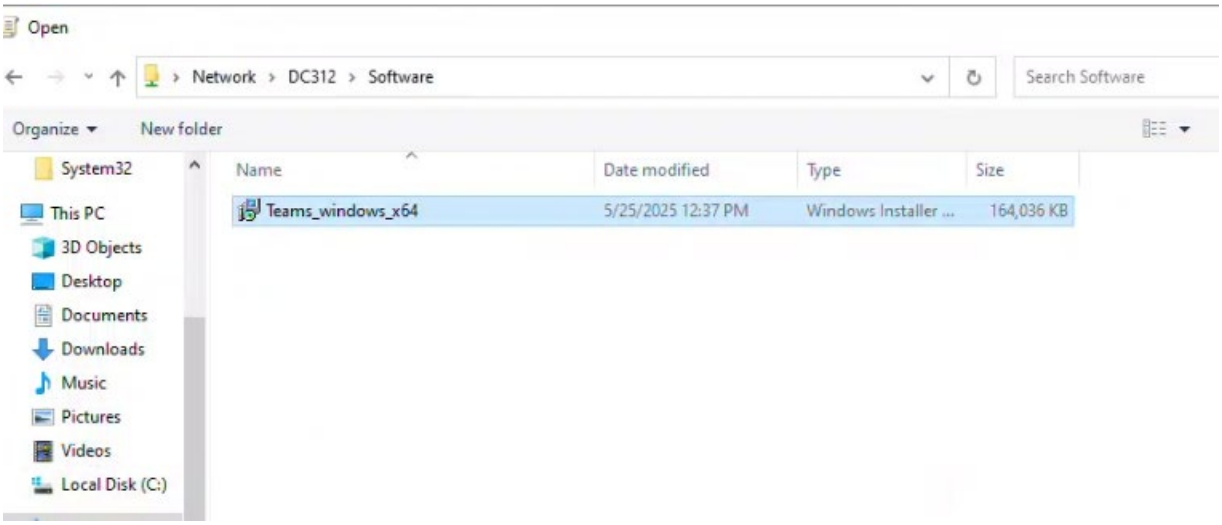


Right-click on the new GPO → Edit → User Configuration → Policies → Software Settings

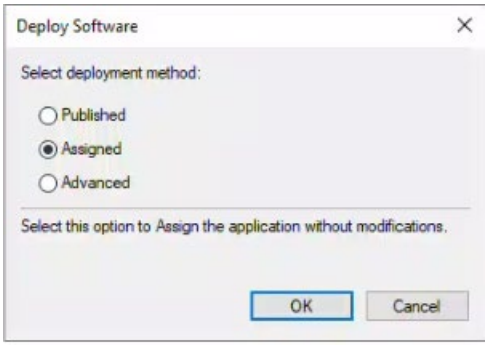
Right click on software installation and go to New → Package



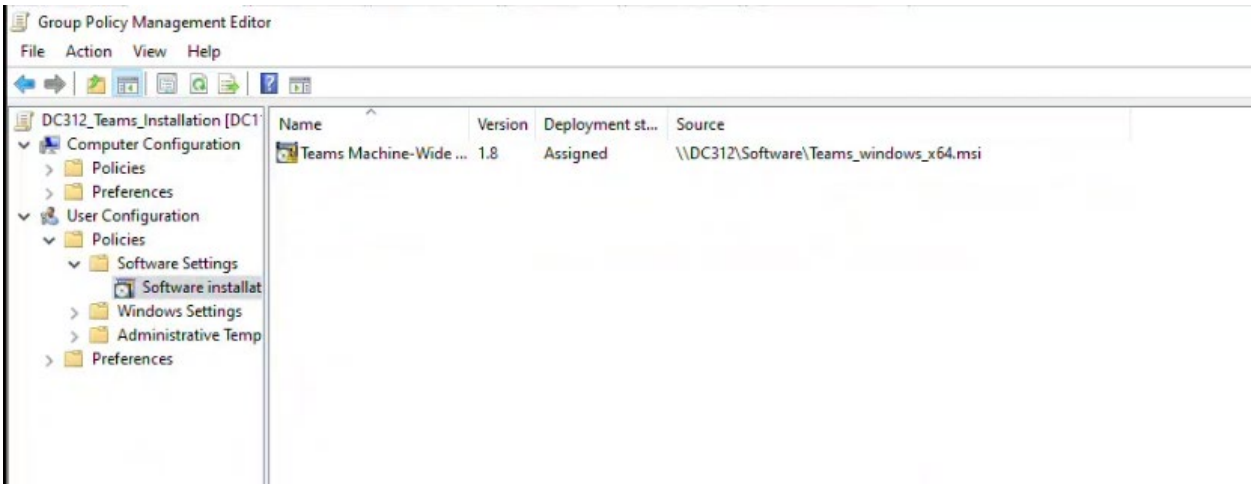
Here you'll select the Teams package we downloaded and placed in the shared Software folder (not documented)



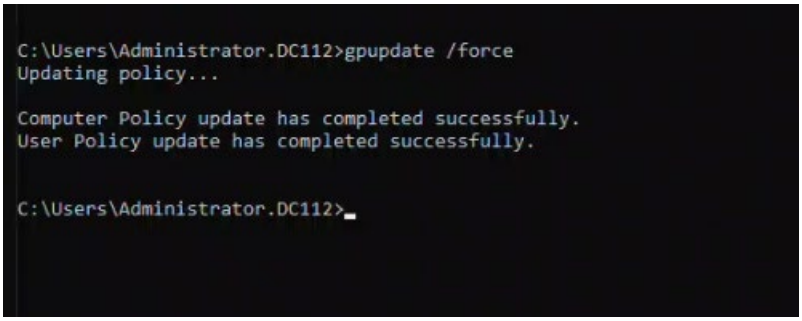
Select "assigned"



Wait a few seconds and you'll see the installation appear under software installation with the path to the package (DC312)



Do a gpupdate /force

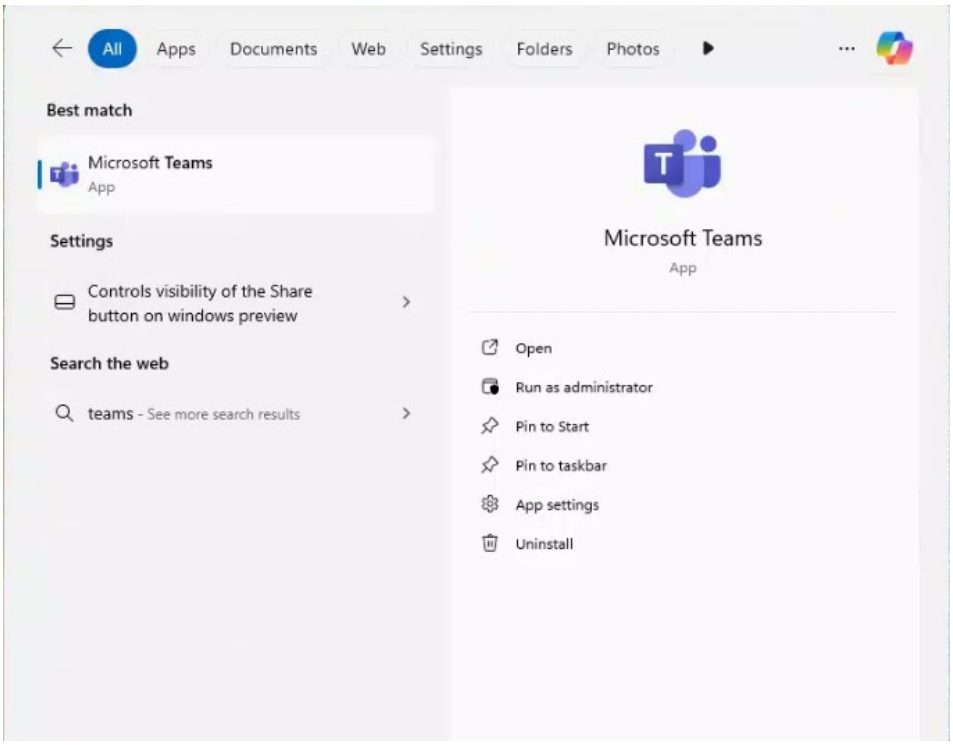


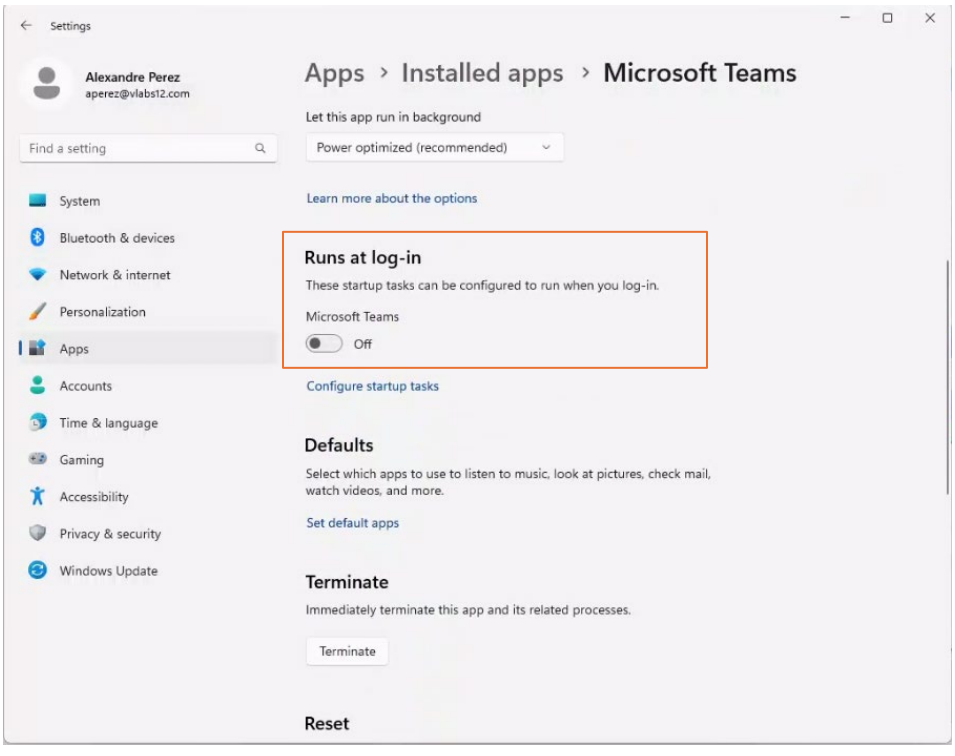
On Client12, sign in to a user from Engineering. I chose Alexandre Perez (aperez)

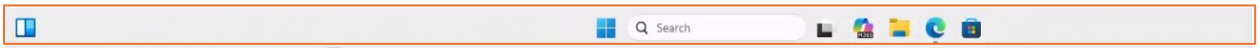
Using the search bar, look up teams to see if it's installed. It's supposed to be due to the GPO we just created.

Also verify that Teams is not running at log-in (the first GPO we created). I couldn't really think of a good way to prove this except for going in app settings and verifying

that it’s set to not run at log-in, also verifying the task bar for Teams running. It was not.







Task 9: Managing Scripts with GPO

Create a shared folder on \\DC312\Public and share it with Everyone (read and write).

Create a logon script (MapDrive.bat) to map this shared network drive. Add this text in this file: net use Z: \\DC312\Public

Store the script in \\DC112\NETLOGON.

Create a new GPO named Public_Share.

Add this new logon script to User Configuration Scripts → Logon.

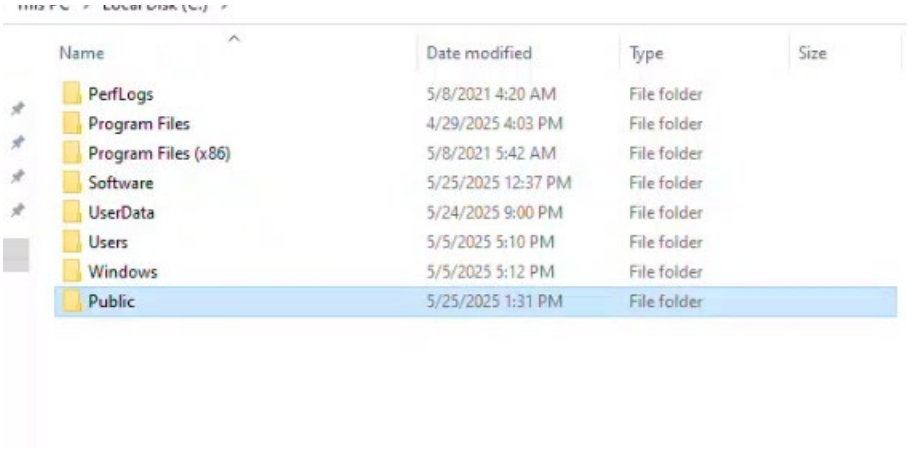
Link GPO to the Domain.

Run gpupdate /force to apply changes.

Test with any by logging into Client12 and verifying the drive mapping.

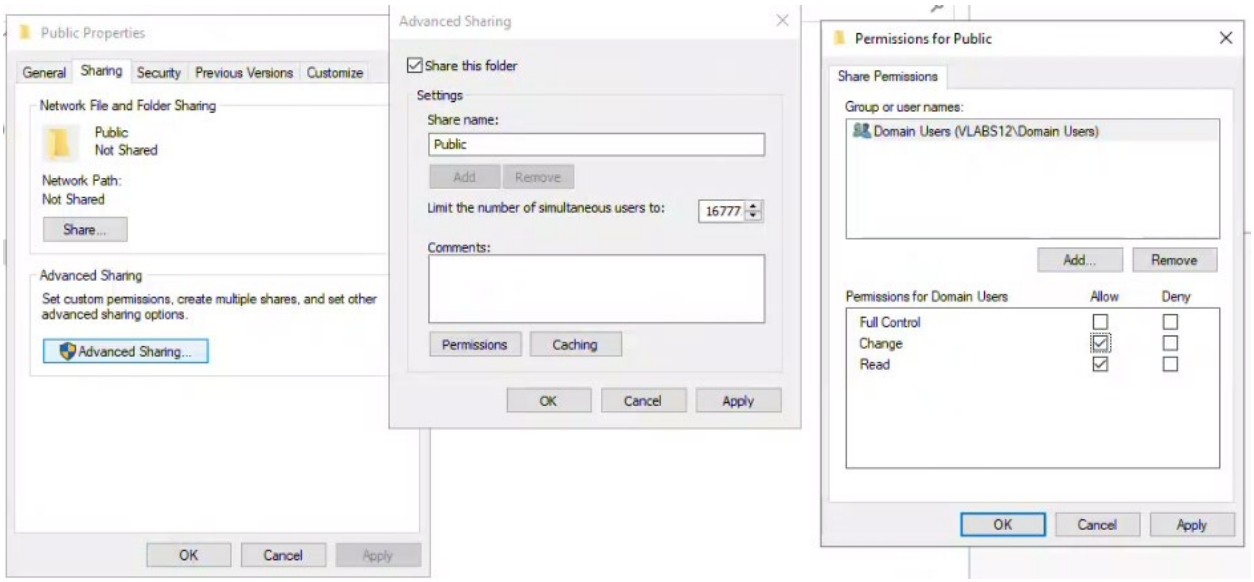
Try to create files and folders in this drive.

On DC312, create the shared folder Public

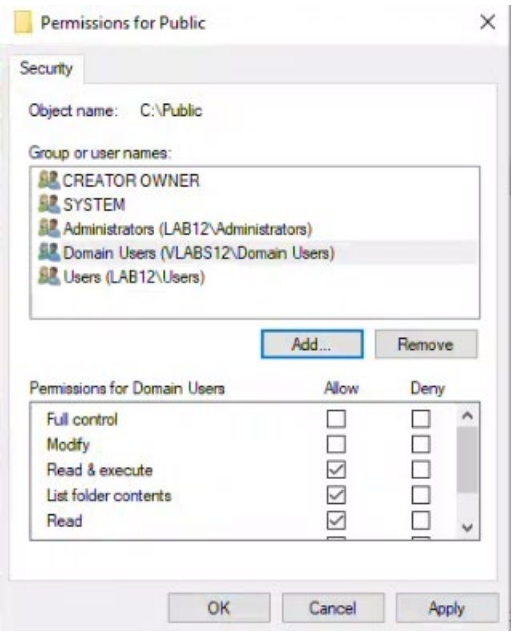


Go to Properties → Sharing

Set the permissions for Domain Users and share the folder



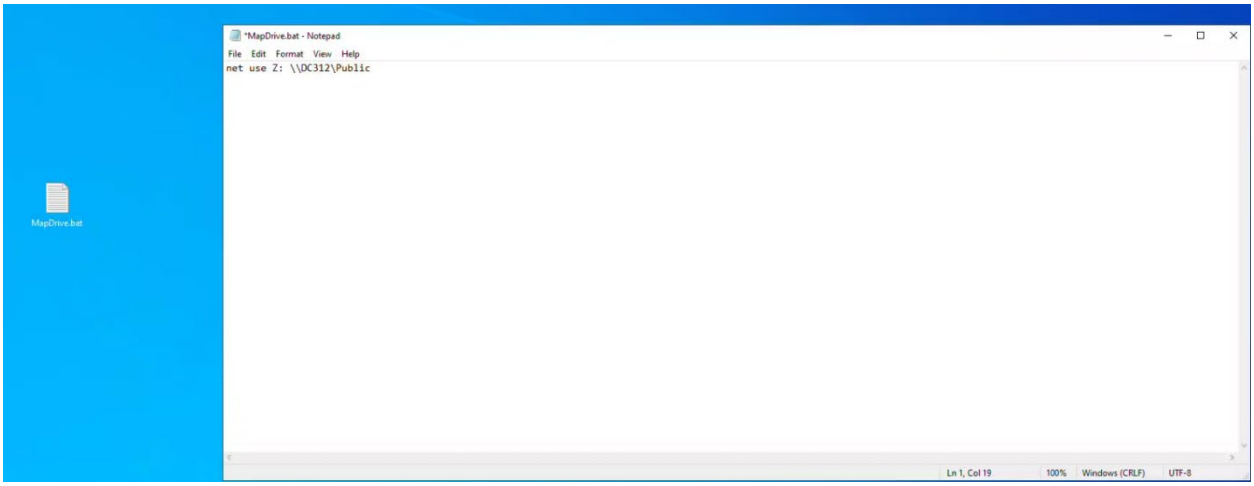
Set the permissions for Domain Users for NTFS

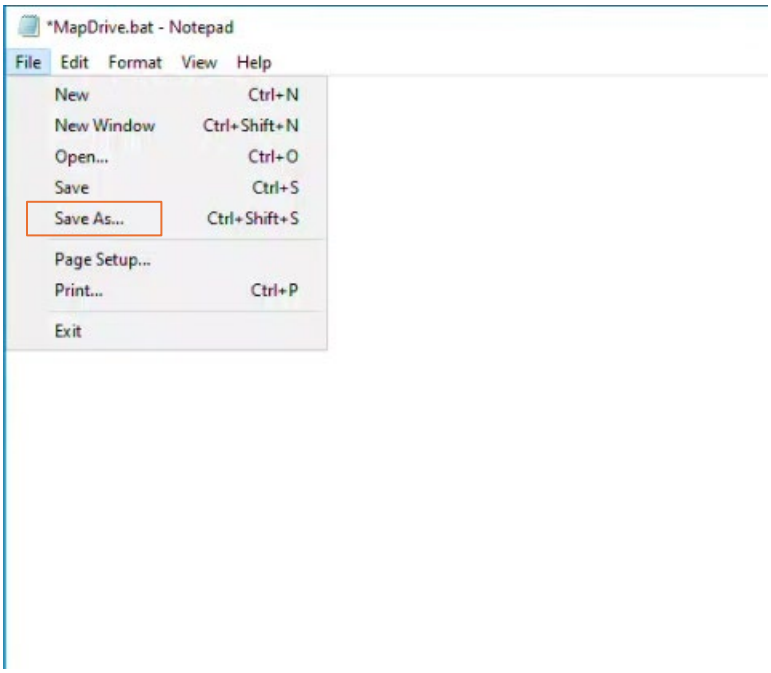


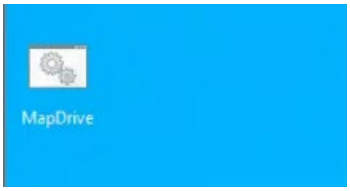
Open Notepad and enter “net use Z: \\DC312\Public”

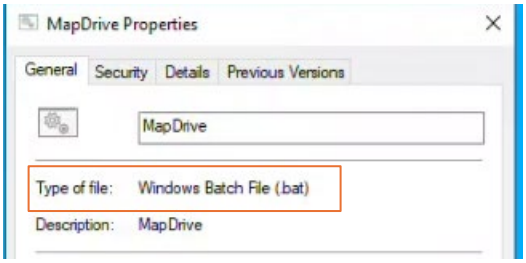
Go to File → Save as.. → and use the drop down menu to select “All files”. Save the file as “MapDrive.bat”

You’ll see it convert to a .bat file once saved.

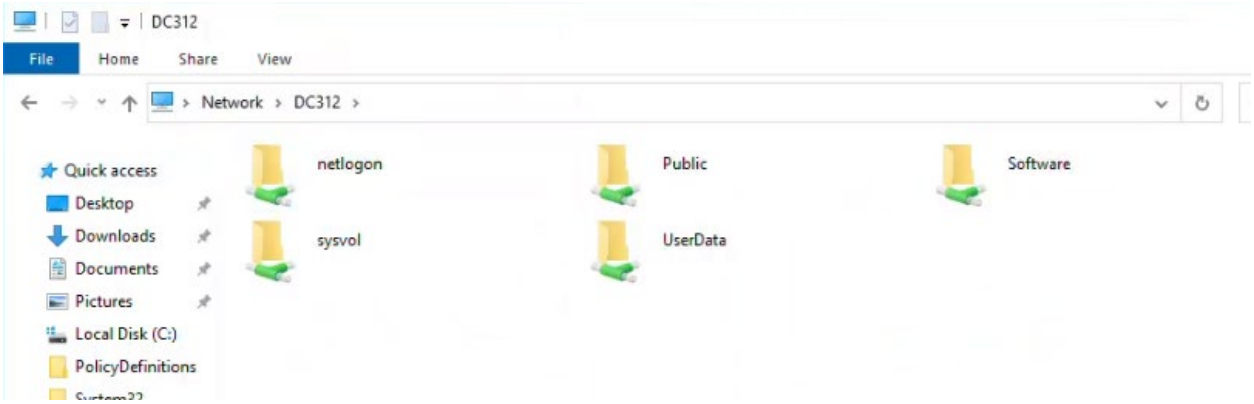


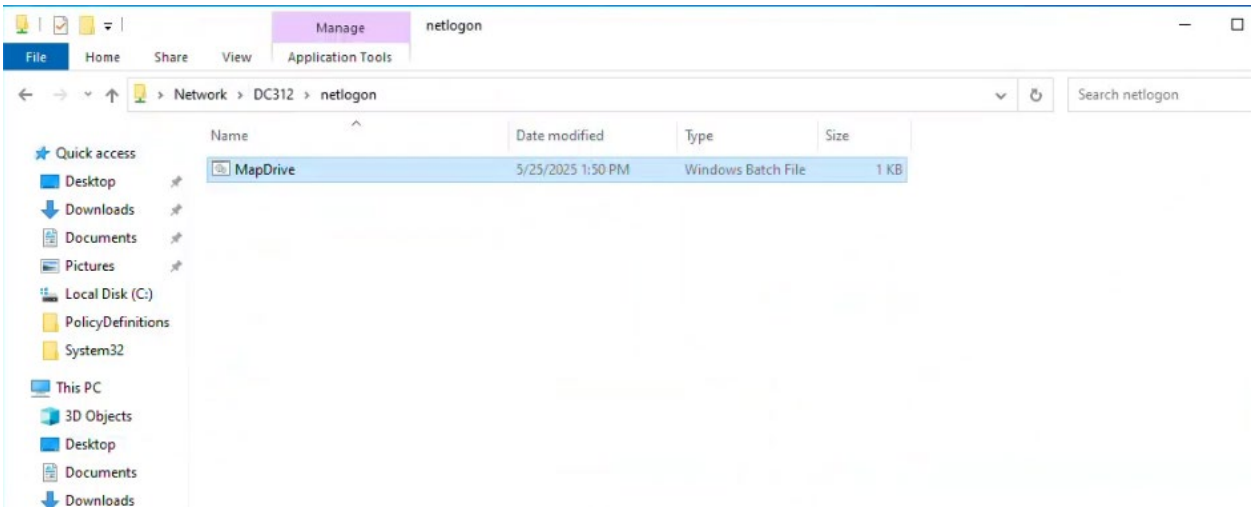




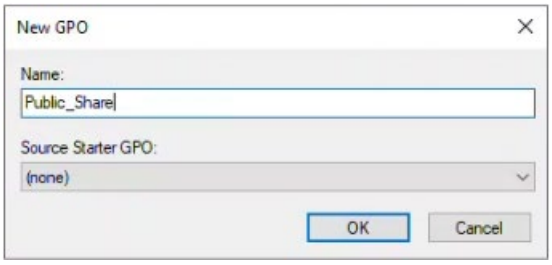


Place the file in the NETLOGON on the Public share





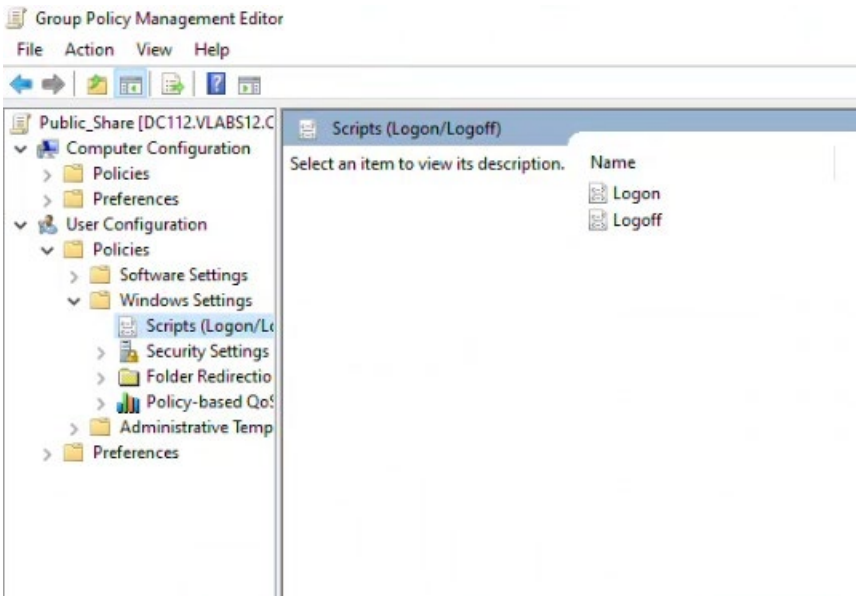
Create a new GPO and name it Public_Share



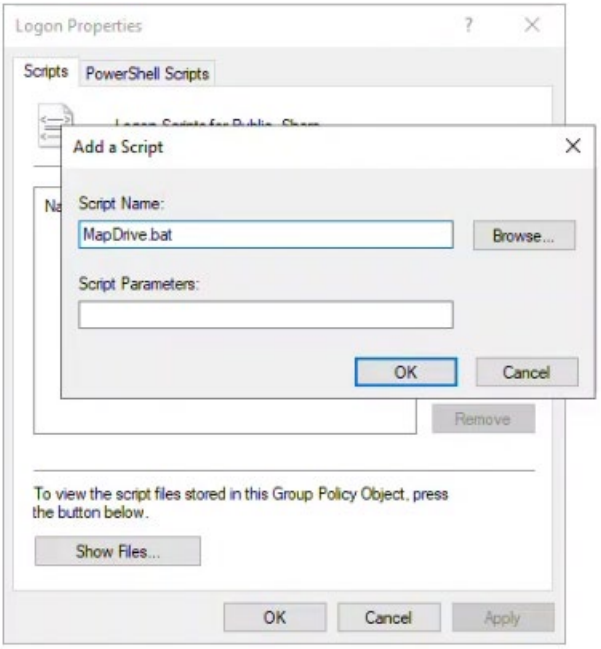
Right click on the GPO Public_Share and go to Edit

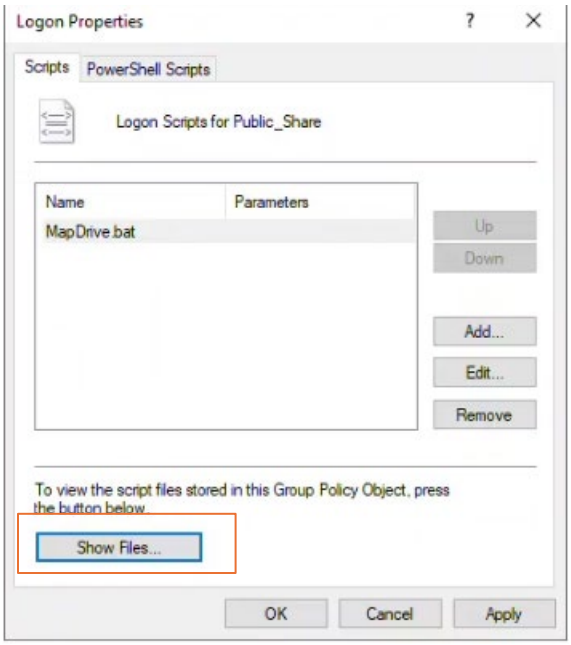
Under User configurations → Policies → Windows settings, right click on Scripts.

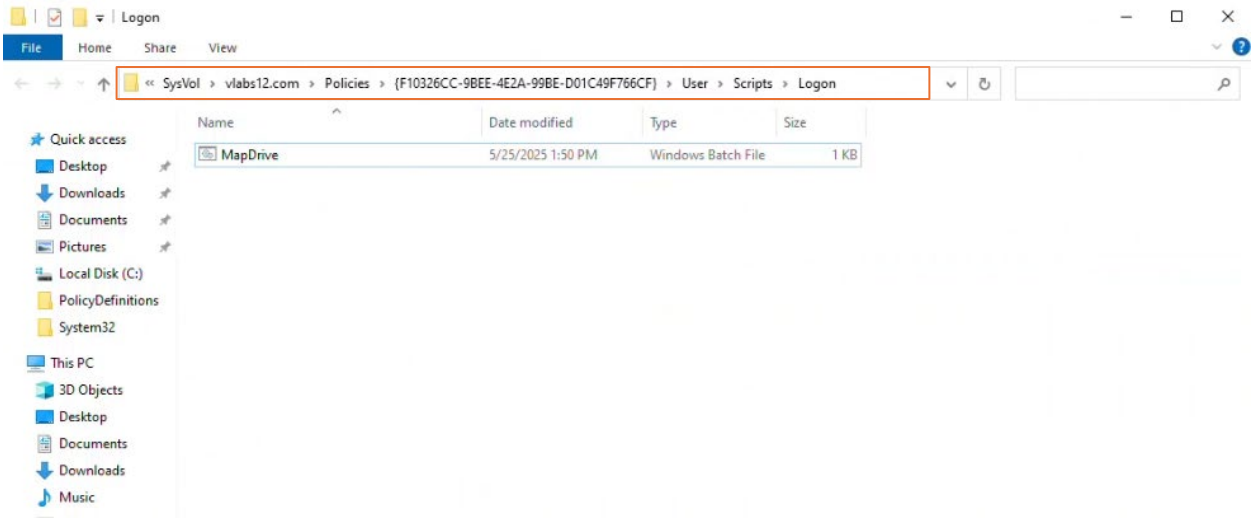
Open “logon”



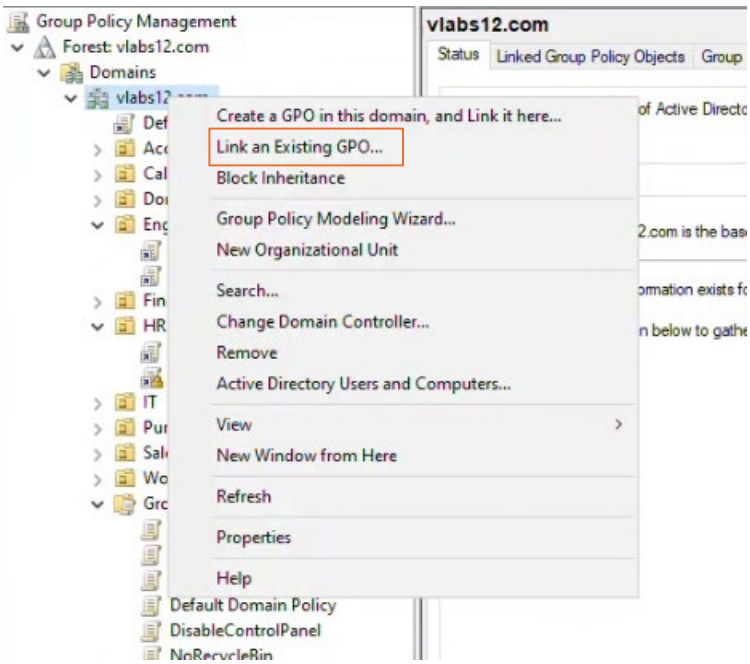
Click on “Add” and enter MapDrive.bat. It should use the correct path. Verify by clicking on Show Files afterwards

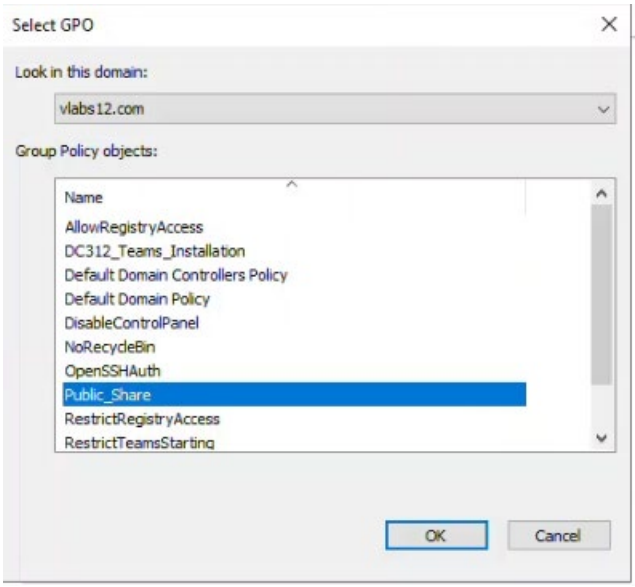


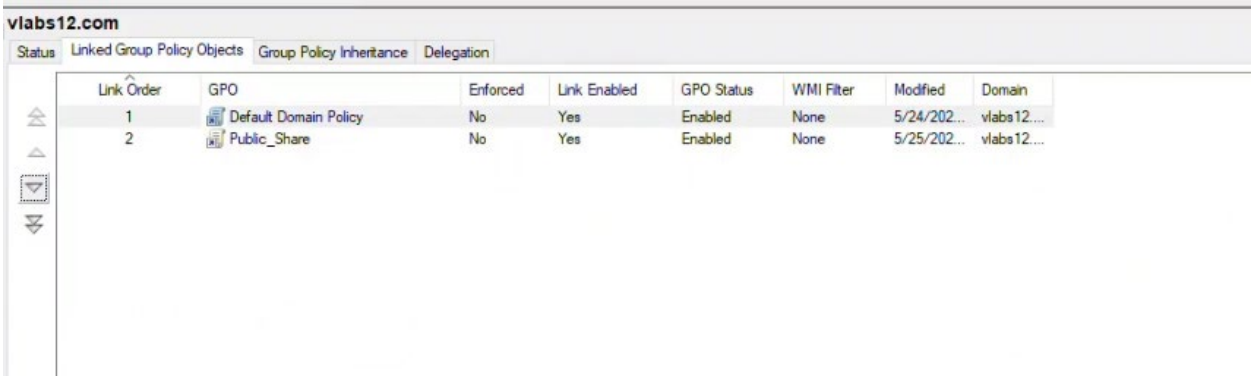




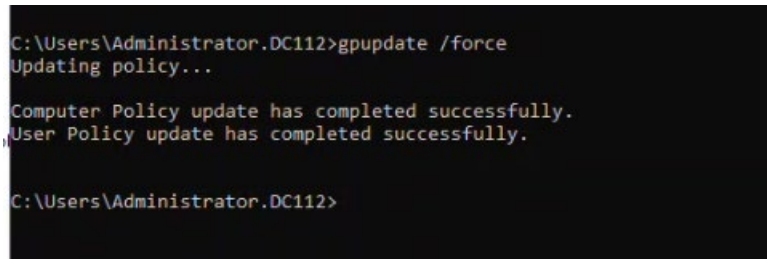
Link the GPO to the domain


Group Policy Management
Forest: vlabs12.com
Domains
vlabs12.com
Status
Linked Group Policy Objects
Group
Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance
Group Policy Modeling Wizard...
New Organizational Unit
Search...
Change Domain Controller...
Remove
Active Directory Users and Computers...
View
New Window from Here
Refresh
Properties
Help
Default Domain Policy
DisableControlPanel

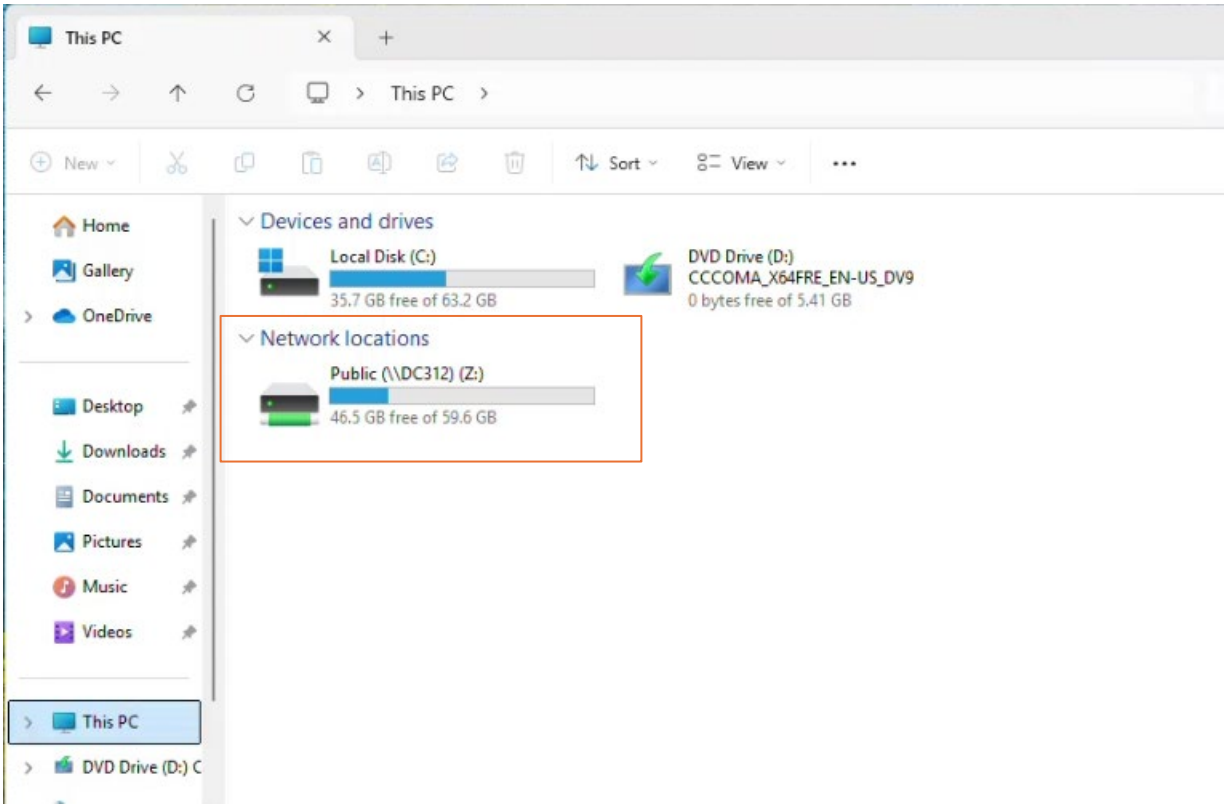

Select GPO
Look in this domain:
vlabs12.com
Group Policy objects:
Name
AllowRegistryAccess
DC312_Teams_Installation
Default Domain Controllers Policy
Default Domain Policy
DisableControlPanel
NoRecycleBin
OpenSSHAuth
Public_Share
RestrictRegistryAccess
RestrictTeamsStarting
OK
Cancel


vlabs12.com
Status
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO Status
WMI Filter
Modified
Domain
1
Default Domain Policy
No
Yes
Enabled
None
5/24/202...
vlabs12....
2
Public_Share
No
Yes
Enabled
None
5/25/202...
vlabs12....

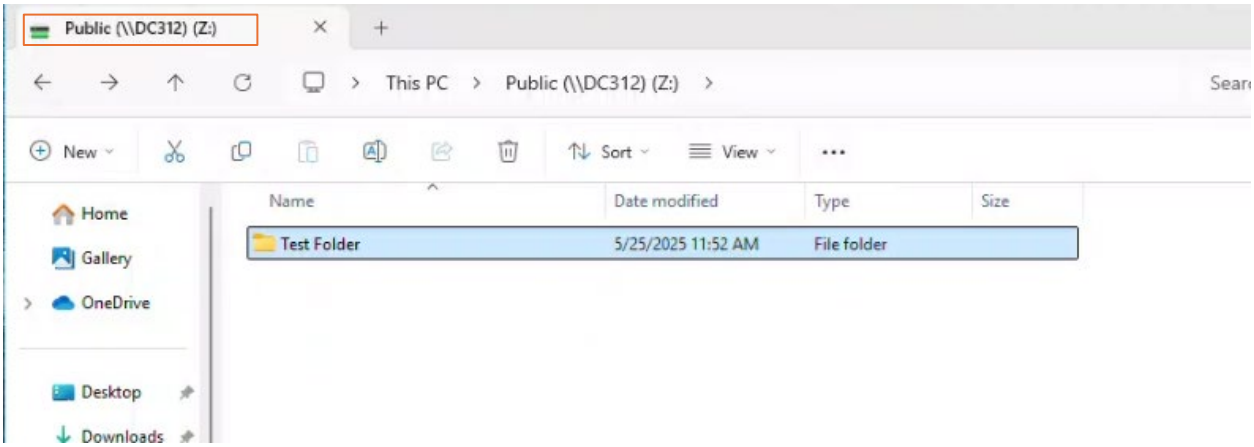
Do a gpupdate /force

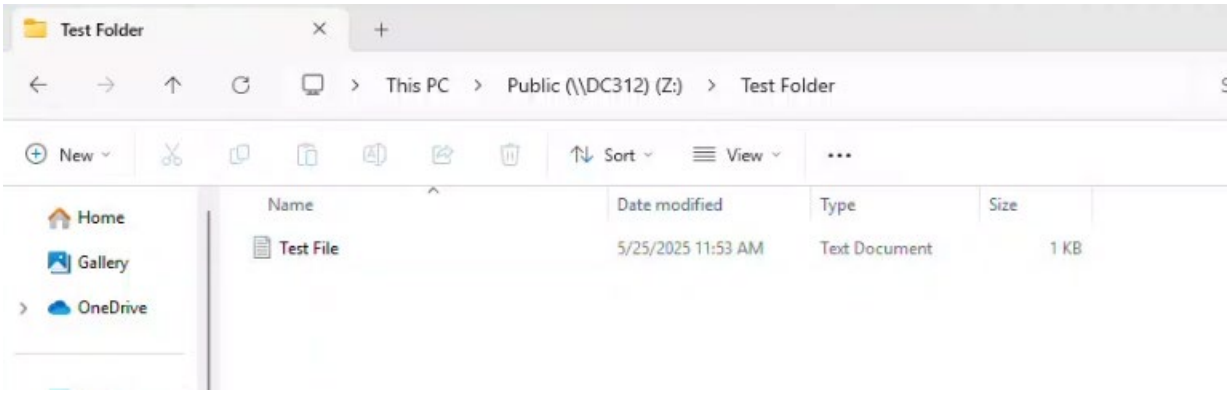


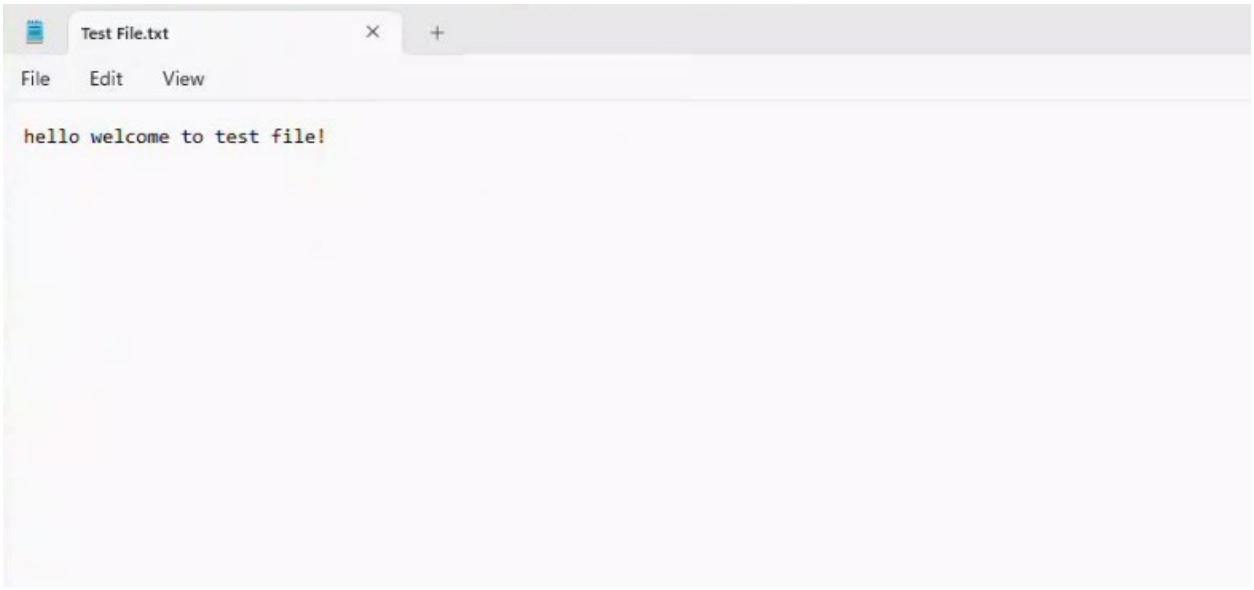
Log in to Client12 with any user and verify that you can see the shared folder **Public** mapped to **Z:**



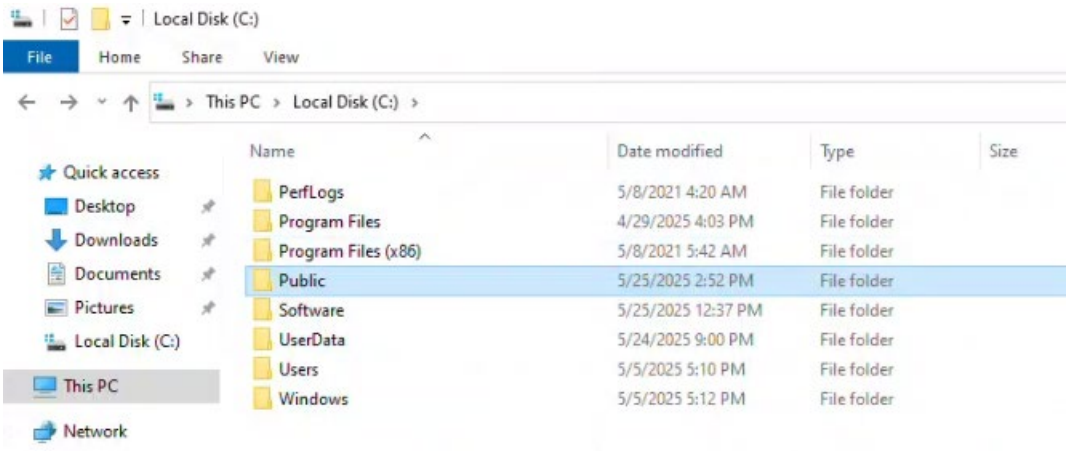
Create a test folder and file inside the folder

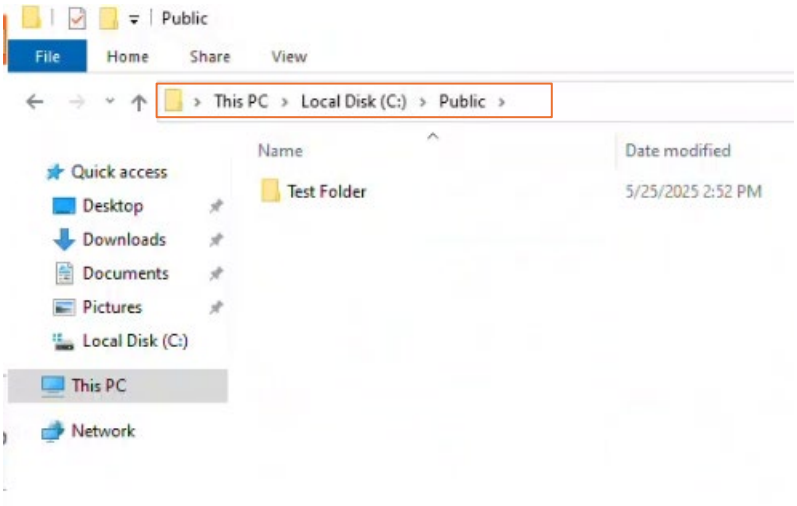

Public (\\DC312) (Z:)
This PC
Public (\\DC312) (Z:)
New
Sort
View
Home
Gallery
OneDrive
Desktop
Downloads
Name
Date modified
Type
Size
Test Folder
5/25/2025 11:52 AM
File folder

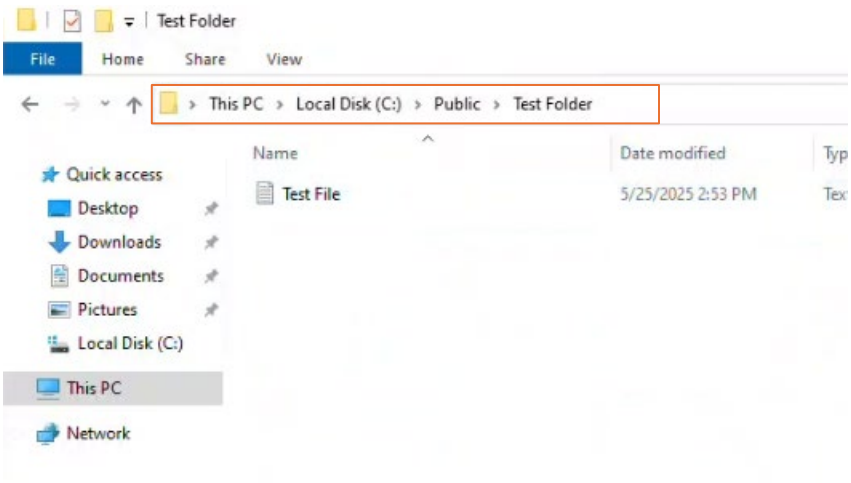

Test Folder
This PC
Public (\\DC312) (Z:)
Test Folder
New
Sort
View
Home
Gallery
OneDrive
Name
Date modified
Type
Size
Test File
5/25/2025 11:53 AM
Text Document
1 KB


Test File.txt
File
Edit
View
hello welcome to test file!

Verify on DC312 that the test folder/file are present in the share and that you can see the text written in the file from user aperez on Client12






Test Folder
File
Home
Share
View
This PC
Local Disk (C:)
Public
Test Folder
Quick access
Desktop
Downloads
Documents
Pictures
Local Disk (C:)
This PC
Network
Name
Date modified
Test File
5/25/2025 2:53 PM


Test File - Notepad
File Edit Format View Help
hello welcome to test file!

ASSIGNMENT 2

Part 3

MAY 26, 2025

NETWORK INSTALLATION AND ADMINISTRATION II

Laetitia Mohammed, 0931512

Contents

Tasks Task 1: Understanding Domain-Based GPOs

On DC112:

Open Group Policy Management Console (GPMC).

Identify existing domain-based GPOs and their link locations.

Delete both Default Domain Policy and Default Domain Controllers Policy.

Restore both policies using PowerShell.

Using GPMC, turn off Local GPO processing.

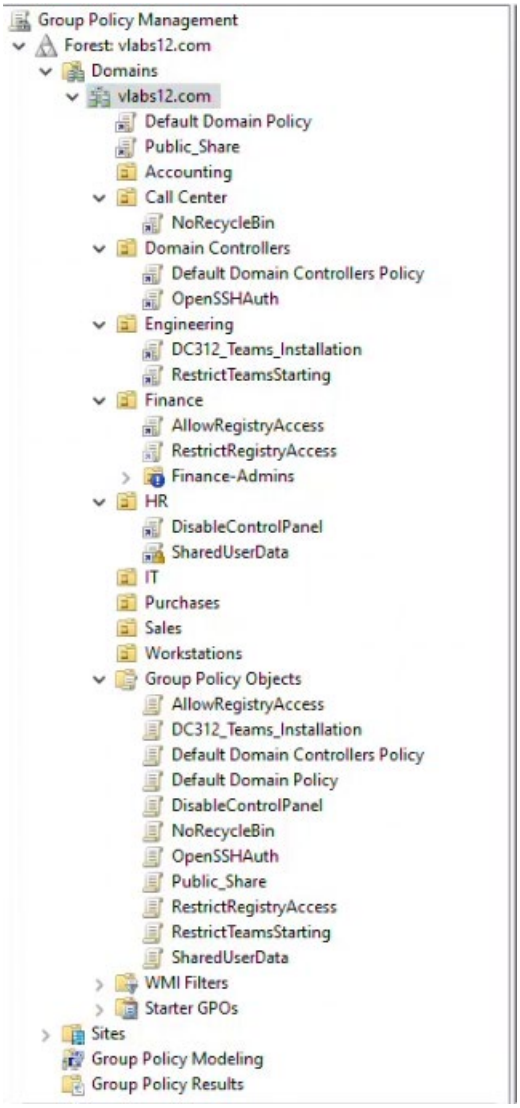
On Client12:

Open Local Group Policy Editor (gpedit.msc) using an Administrator account.

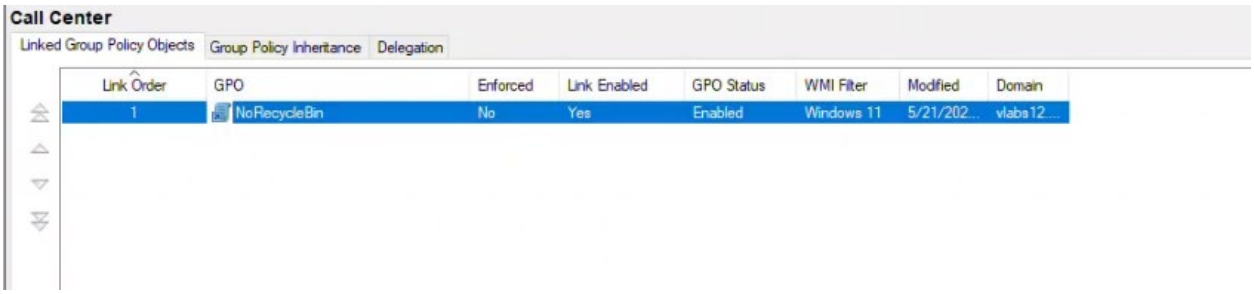
Compare Local GPO settings with the restored domain-based GPOs.

We will use the Group Policy Management Console to find and review all existing domain-based Group Policy Objects (GPOs) and see where they are linked in the domain. We will delete the Default Domain Policy and Default Domain Controllers Policy, then restore them using PowerShell to understand how to recover important policies. We will also turn off Local GPO processing in the console. On the client computer, I will open the Local Group Policy Editor and compare its settings with the restored domain-based GPOs to see how local and domain policies interact.

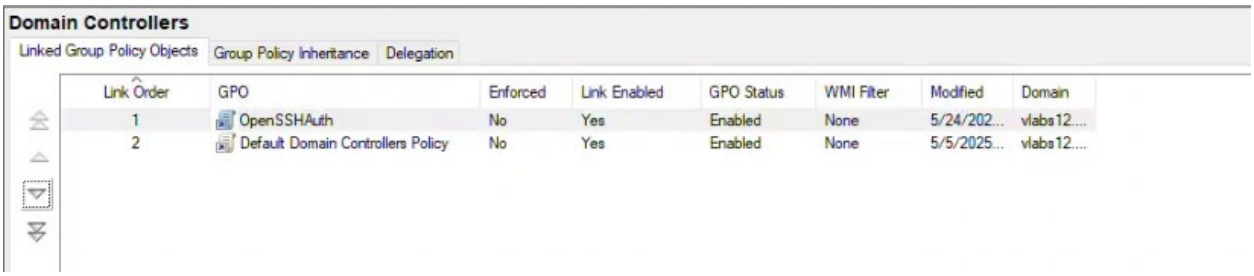
Open Group Policy Management and view the GPOs in the domain



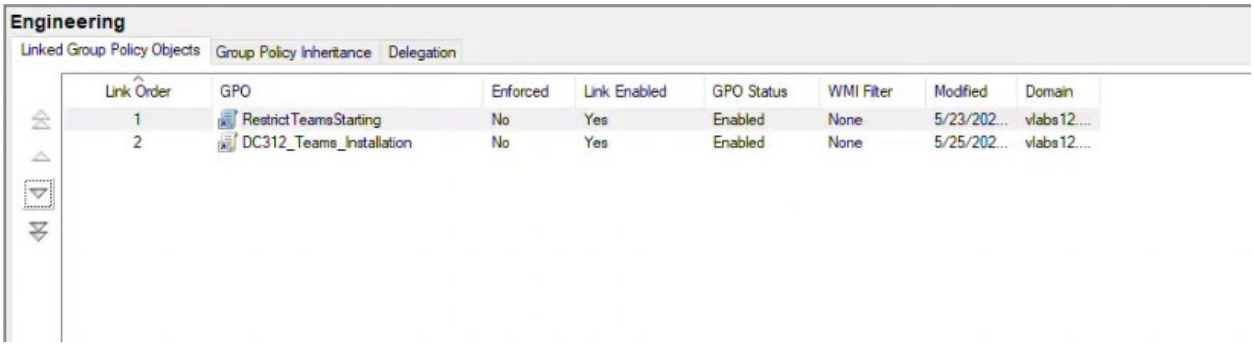
Call center:



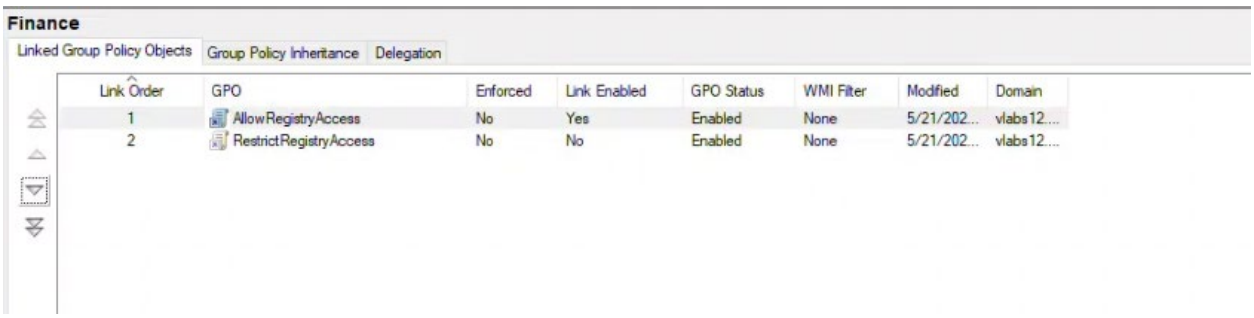
Domain Controllers:



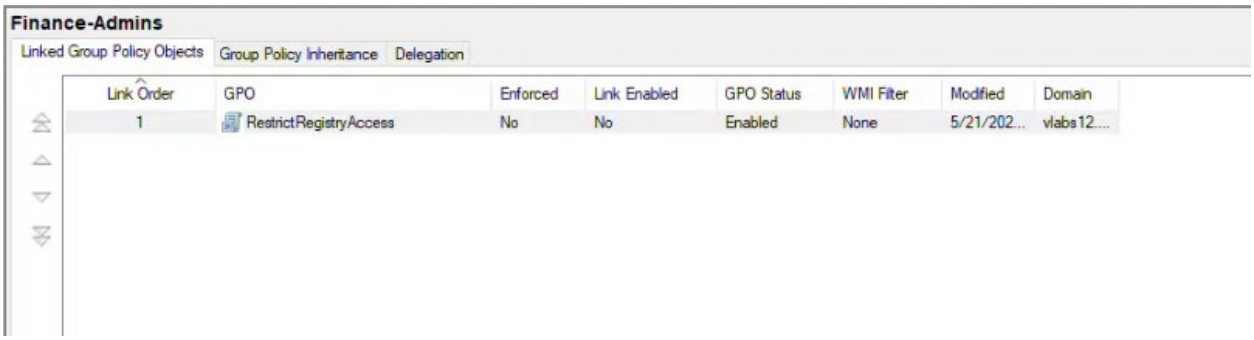
Engineering:



Finance:

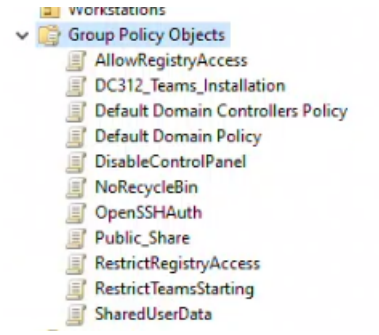


Finance Admins (part of Finance):



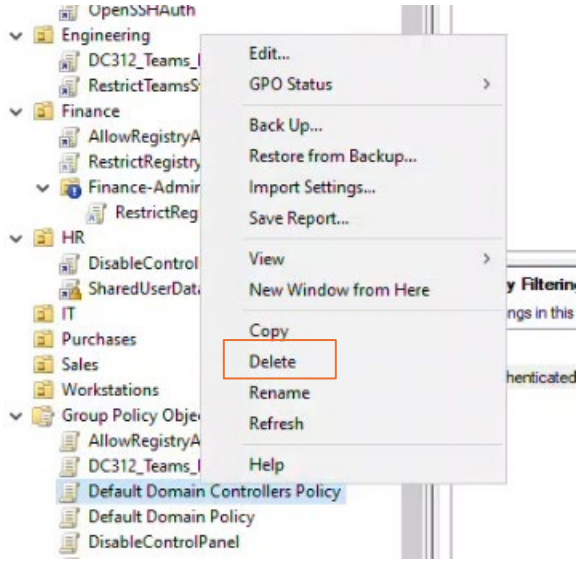
HR:

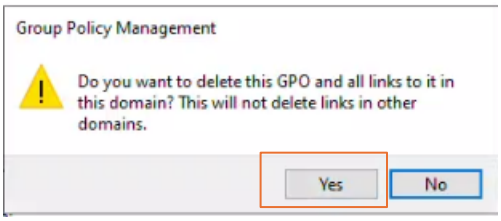
All GPOs part of vlabs12.com



Delete **Default Domain Controllers Policy** and **Default Domain Policy**

Right-click on Default Domain Controllers and Default Domain Policy



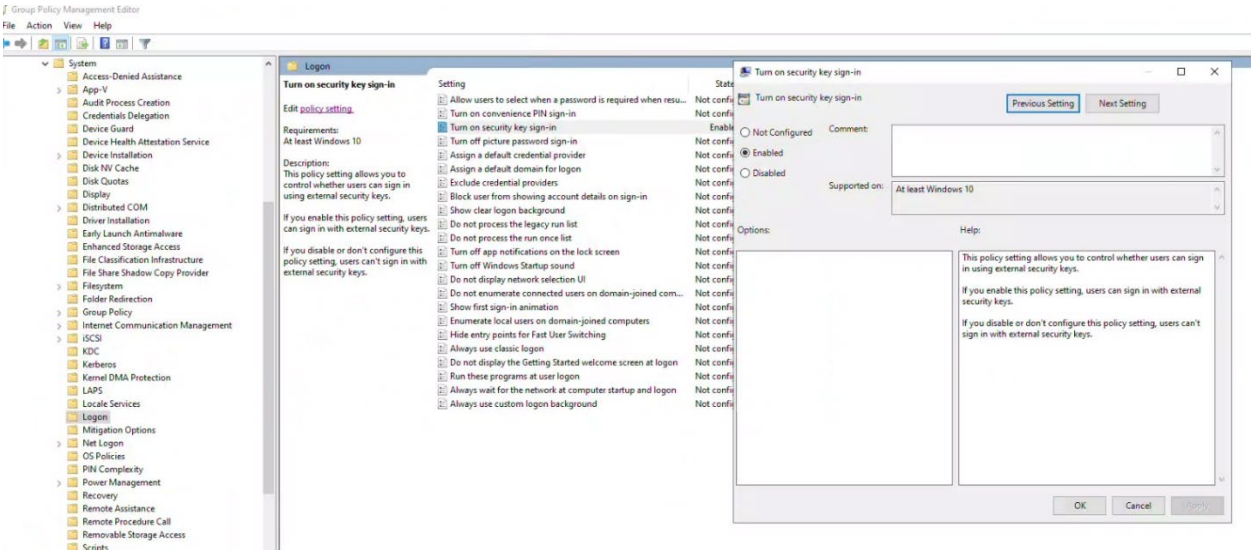


This did not work. After researching, deleting Default Domain Controllers Policy and Default Domain Policy is not possible due to Microsoft intending these two GPOs to not be deleted, only modified, for very good reason.

So we will modify the two GPOs and then restore them in Powershell.

Right click on Default Domain Policy → Edit

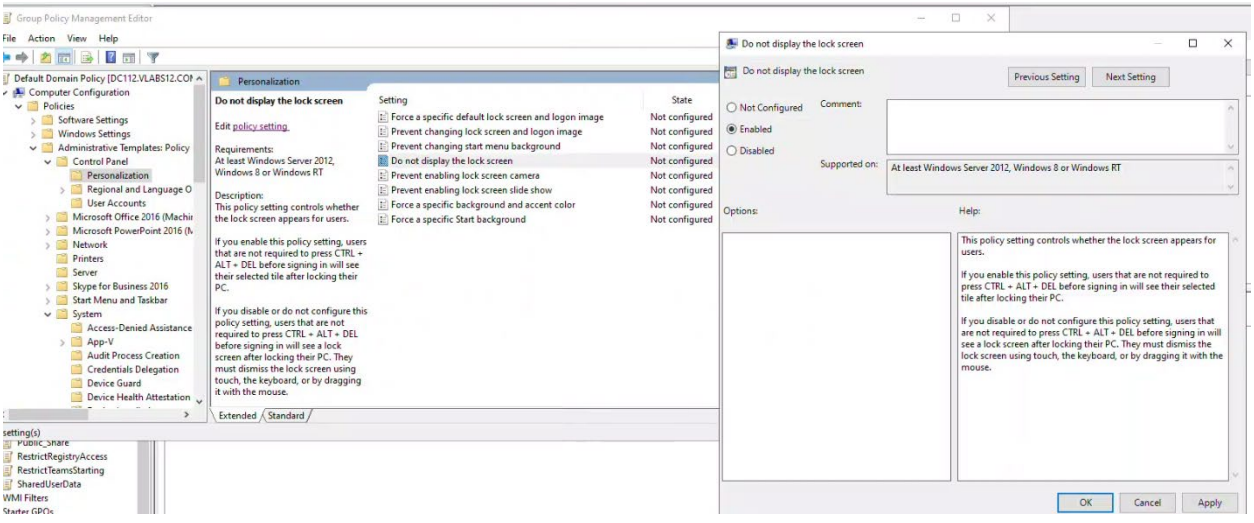
I modified something random like “Turn on security key sign-in”



Repeat the process for Default Domain Controllers Policy

Right-click → Edit

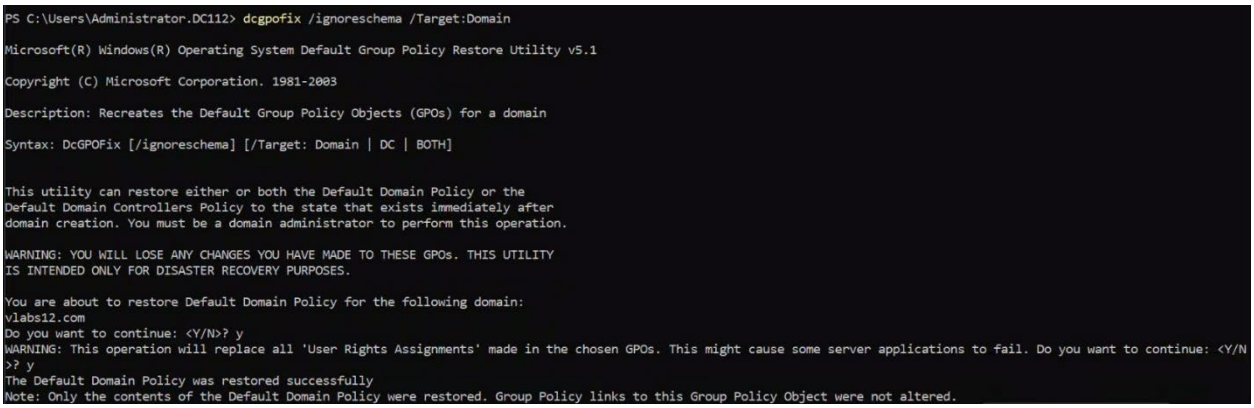
Computer Configuration → Administrative Templates Policy → Control Panel → Personalization → Do not display the lock screen “enabled”



Now that they've been modified (even slightly), on PowerShell, restore them to their defaults.

dcgpofix /ignoreschema /Target:Domain

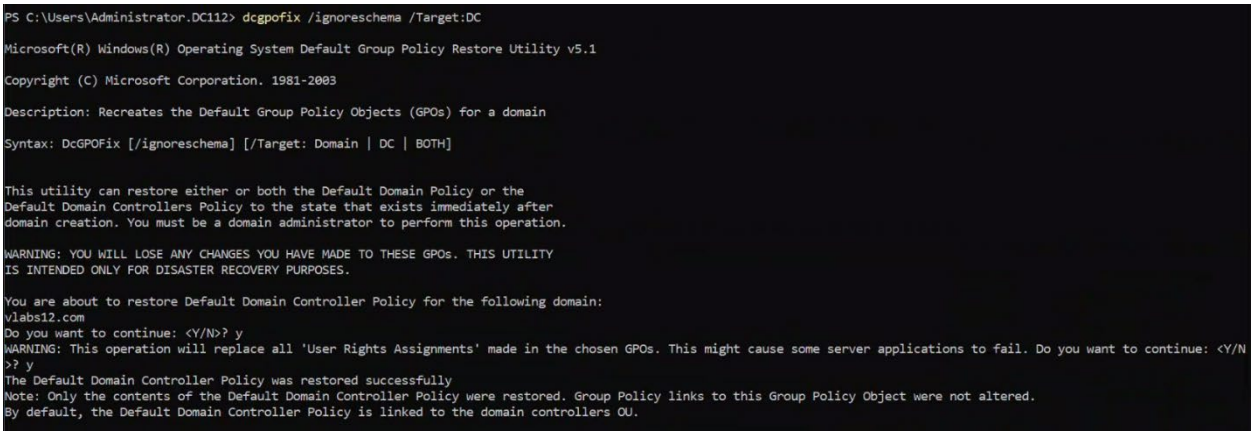
Answer "Y" for both prompts



For Domain Controllers:

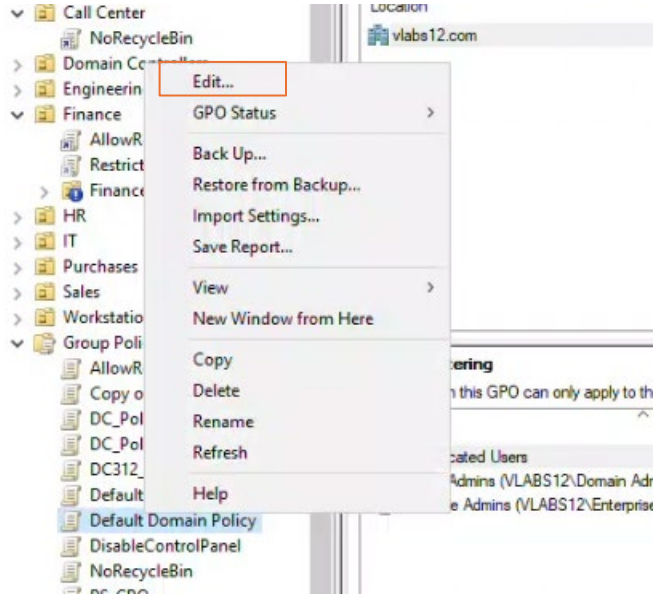
dcgpofix /ignoreschema /Target:DC

Answer "Y" for both prompts



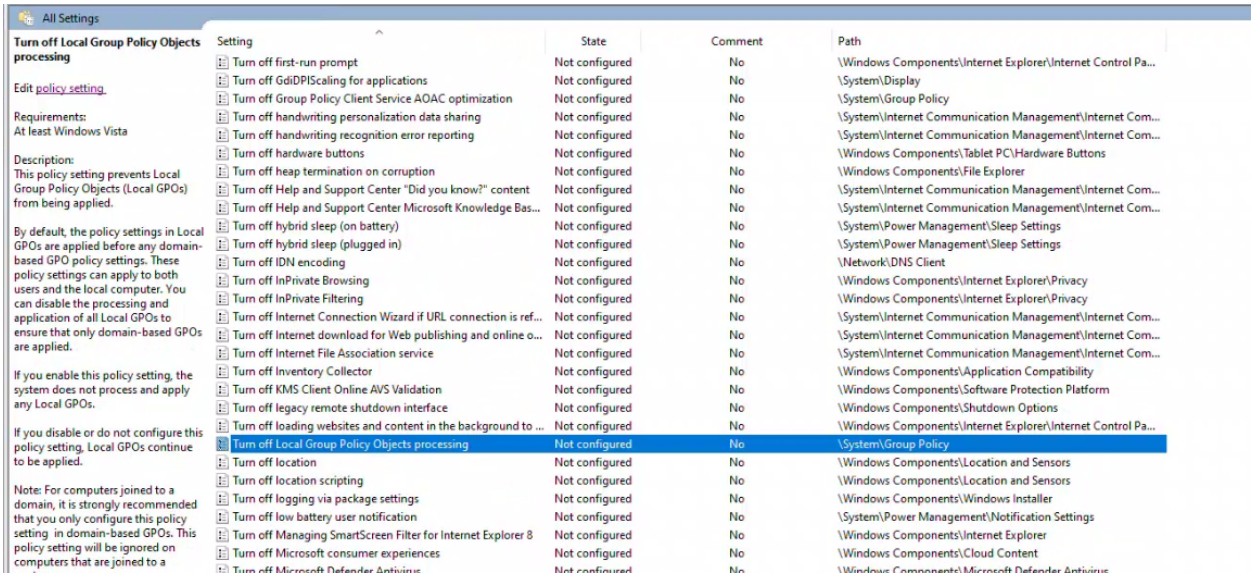
Using GPMC, turn off Local GPO processing.

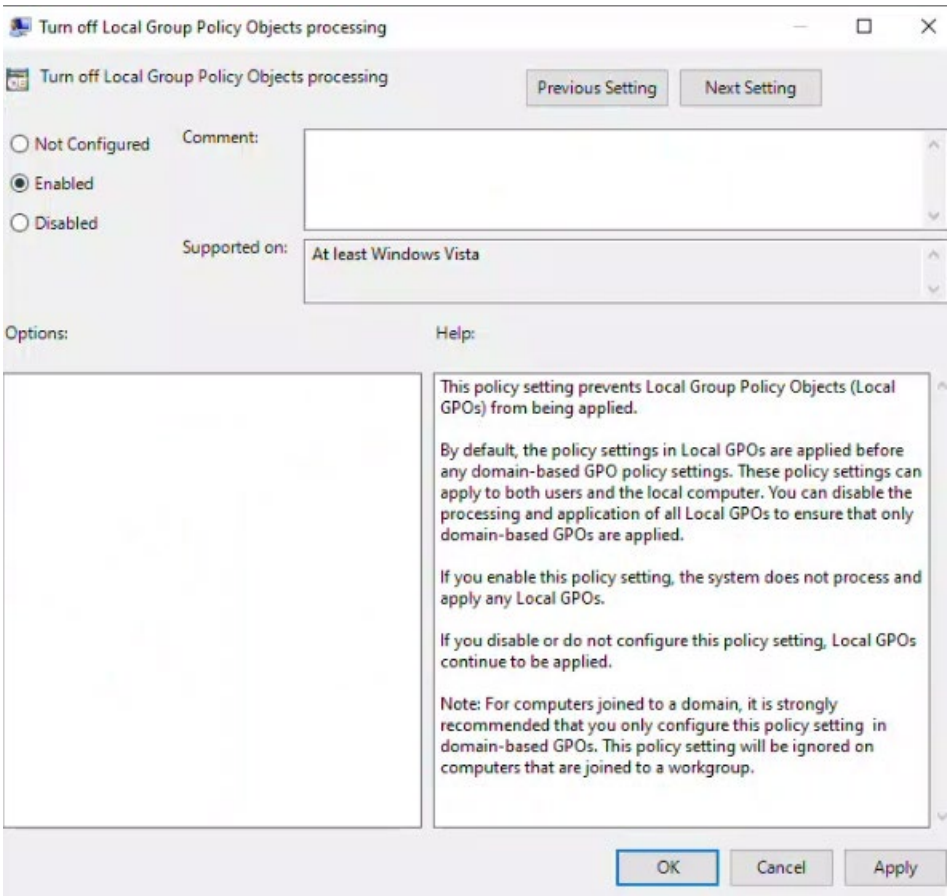
Right-click on Default Domain Policy → Edit



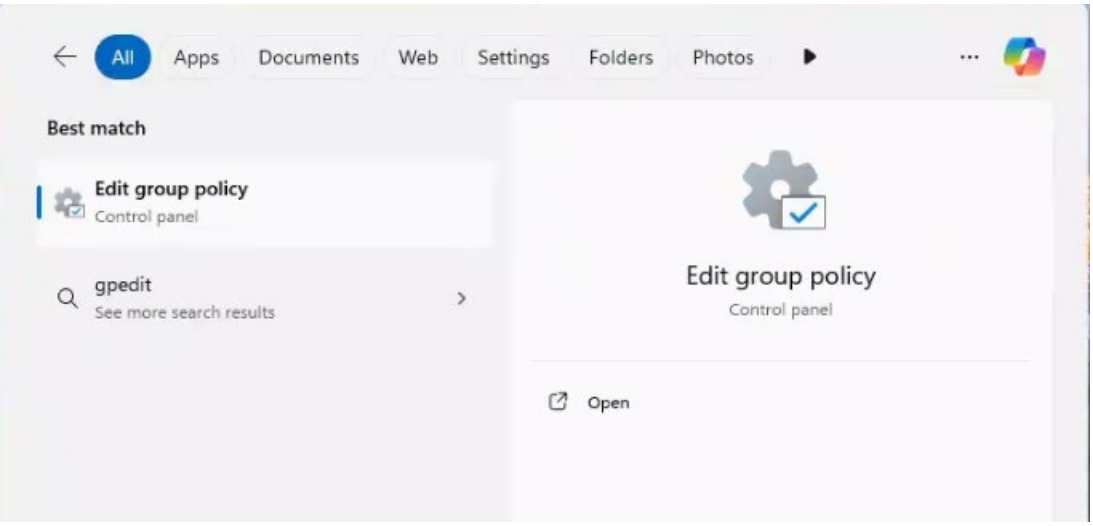
Under Computer Configuration → Policies → Administrative Templates → All Settings

Enable “Turn off Local Group Policy Objects processing”

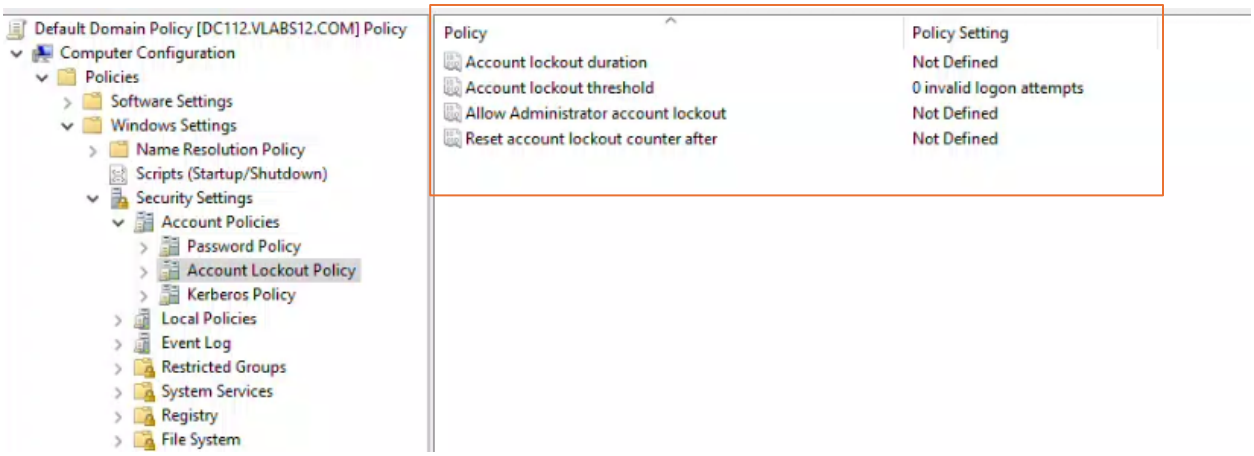




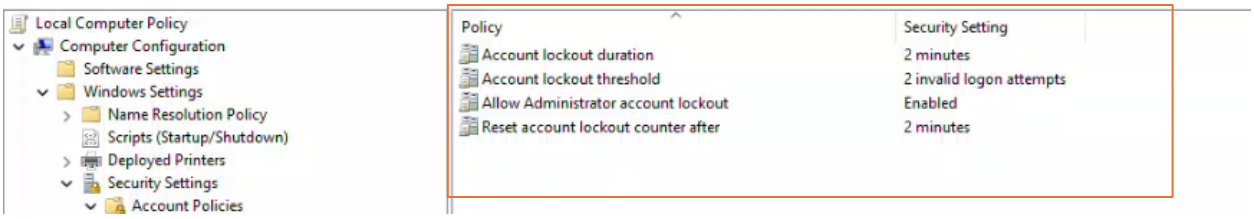
On Client12, Open Local Group Policy Editor (gpedit.msc) using an Administrator account.



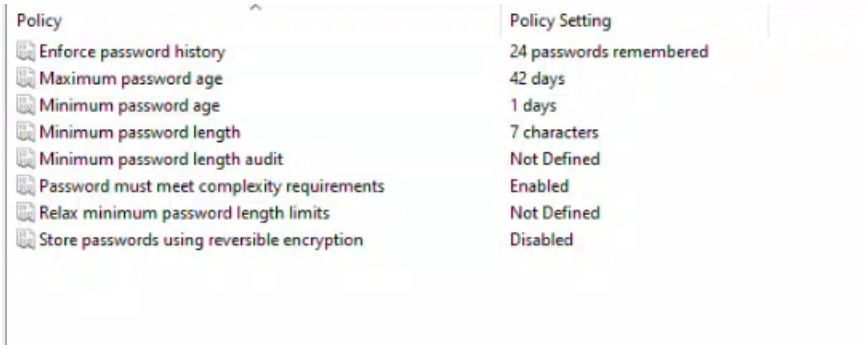
This is Default Domain Policy's "Account lockout policy" for example:



This is the Local Computer Policy



Default Domain Policy "password policy":



Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled

Local Computer “password policy”:

Policy	Security Setting
Enforce password history	24 passwords remember...
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	12 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled

Task 2: GPO Storage and Replication

Using GUI, on DC112:

Navigate to \\DC112\SYSVOL\vlabs12.com\Policies and list stored GPOs.

Use Active Directory Users and Computers (Enable Advanced Features) to view the Policies container.

Using PowerShell, on DC212:

Verify that DFSR service is running.

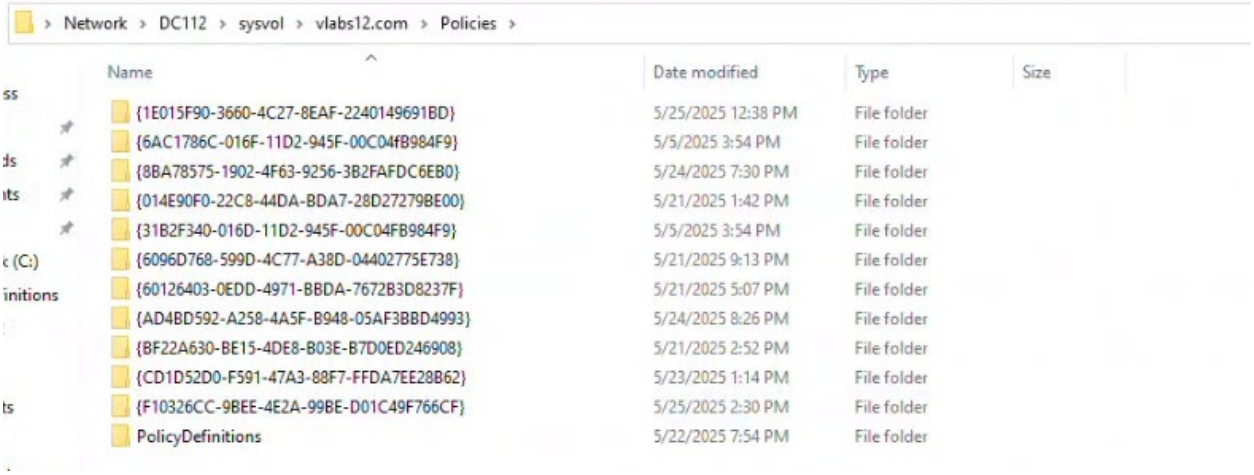
Force manually the DFS replication.

Check the replication status.

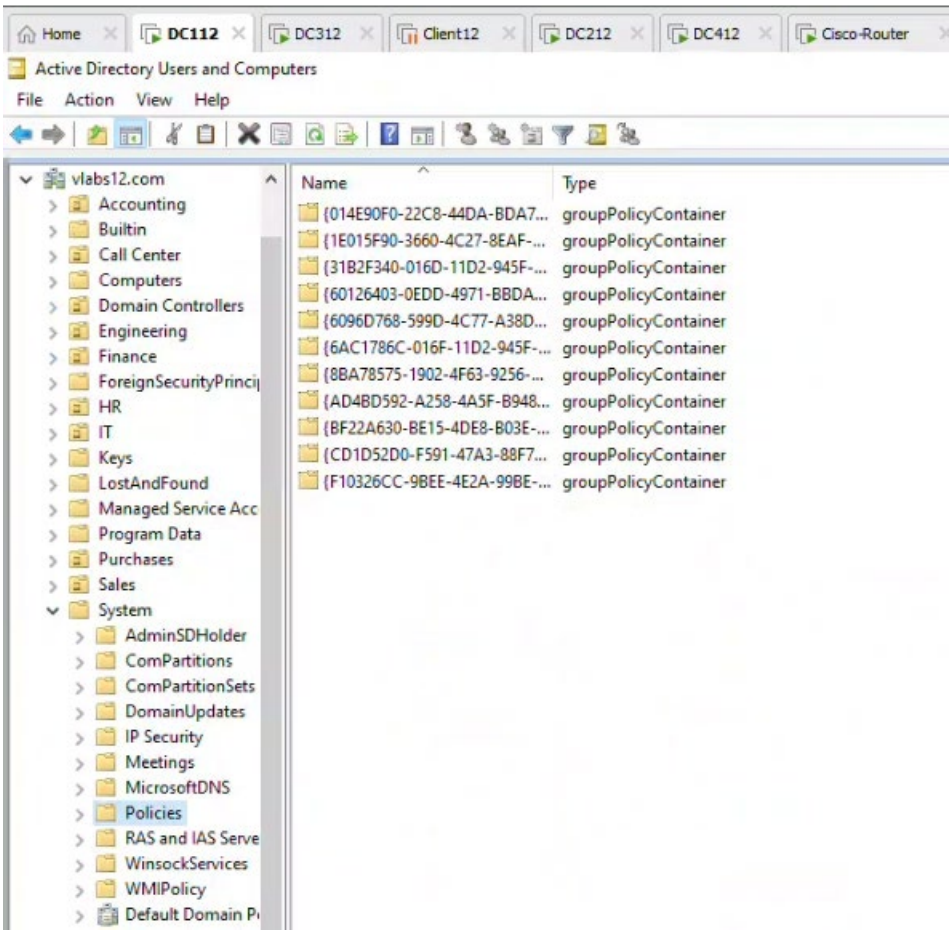
In this task, we will locate where GPOs are stored on the domain controller by browsing to the SYSVOL folder and viewing the Policies directory. We'll use Active Directory Users and Computers with advanced features enabled to see the Policies container in AD. On the second domain controller, check that the DFS Replication service is running, manually trigger replication, and verify that GPO changes are properly copied between controllers to ensure consistency across the domain

In File Explorer, go to \\DC112\SYSVOL\vlabs12.com\Policies

View all the GPOs listed by their GUIDs



In Active Directory Users and Computers, enable Advanced Features, go to System → Policies and view the same GPOs listed by their GUIDs



Verify that DFSR service is running using PowerShell on DC212

Get-Service DFSR

```
PS C:\Users\Administrator.VLABS12.000> Get-Service DFSR

Status   Name               DisplayName
------   ----               -----------
Running  DFSR               DFS Replication


PS C:\Users\Administrator.VLABS12.000>
```

Install-WindowsFeature FS-DFS-Replication

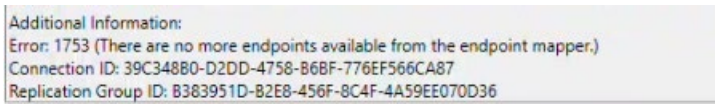
```
PS C:\Users\Administrator.VLABS12.000>  Install-WindowsFeature FS-DFS-Replication

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {DFS Replication}


PS C:\Users\Administrator.VLABS12.000>
PS C:\Users\Administrator.VLABS12.000>
```

dfsrdiag pollad

```
PS C:\Users\Administrator.VLABS12.000>  dfsrdiag pollad

Operation Succeeded

PS C:\Users\Administrator.VLABS12.000>
```

Get-DfsrBacklog -SourceComputerName DC112 -DestinationComputerName DC212

Shows no output. I've run into issues since demoting DC212 in a previous lab. I've confirmed replication is happening however. Example of one of the errors I get on DC112 pertaining to DFSR on DC212 below. Following this, I verified that all firewall ports for DFSR uses are authorized, restarted DFSR on both DC112 and DC212, re-replicated but I still get no output.



```
PS C:\Users\Administrator.VLABS12.000> New-NetFirewallRule -DisplayName "RPC Endpoint Mapper for DFSR" -Direction Inbound -Action Allow -Protocol TCP -LocalPort 135 -Progra
m "%systemroot%\system32\svchost.exe" -Profile Domain


Name                          : {498053d0-c80f-4763-9dac-23cdc912e6c8}
DisplayName                   : RPC Endpoint Mapper for DFSR
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Domain
Platform                      : {}
Direction                     : Inbound
Action                        : Allow
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId                   :
PackageFamilyName             :
```

```
PS C:\Users\Administrator.VLABS12.000> New-NetFirewallRule -DisplayName "RPC Dynamic Ports for DFSR" -Direction Inbound -Action Allow -Protocol TCP -LocalPort 49152-65535 -
Program "%systemroot%\system32\svchost.exe" -Profile Domain


Name                          : {d445909a-15ac-4731-8287-eb3e2be417ea}
DisplayName                   : RPC Dynamic Ports for DFSR
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Domain
Platform                      : {}
Direction                     : Inbound
Action                        : Allow
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId                   :
PackageFamilyName             :
```

```
Syncing all NC's held on DC112.
Syncing partition: DC=ForestDnsZones,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC212,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC312,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC412,CN=Servers,CN=New-York,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC312,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC212,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC412,CN=Servers,CN=New-York,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

Syncing partition: DC=DomainDnsZones,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC212,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC212,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.
```

```
Syncing partition: DC=DomainDnsZones,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC212,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC212,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

Syncing partition: CN=Schema,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC212,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC312,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC412,CN=Servers,CN=New-York,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC312,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC212,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC412,CN=Servers,CN=New-York,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.
```

```
Syncing partition: CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC212,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC312,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC412,CN=Servers,CN=New-York,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC312,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC412,CN=Servers,CN=New-York,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC212,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.
```

```
Syncing partition: DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC212,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC412,CN=Servers,CN=New-York,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC212,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC312,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC412,CN=Servers,CN=New-York,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC312,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

Syncing partition: DC=partner12,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC212,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC312,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC212,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC312,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.
```

```
Syncing partition: DC=lab12,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC212,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC412,CN=Servers,CN=New-York,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC212,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC112,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
    To  : CN=NTDS Settings,CN=DC412,CN=Servers,CN=New-York,CN=Sites,CN=Configuration,DC=vlabs12,DC=com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

PS C:\Users\Administrator.VLABS12.000>
```

Repadmin /replsummary

```
PS C:\Users\Administrator.VLABS12.000> repadmin /replsummary
Replication Summary Start Time: 2025-05-27 08:56:25

Beginning data collection for replication summary, this may take awhile:
  .......


Source DSA          largest delta    fails/total %%   error
 DC112                  01m:41s    0 /  17    0
 DC212                  57m:45s    0 /  12    0
 DC312                  57m:58s    0 /  10    0
 DC412                  42m:45s    0 /   5    0


Destination DSA     largest delta    fails/total %%   error
 DC112                  57m:45s    0 /  17    0
 DC212                  57m:58s    0 /  12    0
 DC312                  02m:58s    0 /  10    0
 DC412                  01m:42s    0 /   5    0
```

```
PS C:\Users\Administrator.DC112> repadmin /replsummary
Replication Summary Start Time: 2025-05-27 08:56:50

Beginning data collection for replication summary, this may take awhile:
  .......


Source DSA          largest delta    fails/total %%   error
 DC112                      02m:06s    0 /  17    0
 DC212                      58m:10s    0 /  12    0
 DC312                      58m:23s    0 /  10    0
 DC412                      43m:10s    0 /   5    0


Destination DSA     largest delta    fails/total %%   error
 DC112                      58m:10s    0 /  17    0
 DC212                      58m:23s    0 /  12    0
 DC312                      03m:23s    0 /  10    0
 DC412                      02m:06s    0 /   5    0


PS C:\Users\Administrator.DC112> _
```

```
PS C:\Users\Administrator.DC112> Get-Service -Name DFSR, RpcSs

Status   Name               DisplayName
------   ----               -----------
Running  DFSR               DFS Replication
Running  RpcSs              Remote Procedure Call (RPC)
```

```
PS C:\Users\Administrator.DC112> dfsrdiag replicationstate
Summary

  Active inbound connections: 0
  Updates received: 0

  Active outbound connections: 0
  Updates sent out: 0

Operation Succeeded
```

Task 3: Common GPO Management Tasks

On DC112 using GUI:

Backup all existing GPOs.

Delete any GPO and attempt to restore it from the backup.

Create new GPO DC_Policy.

Import Default Domian Controllers GPO settings into DC_Policy.

Verify DC_Policy new settings to confirm the importation.

Copy any existing GPO to a new one in the same domain.

Verify copied GPO settings.

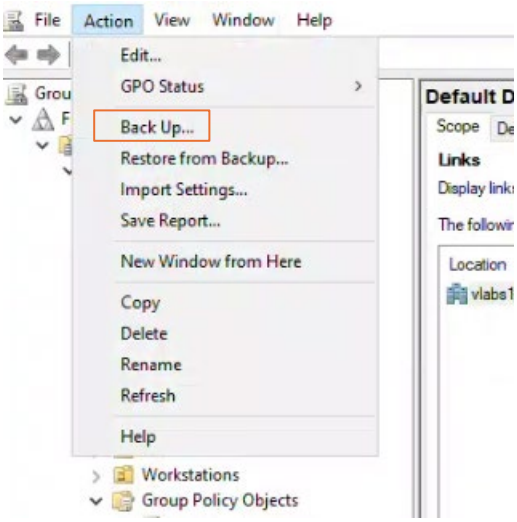
On DC112 using PowerShell:

Perform the previous tasks using PowerShell.

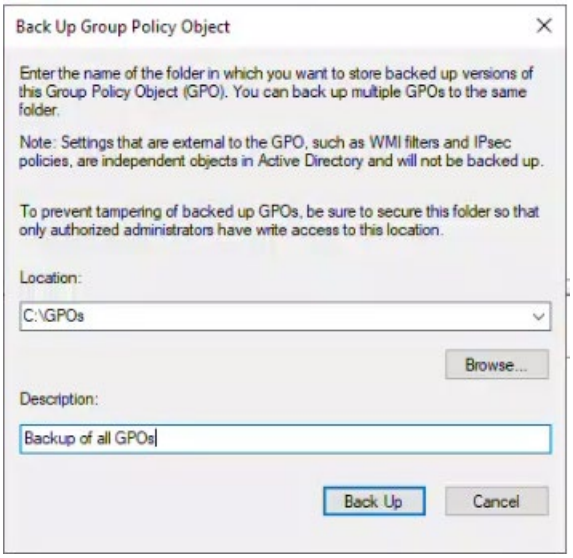
We will back up all current GPOs, delete one, and then restore it from the backup to practice safe policy management. I will create a new GPO called DC_Policy, import settings from the Default Domain Controllers GPO into it, and check that the import was successful. We'll copy an existing GPO to make a new one and verify that the settings match. Repeat all the tasks afterwards using PowerShell

In Group Policy Management, click on Action at the top → "Back up"

This backs up all GPOs in the domain

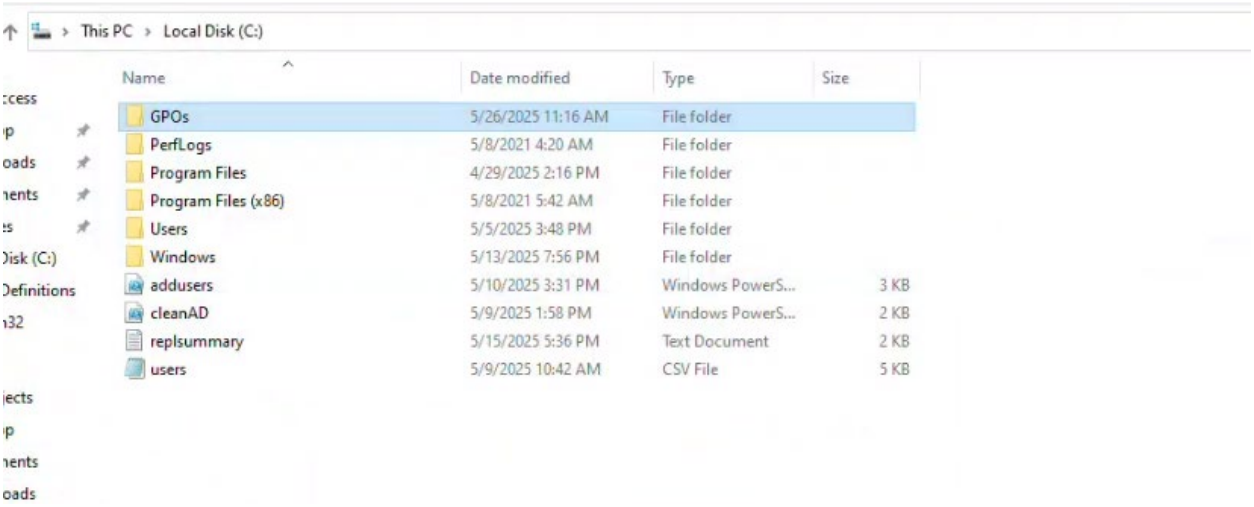


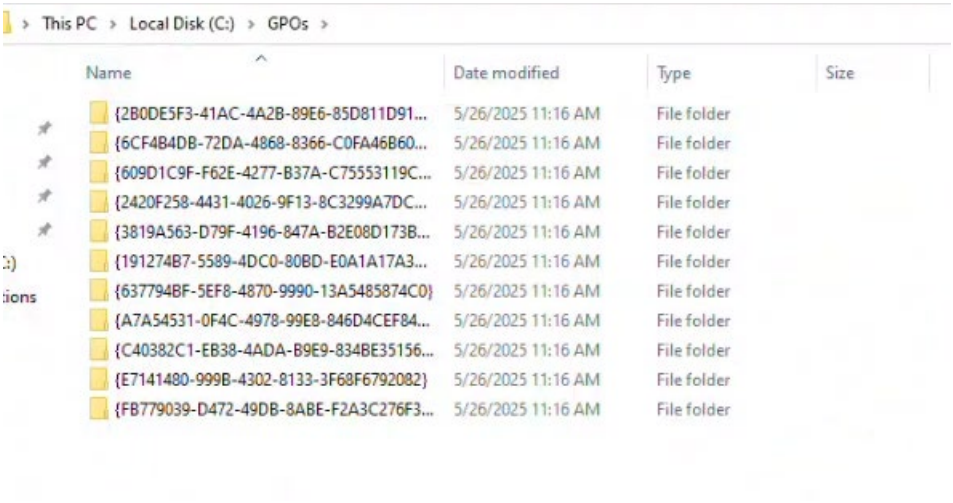
Name your backup and set a description



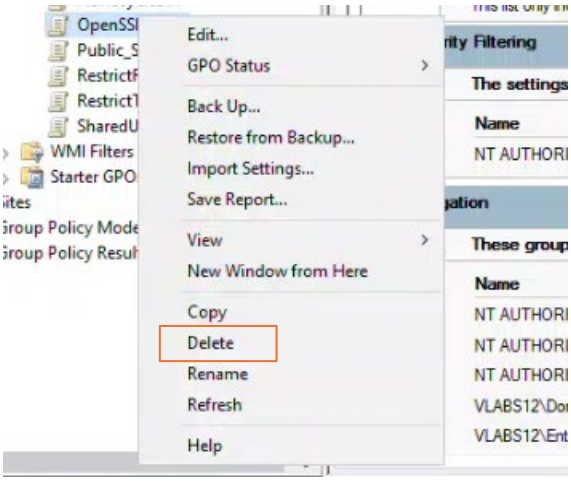
I already had a backup of my GPOs from task 1, before attempting to delete Default Domain Policy and Default Domain Controllers Policy as precaution.

You can view the backup folder in C:/ GPOs

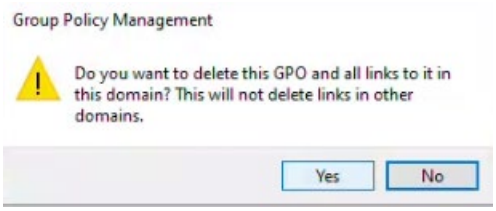




Delete any GPO and attempt to restore it from the backup.

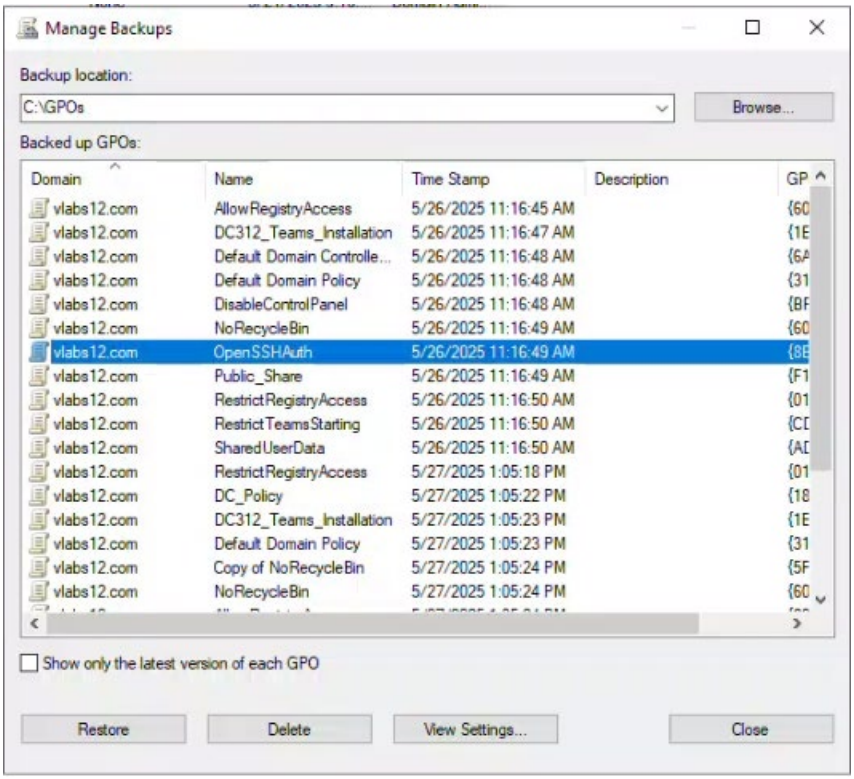


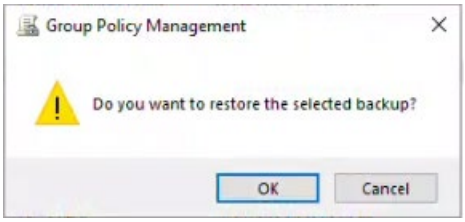
Click Yes

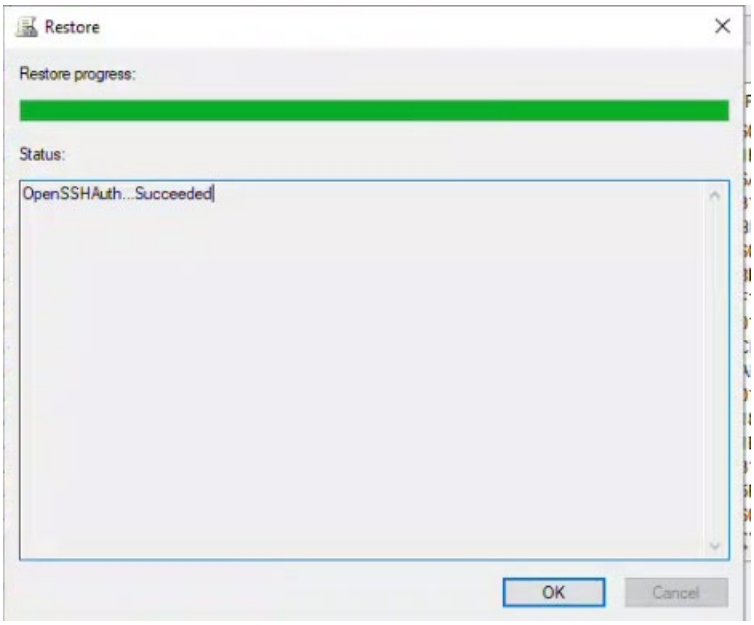


Click on Group Policy Objects, then click on Action at the top and select Manage Backups

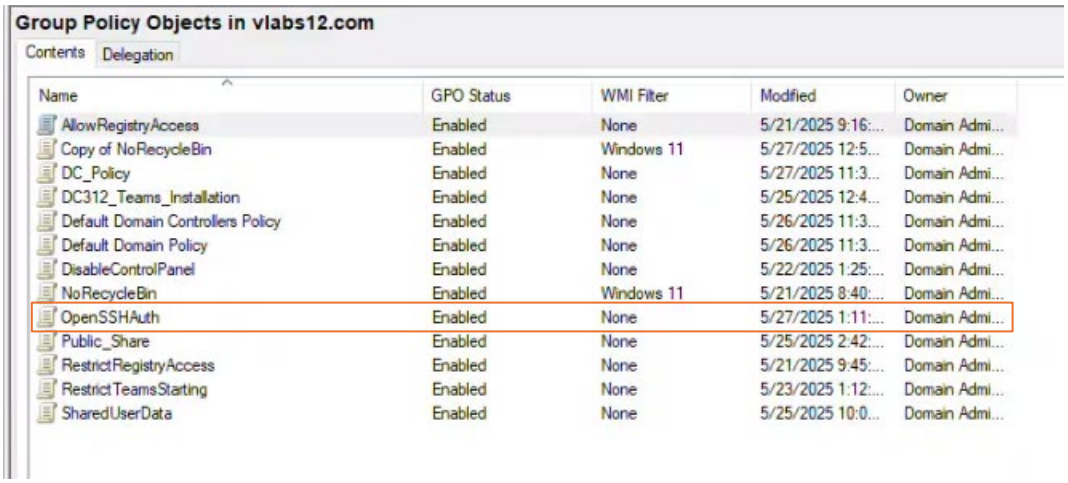
Select the GPO you want to restore



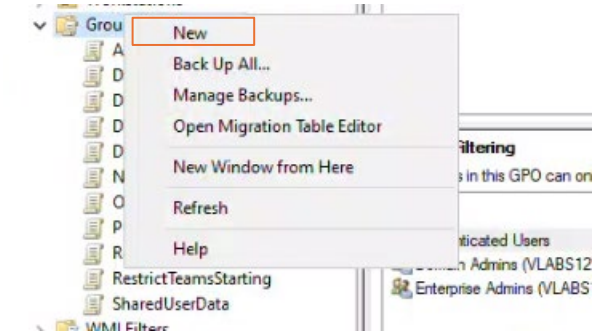


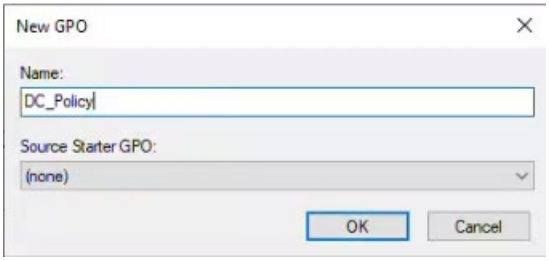


Below you'll see the restored GPO, along with the modified date

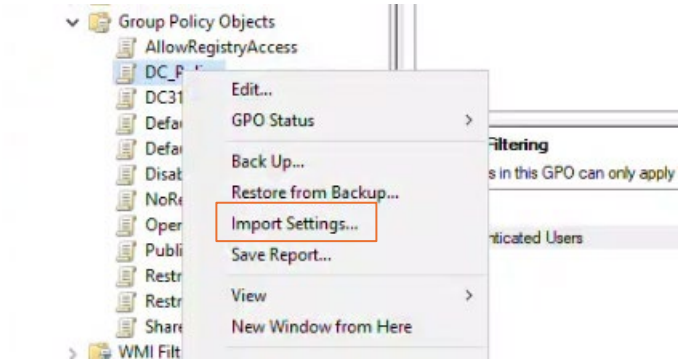


Create new GPO **DC_Policy.**

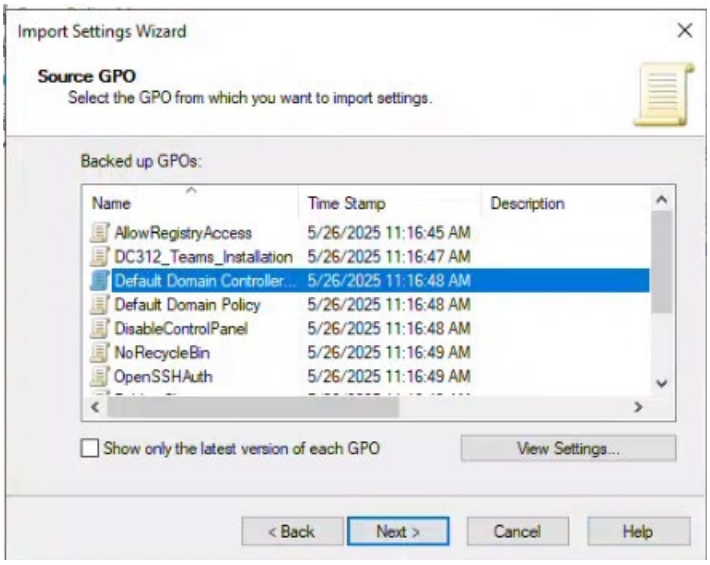




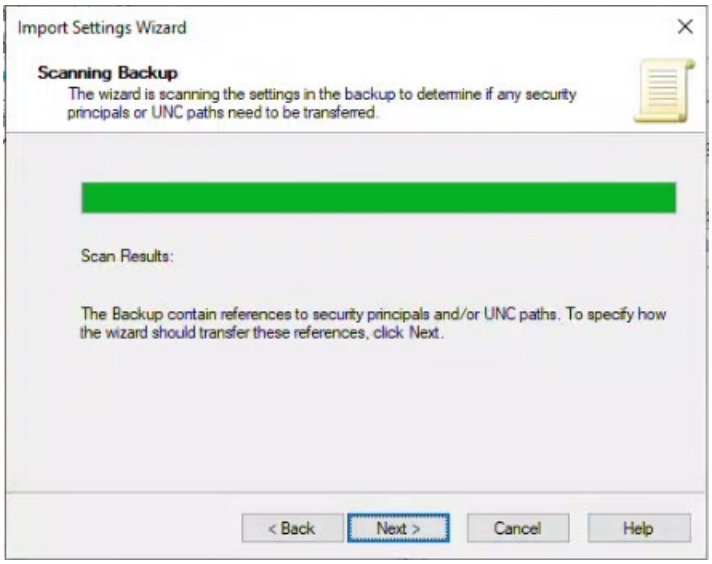
Import the settings from Default Domain Controllers Policy



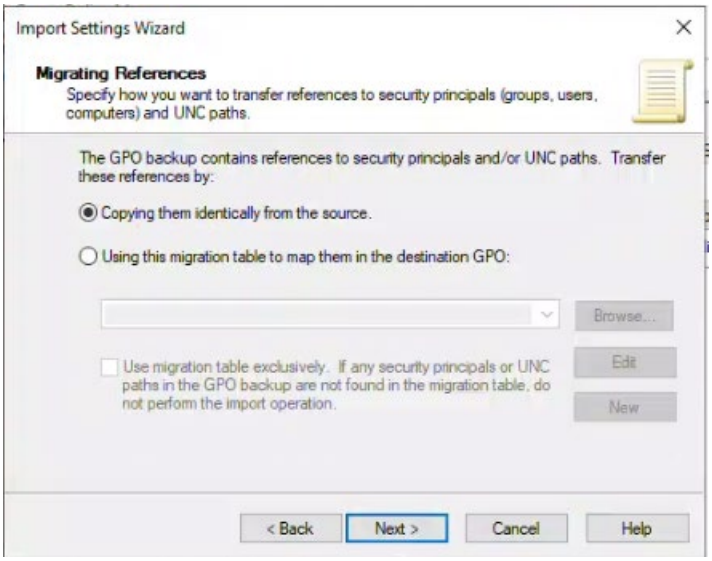
Select the GPO



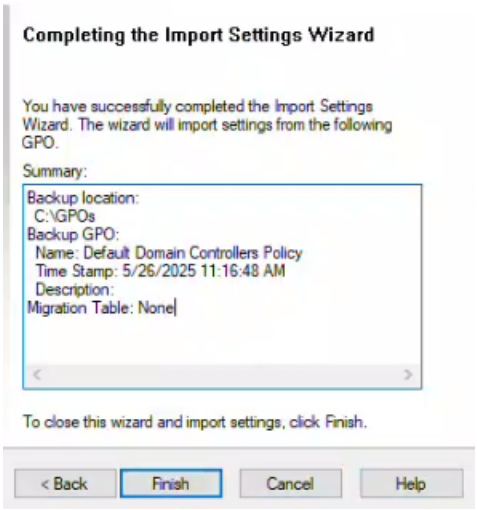
Follow the Wizard, clicking Next

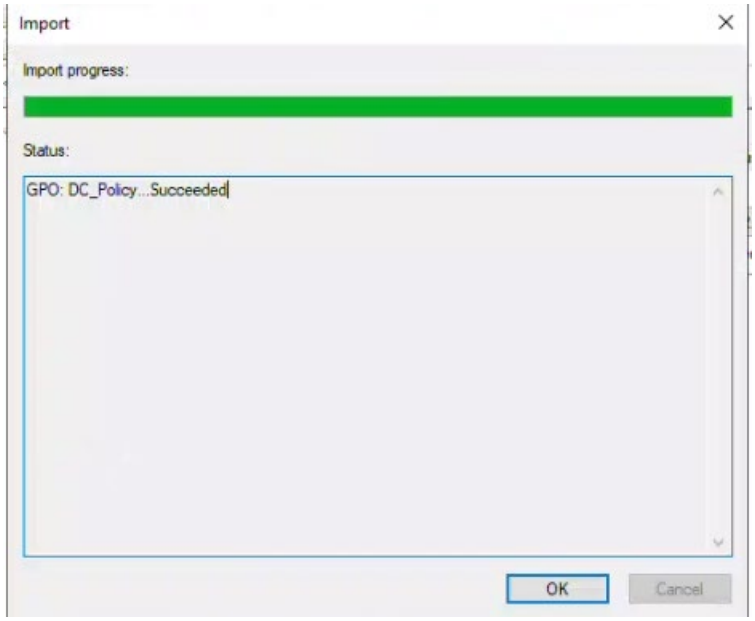


Select “copying them identically from the source”

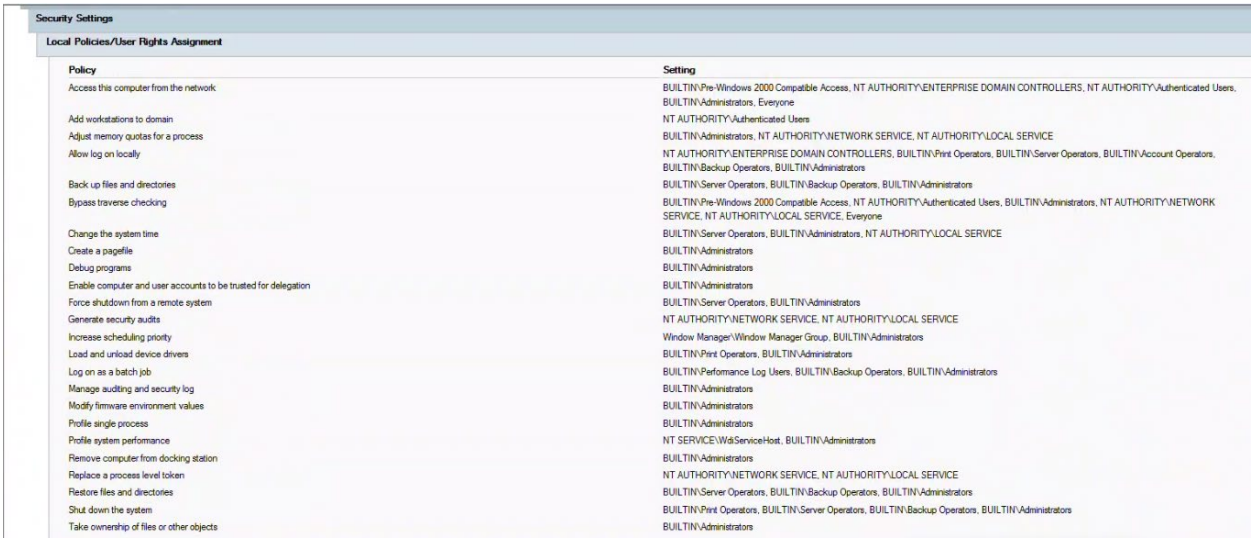


Review your selections and click Finish





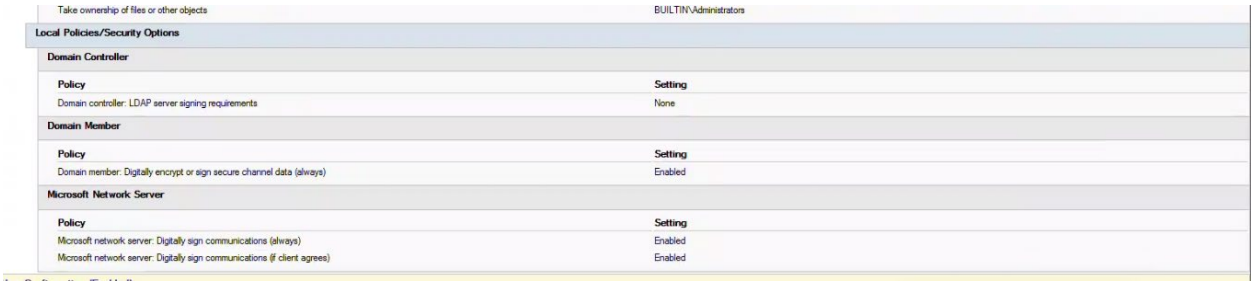
Settings of Default Domain Controllers Policy:



Security Settings

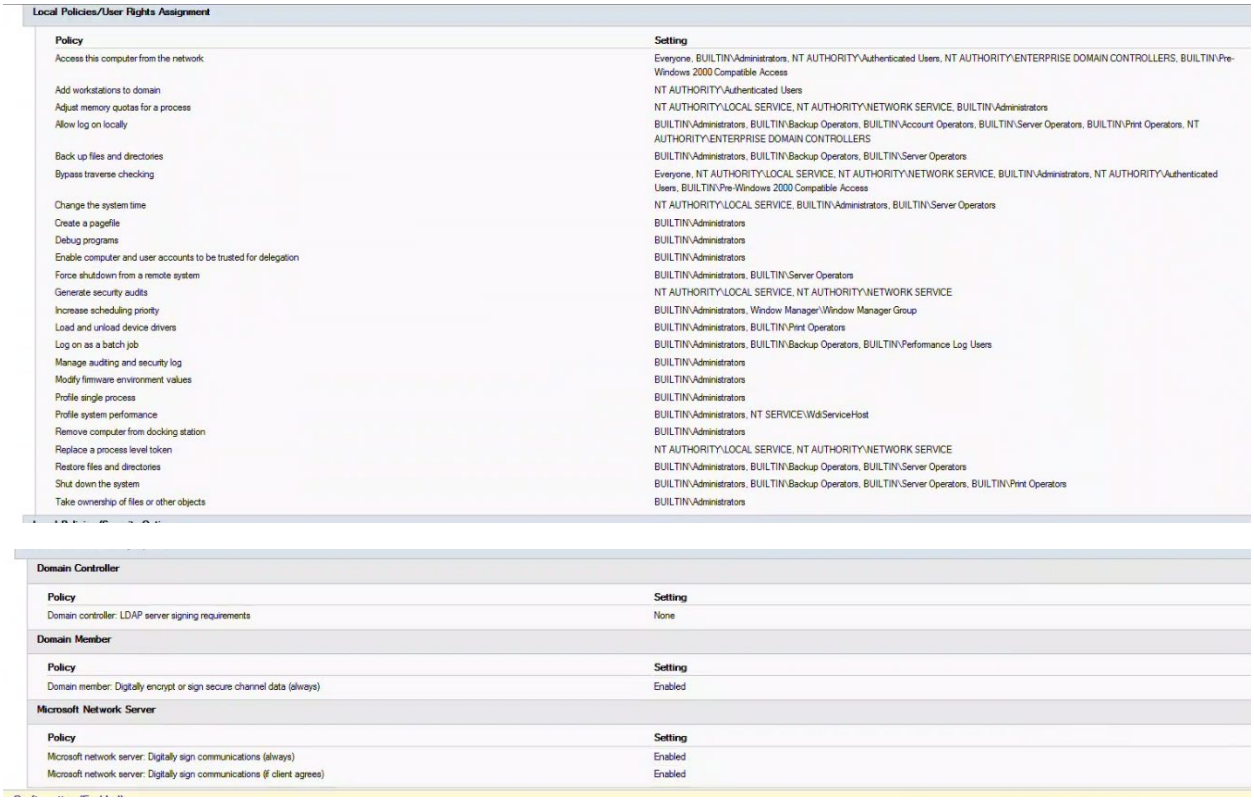
Local Policies/User Rights Assignment

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\WdiServiceHost, 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



Take ownership of files or other objects	BUILTIN\Administrators
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

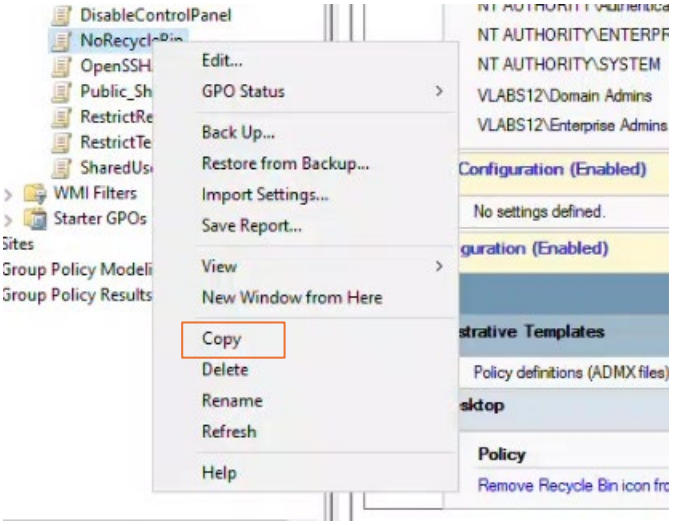
Settings of new GPO DC_Policy:



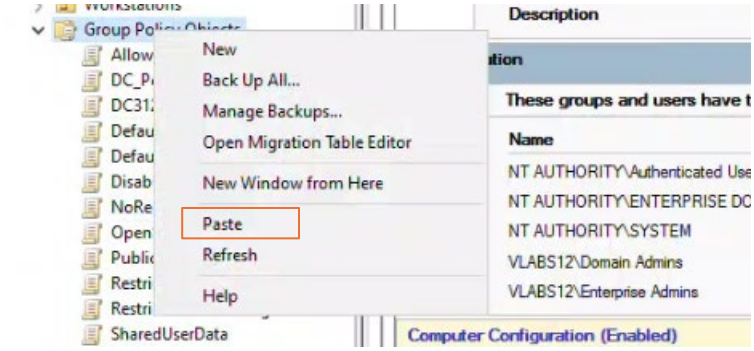
Local Policies/User Rights Assignment	
Policy	**Setting**
Access this computer from the network	Everyone, BUILTIN\Administrators, NT AUTHORITY\Authenticated Users, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, BUILTIN\Pre-Windows 2000 Compatible Access
Add workstations to domain	NT AUTHORITY\Authenticated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

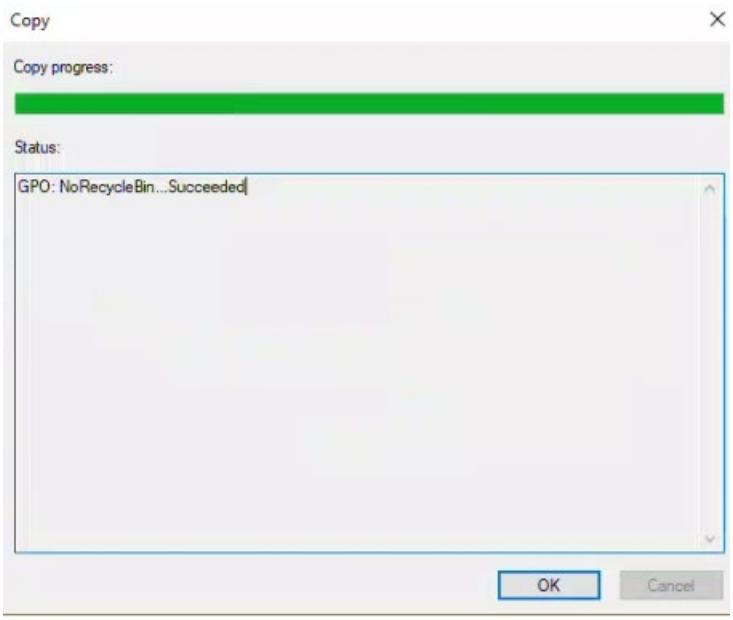
Domain Controller	
Policy	**Setting**
Domain controller: LDAP server signing requirements	None
Domain Member	
Policy	**Setting**
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Microsoft Network Server	
Policy	**Setting**
Microsoft network server: Digitally sign communications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

Copy an existing GPO by right-clicking and selecting “Copy”

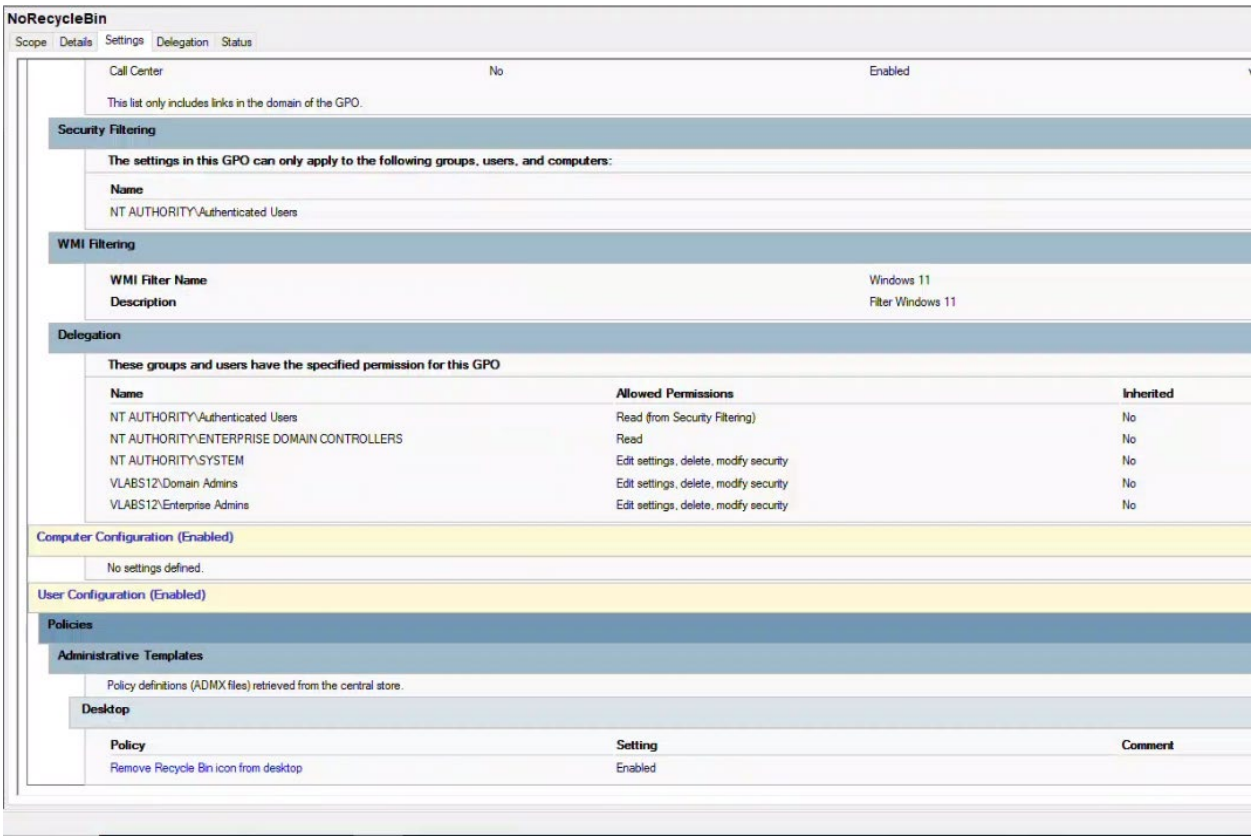


Paste it in Group Policy Objects

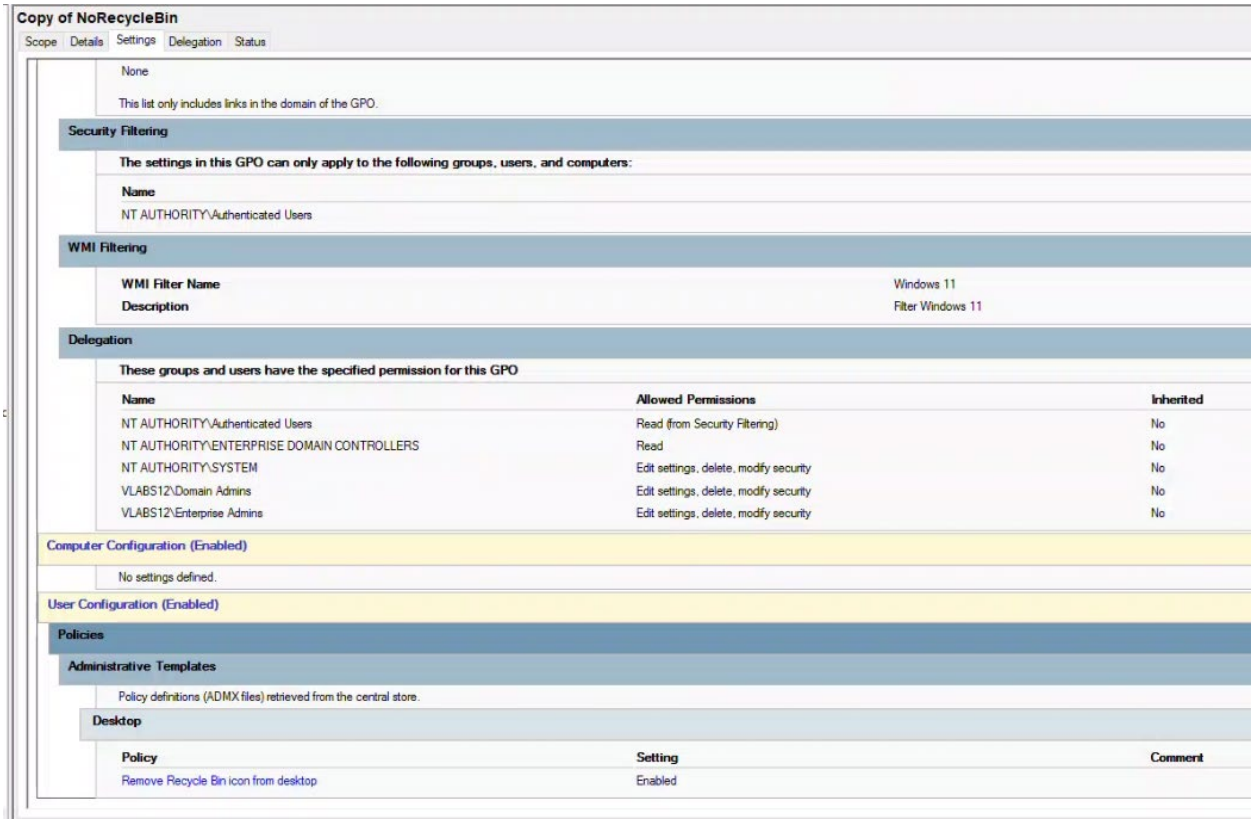




Settings of original NoRecyclingBin GPO:



Settings of Copy:



Perform the previous tasks using PowerShell

Backup-GPO -All -Path "C:\GPOs"

```
PS C:\Users\Administrator.DC112> Backup-GPO -All -Path "C:\GPOs"


DisplayName      : RestrictRegistryAccess
GpoId            : 014e90f0-22c8-44da-bda7-28d27279be00
Id               : 7bac63ba-63df-4f69-b187-5b1097cfa226
BackupDirectory  : C:\GPOs
CreationTime     : 5/27/2025 1:05:18 PM
DomainName       : vlabs12.com
Comment          :

DisplayName      : DC_Policy
GpoId            : 180f0a95-fa5b-4349-ad28-c386f25ae499
Id               : e64c7123-29f8-4a56-9e71-a61767cd87e2
BackupDirectory  : C:\GPOs
CreationTime     : 5/27/2025 1:05:22 PM
DomainName       : vlabs12.com
Comment          :

DisplayName      : DC312_Teams_Installation
GpoId            : 1e015f90-3660-4c27-8eaf-2240149691bd
Id               : 15c0c194-23cc-4404-974a-8b659ec525f0
BackupDirectory  : C:\GPOs
CreationTime     : 5/27/2025 1:05:23 PM
DomainName       : vlabs12.com
Comment          :

DisplayName      : Default Domain Policy
GpoId            : 31b2f340-016d-11d2-945f-00c04fb984f9
Id               : 4cd44417-e7d1-4c89-834a-292c76810208
BackupDirectory  : C:\GPOs
CreationTime     : 5/27/2025 1:05:23 PM
DomainName       : vlabs12.com
```

```
DisplayName      : Copy of NoRecycleBin
GpoId            : 5fb0bae5-58b0-41a0-94f0-9650f386196f
Id               : 9bcf14a0-5bea-45eb-be30-1f5105818207
BackupDirectory  : C:\GPOs
CreationTime     : 5/27/2025 1:05:24 PM
DomainName       : vlabs12.com
Comment          :

DisplayName      : NoRecycleBin
GpoId            : 60126403-0edd-4971-bbda-7672b3d8237f
Id               : 8422552d-93ec-424e-b9c6-8e234f44ea0c
BackupDirectory  : C:\GPOs
CreationTime     : 5/27/2025 1:05:24 PM
DomainName       : vlabs12.com
Comment          :

DisplayName      : AllowRegistryAccess
GpoId            : 6096d768-599d-4c77-a38d-04402775e738
Id               : 526c7bf6-b11d-4de6-a1ba-e0f689aff9d6
BackupDirectory  : C:\GPOs
CreationTime     : 5/27/2025 1:05:24 PM
DomainName       : vlabs12.com
Comment          :

DisplayName      : Default Domain Controllers Policy
GpoId            : 6ac1786c-016f-11d2-945f-00c04fb984f9
Id               : 89c1bbdd-06e5-4812-9f6d-a115b4034cb1
BackupDirectory  : C:\GPOs
CreationTime     : 5/27/2025 1:05:25 PM
DomainName       : vlabs12.com
Comment          :
```

```
DisplayName      : OpenSSHAuth
GpoId            : 8ba78575-1902-4f63-9256-3b2fafdc6eb0
Id               : 5bfdc6bb-d0f7-4f3d-adb0-e366d2bbe92f
BackupDirectory  : C:\GPOs
CreationTime     : 5/27/2025 1:05:25 PM
DomainName       : vlabs12.com
Comment          :

DisplayName      : SharedUserData
GpoId            : ad4bd592-a258-4a5f-b948-05af3bbd4993
Id               : de3dcfc2-f4e5-4856-8f32-703910f503c1
BackupDirectory  : C:\GPOs
CreationTime     : 5/27/2025 1:05:25 PM
DomainName       : vlabs12.com
Comment          :

DisplayName      : DisableControlPanel
GpoId            : bf22a630-be15-4de8-b03e-b7d0ed246908
Id               : 165442a5-073f-4d26-b5a0-4a22b99b7557
BackupDirectory  : C:\GPOs
CreationTime     : 5/27/2025 1:05:26 PM
DomainName       : vlabs12.com
Comment          :

DisplayName      : RestrictTeamsStarting
GpoId            : cd1d52d0-f591-47a3-88f7-ffda7ee28b62
Id               : bdf4609e-42f5-4e54-8c0c-2776cbef0a4f
BackupDirectory  : C:\GPOs
CreationTime     : 5/27/2025 1:05:26 PM
DomainName       : vlabs12.com
Comment          :
```

```
DisplayName      : Public_Share
GpoId            : f10326cc-9bee-4e2a-99be-d01c49f766cf
Id               : 2f2095f8-f2cd-409a-89cc-2cda6c171a19
BackupDirectory  : C:\GPOs
CreationTime     : 5/27/2025 1:05:26 PM
DomainName       : vlabs12.com
Comment          :
```

Delete any GPO and attempt to restore it from the backup

```
PS C:\Users\Administrator.DC112> Remove-GPO -Name "NoRecycleBin"
PS C:\Users\Administrator.DC112>
```

Restore-GPO -Path "C:\GPOs" -BackupId “{DD309684-FB1C-4D76-87B7-4C4632D606BB}”

```
PS C:\Users\Administrator.DC112> Restore-GPO -Path "C:\GPOs" -BackupId "{DD309684-FB1C-4D76-87B7-4C4632D606BB}"


DisplayName      : NoRecycleBin
DomainName       : vlabs12.com
Owner            : VLABS12\Domain Admins
Id               : 60126403-0edd-4971-bbda-7672b3d8237f
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 5/27/2025 2:06:45 PM
ModificationTime : 5/27/2025 2:06:45 PM
UserVersion      : AD Version: 3, SysVol Version: 3
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        : Windows 11


PS C:\Users\Administrator.DC112>
```

New-GPO -Name "DC_Policy2”

```
PS C:\Users\Administrator.DC112> New-GPO -Name "DC_Policy2"


DisplayName      : DC_Policy2
DomainName       : vlabs12.com
Owner            : VLABS12\Domain Admins
Id               : 7cc4388e-eb69-4701-9da5-ae4312e4518a
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 5/27/2025 2:21:11 PM
ModificationTime : 5/27/2025 2:21:11 PM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        :
```

Import-GPO -BackupGpoName “Default Domain Controllers Policy" -TargetName "DC_Policy2" -Path "C:\GPOs"

```
PS C:\Users\Administrator.DC112> Import-GPO -BackupGpoName "Default Domain Controllers Policy" -TargetName "DC_Policy2" -Path "C:\GPOs"


DisplayName      : DC_Policy2
DomainName       : vlabs12.com
Owner            : VLABS12\Domain Admins
Id               : 7cc4388e-eb69-4701-9da5-ae4312e4518a
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 5/27/2025 2:21:11 PM
ModificationTime : 5/27/2025 2:22:36 PM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 1, SysVol Version: 1
WmiFilter        :
```

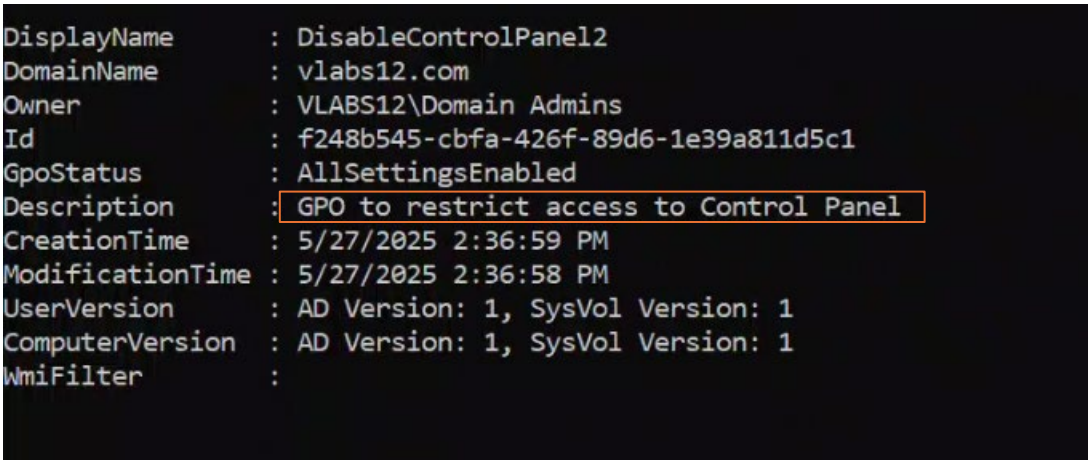
I created another GPO for fun and imported DisableControlPanel since it has a description.

```
PS C:\Users\Administrator.DC112> Import-GPO -BackupGpoName "DisableControlPanel" -TargetName "PS_GPO" -Path "C:\GPOs"


DisplayName      : PS_GPO
DomainName       : vlabs12.com
Owner            : VLABS12\Domain Admins
Id               : d7f18131-7751-4342-a7d0-fc660c52f74d
GpoStatus        : AllSettingsEnabled
Description      : GPO to restrict access to Control Panel
CreationTime     : 5/27/2025 2:12:05 PM
ModificationTime : 5/27/2025 2:15:38 PM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 1, SysVol Version: 1
WmiFilter        :


PS C:\Users\Administrator.DC112>
```

Copy any existing GPO to a new one in the same domain

Copy-GPO -SourceName "DisableControlPanel" -TargetName"DisableControlPanel2"

```
PS C:\Users\Administrator.DC112> Copy-GPO -SourceName "DisableControlPanel" -TargetName "DisableControlPanel2"

DisplayName      : DisableControlPanel2
DomainName       : vlabs12.com
Owner            : VLABS12\Domain Admins
Id               : f248b545-cbfa-426f-89d6-1e39a811d5c1
GpoStatus        : AllSettingsEnabled
Description      : GPO to restrict access to Control Panel
CreationTime     : 5/27/2025 2:36:59 PM
ModificationTime : 5/27/2025 2:36:59 PM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 1, SysVol Version: 1
WmiFilter        :


PS C:\Users\Administrator.DC112> _
```



Task 4: Group Policy Modeling and Results

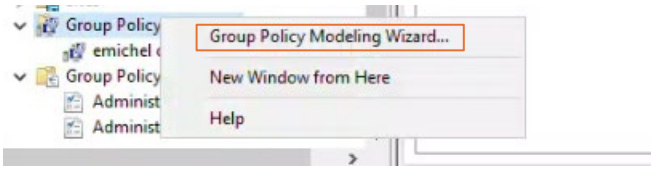
Open Group Policy Management Console.

Use Group Policy Modeling to predict the effect of applied GPOs for a user in HR OU.

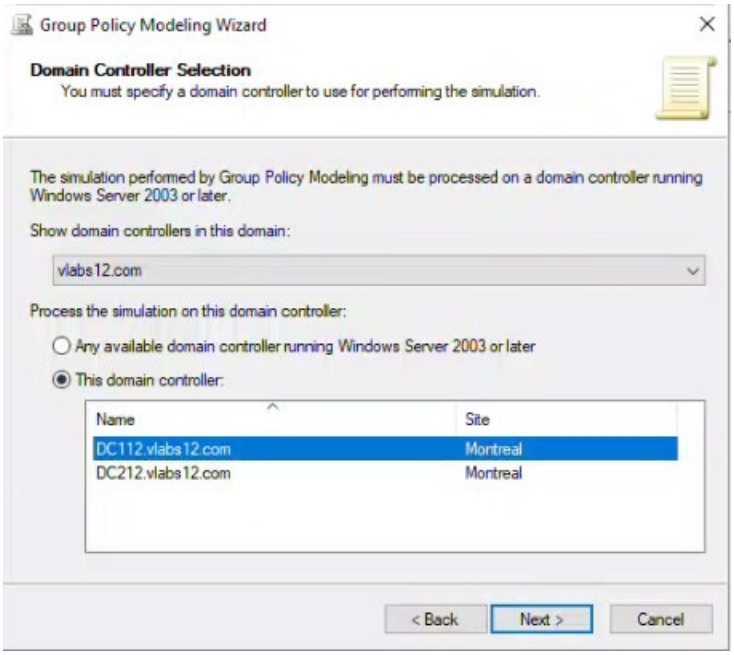
Use Group Policy Results to test the GPOs results on DC112.

We use the Group Policy Management Console to simulate how GPOs will affect a user in the HR organizational unit, to predict the outcome before changes are applied. We'll also use the Group Policy Results tool to see the actual policies applied to a specific computer, which helps confirm and troubleshoot GPO application.

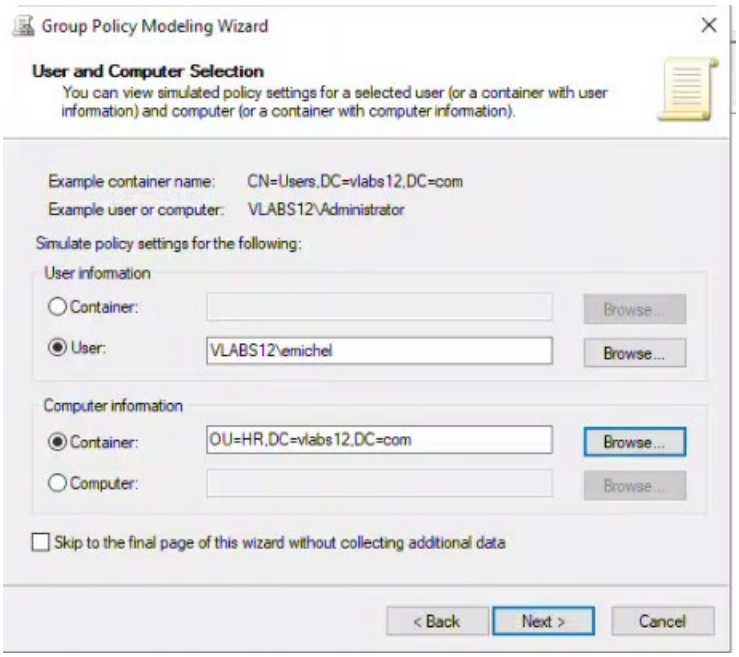
In Group Policy Management, right click on Group Policy Modeling and select the Wizard



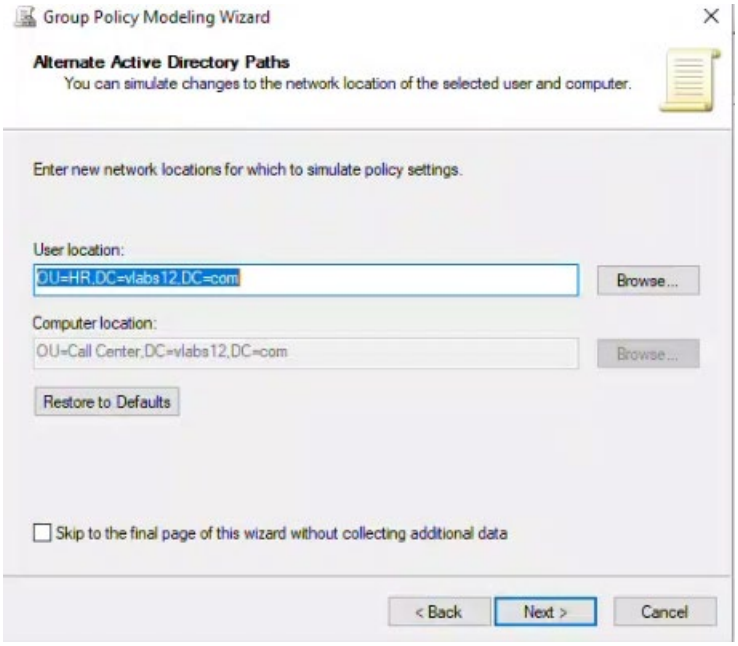
Click on “This domain controller” and select DC112



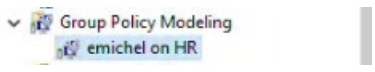
Here select User and “Ethan Michel” in HR



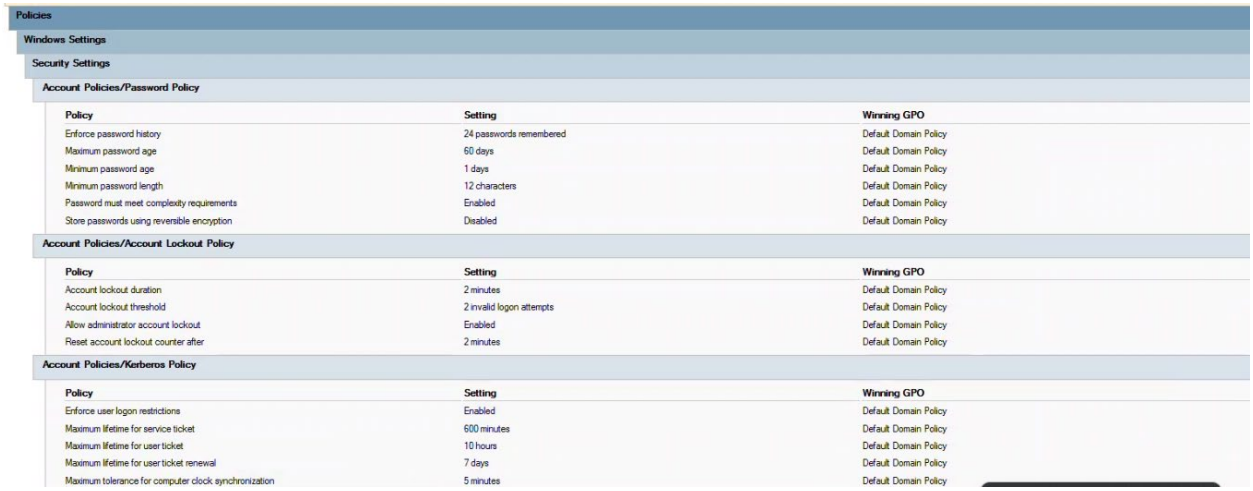
Confirm the location of Ethan Michel



Once the Wizard completes, click on emichel on HR



Below is a generated report of all applied GPOs in HR and their impact on the user Ethan Michel



Policies

Windows Settings

Security Settings

Account Policies/Password Policy

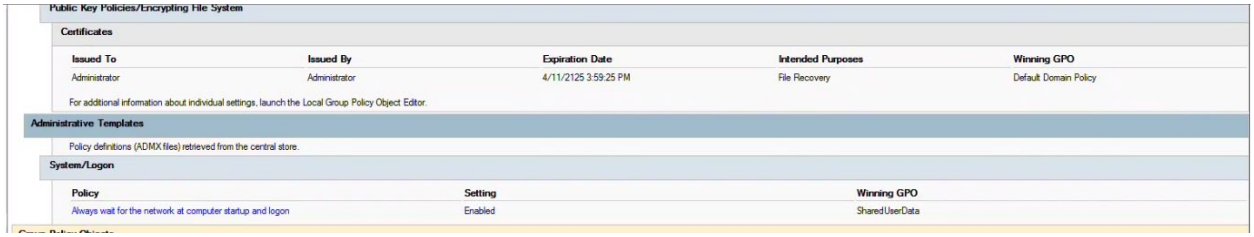
Policy	Setting	Winning GPO
Enforce password history	24 passwords remembered	Default Domain Policy
Maximum password age	60 days	Default Domain Policy
Minimum password age	1 days	Default Domain Policy
Minimum password length	12 characters	Default Domain Policy
Password must meet complexity requirements	Enabled	Default Domain Policy
Store passwords using reversible encryption	Disabled	Default Domain Policy

Account Policies/Account Lockout Policy

Policy	Setting	Winning GPO
Account lockout duration	2 minutes	Default Domain Policy
Account lockout threshold	2 invalid logon attempts	Default Domain Policy
Allow administrator account lockout	Enabled	Default Domain Policy
Reset account lockout counter after	2 minutes	Default Domain Policy

Account Policies/Kerberos Policy

Policy	Setting	Winning GPO
Enforce user logon restrictions	Enabled	Default Domain Policy
Maximum lifetime for service ticket	600 minutes	Default Domain Policy
Maximum lifetime for user ticket	10 hours	Default Domain Policy
Maximum lifetime for user ticket renewal	7 days	Default Domain Policy
Maximum tolerance for computer clock synchronization	5 minutes	Default Domain Policy



Public Key Policies/Encrypting File System

Certificates

Issued To	Issued By	Expiration Date	Intended Purposes	Winning GPO
Administrator	Administrator	4/11/2125 3:59:25 PM	File Recovery	Default Domain Policy

For additional information about individual settings, launch the Local Group Policy Object Editor.

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

System/Logon

Policy	Setting	Winning GPO
Always wait for the network at computer startup and logon	Enabled	SharedUserData

Default Domain Policy [{31B2F340-016D-11D2-945F-00C04FB984F9}]

Link Location	vlabs12.com
Extensions Configured	{B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A} Security Registry
Enforced	No
Disabled	None
Security Filters	VLABS12\Enterprise Admins VLABS12\Domain Admins NT AUTHORITY\Authenticated Users
Revision	AD (59), SYSVOL (59)
WMI Filter	

SharedUserData [{AD4BD592-A258-4A5F-B948-05AF3BBD4993}]

Link Location	vlabs12.com/HR
Extensions Configured	Registry
Enforced	Yes
Disabled	None
Security Filters	NT AUTHORITY\Authenticated Users
Revision	AD (1), SYSVOL (1)
WMI Filter	

Denied GPOs

Policies

Windows Settings

Scripts

Logon

Name	Parameters	Last Run	Script Order in GPO	Winning GPO
MapDrive.bat			Not configured	Public_Share

Folder Redirection

Desktop

Winning GPO	SharedUserData

Setting: Basic (Redirect everyone's folder to the same location)

Path: \\DC312\UserData\%USERNAME%\Desktop

Options

Grant user exclusive rights to Desktop	Enabled
Move the contents of Desktop to the new location	Enabled
Also apply redirection policy to Windows 2000, Windows 2000 server, Windows XP, and Windows Server 2003 operating systems	Disabled
Policy Removal Behavior	Leave contents
Configuration Control	Group Policy
Primary Computer Evaluation	Primary computer, redirection configuration applied

Documents

Winning GPO	SharedUserData

Setting: Basic (Redirect everyone's folder to the same location)

Path: \\DC312\UserData\%USERNAME%\Documents

Applied GPOs

DisableControlPanel [{BF22A630-BE15-4DE8-B03E-B7D0ED246908}]

Link Location	vlabs12.com/HR
Extensions Configured	Registry
Enforced	No
Disabled	None
Security Filters	NT AUTHORITY\Authenticated Users
Revision	AD (1), SYSVOL (1)
WMI Filter	

Public_Share [{F10326CC-9BEE-4E2A-99BE-D01C49F766CF}]

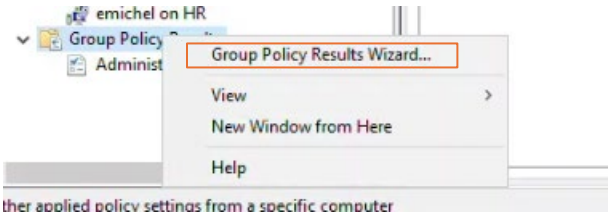
Link Location	vlabs12.com
Extensions Configured	Scripts
Enforced	No
Disabled	None
Security Filters	NT AUTHORITY\Authenticated Users
Revision	AD (2), SYSVOL (2)
WMI Filter	

SharedUserData [{AD4BD592-A258-4A5F-B948-05AF3BBD4993}]

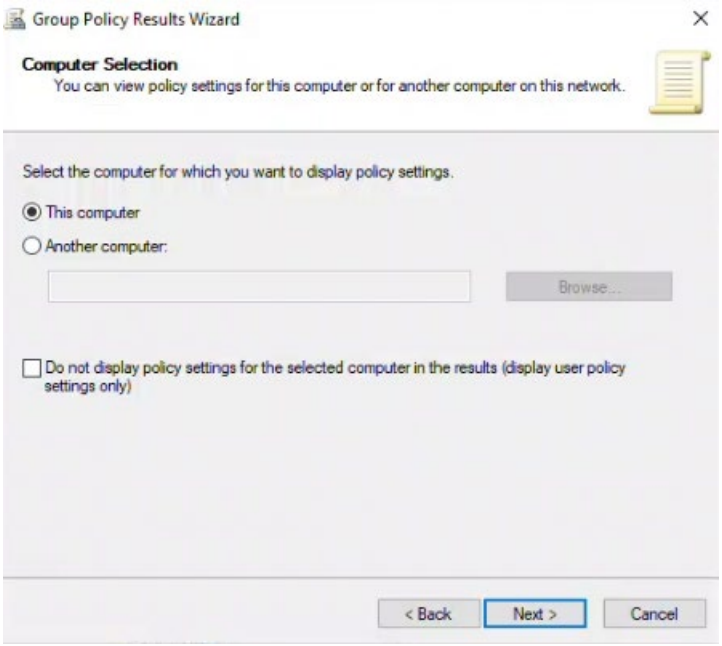
Link Location	vlabs12.com/HR
Extensions Configured	Folder Redirection
Enforced	Yes
Disabled	None
Security Filters	NT AUTHORITY\Authenticated Users
Revision	AD (2), SYSVOL (2)
WMI Filter	

Denied GPOs

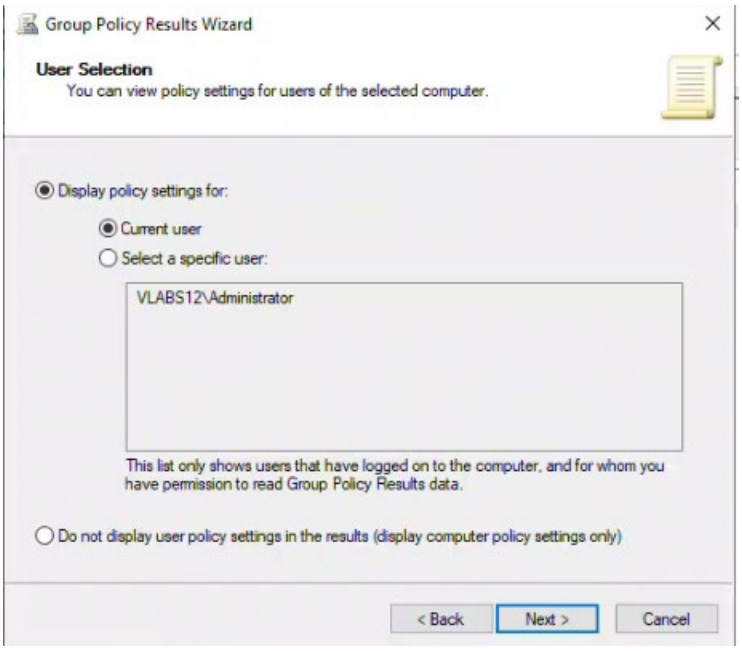
Use Group Policy Results to test the GPOs results on DC112

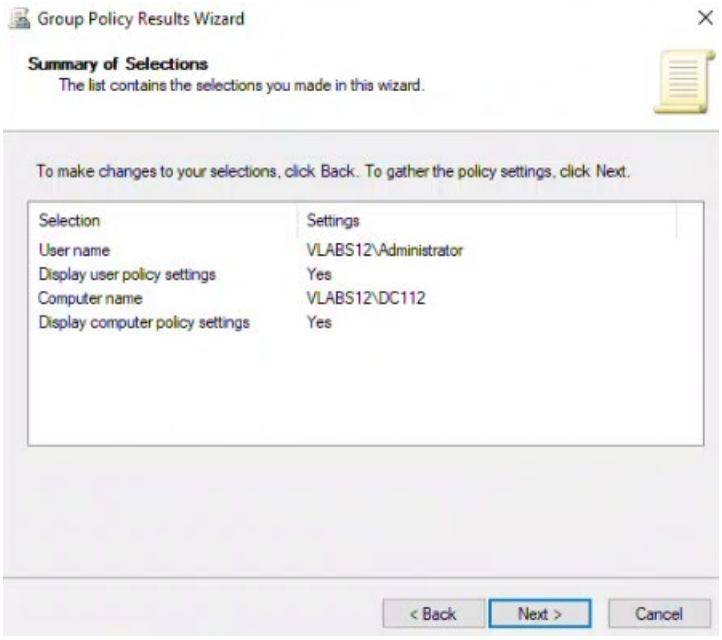


Select this computer

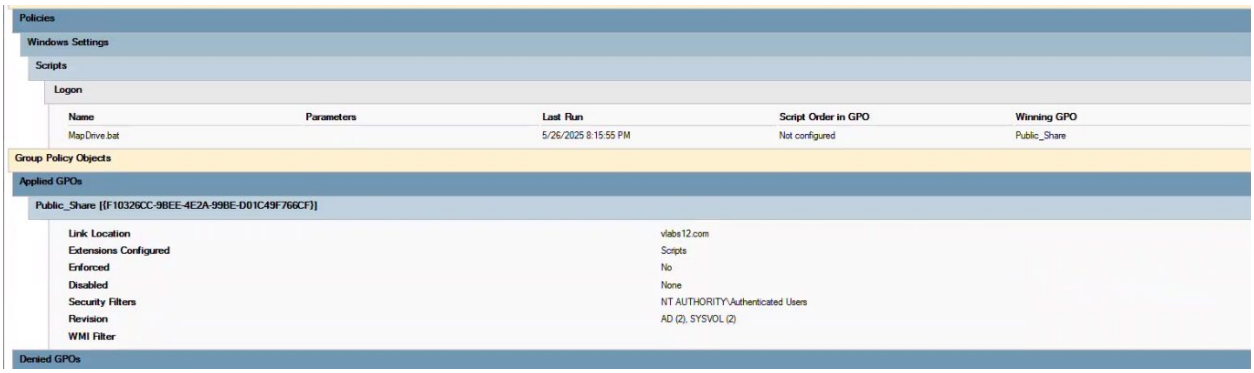


Current user : Admin





Same as Ethan Michel above, this is a generated report of the applied GPOs on DC112 and Administrator



Task 5: Delegating GPO Management

On DC112:

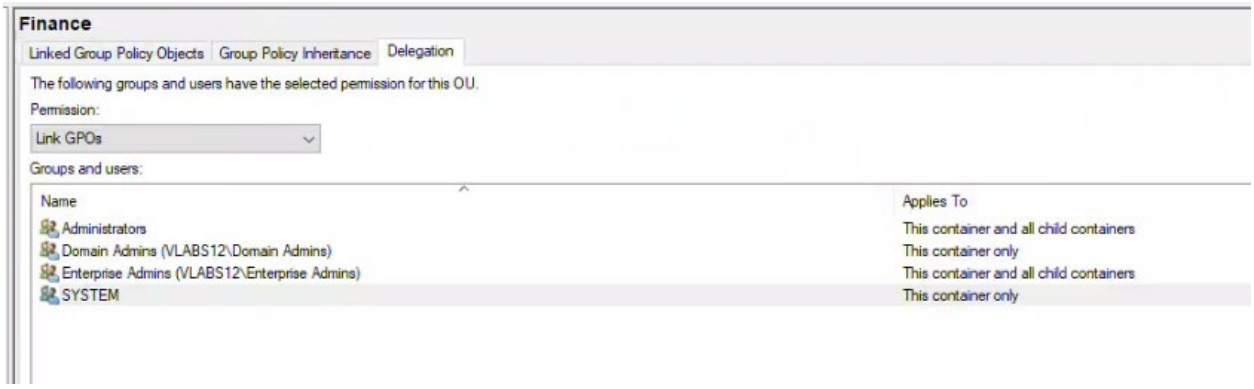
Delegate Lina Gaillard on Finance OU to be able to Edit and Link any GPO to the Finance OU

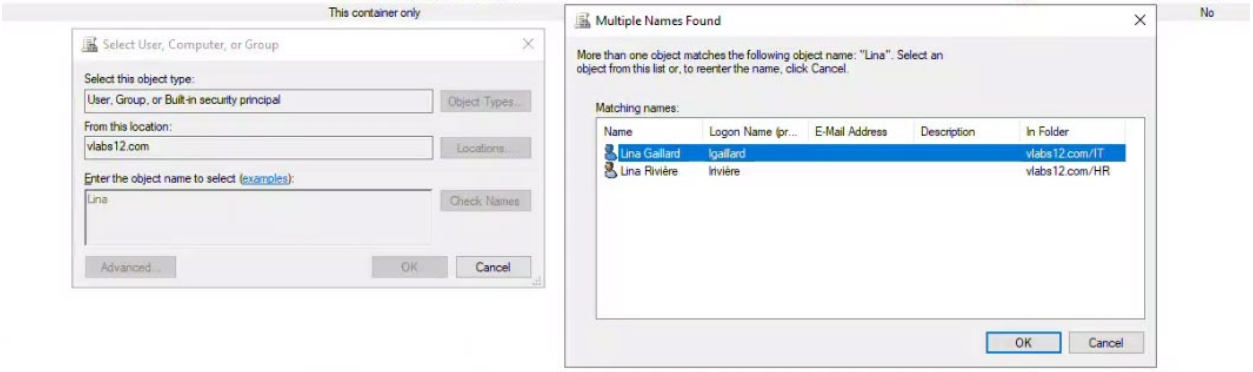
No need to test it.

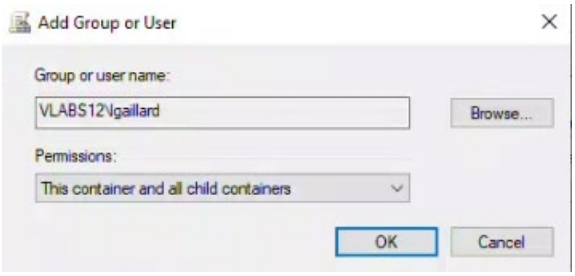
Assign the necessary permissions to another user so they can edit and link GPOs for the Finance OU. This allows us to delegate GPO administration securely and ensure that only authorized users can make changes to policies in specific parts of the organization.

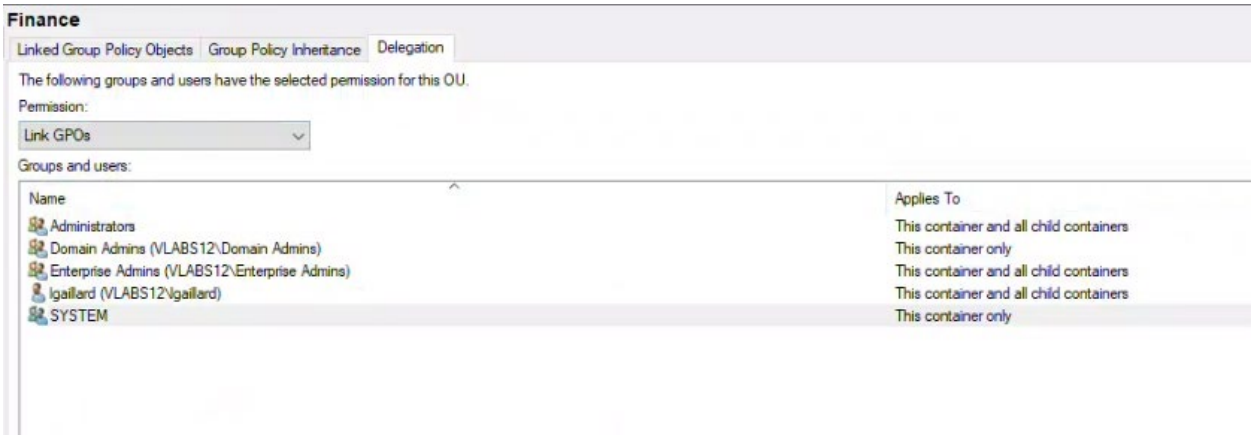
Select Finance and go to the Delegation tab. In the Permissions drop-down menu, delect Link GPOs

Give Lina Gaillard permission to link GPOs, ensuring she has permissions for this container and all child containers


Finance
Linked Group Policy Objects
Group Policy Inheritance
Delegation
The following groups and users have the selected permission for this OU.
Permission:
Link GPOs
Groups and users:
Name
Applies To
Administrators
This container and all child containers
Domain Admins (VLABS12\Domain Admins)
This container only
Enterprise Admins (VLABS12\Enterprise Admins)
This container and all child containers
SYSTEM
This container only


This container only
No
Select User, Computer, or Group
Select this object type:
User, Group, or Built-in security principal
Object Types...
From this location:
vlabs12.com
Locations...
Enter the object name to select (examples):
Lina
Check Names
Advanced...
OK
Cancel
Multiple Names Found
More than one object matches the following object name: "Lina". Select an object from this list or, to reenter the name, click Cancel.
Matching names:
Name
Logon Name (pr...
E-Mail Address
Description
In Folder
Lina Gaillard
lgaillard
vlabs12.com/IT
Lina Rivière
lrivière
vlabs12.com/HR
OK
Cancel


Add Group or User
Group or user name:
VLABS12\lgaillard
Browse...
Permissions:
This container and all child containers
OK
Cancel


Finance
Linked Group Policy Objects
Group Policy Inheritance
Delegation
The following groups and users have the selected permission for this OU.
Permission:
Link GPOs
Groups and users:
Name
Applies To
Administrators
This container and all child containers
Domain Admins (VLABS12\Domain Admins)
This container only
Enterprise Admins (VLABS12\Enterprise Admins)
This container and all child containers
lgaillard (VLABS12\lgaillard)
This container and all child containers
SYSTEM
This container only

When it comes to Edit permissions, the only option I found was to give her Edit permissions within each individual GPO in the Finance OU.