



This lab is designed to configure and test advanced Group Policy Objects (GPOs) in a domain environment.

Lab Assignment 2 (Part II) - GPO

420-636-AB-Network Installation and Administration II

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

Table of Contents

1	Lab Objective	4
2	Lab Environment Requirements.....	4
3	Task 1: Creating a Central Store for Administrative Templates	4
3.1	Objective.....	4
3.2	Steps	4
3.2.1	DC101	4
4	Task 2: Managing and Configuring Administrative Templates.....	8
4.1	Objective.....	8
4.2	Steps	8
4.2.1	DC101	8
4.2.2	Client1.....	16
5	Task 3: Managing Account Policies	18
5.1	Objective.....	18
5.2	Steps	18
5.2.1	DC101	18
5.2.2	Client1.....	22
6	Task 4: Implementing Fine-Grained Password Policies	28
6.1	Objective.....	28
6.2	Steps	28
6.3	DC101	29
6.4	Client1.....	31
7	Task 5: Managing Audit Authentication.....	34
7.1	Objective.....	34
7.2	Steps	34
7.2.1	DC101	34
7.2.2	Client1.....	36
8	Task 6: Managing Security Templates	48
8.1	Objective:.....	49
8.2	Steps	49
9	Task 7: Configuring Folder Redirection	56
9.1	Objective.....	56
9.2	Steps	56
9.2.1	Prepare File Server (DC301).....	56
9.2.2	Create Folder Redirection GPO (DC101).....	59

9.2.3	Configure Documents Redirection (DC101).....	60
9.3	Link GPO to HR OU (DC101)	65
9.4	Apply and Test.....	68
9.4.1	Verify HR users (DC101).....	68
9.4.2	Client1.....	69
10	Task 8: Managing Software Installation.....	76
10.1	Objective:.....	76
10.2	Steps	76
10.2.1	Prepare Software Distribution Point.....	76
10.2.2	Create Software Installation GPO in DC101	81
10.2.3	Link GPO to Engineering OU (DC101).....	83
10.2.4	Apply– Client1.....	84
10.2.5	Verify Teams installation:.....	85
11	Task 9: Managing Scripts with GPO	87
11.1	Objective	88
11.2	Steps	88
11.2.1	1. Prepare Shared Folder on DC301	88
11.2.2	Create Logon Script.....	89
11.2.3	Configure GPO for Script Deployment (DC101)	92
11.2.4	Link GPO to Domain Level	93
11.2.5	Force Policy Update:	94
11.2.6	Verification Testing	94

Lab Assignment 2 (Part II) - GPO

1 Lab Objective

This lab is designed to **configure and test advanced Group Policy Objects (GPOs)** in a domain environment. Students will work with Administrative Templates, security policies, folder redirection, software installation, and scripts.

The lab will focus on implementing these configurations, linking them to appropriate OUs, and verifying their impact.

2 Lab Environment Requirements

- **DC101:** Domain Controller with Active Directory, DNS, and Group Policy Management installed.
- **Client1:** Windows 11 client machine joined the domain.
- **DC301:** File Server for folder sharing.

3 Task 1: Creating a Central Store for Administrative Templates

3.1 Objective

Create a centralized ADMX/ADML repository for vlabs1.com domain to ensure consistent Group Policy administration.

3.2 Steps

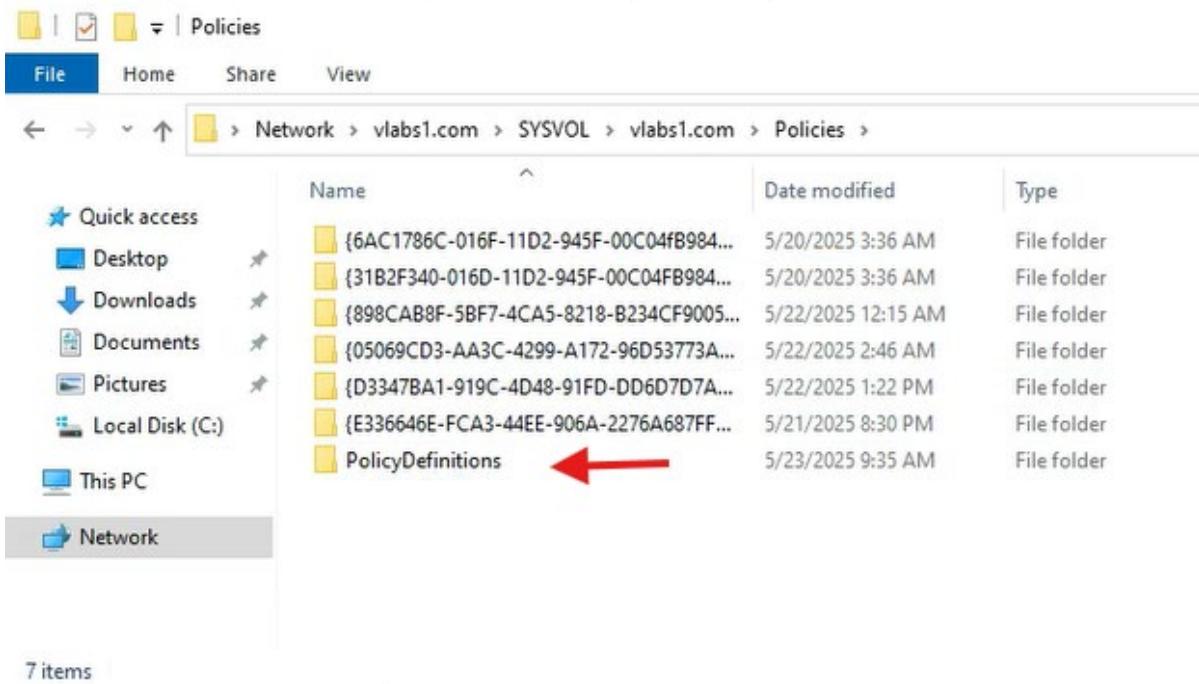
- Create a **central store** for Administrative Templates on **DC101**.
- Copy all **ADMX** and **ADML** files to this Central store.
- Verify that **Group Policy Management Console (GPMC)** loads templates from the **central store**.

3.2.1 DC101

Create the Central Store Directory

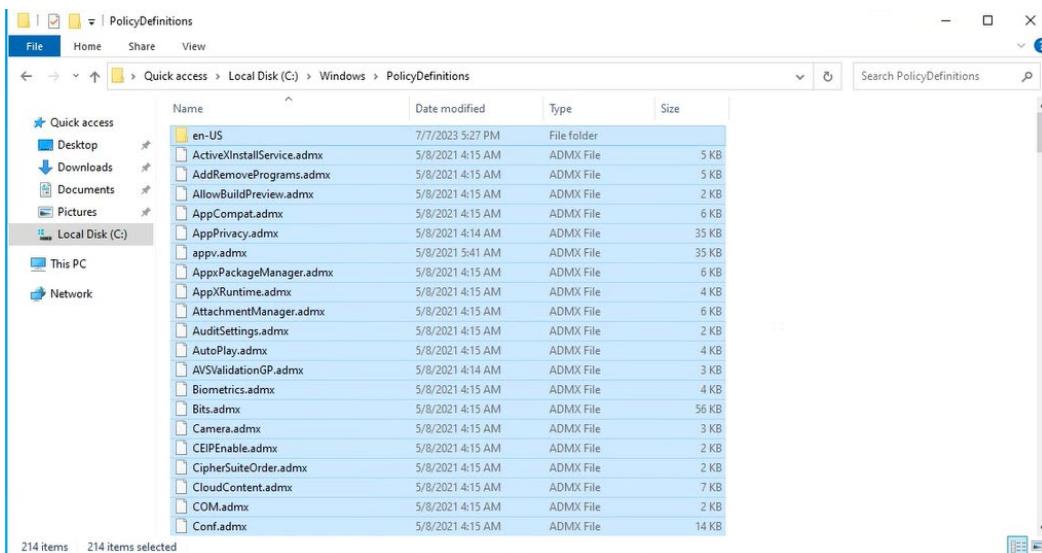
1. On DC101 (Domain Controller):

- Open **File Explorer** and navigate to:
to:\\vlabs1.com\\SYSVOL\\vlabs1.com\\Policies
- **Right-click → New → Folder**
Name it: "**PolicyDefinitions**"
(This becomes your Central Store)



2. Copy ADMX/ADM1 Files

- On DC101, open: C:\Windows\PolicyDefinitions
- Select all files:
 - ADMX files (e.g., WindowsDefender.admx)
 - ADM1 folders (e.g., en-US for English)
- Copy to: \\vlabs1.com\SYSVOL\vlabs1.com\Policies\PolicyDefinitions
(Include all language folders you need)



Name	Date modified	Type	Size
en-US	5/23/2025 10:06 AM	File folder	
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
Camera.admx	5/8/2021 4:15 AM	ADMX File	3 KB
CEIPEnable.admx	5/8/2021 4:15 AM	ADMX File	2 KB
CipherSuiteOrder.admx	5/8/2021 4:15 AM	ADMX File	2 KB
CloudContent.admx	5/8/2021 4:15 AM	ADMX File	7 KB
COM.admx	5/8/2021 4:15 AM	ADMX File	2 KB
Conf.admx	5/8/2021 4:15 AM	ADMX File	14 KB
ControlPanel.admx	5/8/2021 4:15 AM	ADMX File	4 KB
ControlPanelDisplay.admx	5/8/2021 4:15 AM	ADMX File	15 KB
Cpls.admx	5/8/2021 4:15 AM	ADMX File	2 KB
CredentialProviders.admx	5/8/2021 4:15 AM	ADMX File	5 KB
CredSsp.admx	5/8/2021 4:15 AM	ADMX File	14 KB
CredUI.admx	5/8/2021 4:15 AM	ADMX File	3 KB
CtrlAltDel.admx	5/8/2021 4:15 AM	ADMX File	3 KB
DataCollection.admx	5/8/2021 4:15 AM	ADMX File	15 KB
DCOM.admx	5/8/2021 4:15 AM	ADMX File	3 KB
DeliveryOptimization.admx	5/8/2021 4:14 AM	ADMX File	37 KB
Desktop.admx	5/8/2021 4:15 AM	ADMX File	14 KB
DeviceCompat.admx	5/8/2021 4:15 AM	ADMX File	2 KB
DeviceCredential.admx	5/8/2021 4:15 AM	ADMX File	2 KB
DeviceGuard.admx	5/8/2021 4:14 AM	ADMX File	6 KB

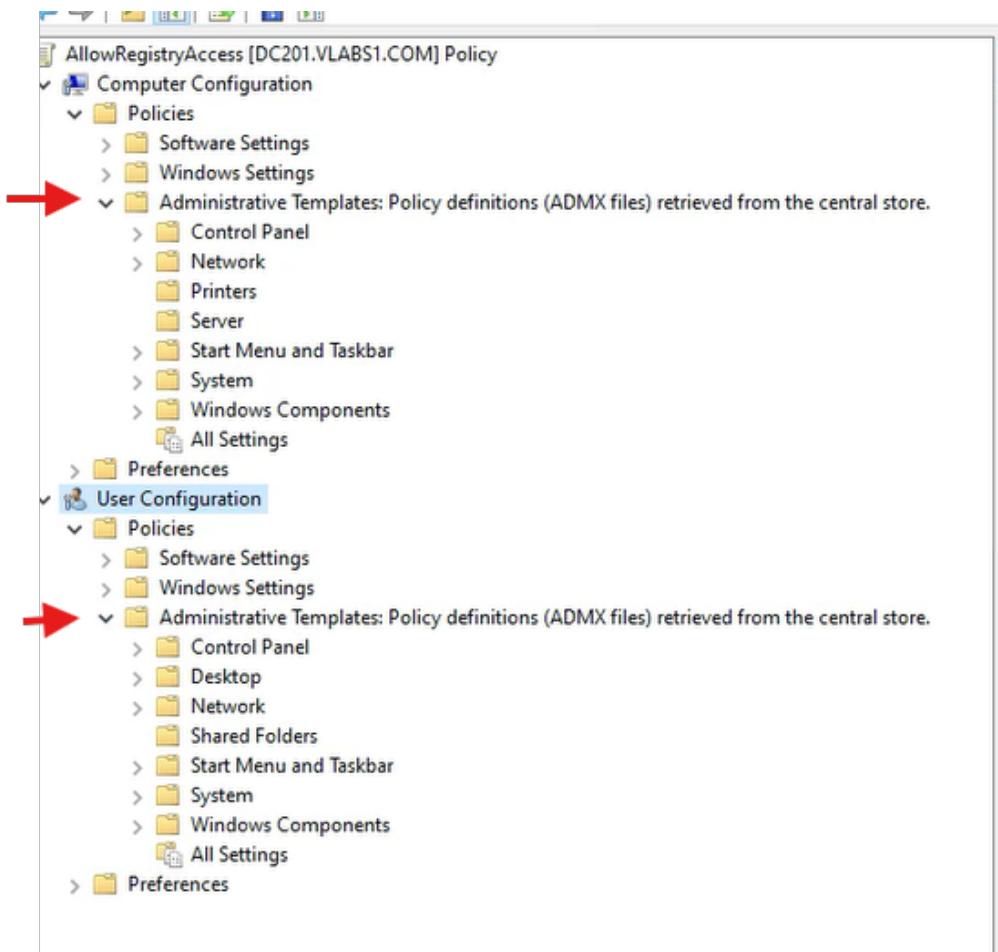
3. Verify Central Store

a) On DC101:

- Open **GPMC** (gpmc.msc)
- Edit any GPO → Navigate to:
Computer Configuration → Policies → Administrative Templates

b) Confirmation:

- No warning about "local ADMX files" appears
- Right-click "Administrative Templates" → **View** → Verify:
"PolicyDefinitions (ADMX files) retrieved from the Central Store"



Item	Path
Source ADMX Files	C:\Windows\PolicyDefinitions
Central Store	\\\vlab1.com\SYSVOL\vlab1.com\Policies\PolicyDefinitions
Language Files	PolicyDefinitions\en-US (or other language codes)

4 Task 2: Managing and Configuring Administrative Templates

4.1 Objective

Configure Office Administrative Templates to restrict Microsoft Teams auto-start behavior for Engineering OU users.

4.2 Steps

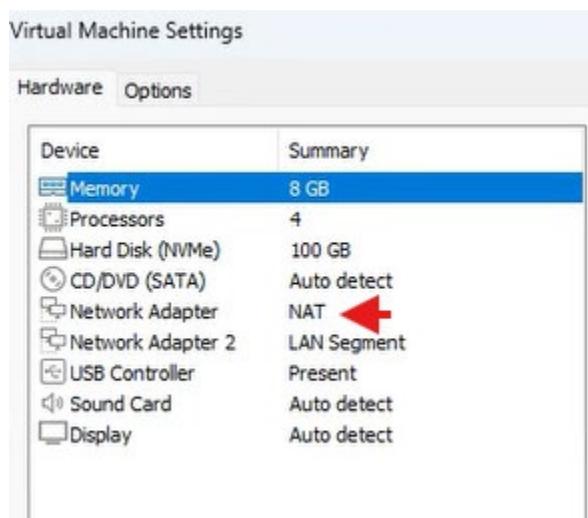
- Download and install **Microsoft Office Administrative Templates** (*You will need to add the NAT NIC to download this package. Remove it after completing the download.*)
- Create a new GPO named **RestrictTeamsStarting**.
- Use **Filter Options for User Configuration** to locate **Microsoft Teams 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.

4.2.1 DC101

1. Download Microsoft Office Administrative Templates

a) On DC101 (Domain Controller):

- Temporarily **enable NAT NIC** for internet access
- Download latest Office ADMX templates from:
<https://www.microsoft.com/en-us/download/details.aspx?id=49030>
- **Disable NAT NIC** after download completes (for security)



A screenshot of a Microsoft browser window displaying the Microsoft 365 landing page. The page features a large "Achieve the extraordinary" headline and a "Shop Microsoft 365" button. To the right is a graphic of various Microsoft Office app icons (Word, Excel, PowerPoint, etc.) floating. At the top, there's a cookie consent banner and a navigation bar with links like Windows, Office, Web browsers, Developer tools, and Xbox.

Administrative Template files (ADMX/ADML) for Microsoft Office

This download includes the Group Policy Administrative Template files (ADMX/ADML) for Microsoft 365 Apps for enterprise, Office LTSC 2024, Office LTSC 2021, Office 2019, and Office 2016 and also includes the OPAX/OPAL files for the Office Customization Tool (OCT) for Office 2016.

Important! Selecting a language below will dynamically change the complete page content to that language.

Select language

English

Download

Activate Windows
Go to Settings to activate Windows.

A screenshot of the Microsoft Download Center showing the details page for the administrative template files. It includes sections for "Details" (Version: 5497.1000, Date Published: 3/28/2025, File Name: admintemplates_x64_5497.1000_en-us.exe, File Size: 12.7 MB; admintemplates_x86_5497.1000_en-us.exe, File Size: 12.5 MB), "System Requirements", and "Install Instructions". A "Collapse all" link is at the top left. An "Expand all" link is at the bottom left. An "Activate Windows" link is at the bottom right.

✓ System Requirements

Supported Operating Systems
Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, Windows Server 2022

Note: Refer to the [System requirements for Office](#) to see the supported operating systems for specific versions of Office.

The Administrative Template files (ADMX/ADML) in this download work with the following Office programs:

- Microsoft 365 Apps for enterprise.
- Desktop versions of Project and Visio that come with subscription plans.
- Volume licensed versions of Office LTSC 2024, Project 2024, and Visio LTSC 2024. For example, Office LTSC Professional Plus 2024, Project Standard 2024, and Visio LTSC Professional 2024.
- Volume licensed versions of Office LTSC 2021, Project 2021, and Visio LTSC 2021. For example, Office LTSC Professional Plus 2021, Project Standard 2021, and Visio LTSC Professional 2021.
- Volume licensed versions of Office 2019, Project 2019, and Visio 2019. For example, Office Standard 2019 and Visio Professional 2019.
- Volume licensed versions of Office 2016, Project 2016, and Visio 2016. For example, Office Professional Plus 2016 and Project Standard 2016.

The Office Customization Tool (OPAX/OPAL) files provided in this download only work with volume licensed versions of Office 2016, Project 2016, and Visio 2016. For example, Office Professional Plus 2016 and Project Standard 2016.

Install Instructions

To download and extract the ADMX/ADML and OPAX/OPAL files:

1. Click the **Download** button (above) and choose whether you want to download the 32-bit (x86) or 64-bit (x64) files, or both. For example, if you're using the Office Customization Tool (OCT) to customize installations of the 64-bit version of Office, download the 64-bit (x64) files. If you just need the ADMX/ADML files, you can download either the 32-bit (x86) or 64-bit (x64) files. The ADMX/ADML files are the same for both.
2. Click **Next** and choose where to save the files.
3. Go to the location where you saved the downloaded files, and double-click the admintemplates executable (.exe) file, and follow the instructions to extract the files to a location of your choosing.

If you have Windows Server and Active Directory Domain Services (AD DS) deployed in your organization, you can configure settings for Office by using Group Policy. Copy the ADMX/ADML files to your AD DS environment and then use the Group Policy Management administrative tool to configure the Group Policy settings for Office.

If you're using the Office Customization Tool (OCT), copy the Admin folder with the OPAX/OPAL files into the folder that contains your Office installation files. For more information about the OCT, see [Office Customization Tool \(OCT\) 2016 Help: Overview](#).

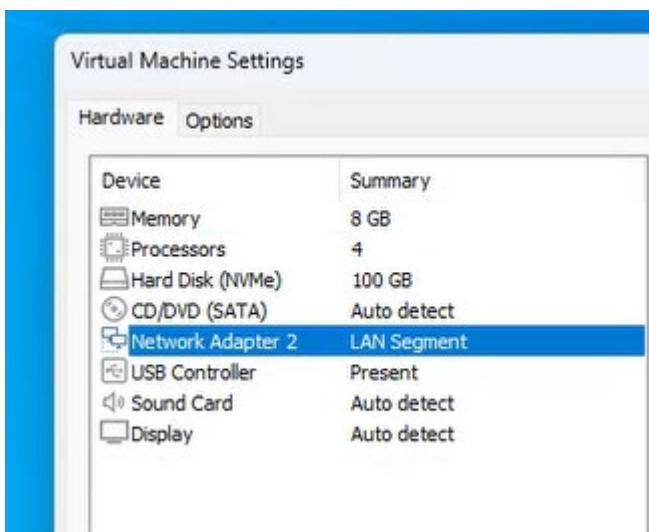
Choose the download you want

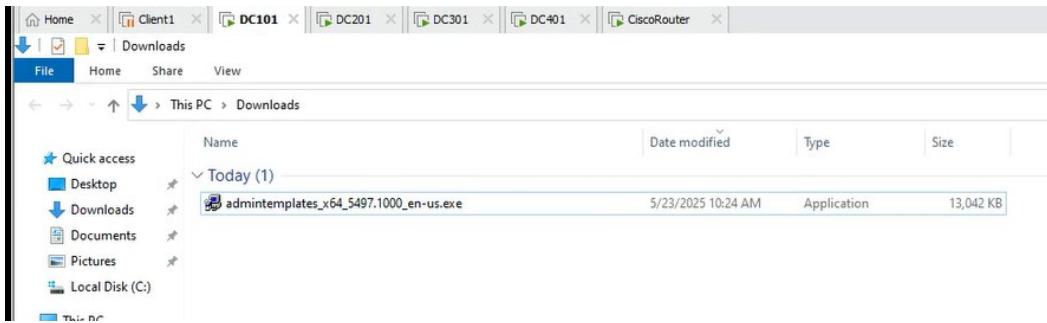
X

<input type="checkbox"/> File Name	Size
<input checked="" type="checkbox"/> admintemplates_x64_5497.1000_en-us.exe	12.7 MB
<input type="checkbox"/> admintemplates_x86_5497.1000_en-us.exe	12.5 MB

Download

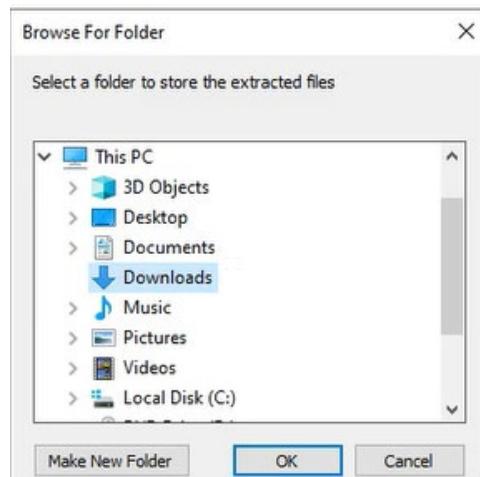
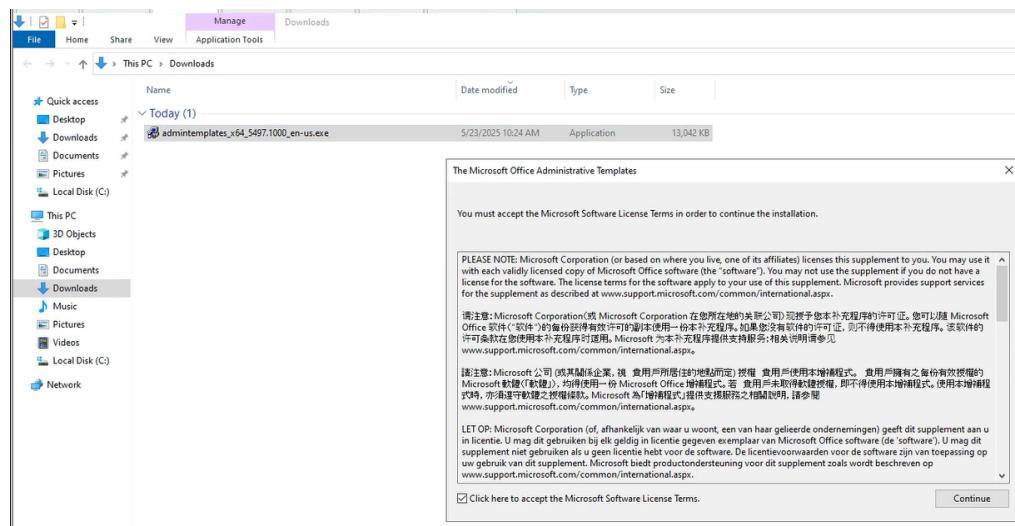
Total size: 12.7 MB

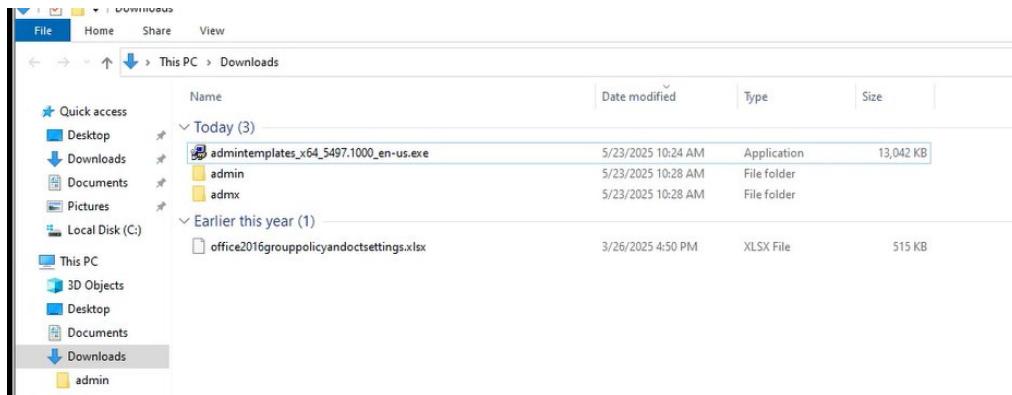




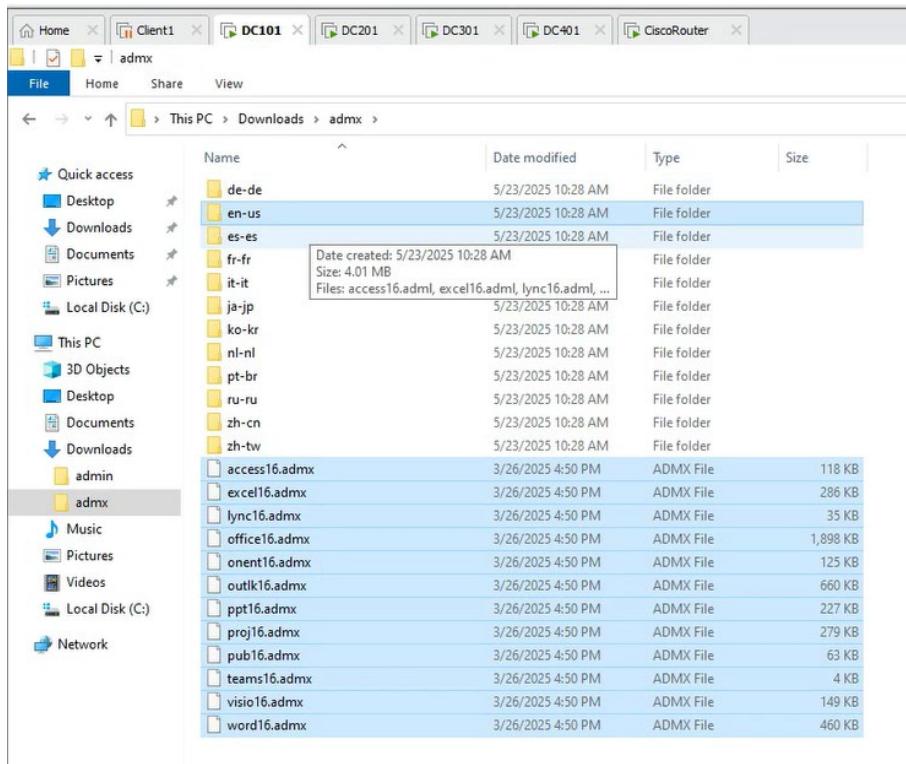
b) Extract and Install Templates:

- o Unzip downloaded package
- o Copy contents to Central Store:
\\vlabs1.com\SYSVOL\vlabs1.com\Policies\PolicyDefinitions
- o Ensure all .admx files and language folders (e.g., en-US) are copied





Open admx and select files and en-us folder



File Home Share View

← → ↑ ↓ Network > Network > vlab1.com > SYSVOL > vlab1.com > Policies > PolicyDefinitions >

Name Date modified Type Size

Quick access

- Desktop
- Downloads
- Documents
- Pictures
- Local Disk (C:)
- PolicyDefinitions
- This PC
- Network

en-US

Name	Date modified	Type	Size
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
Camera.admx	5/8/2021 4:15 AM	ADMX File	3 KB
CEIPEnable.admx	5/8/2021 4:15 AM	ADMX File	2 KB
CipherSuiteOrder.admx	5/8/2021 4:15 AM	ADMX File	2 KB
CloudContent.admx	5/8/2021 4:15 AM	ADMX File	7 KB
COM.admx	5/8/2021 4:15 AM	ADMX File	2 KB
Conf.admx	5/8/2021 4:15 AM	ADMX File	14 KB
ControlPanel.admx	5/8/2021 4:15 AM	ADMX File	4 KB
ControlPanelDisplay.admx	5/8/2021 4:15 AM	ADMX File	15 KB
CplIs.admx	5/8/2021 4:15 AM	ADMX File	2 KB
CredentialProviders.admx	5/8/2021 4:15 AM	ADMX File	5 KB
CredSep.admx	5/8/2021 4:15 AM	ADMX File	14 KB
CredUI.admx	5/8/2021 4:15 AM	ADMX File	3 KB
CtrlAltDel.admx	5/8/2021 4:15 AM	ADMX File	3 KB
DataCollection.admx	5/8/2021 4:15 AM	ADMX File	15 KB
DCOM.admx	5/8/2021 4:15 AM	ADMX File	3 KB
DeliveryOptimization.admx	5/8/2021 4:14 AM	ADMX File	37 KB
Desktop.admx	5/8/2021 4:15 AM	ADMX File	14 KB
DeviceCompat.admx	5/8/2021 4:15 AM	ADMX File	2 KB
DeviceCredential.admx	5/8/2021 4:15 AM	ADMX File	2 KB

226 items 1 item selected

Copy in local too

File Home Share View

← → ↑ ↓ Quick access > Local Disk (C) > Windows > PolicyDefinitions

Name Date modified Type Size

Quick access

- Desktop
- Downloads
- Documents
- Pictures
- Local Disk (C:)
- PolicyDefinitions
- This PC
- Network

en-US

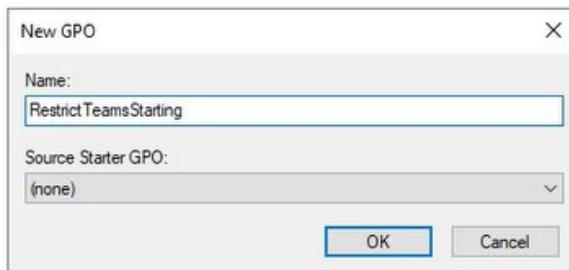
Name	Date modified	Type	Size
access16.admx	5/23/2025 10:40 AM	File folder	
ActiveXInstallService.admx	5/8/2021 4:15 AM	ADMX File	118 KB
AddRemovePrograms.admx	5/8/2021 4:15 AM	ADMX File	5 KB
AllowBuildPreview.admx	5/8/2021 4:15 AM	ADMX File	2 KB
AppCompat.admx	5/8/2021 4:15 AM	ADMX File	6 KB
AppPrivacy.admx	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
Camera.admx	5/8/2021 4:15 AM	ADMX File	3 KB
CEIPEnable.admx	5/8/2021 4:15 AM	ADMX File	2 KB
CipherSuiteOrder.admx	5/8/2021 4:15 AM	ADMX File	2 KB
CloudContent.admx	5/8/2021 4:15 AM	ADMX File	7 KB
COM.admx	5/8/2021 4:15 AM	ADMX File	2 KB

226 items

2. Create and Configure RestrictTeamsStarting GPO

a) In GPMC (gpmc.msc):

- o Right-click **Group Policy Objects** → **New**
- o Name: **RestrictTeamsStarting** → Click **OK**



b) Edit the GPO:

- o Right-click → **Edit**
- o Navigate to: User Configuration → Policies → Administrative Templates → Microsoft Teams

c) Configure Policy Setting:

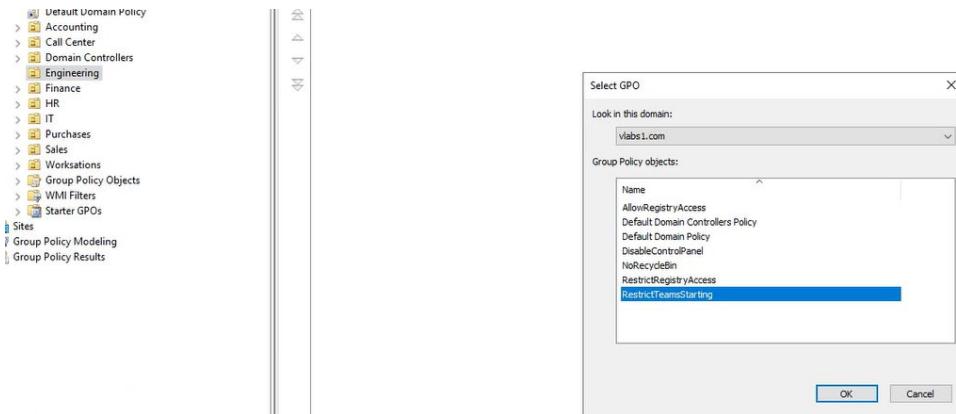
- o Locate: "**Prevent Microsoft Teams from starting automatically after installation**"
- o Set to: **Enabled**
- o Add **Comment**:
Prevents Teams auto-start to improve login performance for Engineering users. Applied 2023-11-15.

Setting	State	Comment
<input checked="" type="checkbox"/> Restrict sign in to Teams to accounts in specific tenants	Not configured	No
<input checked="" type="checkbox"/> Prevent Microsoft Teams from starting automatically after installation	Enabled	Yes

3. Link GPO to Engineering OU

a) In GPMC:

- o Right-click **Engineering OU** → **Link an Existing GPO**
- o Select **RestrictTeamsStarting** → Click **OK**



b) Verify Link Order:

- o Ensure no conflicting policies have higher precedence

1. View Linked GPOs

- o In the "**Linked Group Policy Objects**" tab, you'll see a list of GPOs applied to the Engineering OU.
- o **Higher precedence = Lower link number** (e.g., GPO with **Link Order 1** applies first and can override GPOs below it).

Engineering							
Linked Group Policy Objects		Group Policy Inheritance		Delegation			
Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	<input checked="" type="checkbox"/> RestrictTeamsStarting	No	Yes	Enabled	None	5/23/2025 10:52:16 AM	vlabs1.com

2. Ensure **RestrictTeamsStarting** is Not Overridden

2. Check GPO Inheritance & Enforcement

Engineering				
Linked Group Policy Objects		Group Policy Inheritance	Delegation	
This list does not include any GPOs linked to sites. For more details, see Help.				
Precedence	GPO	Location	GPO Status	WMI Filter
1	Restrict TeamStarting	Engineering	Enabled	None
2	Default Domain Policy	vlabs1.com	Enabled	None

To be tested in **Task 8 Managing Software Installation task**

4.2.2 Client1

1. Force Policy Application

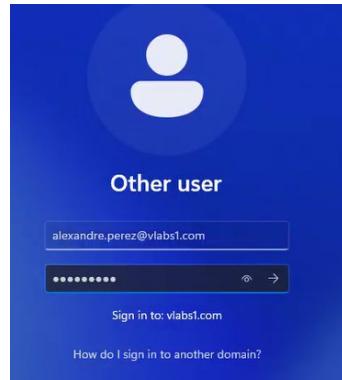
a) On Client1 (Windows 11 test machine):

1. Log in as Engineering OU user
2. Open Command Prompt as Administrator:
gpupdate /force
3. Wait for confirmation: "User Policy update has completed successfully"

Verify users in engineering

The screenshot shows the Active Directory Administrative Center interface. The left navigation pane includes 'Active Directory...', 'Overview', and 'vlabs1 (local)' which is currently selected. Under 'vlabs1 (local)', there are sections for 'Engineering', 'Finance\Finance-Admins', and 'Finance'. The 'Engineering' section is expanded, showing a list of 26 users. The users are listed in a table with columns 'Name' and 'Type'. All entries are 'User' type. The names listed are: Agathe Bonnet, Alexandre Perez, Anaelle Vincent, Antoine Jacquet, Benoit Carr, Callista Boyer, Clea Gauthier, Eliot Fernandez, Elo Roussel, Engineering (Group), Gabin Prevost, Gabriel Lefebvre, Heloise Marie, Ines Robert, Isaac Besson, Leny Leblanc, Leonie Lucas, Loanne Girard, and Mario Caron.

Name	Type
Agathe Bonnet	User
Alexandre Perez	User
Anaelle Vincent	User
Antoine Jacquet	User
Benoit Carr	User
Callista Boyer	User
Clea Gauthier	User
Eliot Fernandez	User
Elo Roussel	User
Engineering	Group
Gabin Prevost	User
Gabriel Lefebvre	User
Heloise Marie	User
Ines Robert	User
Isaac Besson	User
Leny Leblanc	User
Leonie Lucas	User
Loanne Girard	User
Mario Caron	User



```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\alexandre.perez> gpupdate /force
Updating policy...

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

PS C:\Users\alexandre.perez>

```

b) Policy Result Verification:

1. Run:
gpresult /r
2. Confirm RestrictTeamsStarting GPO appears under "Applied Group Policy Objects"

```

PS C:\Users\alexandre.perez> gpresult /r
Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© Microsoft Corporation. All rights reserved.

Created on 2025-05-23 at 12:34:21 PM

RSOP data for VLABS1\alexandre.perez on CLIENT1 : Logging Mode
-----
OS Configuration: Member Workstation
OS Version: 10.0.26100
Site Name: N/A
Roaming Profile: N/A
Local Profile: C:\Users\alexandre.perez
Connected over a slow link?: No

USER SETTINGS
-----
CN=Alexandre Perez,OU=Engineering,DC=vlabs1,DC=com
Last time Group Policy was applied: 2025-05-23 at 12:33:05 PM
Group Policy was applied from: DC201.vlabs1.com
Group Policy slow link threshold: 500 kbps
Domain Name: VLABS1
Domain Type: Windows 2008 or later

Applied Group Policy Objects
-----
RestrictTeamsStarting

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

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

PS C:\Users\alexandre.perez>

```

Key Configuration Summary

Setting	Value	Purpose
GPO Name	RestrictTeamsStarting	Controls Teams auto-start
Policy Path	User Config → Admin Templates → Microsoft Teams	Targets user-level behavior
Linked OU	Engineering	Applies to specific department
Enforcement	gpupdate /force	Immediate policy application

5 Task 3: Managing Account Policies

5.1 Objective

Configure domain-wide password and account lockout policies in the Default Domain Policy, then verify enforcement.

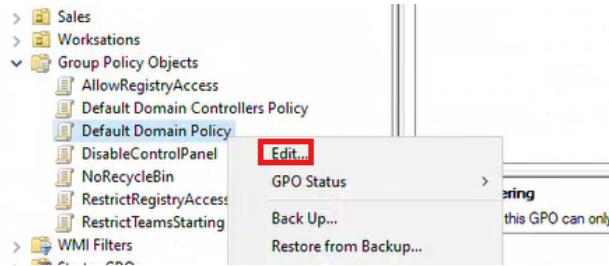
5.2 Steps

- 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 **Client1**, test with **Emma Petit** by attempting password modification and simulating an account lockout.

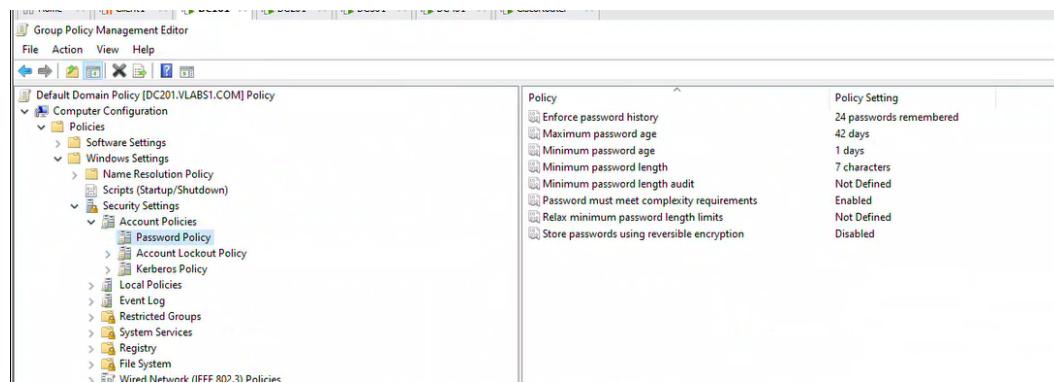
5.2.1 DC101

1. Configure Password Policies

- a) On DC101 (Domain Controller):
 - Open **GPMC** (gpmc.msc)
 - Navigate to: Group Policy Objects → Default Domain Policy → Right-click → Edit

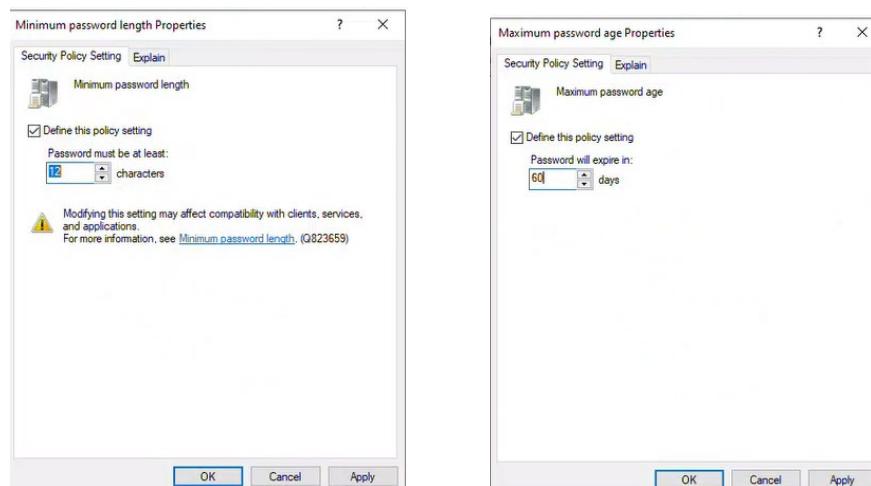


- Go to: Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy



b) Modify Settings:

- **Minimum password length:** 12 characters
(Double-click → Set to 12 → OK)
- **Password must meet complexity requirements:** Enabled
- **Maximum password age:** 60 days



Policy	Policy Setting
Enforce password history	24 passwords remembered
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

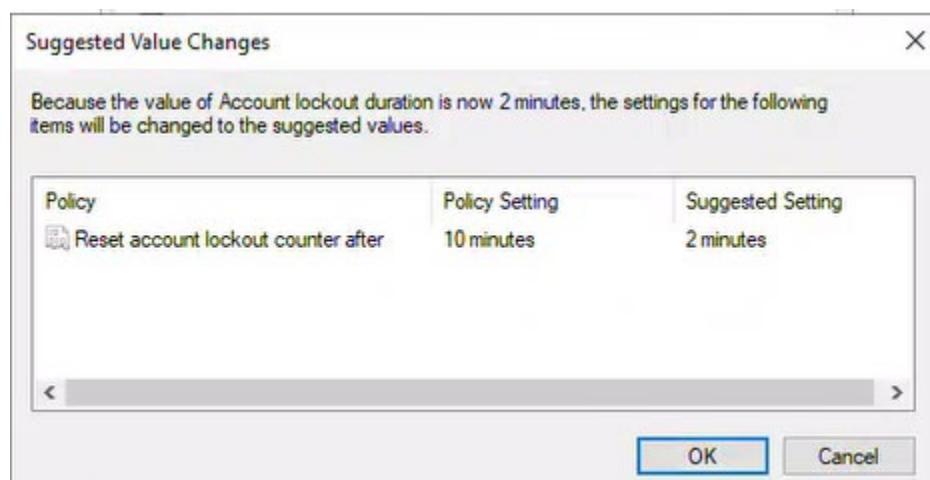
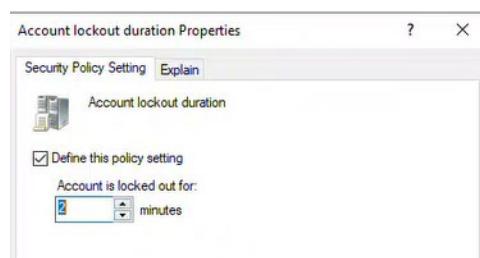
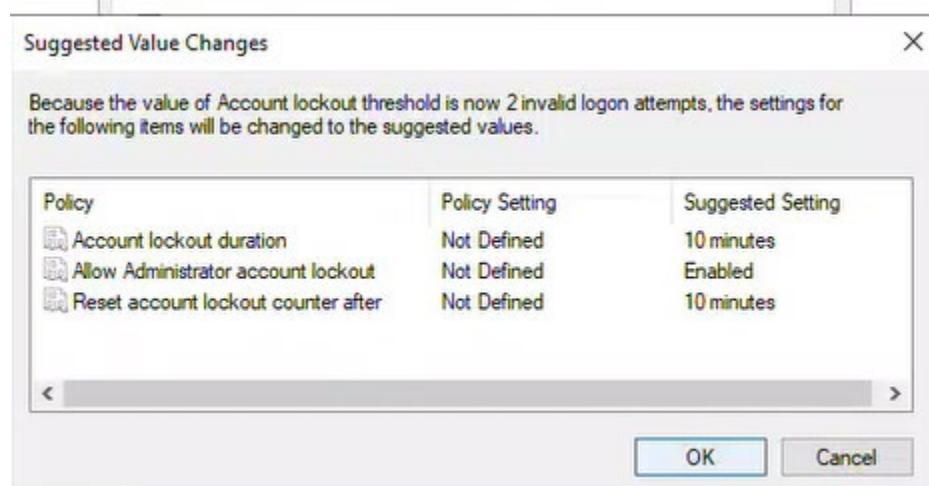
2. Configure Account Lockout Policy

- a) In the same GPO editor:
- o Navigate to: Account Policies → Account Lockout Policy

Policy	Policy Setting
Account lockout duration	Not Defined
Account lockout threshold	0 invalid logon attempts
Allow Administrator account lockout	Not Defined
Reset account lockout counter after	Not Defined

- b) Modify Settings:
- o **Account lockout threshold:** 2 invalid attempts
(Setting this will auto-populate other values)
 - o **Account lockout duration:** 2 minutes
 - o **Reset account lockout counter after:** 2 minutes



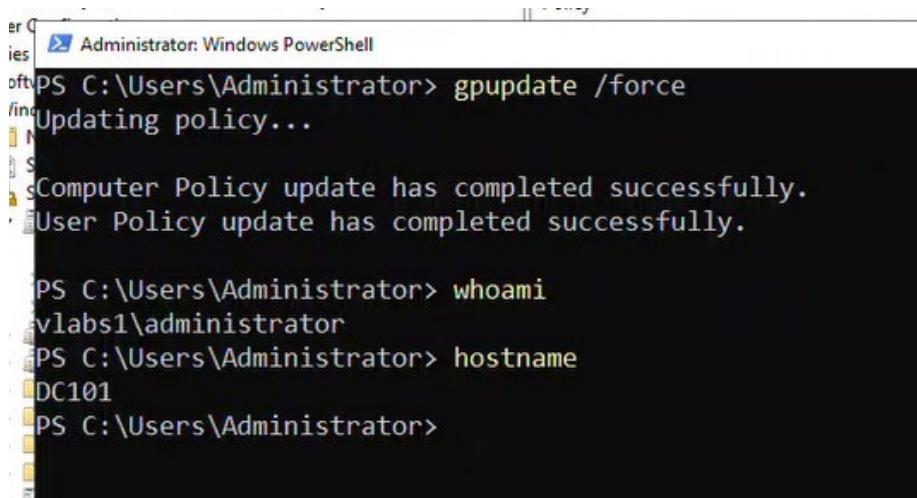


Policy	Policy Setting
Account lockout duration	2 minutes
Account lockout threshold	2 invalid logon attempts
Allow Administrator account lockout	Enabled
Reset account lockout counter after	2 minutes

3. Apply Policies

a) **Force Policy Update:**

- On DC101, run Command Prompt as Administrator:
gpupdate /force
- Wait for confirmation:
"Computer Policy update has completed successfully"



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.

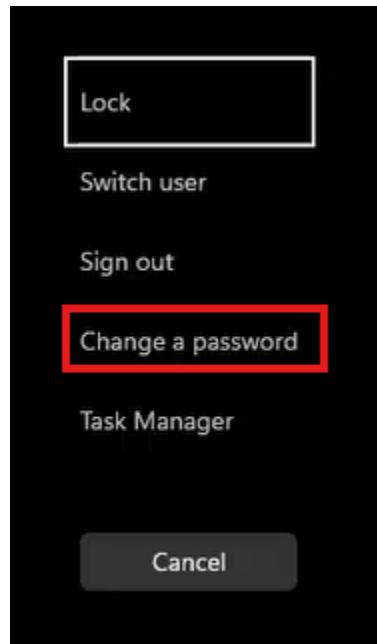
PS C:\Users\Administrator> whoami
vlabs1\administrator
PS C:\Users\Administrator> hostname
DC101
PS C:\Users\Administrator>
```

5.2.2 Client1

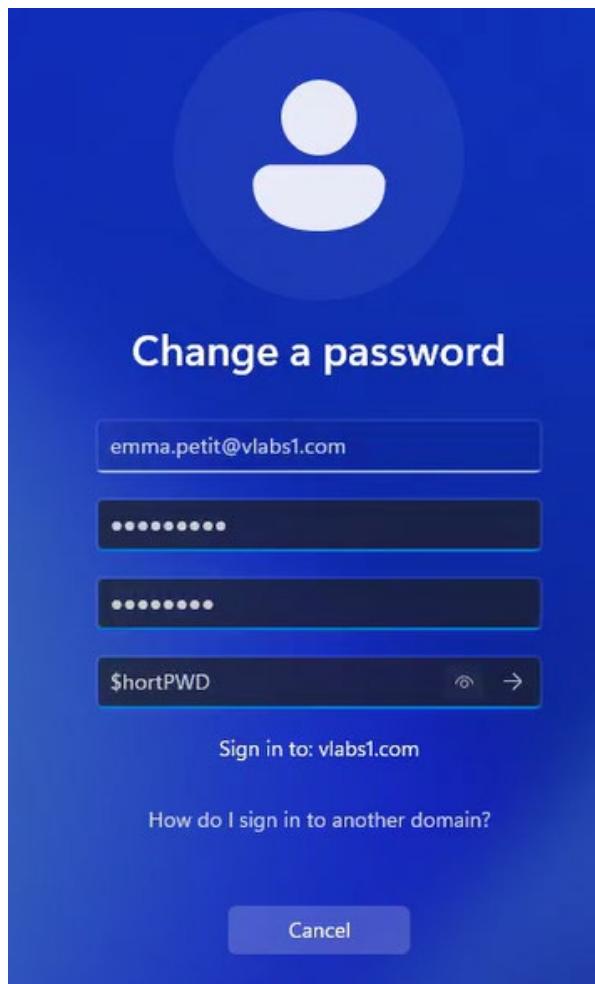
Verification Testing (From Client1)

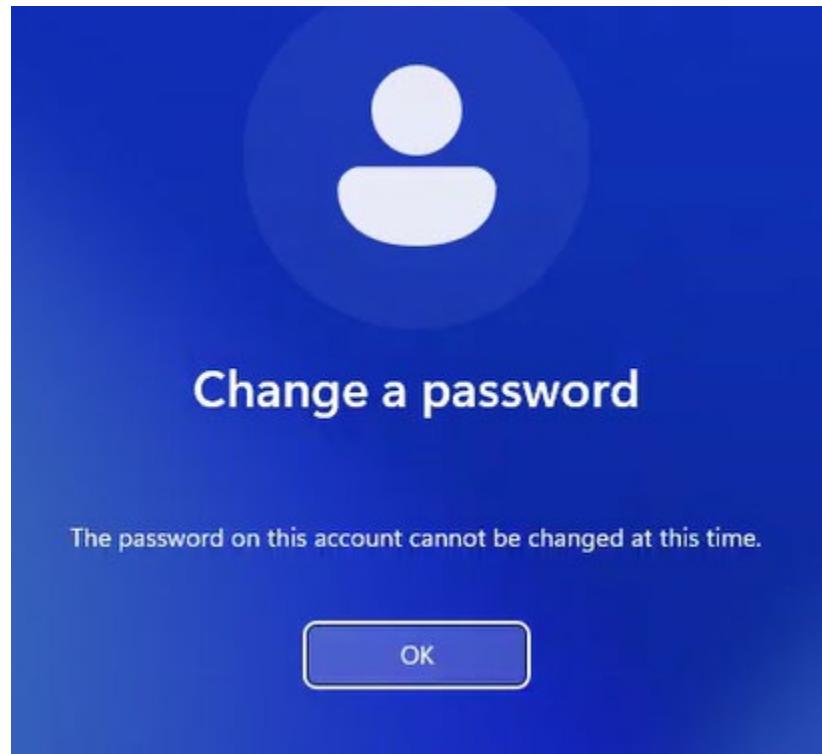
1. Test Password Change (Emma Petit)

- a) **Log in to Client1 as vlabs1.com\emma.petit**
- b) Attempt to change password via Ctrl+Alt+Del → Change a password:

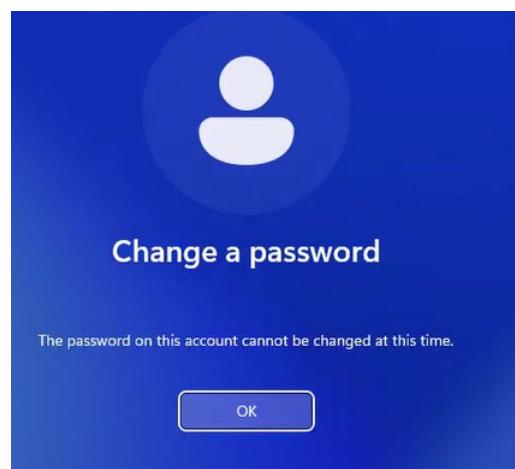
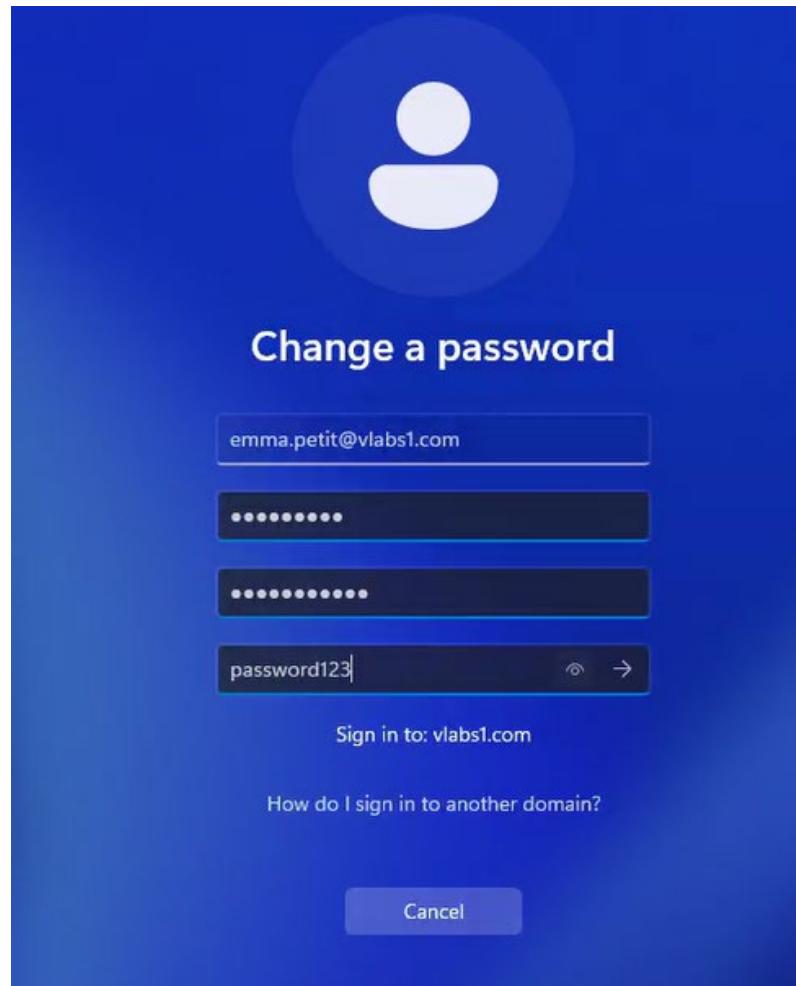


- **Test Case 1:** Try password shorter than 12 chars → Should fail



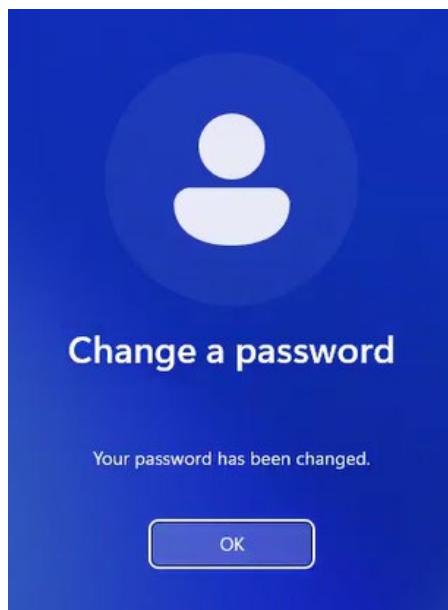
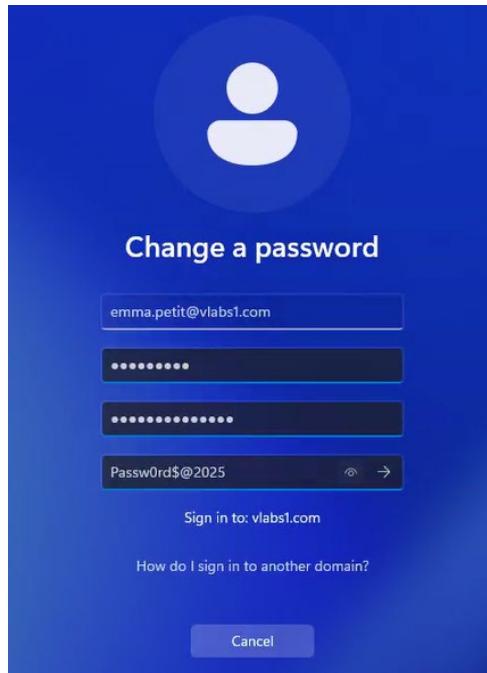


- **Test Case 2:** Try password without complexity (e.g., "password123")
→ Should fail



- **Test Case 3:** Valid password (e.g., "Vlabs1@2025!") → Should

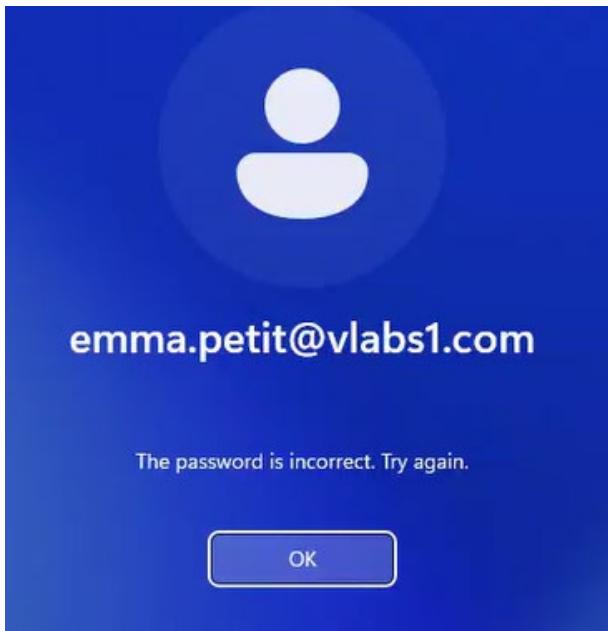
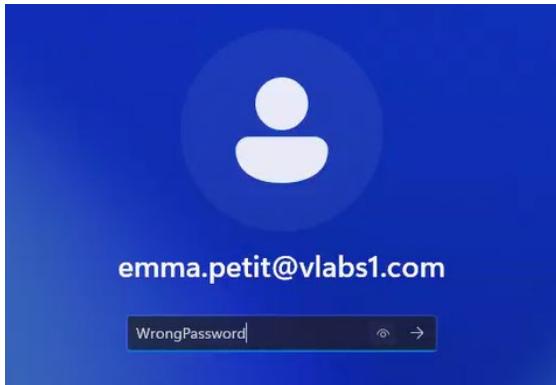
succeed

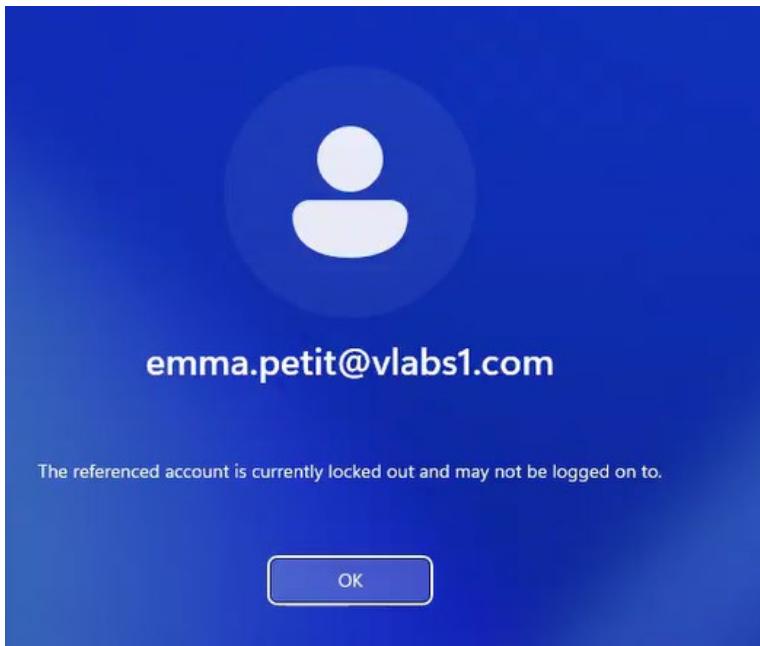


2. Test Account Lockout

- a) Simulate Failed Logins:

- Log out and intentionally enter **wrong password twice**
- b) **Expected Result:**
- After 2nd attempt:
"Your account is locked out. Try again later."
 - Wait 2 minutes → Account should auto-unlock





Policy Configuration Summary

Policy Type	Setting	Value
Password Policy	Minimum length	12 characters
	Complexity requirements	Enabled
	Maximum password age	60 days
Lockout Policy	Lockout threshold	2 attempts
	Lockout duration	2 minutes
	Reset counter after	2 minutes

6 Task 4: Implementing Fine-Grained Password Policies

6.1 Objective

Create and apply customized password policies for the IT group that override Default Domain Policy settings.

6.2 Steps

- 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 **Client1**, test with a **user from the IT group** by attempting password modification.

6.3 DC101

1. Create Fine-Grained Password Policy

Open **Active Directory Administrative Center**

1. Navigate to Fine-Grained Password Policies:
 - In the left pane, select your domain
 - In the middle pane, double-click on "System"
 - Select "Password Settings Container"
2. Create new policy:
 - In the right pane, click "New" → "Password Settings"
 - In the dialog box that appears:
 - Name: **IT_FGPPolicy**
 - Precedence: **1**
3. Modify Password Settings
 - **Minimum password length:** **10**
 - **Password must meet complexity requirements:** **Uncheck**
 - **Enforce minimum password age:** *Leave blank*
 - **Enforce maximum password age:** *Leave blank*
 - *Leave all other fields empty or default.*
4. Apply to IT Group

In the same "Password Settings" dialog box:

 - a) Under "Directly Applies To", click "Add"
 - b) Browse to and select your IT group (e.g., "IT_Group")
 - c) Click "OK" to save the policy

5. Force Policy Update

`gpupdate /force`

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

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

PS C:\Users\Administrator> ■
```

Note – It says Password never expires

2. Verify Policy Application

On DC101, check effective policy:

`Get-ADUserResultantPasswordPolicy -Identity "CN=Aloyse Dupont,OU=IT,DC=vlabs1,DC=com"`

```

PS C:\Users\Administrator> Get-ADUserResultantPasswordPolicy -Identity "CN=Aloyse Dupont,OU=IT,DC=vlabs1,DC=com"

AppliesTo          : {CN=IT,OU=IT,DC=vlabs1,DC=com}
ComplexityEnabled   : False
DistinguishedName   : CN=IT_FGPPolicy,CN=Password Settings Container,CN=System,DC=vlabs1,DC=com
LockoutDuration     : 00:30:00
LockoutObservationWindow : 00:30:00
LockoutThreshold    : 0
MaxPasswordAge      : 00:00:00
MinPasswordAge      : 00:00:00
MinPasswordLength    : 10
Name                : IT_FGPPolicy
ObjectClass         : msDS-PasswordSettings
ObjectGUID          : db729f94-3564-47f4-81fd-fe9e3b50e1a1
PasswordHistoryCount : 0
Precedence          : 1
ReversibleEncryptionEnabled : False

PS C:\Users\Administrator>

```

6.4 Client1

Verification Testing (From Client1)

1. Test Password Change (IT User)

- a) Log in to Client1 as an IT group member (e.g., vlabs1.com\it.user)

The screenshot shows the Windows Start Menu search results for the query 'IT'. The results list 29 items, including user accounts like Aloyse Dupont, Augustine Andre, Axel Poirier, etc., and a 'IT' group account. To the right of the search results, a blue sign-in screen is displayed. It features a large white user icon, the text 'Other user', an email input field containing 'aloyse.dupont@vlabs1.com', a password input field with masked text, and a 'Sign in to: vlabs1.com' button. Below the sign-in screen, a link 'How do I sign in to another domain?' is visible.

Name	Type
Aloyse Dupont	User
Augustine Andre	User
Axel Poirier	User
Camille Martin	User
Capucine Garnier	User
Clement Menard	User
Diane Clement	User
Erwan Collet	User
Faustine Marchand	User
Gildas Leroux	User
Isaline Dufour	User
IT	Group
Josselin LeGoff	User
June Blanchard	User
Lina Gaillard	User
Loan Weber	User
Louise Roy	User
Malo Boulanger	User
Manon Moreau	User

- b) Attempt password change via Ctrl+Alt+Del → Change a password:
- **Test Case 1:** Password never expires → Verify via: net user aloyse.dupont /DOMAIN

```
PS C:\Users\aloyse.dupont> net user aloyse.dupont /DOMAIN
The request will be processed at a domain controller for domain vlabsl.com.

User name          aloyse.dupont
Full Name
Comment
User's comment
Country/region code      000 (System Default)
Account active        Yes
Account expires       Never

Password last set    2025-05-24 12:16:48 PM
Password expires    Never
Password changeable 2025-05-25 12:16:48 PM
Password required     Yes
User may change password Yes

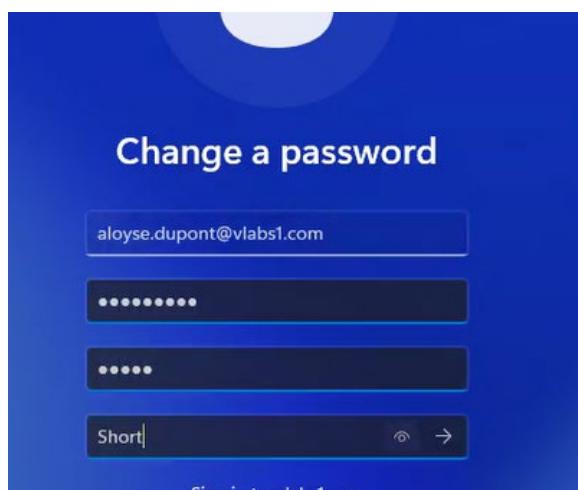
Workstations allowed All
Logon script
User profile
Home directory
Last logon           2025-05-24 12:18:42 PM

Logon hours allowed All

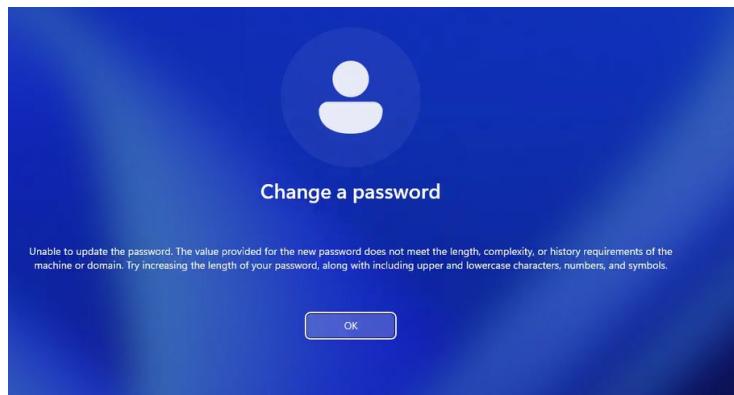
Local Group Memberships
Global Group memberships *Domain Users      *IT
The command completed successfully.

PS C:\Users\aloyse.dupont>
```

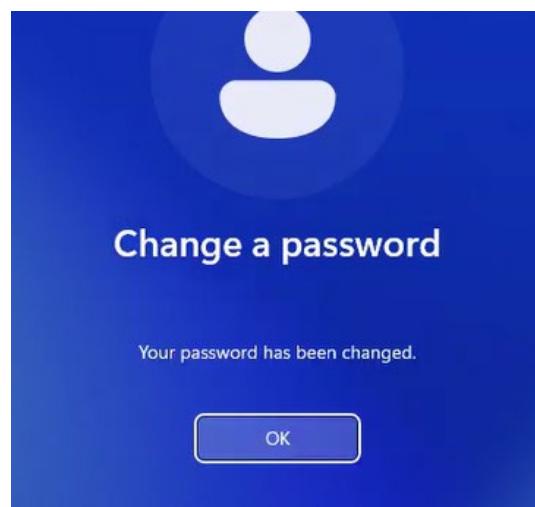
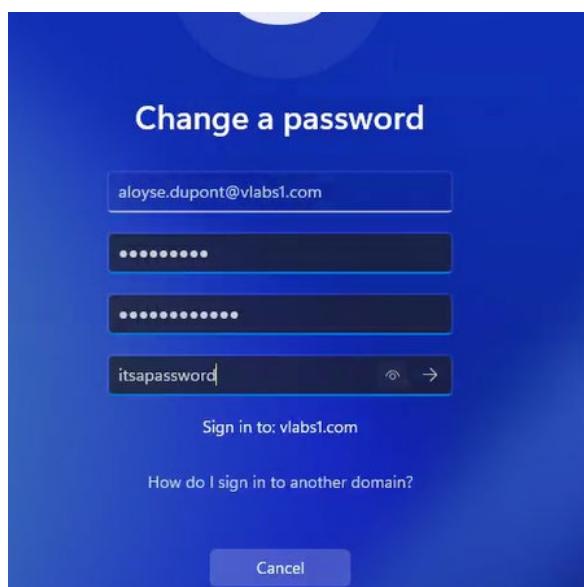
- **Test Case 2:** Try password shorter than 10 chars → Should fail



Password can not be changed



- **Test Case 2:** Try simple password (e.g., "itpassword") → Should succeed (complexity disabled)



7 Task 5: Managing Audit Authentication

- Modify Default Domain Policy GPO to enable Audit Logon Events (Success and Failure).
- Restart the Client1
- Test by failing and successfully logging in with any user on Client1.
- Open Event Viewer on DC101 and verify Security Logs.

7.1 Objective

Configure domain-wide audit policies to track both successful and failed logon attempts, then verify logging functionality.

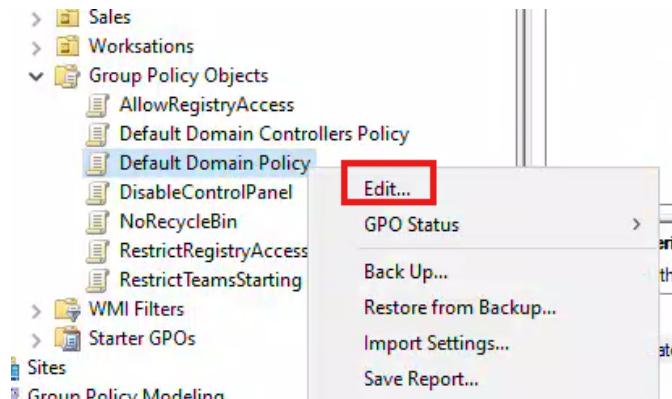
7.2 Steps

7.2.1 DC101

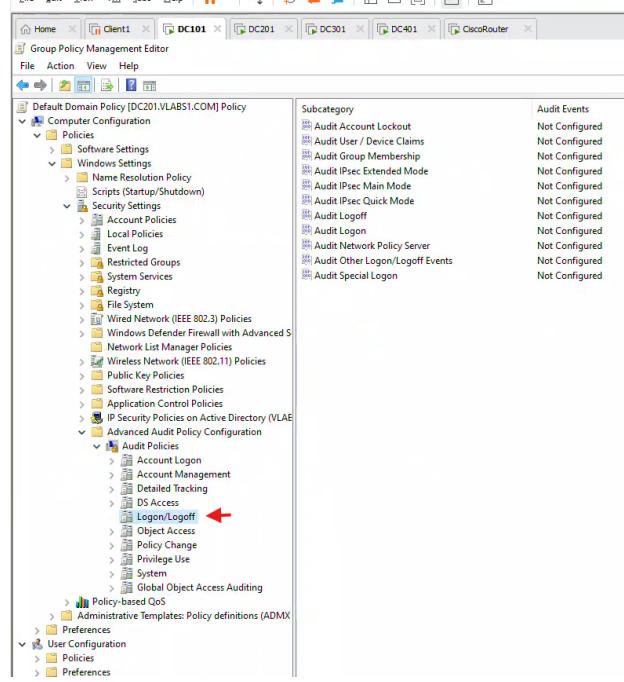
Configure Audit Policy in Default Domain Policy

1. On DC101 (Domain Controller):

- Open Group Policy Management Console (gpmc.msc)
- Navigate to: Group Policy Objects → Default Domain Policy → Right-click → Edit

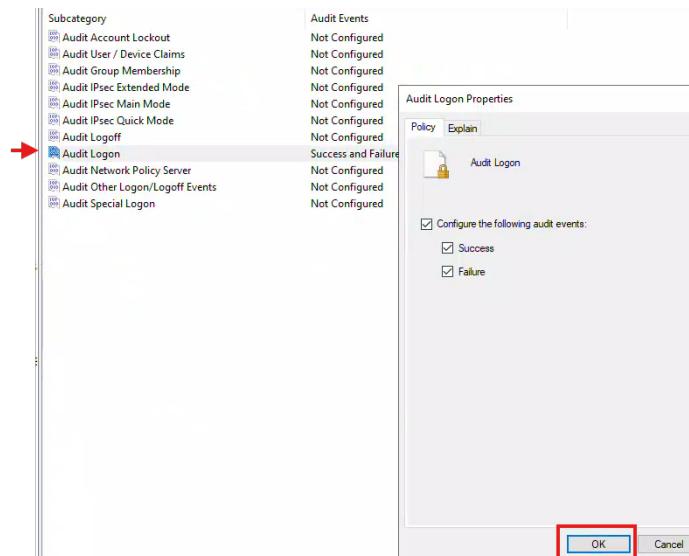


- Go to: Computer Configuration → Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policies → Logon/Logoff



2. Enable Auditing:

- Double-click "Audit Logon Events"
- Check both:
 - "Configure the following audit events"
 - "Success" and "Failure"
- Click OK



3. **Force Policy Update:**

- On DC101, run Command Prompt as Administrator:
gpupdate /force

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

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

PS C:\Users\Administrator>
```

NOTE

Why You Might Not See Client1's Events on DC101:

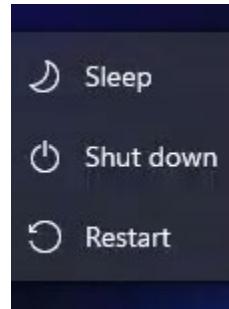
- **Default Behavior:** By default, **client computers do not forward their individual logon/logoff security events to a Domain Controller**. The Domain Controller only logs events related to the authentication requests it *handles* for those clients.
- **Client-Side Logging:** Failed logon attempts to *Client1 itself* would primarily be logged on **Client1's own Security event log**. (e.g., someone trying to log directly into Client1 with local credentials or domain credentials that fail)

7.2.2 Client1

7.2.2.1 Local event in client1

1. **Restart Client1:**

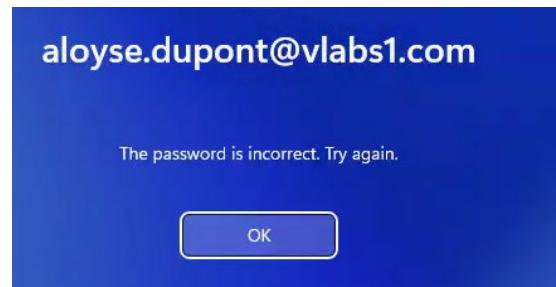
- *Wait for complete reboot*



2. **Generate Test Events (On Client1)**

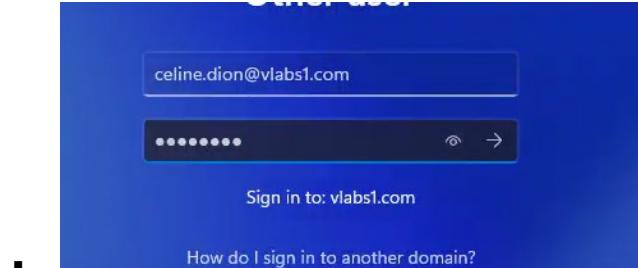
a) **Simulate Failed Logon:**

- Attempt login with:
 - Wrong password (generates Failure event)



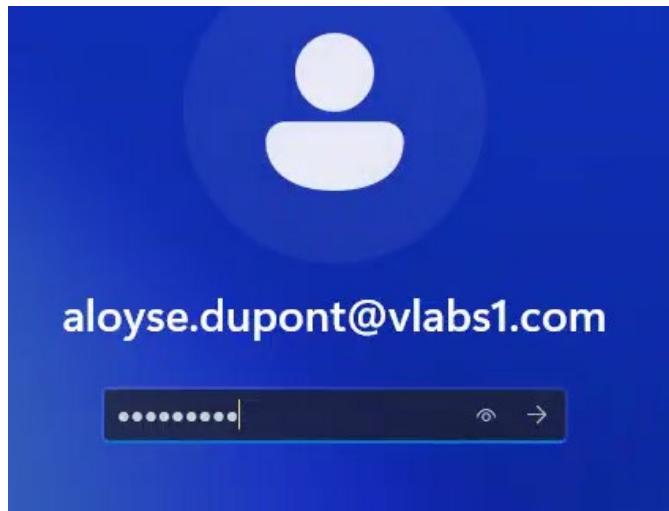
- - Non-existent username (generates Failure event)

○



b) **Perform Successful Logon:**

- Correct credentials for any domain user



3. Check local event log in client1

Connect event viewer as administrator. View 4265 events

A screenshot of the Windows Event Viewer application. The window title is "Event Viewer". The left pane shows a tree view with "Event Viewer (Local)", "Custom Views", "Windows Logs" (expanded to show "Application", "Security", "Setup", "System", "Forwarded Events"), and "Applications and Services Log" and "Subscriptions". The "Security" node under "Windows Logs" is selected, and the status bar indicates "Number of events: 24,252". The main pane displays a table of events with columns "Level", "Date and Time", and "Source". The first few rows show "Information" level events from "Microsoft Windows security auditing." at various times on 2025-05-24. A context menu is open over one of these events, with options like "Copy", "Delete", "Properties", "Search", "Find Next", "Find Previous", "Find All", and "Close". A detailed view of an event is shown in a modal dialog titled "Event Properties - Event 4625, Microsoft Windows security auditing.". The dialog has tabs for "General" and "Details". The "General" tab shows "An account failed to log on." and "Subject: Security ID: SYSTEM". The "Details" tab shows "Network Information" (Workstation Name: CLIENT1, Source Network Address: 127.0.0.1, Source Port: 0), "Detailed Authentication Information" (Logon Process: User32, Authentication Package: Negotiate), and event properties: Log Name: Security, Source: Microsoft Windows security, Event ID: 4625, Level: Information, User: N/A, OpCode: Info. The event was Logged: 2025-05-24 10:52:28 PM, Task Category: Logon, Keywords: Audit Failure, Computer: Client1.vlabs1.com.

+ System

- Provider

[Name] Microsoft-Windows-Security-Auditing
[Guid] {54849625-5478-4994-a5ba-3e3b0328c30d}

EventID 4625

Version 0

Level 0

Task 12544

Opcode 0

Keywords 0x8010000000000000

- TimeCreated

[SystemTime] 2025-05-25T02:52:28.7743802Z

EventRecordID 44435

- Correlation

[ActivityID] {bb6a734c-cd00-0001-ad74-6abb00cddb01}

- Execution

[ProcessID] 804

[ThreadID] 4104

Channel Security

Computer Client1.vlabs1.com

Security

- EventData

SubjectUserSid S-1-5-18

SubjectUserName CLIENT1\$

SubjectDomainName VLABS1

SubjectLogonId 0x3e7
 TargetUserId S-1-0-0
 TargetUserName aloyse.dupont@vlabs1.com
 TargetDomainName -
 Status 0xc000006d
 FailureReason %%2313
 SubStatus 0xc000006a
 LogonType 2
 LogonProcessName User32
 AuthenticationPackageName Negotiate
 WorkstationName CLIENT1
 TransmittedServices -
 LmPackageName -
 KeyLength 0
 ProcessId 0x66c
 ProcessName C:\Windows\System32\svchost.exe
 IpAddress 127.0.0.1
 IpPort 0

Successful connection 4264

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Windows Logs (Security, Application, Setup, System, Forwarded Events), Applications and Services Logs, and Subscriptions. The right pane shows a list of events under the Security category. A specific event (Event ID 4624) is selected and detailed in the bottom-right pane.

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject: Security ID: SYSTEM

Log Name: Security
Source: Microsoft Windows security
Event ID: 4624
Level: Information
User: N/A
OpCode: Info

Task Category: Logon
Keywords: Audit Success

Properties:

- PROCESSNAME: C:\Windows\System32\svchost.exe
- IPADDRESS: -
- IPPORT: -
- IMPERSONATIONLEVEL: %%1833
- RESTRICTEDADMINMODE: -
- REMOTECREDENTIALGUARD: -
- TARGETOUTBOUNDUSERNAME: -
- TARGETOUTBOUNDDOMAINNAME: -
- VIRTUALACCOUNT: %%1843
- TARGETLINKEDLOGONID: 0x0
- ELEVATEDTOKEN: %%1843

+ System

- Provider

[Name] Microsoft-Windows-Security-Auditing
[Guid] {54849625-5478-4994-a5ba-3e3b0328c30d}

EventID 4624

Version 3

Level 0

Task 12544

Opcode 0

Keywords 0x8020000000000000

- TimeCreated

[SystemTime] 2025-05-25T02:52:35.2079530Z

EventRecordID 44439

Correlation

- Execution

[ProcessID] 804

[ThreadID] 4136

Channel Security

Computer Client1.vlabs1.com

Security

- EventData

SubjectUserSid S-1-5-18

SubjectUserName CLIENT1\$

SubjectDomainName VLABS1

SubjectLogonId 0x3e7

TargetUserSid S-1-5-21-1268601764-4050707287-4025116504-1760

```
TargetUserName aloyse.dupont
TargetDomainName VLABS1
TargetLogonId 0x8ec487
LogonType 7
LogonProcessName Negotiate
AuthenticationPackageName Negotiate
WorkstationName CLIENT1
LogonGuid {473595ac-f969-67fb-4ae8-c3de87a9fcb1}
TransmittedServices -
LmPackageName -
KeyLength 0
ProcessId 0x324
ProcessName C:\Windows\System32\lsass.exe
IpAddress -
IpPort -
ImpersonationLevel %%1833
RestrictedAdminMode -
RemoteCredentialGuard -
TargetOutboundUserName -
TargetOutboundDomainName -
VirtualAccount %%1843
TargetLinkedLogonId 0x0
ElevatedToken %%1843
```

7.2.2.2 Event generated in client 1 towards DC101

1. Try to connect with bad password in client1

Followed by a successful login towards DC101

```
PS C:\Users\aloyse.dupont> net use \\DC101\C$ /user:administrator Wrongpassword
System error 86 has occurred.

The specified network password is not correct.

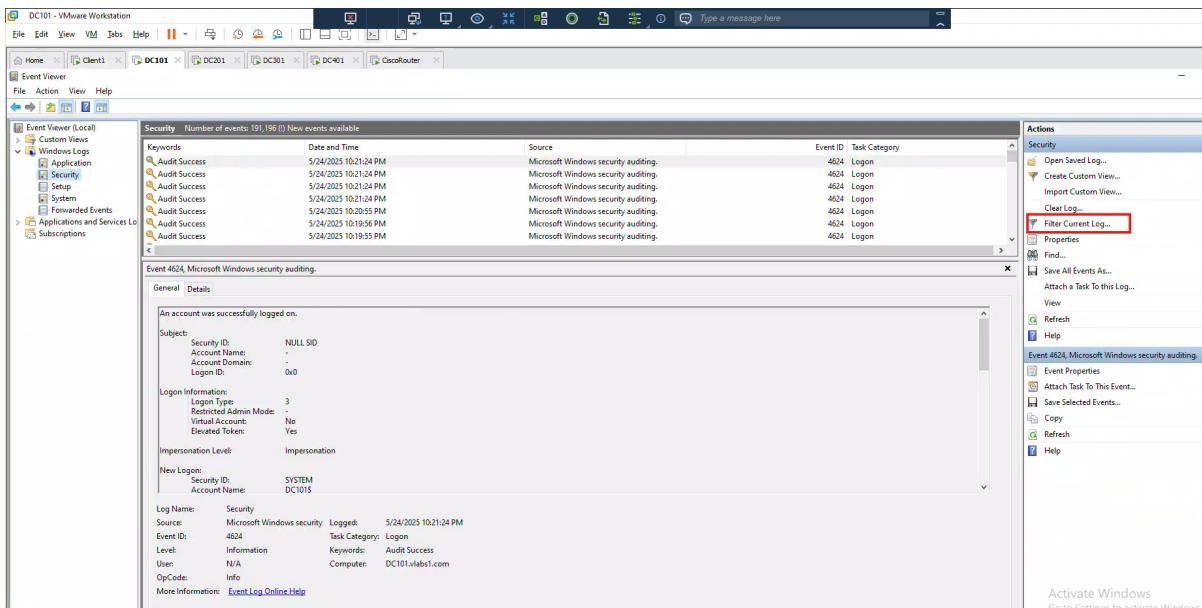
PS C:\Users\aloyse.dupont> net use \\DC101\C$ /user:administrator Passw0rd$
The command completed successfully.

PS C:\Users\aloyse.dupont> whoami
vlabs1\aloyse.dupont
PS C:\Users\aloyse.dupont>
```

2. Check Security Logs (On DC101)

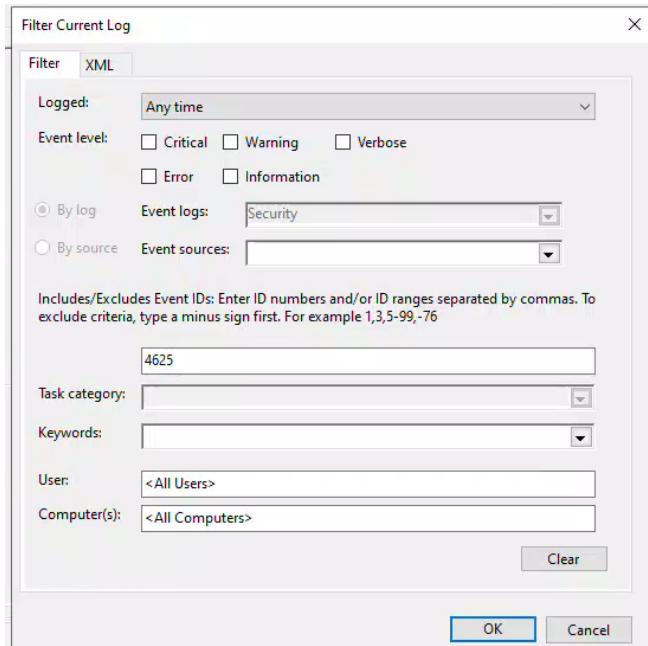
- Open Event Viewer:

- Run eventvwr.msc
- Navigate to: Windows Logs → Security



b) Filter for Relevant Events:

- Click "Filter Current Log"
- Enter Event IDs:
 - **4624** (Successful logon)
 - **4625** (Failed logon)
- Click OK



c) Verify Events:

- o For failed attempts (4625):

- Check "Account Name" matches test user
 - Verify "Failure Reason" appears

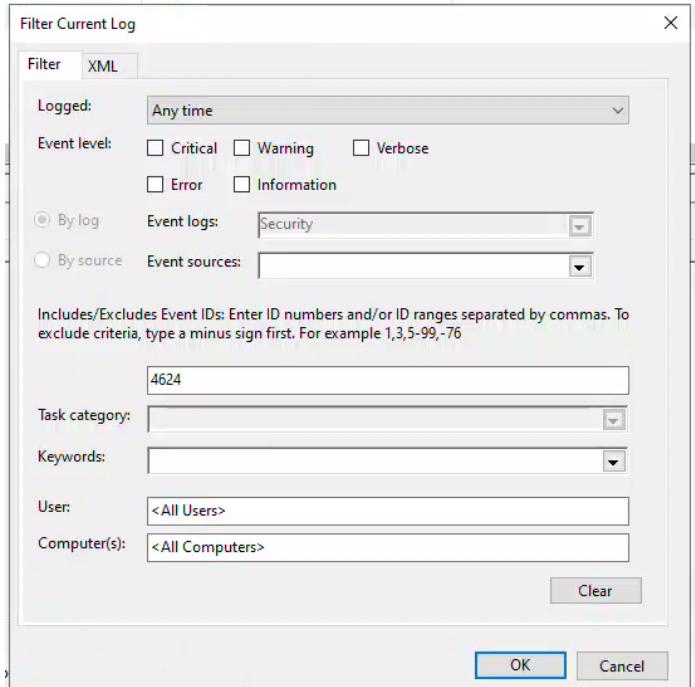
```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
<Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-a5ba-3e3b0328c30d}" />
<EventID>4625</EventID>
<Version>0</Version>
```

```

<Level>0</Level>
<Task>12544</Task>
<Opcode>0</Opcode>
<Keywords>0x8010000000000000</Keywords>
<TimeCreated SystemTime="2025-05-25T02:03:07.7343499Z" />
<EventRecordID>258393</EventRecordID>
<Correlation />
<Execution ProcessID="744" ThreadID="864" />
<Channel>Security</Channel>
<Computer>DC101.vlabs1.com</Computer>
<Security />
</System>
- <EventData>
  <Data Name="SubjectUserSid">S-1-0-0</Data>
  <Data Name="SubjectUserName">-</Data>
  <Data Name="SubjectDomainName">-</Data>
  <Data Name="SubjectLogonId">0x0</Data>
  <Data Name="TargetUserSid">S-1-0-0</Data>
  <Data Name="TargetUserName">administrator</Data>
  <Data Name="TargetDomainName" />
  <Data Name="Status">0xc000006d</Data>
  <Data Name="FailureReason">%2313</Data>
  <Data Name="SubStatus">0xc000006a</Data>
  <Data Name="LogonType">3</Data>
  <Data Name="LogonProcessName">NtLmSsp</Data>
  <Data Name="AuthenticationPackageName">NTLM</Data>
  <Data Name="WorkstationName">CLIENT1</Data>
  <Data Name="TransmittedServices">-</Data>
  <Data Name="LmPackageName">-</Data>
  <Data Name="KeyLength">0</Data>
  <Data Name="ProcessId">0x0</Data>
  <Data Name="ProcessName">-</Data>
  <Data Name="IpAddress">192.168.1.100</Data>
  <Data Name="IpPort">54939</Data>
</EventData>
</Event>

```

- For **successful logons** (4624):
 - Confirm "Logon Type" (2=Interactive, 3=Network)
 - Verify workstation name is Client1



Security Number of events: 191,220 (0) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	5/24/2025 10:27:55 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	5/24/2025 10:27:30 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	5/24/2025 10:27:15 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	5/24/2025 10:27:15 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	5/24/2025 10:27:01 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	5/24/2025 10:26:55 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	5/24/2025 10:26:54 PM	Microsoft Windows security auditing.	4624	Logon

Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Logon Information:

- Logon Type: 3
- Restricted Admin Mode: -
- Virtual Account: No
- Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:

- Security ID: VLABS1\Administrator
- Account Name: Administrator

Log Name: Security

Source: Microsoft Windows security

Event ID: 4624

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

Network Information:

- Workstation Name: CLIENT1
- Source Network Address: 192.168.1.100
- Source Port: 55062

Detailed Authentication Information:

- Log Name: Security
- Source: Microsoft Windows security
- Event ID: 4624
- Level: Information
- Keywords: Audit Success
- User: N/A
- Computer: DC101.vlabs1.com
- OpCode: Info
- More Information: [Event Log Online Help](#)

Copy Close

+ System

- Provider

[Name] Microsoft-Windows-Security-Auditing

[Guid] {54849625-5478-4994-a5ba-3e3b0328c30d}

EventID 4624

Version 2

Level 0

Task 12544

Opcode 0

Keywords 0x8020000000000000

- TimeCreated

[SystemTime] 2025-05-25T02:27:15.6924035Z

EventRecordID 258475

Correlation

- Execution

[ProcessID] 744

[ThreadID] 864

Channel Security

Computer DC101.vlabs1.com

Security

- EventData

SubjectUserSid S-1-0-0

SubjectUserName -

SubjectDomainName -

SubjectLogonId 0x0

TargetUserSid S-1-5-21-1268601764-4050707287-4025116504-500

TargetUserName Administrator

TargetDomainName VLABS1

TargetLogonId 0x54277a0

LogonType 3

LogonProcessName NtLmSsp

AuthenticationPackageName NTLM

```

WorkstationName CLIENT1
LogonGuid {00000000-0000-0000-0000-000000000000}
TransmittedServices -
LmPackageName NTLM V2
KeyLength 128
ProcessId 0x0
ProcessName -
IpAddress 192.168.1.100
IpPort 55062
ImpersonationLevel %%1833
RestrictedAdminMode -
TargetOutboundUserName -
TargetOutboundDomainName -
VirtualAccount %%1843
TargetLinkedLogonId 0x0
ElevatedToken %%1842

```

Key Event Details

Event ID	Description	Important Fields
4624	Successful logon	- TargetUserName - WorkstationName - LogonType
4625	Failed logon	- TargetUserName - FailureReason - SourceNetworkAddress

8 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 **DC101** to apply changes.

- Restart **DC101** and verify in **Services** that **OpenSSH Authentication Agent** has started.

8.1 Objective:

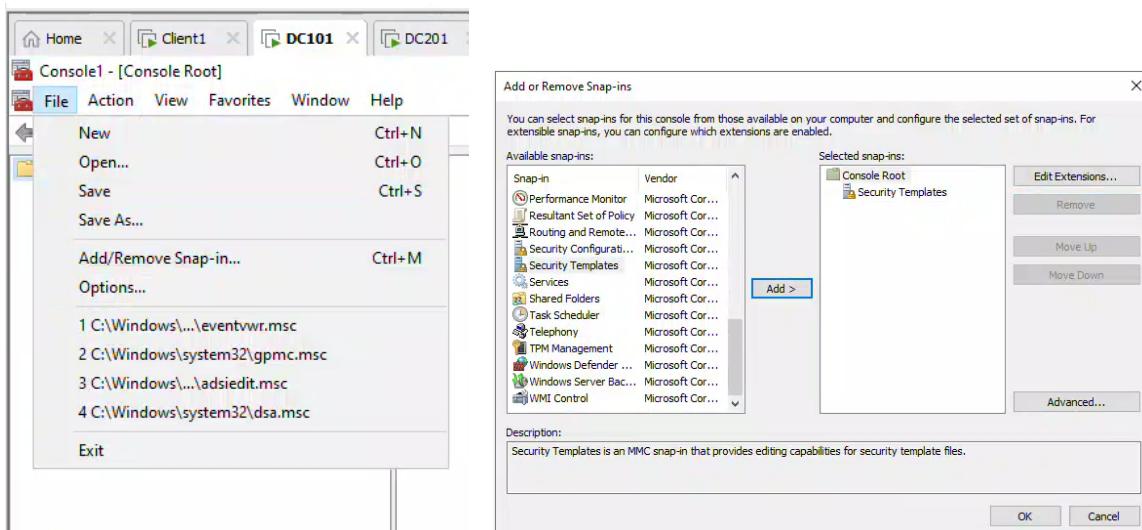
Create and deploy a security template to configure OpenSSH Authentication Agent service startup via Group Policy.

8.2 Steps

1. Create Security Template

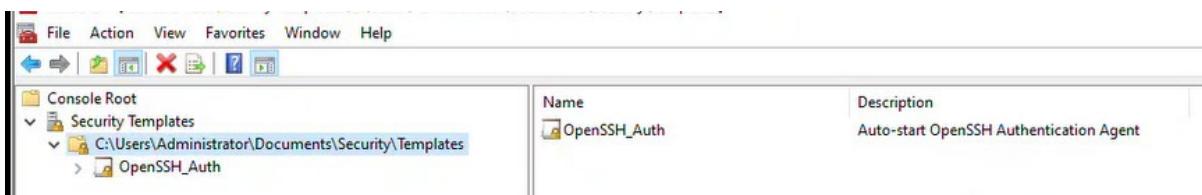
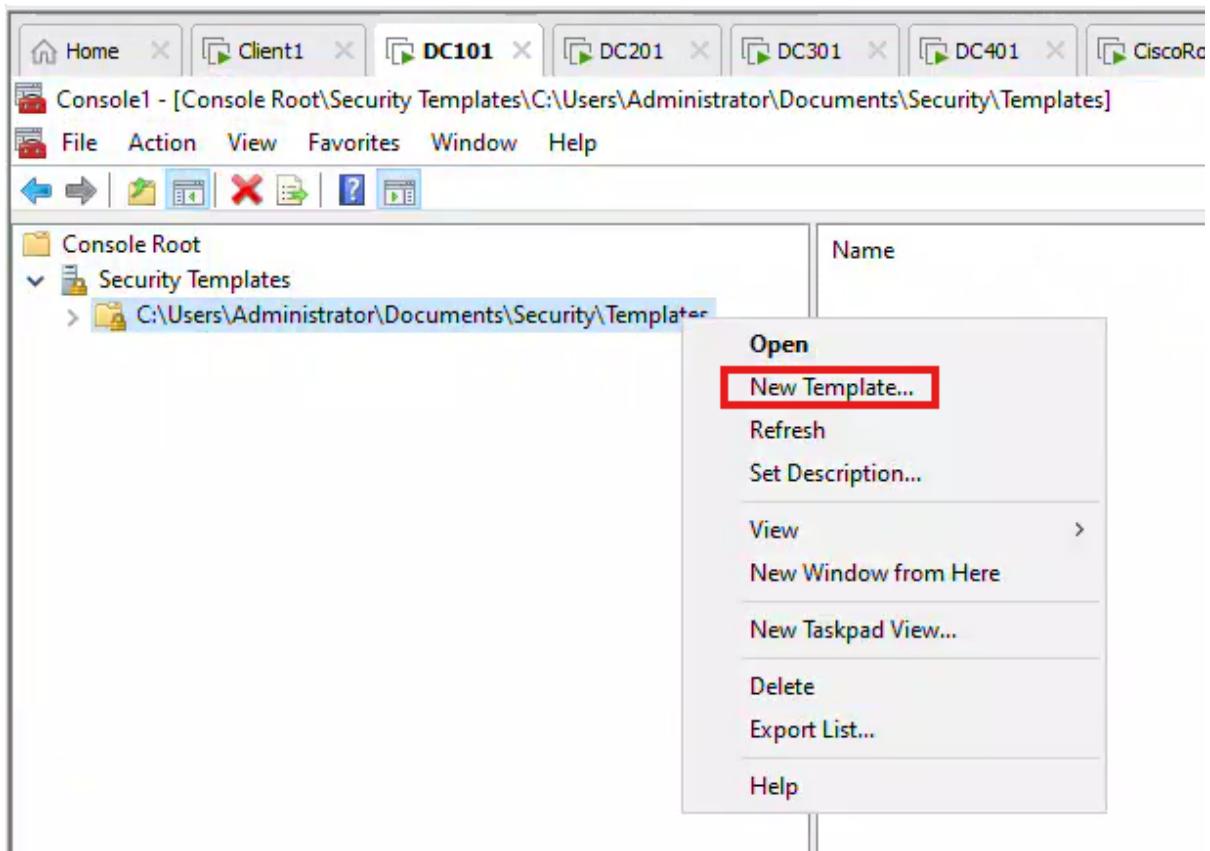
1. On DC101 (Domain Controller):

- Open **Microsoft Management Console** (mmc.exe)
- Go to **File → Add/Remove Snap-in**
- Add **Security Templates** → Click **OK**



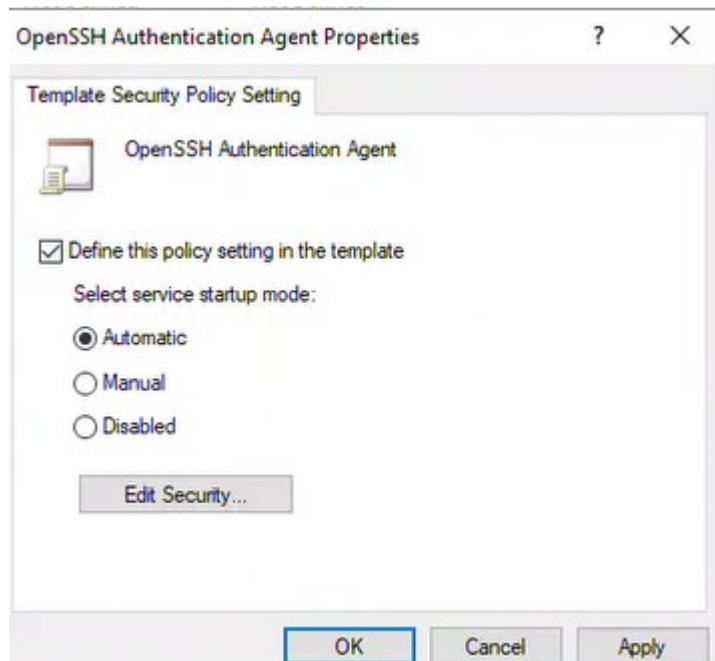
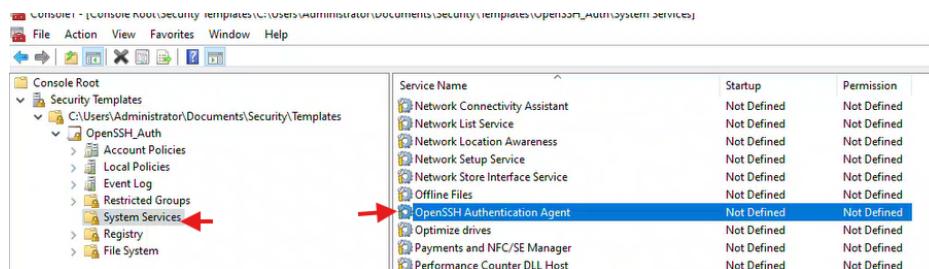
2. Create New Template:

- In the left pane, expand: **Security Templates** → **C:\Users\Administrator\Documents\Security\Templates**
- Right-click → **New Template**
- Name: **OpenSSH_Auth**
- Description: "Auto-start OpenSSH Authentication Agent"



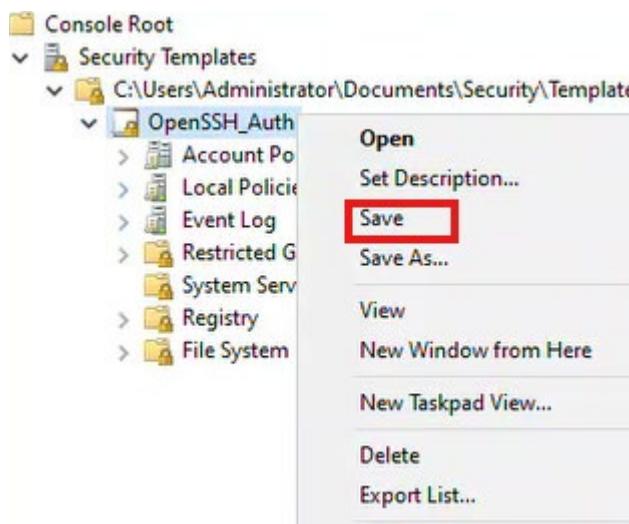
2. Configure OpenSSH Service

1. In the Security Template:
 - o Navigate to: OpenSSH_Auth → System Services
 - o Find "**OpenSSH Authentication Agent**"
 - o Double-click → Select "**Define this policy setting**"
 - o Set to: **Automatic**
 - o Click **OK**



3. Save Template

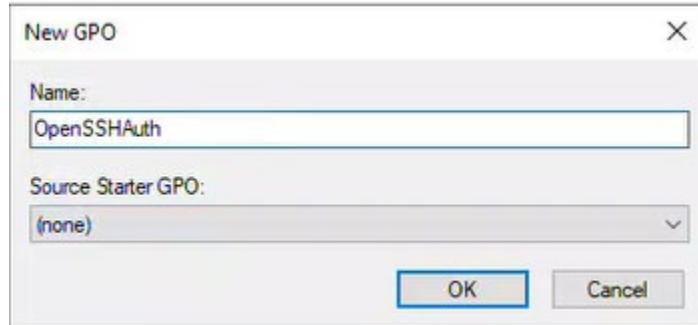
- Right-click OpenSSH_Auth → **Save**



4. Create and Configure GPO

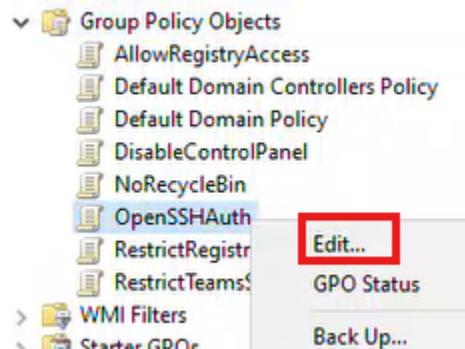
1. In GPMC (gpmc.msc):

- o Right-click **Group Policy Objects** → New
- o Name: OpenSSHAUTH → Click **OK**

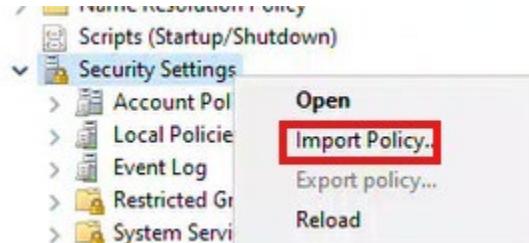


2. Import Template:

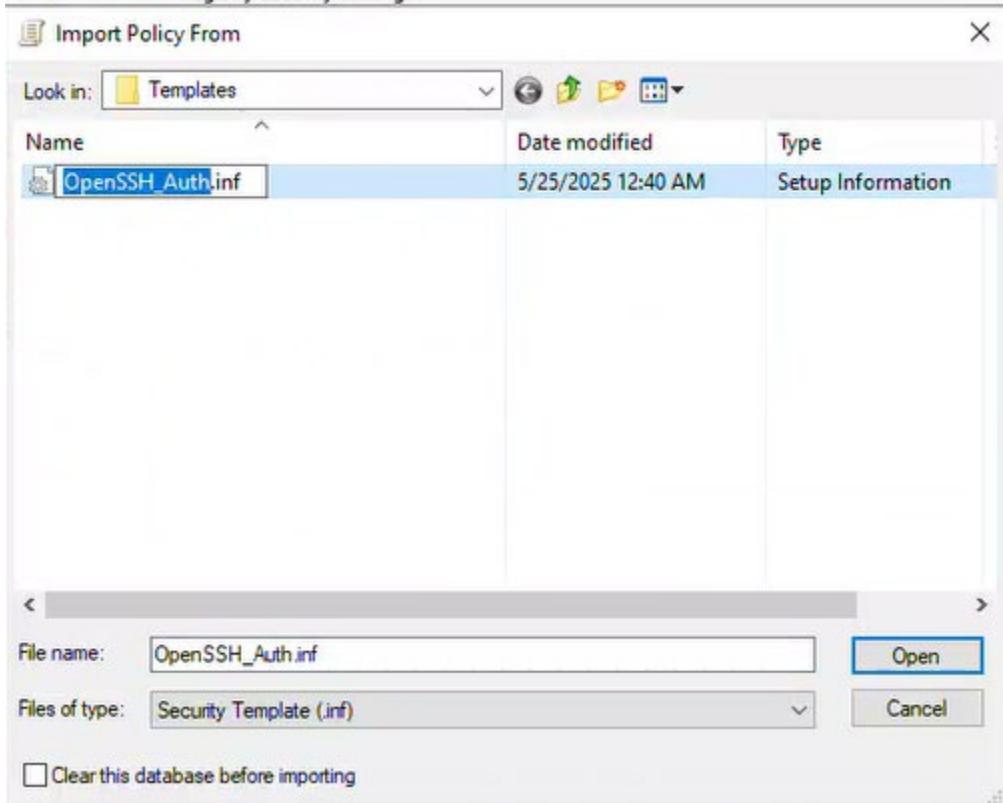
- o Right-click → **Edit**



- o Navigate to: Computer Configuration → Policies → Windows Settings → Security Settings
- o Right-click → **Import Policy**

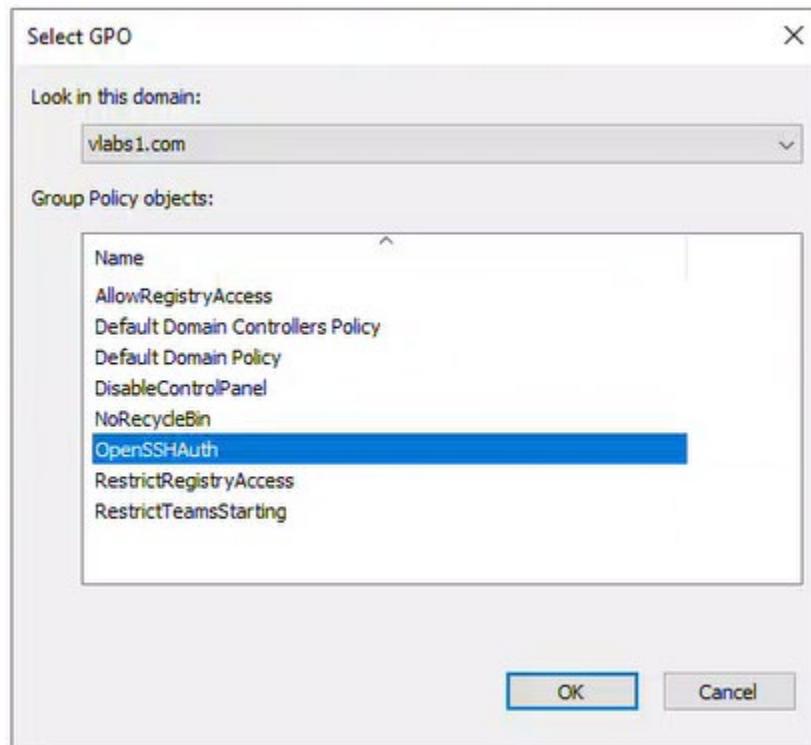
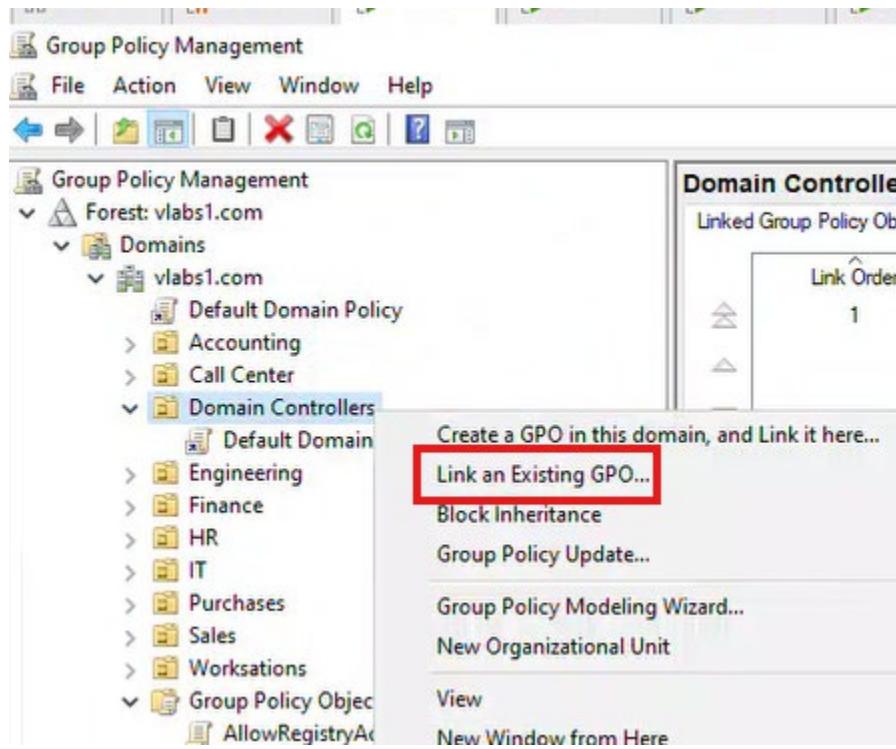


- o Browse to saved template (OpenSSH_Auth.inf)
- o Click **Open**



5. Link GPO to Domain Controllers

1. In GPMC:
 - o Navigate to: Domain Controllers OU
 - o Right-click → **Link an Existing GPO**
 - o Select OpenSSHAUTH → Click **OK**



2. Verify Link Order:

- o Ensure no conflicting policies have higher precedence

Domain Controllers								
	Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
	1	Default Domain Controllers Policy	No	Yes	Enabled	None	5/20/2025 3:30:27 AM	vlabs1.com
	2	OpenSSHAUTH	No	Yes	Enabled	None	5/25/2025 12:45:44 AM	vlabs1.com

6. Apply Policy and Verify

1. Force Policy Update:

- On DC101, run Command Prompt as Administrator:

gpupdate /force

- Wait for confirmation: Computer Policy update has completed successfully

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

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

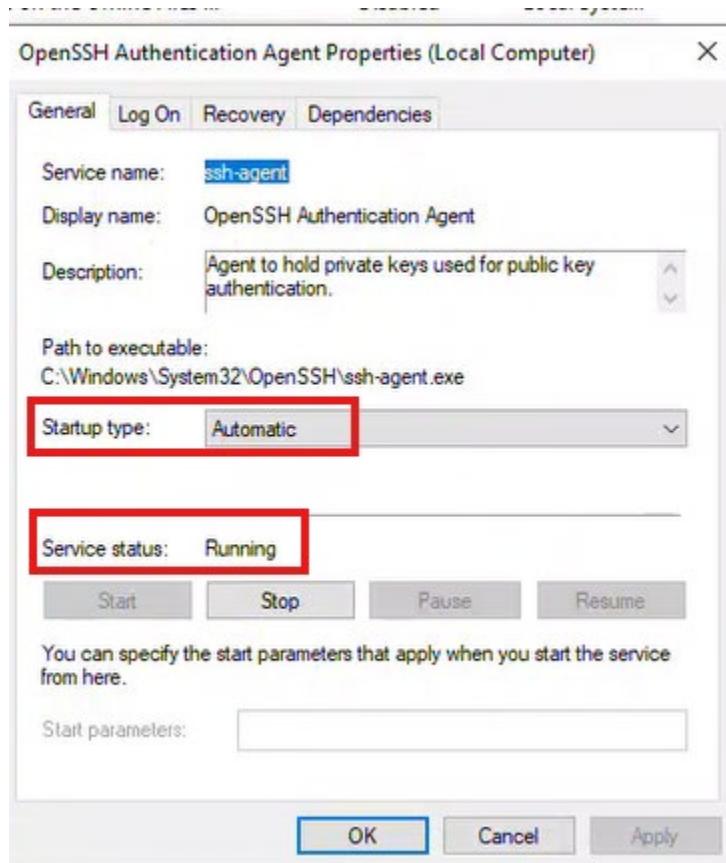
PS C:\Users\Administrator>
```

2. Restart DC101:

3. Verify Service Status:

- After reboot:
 - Open **Services** (services.msc)
 - Locate "**OpenSSH Authentication Agent**"
 - Verify:
 - **Startup Type:** Automatic
 - **Status:** Running

Services (Local)								
Name	Description	Status	Startup Type	Log On As				
OpenSSH Authentication Agent	Agent to hold private keys used for public key authentication.	Running	Automatic	Local System				
Network Store Interface Service	This service delivers network notifications (e.g. interface addition/deleting etc.)	Running	Automatic	Local Service				
Offline Files	The Offline Files service performs maintenance activities on the Offline Files ...	Disabled	Local System	Local System				
Optimize drives	Helps the computer run more efficiently by optimizing files on storage drives.	Manual	Local System	Local System				
Payments and NFC/SE Manager	Manages payments and Near Field Communication (NFC) based secure ele...	Disabled	Local Service	Local Service				
Performance Counter DLL Host	Enables remote users and 64-bit processes to query performance counters p...	Manual	Local Service	Local Service				
Performance Logs & Alerts	Performance Logs and Alerts Collects performance data from local or remot...	Manual	Local Service	Local Service				



9 Task 7: Configuring Folder Redirection

- Use **DC301** as the file server.
- Create a shared folder: **\DC301\(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 **\DC301\userData**.
- Link GPO to **HR** OU,
- Run **gpupdate /force** to apply changes.
- Test with a user from the **HR** OU.

9.1 Objective

Redirect HR users' Documents and Desktop folders to a centralized file server location with user-specific subfolders.

9.2 Steps

9.2.1 Prepare File Server (DC301)

Objective: Create the C:\UserData folder on DC301, set appropriate NTFS permissions, and then create a network share for it, ensuring only the HR group has the necessary access.

a) **Create Shared Folder:**

Open PowerShell or Command Prompt as an administrator. (This is crucial for creating folders under the root, modifying NTFS permissions, and creating network shares.)

```
# 1. Create the folder C:\UserData  
mkdir C:\UserData
```

```
# 2. Set NTFS permissions: Grant the "HR" group Modify rights (OI)(CI)(M)  
# (OI) = Object Inherit: Permissions apply to files in the folder and to files created in  
subfolders.  
# (CI) = Container Inherit: Permissions apply to subfolders in the folder and to subfolders  
created in subfolders.  
# (M) = Modify: Allows reading, writing, executing, and deleting files/subfolders.  
icacls C:\UserData /grant "HR:(OI)(CI)(M)"
```

```
# 3. Share the folder named "UserData" and grant Change permission to the "HR" group  
# "CHANGE" share permission allows users to read, write, and delete files/folders within  
the share.  
net share UserData=C:\UserData /grant:HR,CHANGE
```

The screenshot shows a PowerShell session on a Windows machine. The user runs several commands to create a folder, set NTFS permissions, and share the folder. The output includes the creation of the folder 'UserData' at the root of C:, the execution of 'icacls' command with parameters for inheritance and modification rights, and the execution of 'net share' command to create a share named 'UserData' pointing to the folder 'C:\UserData' with 'CHANGE' permissions granted to the 'HR' group. The session ends with a final command 'PS C:\Users\Administrator> .'. The terminal window has a dark background with white text.

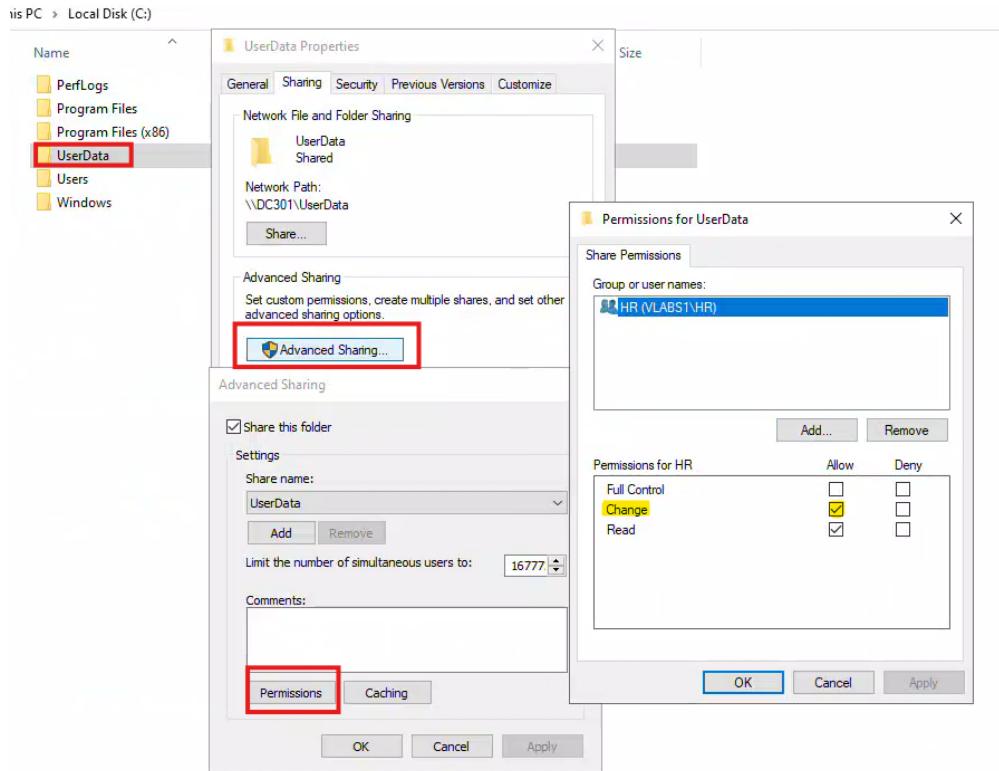
```
PS C:\Users\Administrator> hostname  
DC301  
PS C:\Users\Administrator> whoami  
Labb\administrator  
PS C:\Users\Administrator> # 1. Create the folder C:\UserData  
PS C:\Users\Administrator> mkdir C:\UserData  
  
Directory: C:\  
  
Mode LastWriteTime Length Name  
---- <----- <-----  
d---- 5/25/2025 12:28 PM UserData  
  
PS C:\Users\Administrator> # 2. Set NTFS permissions: Grant the "HR" group Modify rights (OI)(CI)(M)  
PS C:\Users\Administrator> # (OI) = Object Inherit: Permissions apply to files in the folder and to files created in subfolders.  
PS C:\Users\Administrator> # (CI) = Container Inherit: Permissions apply to subfolders in the folder and to subfolders created in subfolders.  
PS C:\Users\Administrator> # (M) = Modify: Allows reading, writing, executing, and deleting files/subfolders.  
PS C:\Users\Administrator> icacls C:\UserData /grant "HR:(OI)(CI)(M)"  
processed file: C:\UserData  
Successfully processed 1 files; Failed processing 0 files  
PS C:\Users\Administrator>  
PS C:\Users\Administrator> # 3. Share the folder named "UserData" and grant change permission to the "HR" group  
PS C:\Users\Administrator> # "CHANGE" share permission allows users to read, write, and delete files/folders within the share.  
PS C:\Users\Administrator> net share UserData=C:\UserData /grant:HR,CHANGE  
UserData was shared successfully.  
  
PS C:\Users\Administrator> .
```

b) **Verify Permissions:**

After running the commands, you can manually verify the permissions by right-clicking on the C:\UserData folder on DC301.

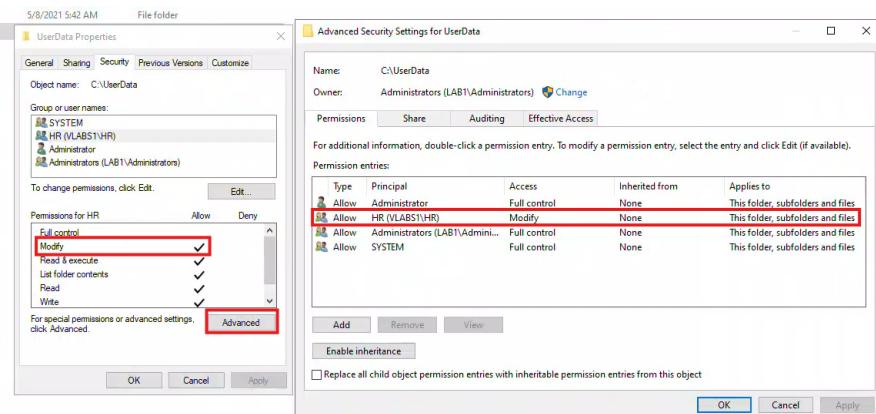
- o Right-click folder → Properties → Sharing → Advance Sharing → Permissions:

- Ensure the HR group has "Change" selected.



- Security tab → NTFS permissions:

Go to **Properties** → **Security** tab → Advance. Ensure the HR group has "**Modify**" permissions, and that it applies to "This folder, subfolders and files".



9.2.2 Create Folder Redirection GPO (DC101)

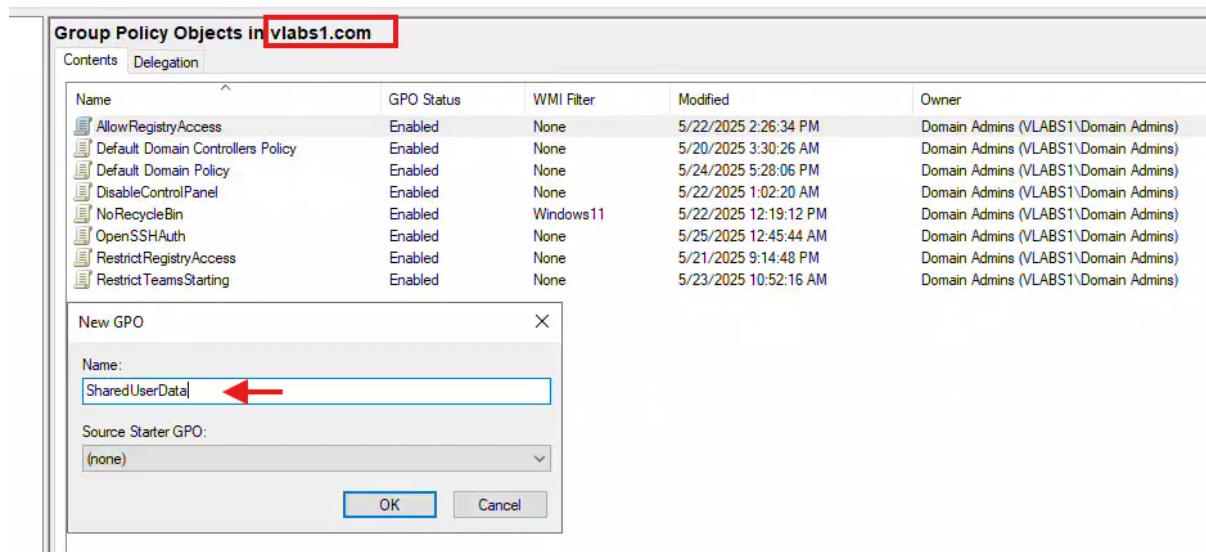
Objective: Create a new GPO named SharedUserData and configure it to redirect users' Documents and Desktop folders to their respective subfolders under <\\DC301\\UserData>.

a) **Open Group Policy Management Console (GPMC):**

On a Domain Controller **DC101**, search for "Group Policy Management" in the Start Menu and open it.

b) **Create the New GPO (SharedUserData):**

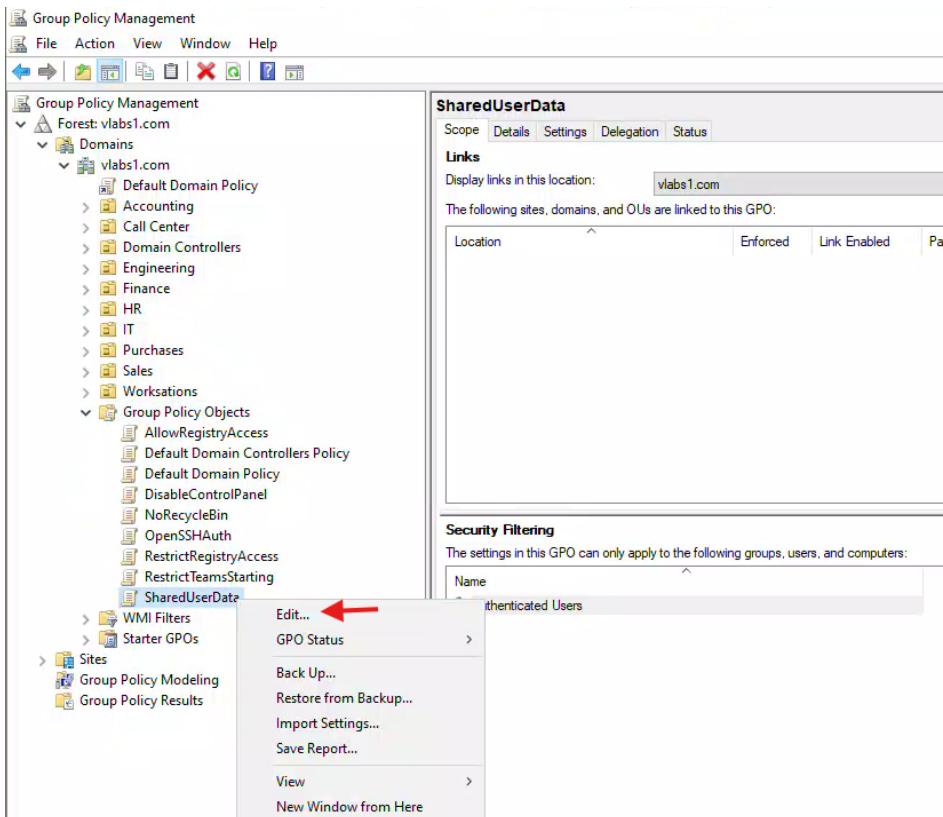
1. In the left-hand pane of GPMC, expand your forest (e.g., vlabs1.com).
2. Expand **Domains**.
3. Expand your domain (vlabs1.com).
4. Right-click on "**Group Policy Objects**" (below your domain name).
5. Select "**New**".
6. In the "New GPO" dialog, type SharedUserData as the GPO name.
7. Click **OK**.



Group Policy Objects in vLabs1.com				
Name	GPO Status	WMI Filter	Modified	Owner
AllowRegistryAccess	Enabled	None	5/22/2025 2:26:34 PM	Domain Admins (VLABS1\Domain Admins)
Default Domain Controllers Policy	Enabled	None	5/20/2025 3:30:26 AM	Domain Admins (VLABS1\Domain Admins)
Default Domain Policy	Enabled	None	5/24/2025 5:28:06 PM	Domain Admins (VLABS1\Domain Admins)
DisableControlPanel	Enabled	None	5/22/2025 1:02:20 AM	Domain Admins (VLABS1\Domain Admins)
NoRecycleBin	Enabled	Windows11	5/22/2025 12:19:12 PM	Domain Admins (VLABS1\Domain Admins)
OpenSSHAuth	Enabled	None	5/25/2025 12:45:44 AM	Domain Admins (VLABS1\Domain Admins)
RestrictRegistryAccess	Enabled	None	5/21/2025 9:14:48 PM	Domain Admins (VLABS1\Domain Admins)
RestrictTeamsStarting	Enabled	None	5/23/2025 10:52:16 AM	Domain Admins (VLABS1\Domain Admins)
SharedUserData	Enabled	None	5/25/2025 6:36:08 PM	Domain Admins (VLABS1\Domain Admins)

c) Edit the New GPO and Navigate to Folder Redirection:

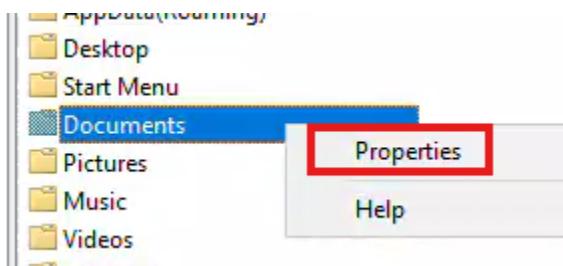
- In the GPMC, under "Group Policy Objects", find your newly created SharedUserData GPO.
- Right-click on SharedUserData and select "**Edit...**". This will open the Group Policy Management Editor.
- In the editor, navigate through the tree: User Configuration -> Policies -> Windows Settings -> Folder Redirection



9.2.3 Configure Documents Redirection (DC101)

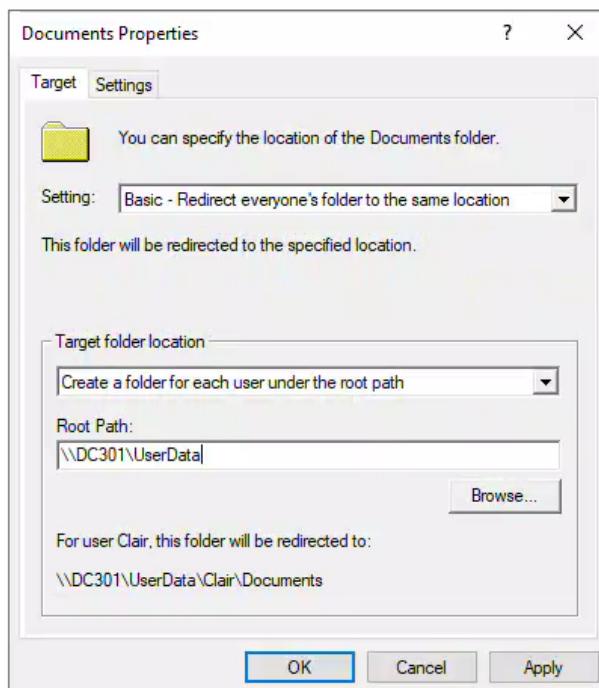
9.2.3.1 Documents

- a) Under Folder Redirection, right-click on "Documents" and select "Properties".



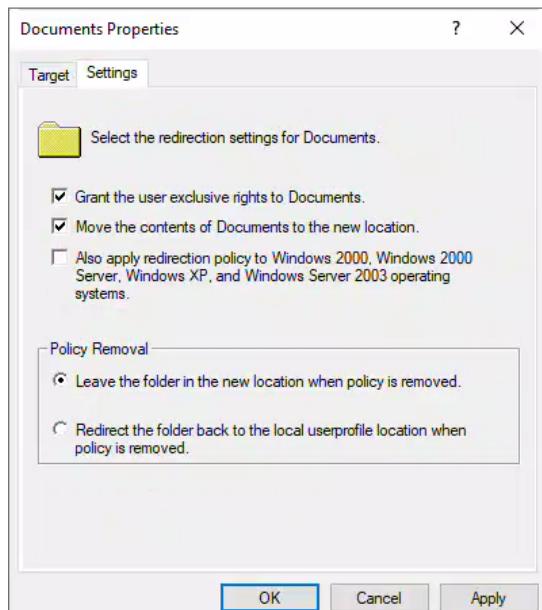
- b) On the "Target" tab:

- o From the "Setting:" drop-down menu, choose: "**Basic - Redirect everyone's folder to the same location**".
- o In the "Root Path:" field, enter the UNC path to your shared folder: \\DC301\(userData)
- o Ensure the checkbox "**Create a folder for each user under the root path**" is selected. (This is crucial for creating <\\DC301\userData\username\Documents>)



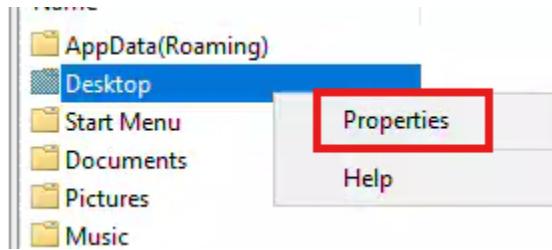
- c) Click on the "Settings" tab:

- Make sure "**Move the contents of Documents to the new location**" is selected (this is usually the default).
 - Check the box for "**Grant the user exclusive rights to Documents**".
 - Uncheck (if checked) "**Redirect the folder back to the local userprofile location when policy is removed**".
- d) Click "**Apply**", then "**OK**". You might get a warning about exclusive rights; click "**Yes**" to confirm.

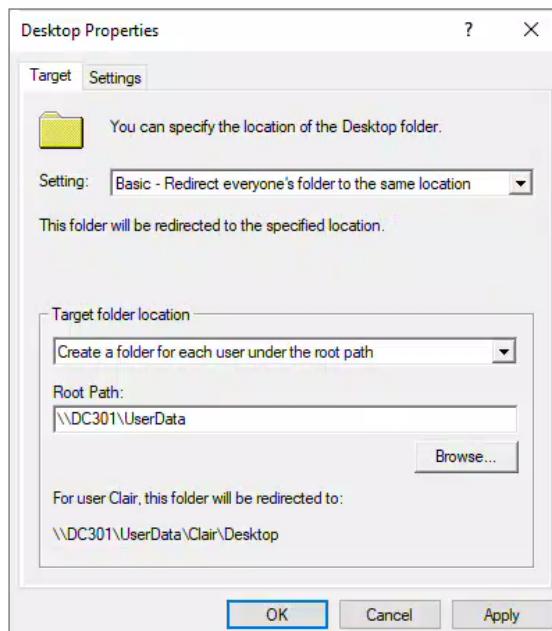


9.2.3.2 Desktop

- a) Ensure you are still in the Group Policy Management Editor for the SharedUserData GPO.
 - o You should be navigated to: User Configuration -> Policies -> Windows Settings -> Folder Redirection.
- b) Right-click on "Desktop" (under Folder Redirection in the left pane).
 - o From the context menu, select "**Properties**".

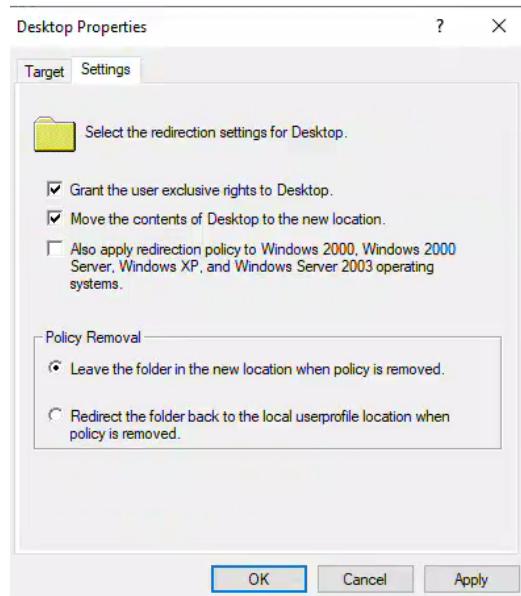


- c) Configure the "Target" Tab:
 - o In the "Desktop Properties" window, go to the "**Target**" tab.
 - o From the "Setting:" drop-down menu, select: "**Basic - Redirect everyone's folder to the same location**".
 - o In the "Root Path:" text field, type the UNC path to your shared folder: \\DC301\ UserData
 - o Verify that the checkbox directly below "Root Path:" which says "**Create a folder for each user under the root path**" is checked. (This will ensure that a structure like \\DC301\ UserData\ <username>\ Desktop is created).



- d) Configure the "Settings" Tab:
 - o Click on the "**Settings**" tab.

- Under "Policy Removal", ensure that:
 - **"Move the contents of Desktop to the new location"** is selected (this is typically the default and moves existing files).
 - The checkbox for **"Grant the user exclusive rights to Desktop"** is **checked**. (This enhances security by ensuring only the user has full control over their redirected folder).
 - The checkbox for **"Redirect the folder back to the local userprofile location when policy is removed"** is **unchecked**. (This means if the GPO is ever removed, the Desktop contents will remain on the network share, preventing data loss).



e) Apply and Confirm:

- Click "**Apply**".
- If a warning message appears (often about granting exclusive rights), click "**Yes**" to proceed.
- Click "**OK**" to close the Desktop Properties window.



You have now configured both Documents and Desktop folder redirection for the SharedUserData GPO. You can now **close** the Group Policy Management Editor.

9.3 Link GPO to HR OU (DC101)

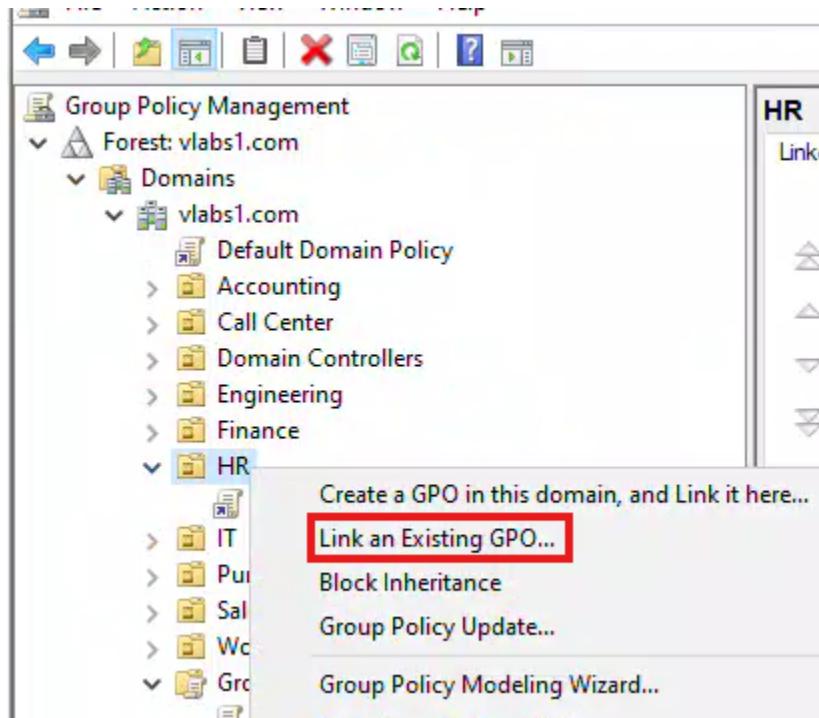
Perform these steps on DC101 or any machine with GPMC installed and administrative access to the domain

Objective: Link the SharedUserData GPO to the HR Organizational Unit (OU) so that its settings apply to users within that OU.

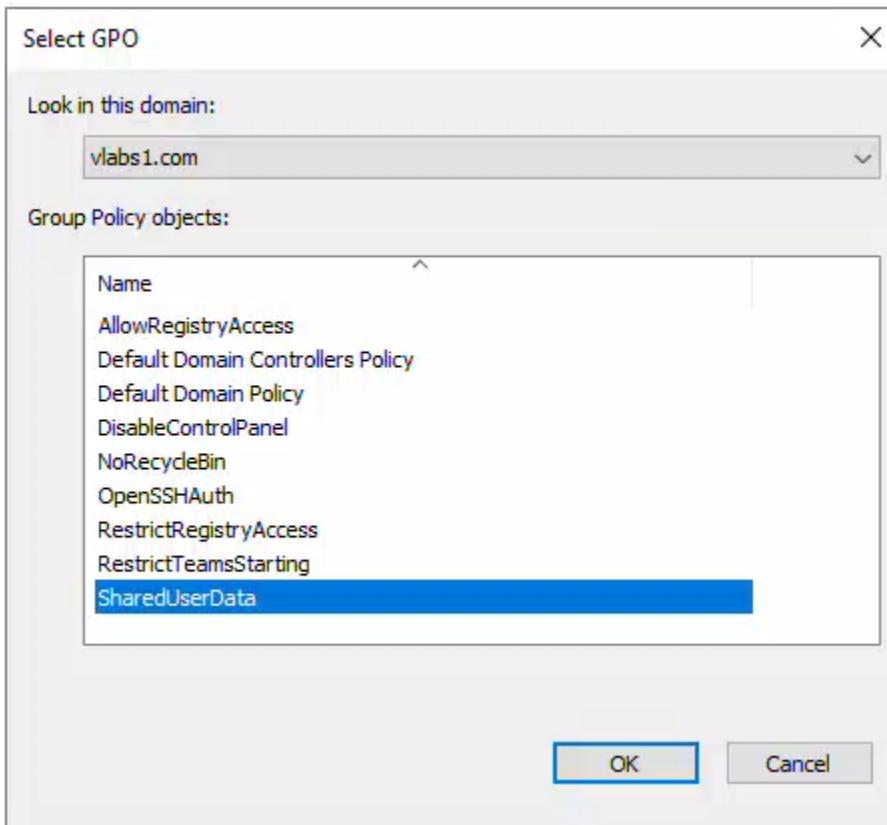
Perform these steps on **DC101**

A. In Group Policy Management Console (GPMC):

- a) In the left-hand pane, navigate to your domain (`vlabs1.com`).
- b) Expand your domain and locate the **HR OU**.
- c) Right-click on the **HR OU**.
- d) Select "**Link an Existing GPO...**".



- e) In the "Select GPO" dialog, choose "**SharedUserData**" from the list.
- f) Click "**OK**".



HR								
		Linked Group Policy Objects	Group Policy Inheritance	Delegation				
	Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
		1	DisableControlPanel	No	Yes	Enabled	None	5/22/2025 1:02:21 AM
		2	SharedUserData	No	Yes	Enabled	None	5/25/2025 7:18:30 PM

B. Verify Link Order:

- With the **HR OU** still selected in the left-hand pane of GPMC, click on the "**Linked Group Policy Objects**" tab in the right-hand pane.
- Observe the "**Link Order**" column.

Is this the right order?

For **Folder Redirection**, the link order with `DisableControlPanel` usually doesn't create a direct conflict. Folder redirection settings are in a different area of Group Policy than Control Panel restrictions.

- `DisableControlPanel` typically configures user interface restrictions (User Configuration -> Policies -> Administrative Templates -> Control Panel).
- `SharedUserData` configures folder redirection (User Configuration -> Policies -> Windows Settings -> Folder Redirection).

These are separate policy areas, so it's **highly unlikely** that `DisableControlPanel` would override or interfere with your folder redirection settings.

Therefore, in this specific scenario, leaving the order as `DisableControlPanel` at 1 and `SharedUserData` at 2 is likely perfectly fine. Your folder redirection should still apply as intended.



9.4 Apply and Test

Objective: Force the policy update on Client1, verify the folder redirection, and test file operations.

9.4.1 Verify HR users (DC101)

On DC101 open Active Directory Administrative Center

The screenshot shows the Active Directory Users and Computers interface. On the left, the navigation pane lists various organizational units under 'vLabs1 (local)'. The 'HR' folder is selected and highlighted in blue. The main pane displays the 'HR (25)' group with a table of users and their types. A detailed view of 'Adem Vasseur' is shown at the bottom.

	Name	Type
	Adem Vasseur	User
	Ambre Rousseau	User
	Andrea Klein	User
	Benjamin Guyot	User
	Blanche Guerin	User
	Charlie Legrand	User
	Dylan Schneider	User
	elise Henry	User
	Emma Petit	User
	Ethan Michel	User
	Evan Julien	User
	Giulia Dumont	User
	HR	Group
	Ilian Breton	User
	Killian Perrier	User
	Lina Rivière	User
	Livia Martinez	User
	Madeline Vidal	User
	Marvin Michaud	User

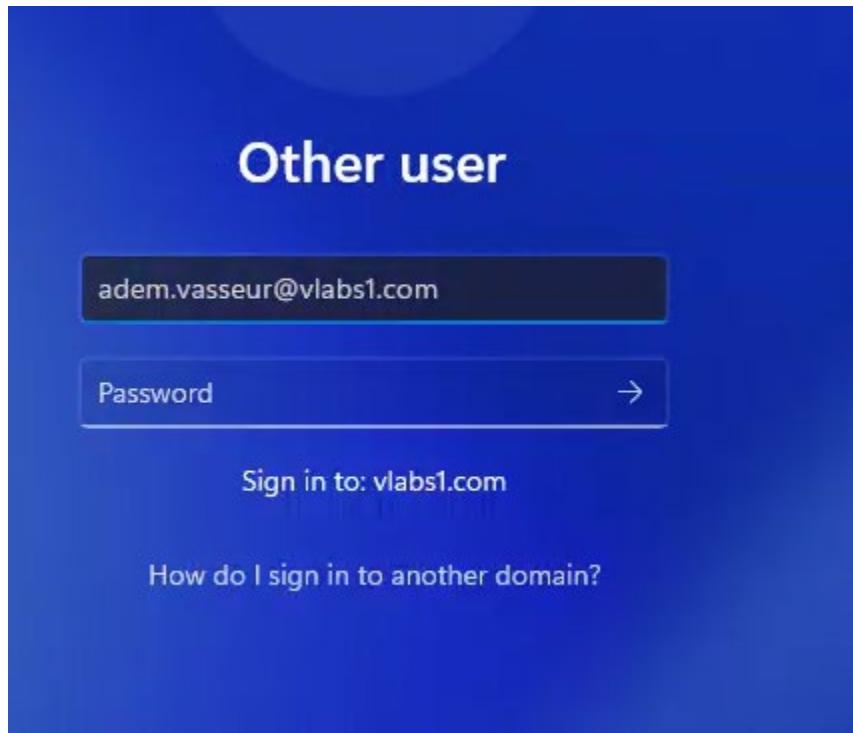
Adem Vasseur

User logon: adem.vasseur
E-mail:
Modified: 5/21/2025 10:31 PM
Description:

9.4.2 Client1

Action (Perform these steps on Client1, logged in as an HR user):

1. **Force Policy Update (On Client1):**
 - o Log in to **Client1** using an account that is a member of the **HR Group**.



- Open **Command Prompt** or **PowerShell** (you don't necessarily need admin privileges for gpupdate /force as a regular user).
- Run the command:

gpupdate /force

This command forces the computer and user policies to refresh immediately.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\adem.vasseur> whoami
vlabs1\adem.vasseur
PS C:\Users\adem.vasseur> hostname
Client1
PS C:\Users\adem.vasseur> gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.

The following warnings were encountered during user policy processing:

The Group Policy Client Side Extension Folder Redirection was unable to apply one or more settings because the changes must be processed before system startup or user logon. The system will wait for Group Policy processing to finish completely before the next startup or logon for this user, and this may result in slow startup and boot performance.

For more detailed information, review the event log or run GPRESULT /H GPReport.html from the command line to access information about Group Policy results.

Certain user policies are enabled that can only run during logon.

OK to log off? (Y/N)
```

- After gpupdate /force completes (or not complete), you will need to **log off from Client1 and then log back on**. Folder redirection settings for users are applied during logon.

Check with:

gpresult /r

```
PS C:\Users\adem.vasseur> gpresult /r

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

Created on 2025- 05- 25 at 7:49:47 PM

RSOP data for VLABS1\adem.vasseur on CLIENT1 : Logging Mode
-----
OS Configuration: Member Workstation
OS Version: 10.0.26100
Site Name: N/A
Roaming Profile: N/A
Local Profile: C:\Users\adem.vasseur
Connected over a slow link?: No

USER SETTINGS
-----
CN=Adem Vasseur,OU=HR,DC=vlabs1,DC=com
Last time Group Policy was applied: 2025-05-25 at 7:49:04 PM
Group Policy was applied from: DC101.vlabs1.com
Group Policy slow link threshold: 500 kbps
Domain Name: VLABS1
Domain Type: Windows 2008 or later

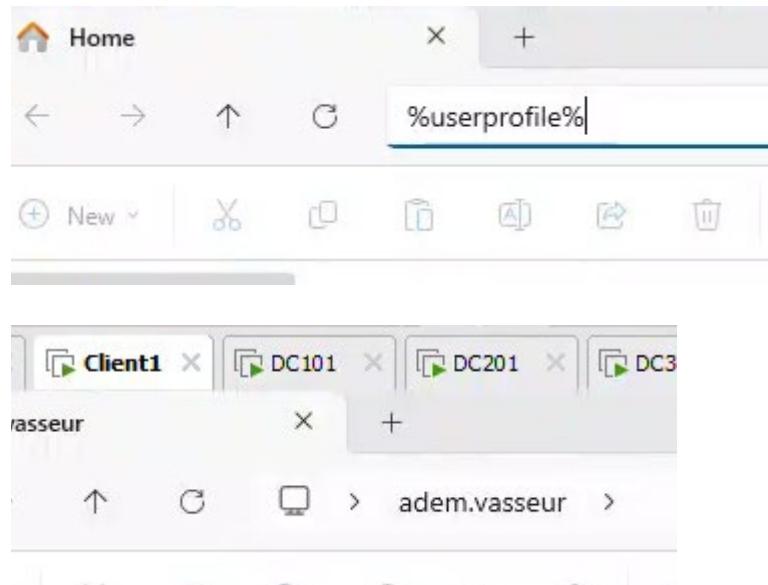
Applied Group Policy Objects
-----
DisableControlPanel
SharedUserData ←

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

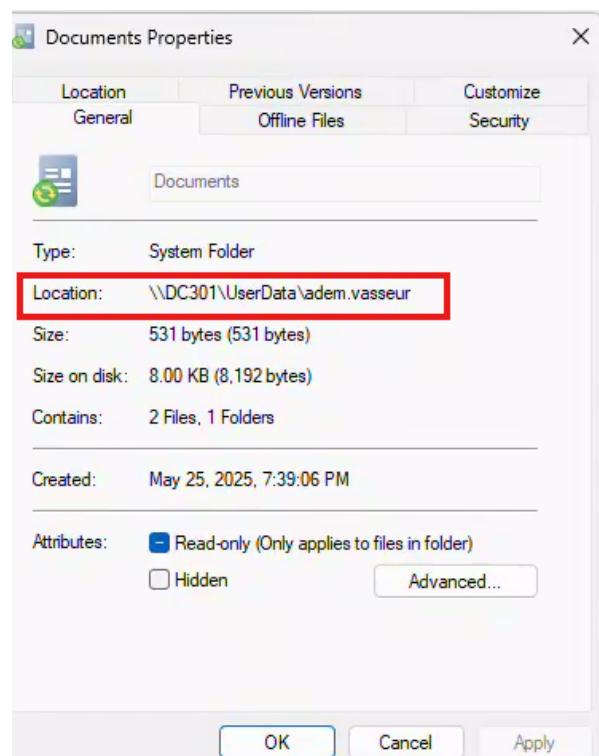
The user is a part of the following security groups
-----
Domain Users
Everyone
BUILTIN\Users
NT AUTHORITY\INTERACTIVE
CONSOLE LOGON
NT AUTHORITY\Authenticated Users
This Organization
LOCAL
HR
Authentication authority asserted identity
Medium Mandatory Level

PS C:\Users\adem.vasseur>
```

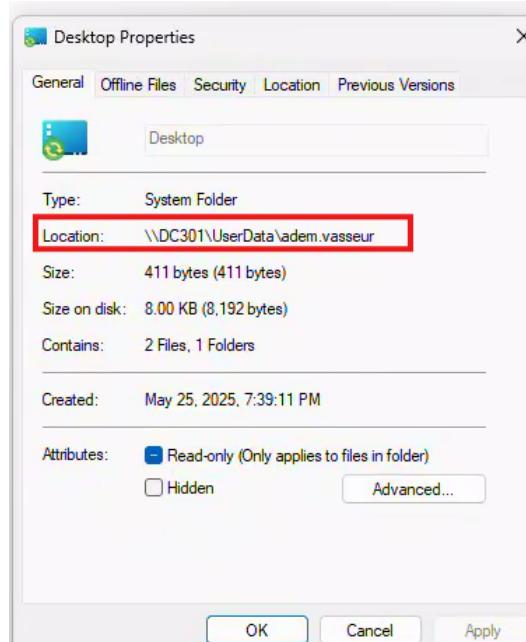
2. Verify Redirection (On Client1, after logging back on as an HR user):
 - o Open File Explorer.
 - o In the address bar, type %userprofile% and press Enter.



- Look for your "**Documents**" and "**Desktop**" folders.
- **Check the path:**
 - For "Documents": Right-click on the "Documents" folder, select **Properties**, then go to the **Location** tab. The path should now show \\DC301\\UserData\\<your_username>\\Documents.



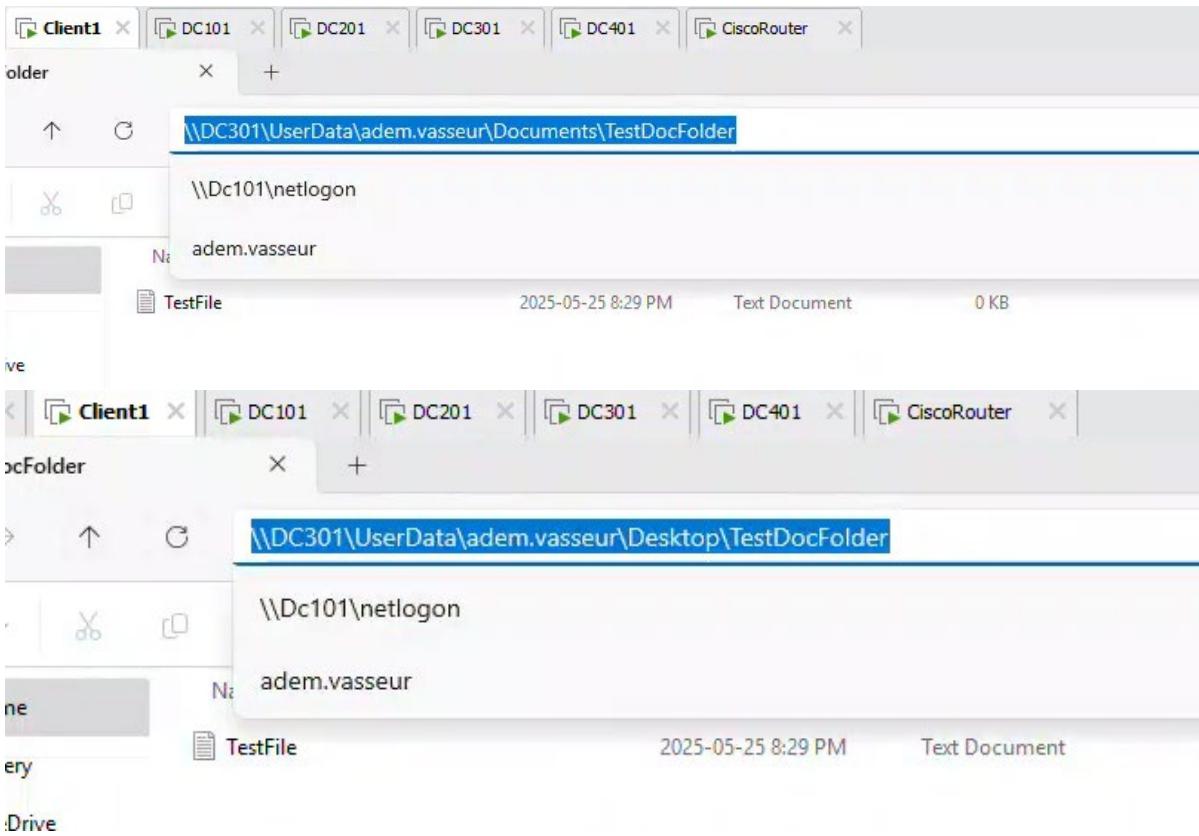
- For "Desktop": Similarly, right-click on the "Desktop" folder, select **Properties**, then go to the **Location** tab. The path should show \\DC301\\UserData\\<your_username>\\Desktop.



- Alternatively, from a **Command Prompt** on Client1, you can type echo %UserProfile%\Desktop and echo %UserProfile%\Documents to see what local paths they point to. If redirection is successful, File Explorer's properties are the most definitive visual check.

3. Test File Operations (On Client1 and DC301):

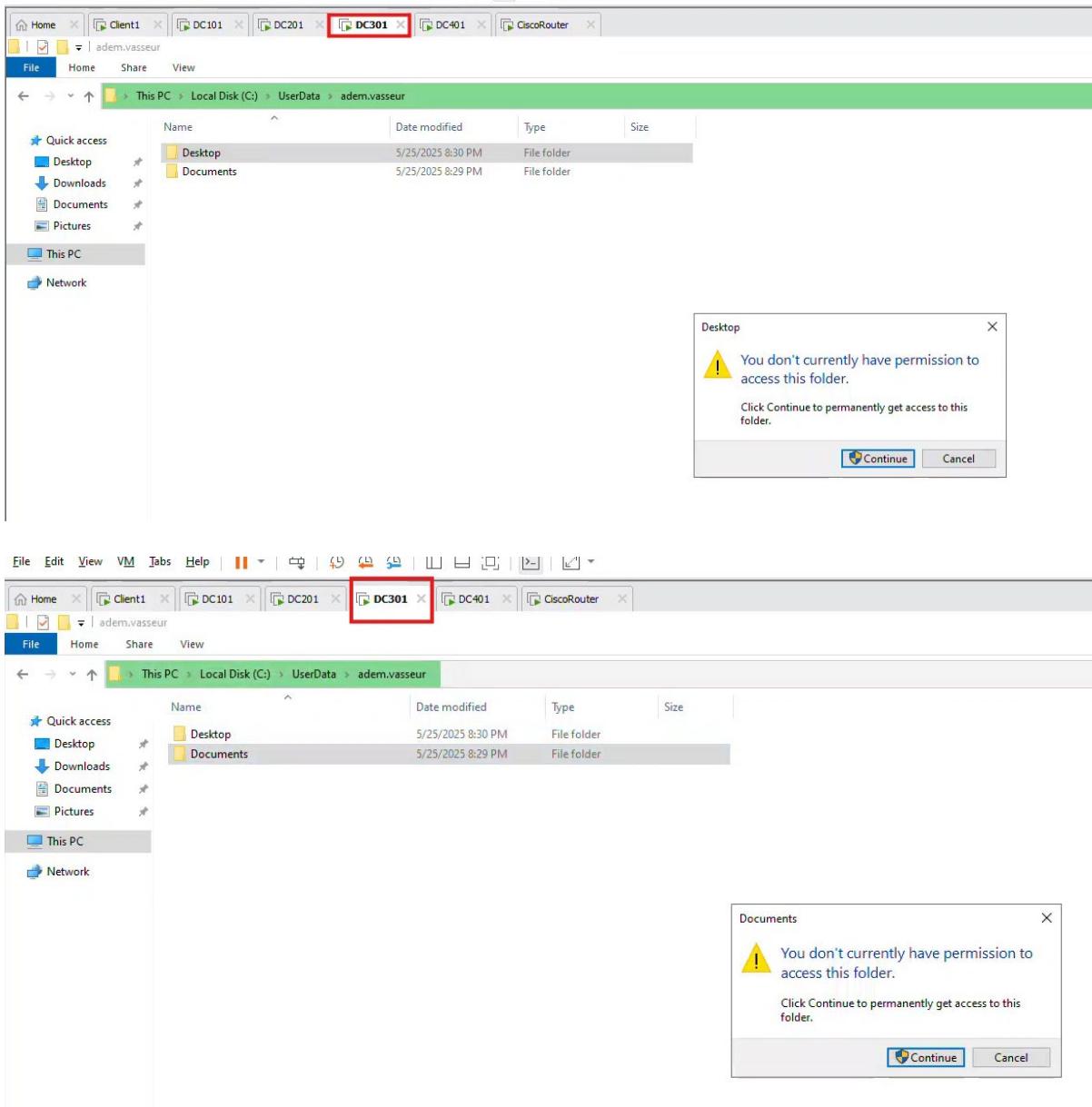
- **On Client1 (as the HR user):**
 - Go to your Documents folder (which is now redirected).
 - Create a new folder (e.g., TestDocFolder).
 - Create a new text file inside it (e.g., TestDocFile.txt).
 - Repeat the same process for your Desktop (create a new folder and a new text file on the desktop).



- **On DC301 (File Server):**

- Open File Explorer and navigate to C:\UserData.
- You should now see a new folder named after the HR user you logged in as (e.g., C:\UserData\HRUser1).
- Open that user's folder, then navigate into the Documents and Desktop subfolders.
- Verify that TestDocFolder and TestDocFile.txt (and any other files/folders you created) appear in their respective locations on DC301. **This part is not working yet I can not access the contents of the folders. I can only see the folders**

- **But on the other hand maybe is not necessary to access the contents of the folders just the folders....**



Verification Table

Check	Expected Result
Documents path	<code>\DC301\ UserData \<user>\Documents</code>
Desktop path	<code>\DC301\ UserData \<user>\Desktop</code>

Check	Expected Result
File creation	Files appear on server
Permissions	Only user+admin can access their folder

10 Task 8: Managing Software Installation

- Create a network share: \\DC301\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 **DC301_Teams_Installation**.
- Assign the **Teams MSI package** installation to the **Engineering OU**.
- Run **gpupdate /force** to apply changes.
- Restart **Client1**, 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).

10.1 Objective:

Deploy Microsoft Teams silently to Engineering OU users and verify installation while testing the auto-start restriction policy.

10.2 Steps

10.2.1 Prepare Software Distribution Point

a) On DC301 (File Server)

```
# Create Software folder
mkdir C:\Software

# Create network share with read access for Everyone
net share Software=C:\Software /grant:Everyone,READ

# Verify share creation
Get-SmbShare -Name Software
```

```

PS C:\UserData\adem.vasseur\Documents> hostname
DC301
PS C:\UserData\adem.vasseur\Documents> whoami
lab1\administrator
PS C:\UserData\adem.vasseur\Documents> # Create Software folder
PS C:\UserData\adem.vasseur\Documents> mkdir C:\Software

    Directory: C:\

Mode                LastWriteTime         Length Name
----                -----          ----- 
d-----        5/26/2025   1:43 AM            Software

PS C:\UserData\adem.vasseur\Documents>
PS C:\UserData\adem.vasseur\Documents> # Create network share with read access for Everyone
PS C:\UserData\adem.vasseur\Documents> net share Software=C:\Software /grant:Everyone,READ
Software was shared successfully.

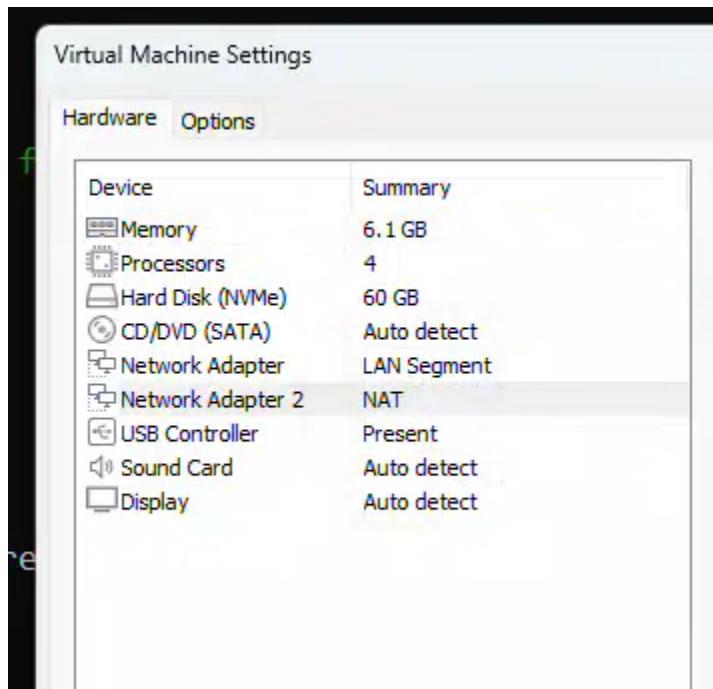
PS C:\UserData\adem.vasseur\Documents>
PS C:\UserData\adem.vasseur\Documents> # Verify share creation
PS C:\UserData\adem.vasseur\Documents> Get-SmbShare -Name Software

Name      ScopeName Path          Description
----      -----      ----- 
Software *      *      C:\Software

PS C:\UserData\adem.vasseur\Documents>

```

- b) Temporarily enable NAT NIC (manually via Hyper-V or network settings)
DC101



- c) Download Teams MSI (check latest version at <https://learn.microsoft.com/en-us/microsoftteams/msi-deployment#msi-files>)

Welcome to Teams

Get started

Deployment overview

Enterprise setup

Enterprise setup overview

Architecture & telephony solutions posters

Get your organization ready

Set up Teams in your org

Adopt

Client deployments

New Teams client

Classic Teams clients

Get the classic Teams clients

Bulk install classic Teams using Windows Installer

Classic Teams for Virtualized Desktop Infrastructure (VDI)

Classic Teams for Remote Desktop environment (RDP)

Learn / Microsoft Teams /

Bulk install classic Teams using Windows Installer (MSI)

Article • 10/30/2024 • 36 contributors • Applies to: Microsoft Teams

[Feedback](#)

In this article

[MSI files](#)

How the Microsoft Teams MSI file works

Clean up and redeployment procedure

Prevent Teams from starting automatically after installation

Important

The classic Team client is no longer supported. This client is not receiving further updates, including security updates. The classic Teams client will not work after June 30, 2025. You must upgrade to the new Teams client before that time. See [The new Microsoft Teams](#) for more information.

Important

MSI files

The table below provides links to 32-bit, 64-bit, and ARM64 MSI files for Teams. Download the MSI that you want to install on computers in your organization. The x86 architecture (32-bit or 64-bit) Teams supports is independent of other Office apps installed on a computer.

 Note

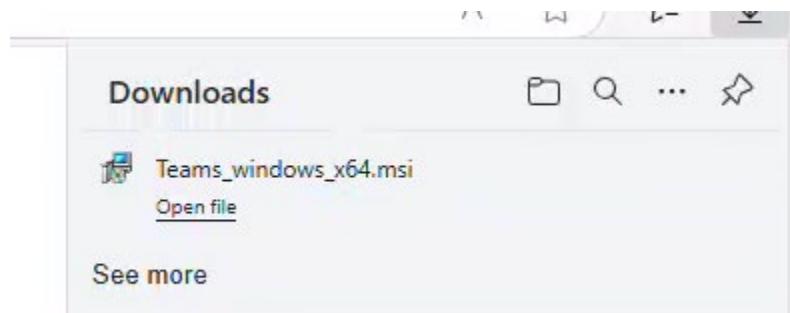
New builds are released regularly. If you have previously downloaded the MSI, confirm if you have the most current version. Learn more: [Version update history for the Microsoft Teams app](#)

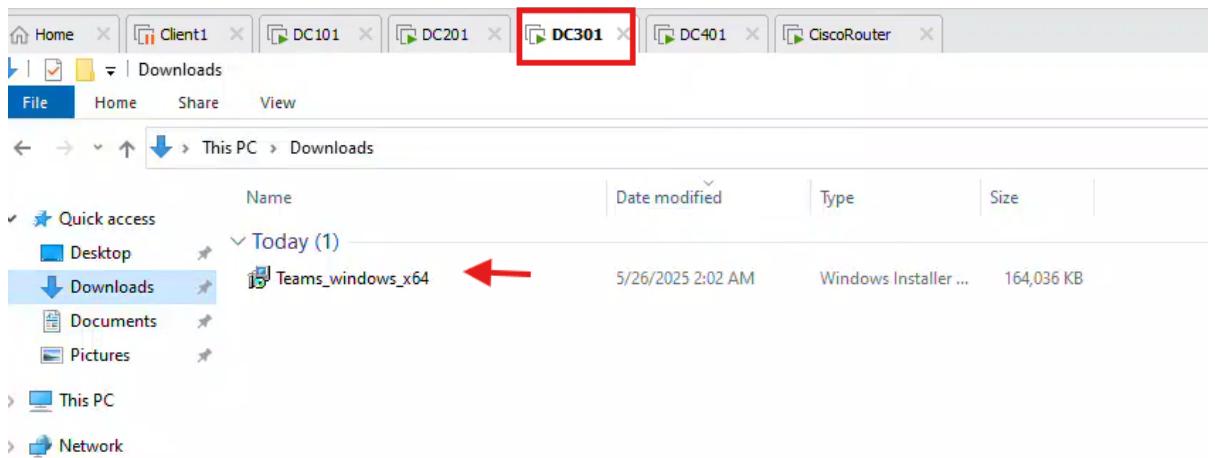
If you have 64-bit computers, we recommend installing the 64-bit Teams MSI even if the computer is running a 32-bit version of Office. The ARM64 MSI can only be installed on computers that use the ARM architecture, such as the Surface Pro X.

 Important

Install the 64-bit version of Teams only on 64-bit operating systems. If you try to install the 64-bit version of Teams on a 32-bit operating system, the installation won't be successful and you won't receive an error message.

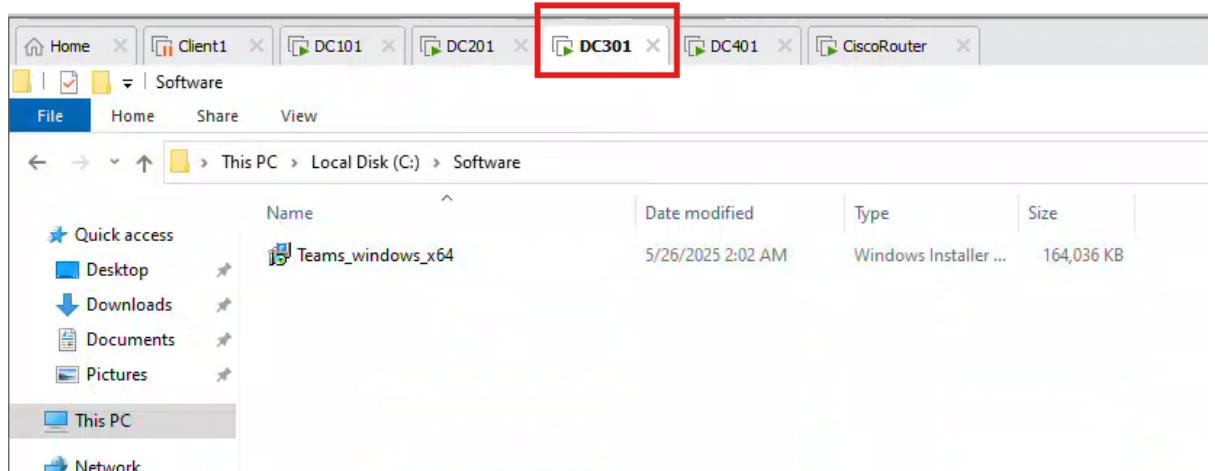
Entity	32-bit	64-bit	ARM64
Commercial	32-bit	64-bit	ARM64
U.S. Government - GCC	32-bit	64-bit	ARM64
U.S. Government - GCC High	32-bit	64-bit	ARM64



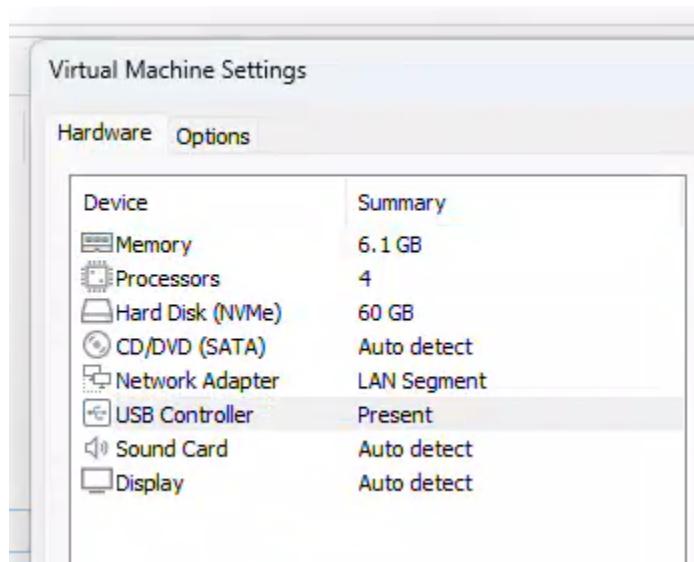


d) Verify download

Move to C:\Software\Teams_windows_x64.msi

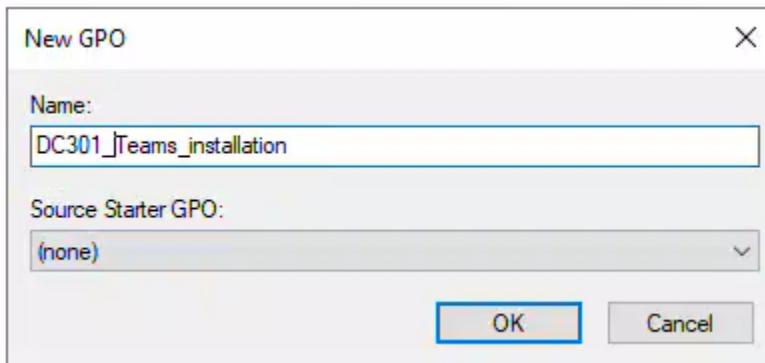


e) Disable NAT NIC (manually via Hyper-V or network settings)

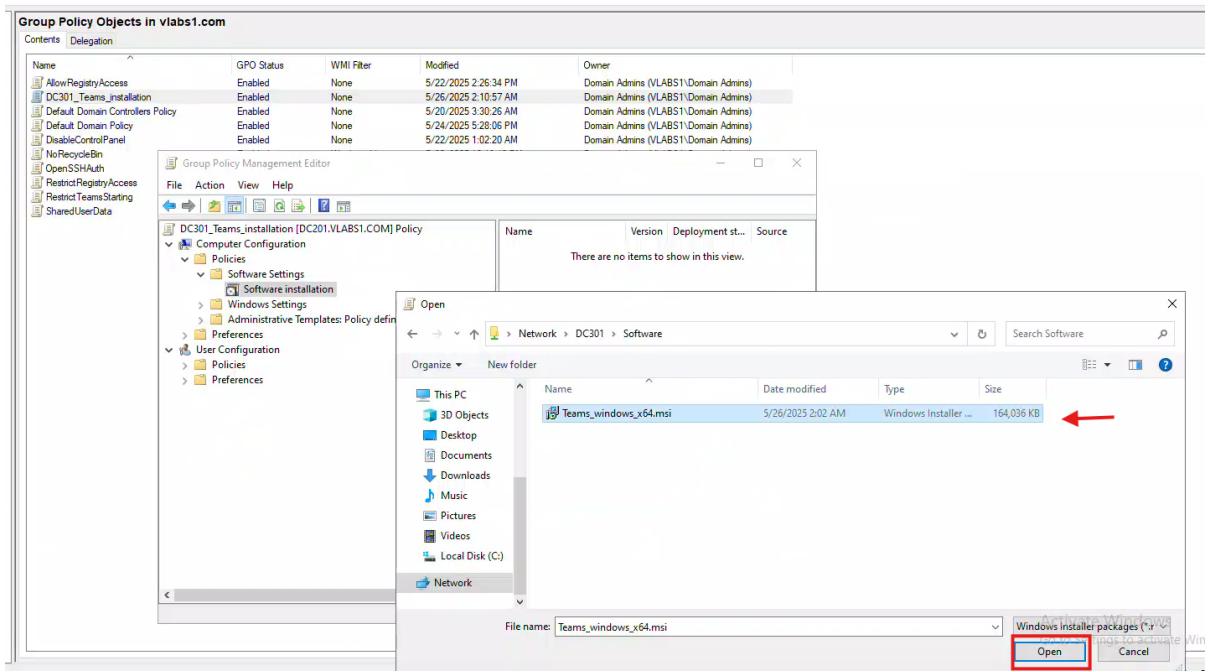


10.2.2 Create Software Installation GPO in DC101

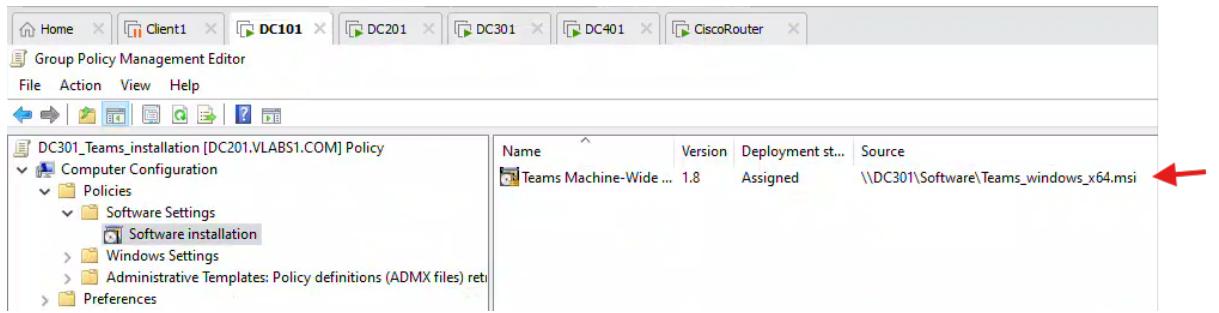
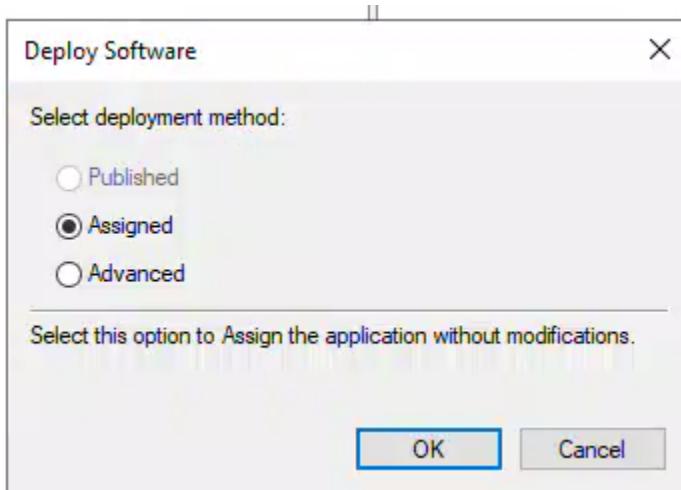
- Open Group Policy Management (gpmc.msc).
- Right-click Group Policy Objects → New.
- Name: DC301_Teams_Installation → OK.



- Right-click the new GPO → Edit.
- Navigate to:
Computer Configuration → Policies → Software Settings → Software Installation.
- Right-click → New → Package.
- Browse to \\DC301\Software\Teams_windows_x64.msi.



h) Select Assigned (mandatory installation).

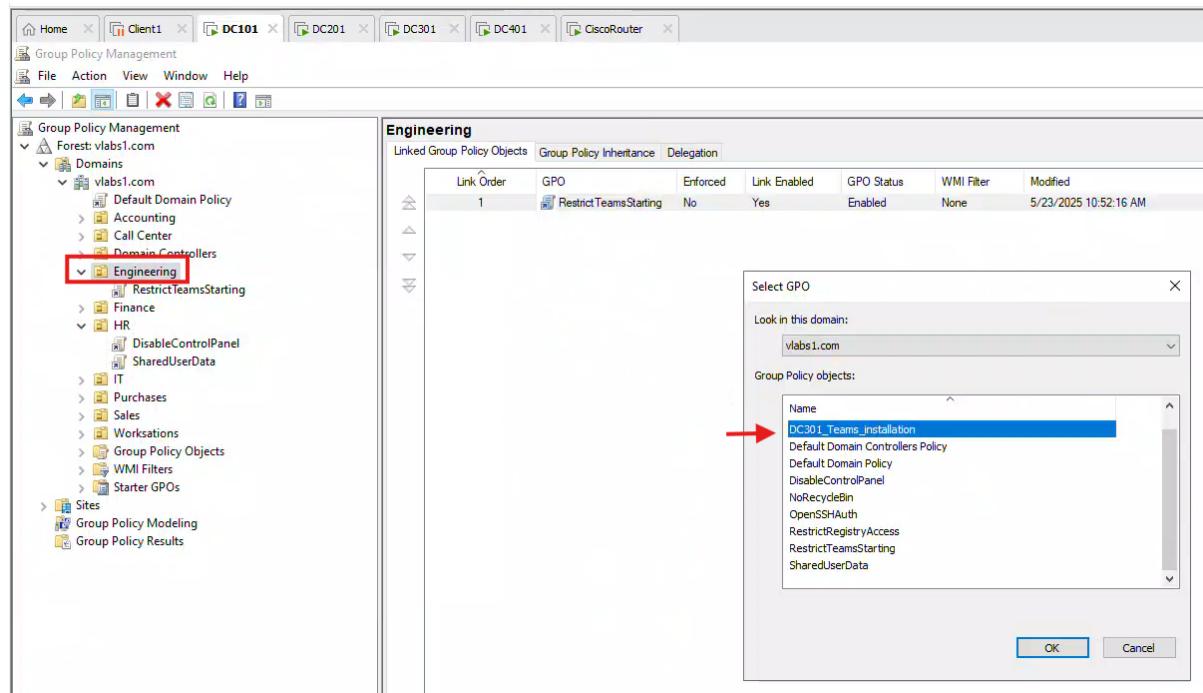


i) Close the GPO Editor.

10.2.3 Link GPO to Engineering OU (DC101)

a) In GPMC:

- o Right-click **Engineering OU** → **Link an Existing GPO**
- o Select **DC301_Teams_Installation** → Click **OK**



b) Verify Precedence:

- o Ensure **RestrictTeamsStarting** GPO (from Task 2) is still applied

Engineering							
Linked Group Policy Objects		Group Policy Inheritance		Delegation			
Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	RestrictTeamsStarting	No	Yes	Enabled	None	5/23/2025 10:52:16 AM	vlab1.com
2	DC301_Teams_Installation	No	Yes	Enabled	None	5/26/2025 2:16:01 AM	vlab1.com

c) Verify engineering users

Active Directory Administrative Center

Active Directory Administrative Center > vlabs1 (local)

Active Directory... < Engineering (26)

Overview

vlabs1 (local)

- Users
- Accounting
- Builtin
- Call Center
- Computers
- Domain Controllers
- Engineering
- Finance
- ForeignSecurityPrincipals
- HR
- IT
- Keys
- LostAndFound
- Managed Service Account
- NTDS Quotas
- Program Data
- Purchases
- Sales
- System
- TPM Devices
- Workstations

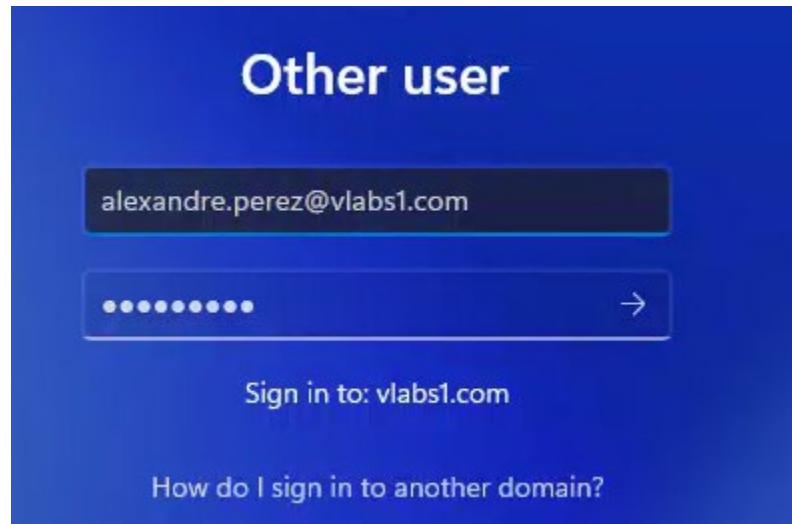
Filter

Name	Type
Agathe Bonnet	User
Alexandre Perez	User
Anaelle Vincent	User
Antoine Jacquet	User
Benoît Carr	User
Callista Boyer	User
Clea Gauthier	User
Eliot Fernandez	User
Elo Roussel	User
Engineering	Group
Gabin Prevost	User
Gabriel Lefebvre	User
Heloïse Marie	User
Inès Robert	User
Isaac Besson	User
Leny Leblanc	User
Leonie Lucas	User
Loanne Girard	User
Mario Caron	User
Agathe Bonnet	User

10.2.4 Apply- Client1

a) Force Policy Update:

1. Log in to Client1. With engineering user



2. Open **Command Prompt** as an administrator.
3. Type `gpupdate /force` and press Enter.
4. Wait for the policy update to complete successfully.

```
PS C:\WINDOWS\system32> whoami
vlabs1\administrator
PS C:\WINDOWS\system32> hostname
Client1
PS C:\WINDOWS\system32> gpupdate /force
Updating policy...

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

PS C:\WINDOWS\system32>
```

10.2.5 Verify Teams installation:

- **Restart Client1.** This is important for the assigned software installation policy to take effect.
- Log in to Client1 with a user account that is a member of the **Engineering OU**.



- **Verify Teams Installation:**

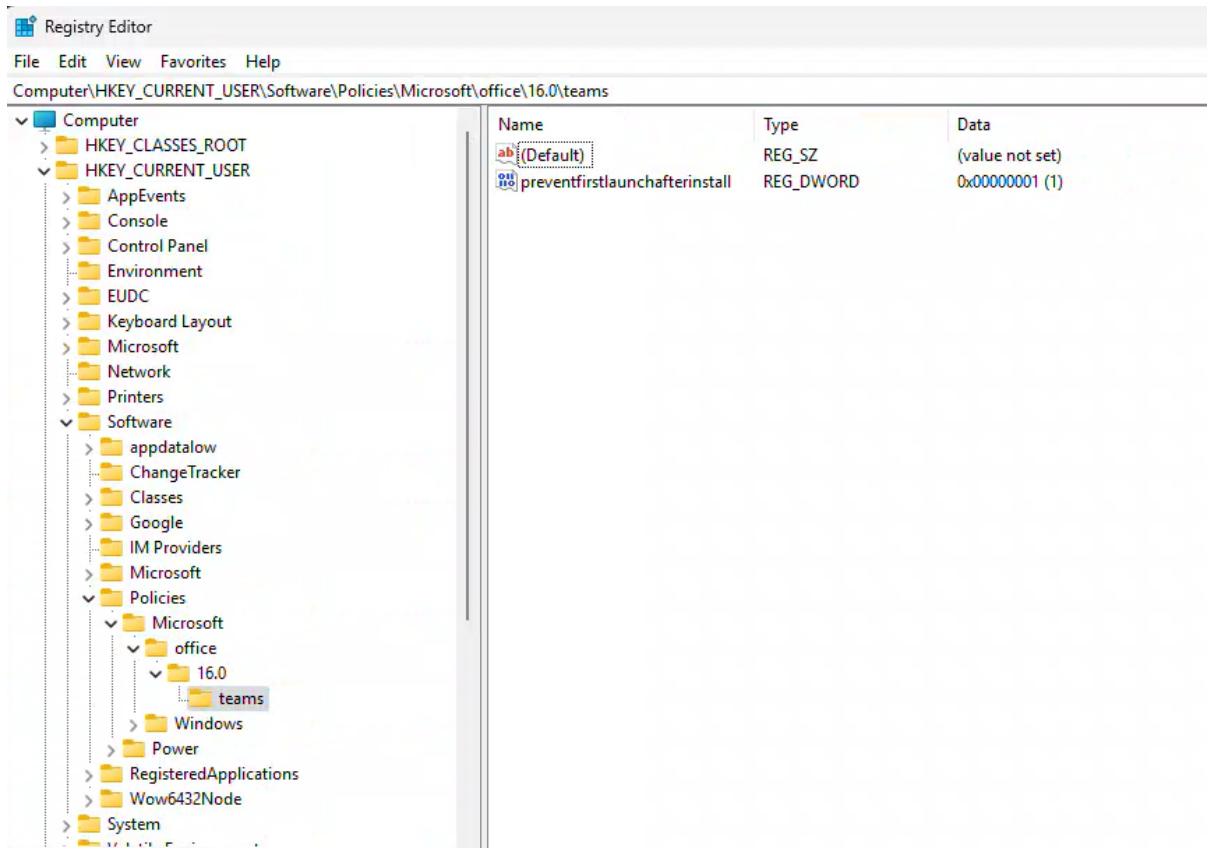
- You can also verify by going to Control Panel > Programs > Programs and Features and looking for Microsoft Teams in the list of installed programs.

```
PS C:\Users\alexandre.perez> Get-Package -Name "*Microsoft Teams*"
Name          Version      Source      ProviderName
---          ---        ---        ---
Microsoft Teams Meeting Add... 1.25.8601      msi

PS C:\Users\alexandre.perez> |
```

- **Confirm Teams Auto-start Behavior:**

Registry Verification: The corresponding registry value, PreventFirstLaunch (or PreventFirstLaunchAfterInstalled), located at HKEY_CURRENT_USER\Software\Policies\Microsoft\Teams, is correctly set to 1 on Client1 for the user. This 1 value signifies that the policy is active and instructing Teams not to auto-start.
Winning GPO: The RestrictTeamsStarting GPO is confirmed as the "Winning GPO" for this particular setting, meaning no other GPO is overriding it.



Verification Table

Check	Expected Result
MSI in network share	Accessible at \\DC301\Software
Software installation	Teams appears in Programs
Auto-start behavior	Teams doesn't launch at login
GPO precedence	RestrictTeamsStarting overrides default behavior

11 Task 9: Managing Scripts with GPO

- Create a shared folder on \\DC301\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: \\DC301\Public**
- Store the script in **\DC101\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 **Client1** and verifying the drive mapping.
- Try to create files and folders in this drive.

11.1 Objective

Create and deploy a logon script via Group Policy to automatically map a network drive for all domain users, then verify functionality.

11.2 Steps

11.2.1 1. Prepare Shared Folder on DC301

1. On DC301 (File Server):

- Create folder and set permissions (use powershell as administrator)

Create the folder

mkdir C:\Public

Set NTFS permissions (Everyone: Modify, which includes Read, Write, Execute)

icacls C:\Public /grant "Everyone:(OI)(CI)(M)"

Create the network share

net share Public=C:\Public /grant:Everyone,FULL

```

PS C:\UserData\adem.vasseur\Documents> # Create the folder
PS C:\UserData\adem.vasseur\Documents> mkdir C:\Public

Directory: C:\

Mode           LastWriteTime     Length Name
----           -----          ---- 
d----  5/26/2025   3:51 AM            Public

PS C:\UserData\adem.vasseur\Documents>
PS C:\UserData\adem.vasseur\Documents> # Set NTFS permissions (Everyone: Modify, which includes Read, Write, Execute)
PS C:\UserData\adem.vasseur\Documents> icacls C:\Public /grant "Everyone:(OI)(CI)(M)"
processed file: C:\Public
Successfully processed 1 files; Failed processing 0 files
PS C:\UserData\adem.vasseur\Documents>
PS C:\UserData\adem.vasseur\Documents> # Create the network share
PS C:\UserData\adem.vasseur\Documents> net share Public=C:\Public /grant:Everyone,FULL
Public was shared successfully.

PS C:\UserData\adem.vasseur\Documents> -

```

2. Verify Share:

- From Client1, test access:

[dir \\DC301\Public](\\DC301\Public)

```

PS C:\Users\alexandre.perez> dir \\DC301\Public
PS C:\Users\alexandre.perez> |

```

11.2.2 Create Logon Script

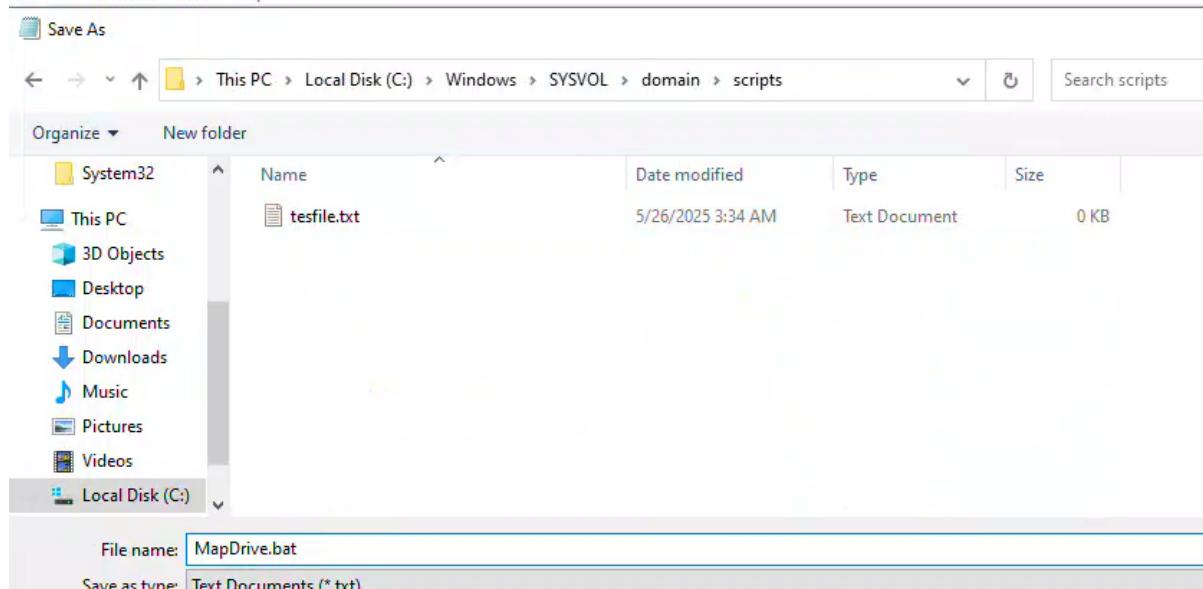
1. On DC101 (Domain Controller):

- Open Notepad and create MapDrive.bat with:

@echo off

net use Z: \\DC301\Public /persistent:yes

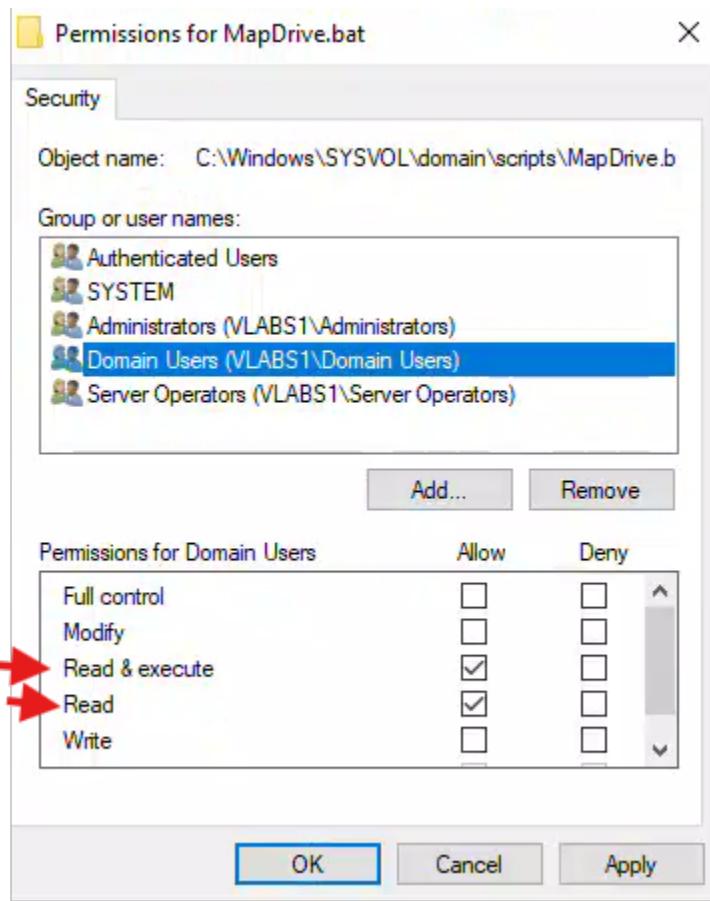
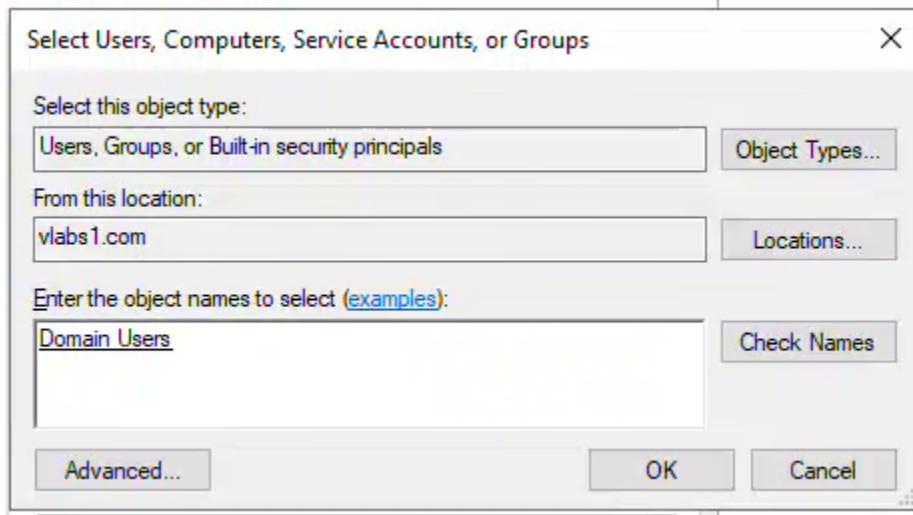
- Save to: C:\Windows\SYSVOL\domain\scripts\MapDrive.bat

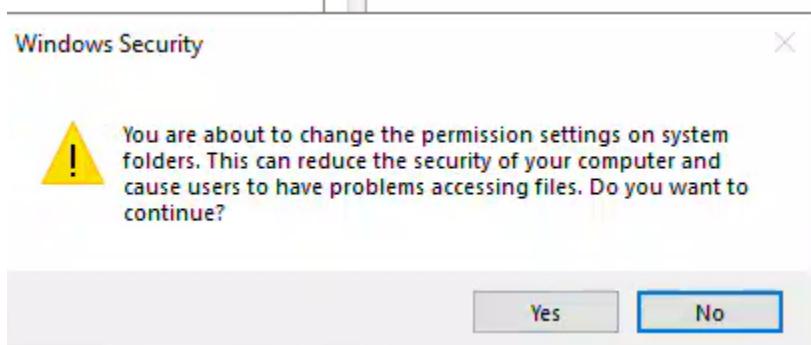


```
@echo off
net use Z: \\DC301\\Public /persistent:yes
```

2. Set Permissions:

- Right-click on `MapDrive.bat` and select **Properties**.
- Go to the **Security** tab.
- Click **Edit...**
- Click **Add...**
- Type `Domain Users` in the object name field, click **Check Names**, then **OK**.
- Select `Domain Users` from the list.
- Ensure `Read & execute` is checked under "Allow." Also ensure `Read` is checked.
- Click **OK** twice to apply the permissions.

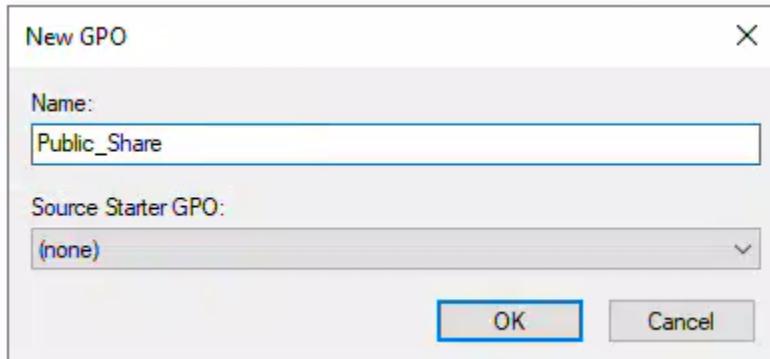




11.2.3 Configure GPO for Script Deployment (DC101)

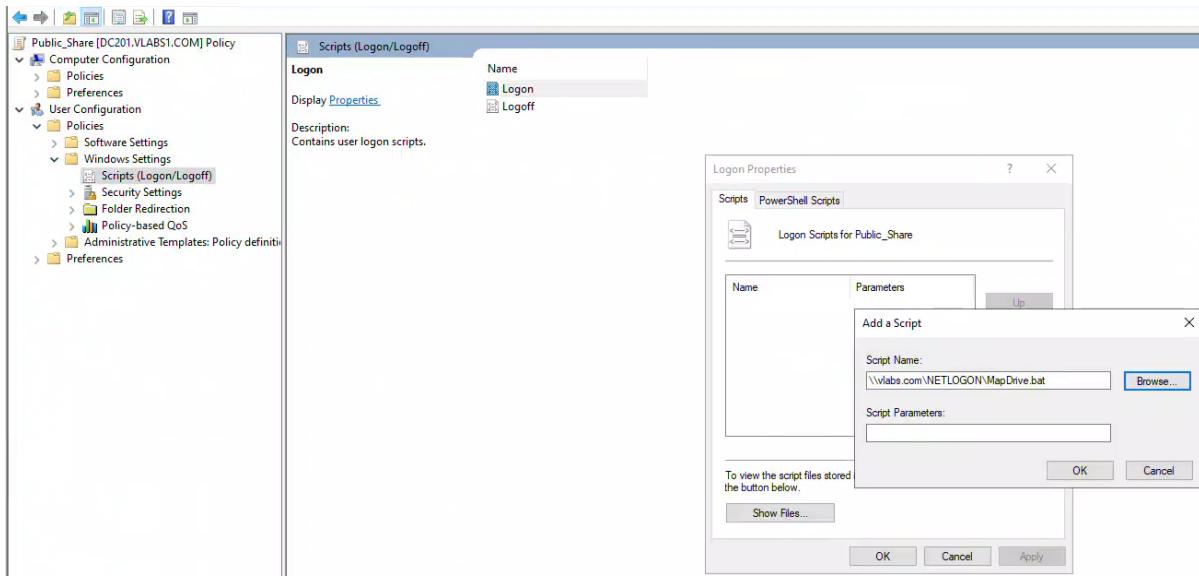
1. In GPMC (gpmc.msc):

- o Right-click **Group Policy Objects** → **New**
- o Name: **Public_Share** → Click **OK**



2. Add Logon Script:

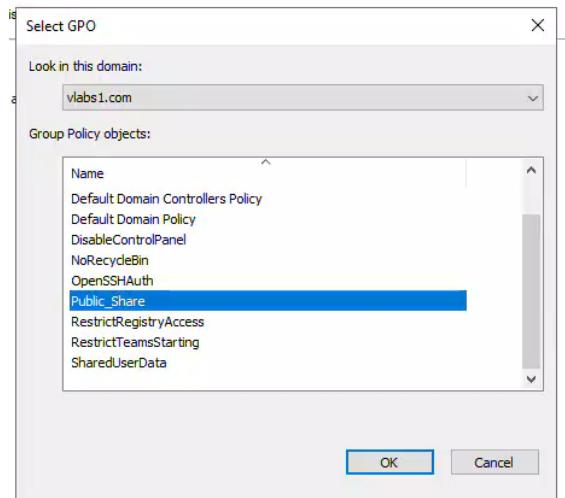
- o Right-click → **Edit**
- o Navigate to: User Configuration → Policies → Windows Settings → Scripts (Logon/Logoff)
- o Double-click **Logon** → Click **Add**
- o Browse to: \\vlabs1.com\NETLOGON\MapDrive.bat
- o Click **OK** twice



11.2.4 Link GPO to Domain Level

1. In GPMC:

- In the left pane, right-click on your **Domain** (vlabs1.com).
- Select **Link an Existing GPO....**
- From the "Select GPO" dialog, choose **Public_Share**.
- Click **OK**.



\

Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	Default Domain Policy	No	Yes	Enabled	None	5/24/2025 5:28:06 PM	vlabs1.com
2	Public_Share	No	Yes	Enabled	None	5/26/2025 4:13:26 AM	vlabs1.com

11.2.5 Force Policy Update:

Open Command Prompt as an Administrator.

Run the following command to force a Group Policy update:

```
gpupdate /force
```

Wait for the policy update to complete successfully.

```
PS C:\WINDOWS\system32> gpupdate /force
Updating policy...

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

PS C:\WINDOWS\system32>
```

11.2.6 Verification Testing

1. Test Drive Mapping

1. Log in to Client1 as any domain user
2. Verify:
 - o Z: drive appears in File Explorer
 - o Command prompt shows mapping:

net use
Should list "Z: \DC301\Public"

```
PS C:\Users\andrea.klein> net use
New connections will be remembered.

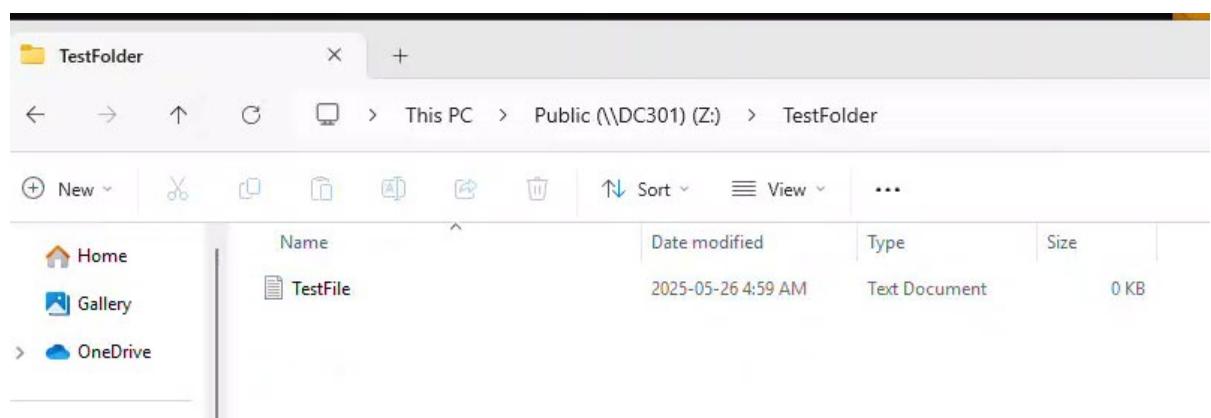
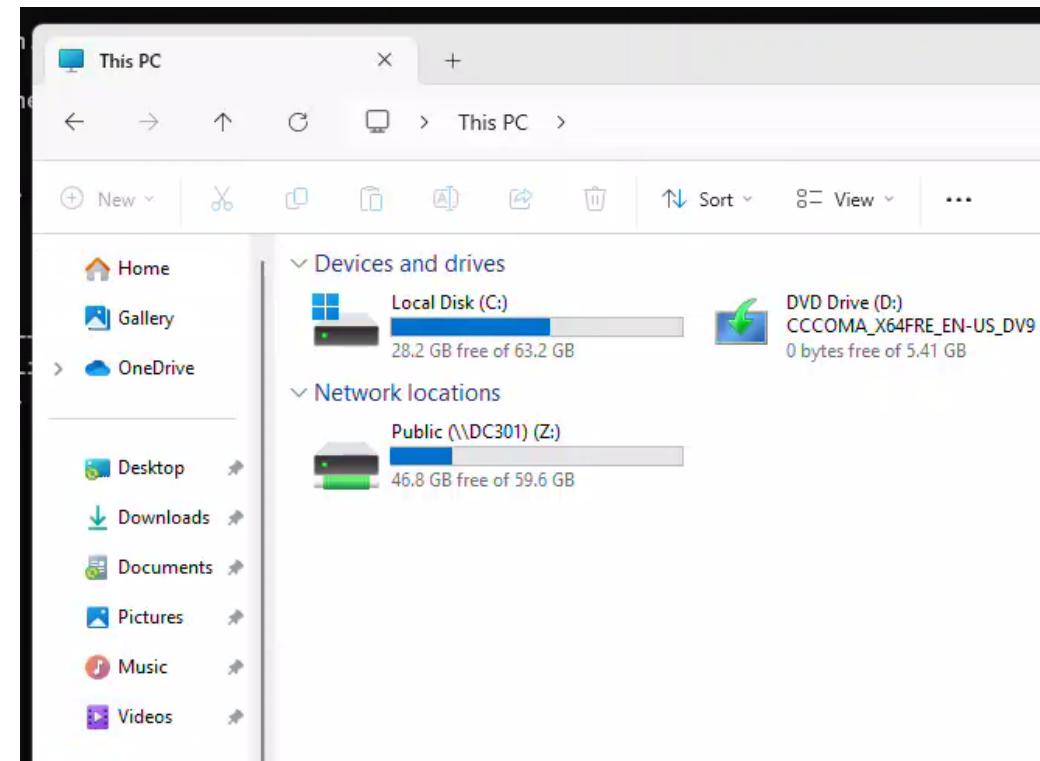
Status       Local     Remote                               Network
-----       ----     -----                               -----
OK          Z:        \\DC301\Public                         Microsoft Windows Network
The command completed successfully.

PS C:\Users\andrea.klein>
```

3. Test File Operations

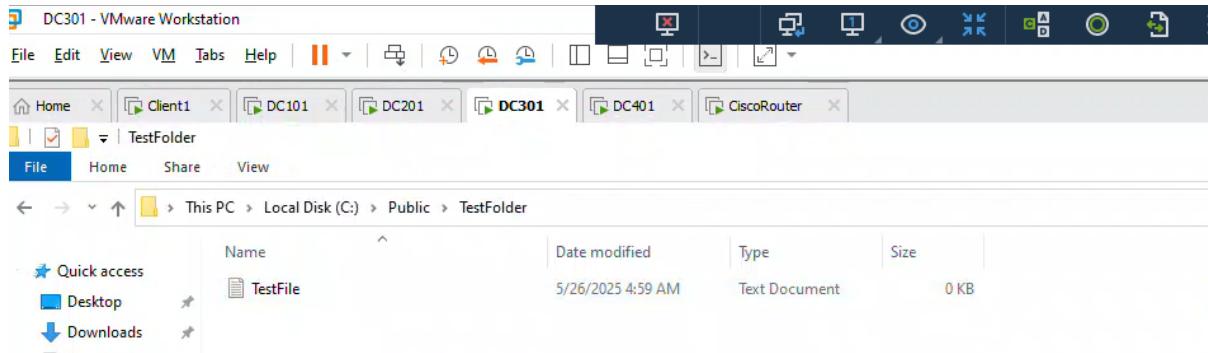
1. Create Test Files:

- o In Z: drive:
 - New folder: Right-click → New → Folder
 - New file: Right-click → New → Text Document

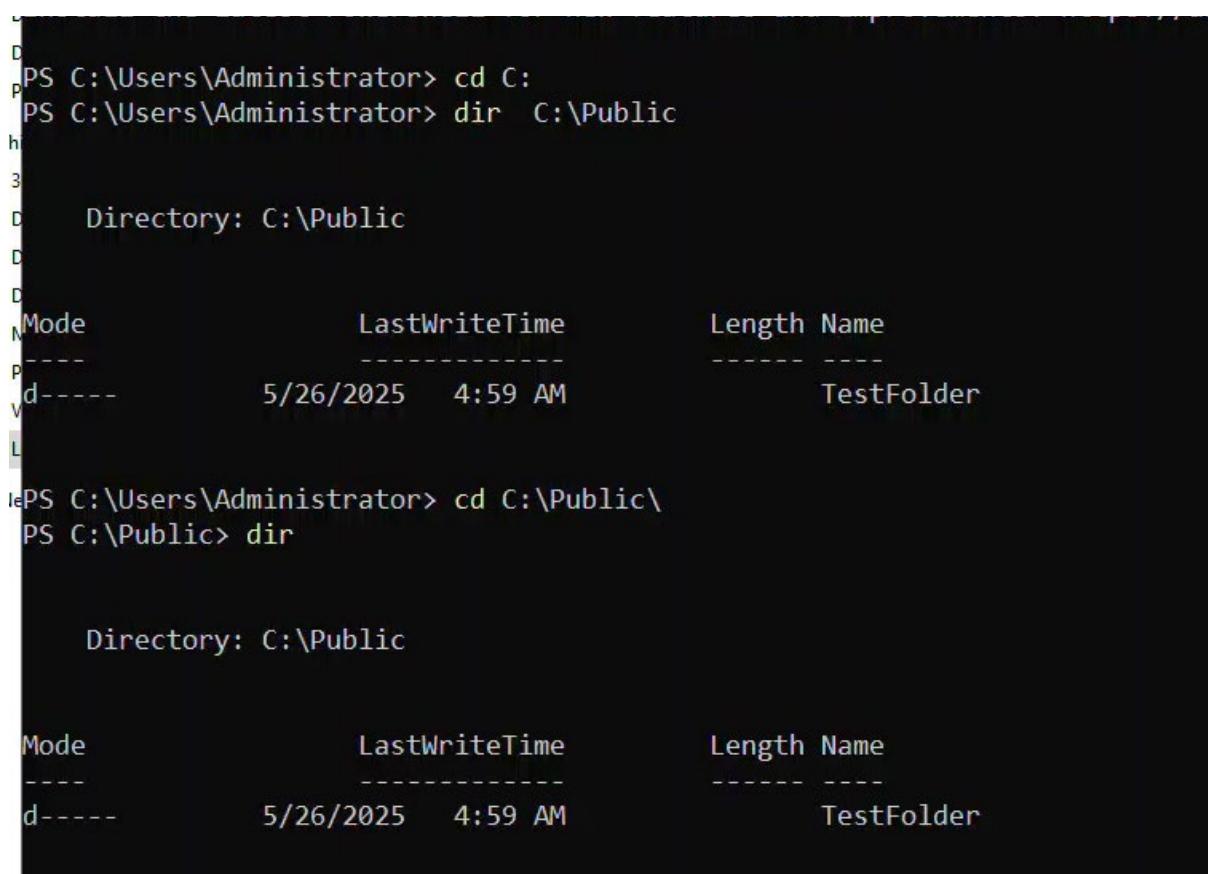


2. Verify on DC301:

- Check files appear in: C:\Public



A screenshot of a Windows File Explorer window titled "DC301 - VMware Workstation". The window shows a navigation pane with tabs for Home, Client1, DC101, DC201, DC301 (which is selected), DC401, and CiscoRouter. Below the tabs, there are buttons for File, Home, Share, and View. The main area displays the path "This PC > Local Disk (C:) > Public > TestFolder". A list of items is shown, with "TestFile" being the only item listed under "Name". The details pane shows "Date modified: 5/26/2025 4:59 AM", "Type: Text Document", and "Size: 0 KB".



A screenshot of a PowerShell session. The command "PS C:\Users\Administrator> cd C:" is run, followed by "PS C:\Users\Administrator> dir C:\Public". The output shows the directory structure and contents of C:\Public. Then, the command "PS C:\Users\Administrator> cd C:\Public\>" is run, followed by "PS C:\Public> dir". The output shows the directory structure and contents of the C:\Public directory.

```
PS C:\Users\Administrator> cd C:
PS C:\Users\Administrator> dir C:\Public
h
3

D Directory: C:\Public
D
D
Mode LastWriteTime      Length Name
N----- -----
P----- 5/26/2025 4:59 AM
V-----                   TestFolder

L

PS C:\Users\Administrator> cd C:\Public\>
PS C:\Public> dir

Directory: C:\Public

Mode LastWriteTime      Length Name
N----- -----
d----- 5/26/2025 4:59 AM
                   TestFolder
```