

Table of Contents

Lab Assignment 2 (Part II) - GPO	2
Task 1: Creating a Central Store for Administrative Templates	2
Task 2: Managing and Configuring Administrative Templates	5
Task 3: Managing Account Policies.....	10
Task 4: Implementing Fine-Grained Password Policies.....	15
Task 5: Managing Audit Authentication	18
Task 6: Managing Security Templates	22
Task 7: Configuring Folder Redirection	28
Task 8: Managing Software Installation.....	34
Task 9: Managing Scripts with GPO	38

Lab Assignment 2 (Part II) - GPO

Task 1: Creating a Central Store for Administrative Templates

System: DC107

Step 1 - What is a Central Store and why are we doing this?

The Central Store is a special shared folder used by Group Policy to load administrative templates (ADMX and ADML files). Instead of each administrator using local template files, the Central Store ensures everyone edits policies using the same files. It also makes the environment easier to manage and avoids version mismatches.

Step 2 - Create the Central Store folder in SYSVOL

We need to create a new folder called PolicyDefinitions inside the domain's SYSVOL path.

This folder must be created using the domain name, not the hostname of the server.

Run this command from DC107 to create the folder:

```
md \\vlabs07.com\SYSVOL\vlabs07.com\Policies\PolicyDefinitions
```

```
PS C:\Users\Administrator> md \\vlabs07.com\SYSVOL\vlabs07.com\Policies\PolicyDefinitions

Directory: \\vlabs07.com\SYSVOL\vlabs07.com\Policies

Mode                LastWriteTime         Length Name
----                -              -          -
d-----        5/23/2025   2:11 PM            PolicyDefinitions
```

Step 3 - Copy ADMX files into the Central Store manually

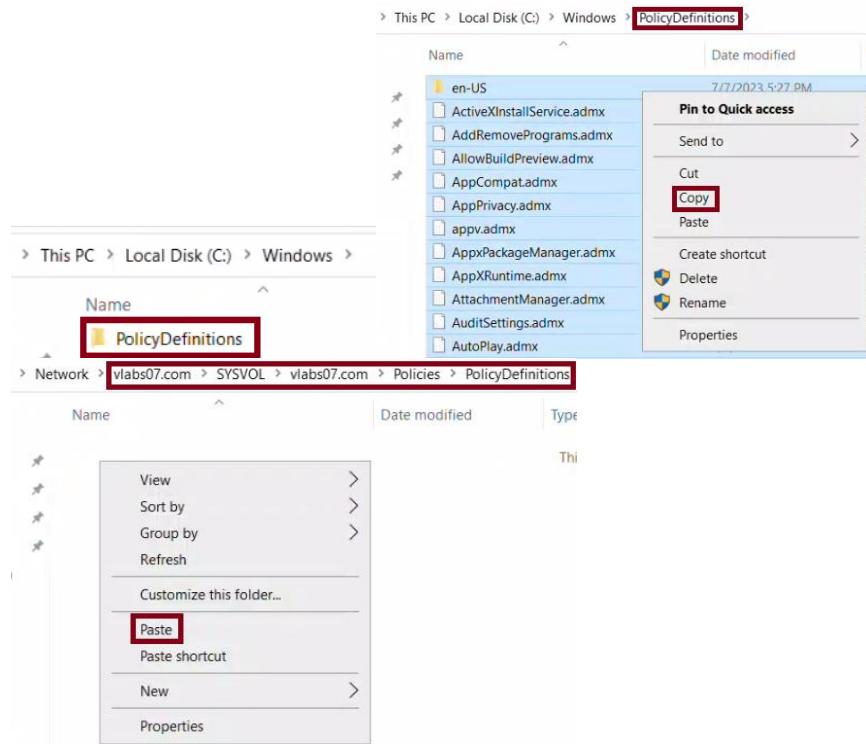
The ADMX files define the settings you see in the Group Policy Editor.

We will manually copy them from the local folder:

C:\Windows\PolicyDefinitions

Open File Explorer and go to: C:\Windows\PolicyDefinitions
Select all the .admx files, right-click → Copy

Now go to: \\vlabs07.com\SYSVOL\vlabs07.com\Policies\PolicyDefinitions
Right-click inside the folder → Paste



Step 4 – Copy the ADM file for your language (en-US)

Each ADMX file has a language file (ADM) that goes inside a subfolder like en-US.

This folder must be copied entirely to the same PolicyDefinitions path.

Still in C:\Windows\PolicyDefinitions, right-click the en-US folder → Copy
Go to: \\vlabs07.com\SYSVOL\vlabs07.com\Policies\PolicyDefinitions
Paste the en-US folder there.

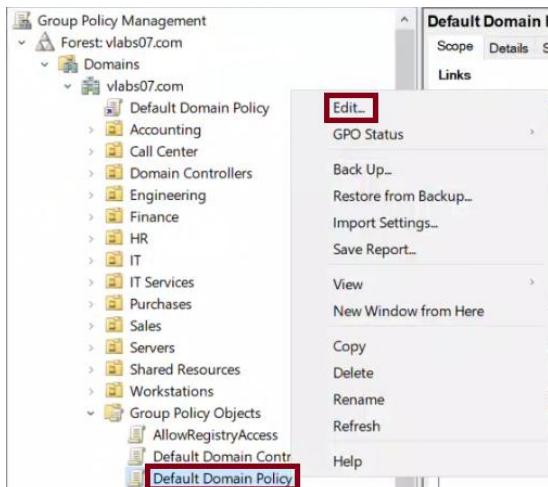
Network > vlabs07.com > SYSVOL > vlabs07.com > Policies > PolicyDefinitions

Name	Date modified	Type
en-US	5/23/2025 2:19 PM	File
ActiveXInstallService.admx	5/8/2021 4:15 AM	ADM
AddRemovePrograms.admx	5/8/2021 4:15 AM	ADM
AllowBuildPreview.admx	5/8/2021 4:15 AM	ADM
AppCompat.admx	5/8/2021 4:15 AM	ADM
AppPrivacy.admx	5/8/2021 4:14 AM	ADM
appv.admx	5/8/2021 5:41 AM	ADM
AppxPackageManager.admx	5/8/2021 4:15 AM	ADM

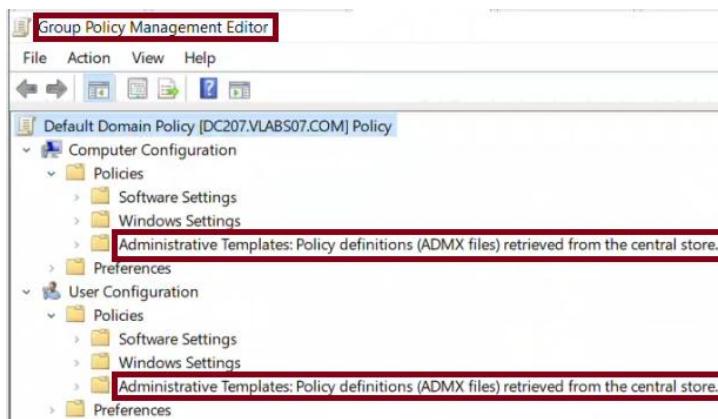
Step 5 – How to verify that the Central Store is being used

We're going to open the **Group Policy Management Console (GPMC)** and check **if** the administrative templates are now loading from the Central Store.

1. On DC107, open the **Start** menu and **type**:
gpmc.msc
Press Enter to launch the **Group Policy Management Console**.
2. **In** the left panel, expand your domain (**vlabs07.com**), then click on "Group Policy Objects".
3. Right-click on the "Default Domain Policy" and choose "Edit".



4. **In** the **Group Policy Management Editor**, expand both:
 - Computer **Configuration** → Policies
 - User **Configuration** → Policies



5. Under each one, click once on "Administrative Templates".

You **should** see the message:

"Administrative Templates: Policy definitions (ADMX files) retrieved from the central store."

This message confirms that the Central Store is working properly.

Task 2: Managing and Configuring Administrative Templates

System: DC107

Step 1 - What are Administrative Templates and why do we need Office ones?

Administrative Templates define settings that control how software and Windows features behave.

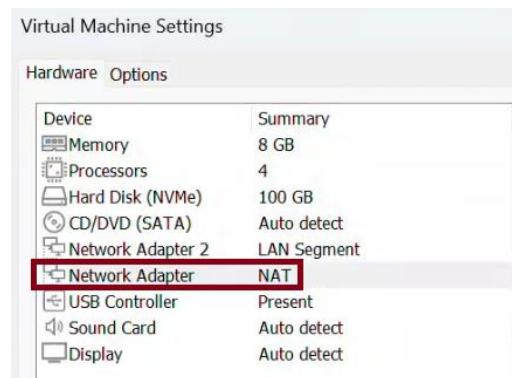
Windows comes with built-in templates (like password policies, control panel settings, etc.), but if we want to manage third-party software like Microsoft Office or Teams, we need to add additional templates.

In this task, we are downloading the Microsoft Office ADMX templates so we can configure a Teams setting using Group Policy.

Step 2 - Download Microsoft Office Administrative Templates

To download the Office templates:

1. Temporarily add a NAT network adapter to DC107 so it has internet access.
2. Open a web browser on DC107 and go to:



<https://www.microsoft.com/en-us/download/details.aspx?id=49030>

3. Click **Download**

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

4. Choose the version that matches your system:
 For Windows Server 2022 (64-bit), choose:
`admintemplates_x64_5497.1000_en-us.exe`

Choose the download you want

<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

Select a folder to store the extracted files

- ▼ This PC
 - > 3D Objects
 - > Desktop
 - > Documents
 - Downloads**
 - > Music
 - > Pictures
 - > Videos
 - > Local Disk (C:)

OK **Cancel**

5. Run the file. It will extract a folder (by default, inside your Downloads folder) that contains:
- A group of `*.admx` files
 - A folder named `en-US` with `*.adml` files

Step 3 – Copy the downloaded ADMX and ADML files to the Central Store

This PC > Downloads > admx >				
Name	Date modified	Type	Size	
de-de	5/23/2025 2:57 PM	File folder		
en-us	5/23/2025 2:57 PM	File folder		
es-es	5/23/2025 2:57 PM	File folder		
fr-fr	5/23/2025 2:57 PM	File folder		
it-it	5/23/2025 2:57 PM	File folder		
ja-jp	5/23/2025 2:57 PM	File folder		
ko-kr	5/23/2025 2:57 PM	File folder		
nl-nl	5/23/2025 2:57 PM	File folder		
pt-br	5/23/2025 2:57 PM	File folder		
ru-ru	5/23/2025 2:57 PM	File folder		
zh-cn	5/23/2025 2:57 PM	File folder		
zh-tw	5/23/2025 2:57 PM	File folder		
access16.admx	3/26/2025 4:50 PM	ADMX File	118 KB	
excel16.admx	3/26/2025 4:50 PM	ADMX File	286 KB	
lync16.admx	3/26/2025 4:50 PM	ADMX File	35 KB	
office16.admx	3/26/2025 4:50 PM	ADMX File	1,898 KB	
onenet16.admx	3/26/2025 4:50 PM	ADMX File	125 KB	
outlook16.admx	3/26/2025 4:50 PM	ADMX File	660 KB	
ppt16.admx	3/26/2025 4:50 PM	ADMX File	227 KB	
proj16.admx	3/26/2025 4:50 PM	ADMX File	279 KB	
word16.admx	3/26/2025 4:50 PM	ADMX File	69 KB	

1. Open the folder `where` you extracted the templates.
2. `Copy` all `*.admx` files and paste them into:
`\vlabs07.com\SYSVOL\vlabs07.com\Policies\PolicyDefinitions`
3. Inside the extracted `en-US` folder, `copy` the `*.adml` files and paste them into:
`\vlabs07.com\SYSVOL\vlabs07.com\Policies\PolicyDefinitions\en-US`

Network > vlabs07.com > SYSVOL > vlabs07.com > Policies > PolicyDefinitions >

Name	Date modified	Type	Size
en-US	5/23/2025 7:47 PM	File folder	
access16.admx	3/26/2025 4:50 PM	ADMX File	118 KB
ActiveXInstallService.admx	5/8/2021 4:15 AM	ADMX File	5 KB
AddRemovePrograms.admx	5/8/2021 4:15 AM	ADMX File	5 KB
AllowBuildPreview.admx	5/8/2021 4:15 AM	ADMX File	2 KB
AppCompat.admx	5/8/2021 4:15 AM	ADMX File	6 KB
AppPrivacy.admx	5/8/2021 4:14 AM	ADMX File	35 KB
appv.admx	5/8/2021 5:41 AM	ADMX File	35 KB
AppxPackageManager.admx	5/8/2021 4:15 AM	ADMX File	6 KB
AppXRuntime.admx	5/8/2021 4:15 AM	ADMX File	4 KB
AttachmentManager.admx	5/8/2021 4:15 AM	ADMX File	6 KB
AuditSettings.admx	5/8/2021 4:15 AM	ADMX File	2 KB
AutoPlay.admx	5/8/2021 4:15 AM	ADMX File	4 KB
AVSValidationGP.admx	5/8/2021 4:14 AM	ADMX File	3 KB
Biometrics.admx	5/8/2021 4:15 AM	ADMX File	4 KB
Bits.admx	5/8/2021 4:15 AM	ADMX File	56 KB
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

Important:

If the folder already exists (from Task 1), that's okay.

Copy the entire contents of the new `en-US` folder and paste it into the Central Store `en-US` folder.

If you are asked whether to **replace existing files**, choose:

Skip – this way, you only add new files without removing existing ones.

This updates your Central Store so that GPMC can now display Microsoft Office settings.

Note – Important Cleanup After Downloading Templates

After downloading the Microsoft Office Administrative Templates using the NAT adapter, make sure to **remove or disable the NAT network adapter** from the server (DC107).

Leaving the NAT adapter enabled can cause:

- Replication errors (e.g., "RPC server is unavailable")
- Incorrect DNS registrations
- Communication issues between domain controllers

Once removed, it's also a good idea to run:

```
ipconfig /flushdns  
ipconfig /registerdns
```

This ensures your server re-registers its correct internal IP address with DNS.

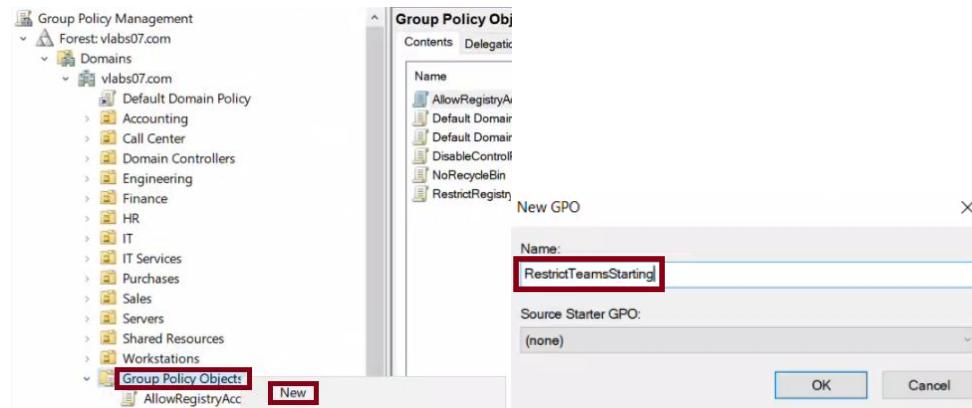
Step 4 – Create a new GPO to manage Teams startup behavior

We are now going to create a new **Group Policy Object** that prevents Microsoft Teams from starting automatically after installation.

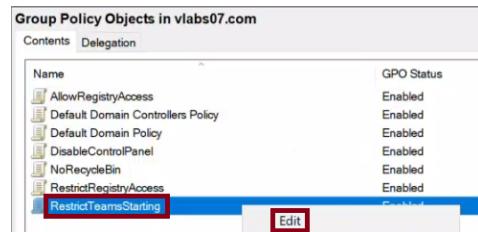
Open **Group Policy Management Console** (`gpmc.msc`) on DC107.
Right-click on **Group Policy Objects** → choose **New**

Name the GPO:

RestrictTeamsStarting



Right-click the new GPO → choose **Edit**



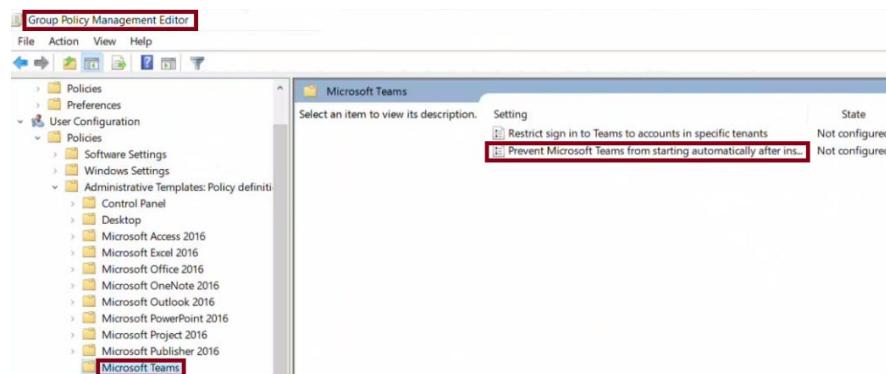
In the **Group Policy Management Editor**, go to:

User **Configuration** → Policies → Administrative Templates → Microsoft Teams
(if not visible, use **filter**)

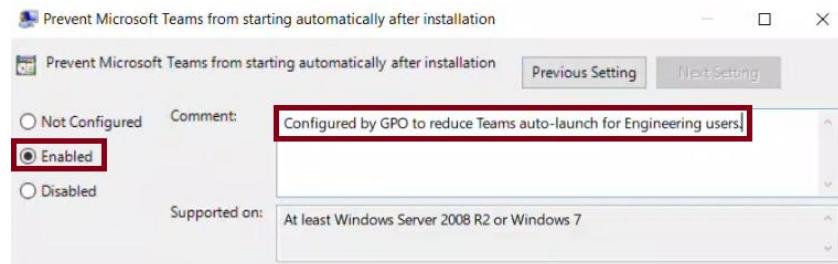
Tip: If you don't see "Microsoft Teams", use the built-in **Filter Options** in the top right to search for Teams-related settings.

Find the setting:

****Prevent Microsoft Teams from starting automatically after installation****



Double-click the setting → **Select **Enabled****
In the Comment box, type:
Configured by GPO to reduce Teams auto-launch **for** Engineering users.

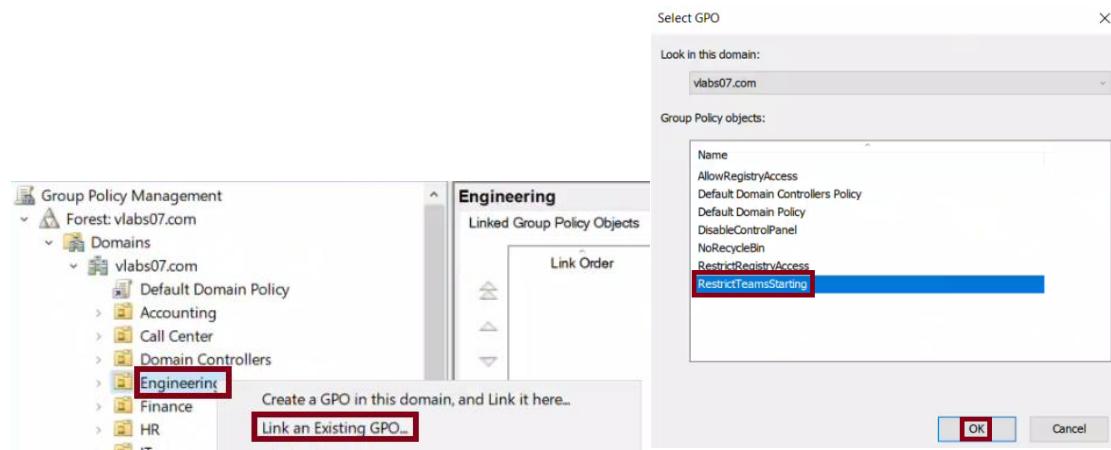


Click **OK** to save.

Step 5 – Link the GPO to the Engineering OU

Back **in** the **Group Policy Management Console**:

1. Expand your domain
2. Right-click the **Engineering OU**
3. Click **Link an Existing GPO**
4. **Select: RestrictTeamsStarting**



Step 6 – Apply the policy

Run this from PowerShell or Command **Prompt** on DC107 to make sure the policy is applied:
gpupdate /force

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

Task 3: Managing Account Policies

System: DC107 and Client07

Step 1 - What are Account Policies and why do they matter?

Account Policies define how secure user passwords must be and how login attempts are handled.

They include:

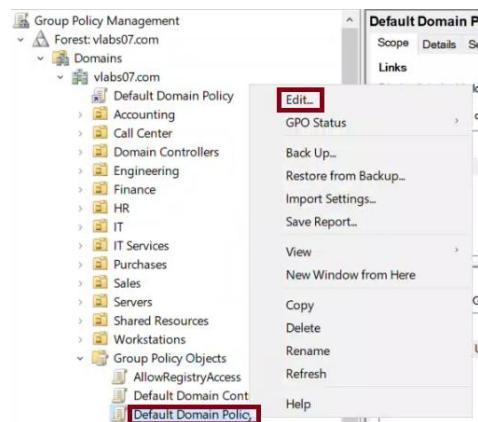
- Password rules (length, complexity, expiration)
- Account lockout rules (how many failed attempts are allowed)

These settings **must** be configured **in** the Default Domain Policy**, or they will not apply to domain users.

In this task, we'll update the password and account lockout policies and test them **using** a user account on Client07.

Step 2 - Edit the Default Domain Policy

1. On DC107, open **Group Policy Management Console (GPMC)**
Run: `gpmc.msc`
2. Expand your domain, then expand **Group Policy Objects**
3. Right-click on **Default Domain Policy** → choose **Edit**



4. In the Group Policy Management Editor, go to:
Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies

You will find two subcategories:

- **Password Policy**
- **Account Lockout Policy**

The screenshot shows the 'Group Policy Management Editor' window. The left pane displays a tree structure of policy settings: 'Computer Configuration' → 'Policies' → 'Windows Settings' → 'Security Settings' → 'Account Policies'. The 'Account Policies' node is highlighted with a red box. The right pane lists three policies with their names and descriptions:

Name	Description
Password Policy	Password Policy
Account Lockout Policy	Account Lockout Policy
Kerberos Policy	Kerberos Policy

Step 3 – Modify the Password Policy settings

Go into ****Password Policy**** and configure the following:

- ****Minimum password length**** → Set to `12 characters`

The screenshot shows the Group Policy Management console. On the left, under 'Default Domain Policy [DC207.VLABS07.COM] Policy' > 'Computer Configuration' > 'Policies' > 'Windows Settings' > 'Security Settings' > 'Account Policies' > 'Password Policy', the 'Minimum password length' policy is selected. On the right, the 'Minimum password length Properties' dialog is open, showing the setting 'Password must be at least: 12 characters'. A warning message at the bottom states: 'Modifying this setting may affect compatibility with clients, services, and applications. For more information, see Minimum password length. (Q823659)'.

- ****Password must meet complexity requirements**** → Set to `Enabled`
- ****Maximum password age**** → Set to `60 days`

The screenshot shows the Group Policy Management console. On the left, under 'Default Domain Policy [DC207.VLABS07.COM] Policy' > 'Computer Configuration' > 'Policies' > 'Windows Settings' > 'Security Settings' > 'Account Policies' > 'Password Policy', the 'Maximum password age' policy is selected. On the right, the 'Maximum password age Properties' dialog is open, showing the setting 'Password will expire in: 60 days'. A checkbox 'Define this policy setting' is checked.

Click Apply & OK after each change.

Step 4 – Modify the Account Lockout Policy settings

Go into ****Account Lockout Policy**** and configure the following:

- ****Account lockout threshold**** → Set to `2` invalid login attempts
(This will auto-fill the lockout duration settings)

The screenshot shows the Group Policy Management console. On the left, under 'Default Domain Policy [DC207.VLABS07.COM] Policy' > 'Computer Configuration' > 'Policies' > 'Windows Settings' > 'Security Settings' > 'Account Policies' > 'Account Lockout Policy', the 'Account lockout threshold' policy is selected. On the right, the 'Account lockout threshold Properties' dialog is open, showing the setting 'Account will lock out after: 2 invalid logon attempts'. A checkbox 'Define this policy setting' is checked. Below the main window, a 'Suggested Value Changes' dialog is open, stating: 'Because the value of Account lockout threshold is now 2 invalid logon attempts, the settings for the following items will be changed to the suggested values.' It lists three items with their current and suggested settings:

Policy	Policy Setting	Suggested Setting
Account lockout duration	Not Defined	10 minutes
Allow Administrator account lockout	Not Defined	Enabled
Reset account lockout counter after	Not Defined	10 minutes

- ****Account lockout duration**** → Set to `2 minutes`

The screenshot shows the 'Account lockout duration Properties' dialog box. On the left, there's a list of policy settings: 'Account lockout duration' (selected), 'Account lockout threshold', 'Allow Administrator account lockout', and 'Reset account lockout counter after'. On the right, the 'Policy Setting' for 'Account lockout duration' is shown as '10 minutes'. Below it, the 'Reset account lockout counter after' setting is shown as '2 invalid logon attempts'. A red box highlights the 'Reset account lockout counter after' row. To the right of the main pane, there's a sidebar with a server icon and the text 'Account lockout duration'. At the bottom, there's a section titled 'Account is locked out for:' with a dropdown menu set to '2 minutes', also highlighted with a red box.

- ****Reset account lockout counter after**** → Set to `2 minutes`

This screenshot shows the same 'Account lockout duration Properties' dialog box as the previous one, but with a different focus. The 'Reset account lockout counter after' policy setting is now highlighted with a red box and its value is set to '2 minutes'. The other settings ('Account lockout duration' and 'Account lockout threshold') are also listed below it.

Click Apply & OK after each setting.

Step 5 – Apply the policy changes

Back **in** PowerShell or Command Prompt on DC107, run:

```
gpupdate /force
```

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

This ensures that the new settings are applied to domain members.

Step 6 – Test the settings **using** a domain user (**Emma Petit**)

We will now test the password and account lockout settings **using** a domain user called ****Emma Petit**** on Client07.

This will confirm that the policy settings from the Default Domain Policy are correctly applied.

Step 6.1 – Apply the GPO on Client07

Before starting, log **in** to Client07 with a domain administrator account and open PowerShell or Command **Prompt**.

Run the following command to force immediate GPO refresh on the client:

```
gpupdate /force
```

```
C:\Users\Emma.Petit>gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

This ensures that the latest password and lockout policy changes are downloaded and applied from the domain controller.

Step 6.2 – Log **in as Emma Petit**

1. Log off from the admin session and log **in** as the user Emma Petit.
 - Username format: `Emma.Petit@vlabs07.com`
 - Use the correct password to ensure the account is active.

Step 6.3 – Attempt to change the password **using the GUI (optional)**

Note:

In a virtual lab **using** VMware Workstation, the GUI option **Ctrl + Alt + Del** → **Change a password**** may not **function** properly due to secure input limitations **in** virtual machines.

You may see a generic message like:

```
> "The password on this account cannot be changed at this time."
```

This is not caused by the password policy but by the lab environment itself.

If the GUI fails, proceed to the next step to use a reliable command-line method.

Step 6.4 – Attempt to change the password **using Command **Prompt****

1. Open **Command Prompt** as Administrator****** on Client07 (still logged **in** as Emma Petit).
2. Run the following command:
`net user Emma.Petit * /domain`
3. When prompted, enter a weak password like: `abc123`

If the password policy is applied, you will see this message:
> "The password does not meet the password policy requirements."

```
C:\Windows\System32>net user Emma.Petit * /domain
The request will be processed at a domain controller for domain vlabs07.com.

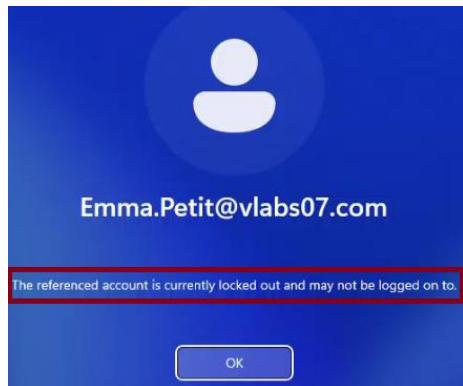
Type a password for the user:
Retype the password to confirm:
The password does not meet the password policy requirements. Check the minimum password length, p
assword complexity and password history requirements.
```

This confirms the **minimum length****, **complexity****, and **history**** settings are working.

Step 6.5 – Trigger account lockout by entering wrong passwords

1. Log off from Emma's session.
2. Attempt to log **in** again with the ***wrong password****.
3. Repeat this ***twice*** (to match the lockout threshold **set earlier**).

After the second failed attempt, you **should** see a message like:
> "Your account has been locked. Please contact your administrator."



This confirms that the ****account lockout threshold**** is working.

Step 6.6 – Wait for the lockout duration to expire

1. Wait ***2 minutes*** (based on your lockout duration setting).
2. Try logging **in** again with the ***correct password****.

If successful, this confirms the ****lockout duration**** and ****reset timer**** are functioning as expected.

Step 6.7 – Optional: Confirm results on the domain controller

1. Log **in** to ****DC107****
2. Open ****Event Viewer**** → Windows Logs → Security

Look **for**:

- Event ID ****4740**** – User account locked out

Two side-by-side screenshots of the Windows Event Viewer. Both windows have a title bar "Event Properties - Event 4740, Microsoft Windows security auditing." and tabs for "General" and "Details".

Left Window (General Tab):
- Subject: A user account was locked out.
- Log Name: Security
- Source: Microsoft Windows security
- Event ID: 4740
- Level: Information
- User: N/A
- OpCode: Info
- More Information: [Event Log Online Help](#)

Right Window (General Tab):
- Account That Was Locked Out: Security ID: VLABS07\Emma.Petit; Account Name: Emma.Petit
- Additional Information: Caller Computer Name: CLIENT07

Both windows have a red box highlighting the "Account That Was Locked Out" section in the right window.

These logs validate that the policy enforcement is captured at the domain level.

Task 4: Implementing Fine-Grained Password Policies

System: DC107 and Client07

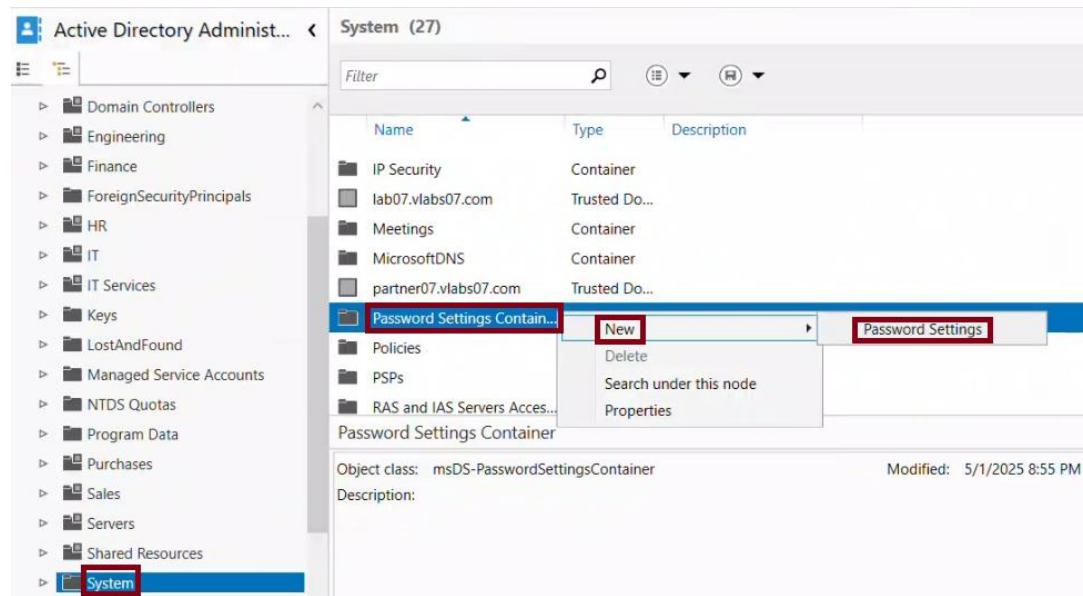
Step 1 – What is a Fine-Grained Password Policy (FGPP)?

In Active Directory, password and lockout settings are normally applied **using** the Default Domain Policy. However, **if** we want **different password rules for specific users or groups**** (like IT or Admins), we need to use **Fine-Grained Password Policies (FGPP)**.

These are **not configured using Group Policy**, but instead **using Active Directory Administrative Center (ADAC)** or PowerShell, and are stored as objects **in** Active Directory.

Step 2 – Open Active Directory Administrative Center (ADAC)

1. On DC107, open **Server Manager**
2. Click **Tools → Active Directory Administrative Center**
3. In the left pane, **select** your domain & Locate **System**
4. In the **middle pane**, scroll down to **Password Settings Container**
5. Right-click on **it** → **New → Password Settings**



Step 3 – Create a new Fine-Grained Password Policy

1. Name: `IT_FGPPolicy`
2. Precedence: `1` (lower number = higher priority)
3. Set the following values:
 - **Minimum password length**: `10`
 - **Password complexity**: `Disabled`
 - **Password expiration**: `0` (set to **Never**)
 - Other values can stay at defaults.

4. Under **Directly Applies To**, click **Add...**, and select the **IT Group**** (must already exist).
5. Click **OK** to save.

The screenshot shows the 'Password Settings' configuration screen. The policy name is 'IT_FGPPolicy'. Under 'Directly Applies To', the 'Add...' button is highlighted with a red box. Below it, a 'Select Users or Groups' dialog is open, showing the 'IT' group selected. To the right, a preview window shows the 'IT' group added to the 'Directly Applies To' list.

Step 4 - Confirm that the policy is applied

1. After creation, you will see `IT_FGPPolicy` listed in the Password Settings Container.
2. You can double-click to reopen it and verify the settings and applied group.

The screenshot shows the 'Password Settings Container' list. The 'IT_FGPPolicy' entry is selected and highlighted with a blue bar. The left pane shows various Active Directory objects like Default Domain Policy, Dfs-Configuration, etc.

Step 5 – Apply the policy on the client

On **Client07**, open PowerShell and run:

```
gpupdate /force
```

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

This ensures the client system picks up the updated password rules **for** the user **in** the **IT group**.

Step 6 – Test the FGPP with a user from the IT group

1. Log **in** to ClientXX as a user who belongs to the ****IT Group****
2. Open **Command Prompt** as Administrator
3. Run:

```
net user [username] * /domain
```
4. Enter a password that:
 - Has ****no complexity**** (e.g., `simplepass`)
 - Is at least ****10 characters****

```
C:\Windows\System32>net user Yales.Sanchez * /domain
The request will be processed at a domain controller for domain vlabs07.com.

Type a password for the user:
Retype the password to confirm:
The command completed successfully.
```

If the password is accepted, the FGPP is working correctly.

If the password is rejected due to complexity, the default domain policy is still **in effect** or the FGPP was not applied.

Step 7 – Optional: Confirm FGPP via PowerShell

To see which FGPP is applied to a user, run this on DC107:

```
**powershell**
Get-ADUserResultantPasswordPolicy -Identity [username]
```

```
PS C:\Users\Administrator> Get-ADUserResultantPasswordPolicy -Identity Yales.Sanchez

AppliesTo          : {CN=IT,OU=IT,DC=vlabs07,DC=com}
ComplexityEnabled : False
DistinguishedName : CN=IT_FGPPolicy,CN=Password Settings
                    Container,CN=System,DC=vlabs07,DC=com
LockoutDuration   : 00:30:00
LockoutObservationWindow : 00:30:00
LockoutThreshold  : 0
MaxPasswordAge    : 00:00:00
MinPasswordAge    : 1.00:00:00
MinPasswordLength : 10
Name               : IT_FGPPolicy
ObjectClass        : msDS-PasswordSettings
ObjectGUID         : 19f88092-53e7-4768-a5f5-b12f503b6ea1
PasswordHistoryCount : 24
Precedence         : 1
ReversibleEncryptionEnabled : False
```

Task 5: Managing Audit Authentication

System: DC107 (GPO configuration and log review), ClientXX (logon tests)

Step 1 - What is Audit Logon?

Audit Logon is used to track and record both successful and failed login attempts. This helps IT staff detect unauthorized access or troubleshoot user issues. In this task, we will enable Audit Logon Events using the Default Domain Policy and then test and validate the results using Event Viewer.

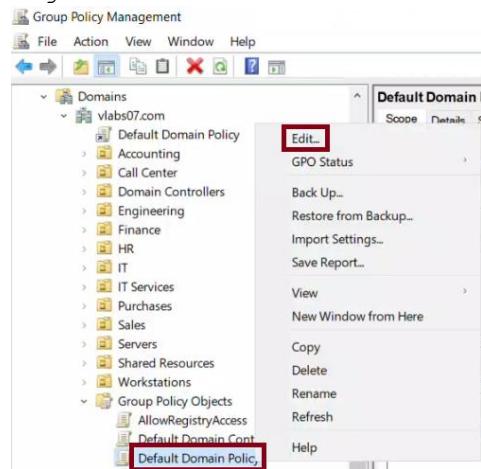
Step 2 - Enable Audit Logon Events in Default Domain Policy

Open Group Policy Management Console on DC107

Run: gpmc.msc

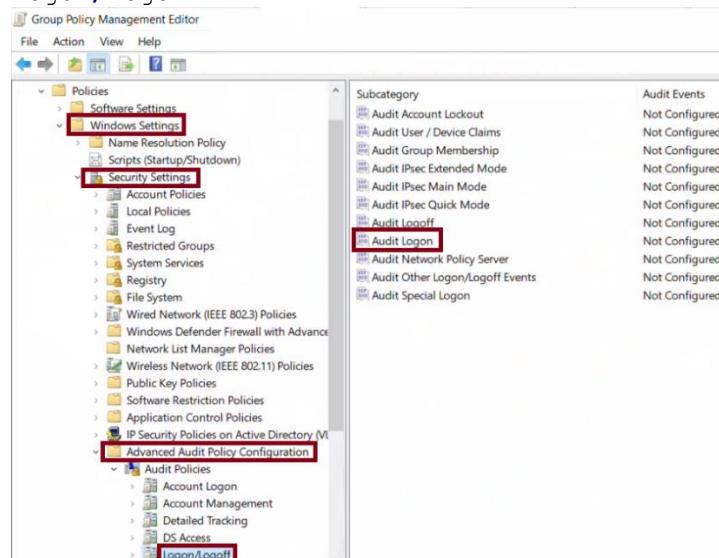
In GPMC:

Expand your domain → Group Policy Objects
Right-click on Default Domain Policy → Edit

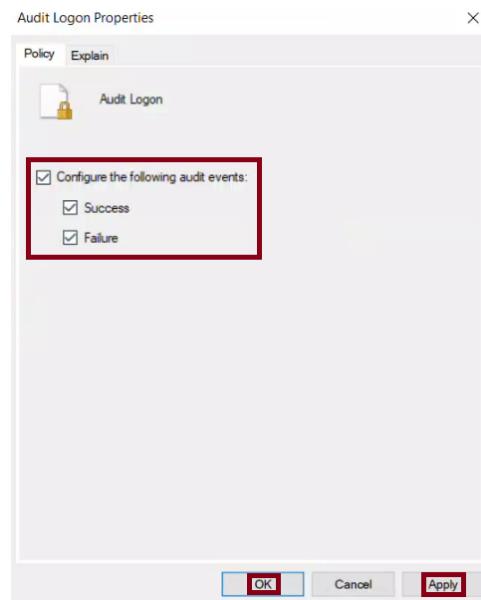


In the Group Policy Management Editor:

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



Double-click on Audit Logon
Check the box **for:** Configure the following audit events
Check both: Success and Failure
Click OK and close the window



Step 3 – Apply the policy update on DC107

Open PowerShell or CMD on DC107 and run:
`gpupdate /force`

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

This forces the domain controller to apply the updated GPO immediately.

Step 4 – Restart Client07

Log **in** to Client07 and restart the system to ensure **it** receives the latest policy updates.

Step 5 – Test both successful and failed logon attempts on Client07

Log **in** with a domain user (**e.g.,** Emma.Petit or Yales.Sanchez)

First, test a successful login by entering the correct password
Then, log out and **try** at least one failed login **using** an incorrect password

Each attempt will be recorded by the domain controller (**DC107**)

Step 6 – Verify Audit Logs on DC107

On DC107, open Event Viewer:
Run: eventvwr.msc

Navigate to:
Event Viewer → Windows Logs → Security

Look **for**:
Event ID 4624 → Successful logon
Event ID 4625 → Failed logon

Optional: In the right-hand pane, click **Filter Current Log**
Enter: 4624, 4625 as the Event IDs to **filter** login activity quickly

The screenshot shows the Windows Event Viewer interface for the Security log. The title bar says "Security Number of events: 191,519". A filter bar at the top indicates "Filtered: Log: Security; Source: ; Event ID: 4625. Number of events: 16". The main pane displays a table of audit failure events. The first event is selected, showing its details in the bottom pane. The details pane for event 4625 states: "An account failed to log on." under the "Subject:" section. The subject information includes: Security ID: NULL SID, Account Name: -, and Account Domain: -.

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	5/16/2025 9:27:47 PM	Microsoft Windows secur...	4625	Logon
Audit Failure	5/15/2025 12:27:19 PM	Microsoft Windows secur...	4625	Logon
Audit Failure	5/15/2025 12:26:19 PM	Microsoft Windows secur...	4625	Logon
Audit Failure	5/15/2025 12:26:10 PM	Microsoft Windows secur...	4625	Logon

The screenshot shows the Windows Event Viewer interface for the Security log. The title bar says "Security Number of events: 191,511 (1) New events available". A filter bar at the top indicates "Filtered: Log: Security; Source: ; Event ID: 4624. Number of events: 16". The main pane displays a table of audit success events. The first event is selected, showing its details in the bottom pane. The details pane for event 4624 states: "An account successfully logged on." under the "Subject:" section. The subject information includes: Security ID: SYSTEM, Account Name: DC107\$, Account Domain: VLABS07.COM, Logon ID: 0x765E6C9, Linked Logon ID: 0x0, Network Account Name: -, and Network Account Domain: -.

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	5/24/2025 10:16:28 PM	Microsoft Windows secur...	4624	Logon
Audit Success	5/24/2025 10:16:27 PM	Microsoft Windows secur...	4624	Logon
Audit Success	5/24/2025 10:16:27 PM	Microsoft Windows secur...	4624	Logon
Audit Success	5/24/2025 10:16:27 PM	Microsoft Windows secur...	4624	Logon
Audit Success	5/24/2025 10:16:24 PM	Microsoft Windows secur...	4624	Logon

Step 7 – Verify Audit Logon Policy Using auditpol

To confirm that the Audit Logon settings were successfully applied to DC107, we use the auditpol command-line utility.

This tool allows us to view the effective audit policy currently **in** place on the system.

Run the following command on DC107:

```
auditpol /get /category:"Logon/Logoff"
```

PS C:\Users\Administrator> auditpol /get /category:"Logon/Logoff"	
System audit policy	
Category/Subcategory	Setting
Logon/Logoff	
Logon	Success and Failure
Logoff	No Auditing
Account Lockout	No Auditing
IPsec Main Mode	No Auditing
IPsec Quick Mode	No Auditing
IPsec Extended Mode	No Auditing
Special Logon	No Auditing
Other Logon/Logoff Events	No Auditing
Network Policy Server	No Auditing
User / Device Claims	No Auditing
Group Membership	No Auditing

This confirms that both Success and Failure auditing is enabled **for** logon activity, as required by the lab instructions.

Screenshot – Show the auditpol output on DC107, verifying “Success and Failure” is active under the Logon category.

Task 6: Managing Security Templates

System: DC107

Step 1 - What is a Security Template?

Security Templates are saved **configuration** files (**.inf**) that contain predefined security settings such as system services, file permissions, and user rights. They allow administrators to apply consistent settings **using** tools like the Security Configuration and Analysis snap-in or Group Policy.

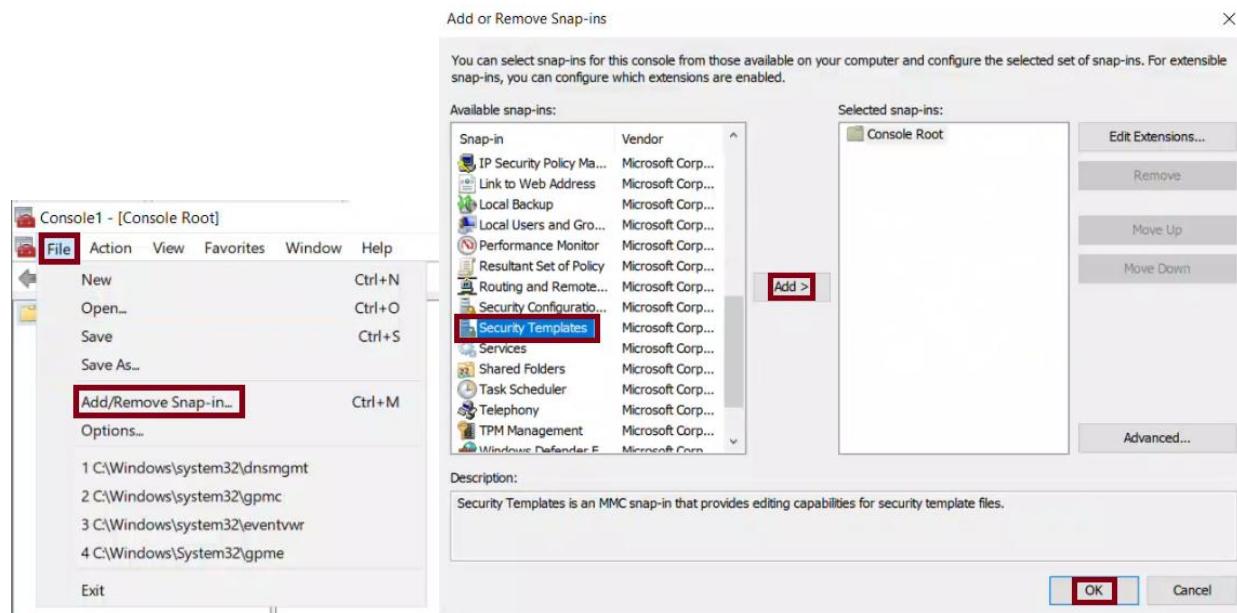
In this task, we will:

- Create a new Security Template called OpenSSH_Auth
- Configure the OpenSSH Authentication Agent service to **start** automatically
- Import this template into a new GPO named OpenSSHAAuth
- Link the GPO to the DomainControllers OU
- Verify the service is running after a reboot

Step 2 - Create the Security Template

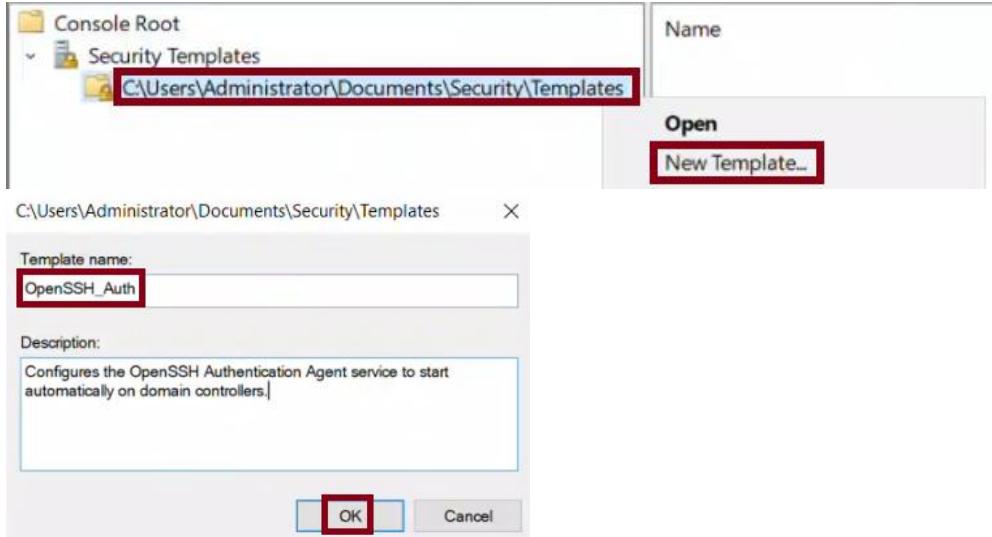
Open the MMC console on DC107:

1. Run: mmc (Windows + R)
2. Go to File → Add/Remove Snap-in
3. Add: Security Templates
4. Click OK



In the left pane:

- Expand: Security Templates
- Right-click the folder: C:\Windows\Security\Templates → New Template
- Name the template: OpenSSH_Auth
- Click OK



Step 3 - Configure OpenSSH Authentication Agent

1. Expand the new template (OpenSSH_Auth)
2. Go to: System Services
3. Double-click: OpenSSH Authentication Agent
4. Set startup mode to: Automatic
5. Click OK

The screenshot displays two windows. On the left, the 'OpenSSH Authentication Agent Properties' window shows the 'System Services' tab. It lists various services, with 'OpenSSH Authentication ...' selected. On the right, a separate window shows the 'Service Name' column with 'OpenSSH Authentication ...' highlighted. Both windows have 'OK' and 'Cancel' buttons at the bottom.

OpenSSH Authentication Agent Properties

Template Security Policy Setting

OpenSSH Authentication Agent

Define this policy setting in the template

Select service startup mode:

Automatic

Manual

Disabled

Edit Security...

OK Cancel Apply

Service Name	Startup	Permission
Network List Service	Not Defined	Not Defined
Network Location Aware...	Not Defined	Not Defined
Network Setup Service	Not Defined	Not Defined
Network Store Interface Se...	Not Defined	Not Defined
Offline Files	Not Defined	Not Defined
OpenSSH Authentication ...	Not Defined	Not Defined
Optimize drives	Not Defined	Not Defined
Power Management Service	Not Defined	Not Defined

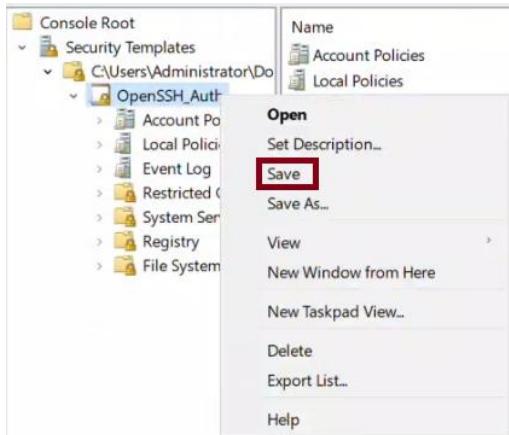
Step 4 – Save the Template

Explanation:

After configuring the OpenSSH Authentication Agent service to [start](#) automatically, we must manually save the security template to ensure the settings are written to an .inf file. This step is often missed because clicking "OK" or "Apply" does not automatically save the file.

How to Save the Template:

1. In the MMC console, locate the template named 'OpenSSH_Auth' under the Security Templates node.
2. Right-click on 'OpenSSH_Auth'.
3. Click 'Save'.



Important:

This action creates the actual .inf file used later [for](#) GPO import. Skipping this step means the settings will not be saved, even [if](#) you clicked "OK" earlier.

Template Save Location:

C:\Users\<YourUsername>\Documents\Security\Templates\OpenSSH_Auth.inf

> This PC > Local Disk (C:) > Users > Administrator > Documents > Security > Templates

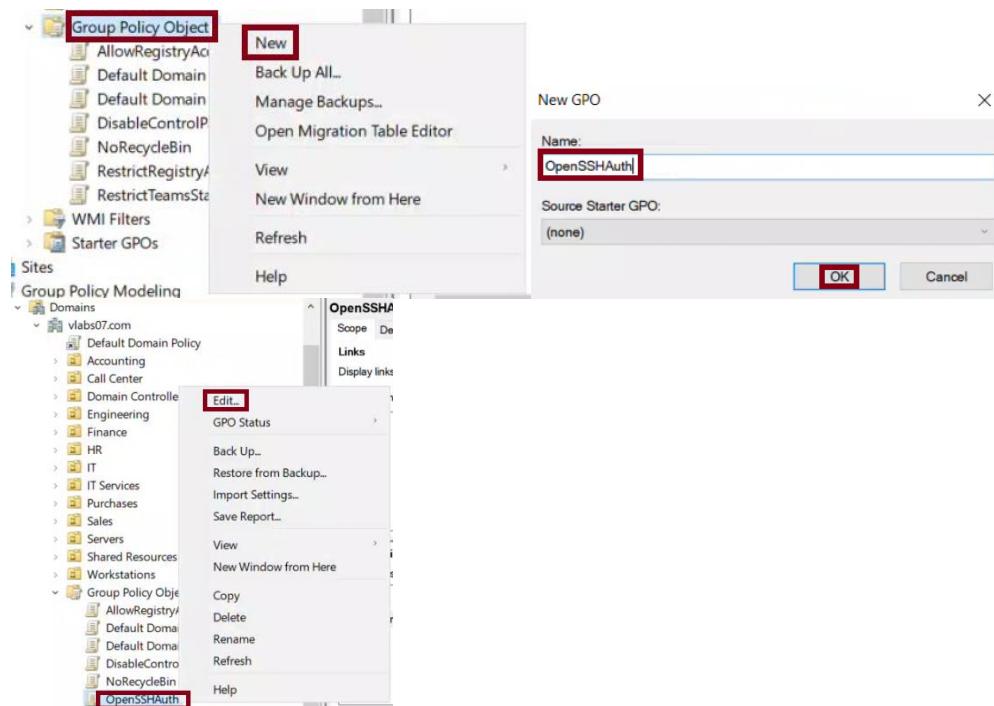
Name	Date modified	Type
OpenSSH_Auth	5/24/2025 10:43 PM	Setup Information

Expected .inf File Content:

```
-----  
[OpenSSH_Auth.inf - Notepad]  
File Edit Format View Help  
[Unicode]  
Unicode=yes  
[Version]  
signature="$CHICAGO$"  
Revision=1  
[Service General Setting]  
"ssh-agent",2,""  
[Registry Values]  
[Profile Description]  
Description=Configures the OpenSSH Authentication Agent service to start automatically on domain controllers.  
  
Ln 1, Col 1 100% Windows (CRLF) UTF-16 LE  
  
[Service General Setting]  
"ssh-agent",2,""
```

Step 5 – Import the Template into a New GPO

1. Open **Group Policy Management Console (GPMC)**: gpmc.msc
2. Right-click **Group Policy Objects** → New
3. Name the GPO: OpenSSHAUTH → Click OK
4. Right-click OpenSSHAUTH → Edit



In the Group Policy Management Editor:

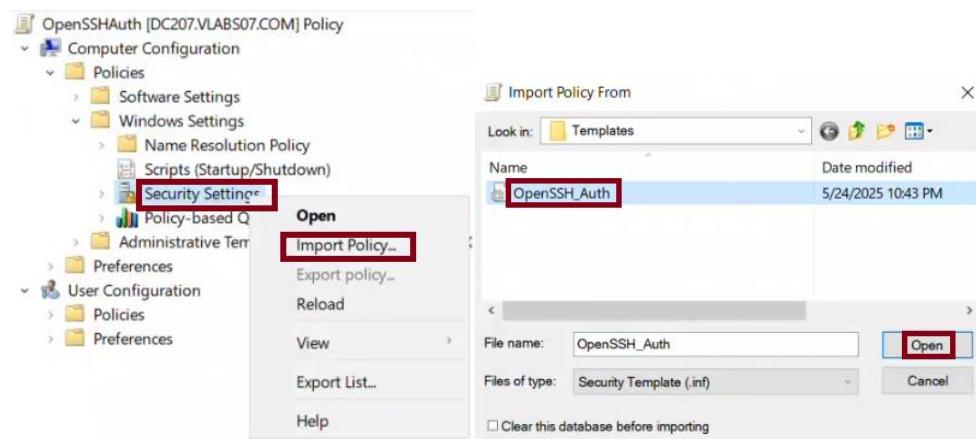
Go to:

Computer Configuration → Policies → Windows Settings → Security Settings
Right-click: Security Settings → Import Policy...

Navigate to:

C:\Windows\Security\Templates\OpenSSH_Auth.inf

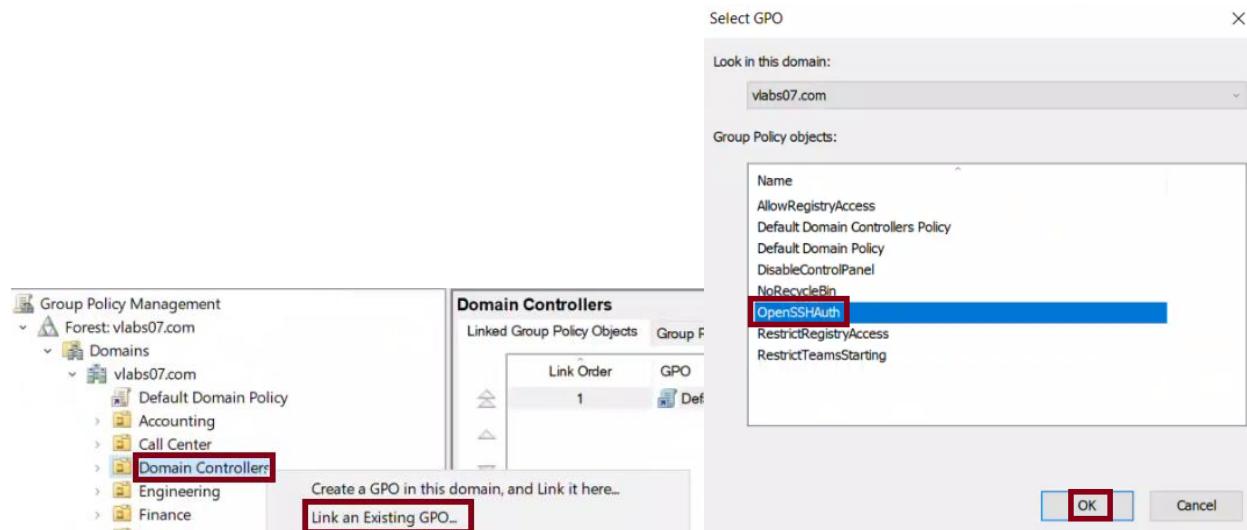
Click Open



Step 6 – Link the GPO to DomainControllers OU

In GPMC:

1. Expand: vlabs07.com → Domain Controllers
2. Right-click Domain Controllers → Link an Existing GPO
3. Select: OpenSSHAUTH → Click OK



Step 7 – Apply and Verify

- Run on DC107:
gpupdate /force

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

- Restart DC107

- After reboot, verify the OpenSSH Authentication Agent service is running:

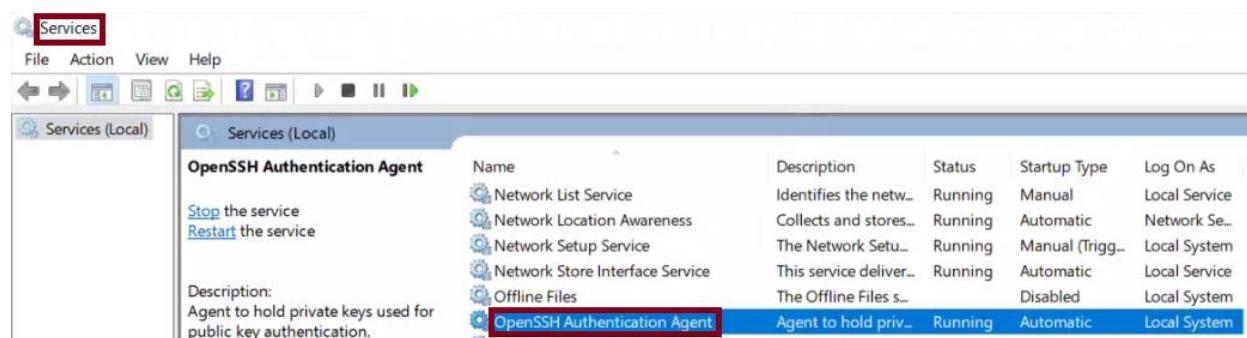
Open Services:

Run: services.msc

Check: OpenSSH Authentication Agent

Startup Type: Automatic

Status: Running



Task 7: Configuring Folder Redirection

Systems Involved:

- DC307 (file server)
- DC107 (GPO configuration)
- Client07 (testing)

Step 1 - What is Folder Redirection?

Folder Redirection allows administrators to redirect the path of known folders (like Documents and Desktop) to a network location. This makes user **data** available from any domain-joined device and centralizes storage.

We will use **Basic Redirection**, which creates one private folder per user inside a shared path.

Step 2 - Create and Share the Redirection Folder on DC307

On DC307:

1. Create the folder:

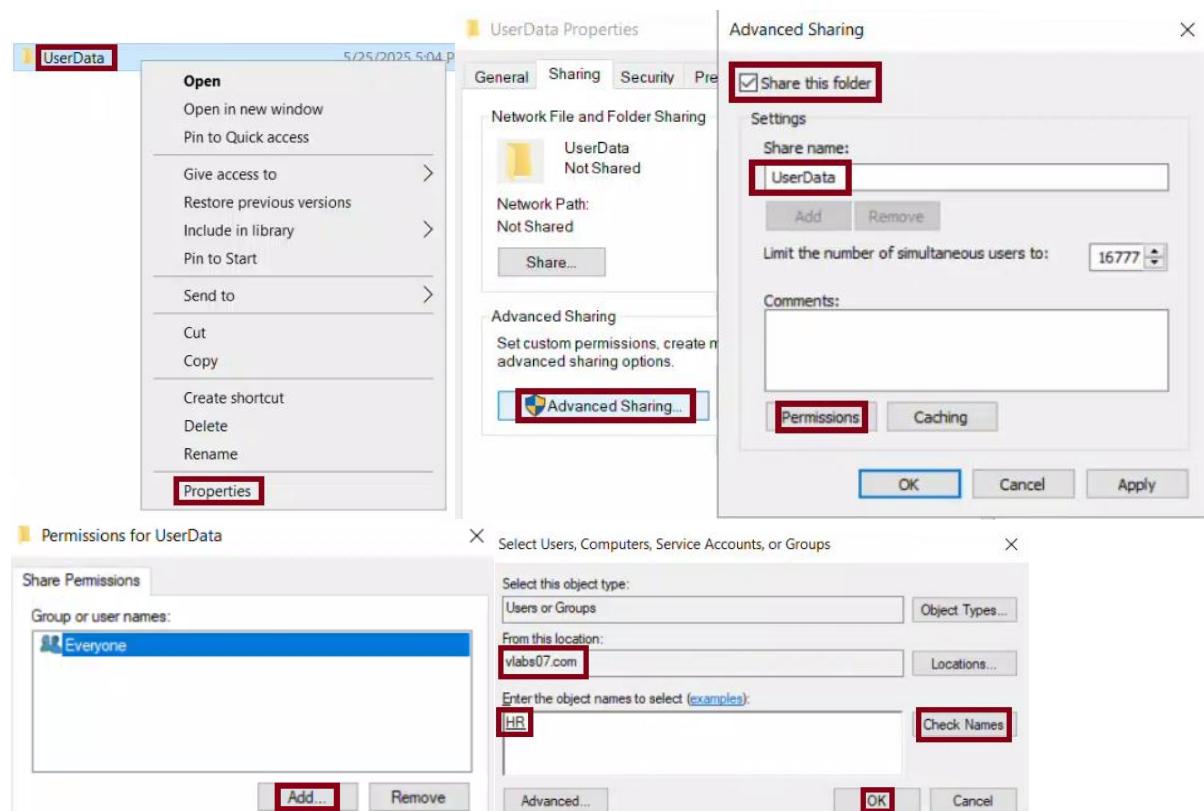
C:\UserData

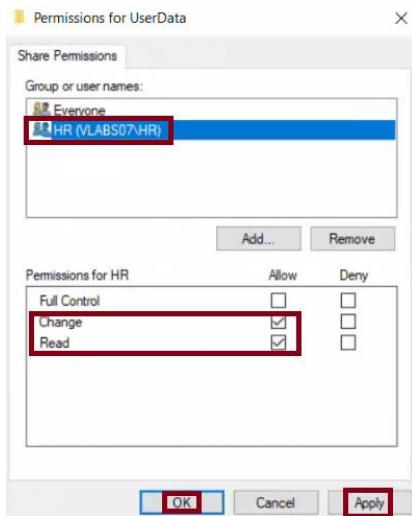
2. Right-click the folder → Properties → Sharing tab

Click "Advanced Sharing"

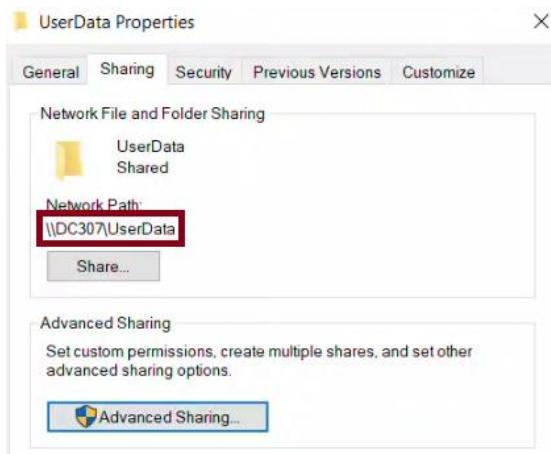
- Check "Share this folder"
- Share name: UserData

- Permissions: Add the **HR Group**, allow **Read and Change**



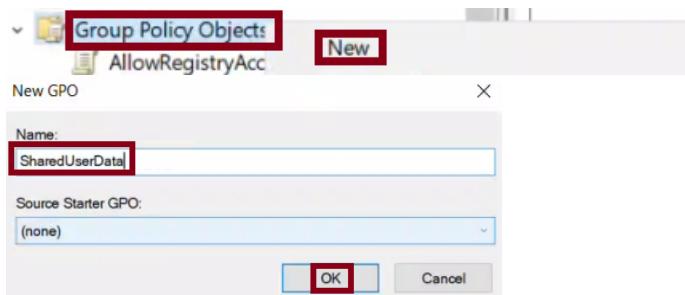


3. Confirm the shared path is:
 \\DC307\UserData



Step 3 - Create a New GPO

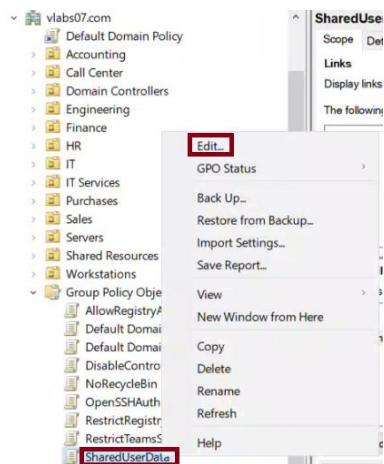
On DC107 open GPMC (gpmc.msc)
 Right-click **Group Policy Objects** → New
 Name the new GPO: SharedUserData



Step 4 – Configure Folder Redirection Settings

Right-click SharedUserData GPO → Edit

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

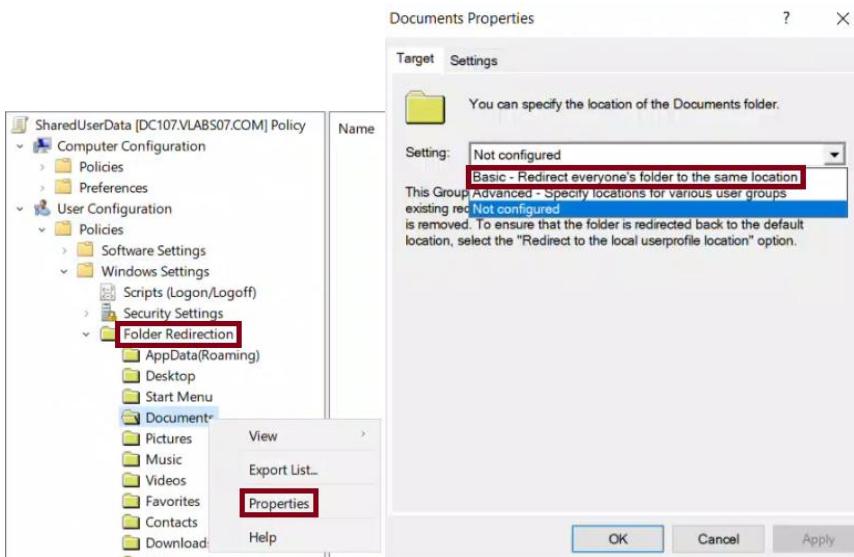


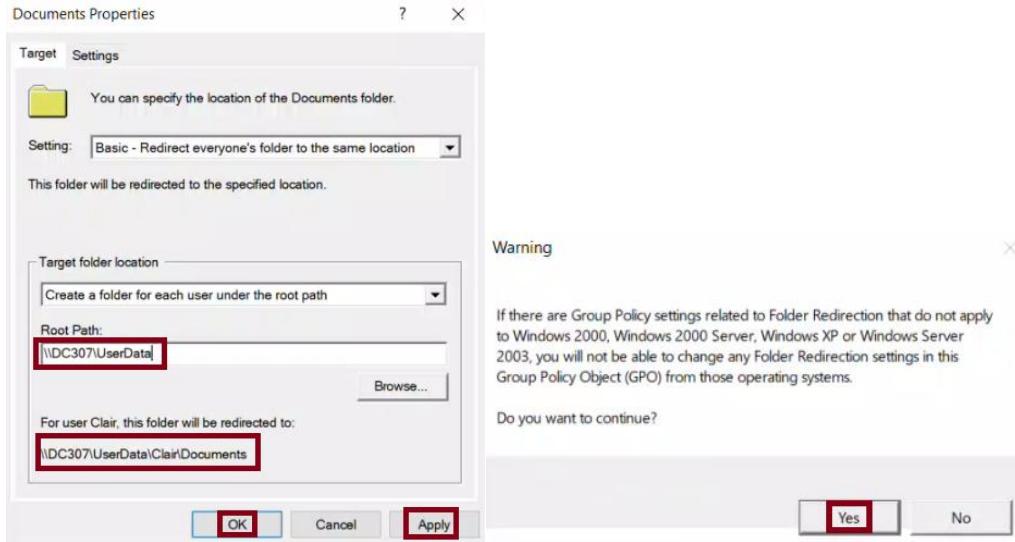
Right-click Documents → Properties

Set: Basic – Redirect everyone's folder to the same location

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

Root path: \DC307\ UserData





Step 4.5 – Configure Desktop Folder Redirection

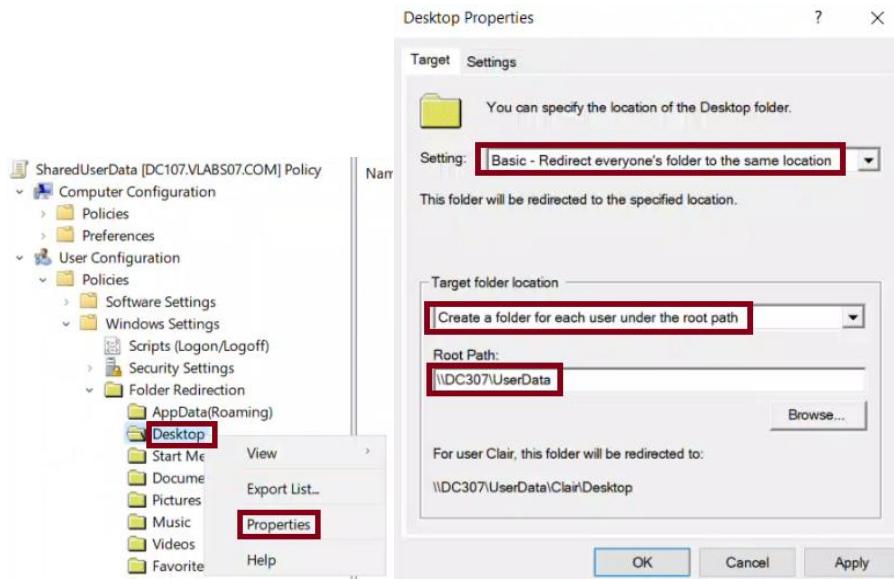
In the same GPO editor window **for** SharedUserData

Right-click Desktop → Properties

Set: Basic - Redirect everyone's folder to the same location

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

Root path: \\DC307\ UserData

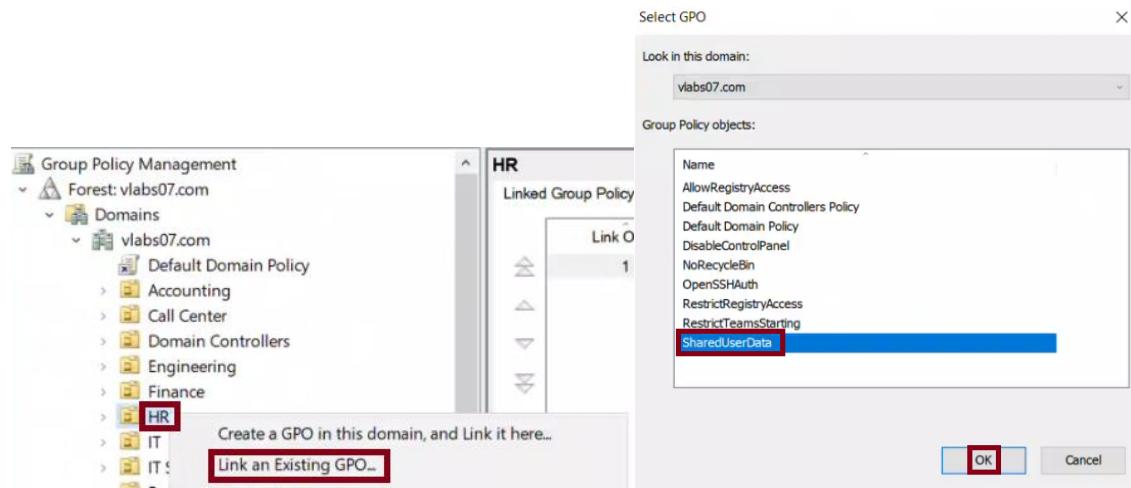


Click Apply and OK

Step 5 – Link GPO to HR OU

In GPMC, locate the HR OU

Right-click HR → Link an existing GPO → Select SharedUserData



Step 6 – Apply the GPO on Client07

Login to Client07 as a user from the HR group

Run in PowerShell:

```
gpupdate /force
```

```
PS C:\Users\Tess.Dupuy> 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 t
he 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 informati
on about Group Policy results.

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

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

Activate Windows
Go to Settings to activate Windows.

Logoff when prompted

Step 7 – Enable Network Wait Policy to Force Redirection on First Logon

This step ensures folder redirection applies immediately at login.

Edit the SharedUserData GPO:

Navigate to: Computer Configuration → Policies → Administrative Templates → System → Logon

Enable the policy:

Always wait **for** the network at computer startup and logon → Enabled

The screenshot shows the Group Policy Management Editor. On the left, under 'System', the 'Logon' policy is selected. In the main pane, the 'Always wait for the network at computer startup and logon' setting is highlighted. The 'Edit policy setting' button is visible. Below it, the 'Requirements' section specifies 'At least Windows Server 2003 operating systems or Windows XP Professional'. A detailed description follows, explaining the policy's purpose. A note at the bottom states that because this is a background refresh, extensions may not be applied. At the bottom of the window, there are 'Previous Setting' and 'Next Setting' buttons, and a status bar with 'Activate Win'.

Always wait for the network at computer startup and logon

Setting

State

Comment

Always wait for the network at computer startup and logon

Requirements:

At least Windows Server 2003 operating systems or Windows XP Professional

Description:

This policy setting determines whether Group Policy processing is synchronous (that is, whether computers wait for the network to be fully initialized during computer startup and user logon). By default, on client computers, Group Policy processing is not synchronous; client computers typically do not wait for the network to be fully initialized at startup and logon. Existing users are logged on using cached credentials, which results in shorter logon times. Group Policy is applied in the background after the network becomes available.

Note that because this is a background refresh, extensions

Always wait for the network at computer startup and logon

Always wait for the network at computer startup and logon

Previous Setting Next Setting

Not Configured Enabled

Comment:

Enabled

Disabled

Supported on:

At least Windows Server 2003 operating systems or Windows XP Professional

Activate Win

Step 8 – Validate Folder Redirection

Log **in** again as the user on Client07

The screenshot shows a File Explorer window. The path is C:\Network\DC307\UserData. Inside the 'UserData' folder, there is a single item named 'Tess.Dupuy'. The file details show it was modified on 5/25/2025 6:48 PM and is a File folder.

Name Date modified Type

Tess.Dupuy 5/25/2025 6:48 PM File folder

Task 8: Managing Software Installation

Systems: DC307 (File Server), DC107 (GPO Configuration), Client07 (Testing)

Step 1 - What is Software Installation via GPO?

Group Policy can be used to deploy software packages such as Microsoft Teams across multiple machines in a domain environment. This method is ideal for large-scale deployment where users receive the application automatically at startup or logon.

In this task, we will deploy Microsoft Teams silently to all computers in the Engineering OU. The software will be delivered from a shared folder on DC3XX using a GPO created and linked via DC1XX.

Step 2 - Create a Network Share on DC307

Open File Explorer on DC307

Create the folder C:\Software

Right-click the folder → Properties → Sharing tab

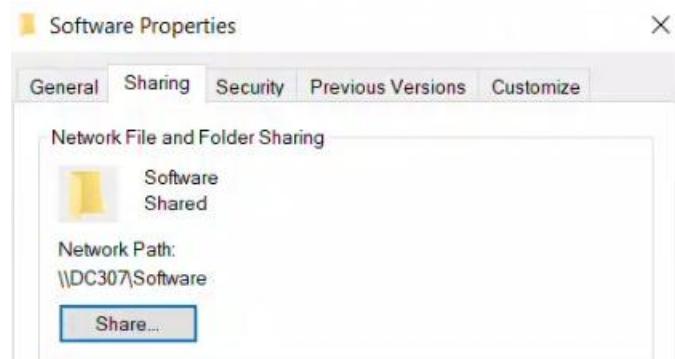
Click Advanced Sharing

Check Share this folder

Set share name to: Software

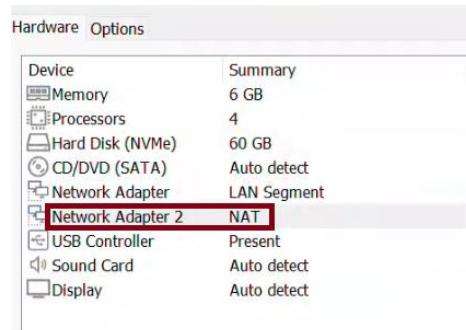
Click Permissions → Add Everyone with Read access

Click OK on all windows



Step 3 - Download Microsoft Teams MSI on DC307

Add NAT NIC temporarily in VMware to get internet access



Open a browser on DC307 and go to:

<https://learn.microsoft.com/en-us/microsoftteams/msi-deployment#msi-files>

Download the 64-bit installer and save it to C:\Software

Remove the NAT NIC after download

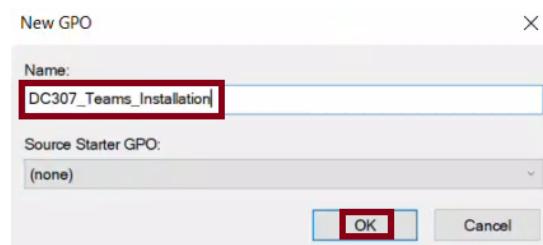


Step 4 – Create a New GPO on DC107

Open Group Policy Management (gpmc.msc)

Right-click Group Policy Objects → New

Name the GPO: DC307_Teams_Installation



Click OK

Step 5 – Assign the Teams MSI Package to the GPO on DC107

Open Group Policy Management (gpmc.msc)

Right-click the GPO DC307_Teams_Installation → Edit

Navigate to: Computer Configuration → Policies → Software Settings → Software installation

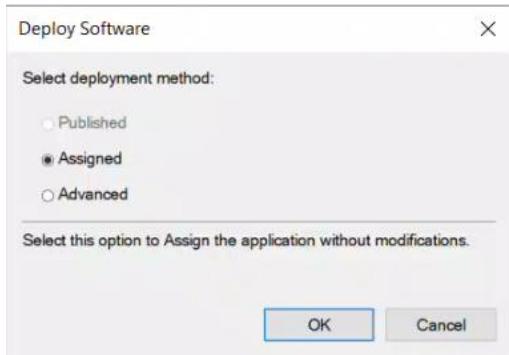
Right-click Software installation → New → Package

Enter the UNC path: \\DC307\Software\Teams_windows_x64.msi

When prompted in the 'Deploy Software' window, select: Assigned

Click OK to confirm the package deployment method

The image shows two windows. The top window is the 'Search Software' search interface, showing a result for 'Teams_windows_x64.msi'. The bottom window is the 'Edit DC307_Teams_Installation [DC207.VLABS07.COM] Policy' window. It shows the navigation tree: Computer Configuration > Policies > Software Settings > Software installation. A 'New' button is highlighted in red. To its right is a 'Package...' button. A small 'File name:' dropdown also has 'Teams_windows_x64.msi' selected. The status bar at the bottom right says 'Windows Installer packages (*.m'.



Step 6 - Link the GPO to the Engineering OU on DC107

In GPMC, locate the Engineering OU
Right-click Engineering → Link an Existing GPO
Select DC307_Teams_Installation → Click OK

The screenshot displays two windows. On the left is the 'Select GPO' dialog box, which has 'vslabs07.com' selected in the 'Look in this domain:' dropdown. In the 'Group Policy objects:' list, 'DC307_Teams_Installation' is highlighted with a blue selection bar. At the bottom are 'OK' and 'Cancel' buttons. On the right is the 'Engineering' GPO properties window, specifically the 'Linked Group Policy Objects' tab. It lists two GPOs: 'RestrictTeamsStarting' (order 1) and 'DC307_Teams_Installation' (order 2). The 'OK' button is highlighted with a red square.

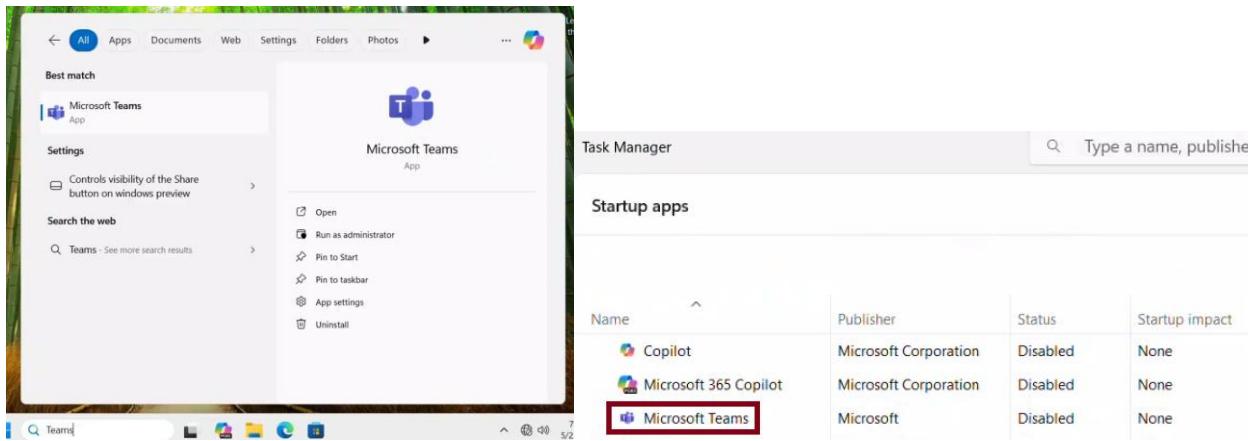
Step 7 - Apply the GPO and Restart Client07

Log in to Client07
Open Command Prompt
Run the command: gpupdate /force
Then run: shutdown /r /t 0

```
C:\Users\Mario.Caron>gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

Step 8 – Validate the Installation on Client07

Log **in** as a user from the Engineering OU
Open **Start** Menu and check **for** Microsoft Teams
Confirm Teams is installed and does not auto-start



Task 9: Managing Scripts with GPO

Systems Involved:

- DC307 (File Server hosting the shared Public folder)
- DC107 (GPO Configuration and script storage via NETLOGON)
- Client07 (Validation of drive mapping and script execution)

Step 1 - What is a Logon Script?

Logon scripts are automated actions triggered when a user signs into a domain account. These scripts can be used to map drives, launch programs, or apply settings. In this task, we will map a shared network folder from DC3XX to drive letter Z: every time a user logs in.

We will store the script centrally in the NETLOGON folder so it replicates across domain controllers, and assign it through a domain-linked GPO.

Step 2 - Create and Share the Public Folder on DC307

Open File Explorer on DC307

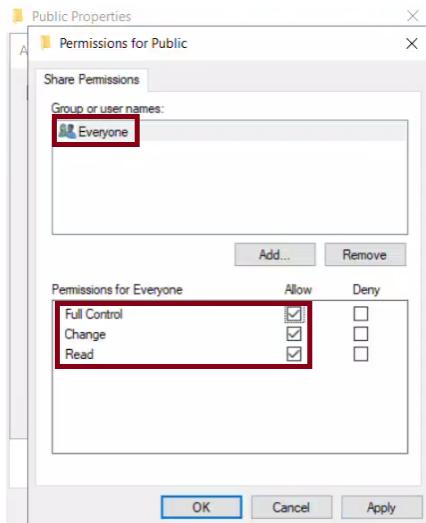
Create the folder C:\Public

Right-click the folder → Properties → Sharing tab → Advanced Sharing

Check Share this folder

Set share name to: Public

Click Permissions → Add Everyone → Allow Full Control



Click OK and apply all windows

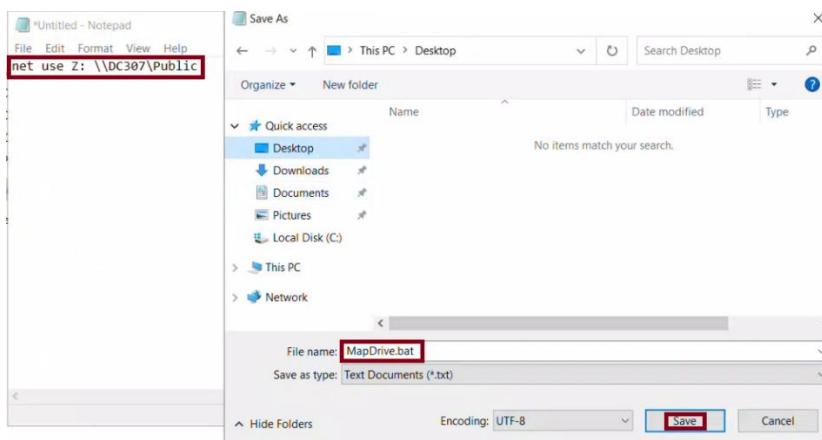
Step 3 – Create the Logon Script

Open Notepad on DC307

Type the following line:

```
net use Z: \\DC307\Public
```

Save the file as MapDrive.bat to the Desktop or another temporary location

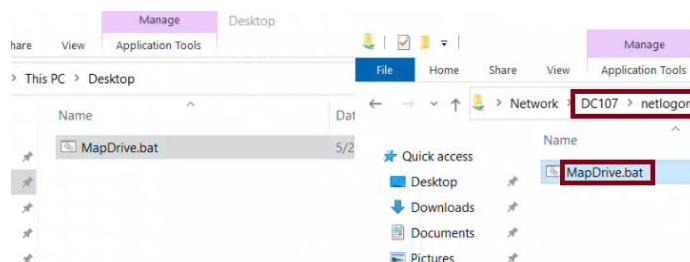


Step 4 – Store the Script in NETLOGON on DC107

Open File Explorer on DC107

Navigate to: C:\Windows\SYSVOL\sysvol\vlabs07.com\SCRIPTS

Copy MapDrive.bat into this folder



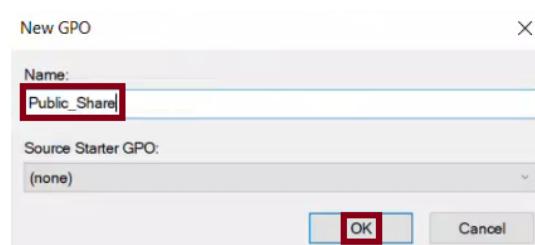
This location is automatically shared as \\DC107\NETLOGON

Step 5 – Create the GPO

On DC107, open Group Policy Management

Right-click Group Policy Objects → New

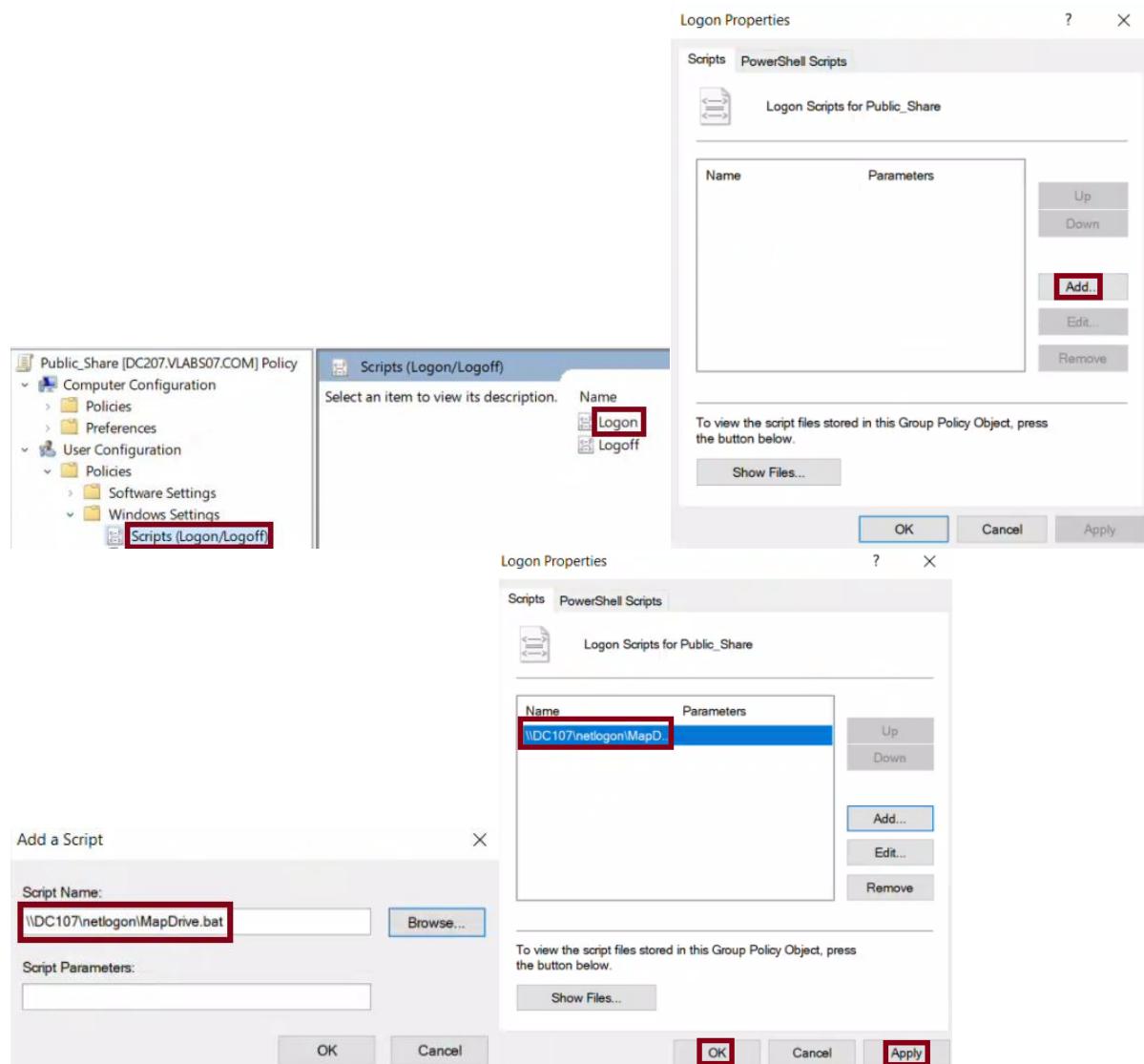
Name the new GPO: Public_Share



Click OK

Step 6 – Assign Logon Script in GPO

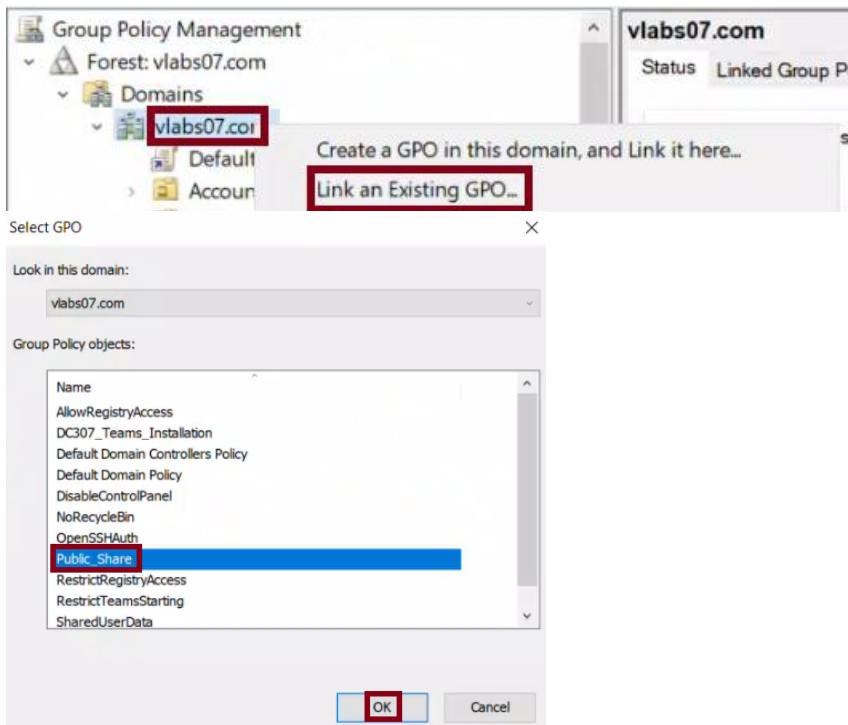
Right-click the GPO Public_Share → Edit
Navigate to: User Configuration → Policies → Windows Settings → Scripts (Logon/Logoff)
Double-click Logon → Click Add
Click Browse → Select MapDrive.bat from the NETLOGON folder



Click OK and Apply

Step 7 – Link the GPO to the Domain

In GPMC, drag or link the Public_Share GPO to the domain root (vlabs07.com)
Confirm the GPO appears under the domain with a link enabled



Step 8 – Apply the GPO and Validate on Client07

Log [in](#) to Client07 as any domain user
Open Command [Prompt](#) and run: gpupdate /force
Log off and back [in](#)

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

Step 9 – Confirm Drive Mapping and Write Access

Open File Explorer on Client07
Verify that drive Z: is mapped to \\DC307\Public
Open the Z: drive and [try](#) to create a new folder or text file
Confirm that the user has [write](#) access to the public share

