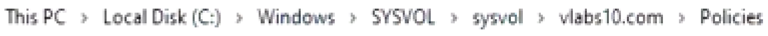
Jacob Chedore

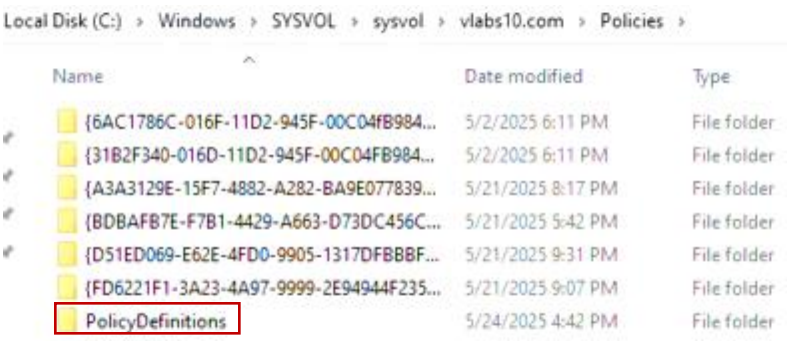
Lab Assignment 2 (Part 2) – GPO

Task 1: Creating a Central Store for Administrative Templates

- Create a central store for Administrative Templates on DC1XX.



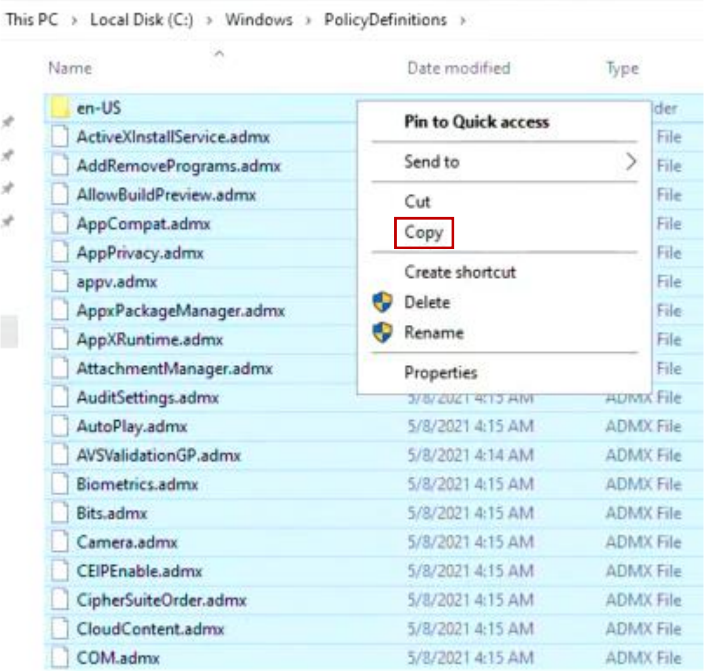
This PC > Local Disk (C:) > Windows > SYSVOL > sysvol > vlabs10.com > Policies



Local Disk (C:) > Windows > SYSVOL > sysvol > vlabs10.com > Policies >

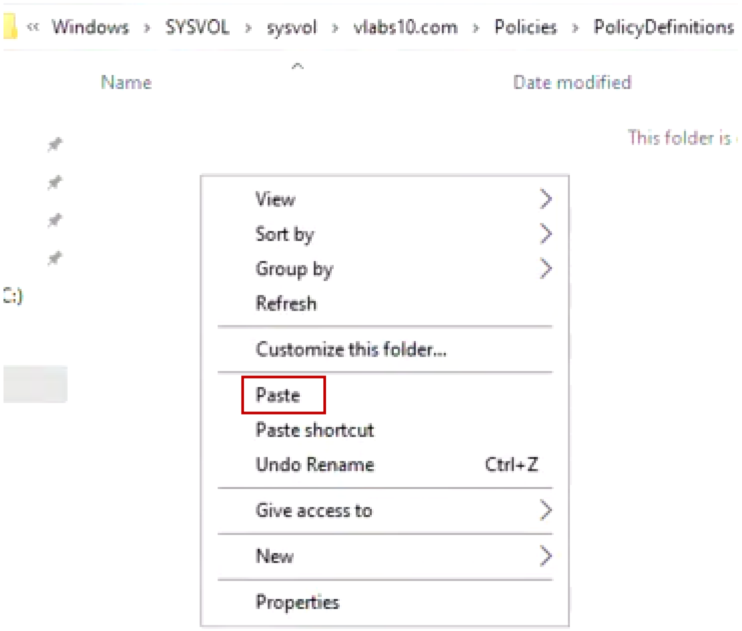
Name	Date modified	Type
{6AC1786C-016F-11D2-945F-00C04fB984...	5/2/2025 6:11 PM	File folder
{31B2F340-016D-11D2-945F-00C04FB984...	5/2/2025 6:11 PM	File folder
{A3A3129E-15F7-4882-A282-BA9E077839...	5/21/2025 8:17 PM	File folder
{BDBAFB7E-F7B1-4429-A663-D73DC456C...	5/21/2025 5:42 PM	File folder
{D51ED069-E62E-4FD0-9905-1317DFBBBF...	5/21/2025 9:31 PM	File folder
{FD6221F1-3A23-4A97-9999-2E94944F235...	5/21/2025 9:07 PM	File folder
PolicyDefinitions	5/24/2025 4:42 PM	File folder

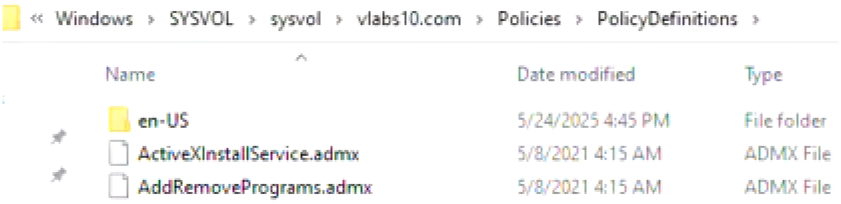
- Copy all ADMX and ADML files to this Central store.



This PC > Local Disk (C:) > Windows > PolicyDefinitions >

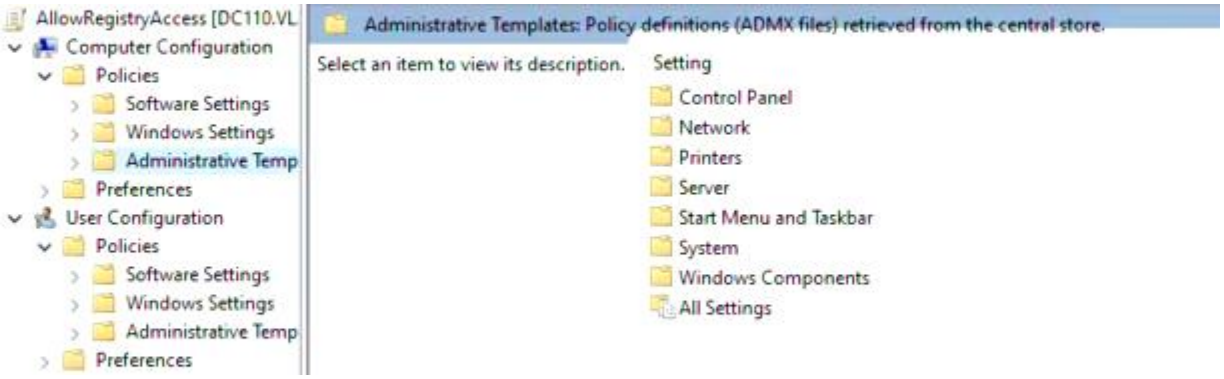
Name	Date modified	Type
en-US		der
ActiveXInstallService.admx		File
AddRemovePrograms.admx		File
AllowBuildPreview.admx		File
AppCompat.admx		File
AppPrivacy.admx		File
appv.admx		File
AppxPackageManager.admx		File
AppXRuntime.admx		File
AttachmentManager.admx		File
AuditSettings.admx	5/8/2021 4:15 AM	ADMX File
AutoPlay.admx	5/8/2021 4:15 AM	ADMX File
AVSValidationGP.admx	5/8/2021 4:14 AM	ADMX File
Biometrics.admx	5/8/2021 4:15 AM	ADMX File
Bits.admx	5/8/2021 4:15 AM	ADMX File
Camera.admx	5/8/2021 4:15 AM	ADMX File
CEIPEnable.admx	5/8/2021 4:15 AM	ADMX File
CipherSuiteOrder.admx	5/8/2021 4:15 AM	ADMX File
CloudContent.admx	5/8/2021 4:15 AM	ADMX File
COM.admx	5/8/2021 4:15 AM	ADMX File




« Windows › SYSVOL › sysvol › vlabs10.com › Policies › PolicyDefinitions ›

Name	Date modified	Type
en-US	5/24/2025 4:45 PM	File folder
ActiveXInstallService.admx	5/8/2021 4:15 AM	ADMX File
AddRemovePrograms.admx	5/8/2021 4:15 AM	ADMX File

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

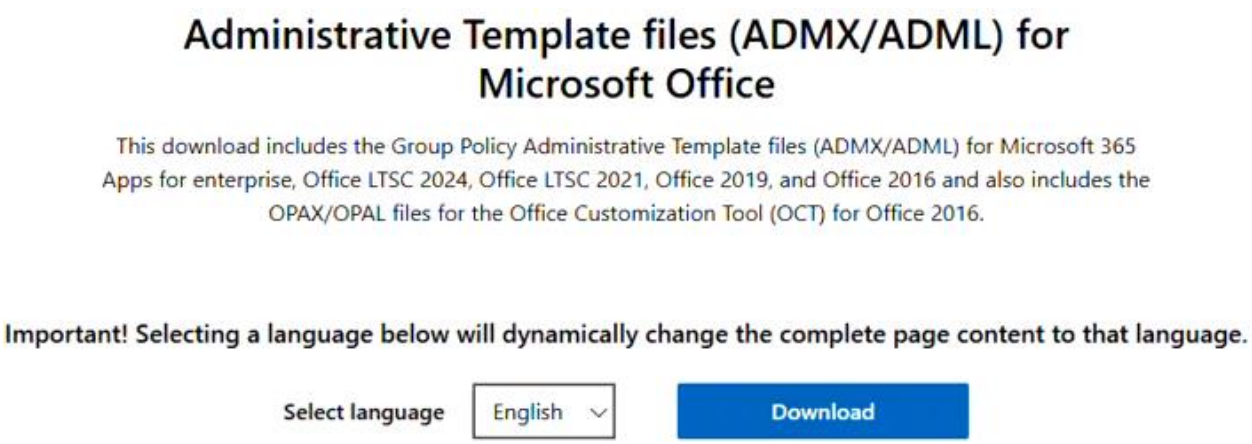


Administrative Templates: Policy definitions (ADMX files) retrieved from the central store.

Select an item to view its description.

Task 2: Managing and Configuring Administrative Templates

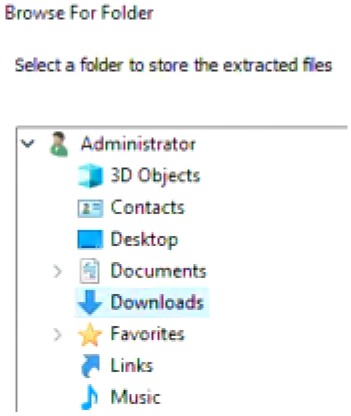
- Download and install Microsoft Office Administrative Templates (You will need to add the NAT NIC to download this package. Remove it after completing the download).



Administrative Template files (ADMX/ADML) for Microsoft Office

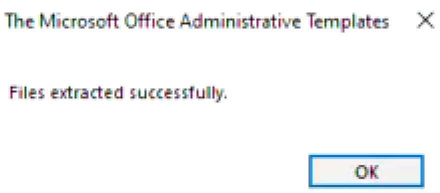
This download includes the Group Policy Administrative Template files (ADMX/ADML) for Microsoft 365 Apps for enterprise, Office LTSC 2024, Office LTSC 2021, Office 2019, and Office 2016 and also includes the OPAX/OPAL files for the Office Customization Tool (OCT) for Office 2016.

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



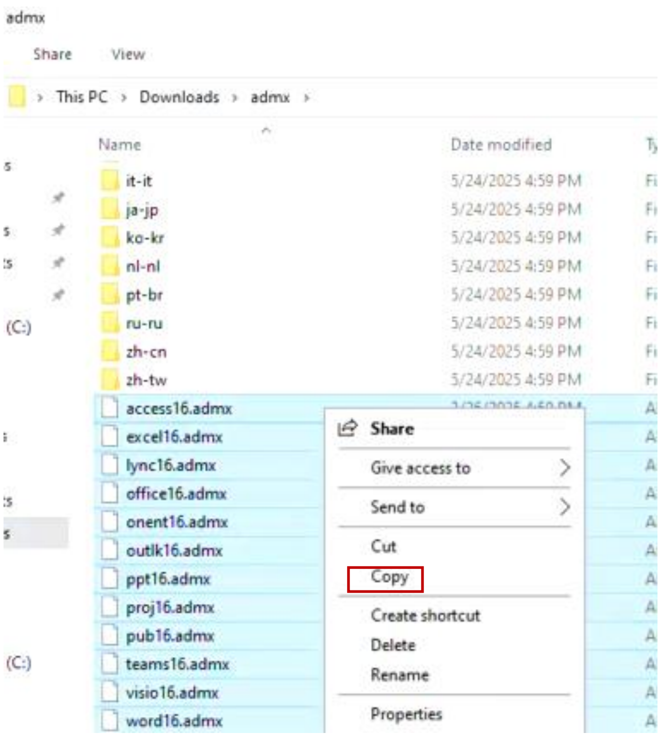
Browse For Folder

Select a folder to store the extracted files



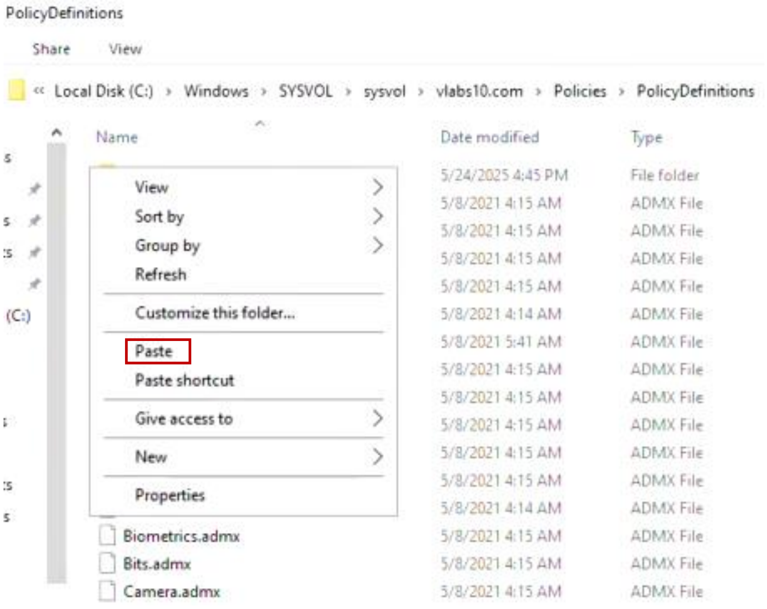
The Microsoft Office Administrative Templates

Files extracted successfully.

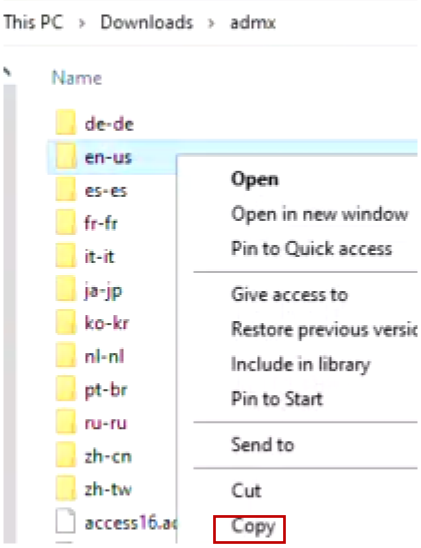


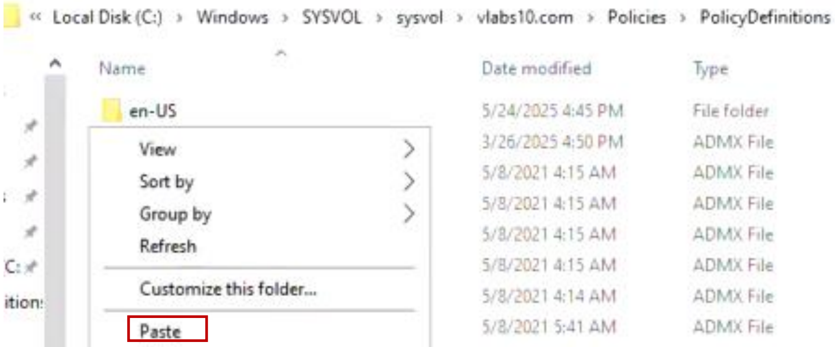
admx

Name	Date modified	T
it-it	5/24/2025 4:59 PM	Fi
ja-jp	5/24/2025 4:59 PM	Fi
ko-kr	5/24/2025 4:59 PM	Fi
nl-nl	5/24/2025 4:59 PM	Fi
pt-br	5/24/2025 4:59 PM	Fi
ru-ru	5/24/2025 4:59 PM	Fi
zh-cn	5/24/2025 4:59 PM	Fi
zh-tw	5/24/2025 4:59 PM	Fi
access16.admx		A
excel16.admx		A
lync16.admx		A
office16.admx		A
onent16.admx		A
outlk16.admx		A
ppt16.admx		A
proj16.admx		A
pub16.admx		A
teams16.admx		A
visio16.admx		A
word16.admx		A



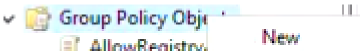
Name	Date modified	Type
	5/24/2025 4:45 PM	File folder
	5/8/2021 4:15 AM	ADMX File
	5/8/2021 4:15 AM	ADMX File
	5/8/2021 4:15 AM	ADMX File
	5/8/2021 4:15 AM	ADMX File
	5/8/2021 4:14 AM	ADMX File
	5/8/2021 5:41 AM	ADMX File
	5/8/2021 4:15 AM	ADMX File
	5/8/2021 4:15 AM	ADMX File
	5/8/2021 4:15 AM	ADMX File
	5/8/2021 4:15 AM	ADMX File
	5/8/2021 4:15 AM	ADMX File
	5/8/2021 4:14 AM	ADMX File
Biometrics.admx	5/8/2021 4:15 AM	ADMX File
Bits.admx	5/8/2021 4:15 AM	ADMX File
Camera.admx	5/8/2021 4:15 AM	ADMX File

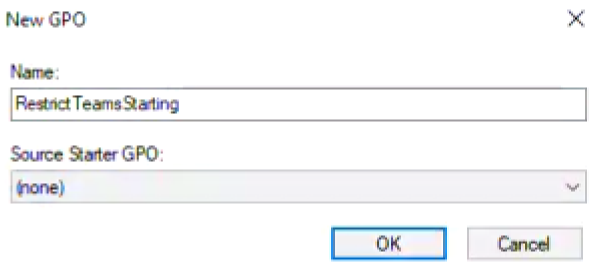



« Local Disk (C:) › Windows › SYSVOL › sysvol › vlabs10.com › Policies › PolicyDefinitions
C:
ition
View
Sort by
Group by
Refresh
Customize this folder...
Paste

Name	Date modified	Type
en-US	5/24/2025 4:45 PM	File folder
	3/26/2025 4:50 PM	ADMX File
	5/8/2021 4:15 AM	ADMX File
	5/8/2021 4:15 AM	ADMX File
	5/8/2021 4:15 AM	ADMX File
	5/8/2021 4:15 AM	ADMX File
	5/8/2021 4:14 AM	ADMX File
	5/8/2021 5:41 AM	ADMX File

- Create a new GPO named RestrictTeamsStarting.



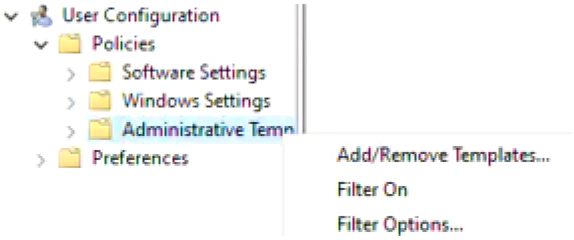


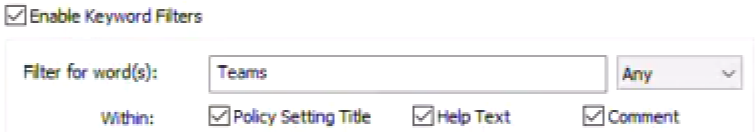
New GPO

Name: Restrict Teams Starting

Source Starter GPO: (none)

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

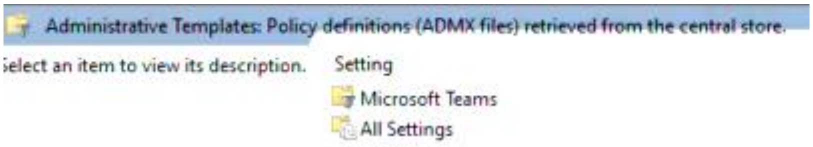




☑ Enable Keyword Filters

Filter for word(s): Teams — Any

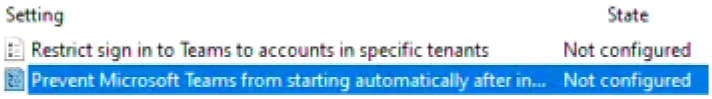
Within: ☑ Policy Setting Title ☑ Help Text ☑ Comment



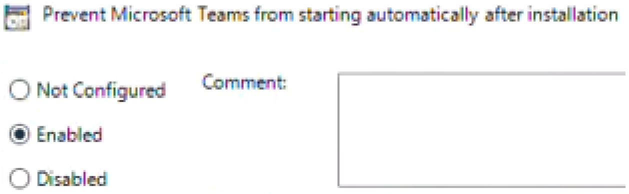
Administrative Templates: Policy definitions (ADMX files) retrieved from the central store.

Select an item to view its description.

- Enable Prevent Microsoft Teams from starting automatically after installation.



Setting	State
Restrict sign in to Teams to accounts in specific tenants	Not configured
Prevent Microsoft Teams from starting automatically after in...	Not configured

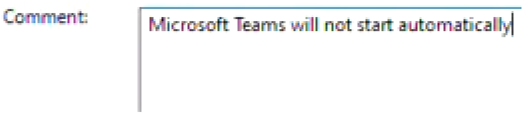


Prevent Microsoft Teams from starting automatically after installation

○ Not Configured
● Enabled
○ Disabled

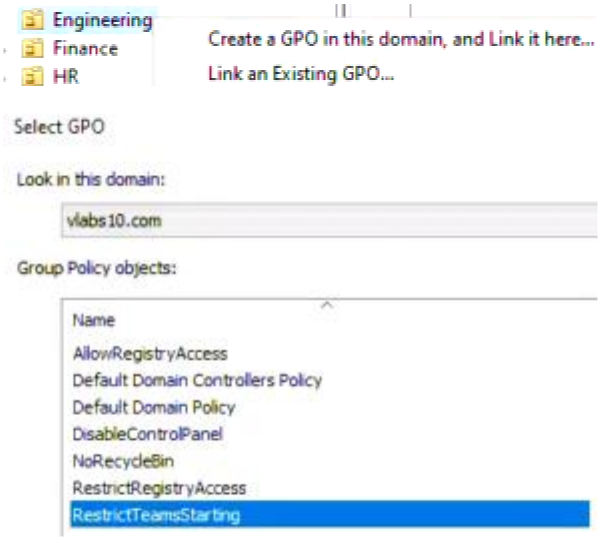
Comment:

- Add a comment to document this setting.



Comment: Microsoft Teams will not start automatically

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



Select GPO

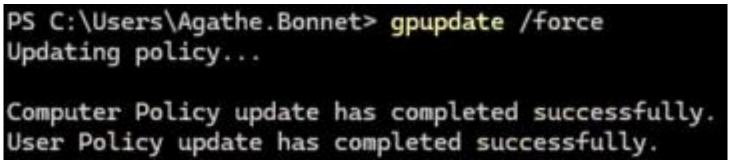
Look in this domain:

vlabs10.com

Group Policy objects:

Name
AllowRegistryAccess
Default Domain Controllers Policy
Default Domain Policy
DisableControlPanel
NoRecycleBin
RestrictRegistryAccess
RestrictTeamsStarting

- Run gpupdate /force to apply changes.



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

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

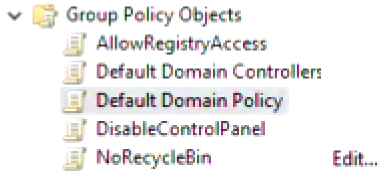
Task 3: Managing Account Policies

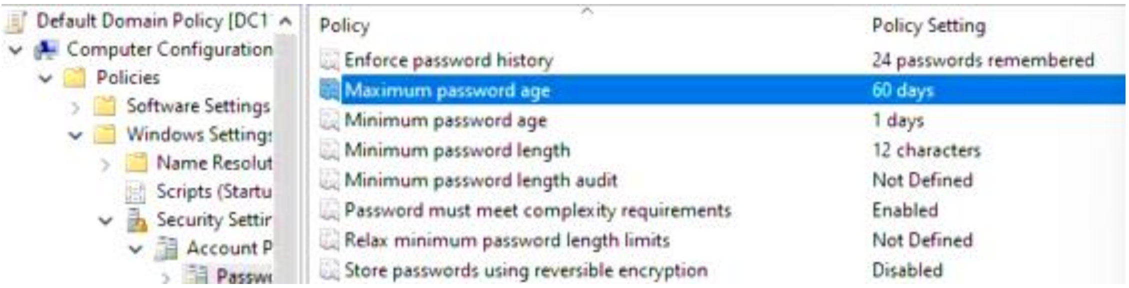
- Modify password policies in the Default Domain Policy GPO:

o Minimum password length: 12 characters.

o Password complexity: Enabled.

o Password expiration: 60 days.



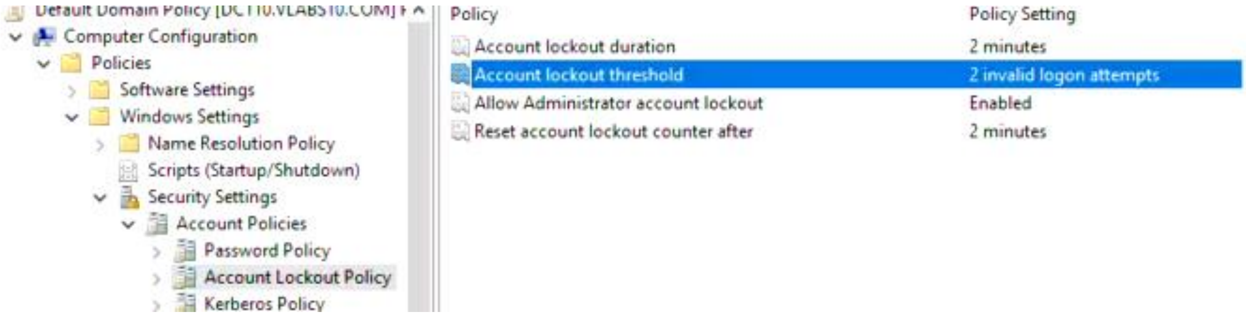


Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	12 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Not Defined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

- Apply Account Lockout Policy:

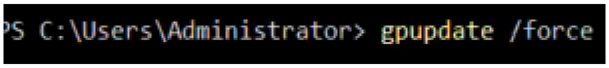
o Lock account after 2 failed login attempts.

o Lockout duration: 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

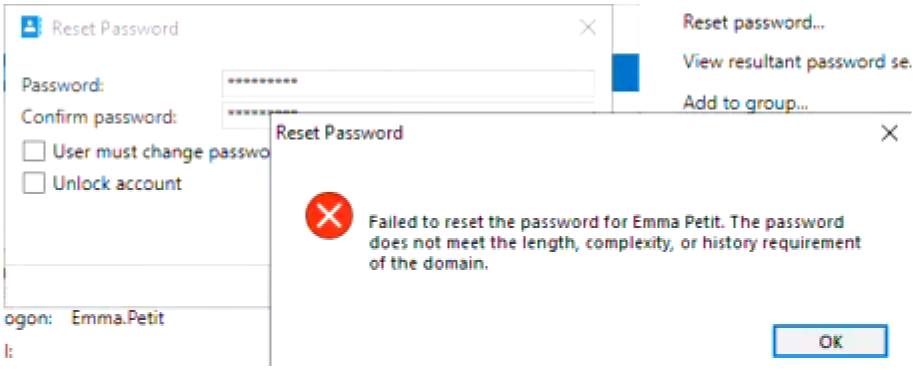
- Run gpupdate /force to apply changes.



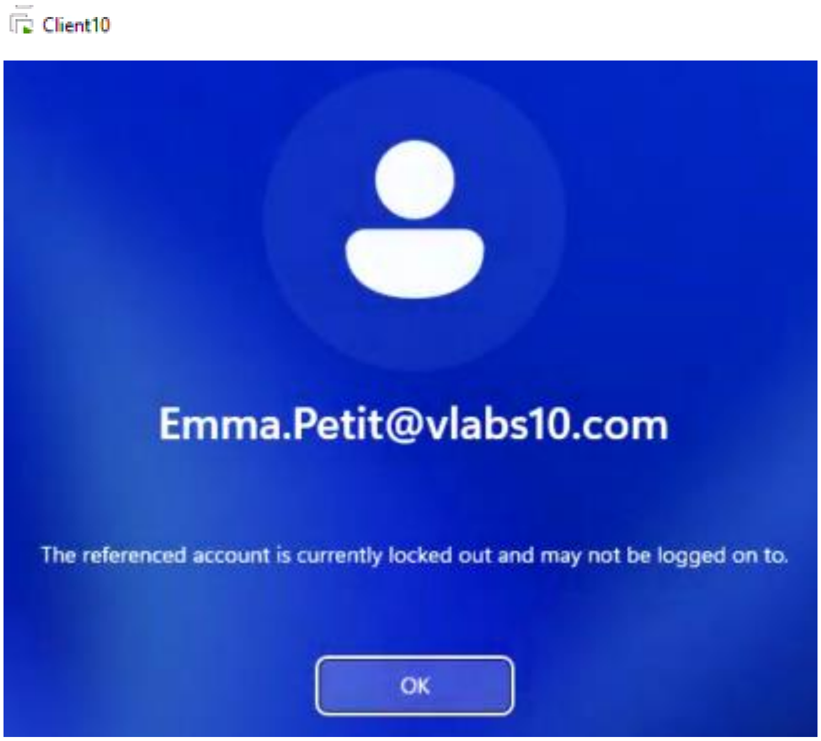
```
PS C:\Users\Administrator> gpupdate /force
```

- Restart the ClientXX.

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

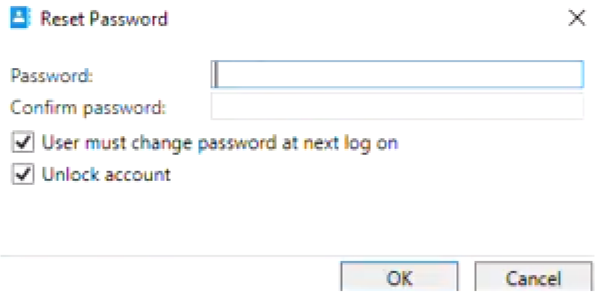


Failed to reset the password for Emma Petit. The password does not meet the length, complexity, or history requirement of the domain.



Emma.Petit@vlabs10.com

The referenced account is currently locked out and may not be logged on to.



Reset Password

Password:

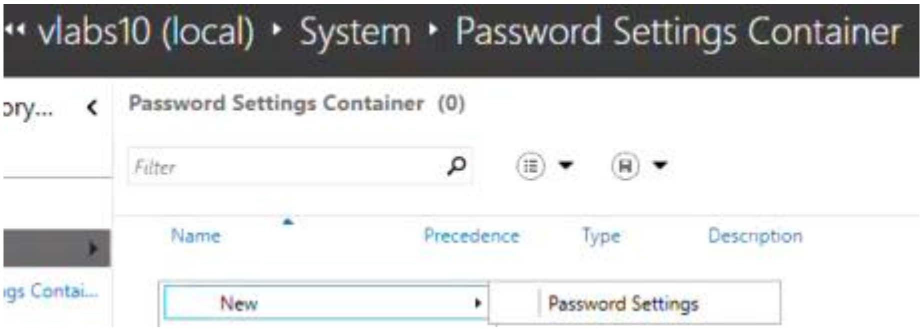
Confirm password:

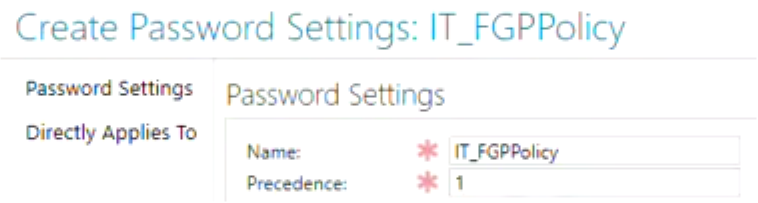
☑ User must change password at next log on

☑ Unlock account

Task 4: Implementing Fine-Grained Password Policies

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


vlabs10 (local) ▸ System ▸ Password Settings Container
ory...
Password Settings Container (0)
Filter
Name
Precedence
Type
Description
gs Contai...
New
Password Settings



Create Password Settings: IT_FGPPolicy

Password Settings

Name: * IT_FGPPolicy

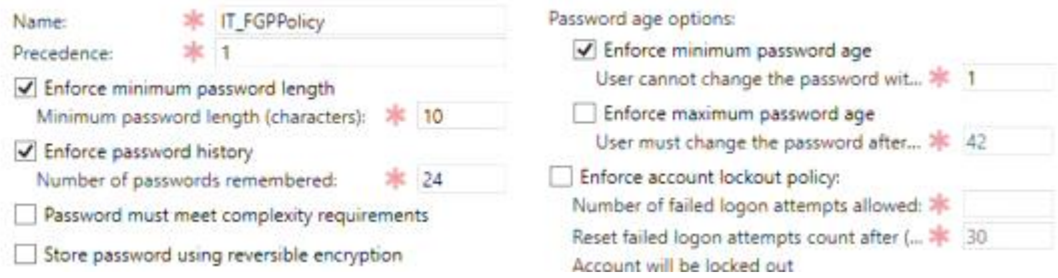
Precedence: * 1

- Modify password settings:

o Minimum password length: 10 characters.

o Password complexity: Disabled.

o Password expiration: Never.



Name: * IT_FGPPolicy

Precedence: * 1

☑ Enforce minimum password length

Minimum password length (characters): * 10

☑ Enforce password history

Number of passwords remembered: * 24

□ Password must meet complexity requirements

□ Store password using reversible encryption

Password age options:

☑ Enforce minimum password age

User cannot change the password wit... * 1

□ Enforce maximum password age

User must change the password after... * 42

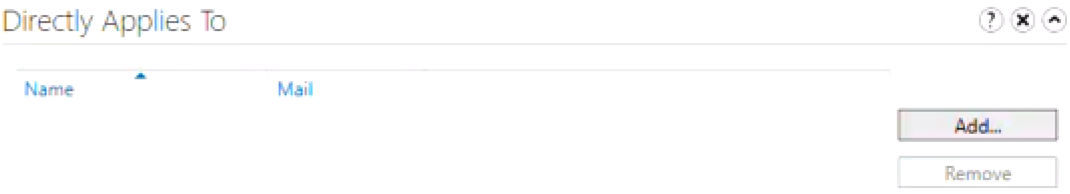
□ Enforce account lockout policy:

Number of failed logon attempts allowed: *

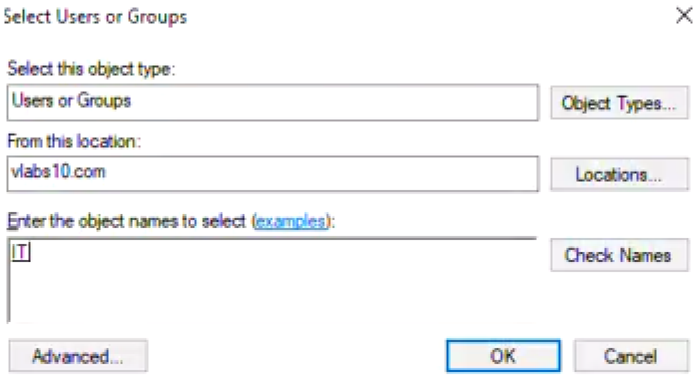
Reset failed logon attempts count after (... * 30

Account will be locked out

- Directly apply it to the IT Group.



Directly Applies To



Select Users or Groups

Select this object type:

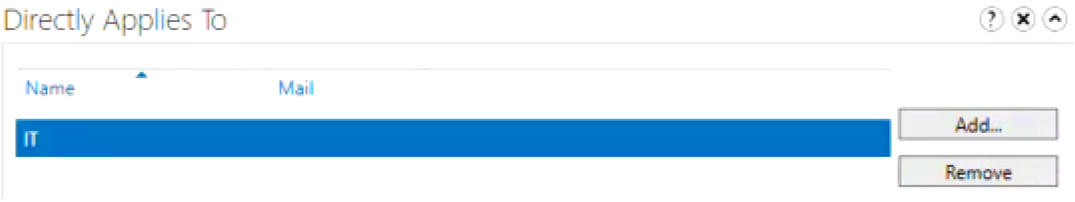
Users or Groups

From this location:

vlabs10.com

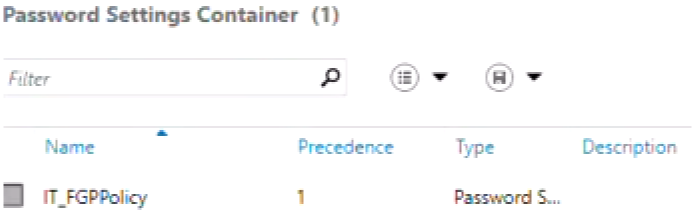
Enter the object names to select (examples):

IT



Directly Applies To

Name	Mail
IT	

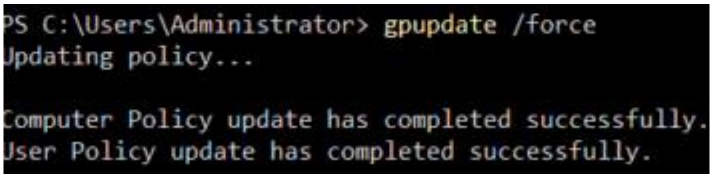


Password Settings Container (1)

Filter

Name	Precedence	Type	Description
IT_FGPPolicy	1	Password S...	

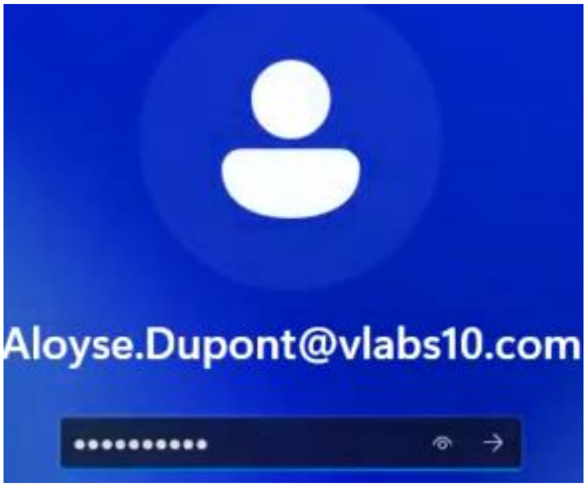
- Run gpupdate /force to apply changes.



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

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

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

Client10

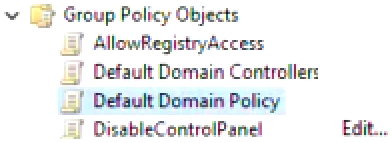


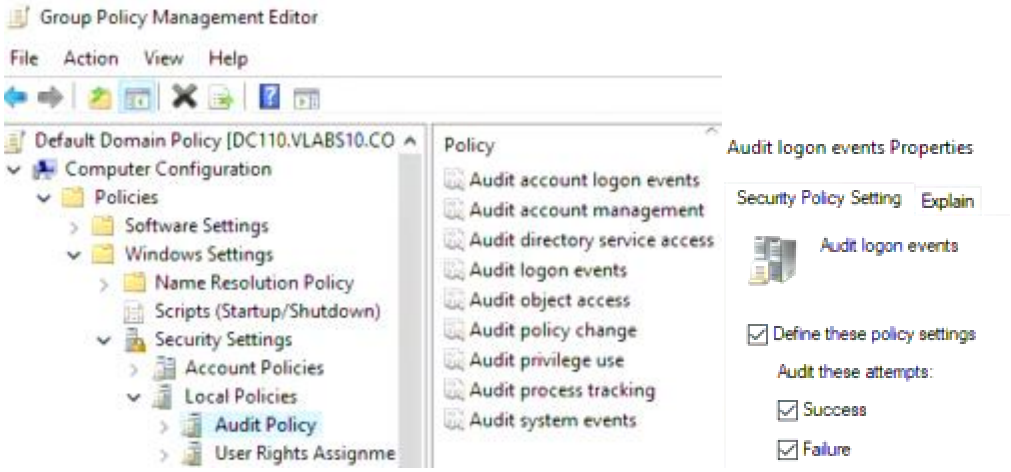
Aloyse.Dupont@vlabs10.com

•••••••••••

Task 5: Managing Audit Authentication

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





Audit logon events

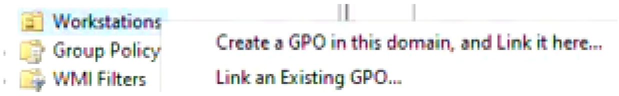
☑ Define these policy settings

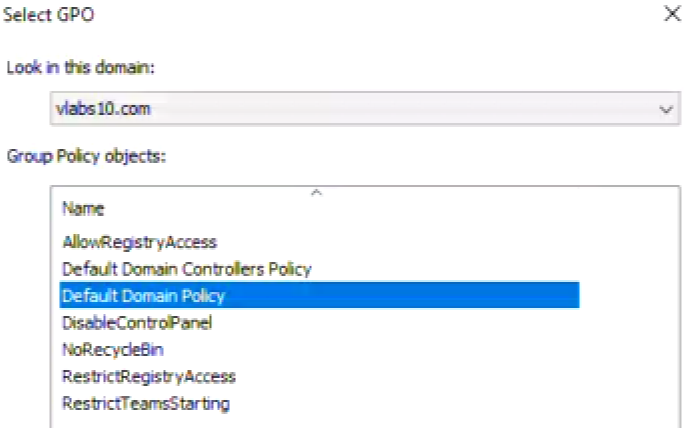
Audit these attempts:

☑ Success

☑ Failure

- Link the GPO to Workstations OU (where ClientXX is located).





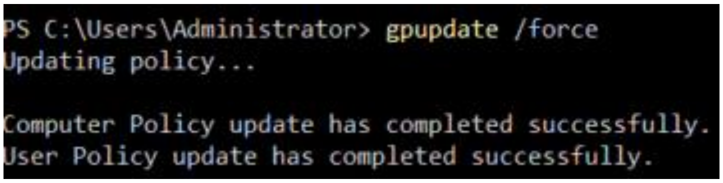
Look in this domain:

vlabs10.com

Group Policy objects:

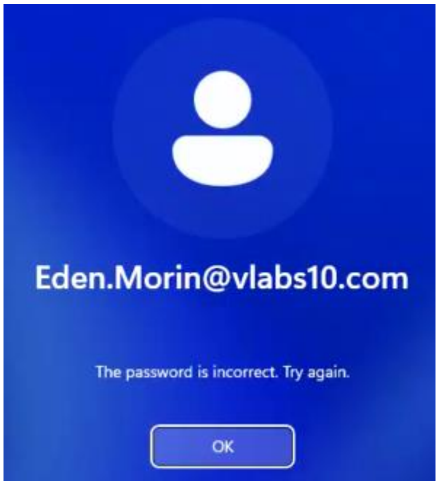
Name
AllowRegistryAccess
Default Domain Controllers Policy
Default Domain Policy
DisableControlPanel
NoRecycleBin
RestrictRegistryAccess
RestrictTeamsStarting

- Run gpupdate /force to apply changes.



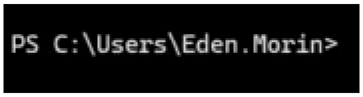
```
PS C:\Users\Administrator> gpupdate /force
Updating policy...

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

- Test by failing and successfully logging in with any user on ClientXX.



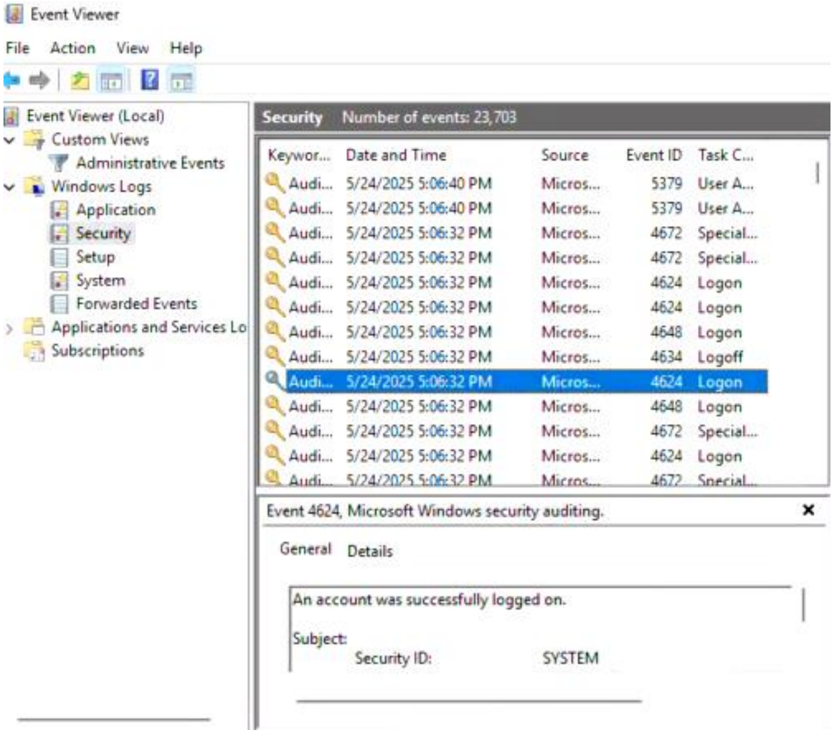
Eden.Morin@vlabs10.com

The password is incorrect. Try again.



```
PS C:\Users\Eden.Morin>
```

- Open Event Viewer on ClientXX using an Administrator account and verifying logged events.



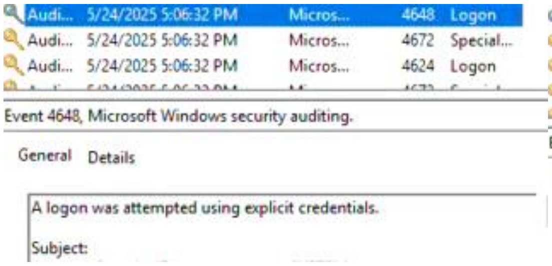
Security Number of events: 23,703

Keywor...	Date and Time	Source	Event ID	Task C...
Audi...	5/24/2025 5:06:40 PM	Micros...	5379	User A...
Audi...	5/24/2025 5:06:40 PM	Micros...	5379	User A...
Audi...	5/24/2025 5:06:32 PM	Micros...	4672	Special...
Audi...	5/24/2025 5:06:32 PM	Micros...	4672	Special...
Audi...	5/24/2025 5:06:32 PM	Micros...	4624	Logon
Audi...	5/24/2025 5:06:32 PM	Micros...	4624	Logon
Audi...	5/24/2025 5:06:32 PM	Micros...	4648	Logon
Audi...	5/24/2025 5:06:32 PM	Micros...	4634	Logoff
Audi...	5/24/2025 5:06:32 PM	Micros...	4624	Logon
Audi...	5/24/2025 5:06:32 PM	Micros...	4648	Logon
Audi...	5/24/2025 5:06:32 PM	Micros...	4672	Special...
Audi...	5/24/2025 5:06:32 PM	Micros...	4624	Logon
Audi...	5/24/2025 5:06:32 PM	Micros...	4672	Special...

Event 4624, Microsoft Windows security auditing.

An account was successfully logged on.

Subject:
Security ID: SYSTEM

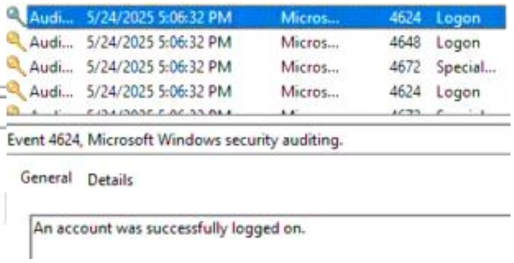


```
Audi...  5/24/2025 5:06:32 PM  Micros...  4648  Logon
Audi...  5/24/2025 5:06:32 PM  Micros...  4672  Special...
Audi...  5/24/2025 5:06:32 PM  Micros...  4624  Logon
```

Event 4648, Microsoft Windows security auditing.

A logon was attempted using explicit credentials.

Subject:



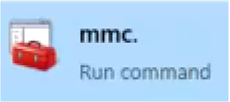
```
Audi...  5/24/2025 5:06:32 PM  Micros...  4624  Logon
Audi...  5/24/2025 5:06:32 PM  Micros...  4648  Logon
Audi...  5/24/2025 5:06:32 PM  Micros...  4672  Special...
Audi...  5/24/2025 5:06:32 PM  Micros...  4624  Logon
```

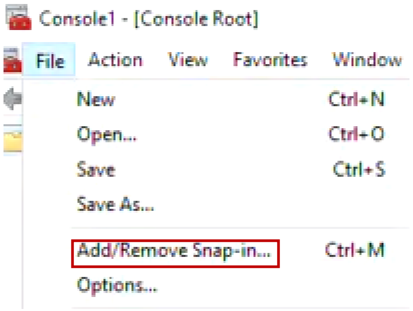
Event 4624, Microsoft Windows security auditing.

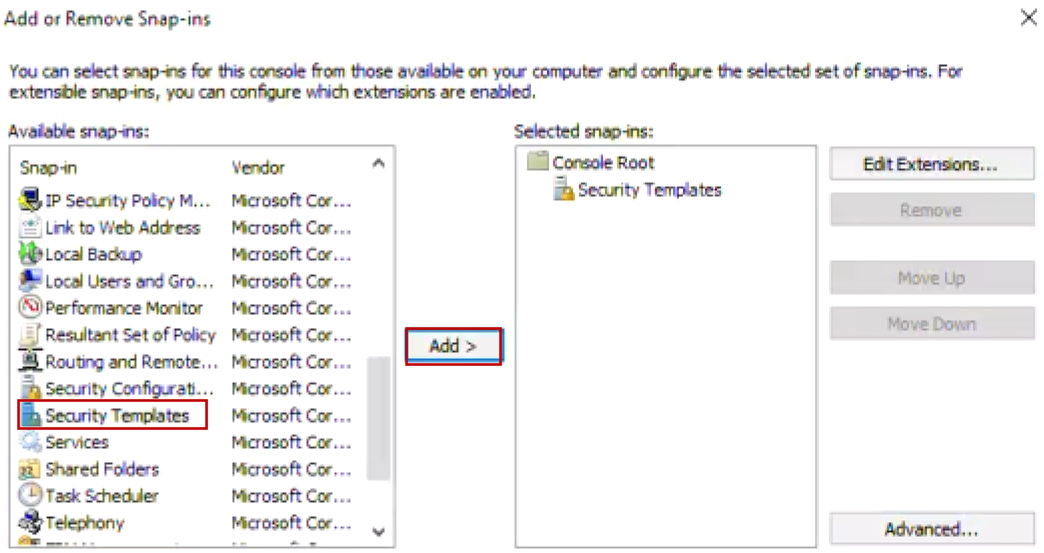
An account was successfully logged on.

Task 6: Managing Security Templates

- Create a security template named OpenSSH_Auth.







Add or Remove Snap-ins

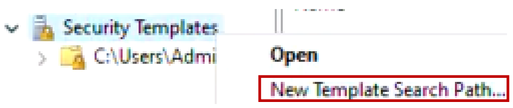
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

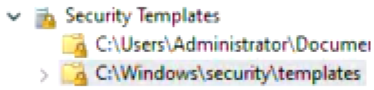
Available snap-ins:

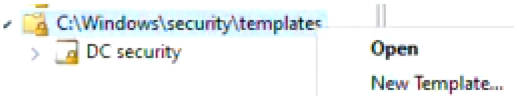
Snap-in	Vendor
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...
Local Backup	Microsoft Cor...
Local Users and Gro...	Microsoft Cor...
Performance Monitor	Microsoft Cor...
Resultant Set of Policy	Microsoft Cor...
Routing and Remote...	Microsoft Cor...
Security Configurati...	Microsoft Cor...
Security Templates	Microsoft Cor...
Services	Microsoft Cor...
Shared Folders	Microsoft Cor...
Task Scheduler	Microsoft Cor...
Telephony	Microsoft Cor...

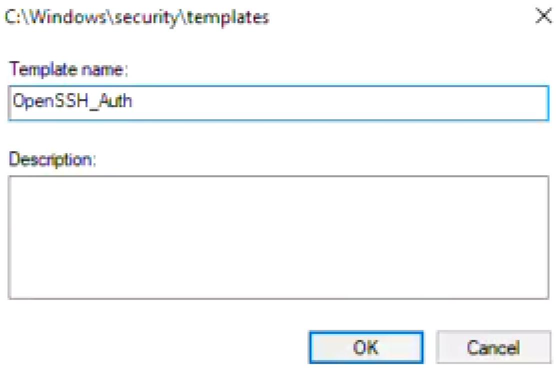
Selected snap-ins:

Console Root
Security Templates





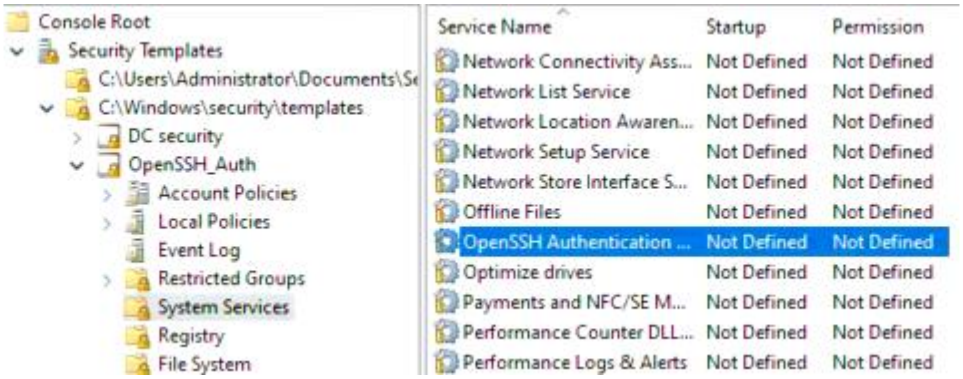



C:\Windows\security\templates

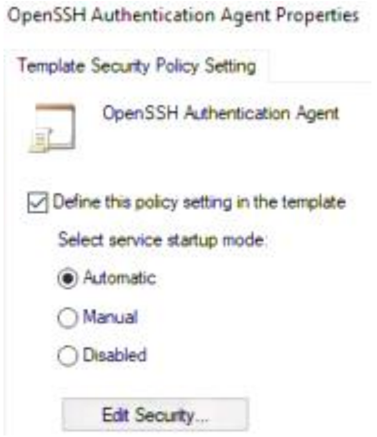
Template name: OpenSSH_Auth

Description:

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



Service Name	Startup	Permission
Network Connectivity Ass...	Not Defined	Not Defined
Network List Service	Not Defined	Not Defined
Network Location Awaren...	Not Defined	Not Defined
Network Setup Service	Not Defined	Not Defined
Network Store Interface S...	Not Defined	Not Defined
Offline Files	Not Defined	Not Defined
OpenSSH Authentication ...	Not Defined	Not Defined
Optimize drives	Not Defined	Not Defined
Payments and NFC/SE M...	Not Defined	Not Defined
Performance Counter DLL...	Not Defined	Not Defined
Performance Logs & Alerts	Not Defined	Not Defined


OpenSSH Authentication Agent Properties

Template Security Policy Setting

OpenSSH Authentication Agent

☑ Define this policy setting in the template

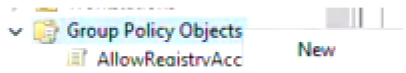
Select service startup mode:

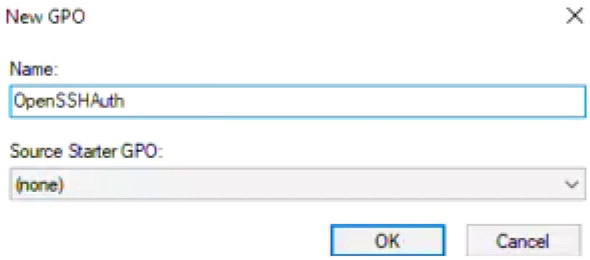
● Automatic

○ Manual

○ Disabled

- Import this new template into a new GPO named OpenSSHAuth.

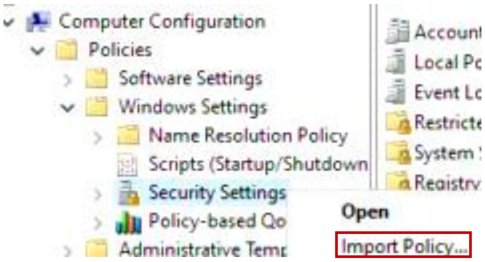


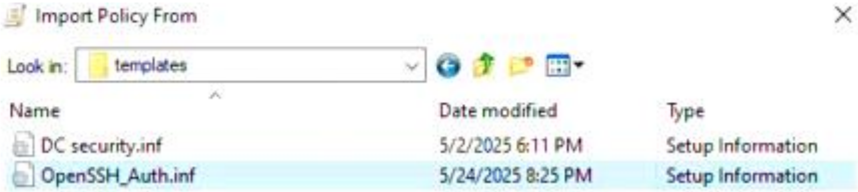


New GPO

Name:
OpenSSHAuth

Source Starter GPO:
(none)



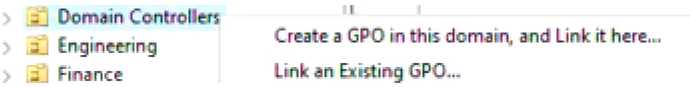


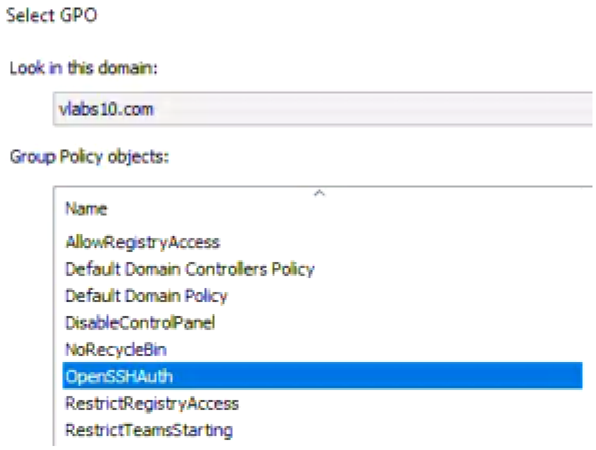
Import Policy From

Look in: templates

Name	Date modified	Type
DC security.inf	5/2/2025 6:11 PM	Setup Information
OpenSSH_Auth.inf	5/24/2025 8:25 PM	Setup Information

- Link the GPO to DomainControllers OU.





Select GPO

Look in this domain:

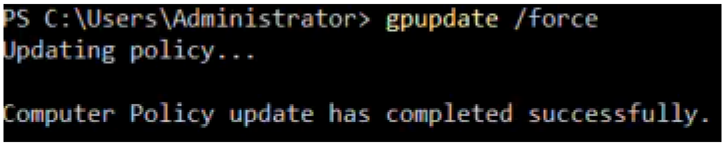
vlabs10.com

Group Policy objects:

Name

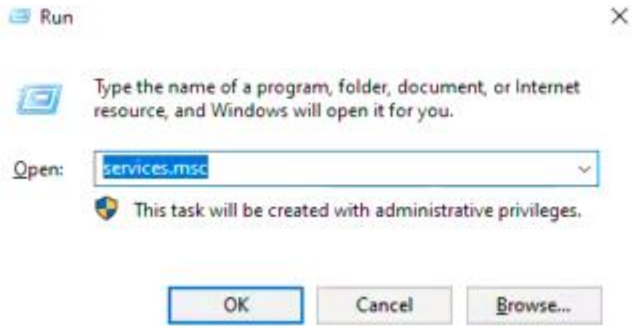
AllowRegistryAccess
Default Domain Controllers Policy
Default Domain Policy
DisableControlPanel
NoRecycleBin
OpenSSHAuth
RestrictRegistryAccess
RestrictTeamsStarting

- Run gpupdate /force on DC1XX to apply changes.



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

Computer Policy update has completed successfully.
```

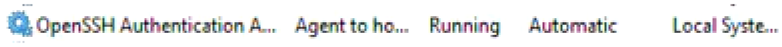
- Restart DC1XX and verify in Services that OpenSSH Authentication Agent has started.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: services.msc

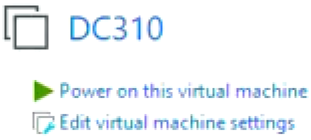
This task will be created with administrative privileges.



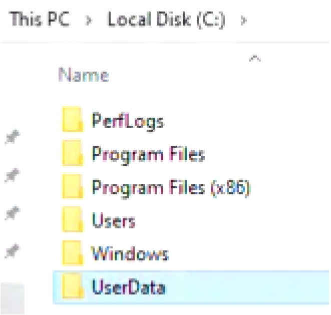
```
OpenSSH Authentication A...   Agent to ho...   Running   Automatic   Local Syste...
```

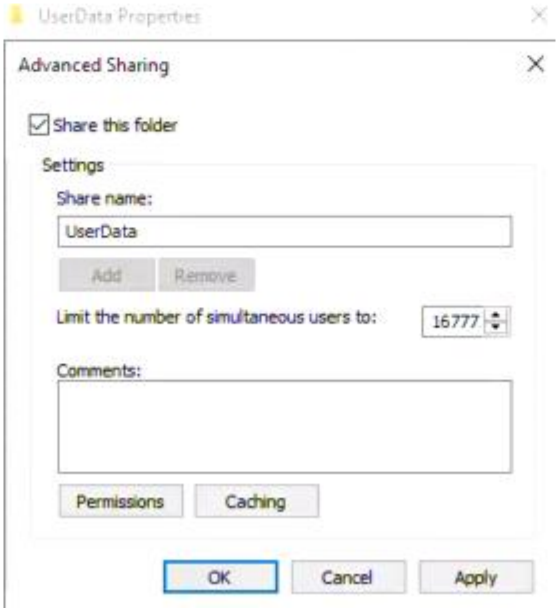
Task 7: Configuring Folder Redirection

- Use DC3XX as the file server.



- Create a shared folder: \\DC3XX\UserData to the HR Group (r & w).





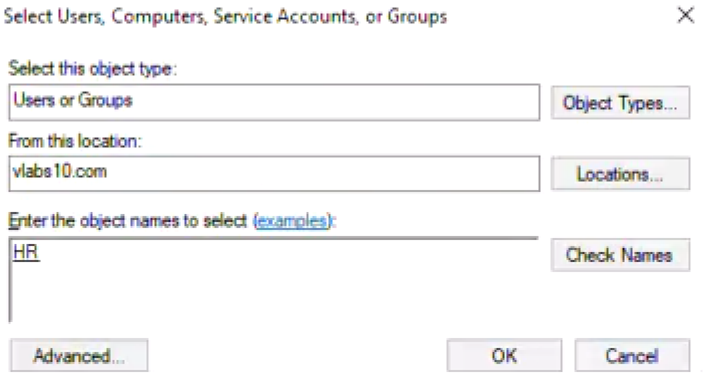
☑ Share this folder

Settings

Share name: UserData

Limit the number of simultaneous users to: 16777

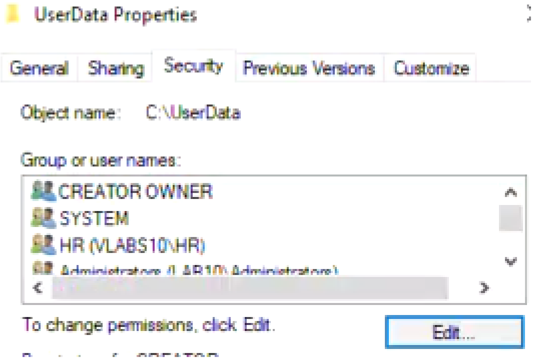
Comments:



Select this object type: Users or Groups

From this location: vlabs10.com

Enter the object names to select (examples): HR



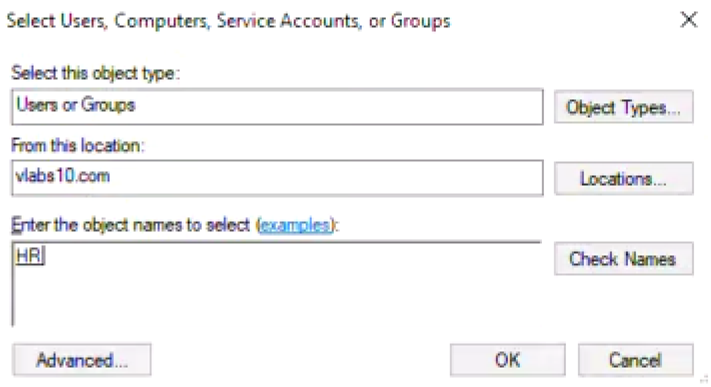
Object name: C:\UserData

Group or user names:

CREATOR OWNER
SYSTEM
HR (VLABS10\HR)
Administrators (LAB10\Administrators)

To change permissions, click Edit.

Permissions for CREATOR

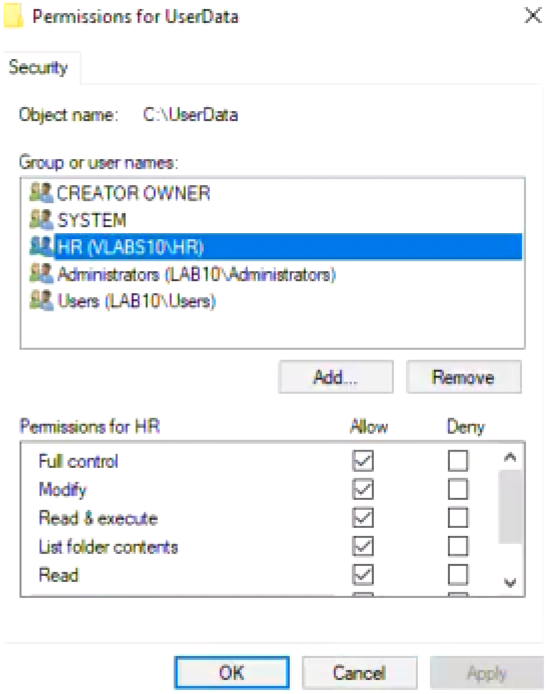


Select Users, Computers, Service Accounts, or Groups

Select this object type:
Users or Groups

From this location:
vlabs10.com

Enter the object names to select (examples):
HR



Permissions for UserData

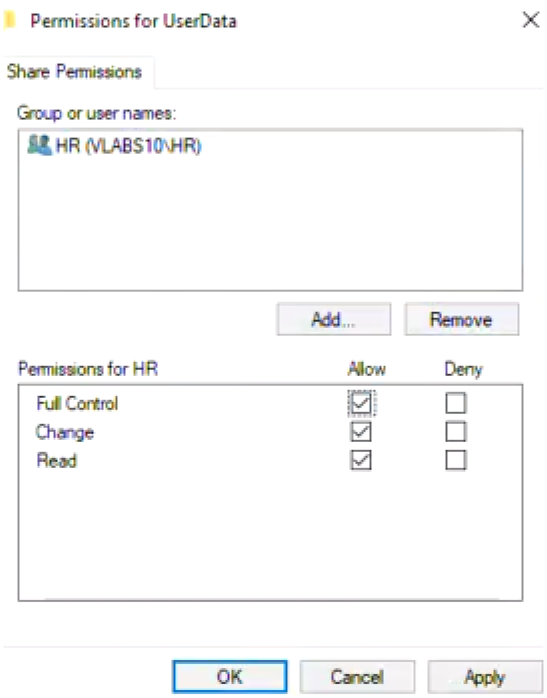
Security

Object name: C:\UserData

Group or user names:

- CREATOR OWNER
- SYSTEM
- HR (VLABS10\HR)
- Administrators (LAB10\Administrators)
- Users (LAB10\Users)

Permissions for HR	Allow	Deny
Full control	☑	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□


Permissions for UserData

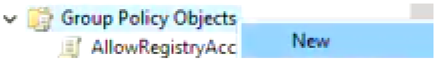
Share Permissions

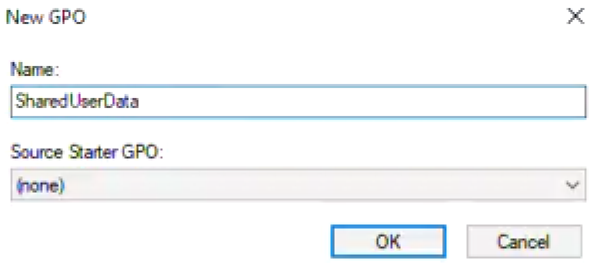
Group or user names:

HR (VLABS10\HR)

Permissions for HR	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

- Create a new GPO named SharedUserData

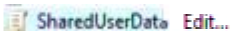


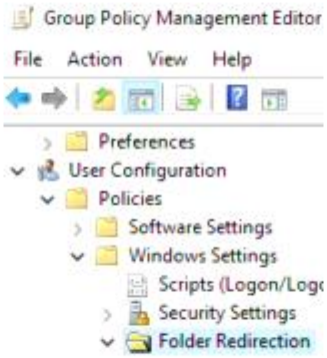

New GPO

Name: SharedUserData

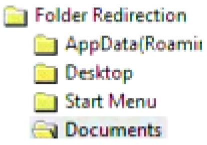
Source Starter GPO: (none)

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

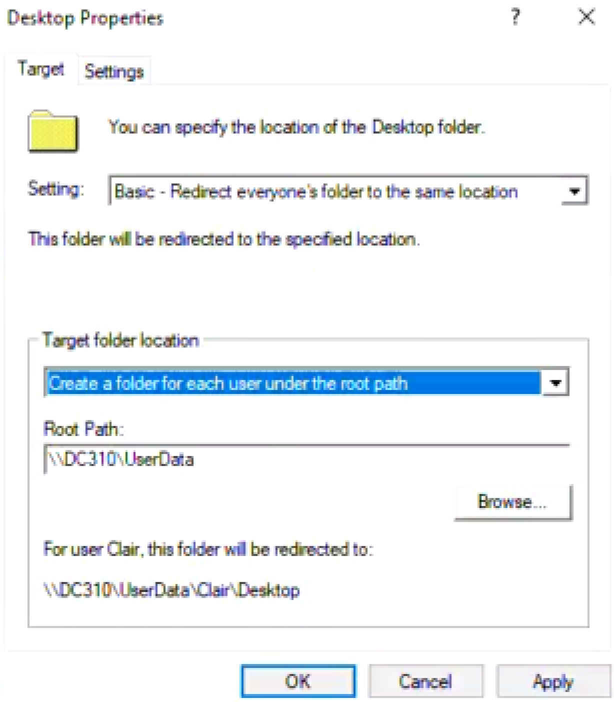




- Redirect Documents and Desktop to the user's respective folder under \\DC3XX\UserData.



Folder Redirection
- AppData(Roamir
- Desktop
- Start Menu
- Documents



Desktop Properties

You can specify the location of the Desktop folder.

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

This folder will be redirected to the specified location.

Target folder location

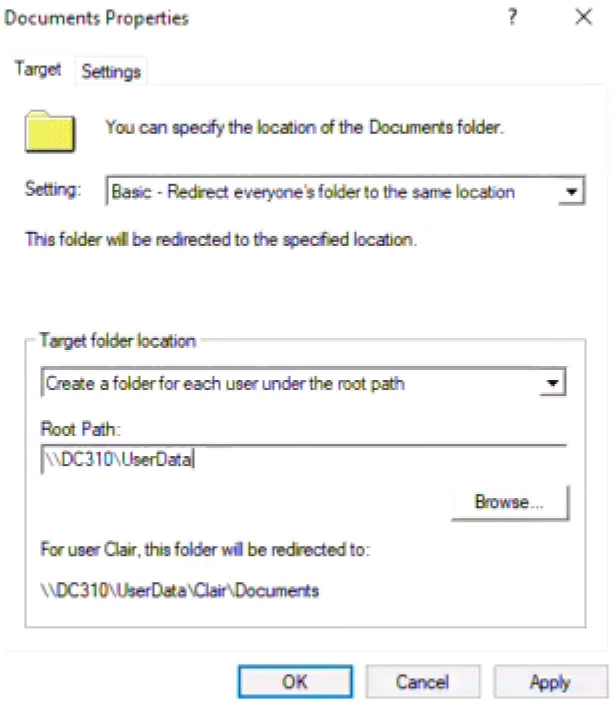
Create a folder for each user under the root path

Root Path:

\\DC310\UserData

For user Clair, this folder will be redirected to:

\\DC310\UserData\Clair\Desktop



Documents Properties

You can specify the location of the Documents folder.

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

This folder will be redirected to the specified location.

Target folder location

Create a folder for each user under the root path

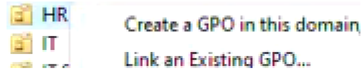
Root Path:

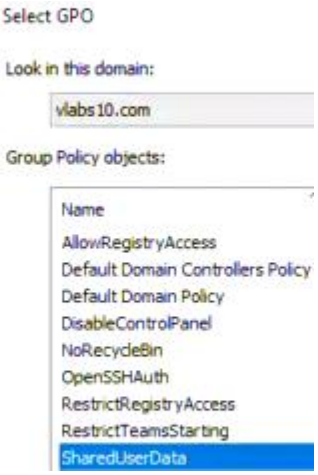
\\DC310\UserData

For user Clair, this folder will be redirected to:

\\DC310\UserData\Clair\Documents

- Link GPO to HR OU




Select GPO

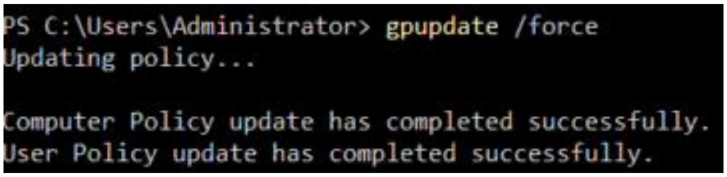
Look in this domain:

vlabs10.com

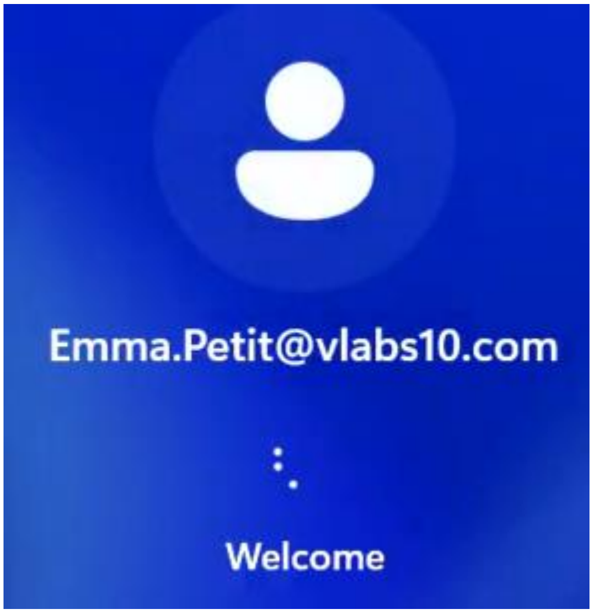
Group Policy objects:

Name
AllowRegistryAccess
Default Domain Controllers Policy
Default Domain Policy
DisableControlPanel
NoRecycleBin
OpenSSHAuth
RestrictRegistryAccess
RestrictTeamsStarting
SharedUserData

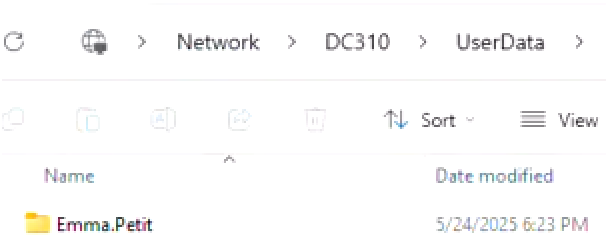
- Run gpupdate /force to apply changes.


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

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

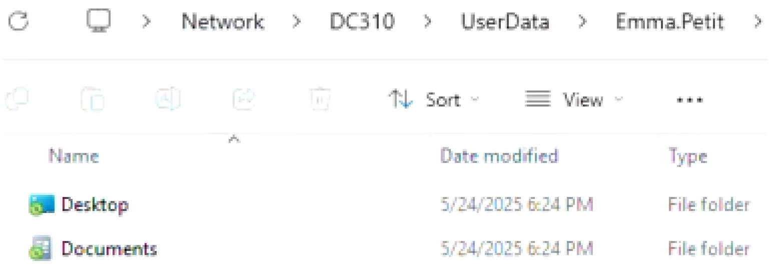
- Test with a user from the HR OU.


Emma.Petit@vlabs10.com

Welcome



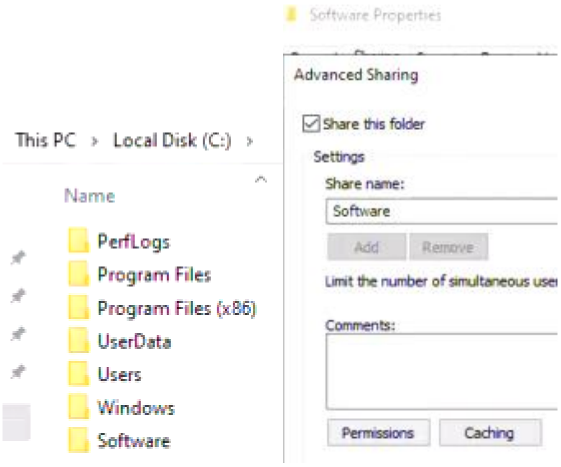
Name	Date modified
Emma.Petit	5/24/2025 6:23 PM



Name	Date modified	Type
Desktop	5/24/2025 6:24 PM	File folder
Documents	5/24/2025 6:24 PM	File folder

Task 8: Managing Software Installation

- Create a network share: \\DC3XX\Software.



Name
PerfLogs
Program Files
Program Files (x86)
UserData
Users
Windows
Software

Advanced Sharing

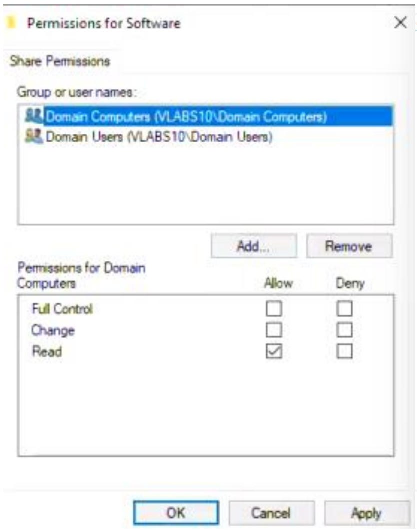
☑ Share this folder

Settings

Share name: Software

Limit the number of simultaneous use

Comments:



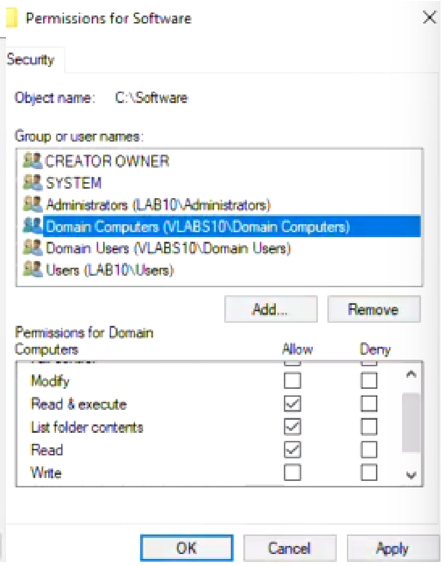
Permissions for Software

Share Permissions

Group or user names:

- Domain Computers (VLABS10\Domain Computers)
- Domain Users (VLABS10\Domain Users)

Permissions for Domain Computers	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□



Permissions for Software

Security

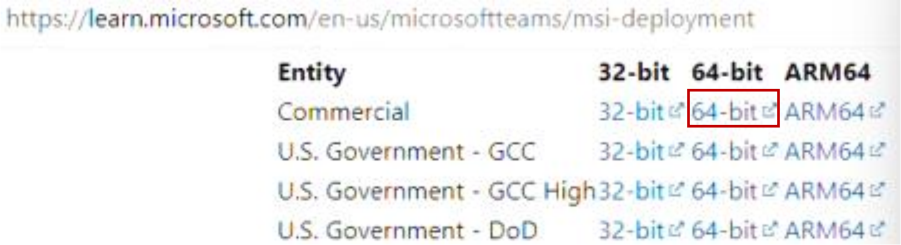
Object name: C:\Software

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (LAB10\Administrators)
- Domain Computers (VLABS10\Domain Computers)
- Domain Users (VLABS10\Domain Users)
- Users (LAB10\Users)

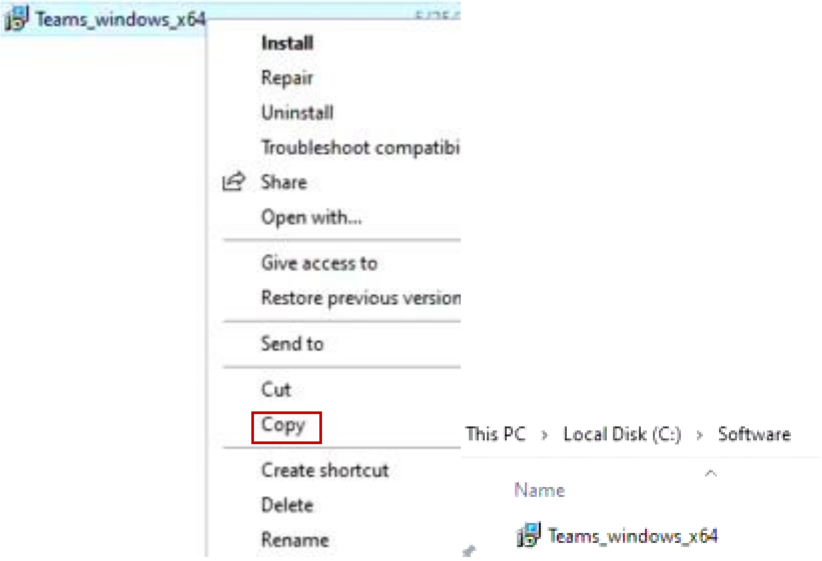
Permissions for Domain Computers	Allow	Deny
Modify	□	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□
Write	□	□

- Download the Microsoft Teams MSI package (You will need to add the NAT NIC to download this package. Remove it after completing the download).

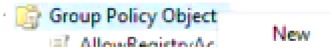


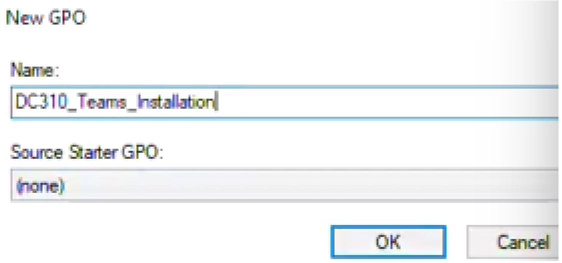
https://learn.microsoft.com/en-us/microsoftteams/msi-deployment

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
U.S. Government - DoD	32-bit	64-bit	ARM64



- Create a new GPO named DC3XX_Teams_Installation.

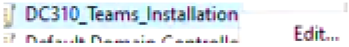


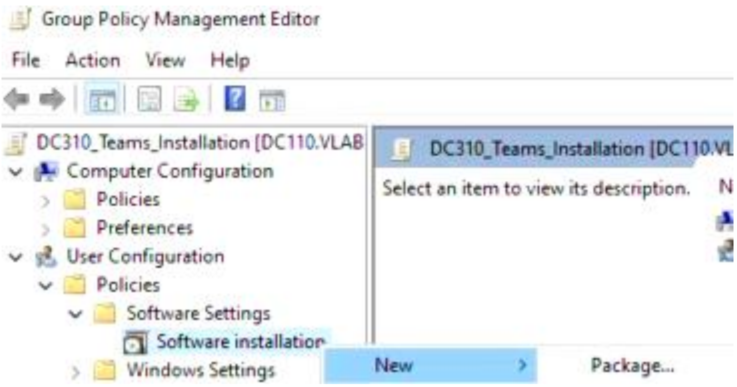


New GPO

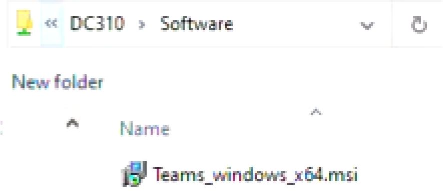
Name: DC310_Teams_Installation

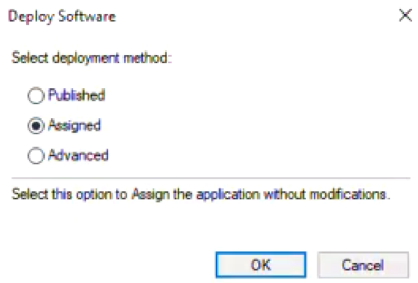
Source Starter GPO: (none)





Select an item to view its description.





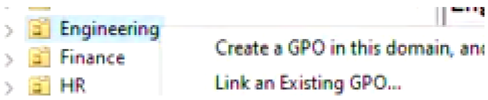
Deploy Software

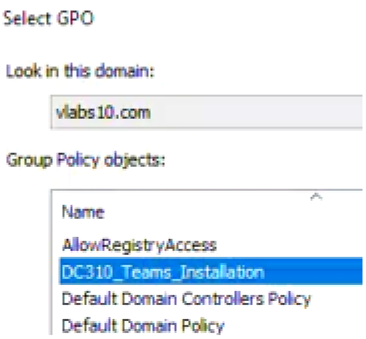
Select deployment method:

○ Published
● Assigned
○ Advanced

Select this option to Assign the application without modifications.

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





Select GPO

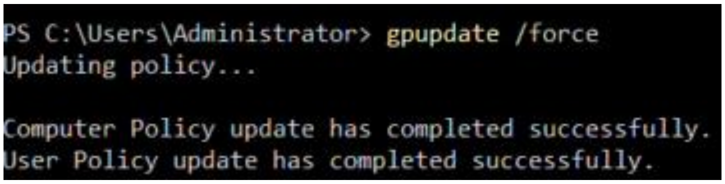
Look in this domain:

vlabs10.com

Group Policy objects:

Name
AllowRegistryAccess
DC310_Teams_Installation
Default Domain Controllers Policy
Default Domain Policy

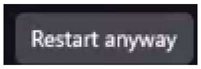
- Run gpupdate /force to apply changes.



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

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

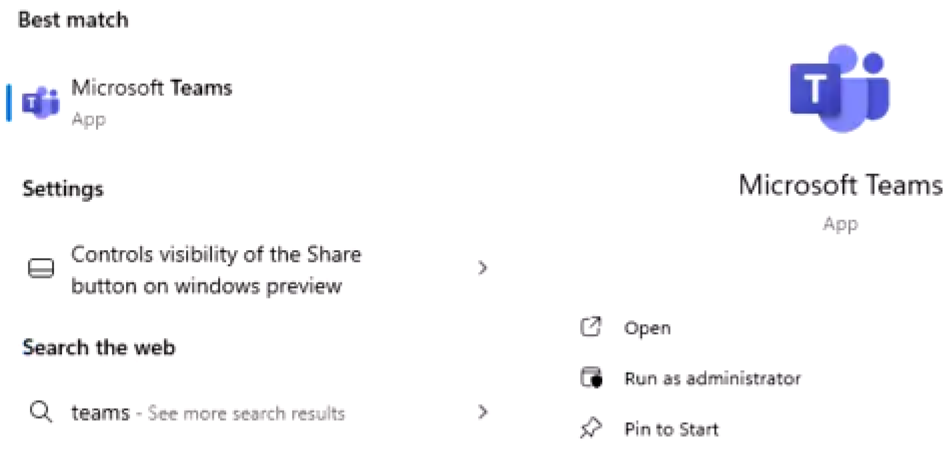
- Restart ClientX, log in with a user from Engineering OU, and verify that Microsoft Teams is installed.

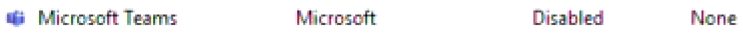
Client10



Agathe.Bonnet

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

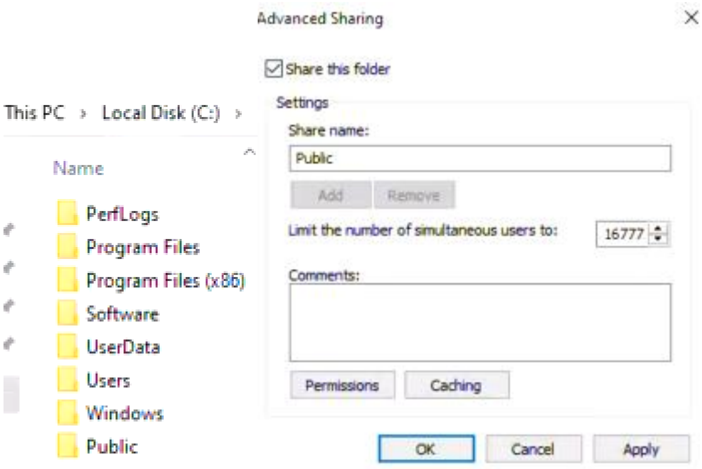




Microsoft Teams	Microsoft	Disabled	None

Task 9: Managing Scripts with GPO

- Create a shared folder on \\DC3XX\Public and share it with Everyone (read and write).



This PC › Local Disk (C:) ›

Name

PerfLogs
Program Files
Program Files (x86)
Software
UserData
Users
Windows
Public

Advanced Sharing

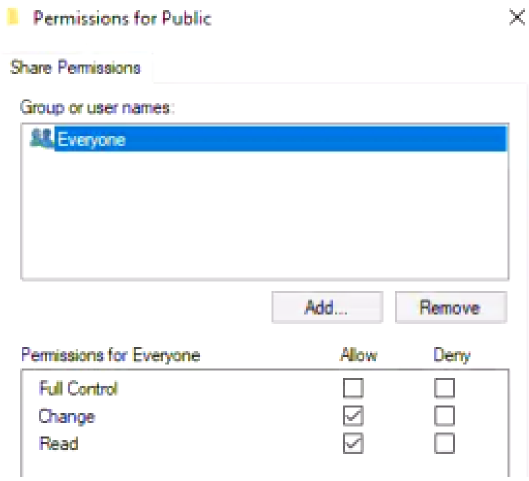
☑ Share this folder

Settings

Share name: Public

Limit the number of simultaneous users to: 16777

Comments:



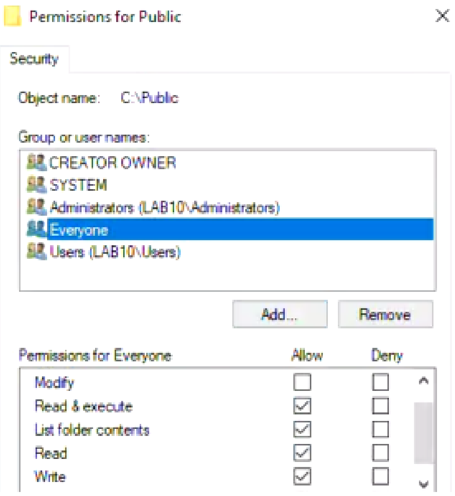
Permissions for Public

Share Permissions

Group or user names:

Everyone

Permissions for Everyone	Allow	Deny
Full Control	□	□
Change	☑	□
Read	☑	□



Permissions for Public

Security

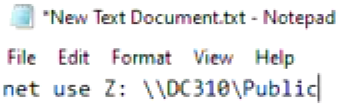
Object name: C:\Public

Group or user names:

CREATOR OWNER
SYSTEM
Administrators (LAB10\Administrators)
Everyone
Users (LAB10\Users)

Permissions for Everyone	Allow	Deny
Modify	□	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□
Write	☑	□

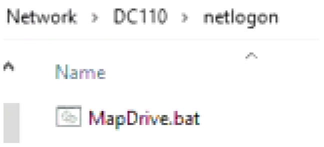
- Create a logon script (MapDrive.bat) to map this shared network drive. Add this text in this file: net use Z: \\DC3XX\Public



*New Text Document.txt - Notepad

```
net use Z: \\DC310\Public
```

- Store the script in \\DC1XX\NETLOGON.

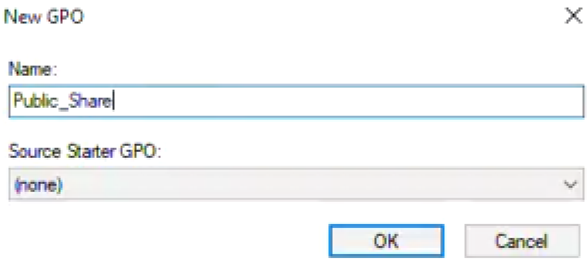


Network › DC110 › netlogon

Name

MapDrive.bat

- Create a new GPO named Public_Share.

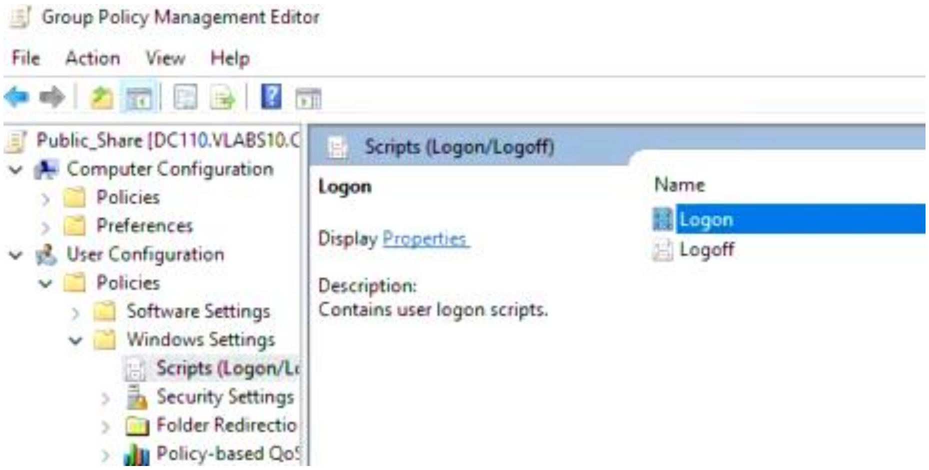


New GPO

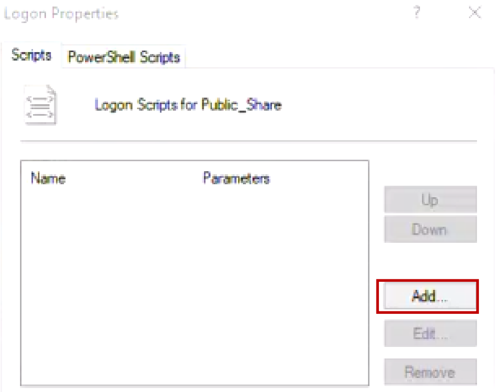
Name: Public_Share

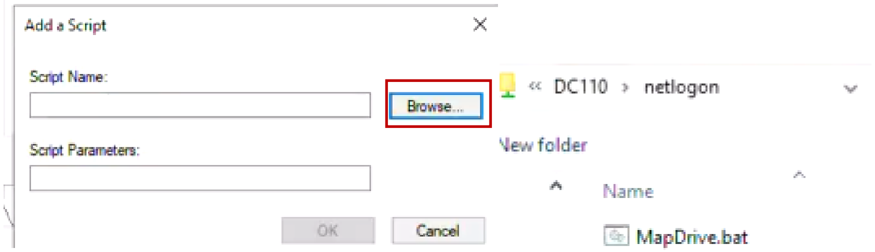
Source Starter GPO: (none)

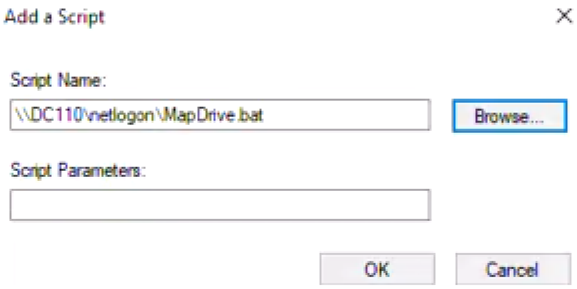
- Add this new logon script to User Configuration Scripts → Logon.



Description:
Contains user logon scripts.



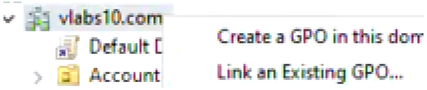


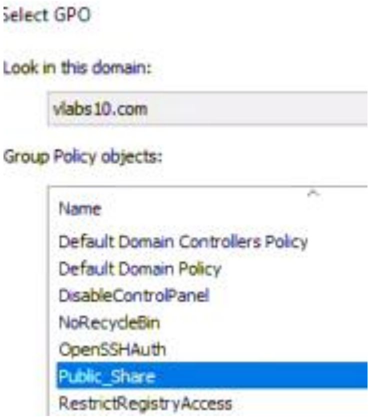


Script Name: \\DC110\netlogon\MapDrive.bat

Script Parameters:

- Link GPO to the Domain.



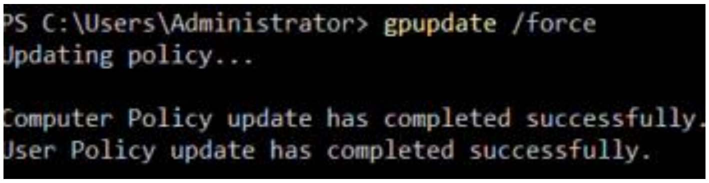


Look in this domain: vlabs10.com

Group Policy objects:

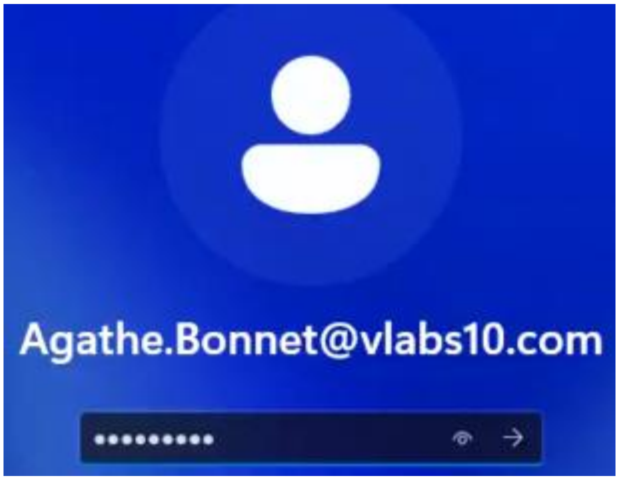
Name
Default Domain Controllers Policy
Default Domain Policy
DisableControlPanel
NoRecycleBin
OpenSSHAuth
Public_Share
RestrictRegistryAccess

- Run gpupdate /force to apply changes.



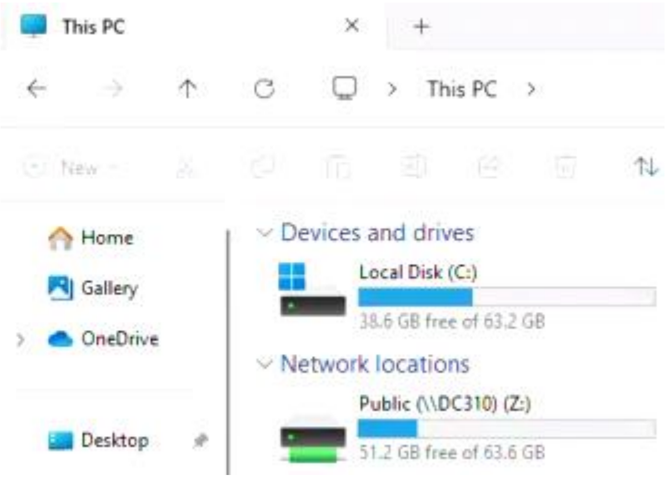
```
PS C:\Users\Administrator> gpupdate /force
Updating policy...

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

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



Agathe.Bonnet@vlabs10.com

••••••••••

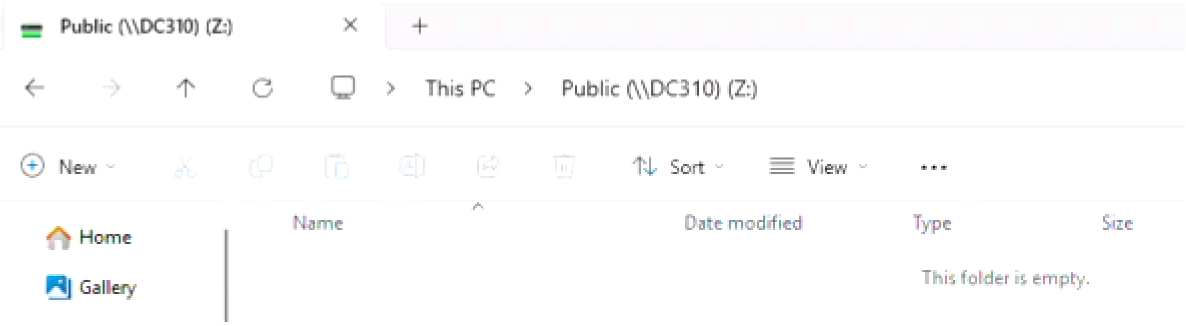


Devices and drives

Local Disk (C:)
38.6 GB free of 63.2 GB

Network locations

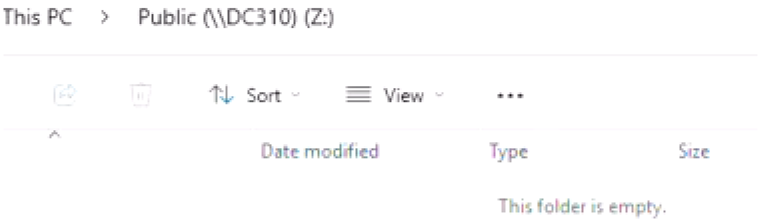
Public (\\DC310) (Z:)
51.2 GB free of 63.6 GB

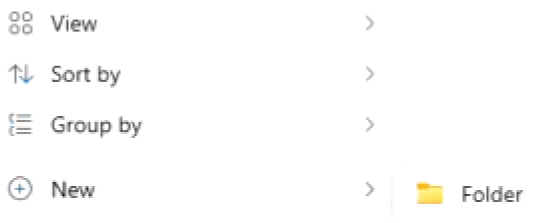


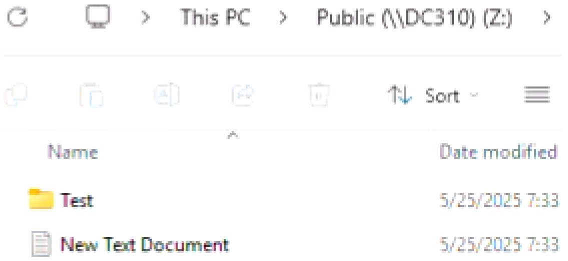
Name	Date modified	Type	Size

This folder is empty.

- Try to create files and folders in this drive.







Name	Date modified
Test	5/25/2025 7:33
New Text Document	5/25/2025 7:33