

System Administration 1

Prepared by Dr. Ahmed Omar

IT391

System Administration 1

Lecture 6



File Servers and Group Policy

Lecture 6

IT391

System Administration 1

Prepared by
Dr. Ahmed Omar



Agenda

- ☐ What is a File Server?
- ☐ File Server Permissions (Access Control)
- ☐ Sharing Folders on a Server
- ☐ Introduction to Group Policy
- ☐ Applying Group Policy

File Server

What is a File Server?

- ☐ A dedicated server (physical or virtual) designed for **storing** and **managing files** and folders.
- ☐ Acts as a **central repository** for an organization's digital data.
- ☐ Accessible by **multiple users** and devices across a network.

File Server

Key Role & Purpose

- ❑ **Centralized Storage:** Provides a single, organized location for all shared documents, projects, and resources.
- ❑ **Data Consistency:** Ensures everyone works on the latest versions of files, reducing confusion and errors.
- ❑ **Enhanced Collaboration:** Facilitates teamwork by allowing multiple users to access and work on shared files.

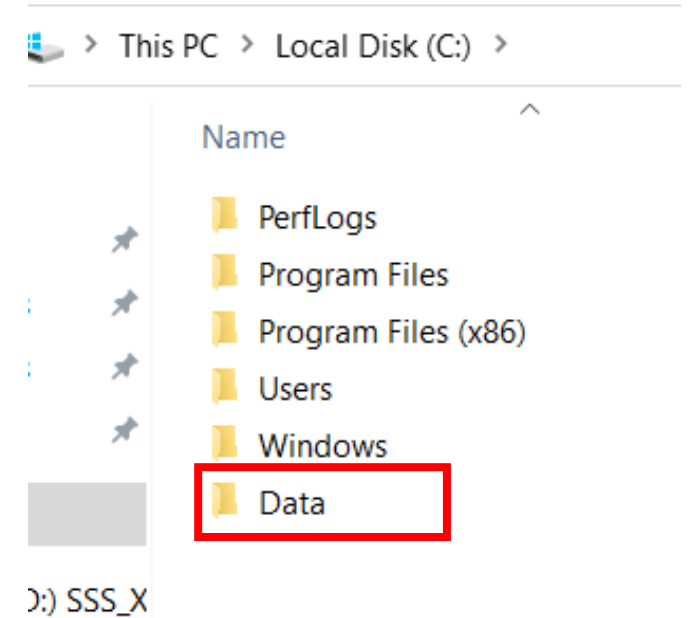
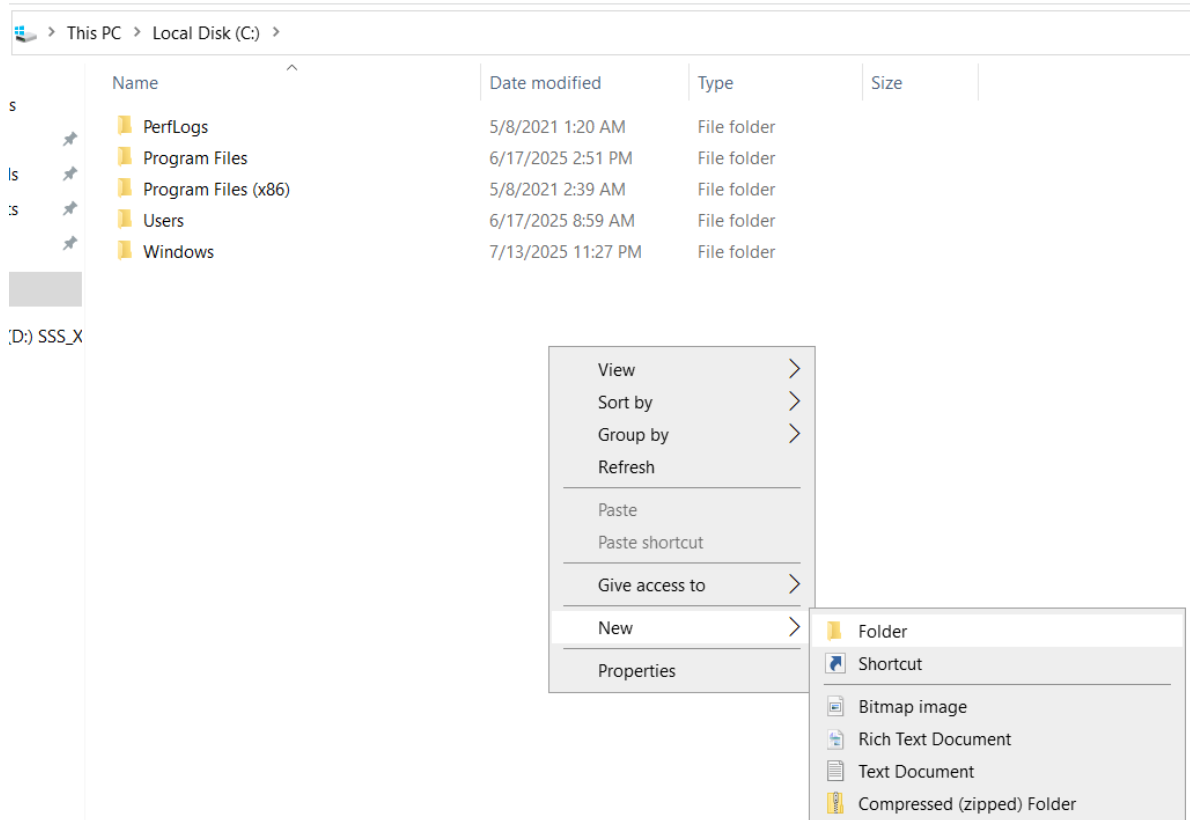
File Server

Core Functions

- ❑ **File Storage:** Houses vast amounts of data, from documents and spreadsheets to media files.
- ❑ **File Sharing:** Allows authorized users to access, read, write, and modify shared content over the network.
- ❑ **Access Control:** Implements robust security permissions (NTFS and Share permissions) to dictate who can access what.
- ❑ **Data Management:** Supports features like quotas, auditing, and data deduplication.

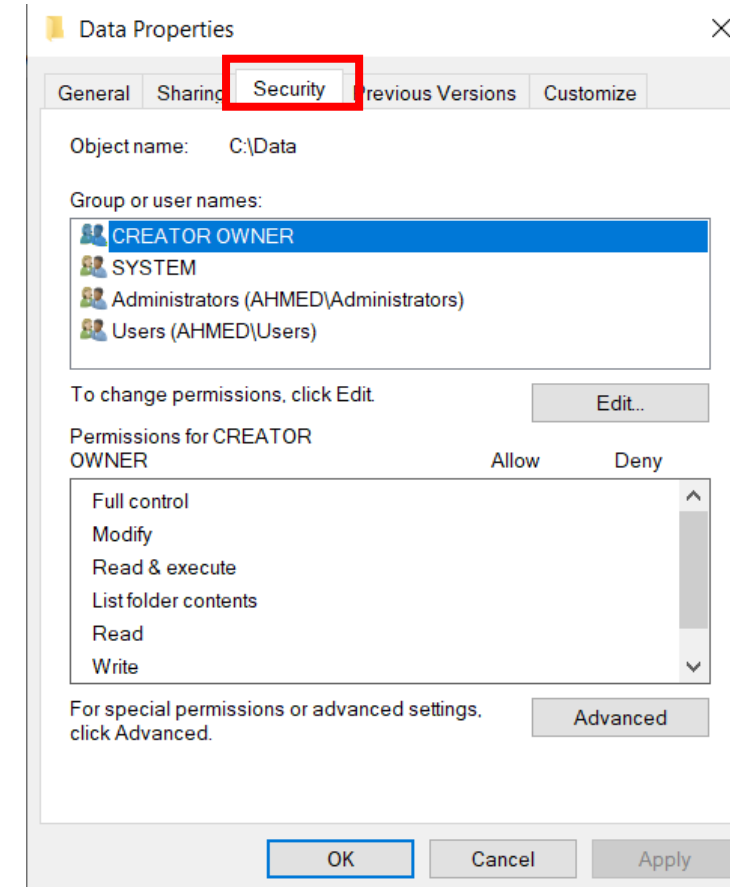
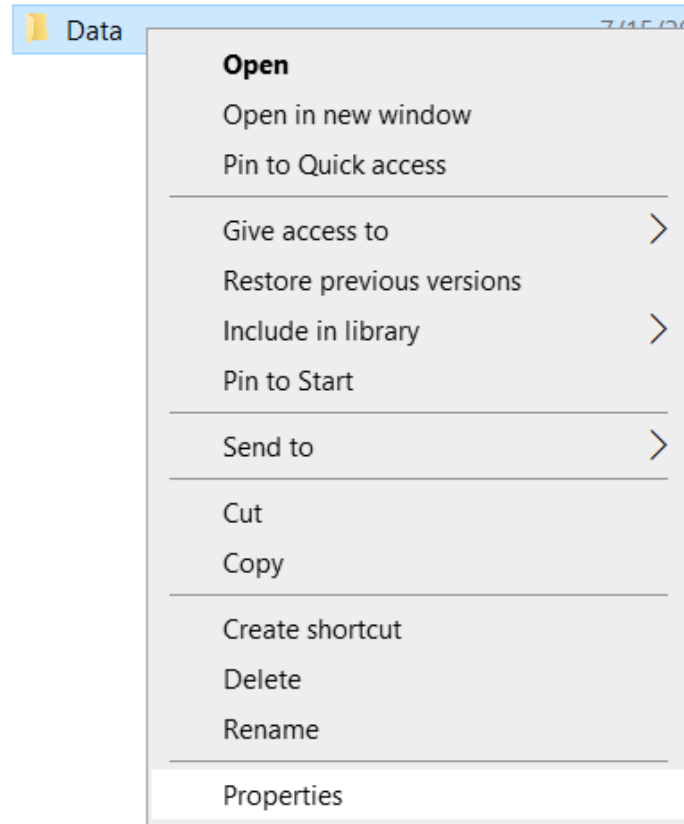
File Server

Create Folder in Client ([Login as Administrator](#))



File Server

Security tap : access from the same machine



File Server

This is a critical security aspect. File servers implement robust mechanisms to control who can do what with shared data. This involves:

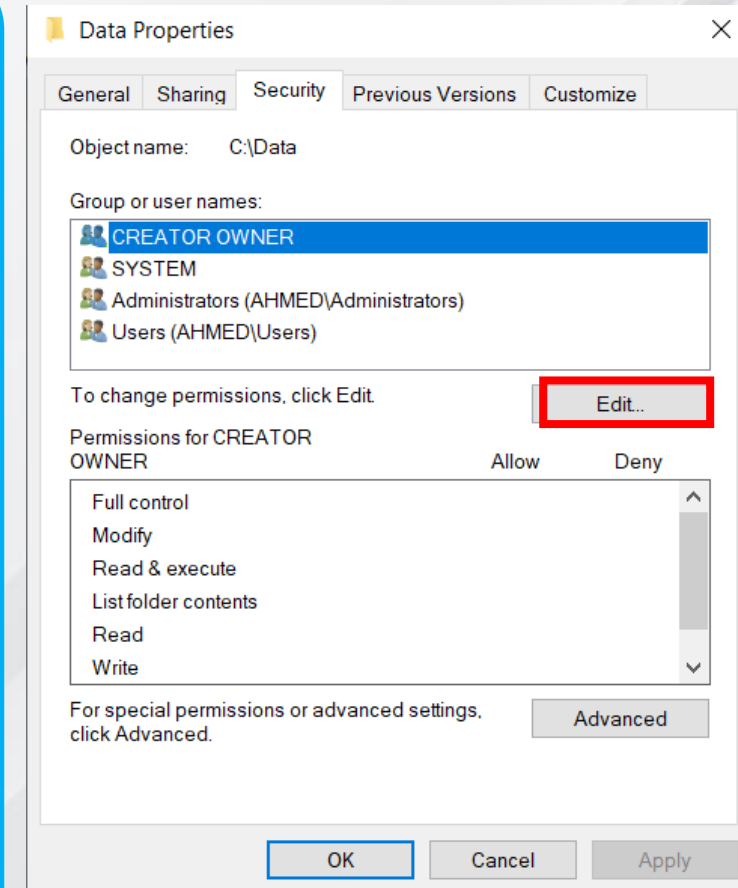
"Full control," "Modify," "Read & execute,"

"List folder contents," "Read," and "Write"

for different user or group names (like

"CREATOR OWNER," "SYSTEM,"

"Administrators," and "Users").



File Server Permissions

- ❑ **Full control:** Grants complete access to a file or folder, including the ability to read, write, modify, delete, and change permissions or take ownership.
- ❑ **Modify:** Allows users to read, write, and delete files or folders, and to change attributes or execute files.
- ❑ **Read & execute:** Permits viewing a file's contents, running executable files, and navigating through folders.
- ❑ **List folder contents:** Specifically allows **viewing** the names of files and subfolders within a directory, but does not grant access to the contents of those files or subfolders unless other permissions are present.
- ❑ **Read:** Grants permission to view the contents of a file or folder, including attributes and permissions, but not to make changes.
- ❑ **Write:** Enables users to create new files and folders, write data to existing files, and change file attributes.

File Server

Click Edit and Add/Remove permission
Or Add User

Permissions for Data

Security

Object name: C:\Data

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (AHMED\Administrators)
- Users (AHMED\Users)

Add... Remove

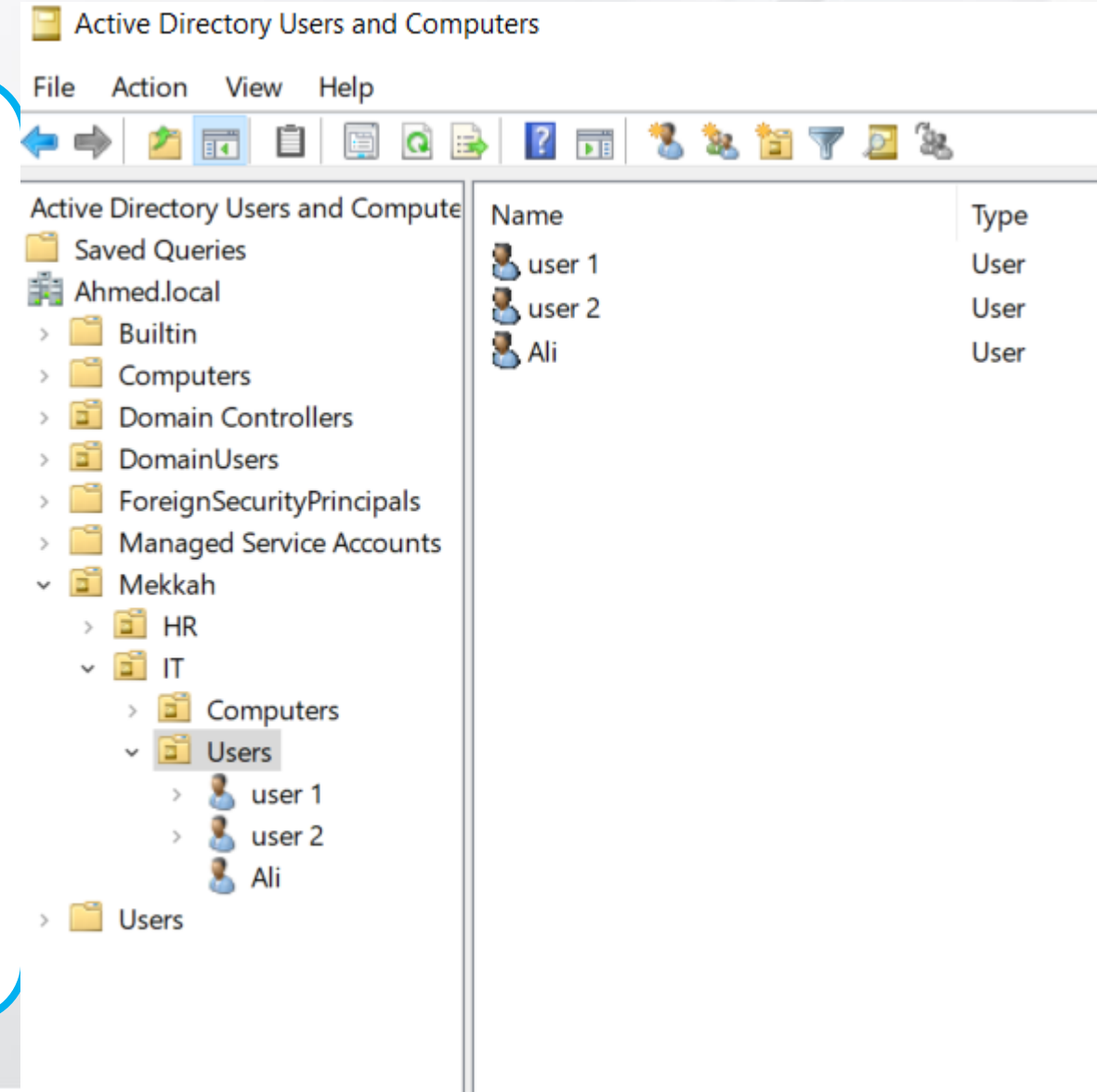
Permissions for CREATOR OWNER

	Allow	Deny
Full control	☐	☐
Modify	☐	☐
Read & execute	☐	☐
List folder contents	☐	☐
Read	☐	☐

OK Cancel Apply

File Server

Form Active Directory Users And Computers
see/ add **users**



File Server

Write username then click **Check Names**

Select Users, Computers, Service Accounts, or Groups

Select this object type:
Users, Groups, or Built-in security principals

From this location:
Ahmed.local

Enter the object names to select (examples):
Ali

Check Names

Advanced... OK Cancel



Select Users, Computers, Service Accounts, or Groups

Select this object type:
Users, Groups, or Built-in security principals

From this location:
Ahmed.local

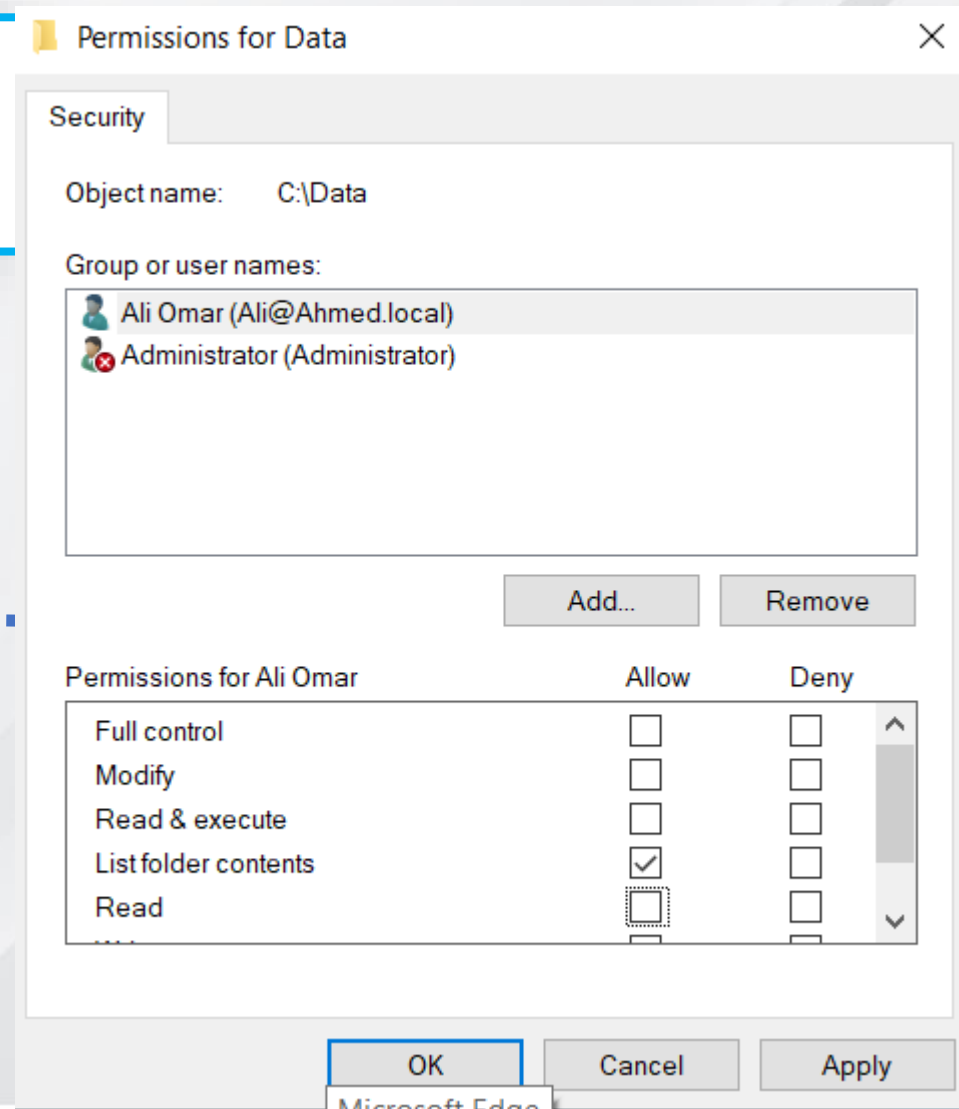
Enter the object names to select (examples):
Ali (Ali@Ahmed.local)

Check Names

Advanced... OK Cancel

File Server

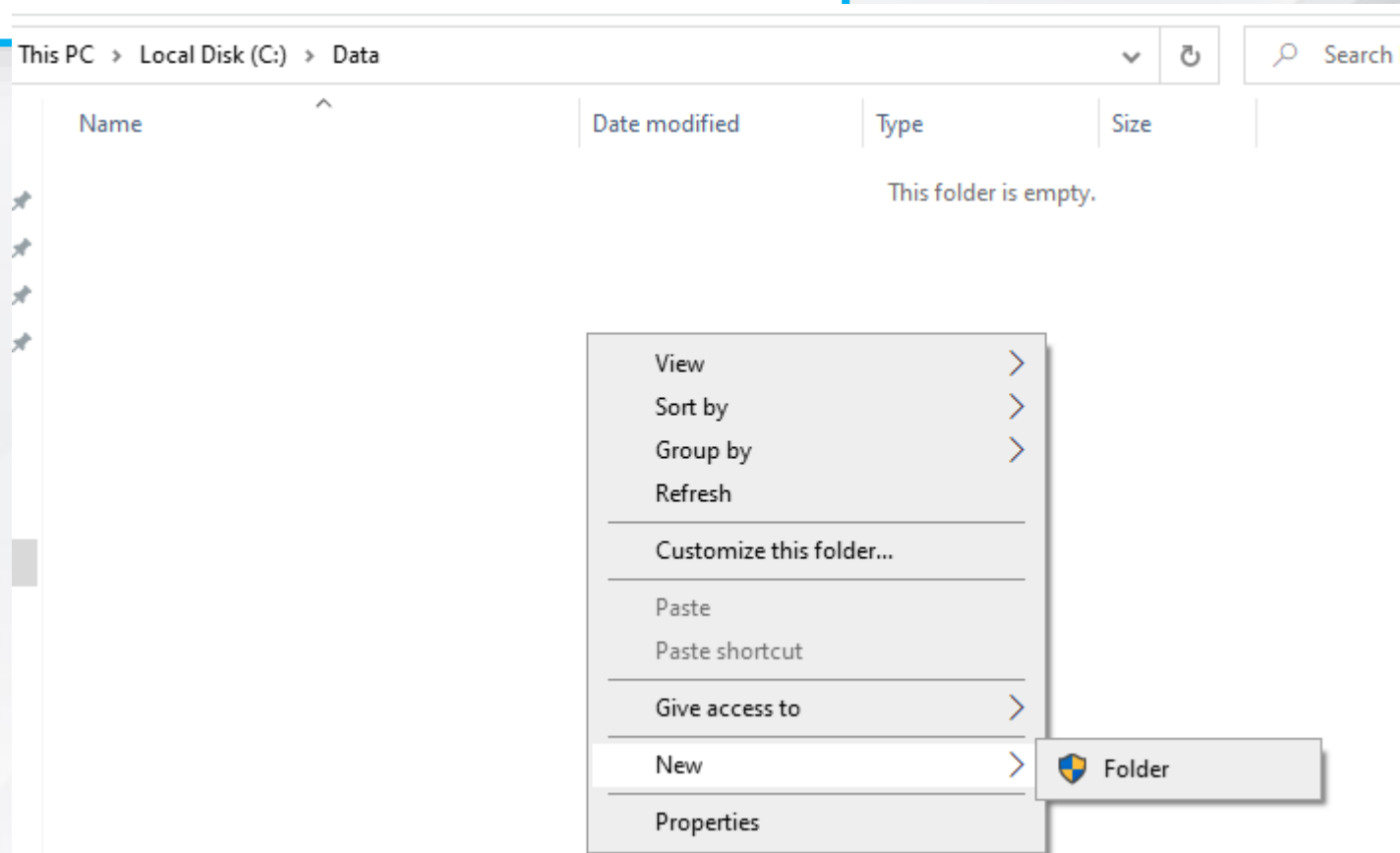
Select The required permissions



File Server

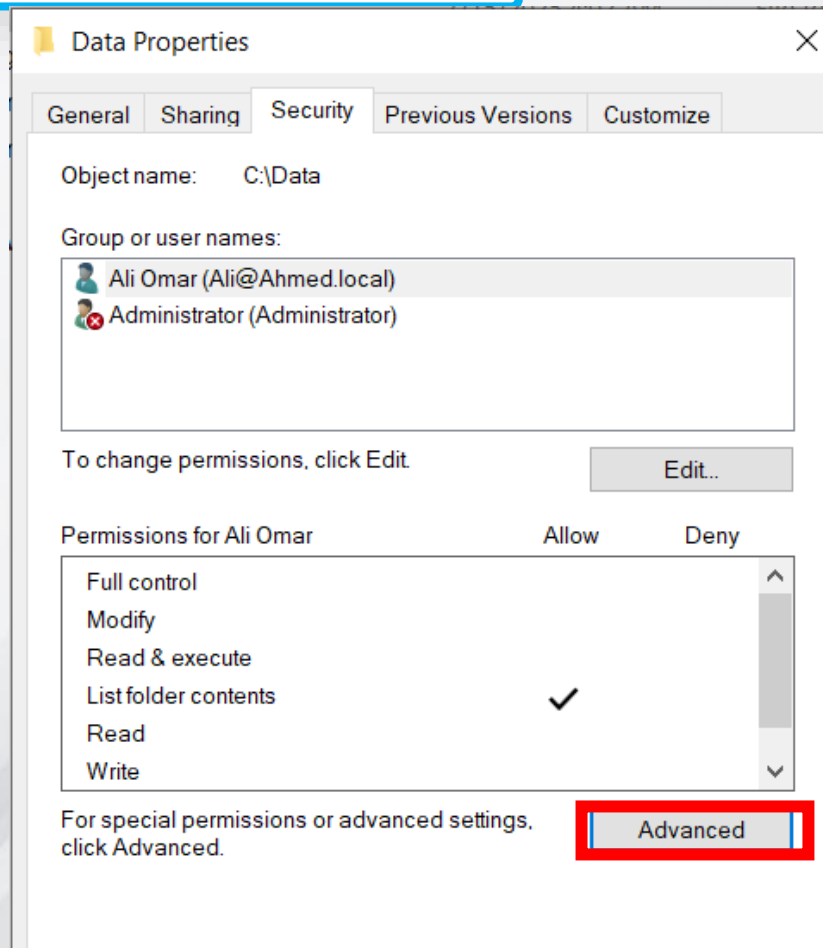
Trying create new Folder (Log in as Ali)

Not Allowed



File Server

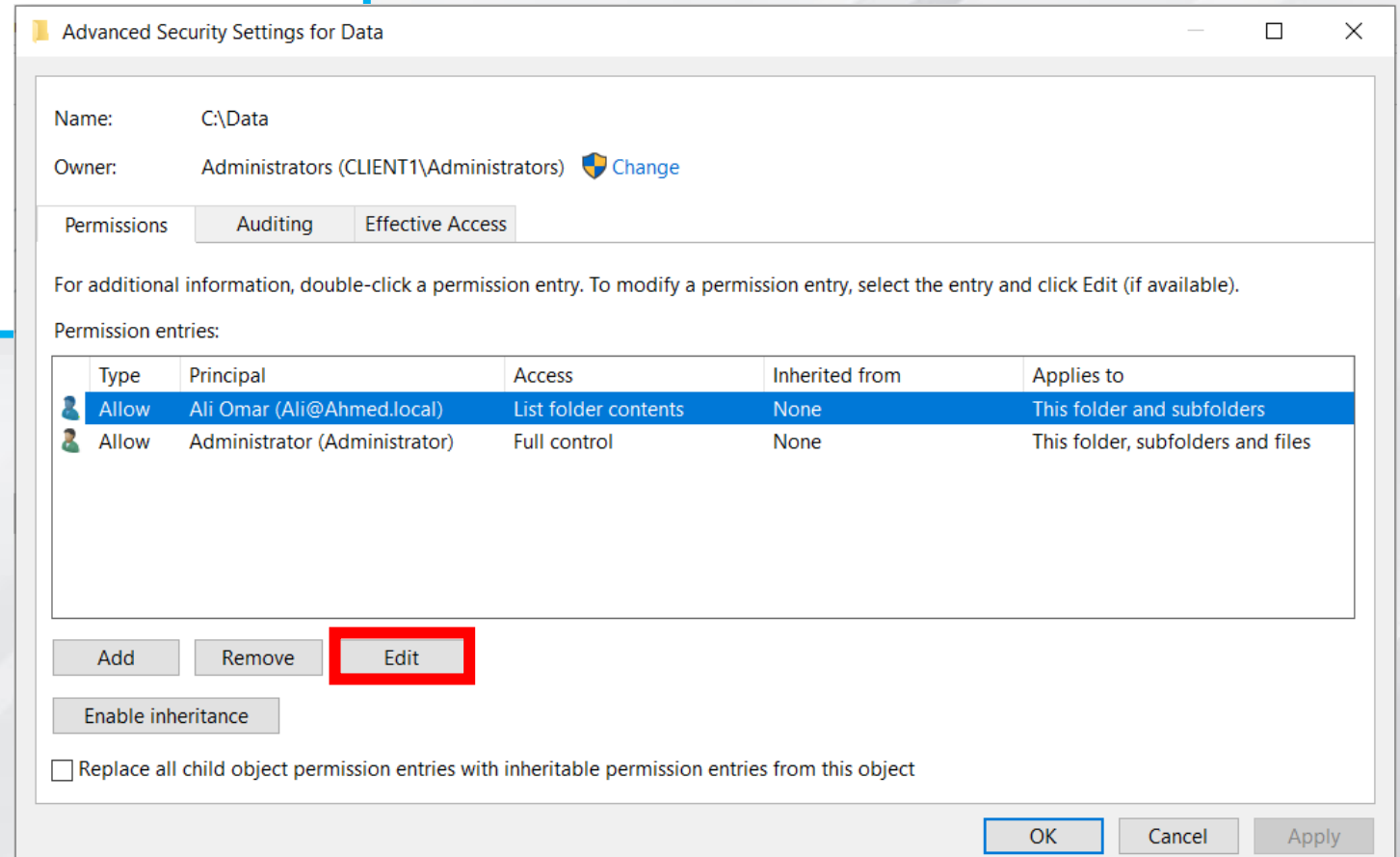
More Advanced Permissions



File Server

More Advanced Permissions

Select user and Click **Edit**



File Server

More Advanced Permissions

Click :

Show advanced permissions

Permission Entry for Data

Principal: Ali Omar (Ali@Ahmed.local) [Select a principal](#)

Type: Allow

Applies to: This folder and subfolders

Basic permissions:

- ☐ Full control
- ☐ Modify
- ☒ Read & execute
- ☒ List folder contents
- ☒ Read
- ☐ Write
- ☐ Special permissions

☐ Only apply these permissions to objects and/or containers within this container

[Show advanced permissions](#)

[Clear all](#)

Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

[Add a condition](#)

OK Cancel

File Server

More Advanced Permissions

Permission Entry for Data

Principal: Ali Omar (Ali@Ahmed.local) [Select a principal](#)

Type: Allow

Applies to: This folder and subfolders

Advanced permissions:

☐ Full control	☐ Write attributes
☒ Traverse folder / execute file	☐ Write extended attributes
☒ List folder / read data	☐ Delete subfolders and files
☒ Read attributes	☐ Delete
☒ Read extended attributes	☒ Read permissions
☐ Create files / write data	☐ Change permissions
☐ Create folders / append data	☐ Take ownership

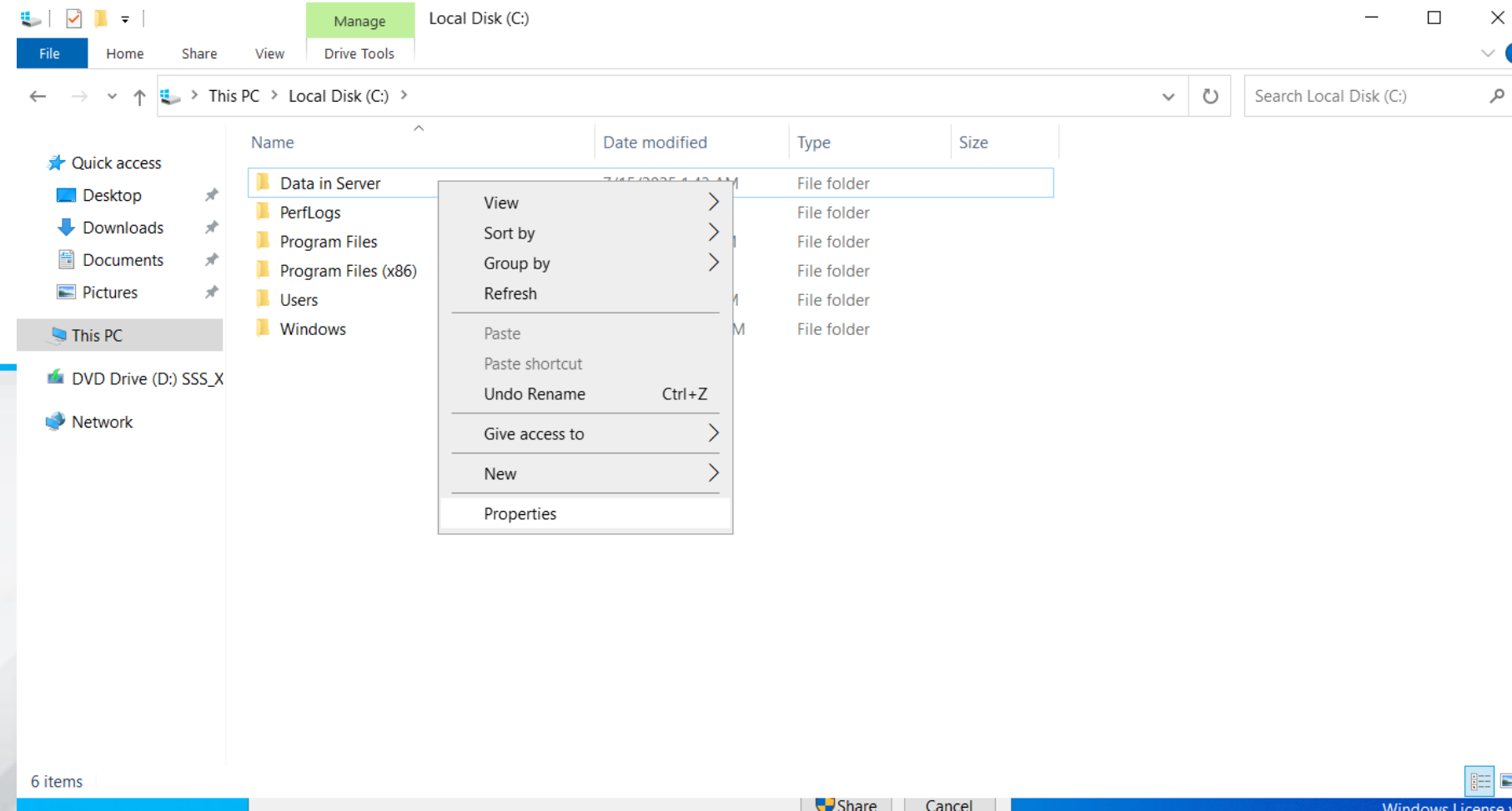
☐ Only apply these permissions to objects and/or containers within this container

[Show basic permissions](#)

[Clear all](#)

File Server

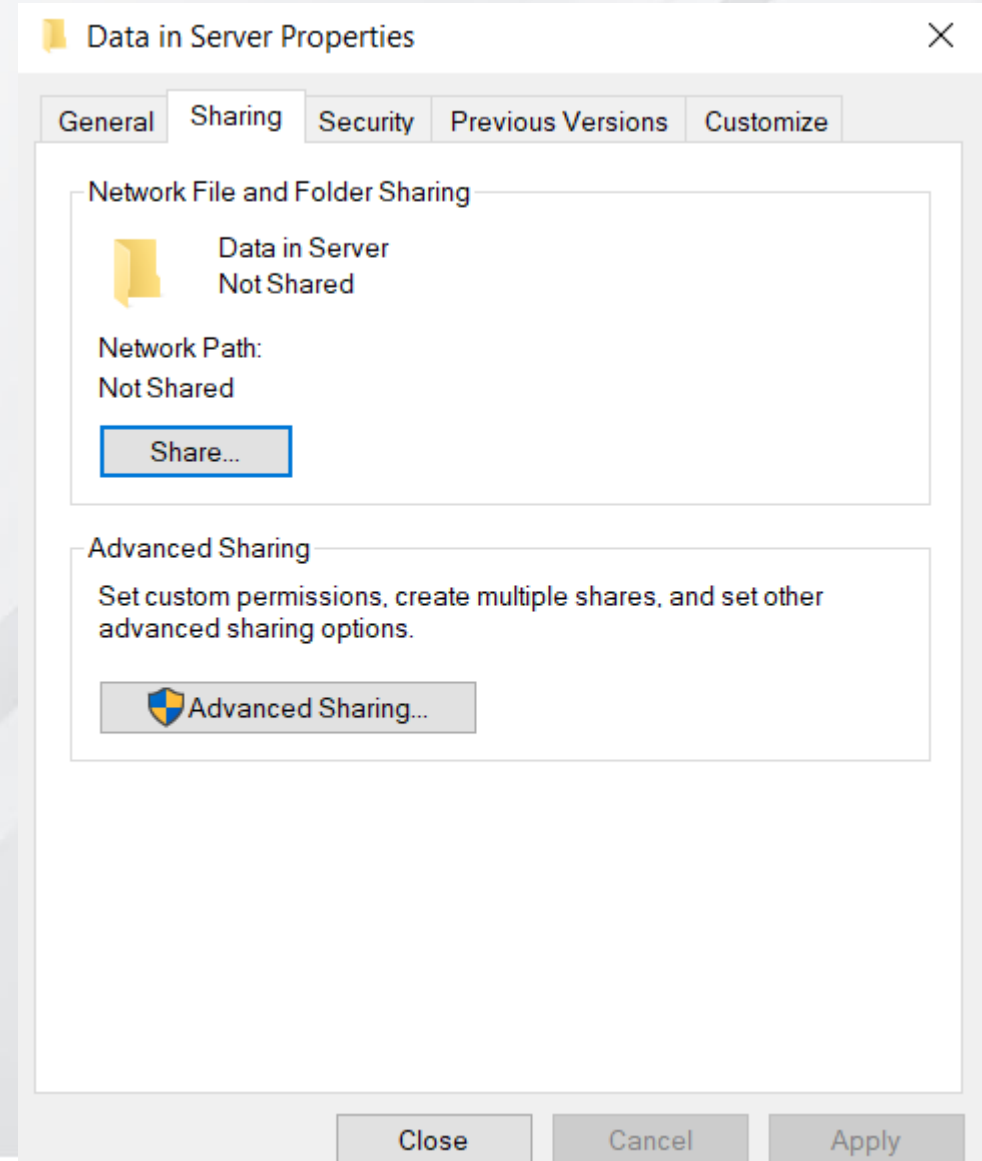
Share Folder on Server
Only Admin can share



File Server

Share Folder on Server

Click **Advanced Sharing**



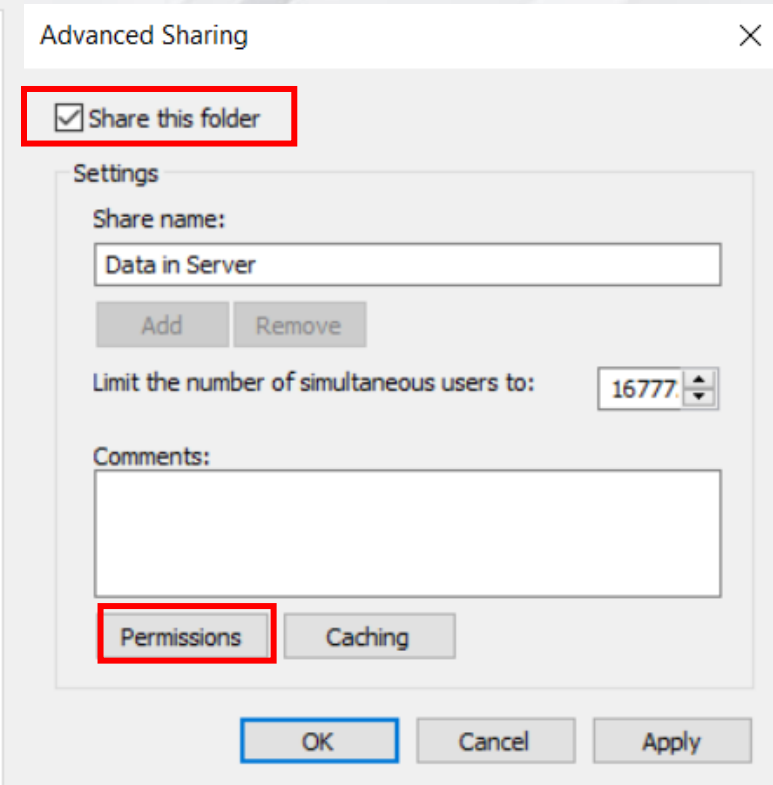
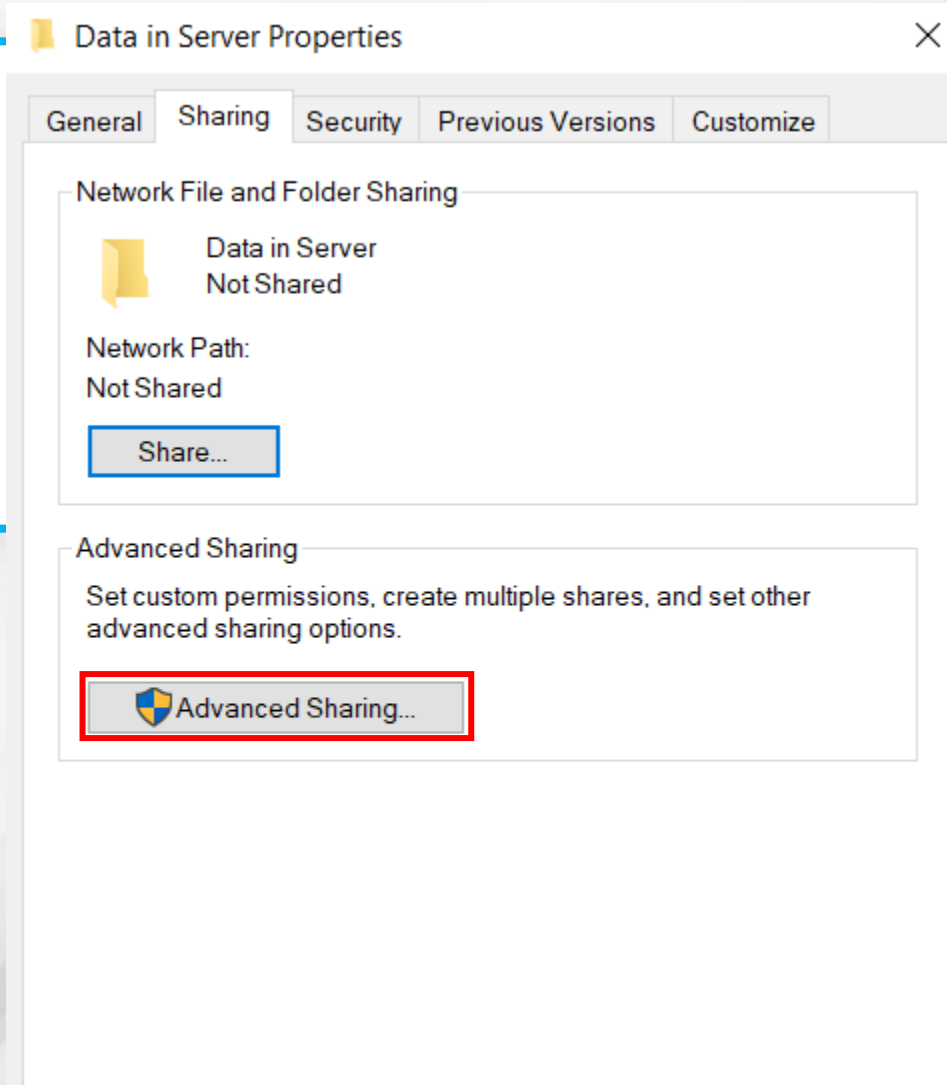
File Server

Share Folder on Server

Click **Advanced Sharing**

Check **Share this folder**

Click **Permissions**



File Server

Share Folder on Server

Everyone is allowed to read

Click **Add**

Add user

Data in Server Properties

Permissions for Data in Server

Share Permissions

Group or user names:

Everyone

Add... Remove

Permissions for Everyone	Allow	Deny
Full Control	☐	☐
Change	☐	☐
Read	☒	☐

Select Users, Computers, Service Accounts, or Groups

Select this object type:

Users, Groups, or Built-in security principals

Object Types...

From this location:

Ahmed.local

Locations...

Enter the object names to select (examples):

Ali (Ali@Ahmed.local)

Check Names

Advanced... OK Cancel

File Server

Share Folder on Server

Add permission to Ali

Data in Server Properties

Permissions for Data in Server

Share Permissions

Group or user names:

Ali (Ali@Ahmed.local)

Everyone

Add...
Remove

Permissions for Ali

	Allow	Deny
Full Control	☐	☐
Change	☒	☐
Read	☒	☐

OK
Cancel
Apply

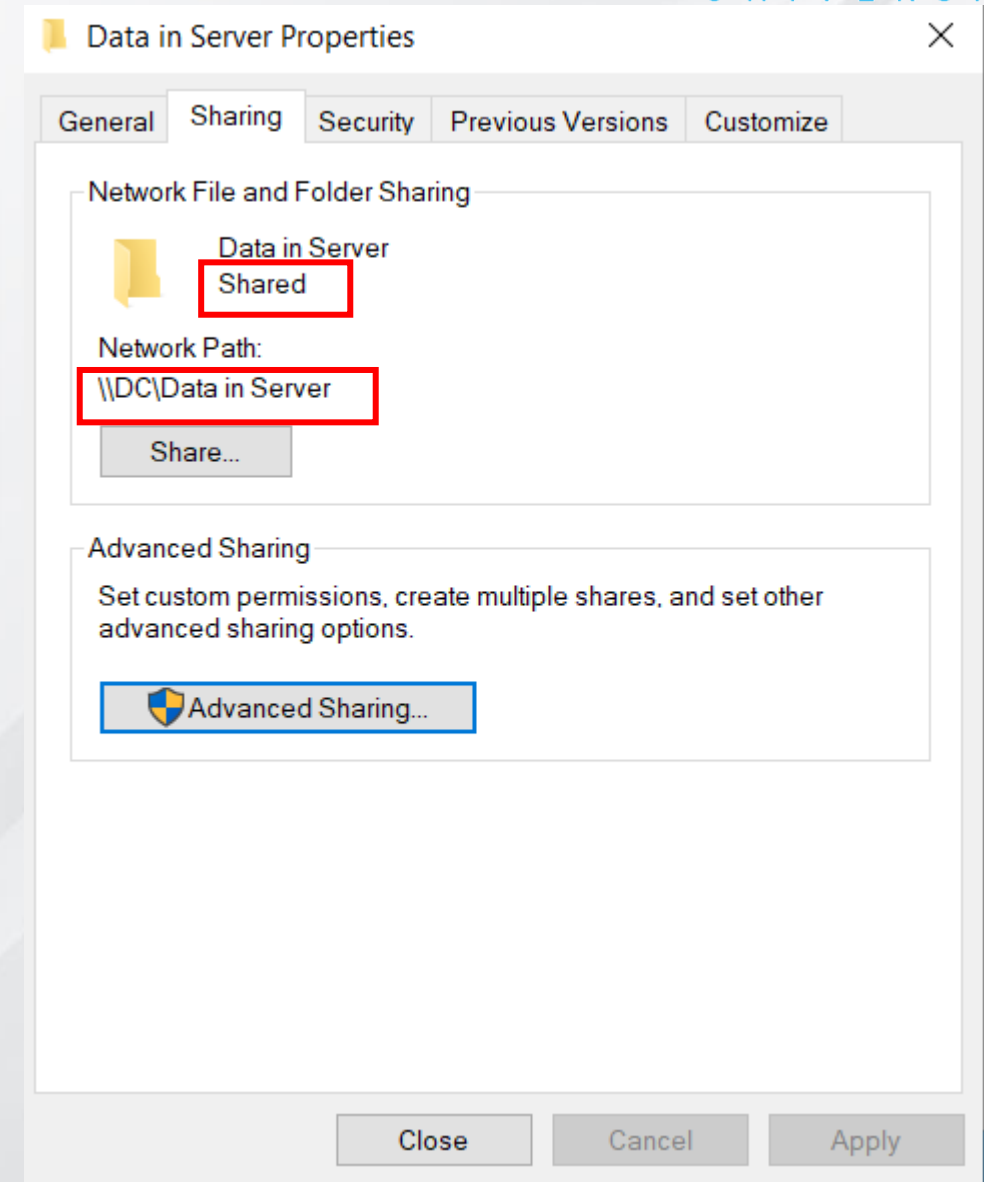
File Server

Share Folder on Server

The folder become Shared

In the Network path

\\DC\Data in Server



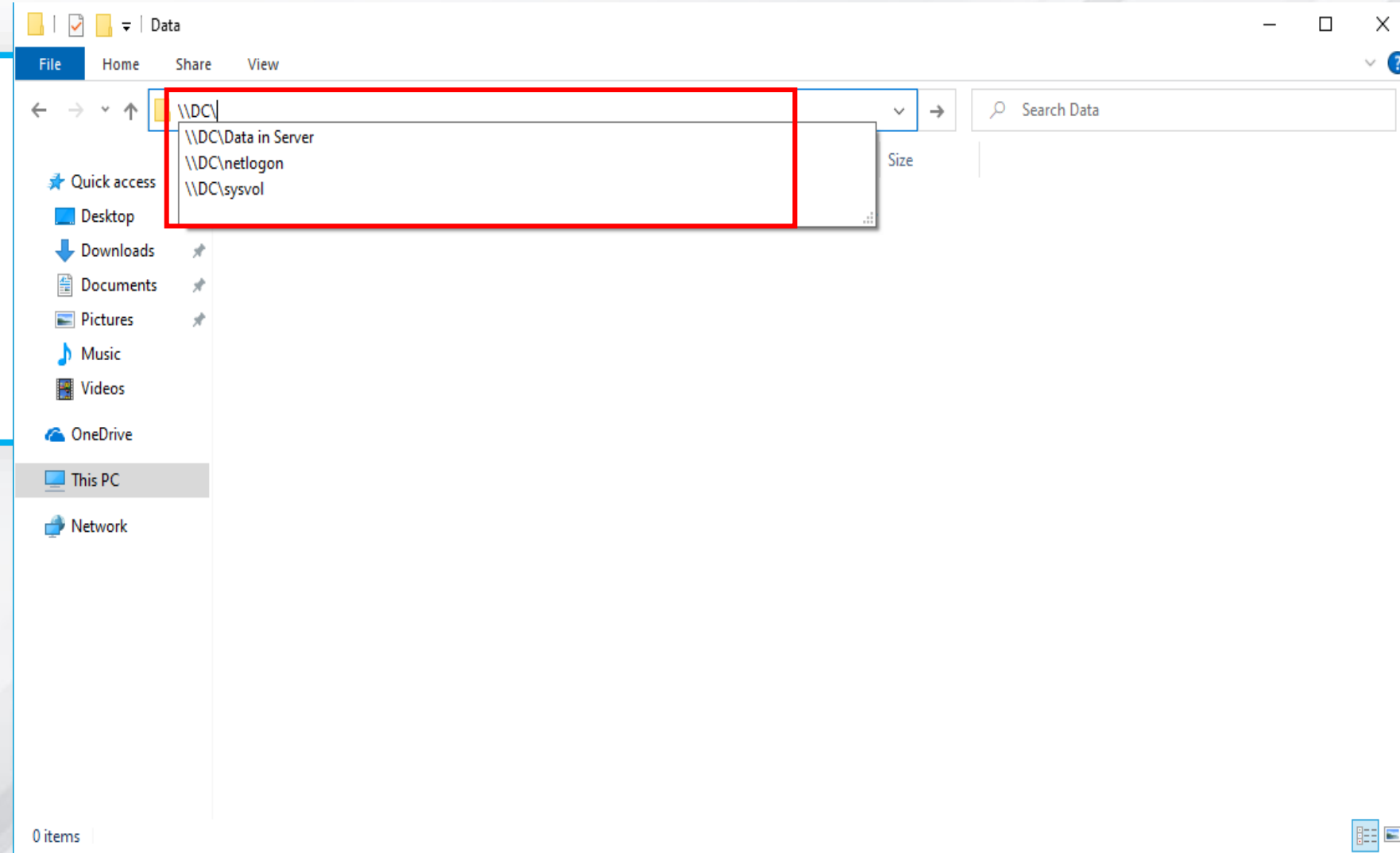
File Server

Open Client as Ali

Open File Explorer

Write

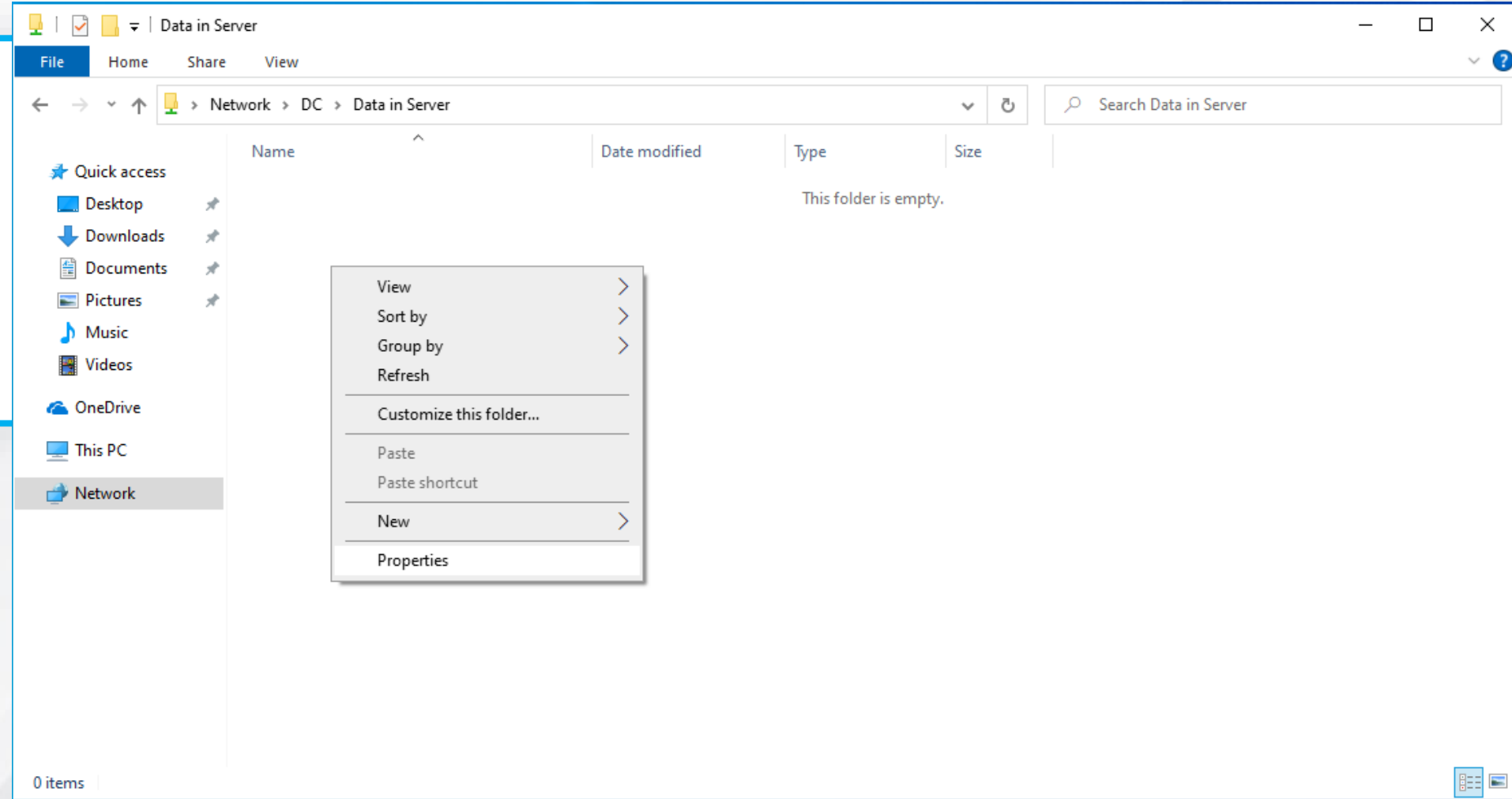
`\\DC\Data in Server`



File Server

Open Client as Ali

Open the shared Folder



Introduction to Group Policy

What is Group Policy?

- ☐ A cornerstone feature in Microsoft Windows operating systems.
- ☐ Provides a robust framework for centrally managing and securing user and computer settings across an Active Directory (AD) environment.
- ☐ Purpose: Deliver consistent configurations to a multitude of computers and users, streamlining administrative tasks and enforcing organizational policies.
- ☐ Extends to server machines for configuring operational and security settings

Introduction to Group Policy

Group Policy settings are contained within **Group Policy Objects (GPOs)**. A GPO is a collection of policy settings that can be applied to users and computers. These GPOs are linked to Active Directory containers such as sites, domains, or Organizational Units (OUs).

Introduction to Group Policy

Group Policy Objects (GPOs):

- ☐ When integrated with Active Directory, Group Policy settings are encapsulated within a Group Policy Object (**GPO**).
- ☐ A **GPO** is a virtual collection of policy settings, security permissions, and a defined scope of management (SOM).
- ☐ Serves as the logical container for all Group Policy configurations.

Introduction to Group Policy

Configuration Types within GPOs:

- ☐ **Computer settings**: Apply system-wide (e.g., power management, firewall rules); applied at computer startup.
- ☐ **User settings**: Affect only the current user (e.g., Internet Explorer settings, Folder Redirection); applied at user sign-in.

Distinction: Computer settings are enforced regardless of the logged-in user; user settings typically follow the user across machines.

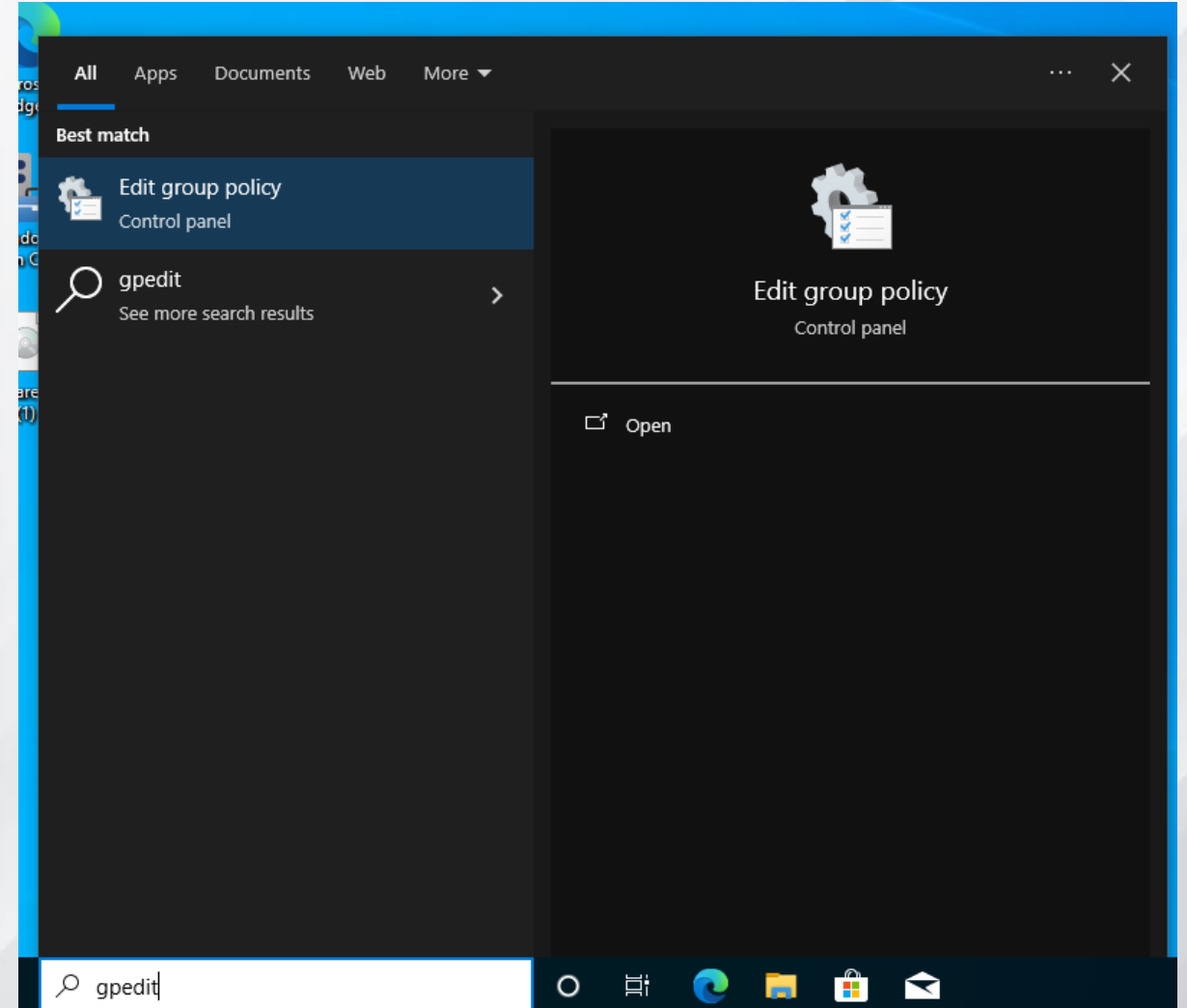
Open Group Policy in Local Computer

- Type **gpedit** in the search bar
- Open **Edit group policy**

- Note Login as Administrator

User name: [Ahmed.local\Administrator](#)

Password : [*****](#)



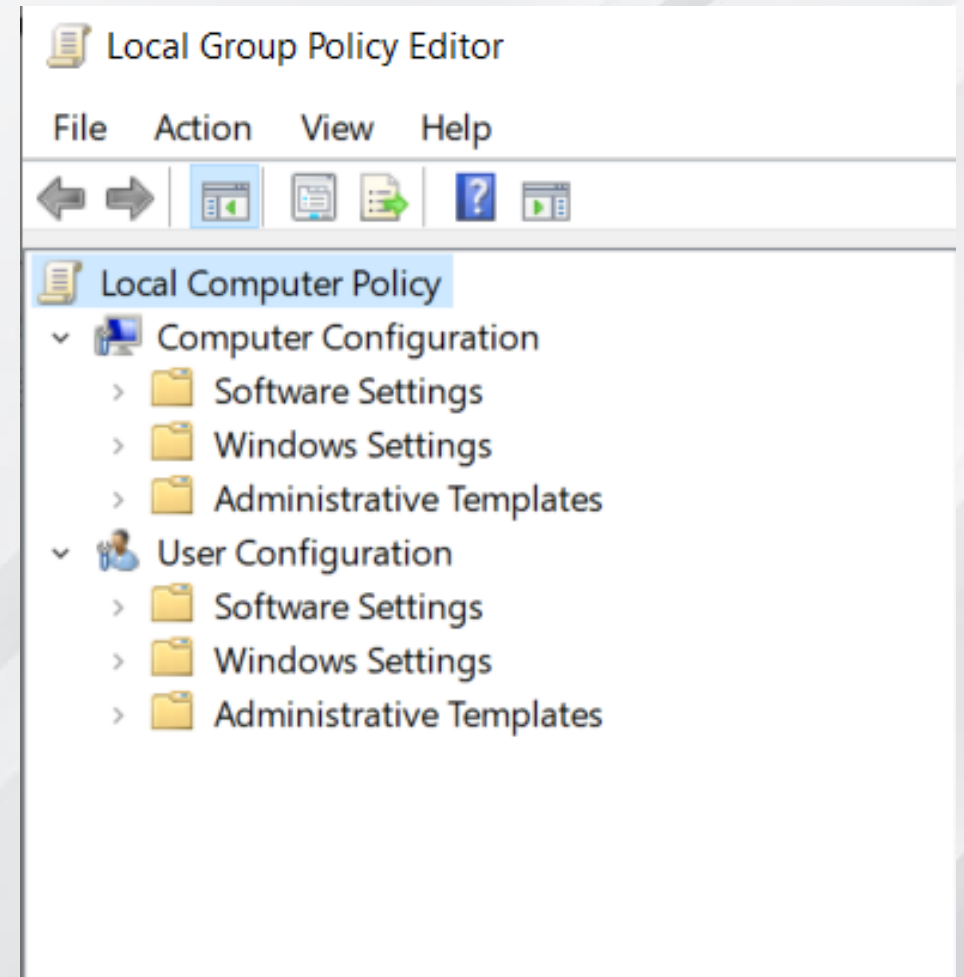
Open Group Policy in Local Computer

The Console Divide into:

- Computer Configuration
- User Configuration

Each one contains:

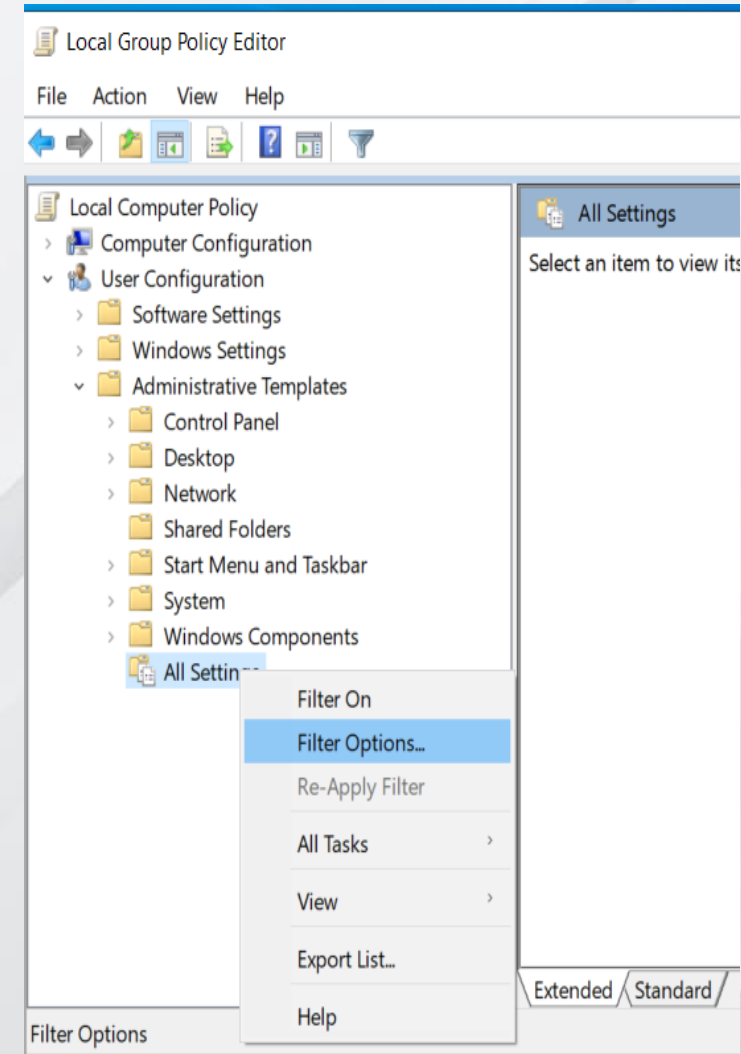
- ☐ Software settings
- ☐ Windows settings
- ☐ Administrative settings



Apply Group Policy in Local Computer

Hide Clock from Taskbar

- Open **All settings** in **User Configuration** → **Administrative settings**
- **Right click** → **Filter Options**



Apply Group Policy in Local Computer

Hide Clock from Taskbar

- Check **Enable Keyword Filters**
- Write the **Word**
- Click **OK**

Filter Options

Select options below to enable and change or disable types of global filters that will be applied to the Administrative Templates nodes.

Select the type of policy settings to display.

Managed: Yes Configured: Any Commented: Any

☒ Enable Keyword Filters

Filter for word(s): Clock Any

Within: ☒ Policy Setting Title ☒ Help Text ☒ Comment

☐ Enable Requirements Filters

Select the desired platform and application filter(s):

Include settings that match any of the selected platforms.

☐ BITS 1.5
☐ BITS 2.0
☐ BITS 3.5
☐ BITS 4.0
☐ Internet Explorer 10
☐ Internet Explorer 11
☐ Internet Explorer 3
☐ Internet Explorer 4
☐ Internet Explorer 5

Select All Clear All

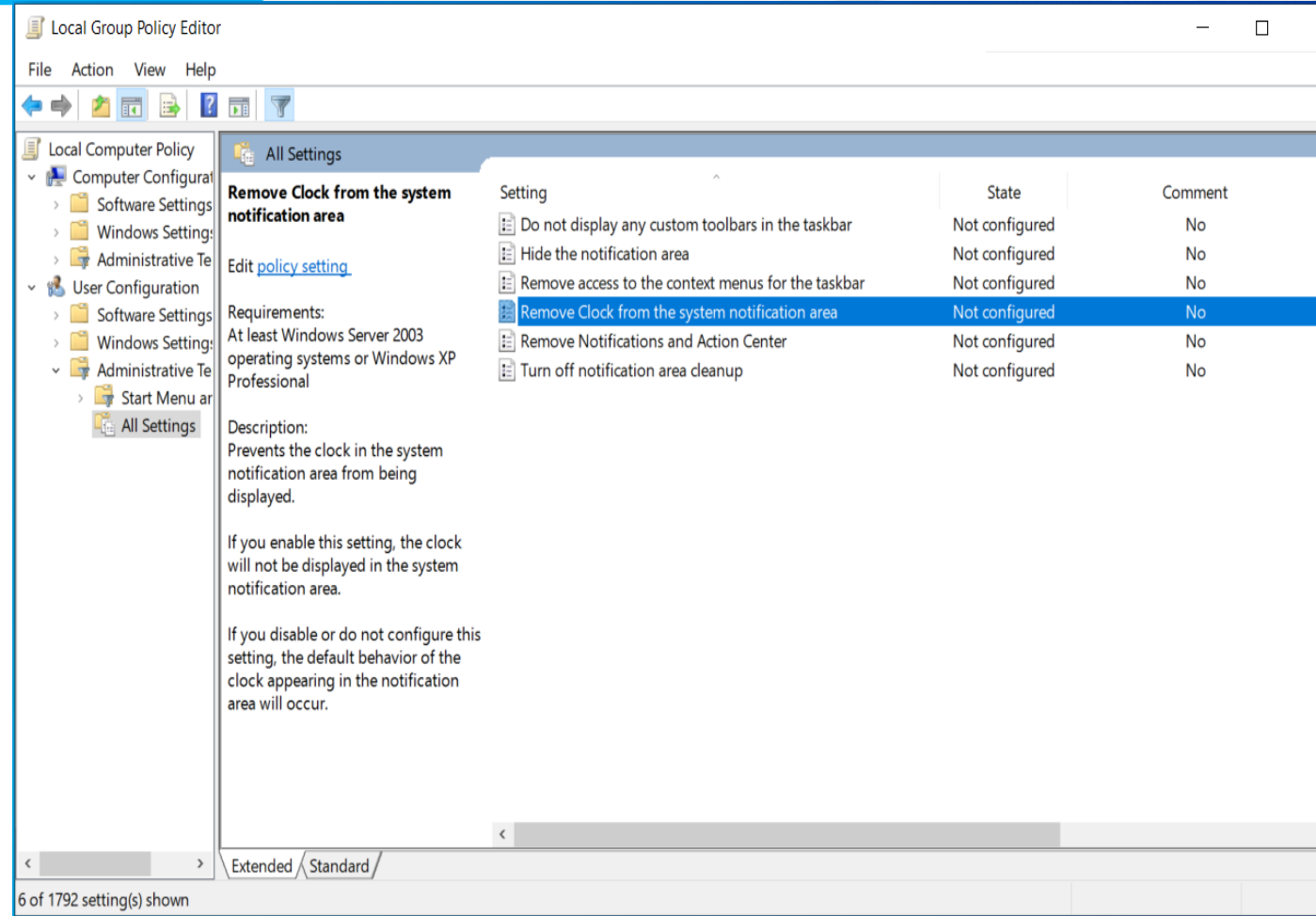
OK Cancel

Apply Group Policy in Local Computer

Hide Clock from Taskbar

- Select:

Remove clock from the system notification area



The screenshot shows the Local Group Policy Editor window. The left pane displays the tree structure with 'Local Computer Policy' expanded, and 'All Settings' selected under 'Administrative Templates'. The right pane shows the details for the 'Remove Clock from the system notification area' policy, which is currently 'Not configured'. A table below the policy details lists several other taskbar-related settings.

Setting	State	Comment
Do not display any custom toolbars in the taskbar	Not configured	No
Hide the notification area	Not configured	No
Remove access to the context menus for the taskbar	Not configured	No
Remove Clock from the system notification area	Not configured	No
Remove Notifications and Action Center	Not configured	No
Turn off notification area cleanup	Not configured	No

Requirements:
At least Windows Server 2003 operating systems or Windows XP Professional

Description:
Prevents the clock in the system notification area from being displayed.

If you enable this setting, the clock will not be displayed in the system notification area.

If you disable or do not configure this setting, the default behavior of the clock appearing in the notification area will occur.

6 of 1792 setting(s) shown

Apply Group Policy in Local Computer

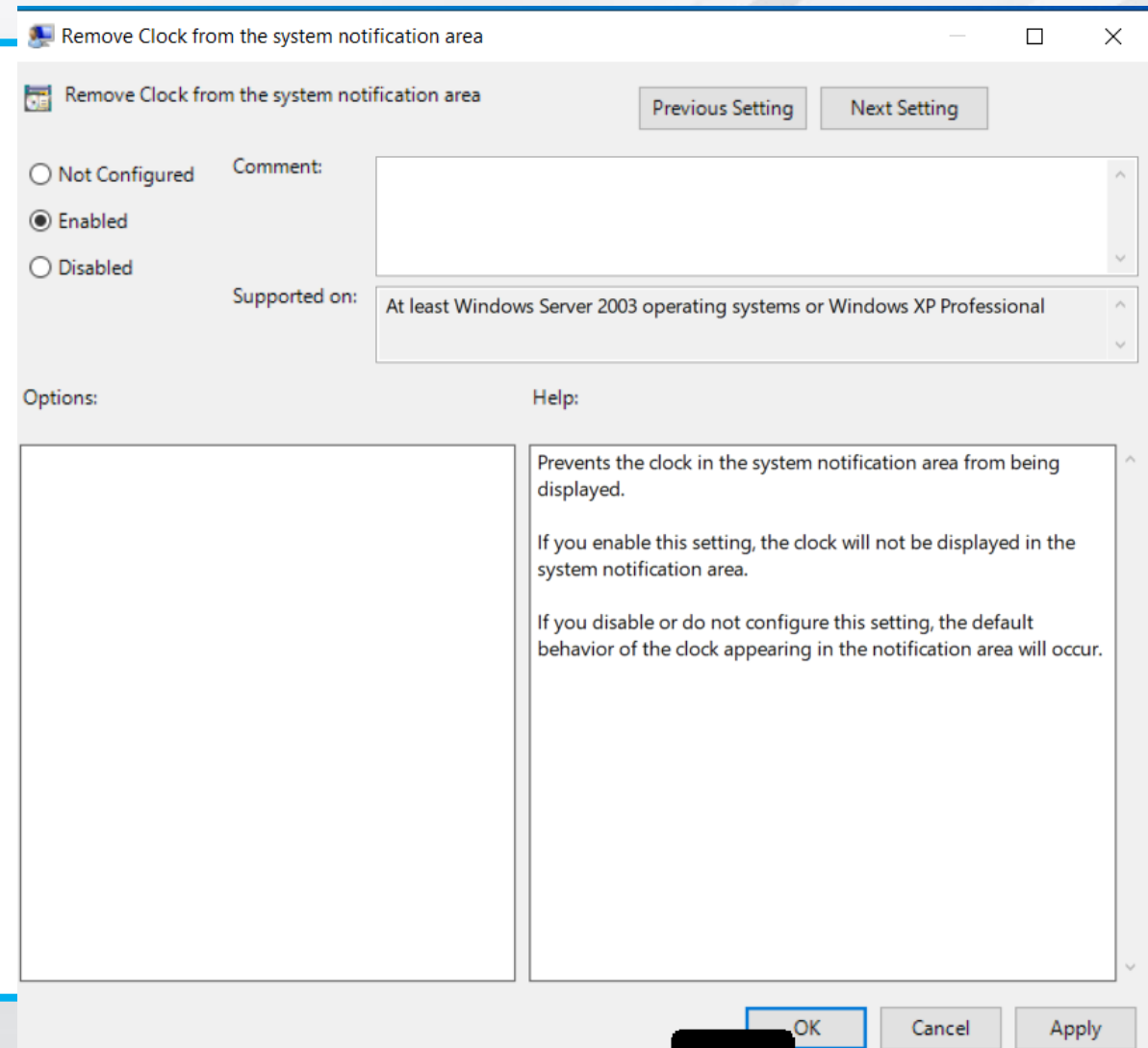
Hide Clock from Taskbar

- Select:

Enabled

❖ Review the support area

❖ You must log off then log on to see the changes



The screenshot shows the 'Remove Clock from the system notification area' Group Policy dialog box. The 'Enabled' radio button is selected. The 'Supported on:' field indicates 'At least Windows Server 2003 operating systems or Windows XP Professional'. The 'Help' section explains that enabling this setting prevents the clock from being displayed in the system notification area.

Remove Clock from the system notification area

Remove Clock from the system notification area

Previous Setting Next Setting

☐ Not Configured
 ☒ Enabled
 ☐ Disabled

Comment:

Supported on: At least Windows Server 2003 operating systems or Windows XP Professional

Options:

Help:

Prevents the clock in the system notification area from being displayed.

If you enable this setting, the clock will not be displayed in the system notification area.

If you disable or do not configure this setting, the default behavior of the clock appearing in the notification area will occur.

OK Cancel Apply

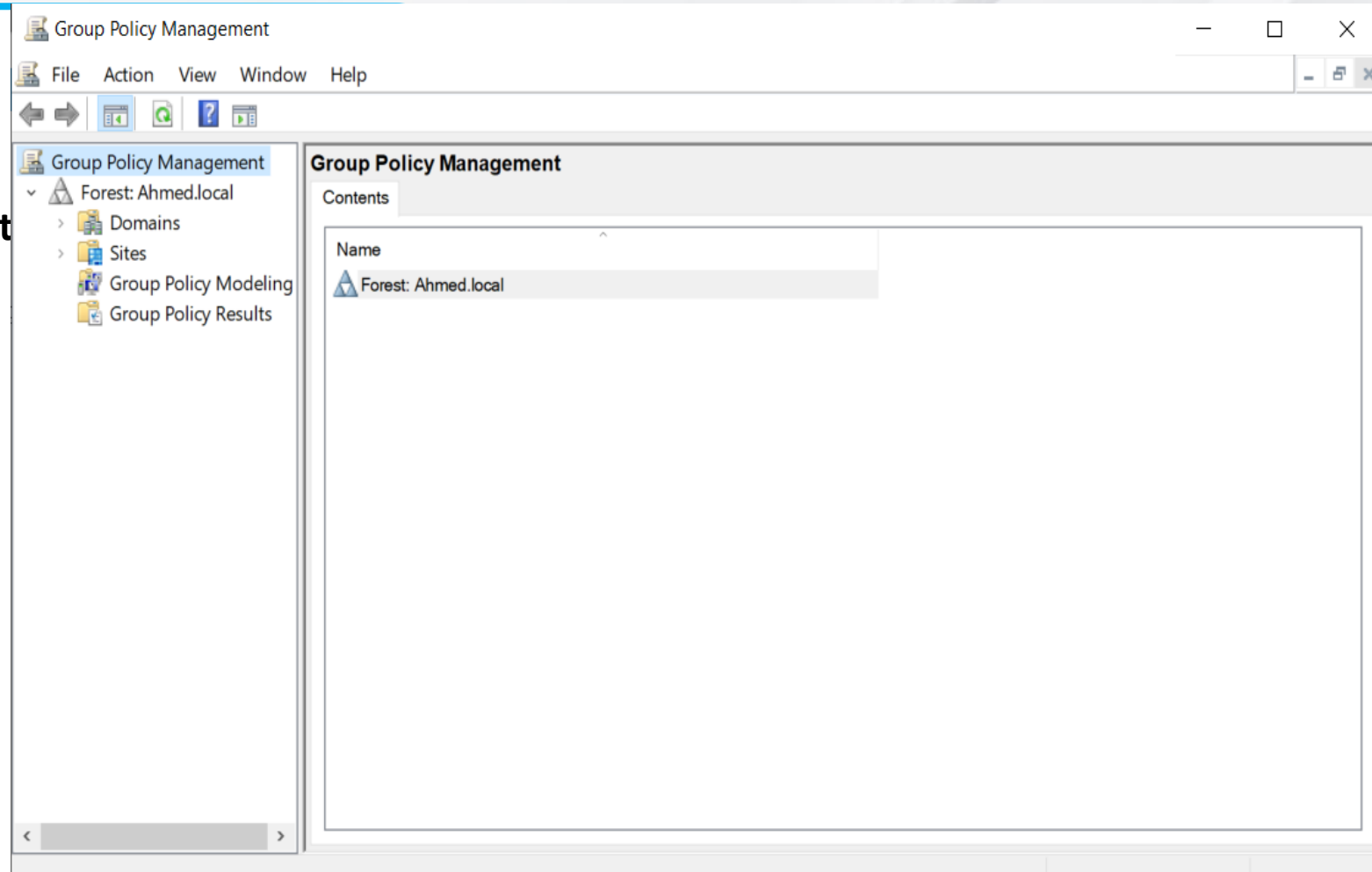
Apply Group Policy in Domain Controller

This pane shows the hierarchical structure of the Active Directory forest.

From **tools** open > **Group Policy Management**

Under "Forest: Ahmed.local" :

- **Domains**
- **Sites**
- **Group Policy Modeling**
- **Group Policy Results**



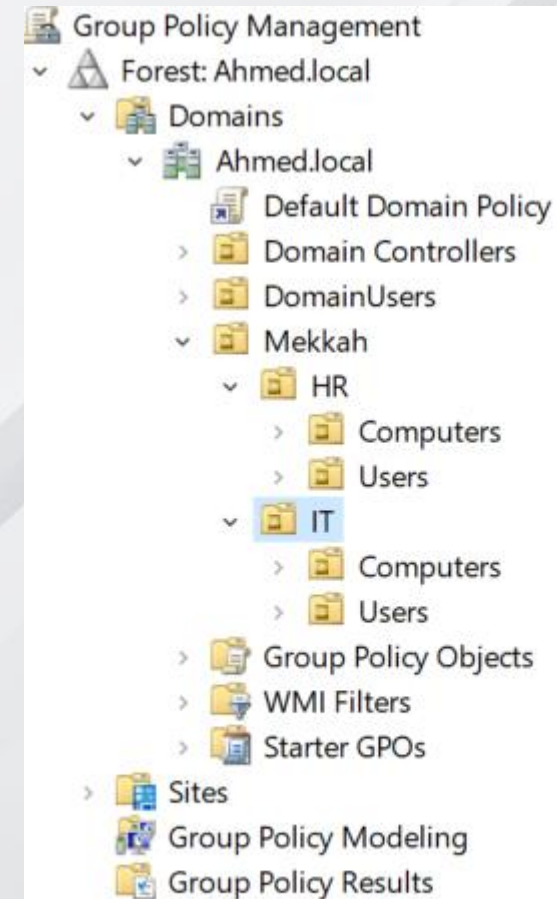
Apply Group Policy in Domain Controller

❑ **HR:** An OU nested under "**Mekkah**",

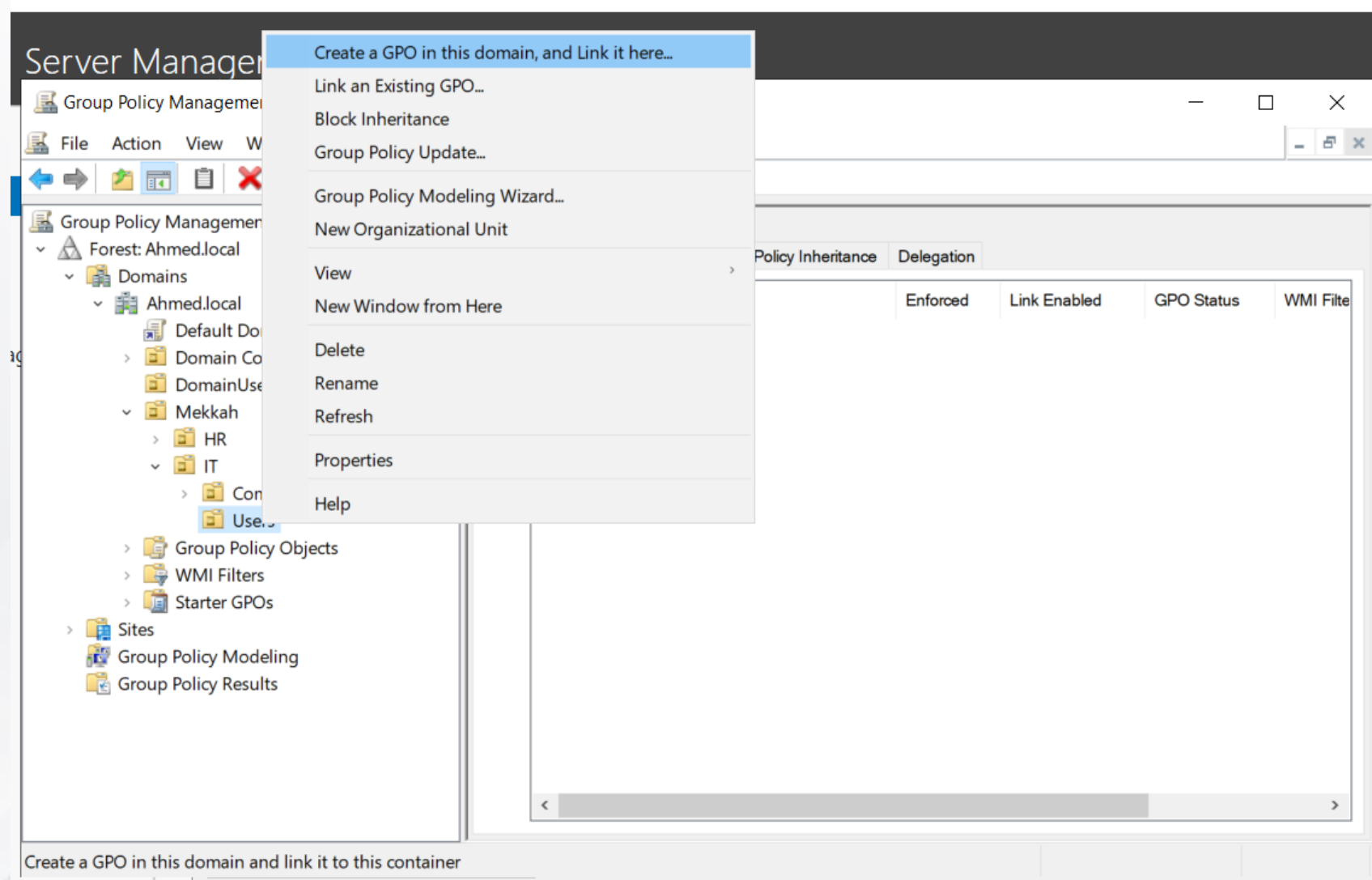
- **Computers:** A sub-container or **OU** under HR, for computer objects.
- **Users:** A sub-container or OU under HR, for user accounts.

❑ **IT :** Another OU nested under "Mekkah",

- **Computers:** A sub-container or OU under IT, for computer objects.
- **Users:** A sub-container or OU under IT, for user accounts.

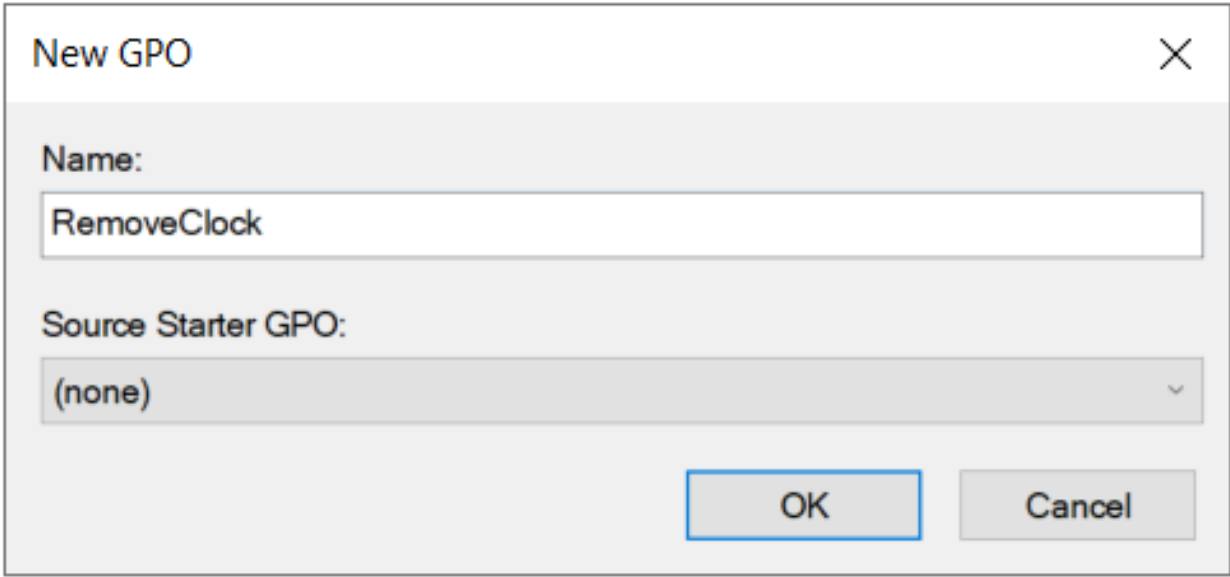


Apply Group Policy in Domain Controller



Apply Group Policy in Domain Controller

Write a descriptive name for the GPO



The screenshot shows a 'New GPO' dialog box with a close button (X) in the top right corner. It contains two input fields: 'Name:' with the text 'RemoveClock' entered, and 'Source Starter GPO:' with a dropdown menu showing '(none)'. At the bottom right are 'OK' and 'Cancel' buttons.

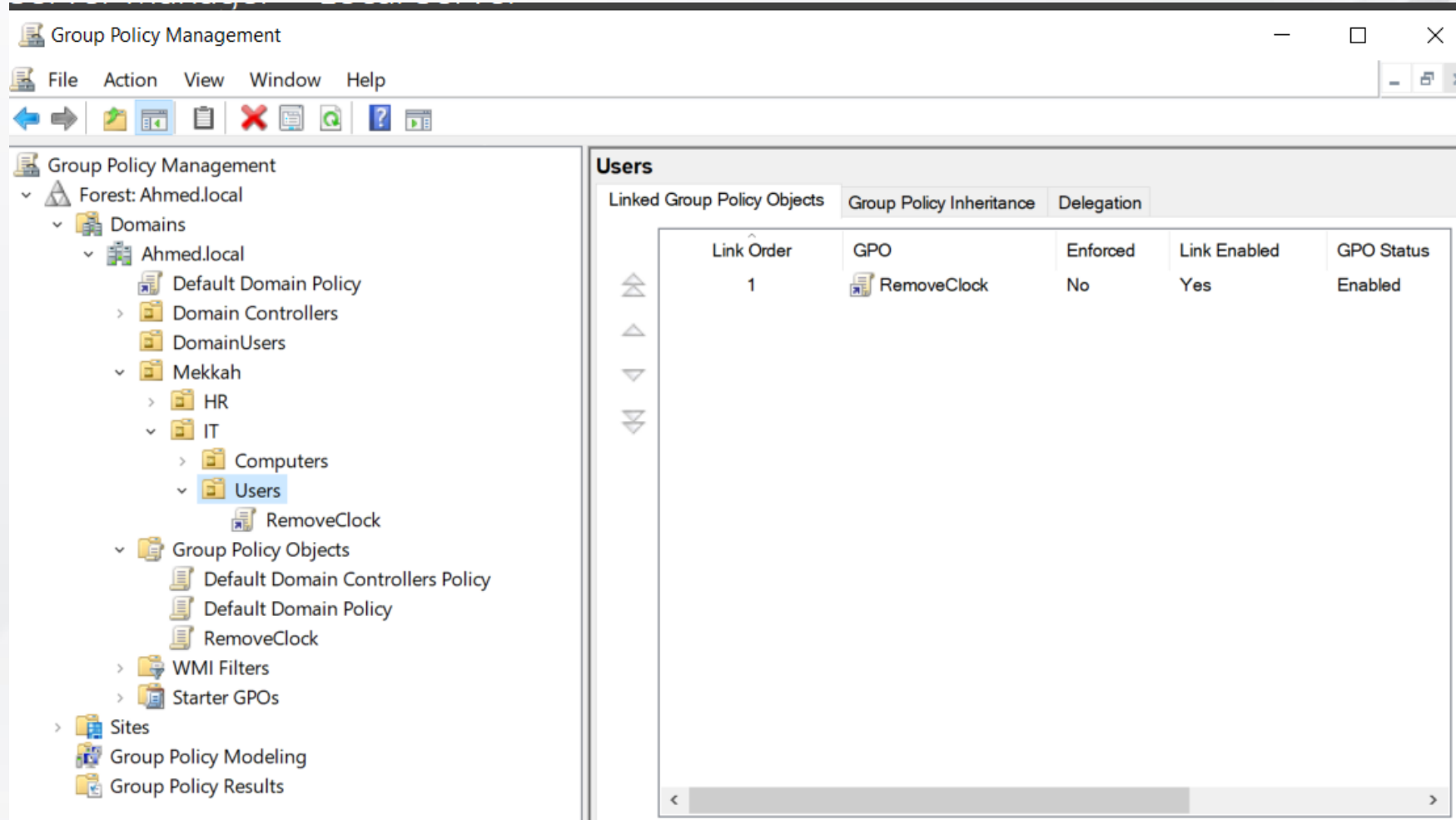
New GPO

Name:
RemoveClock

Source Starter GPO:
(none)

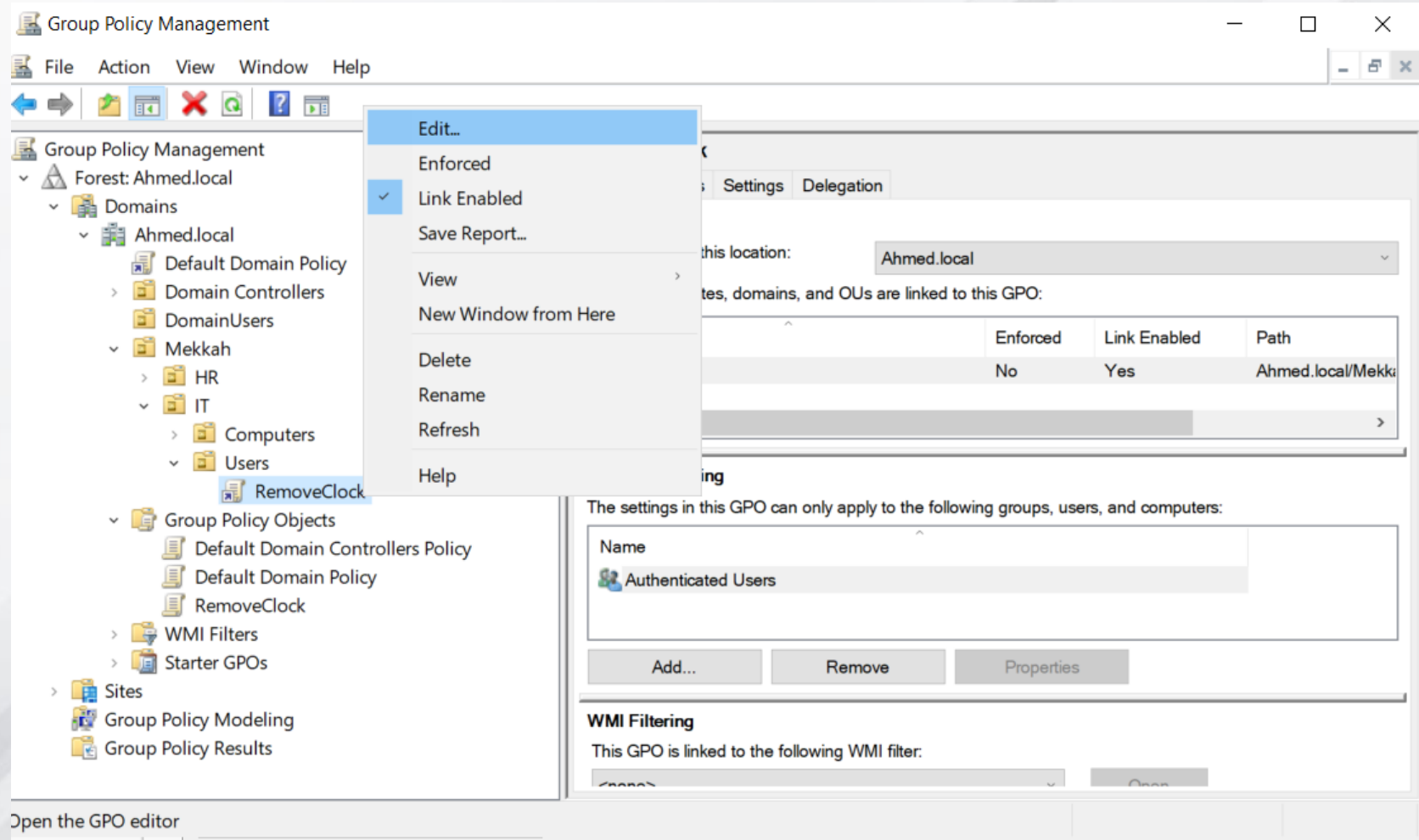
OK Cancel

Apply Group Policy in Domain Controller



Apply Group Policy in Domain Controller

Right click in
“RemoveClock”
Select -> Edit



Apply Group Policy in Domain Controller

Group Policy Management Editor

File Action View Help

RemoveClock [DC.AHMED.LOCAL] Policy

- Computer Configuration
 - Policies
 - Preferences
 - User Configuration
 - Policies
 - Software Settings
 - Windows Settings
 - Administrative Templates: Policy definitions (ADMX files) retrieved from
 - Control Panel
 - Desktop
 - Network
 - Shared Folders
 - Start Menu and Taskbar
 - Notifications
 - System
 - Windows Components
 - All Settings
 - Preferences

Start Menu and Taskbar

Remove Clock from the system notification area

Edit [policy setting](#)

Requirements:
At least Windows Server 2003 operating systems or Windows XP Professional

Description:
Prevents the clock in the system notification area from being displayed.

If you enable this setting, the clock will not be displayed in the system notification area.

If you disable or do not configure this setting, the default behavior of the clock appearing in the notification area will occur.

Setting	State	Co
Prevent users from customizing their Start Screen	Not configured	
Prevent users from moving taskbar to another screen dock lo...	Not configured	
Prevent users from rearranging toolbars	Not configured	
Prevent users from resizing the taskbar	Not configured	
Prevent users from uninstalling applications from Start	Not configured	
Remove "Recently added" list from Start Menu	Not configured	
Remove access to the context menus for the taskbar	Not configured	
Remove All Programs list from the Start menu	Not configured	
Remove and prevent access to the Shut Down, Restart, Sleep, ...	Not configured	
Remove Balloon Tips on Start Menu items	Not configured	
Remove Clock from the system notification area	Not configured	
Remove common program groups from Start Menu	Not configured	
Remove Default Programs link from the Start menu.	Not configured	
Remove Documents icon from Start Menu	Not configured	
Remove Downloads link from Start Menu	Not configured	
Remove Favorites menu from Start Menu	Not configured	
Remove frequent programs list from the Start Menu	Not configured	

Apply Group Policy in Domain Controller

Remove Clock from the system notification area

Remove Clock from the system notification area Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled Supported on: At least Windows Server 2003 operating systems or Windows XP Professional

Options: Help:

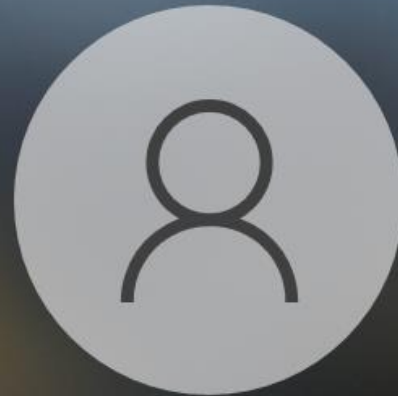
Prevents the clock in the system notification area from being displayed.

If you enable this setting, the clock will not be displayed in the system notification area.

If you disable or do not configure this setting, the default behavior of the clock appearing in the notification area will occur.

OK Cancel Apply

Apply Group Policy in Domain Controller



Other user

Ahmed\user1

.....

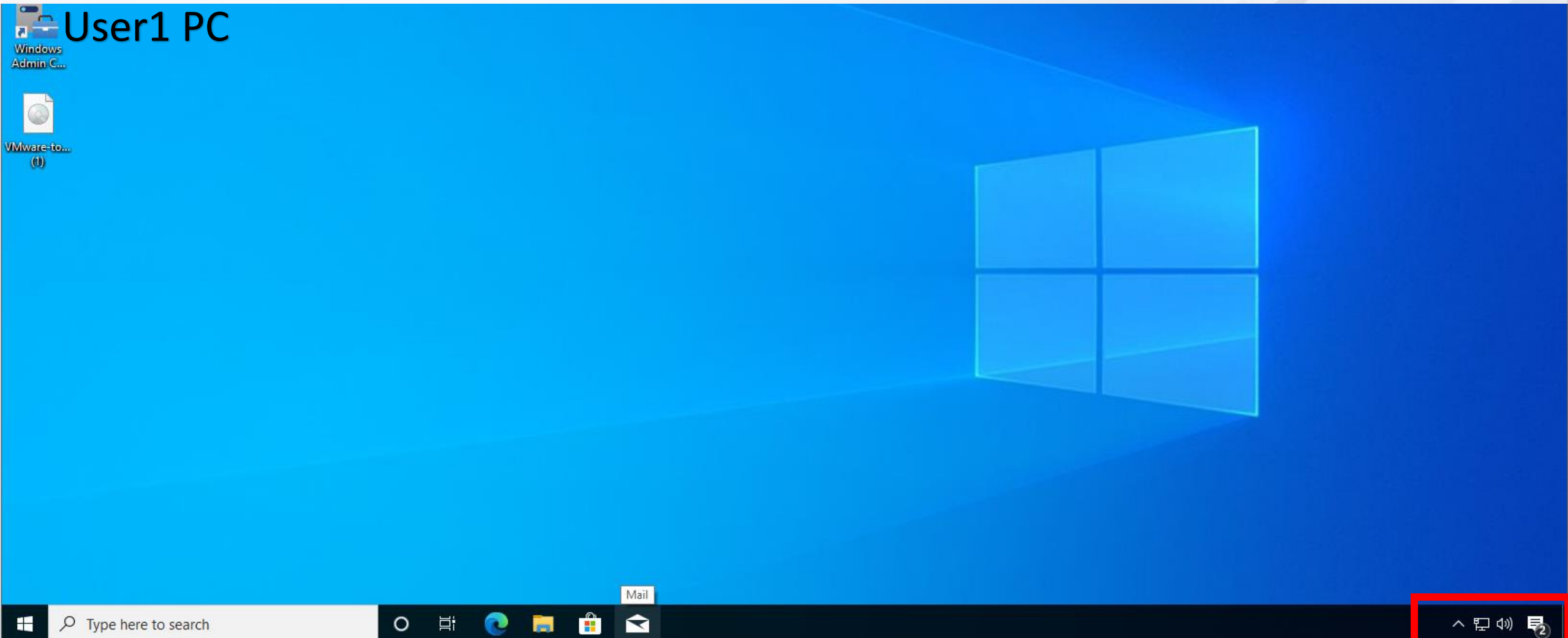


Sign in to: Ahmed

[How do I sign in to another domain?](#)

Apply Group Policy in Domain Controller

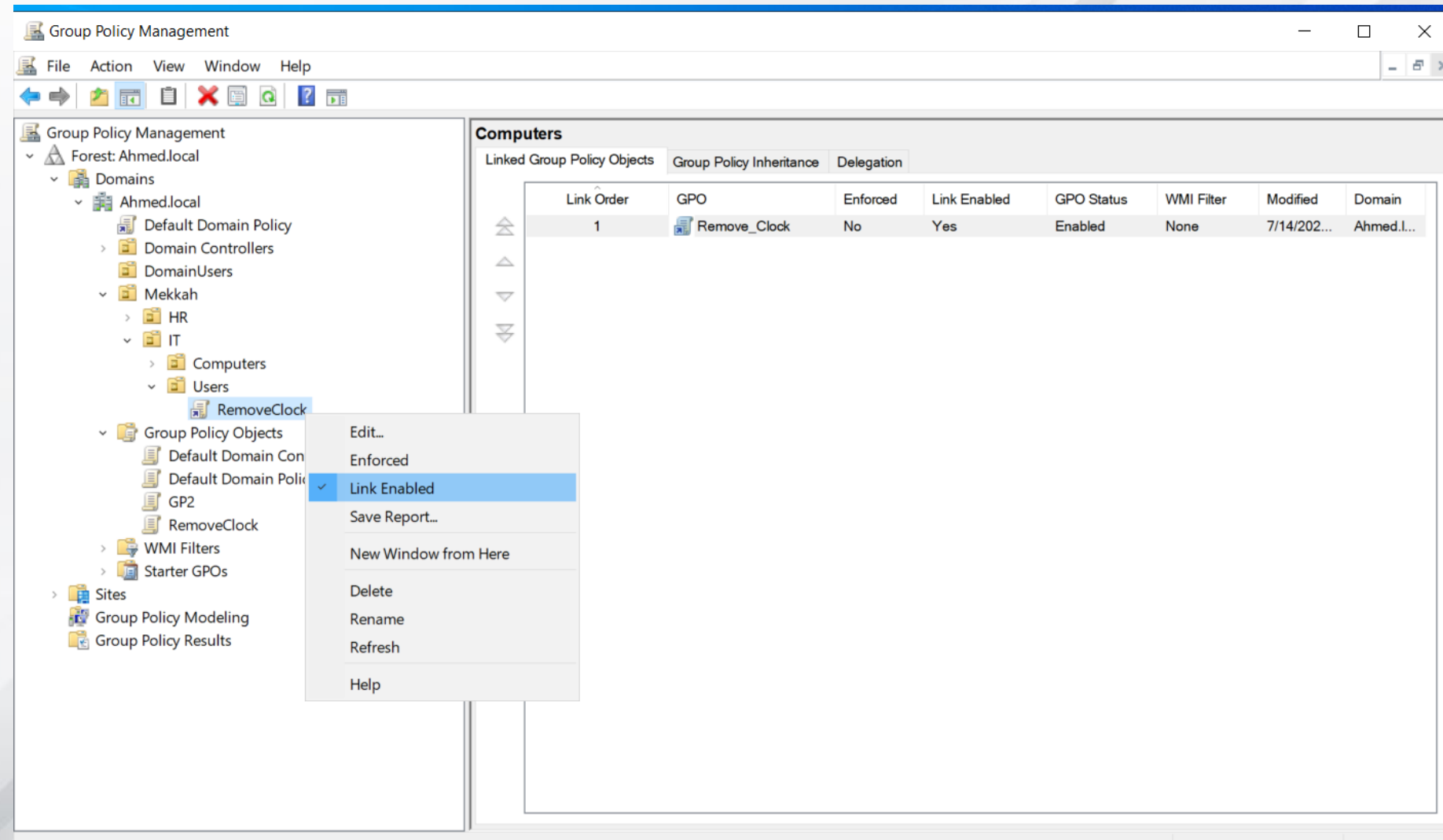
User1 PC



Apply Group Policy in Domain Controller

To Remove GPO Link
from OU

Right click-> Link Enabled

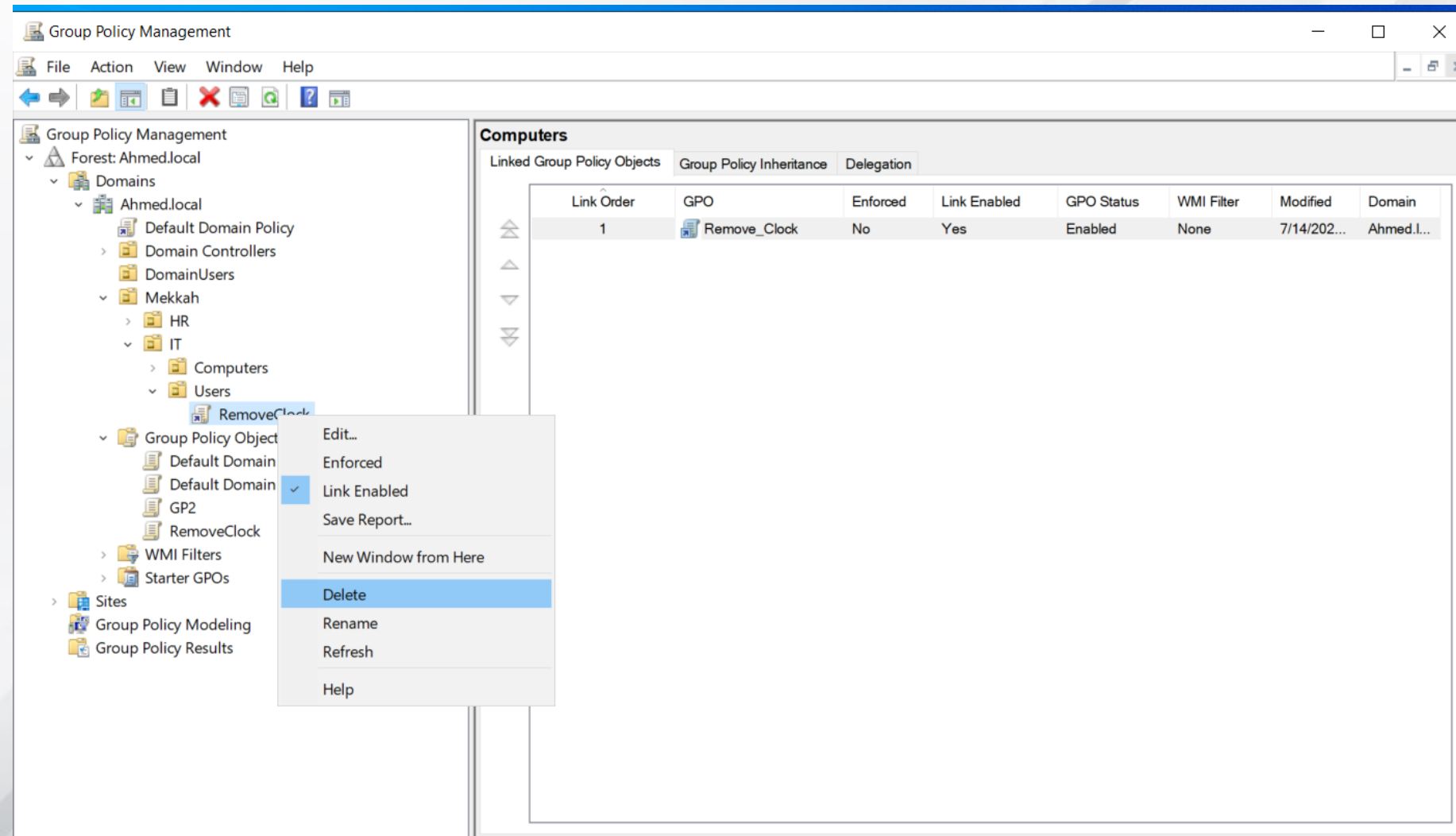


Apply Group Policy in Domain Controller

To Remove GPO
from OU

Right click-> Delete

It will still in:
Group Policy Objects

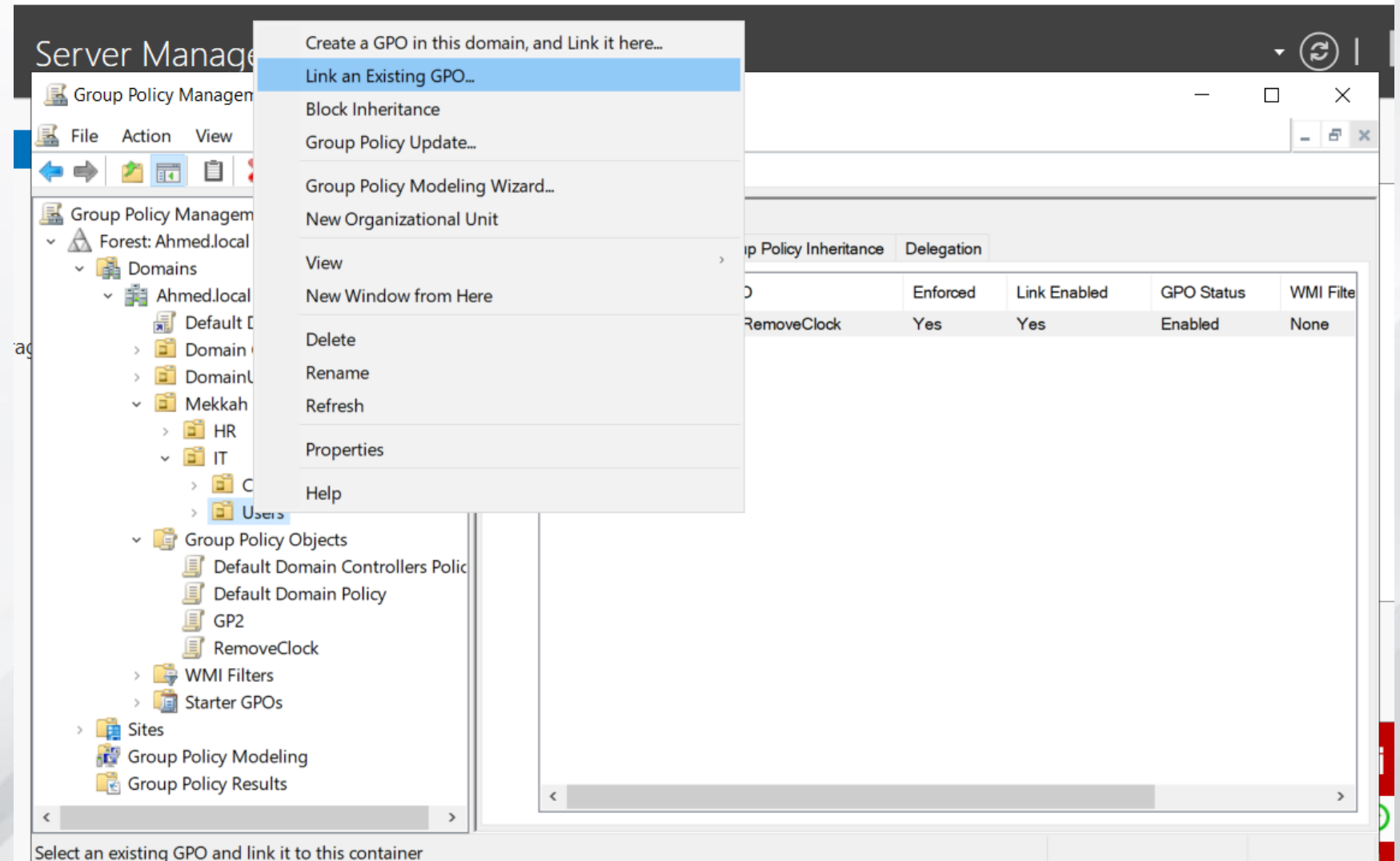


Deletes the current selection.

Apply Group Policy in Domain Controller

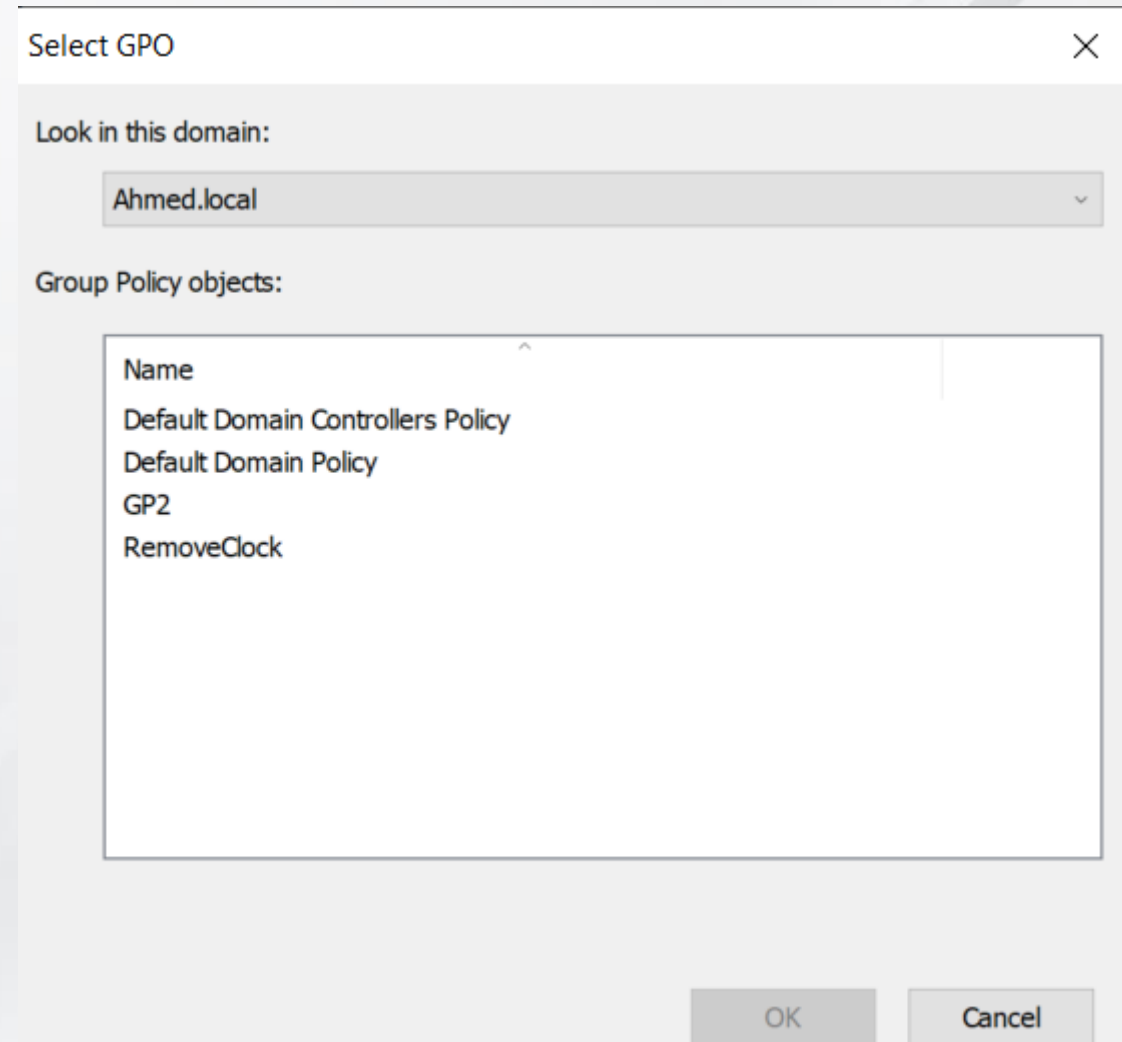
To Re-Link GPO
to OU

Right click->
Link an Existing GPO



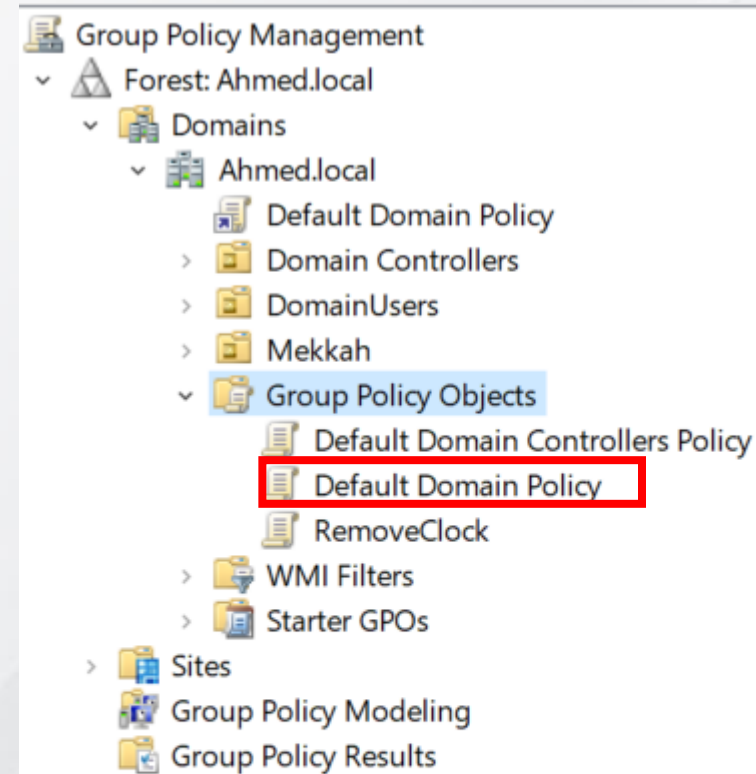
Apply Group Policy in Domain Controller

Then Select the **GPO**



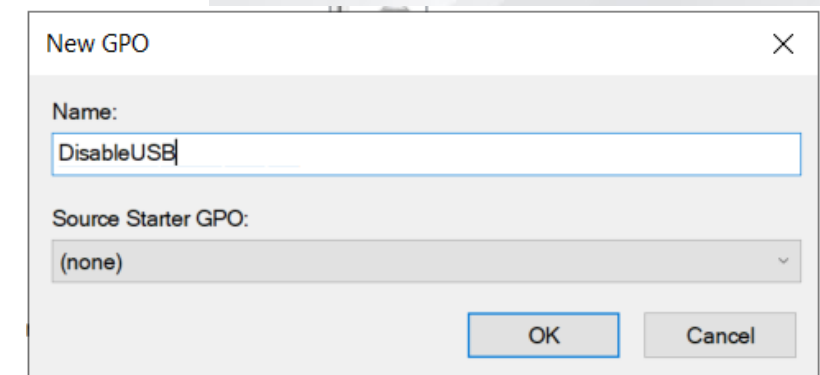
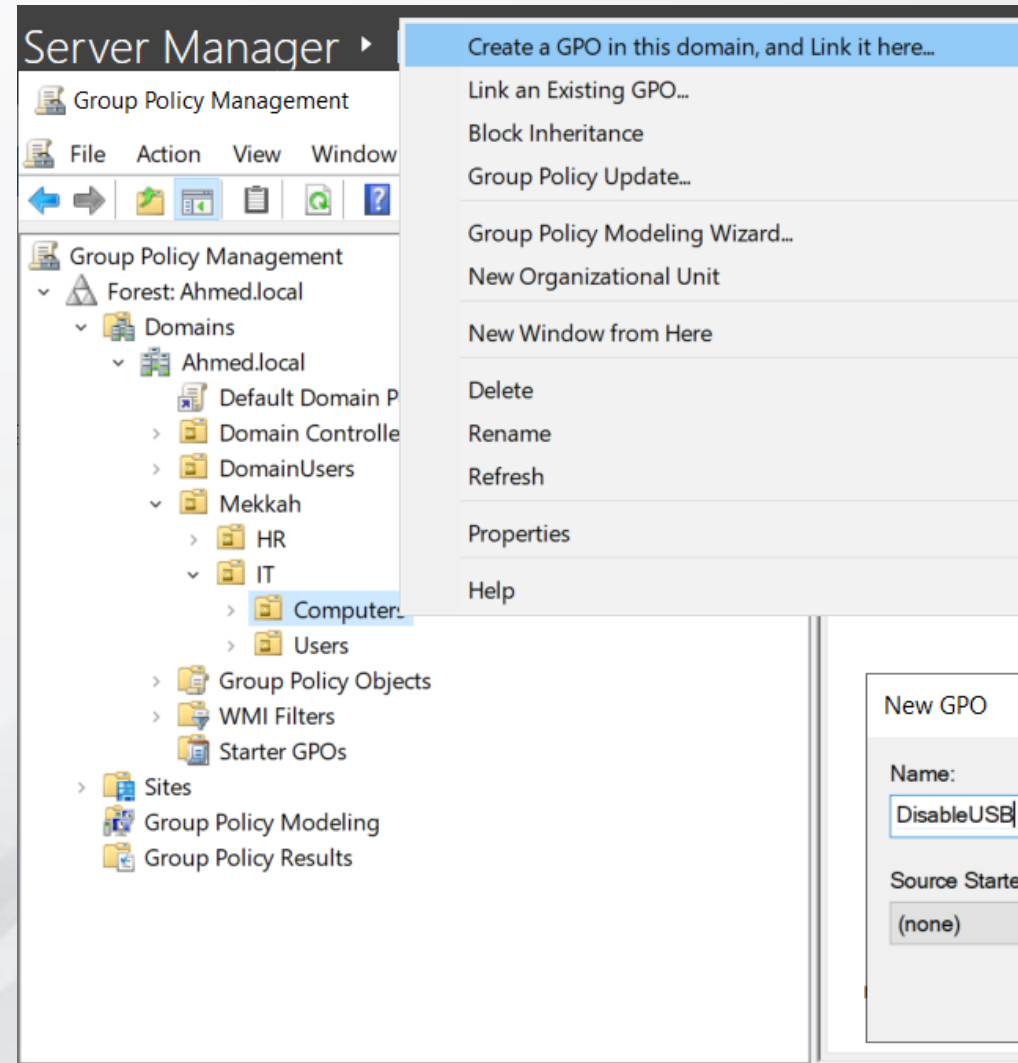
Apply Group Policy in Domain Controller

- Default Domain Policy
GPO For the entire Domain



Apply Group Policy in Domain Controller

- Create GPO to disable USB

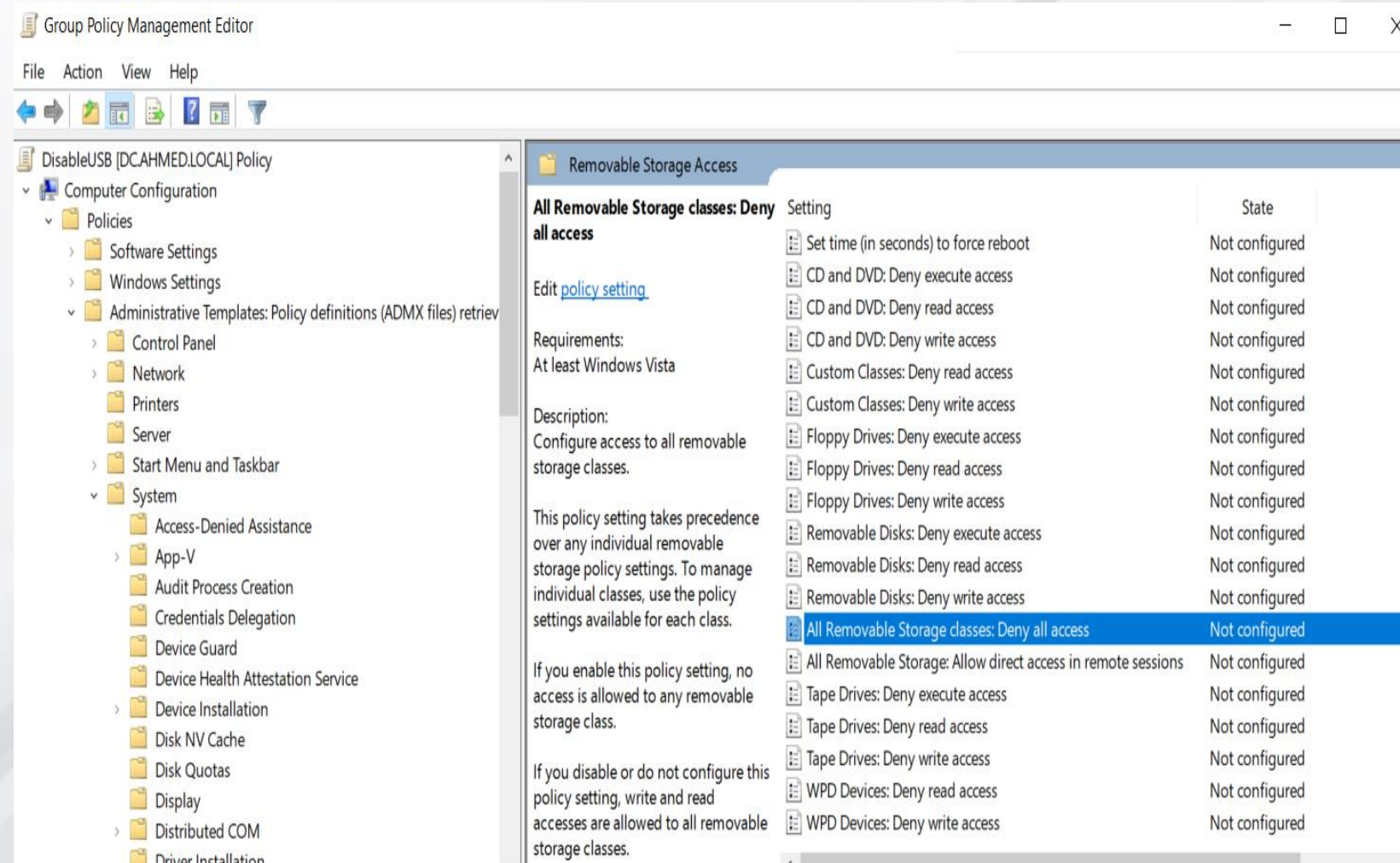


Apply Group Policy in Domain Controller

GPO to disable USB

- Computer Configuration
 - > Policies > Administrative Templates
 - > System > Removable Storage Access

"All Removable Storage classes: Deny all access"



Apply Group Policy in Domain Controller

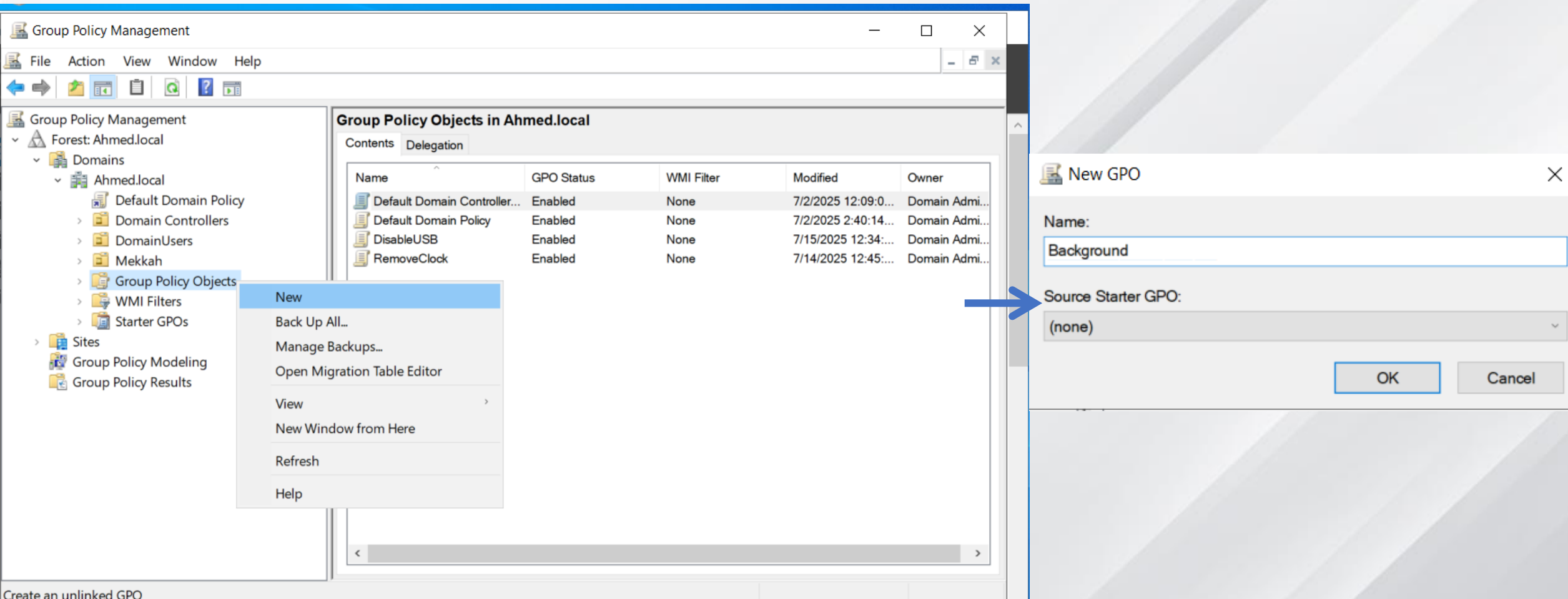
GPO to disable USB

- In the policy settings window, select the "Enabled" radio button.
- Click "Apply" and then "OK" to save your changes

The screenshot shows the Group Policy settings window for the policy "All Removable Storage classes: Deny all access". The window has a title bar with the policy name and standard window controls. Below the title bar, there are "Previous Setting" and "Next Setting" buttons. The main configuration area includes three radio buttons: "Not Configured", "Enabled" (which is selected), and "Disabled". To the right of these buttons is a "Comment:" text box. Below the radio buttons is a "Supported on:" dropdown menu set to "At least Windows Vista". At the bottom of the window, there are two sections: "Options:" and "Help:". The "Options:" section is currently empty. The "Help:" section contains the following text: "Configure access to all removable storage classes. This policy setting takes precedence over any individual removable storage policy settings. To manage individual classes, use the policy settings available for each class. If you enable this policy setting, no access is allowed to any removable storage class. If you disable or do not configure this policy setting, write and read accesses are allowed to all removable storage classes."

Force Desktop Background via Group Policy

Create New GPO



Group Policy Management

File Action View Window Help

Group Policy Management

Forest: Ahmed.local

Domains

Ahmed.local

Default Domain Policy

Domain Controllers

DomainUsers

Mekkah

Group Policy Objects

WMI Filters

Starter GPOs

Sites

Group Policy Modeling

Group Policy Results

Group Policy Objects in Ahmed.local

Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controller...	Enabled	None	7/2/2025 12:09:0...	Domain Admi...
Default Domain Policy	Enabled	None	7/2/2025 2:40:14...	Domain Admi...
DisableUSB	Enabled	None	7/15/2025 12:34:...	Domain Admi...
RemoveClock	Enabled	None	7/14/2025 12:45:...	Domain Admi...

New

Back Up All...

Manage Backups...

Open Migration Table Editor

View

New Window from Here

Refresh

Help

New GPO

Name:

Background

Source Starter GPO:

(none)

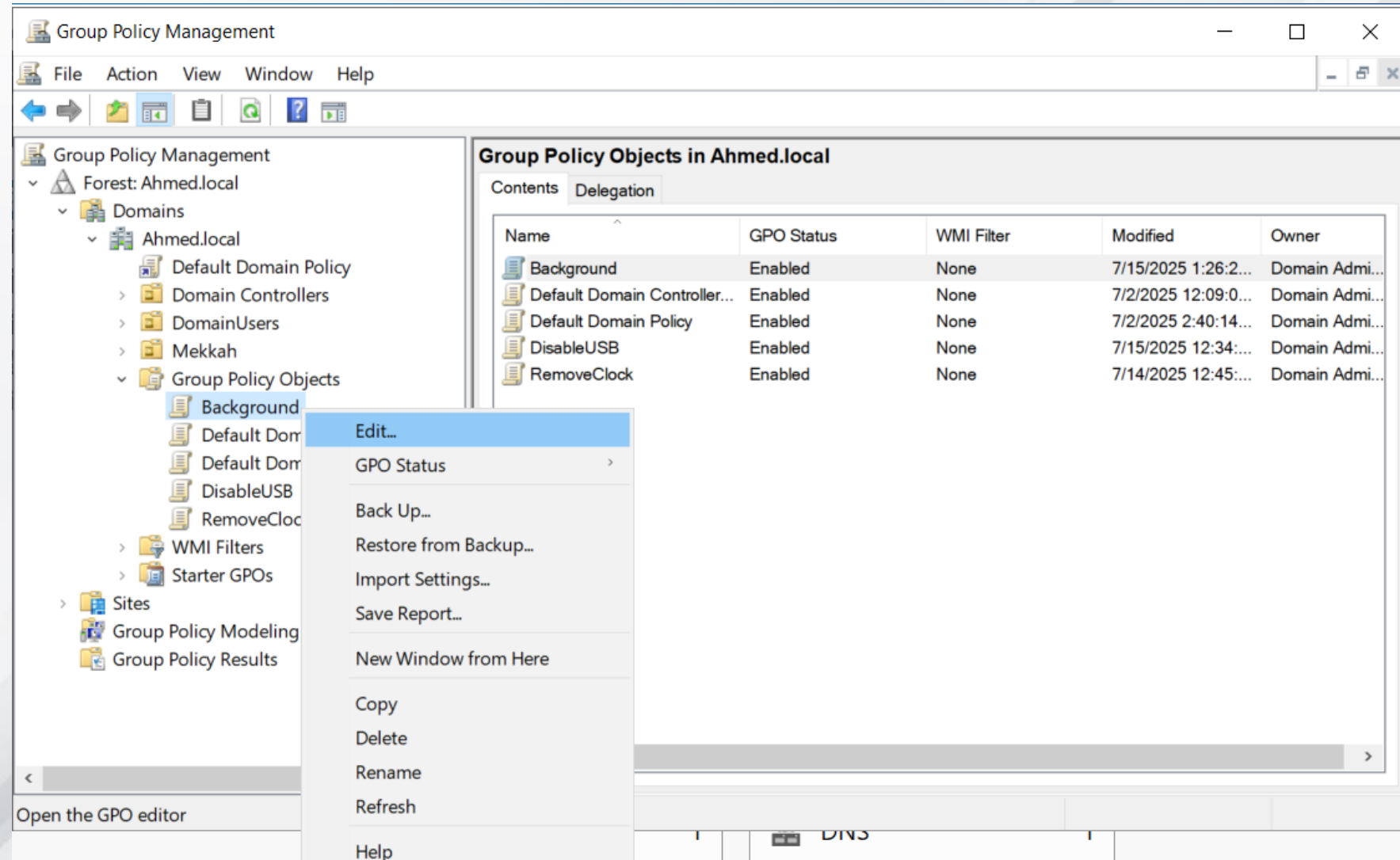
OK

Cancel

Create an unlinked GPO

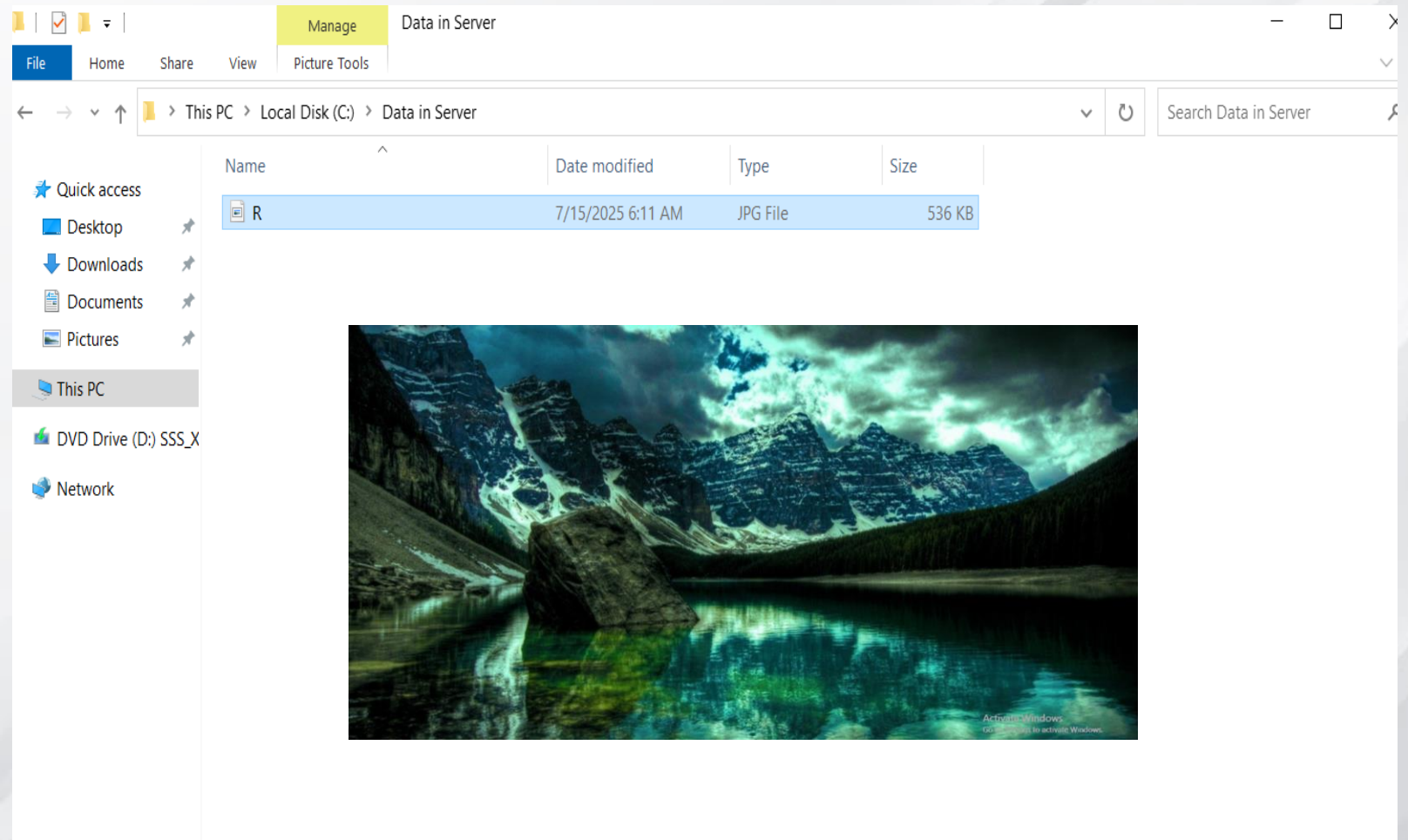
Force Desktop Background via Group Policy

Right click > Edit



Force Desktop Background via Group Policy

Save The Desktop image in
Shared Folder



Force Desktop Background via Group Policy

In the Group Policy Management Editor, navigate to:

User Configuration > Policies > Administrative Templates > Desktop > Desktop

Desktop Wallpaper

The screenshot shows the Group Policy Management Editor window. The left pane displays the navigation tree with 'Desktop' selected under 'Administrative Templates'. The right pane shows the 'Desktop Wallpaper' policy, which is currently 'Not configured'. Below the policy name, there is a list of settings and their states.

Setting	State	Comment
Enable Active Desktop	Not configured	No
Disable Active Desktop	Not configured	No
Prohibit changes	Not configured	No
Desktop Wallpaper	Not configured	No
Prohibit adding items	Not configured	No
Prohibit closing items	Not configured	No
Prohibit deleting items	Not configured	No
Prohibit editing items	Not configured	No
Disable all items	Not configured	No
Add/Delete items	Not configured	No
Allow only bitmapped wallpaper	Not configured	No

Desktop Wallpaper

Edit [policy setting](#).

Requirements:
At least Windows 2000

Description:
Specifies the desktop background ("wallpaper") displayed on all users' desktops.

This setting lets you specify the wallpaper on users' desktops and prevents users from changing the image or its presentation. The wallpaper you specify can be stored in a bitmap (*.bmp) or JPEG (*.jpg) file.

To use this setting, type the fully qualified path and name of the file that stores the wallpaper image. You can type a local path, such as C:\Windows\web\wallpaper\home

Force Desktop Background via Group Policy

\\DC\Data in Server\R.jpg

Desktop Wallpaper

Desktop Wallpaper

Previous Setting Next Setting

☐ Not Configured
 ☒ Enabled
 ☐ Disabled

Comment:

Supported on: At least Windows 2000

Options:

Wallpaper Name:

\\DC\Data in Server\R.jpg

Example: Using a local path:
C:\windows\web\wallpaper\home.jpg

Example: Using a UNC path:
\\Server\Share\Corp.jpg

Wallpaper Style: Fill

Center
Fill
Fit
Span
Stretch
Tile

Help:

Specifies the desktop background ("wallpaper") displayed on all users' desktops.

This setting lets you specify the wallpaper on users' desktops and prevents users from changing the image or its presentation. The wallpaper you specify can be stored in a bitmap (*.bmp) or JPEG (*.jpg) file.

To use this setting, type the fully qualified path and name of the file that stores the wallpaper image. You can type a local path, such as C:\Windows\web\wallpaper\home.jpg or a UNC path, such as \\Server\Share\Corp.jpg. If the specified file is not available when the user logs on, no wallpaper is displayed. Users cannot specify alternative wallpaper. You can also use this setting to specify that the wallpaper image be centered, tiled, or stretched. Users cannot change this specification.

If you disable this setting or do not configure it, no wallpaper is displayed. However, users can select the wallpaper of their choice.

Force Desktop Background via Group Policy

Prevent Changing Desktop Background

User Configuration > Policies > Administrative Templates > Control Panel > **Personalization**

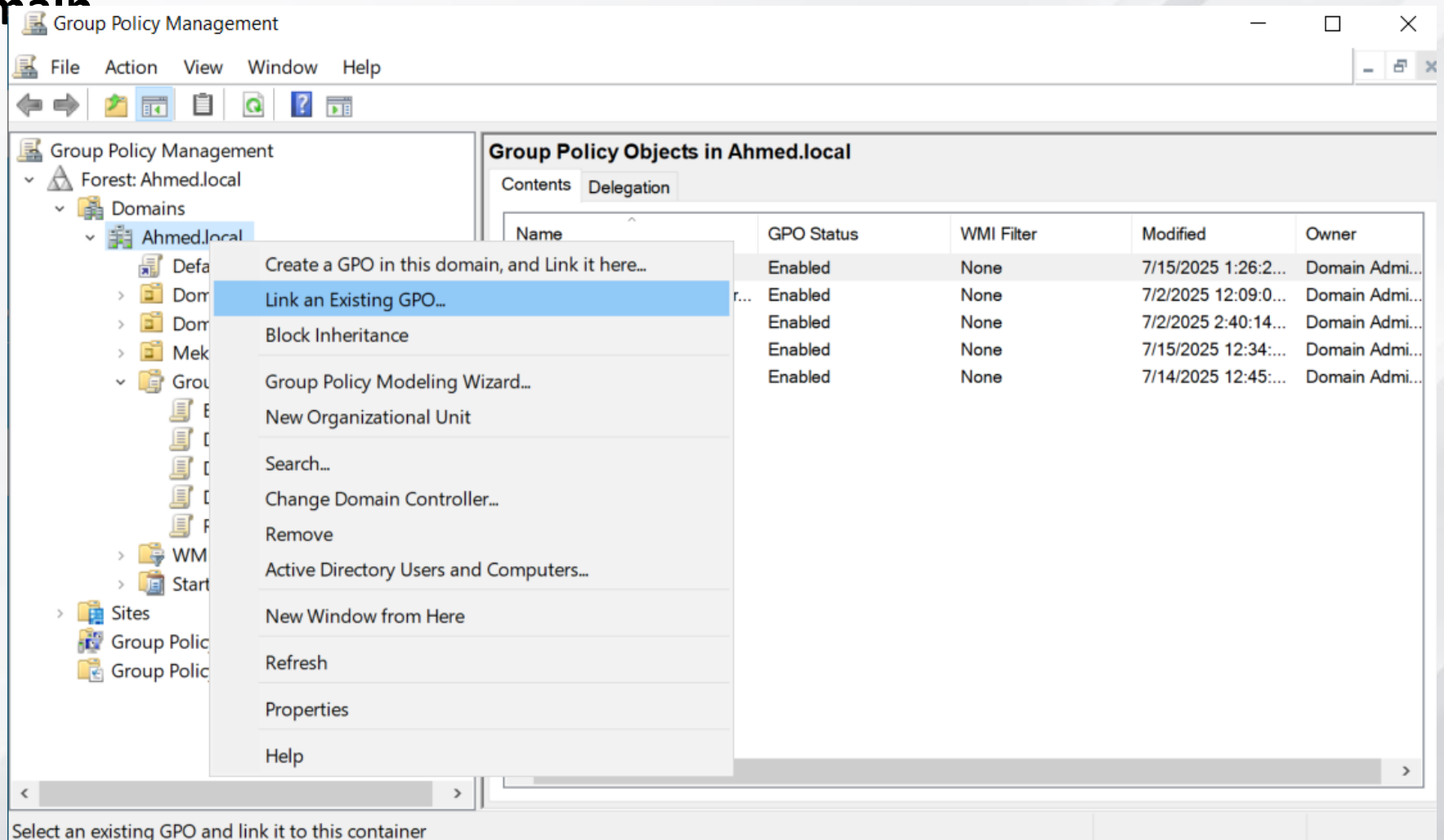
Enable

The screenshot shows the Group Policy Management Editor window. The left pane displays the tree structure: Background [DCAHMED.LOCAL] Policy > Computer Configuration > Policies > User Configuration > Policies > Administrative Templates: Policy definition > Control Panel > Personalization. The right pane shows the 'Prevent changing desktop background' policy, which is currently 'Not configured'. The policy description states: 'Prevents users from adding or changing the background design of the desktop. By default, users can use the Desktop Background page in the Personalization or Display Control Panel to add a background design (wallpaper) to their desktop. If you enable this setting, none of the Desktop Background settings can be changed by the user. To specify wallpaper for a group, use the "Desktop Wallpaper" setting.'

Setting	State	Comment
Prevent changing color scheme	Not configured	No
Prevent changing theme	Not configured	No
Prevent changing visual style for windows and buttons	Not configured	No
Enable screen saver	Not configured	No
Prohibit selection of visual style font size	Not configured	No
Prevent changing color and appearance	Not configured	No
Prevent changing desktop background	Not configured	No
Prevent changing desktop icons	Not configured	No
Prevent changing mouse pointers	Not configured	No
Prevent changing screen saver	Not configured	No
Prevent changing sounds	Not configured	No
Password protect the screen saver	Not configured	No
Screen saver timeout	Not configured	No
Force specific screen saver	Not configured	No
Load a specific theme	Not configured	No
Force a specific visual style file or force Windows Classic	Not configured	No

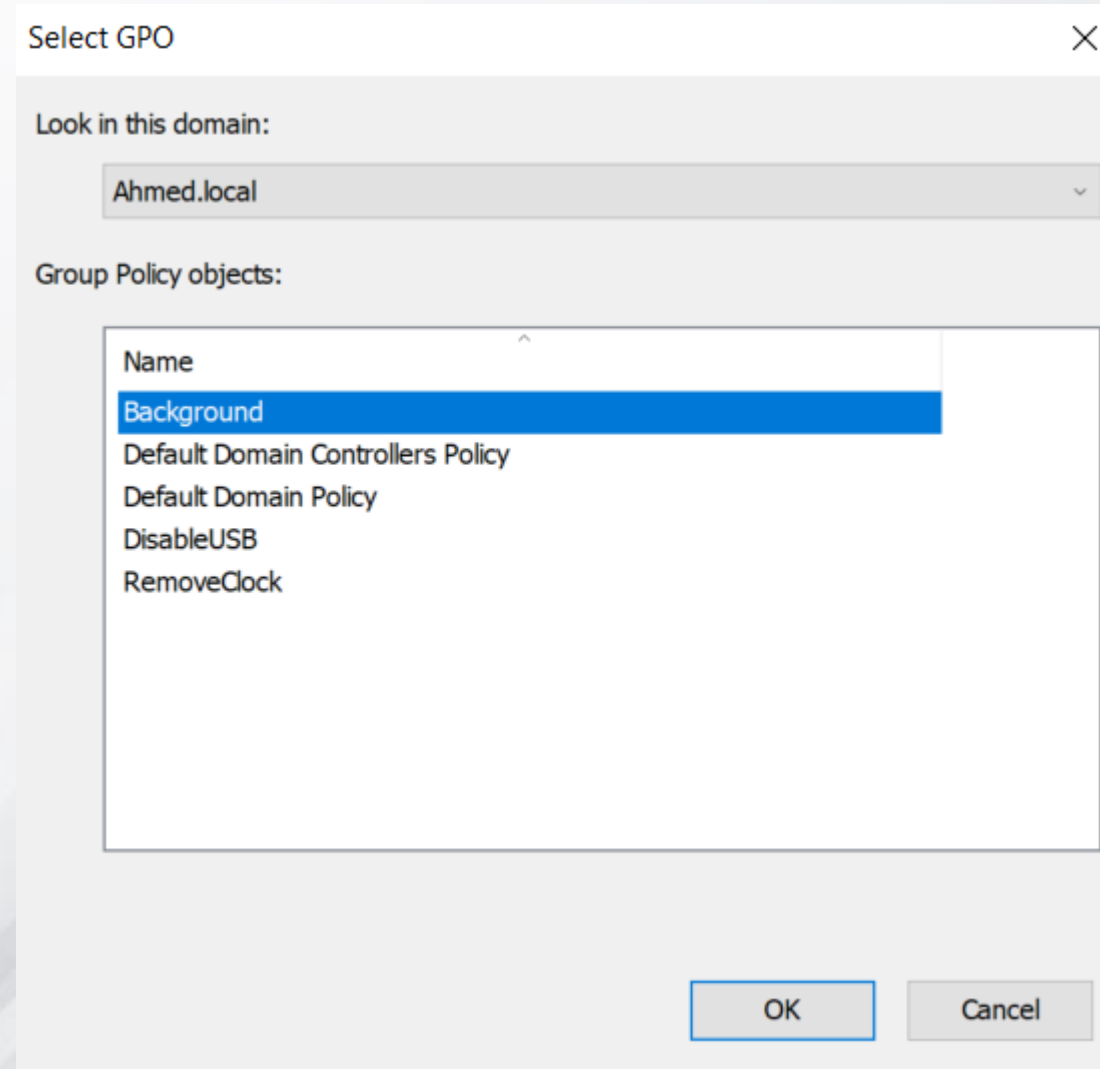
Force Desktop Background via Group Policy

Link the GPO to the Domain



Force Desktop Background via Group Policy

Link the GPO to the Domain



Force Desktop Background via Group Policy

Open Client PC



Default Domain Policy -Security

The screenshot displays the Group Policy Management console with the following structure:

- Group Policy Management
 - Forest: Ahmed.local
 - Domains
 - Ahmed.local
 - Background
 - Default Domain Policy**
 - Domain Controllers
 - DomainUsers
 - Mekkah
 - Group Policy Objects
 - WMI Filters
 - Starter GPOs
 - Sites
 - Group Policy Modeling
 - Group Policy Results

The Group Policy Management Editor window shows the following hierarchy:

- Group Policy Management Editor
 - Default Domain Policy [DCAHMED.LOCAL] Policy
 - Computer Configuration
 - Policies
 - Software Settings
 - Windows Settings
 - Name Resolution Policy
 - Scripts (Startup/Shutdown)
 - Security Settings
 - Account Policies
 - Password Policy**
 - Account Lockout Policy
 - Kerberos Policy
 - Local Policies
 - Event Log
 - Restricted Groups
 - System Services
 - Registry
 - File System
 - Wired Network (IEEE 802.3) Policies
 - Windows Defender Firewall with Advanced Security
 - Network List Manager Policies
 - Wireless Network (IEEE 802.11) Policies
 - Public Key Policies
 - Software Restriction Policies

The Password Policy settings are as follows:

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

Default Domain Policy -Security

- ❑ **Enforce password history:** This setting determines how many unique new passwords a user must create before they can reuse an old password. In your image, it's set to "**24 passwords remembered**," meaning a user cannot reuse any of their last 24 passwords.
- ❑ **Maximum password age:** This specifies the maximum number of days a password can be used before the system requires the user to change it. In your image, it's set to "**42 days**," meaning users must change their password every 42 days.
- ❑ **Minimum password age:** This defines the minimum number of days a password must be used before a user can change it. This prevents users from immediately changing their password multiple times to bypass the password history requirement. In your image, it's set to "**1 day**."
- ❑ **Minimum password length:** This sets the minimum number of characters required for a user's password. In your image, it's set to "**7 characters**."
- ❑ **Password must meet complexity requirements:** This setting, when enabled, enforces rules like requiring passwords to contain characters from three of the four categories (uppercase letters, lowercase letters, numbers, and symbols). In your image, it's "**Enabled**."
- ❑ **Store passwords using reversible encryption:** This setting determines whether the operating system stores passwords in a format that can be easily decrypted. It's almost always "**Disabled**" for security reasons, as it makes passwords more vulnerable if the system is compromised. In your image, it's correctly "**Disabled**."

Apply Group Policy in Domain Controller

GPO to Control Panel

- **User Configuration > Policies > Administrative Templates > Control Panel**
- **Prohibit access to Control Panel and PC settings**
- In the policy settings window, select the "**Enabled**" radio button.
- This setting will prevent users from launching Control Panel or the modern "PC settings" application

Apply Group Policy in Domain Controller

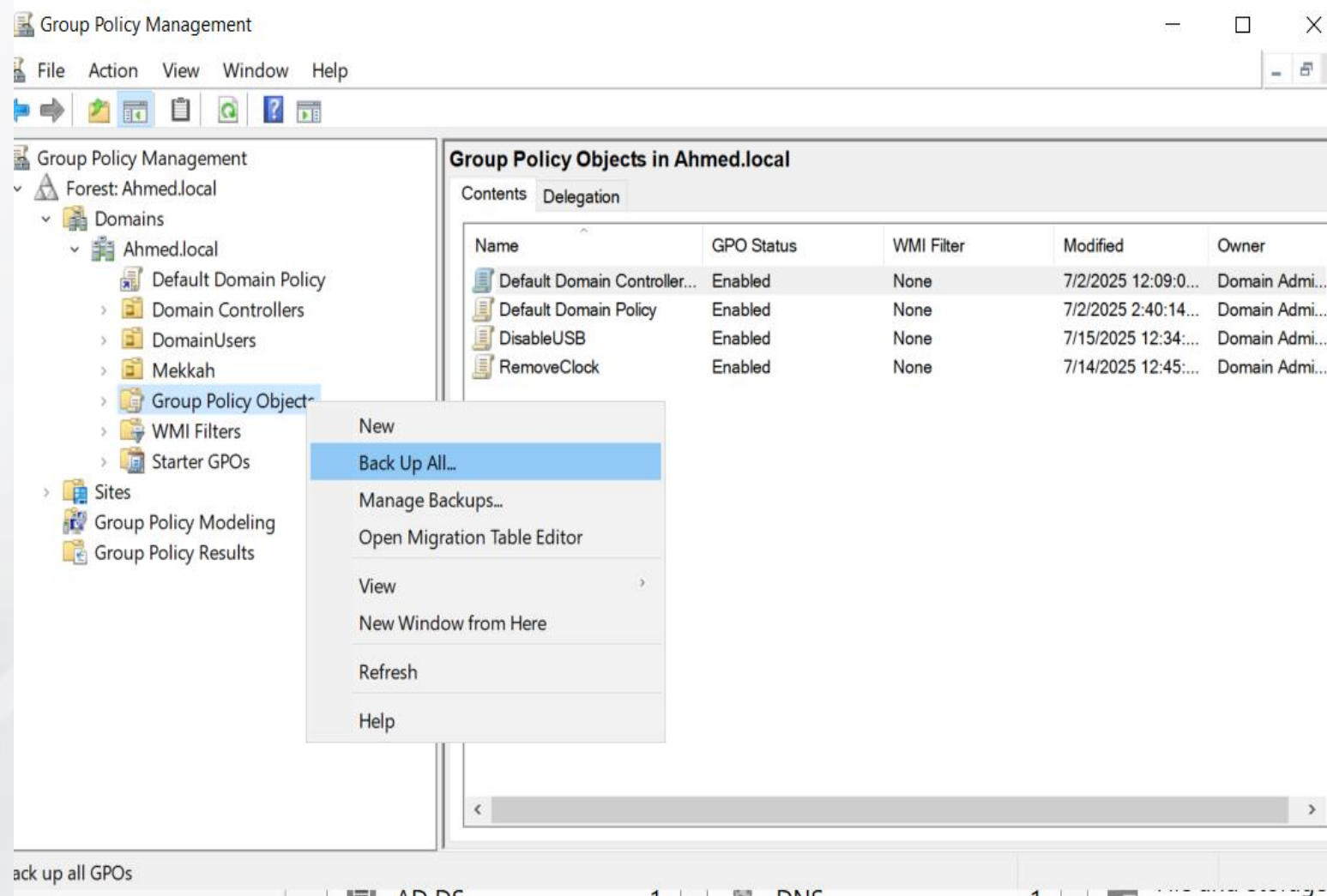
Backing Up GPOs

Right-click on the **"Group Policy Objects"**
Select **"Back Up All..."**

Chose Save Location

Restore Saved Backup

Right-click on the **"Group Policy Objects"**
Select **Manage Backups**



Default Group Policy Refresh Interval

The Group Policy **refresh interval** dictates how often client computers and users check for updates to Group Policy Objects (GPOs) from domain controllers. This is a crucial setting for how quickly policy changes propagate throughout your network.

By default, the refresh interval for **client computers** and users is:

- **90 minutes** (1 hour and 30 minutes)
- **A random offset** of up to 30 minutes is added to this interval.

For **Domain Controllers** the default refresh interval typically **5 minutes**, with a random offset of **0 minutes**

Default Group Policy Refresh Interval

How to Change the Group Policy Refresh Interval

Computer Configuration > Policies > Administrative Templates > System > Group Policy > "Set Group Policy refresh interval for computers"

User Configuration > Policies > Administrative Templates > System > Group Policy > "Set Group Policy refresh interval for users"

Set Group Policy refresh interval for computers

Previous Setting Next Setting

☐ Not Configured
☒ Enabled
☐ Disabled

Comment:

Supported on: At least Windows 2000

Options:

This setting allows you to customize how often Group Policy is applied to computers. The range is 0 to 44640 minutes (31 days).

Minutes: 90

This is a random time added to the refresh interval to prevent all clients from requesting Group Policy at the same time.

The range is 0 to 1440 minutes (24 hours)

Minutes: 30

Help:

This policy setting specifies how often Group Policy for computers is updated while the computer is in use (in the background). This setting specifies a background update rate only for Group Policies in the Computer Configuration folder.

In addition to background updates, Group Policy for the computer is always updated when the system starts.

By default, computer Group Policy is updated in the background every 90 minutes, with a random offset of 0 to 30 minutes.

If you enable this setting, you can specify an update rate from 0 to 64,800 minutes (45 days). If you select 0 minutes, the computer tries to update Group Policy every 7 seconds. However, because updates might interfere with users' work and increase network traffic, very short update intervals are not appropriate for most installations.

If you disable this setting, Group Policy is updated every 90 minutes (the default). To specify that Group Policy should never

Group Policy Refresh Interval

Considerations when Changing the Refresh Interval:

- **Impact on Network Traffic:** Shorter refresh intervals (e.g., every 15-30 minutes) can increase network traffic, especially in large environments with many clients.
- **Policy Propagation Speed:** Shorter intervals mean that policy changes will apply more quickly to client machines. This is often desired for security policies or urgent configurations.
- **Performance:** While modern systems handle GPO processing efficiently, extremely short intervals (like 7 seconds) can consume CPU cycles and network bandwidth unnecessarily.
- **Random Offset:** Always use a random offset. It's crucial for preventing "thundering herd" scenarios where all clients try to update at the exact same moment.

Summary

- ✓ **File Servers**
- ✓ **Practical Steps for Sharing Folders**
- ✓ **Group Policy**



Thank You