Active Directory

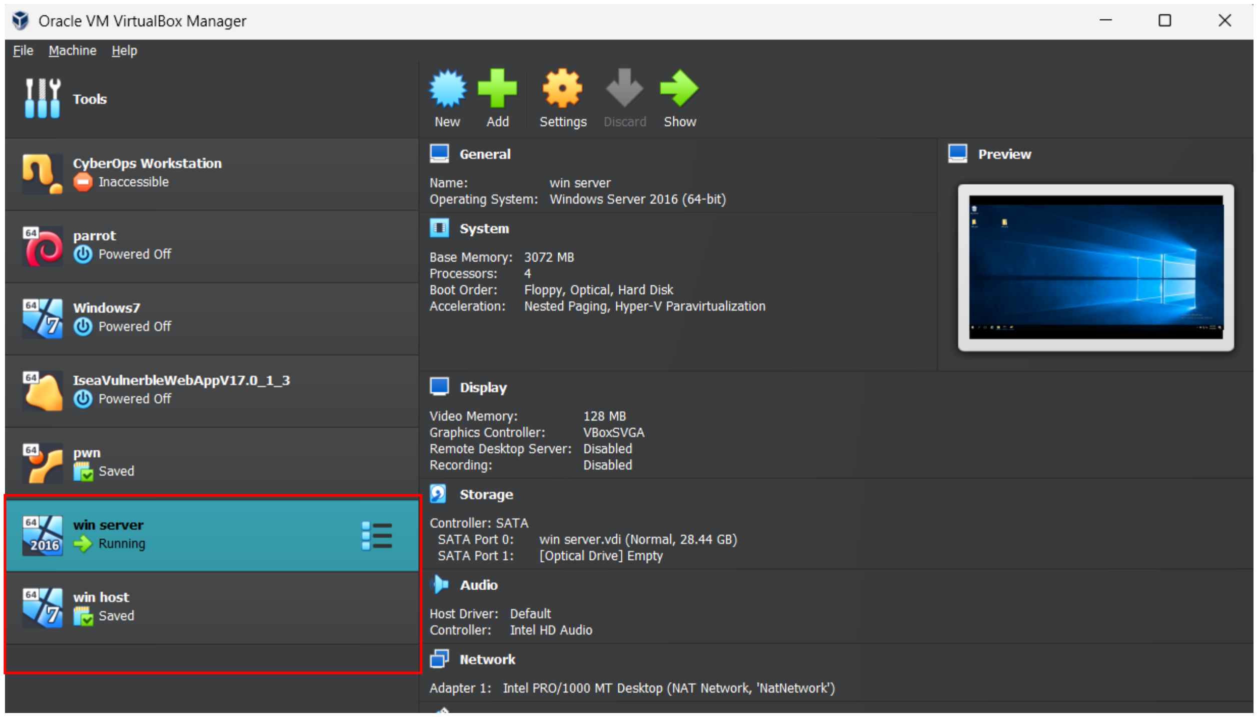
Author Wessam Alkhushman

DATE 16/5/2025

Table of Contents

Setting up the Active Directory Environment

I've already done the AD setup in windows server 2016 and setting up for it:



CyberOps Workstation
Inaccessible

parrot
Powered Off

Windows7
Powered Off

IseaVulnerbleWebAppV17.0_1_3
Powered Off

pwn
Saved

win server
Running

win host
Saved

General

Name: win server
Operating System: Windows Server 2016 (64-bit)

System

Base Memory: 3072 MB
Processors: 4
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, Hyper-V Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: SATA
SATA Port 0: win server.vdi (Normal, 28.44 GB)
SATA Port 1: [Optical Drive] Empty

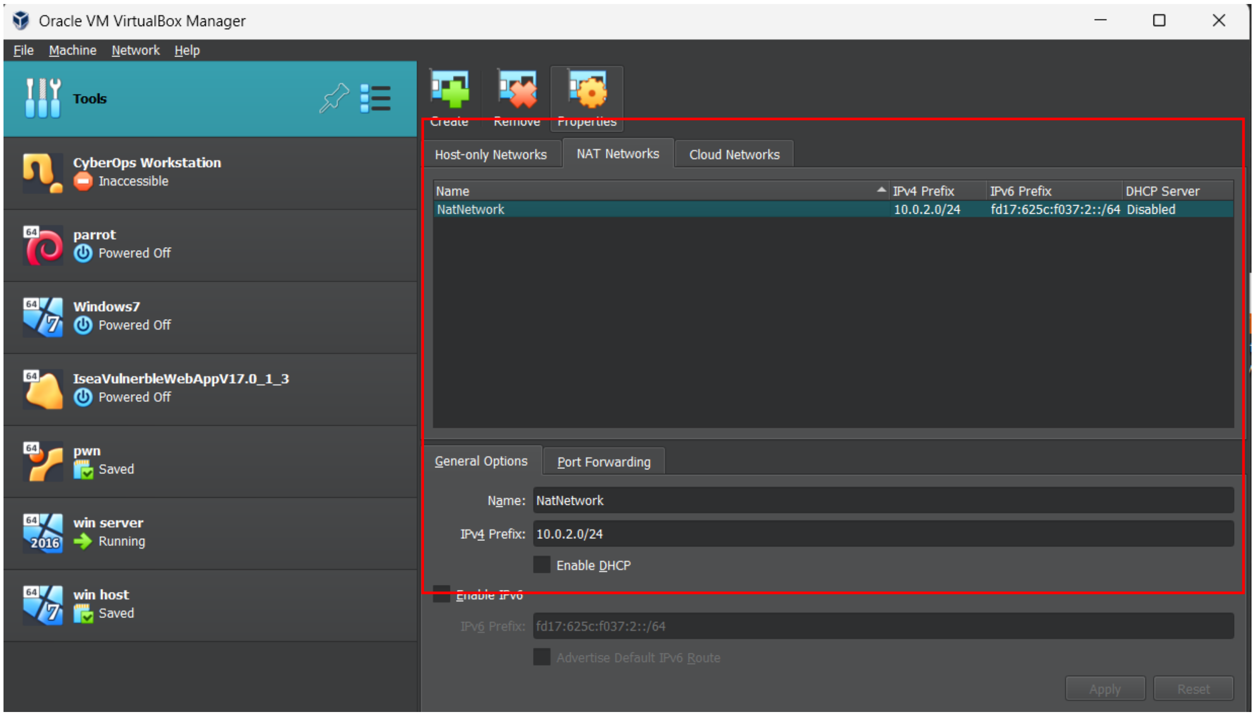
Audio

Host Driver: Default
Controller: Intel HD Audio

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT Network, 'NatNetwork')

And setting up the network for the machine:



CyberOps Workstation
Inaccessible

parrot
Powered Off

Windows7
Powered Off

IseaVulnerbleWebAppV17.0_1_3
Powered Off

pwn
Saved

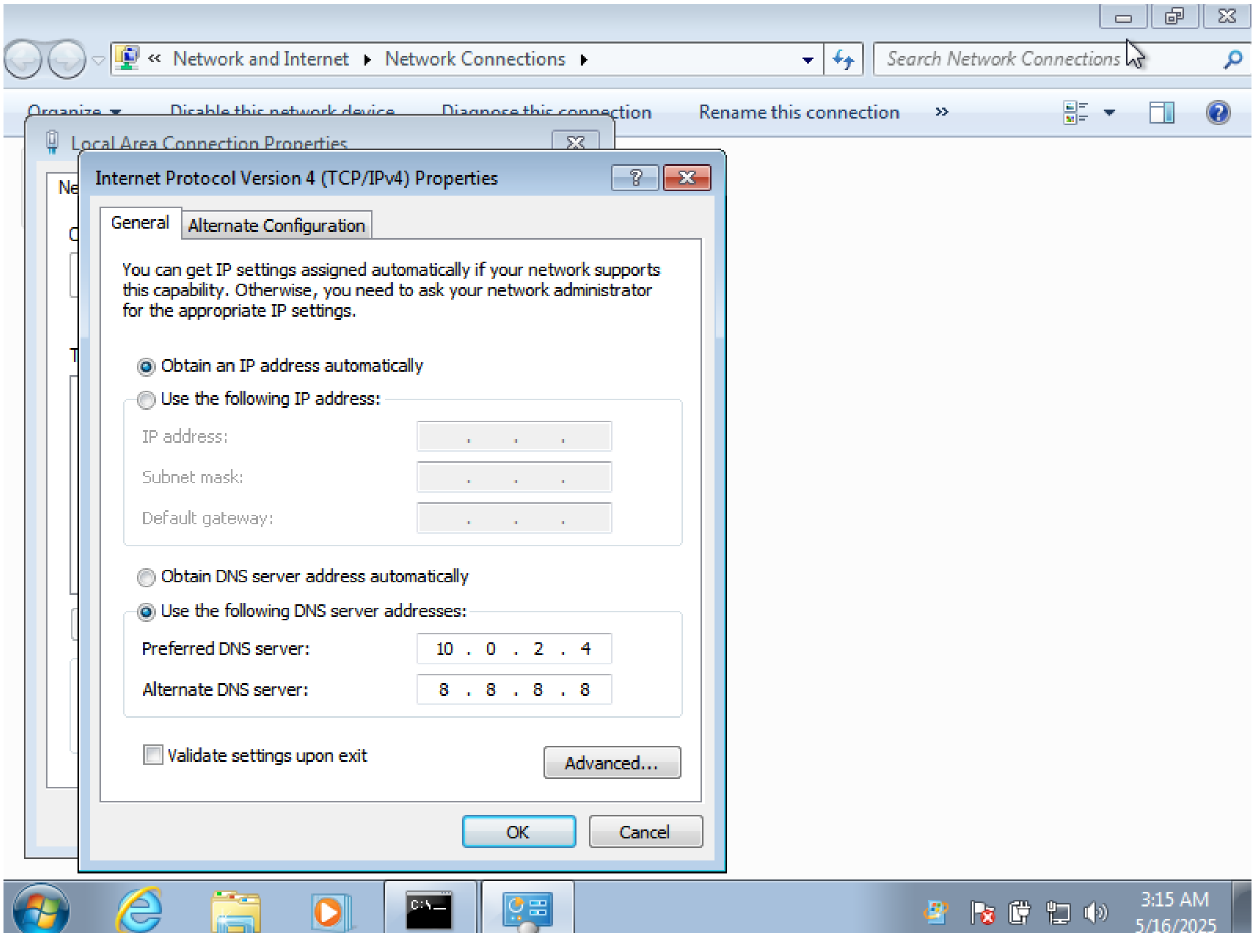
win server
Running

win host
Saved

Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
NatNetwork	10.0.2.0/24	fd17:625c:f037:2::/64	Disabled

Name: NatNetwork
IPv4 Prefix: 10.0.2.0/24
□ Enable DHCP
□ Enable IPv6
IPv6 Prefix: fd17:625c:f037:2::/64
□ Advertise Default IPv6 Route

Setting up machine to join a domain and give it DNS:


« Network and Internet ▸ Network Connections ▸
Search Network Connections
Organize ▾
Disable this network device
Diagnose this connection
Rename this connection
»
Local Area Connection Properties
3:15 AM
5/16/2025

Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

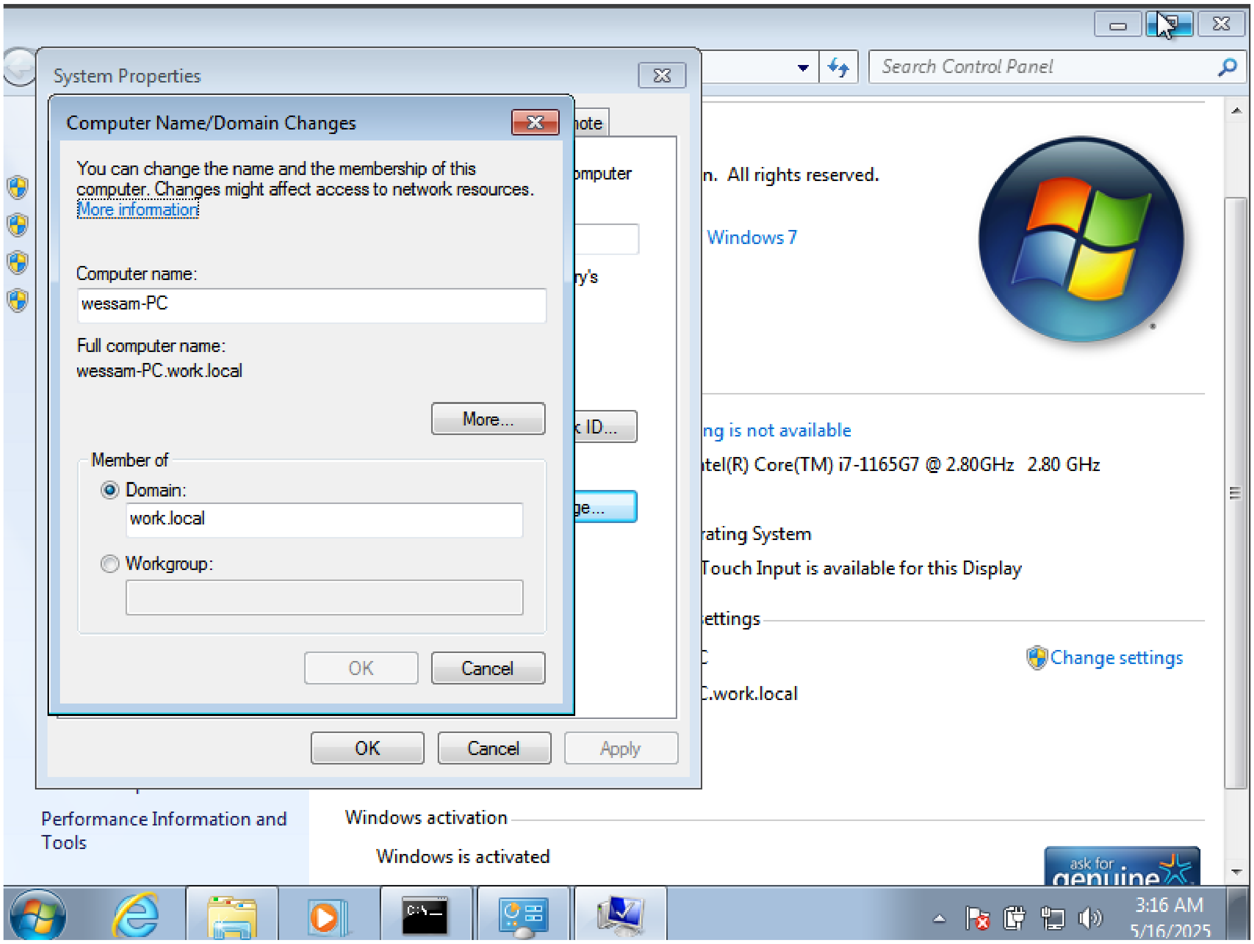
Preferred DNS server: 10 . 0 . 2 . 4

Alternate DNS server: 8 . 8 . 8 . 8

□ Validate settings upon exit

Advanced...

OK Cancel



System Properties

Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources. More information

Computer name:

wessam-PC

Full computer name:

wessam-PC.work.local

More...

Member of

● Domain:

work.local

○ Workgroup:

OK Cancel

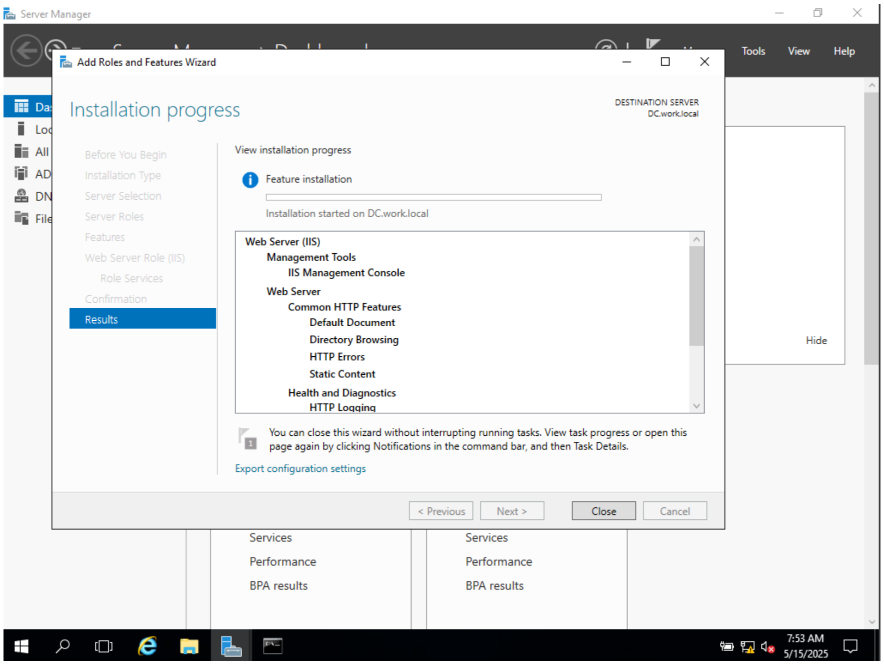
OK Cancel Apply

And, I installed the required services in the Same server such as DC server, DHCP Server, DNS Server and IIS Server:

Note: I've already setting up a DC and DNS server.

In server manager and in "configure this local server" scope, go to "Add roles and features" to install the required services :

1- IIS Server => select the server roles and choose the IIS and go next, and I've added authentication role feature :



Installation progress

DESTINATION SERVER
DC.work.local

View installation progress

Feature installation

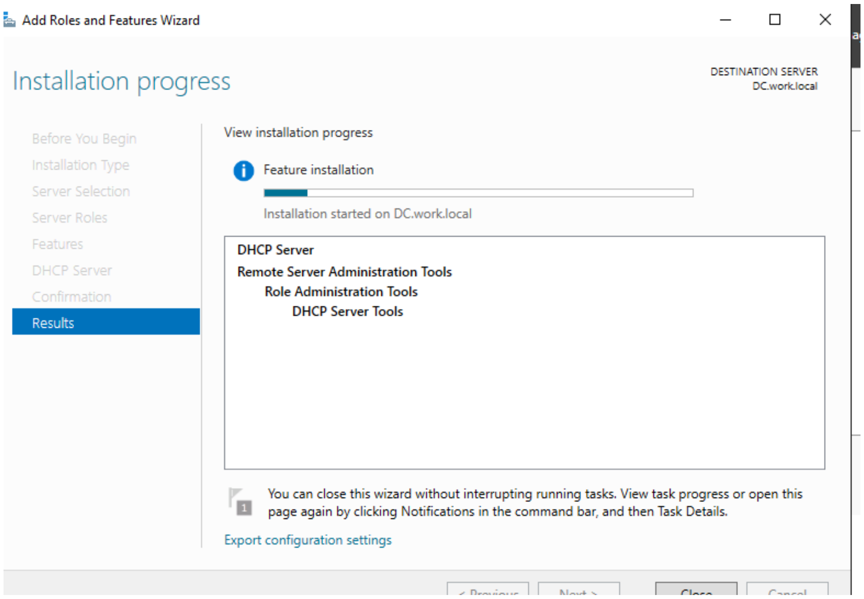
Installation started on DC.work.local

Web Server (IIS)
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
Health and Diagnostics
HTTP Logging

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

2- DHCP Server =>I've done same thing in IIS without add feature:



Installation progress

DESTINATION SERVER
DC.work.local

View installation progress

Feature installation

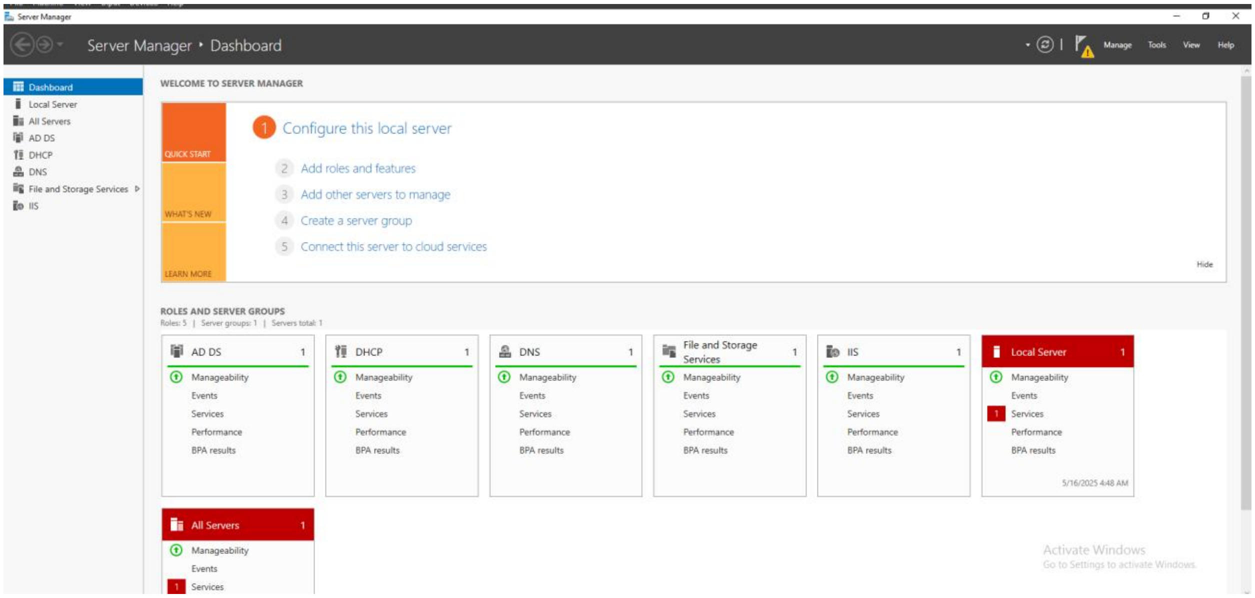
Installation started on DC.work.local

DHCP Server
Remote Server Administration Tools
Role Administration Tools
DHCP Server Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

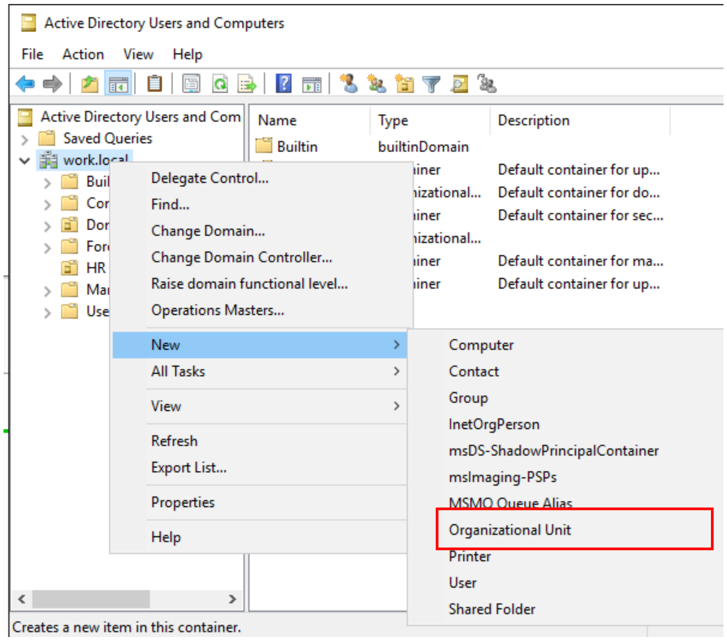
This is a serves I've done it.



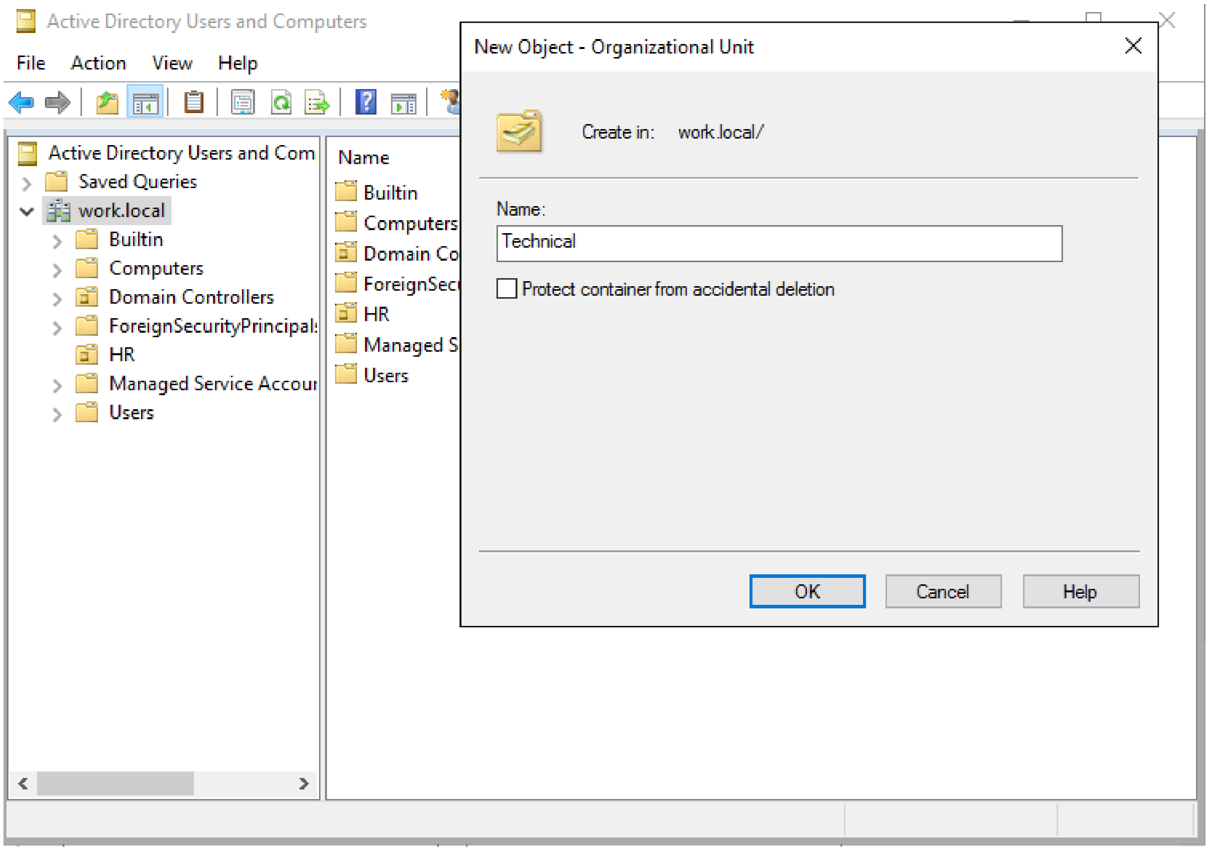
User and OU Management

I've Create four domain accounts and I added two (own and saif) to an OU named "HR" and the other two (wessam and ahmad) to an OU named "Technical":

First, I've create a OU's for HR then Technical :



Then, choose name for OU .



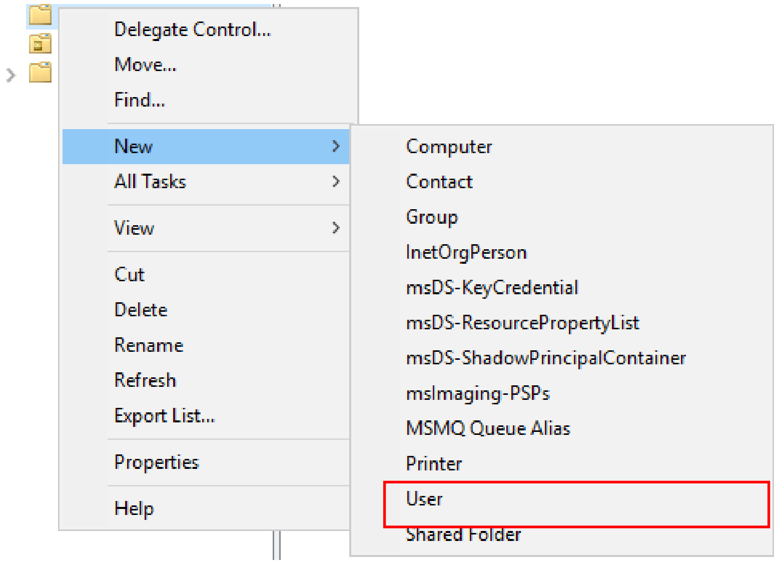
Create in: work.local/

Name:
Technical

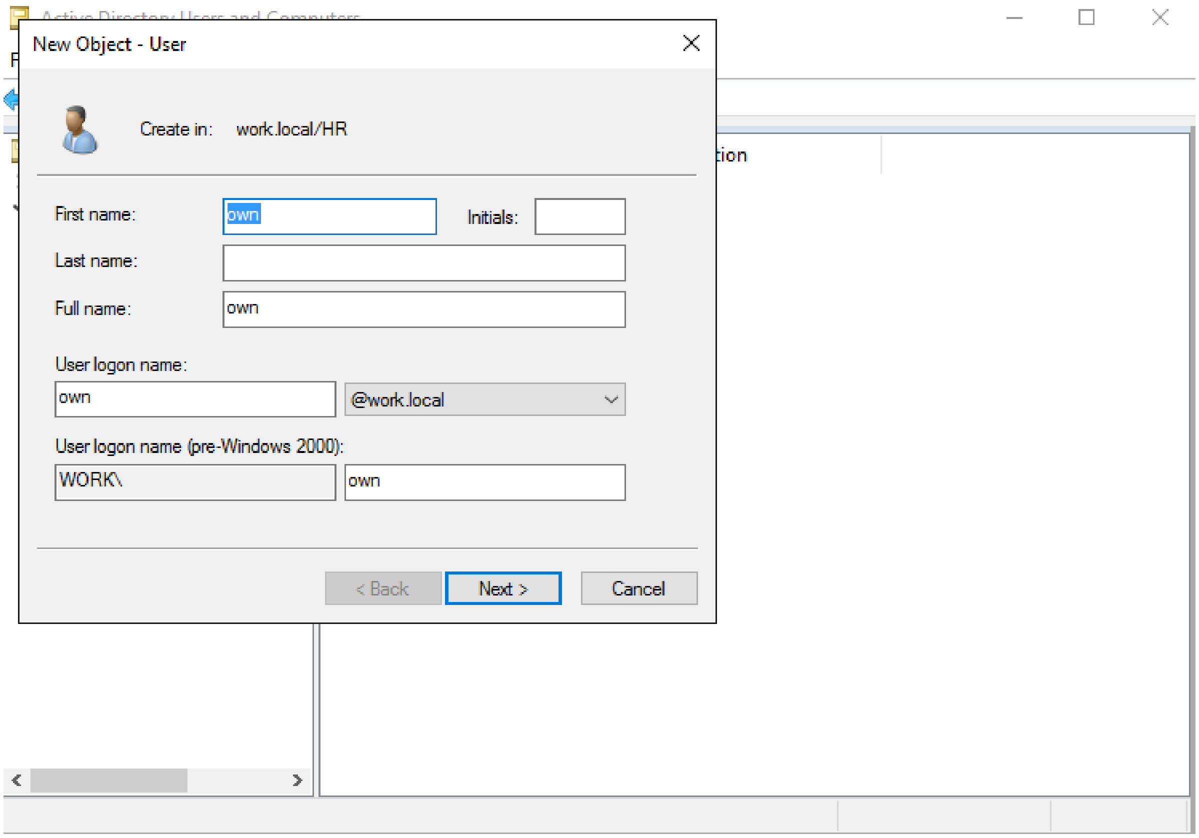
□ Protect container from accidental deletion

Same steps I use for create HR .

Then, I create an new user for units ,two for each unit.



Then, choose name and domain :



New Object - User

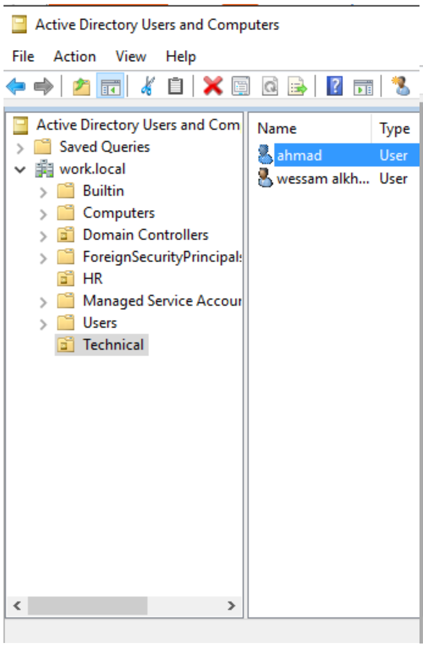
Create in: work.local/HR

First name:	own
Initials:	
Last name:	
Full name:	own

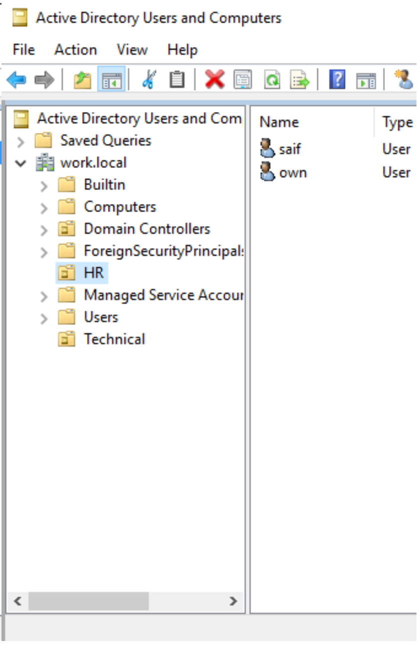
User logon name: own @work.local

User logon name (pre-Windows 2000): WORK\ own

Thes steps for creating all user.



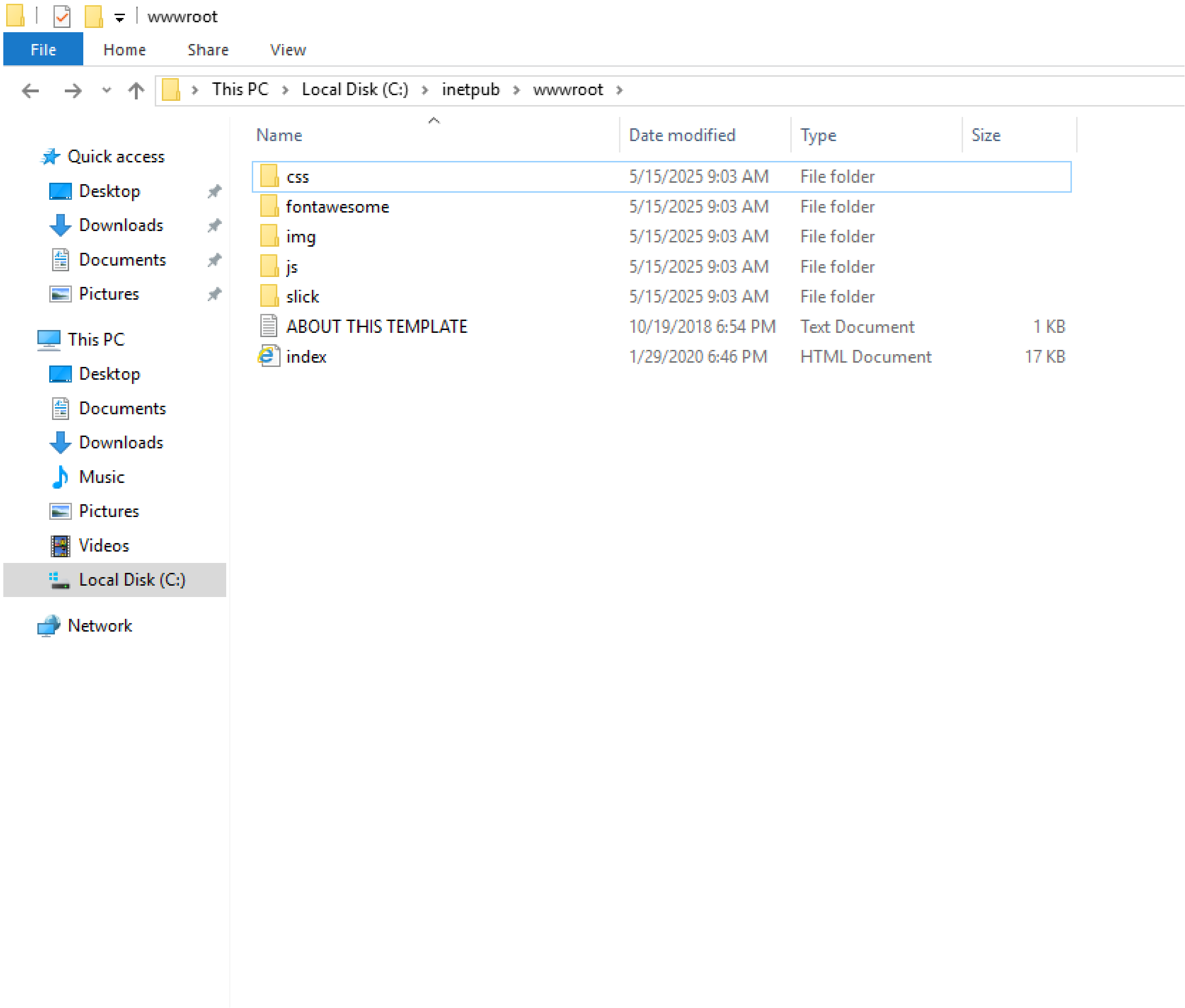
Name	Type
ahmad	User
wessam alkh...	User



Name	Type
saif	User
own	User

Website Hosting

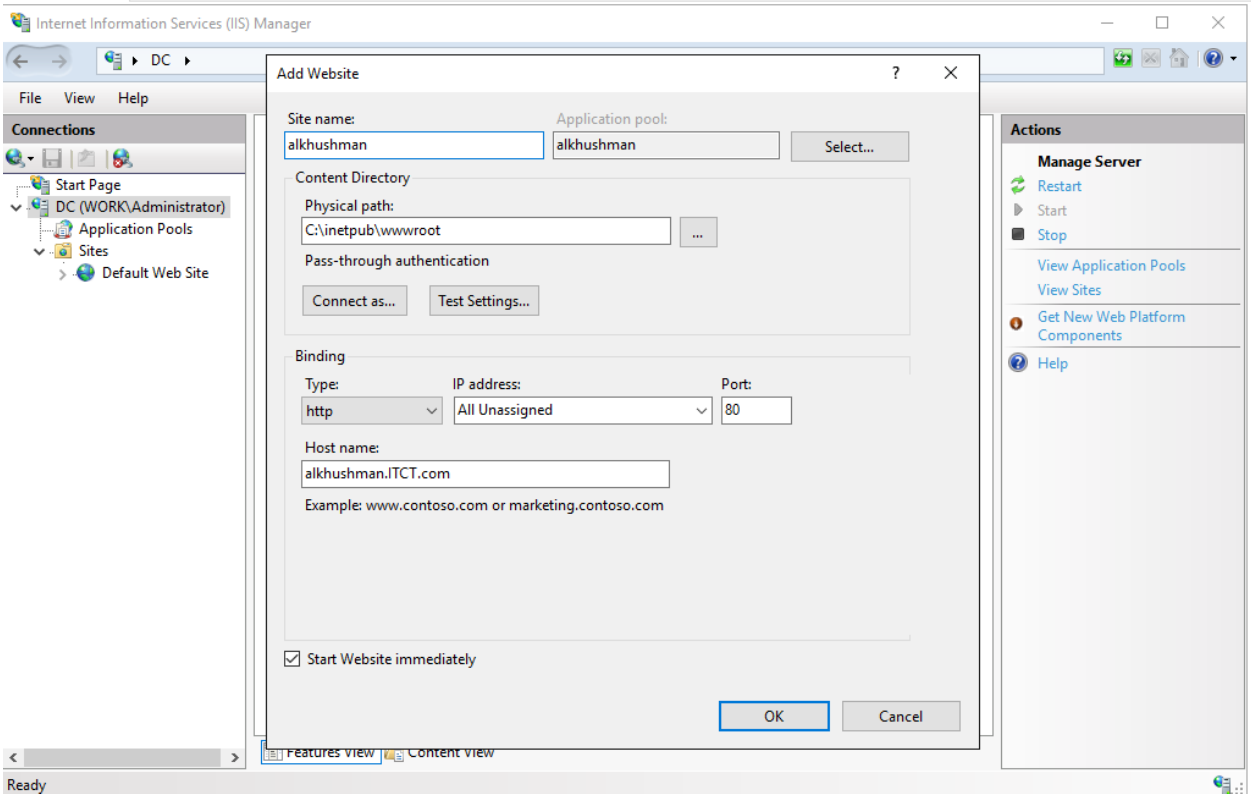
After install IIS, I install template for website and put it in this path :



This PC › Local Disk (C:) › inetpub › wwwroot ›

Name	Date modified	Type	Size
css	5/15/2025 9:03 AM	File folder	
fontawesome	5/15/2025 9:03 AM	File folder	
img	5/15/2025 9:03 AM	File folder	
js	5/15/2025 9:03 AM	File folder	
slick	5/15/2025 9:03 AM	File folder	
ABOUT THIS TEMPLATE	10/19/2018 6:54 PM	Text Document	1 KB
index	1/29/2020 6:46 PM	HTML Document	17 KB

Then, I configure this server to accept and run this website :



Add Website

Site name: alkhushman

Application pool: alkhushman

Select...

Content Directory

Physical path: C:\inetpub\wwwroot

Pass-through authentication

Connect as... Test Settings...

Binding

Type: http

IP address: All Unassigned

Port: 80

Host name: alkhushman.ITCT.com

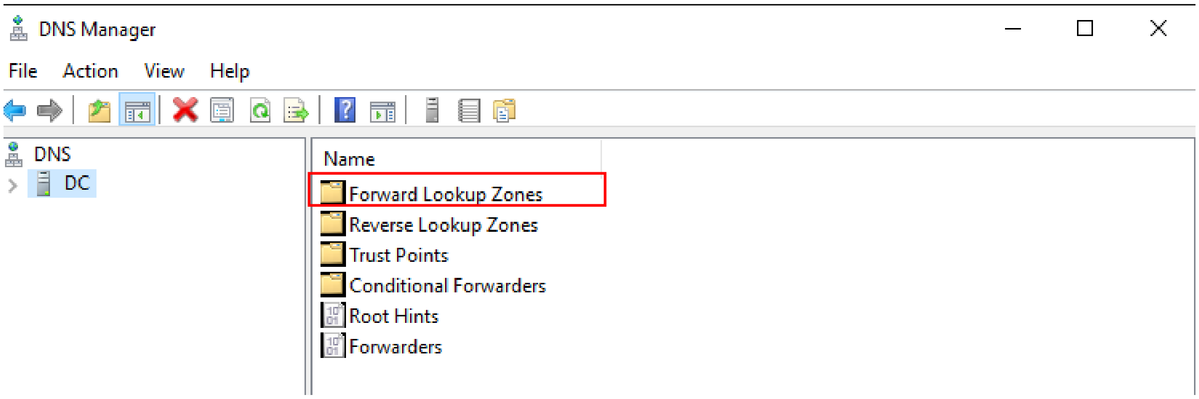
Example: www.contoso.com or marketing.contoso.com

☑ Start Website immediately

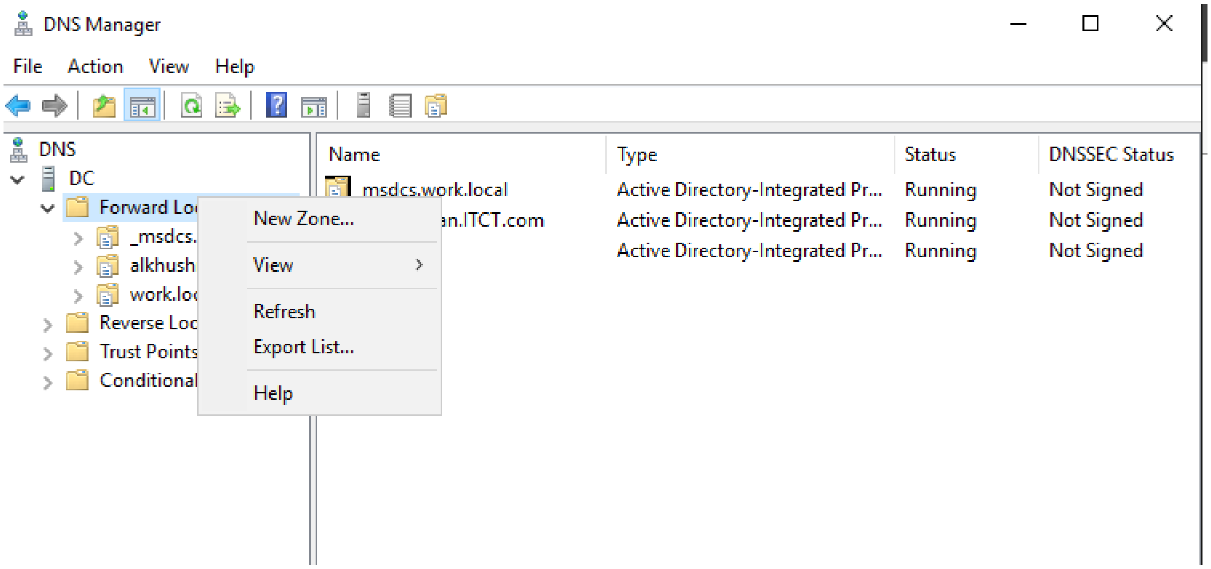
OK Cancel

Configuration DNS server

I've insert the host name and IP address for server to enable DNS:

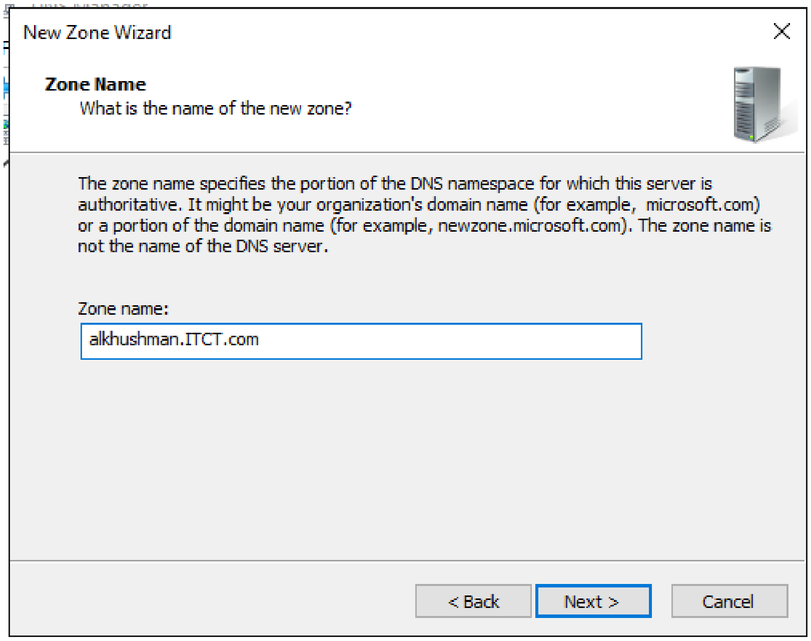


In Forward Lookup Zones ,I've created a new zone and configure it .



Name	Type	Status	DNSSEC Status
msdcs.work.local	Active Directory-Integrated Pr...	Running	Not Signed
...n.ITCT.com	Active Directory-Integrated Pr...	Running	Not Signed
	Active Directory-Integrated Pr...	Running	Not Signed

Then set name of zone:

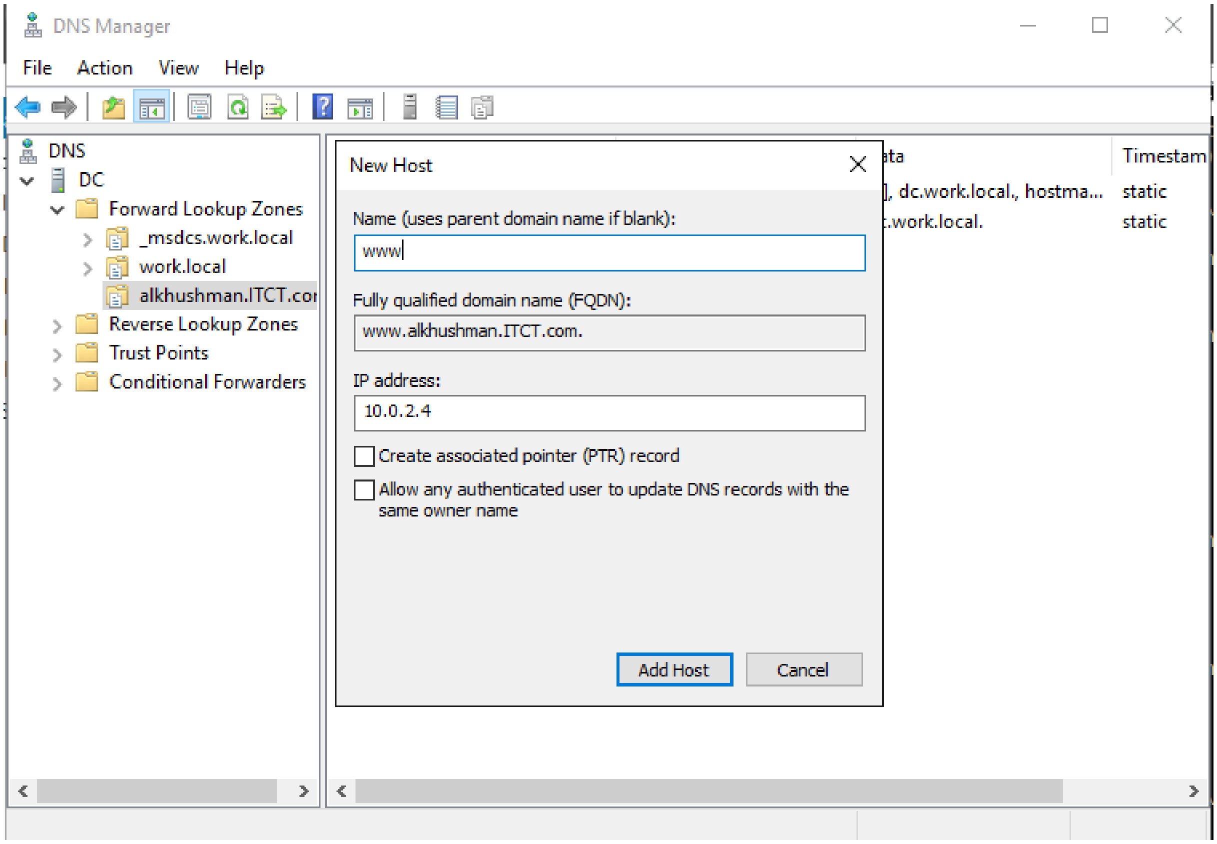


Zone Name
What is the name of the new zone?

The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name: alkhushman.ITCT.com

Then , I've createda new host and configer it:



New Host

Name (uses parent domain name if blank):

www

Fully qualified domain name (FQDN):

www.alkhushman.ITCT.com.

IP address:

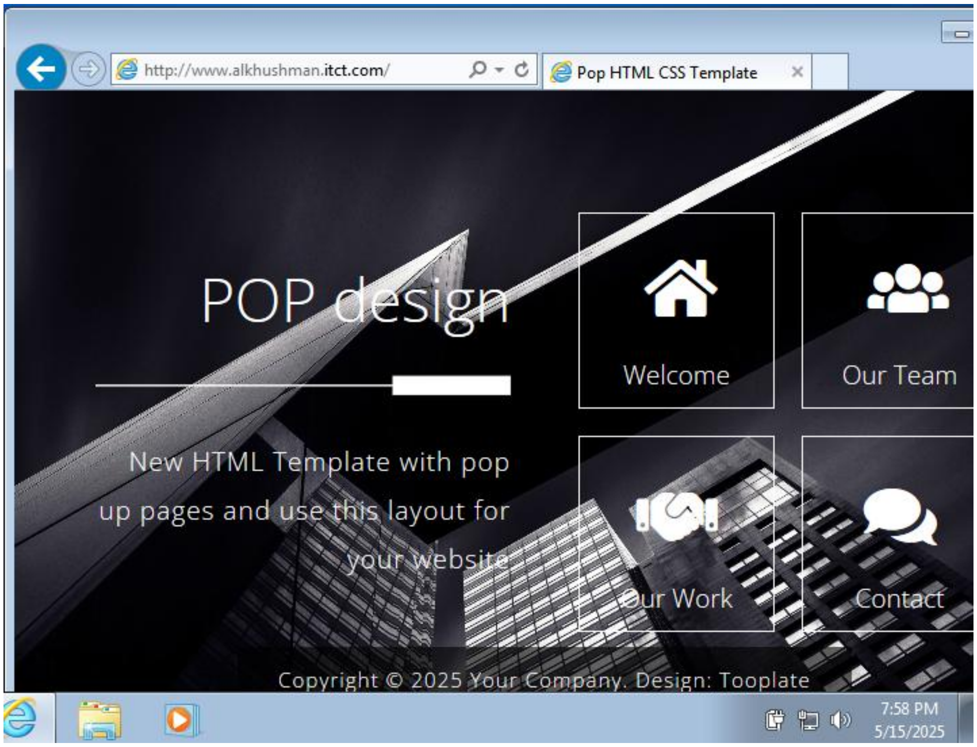
10.0.2.4

□ Create associated pointer (PTR) record

□ Allow any authenticated user to update DNS records with the same owner name

Add Host | Cancel

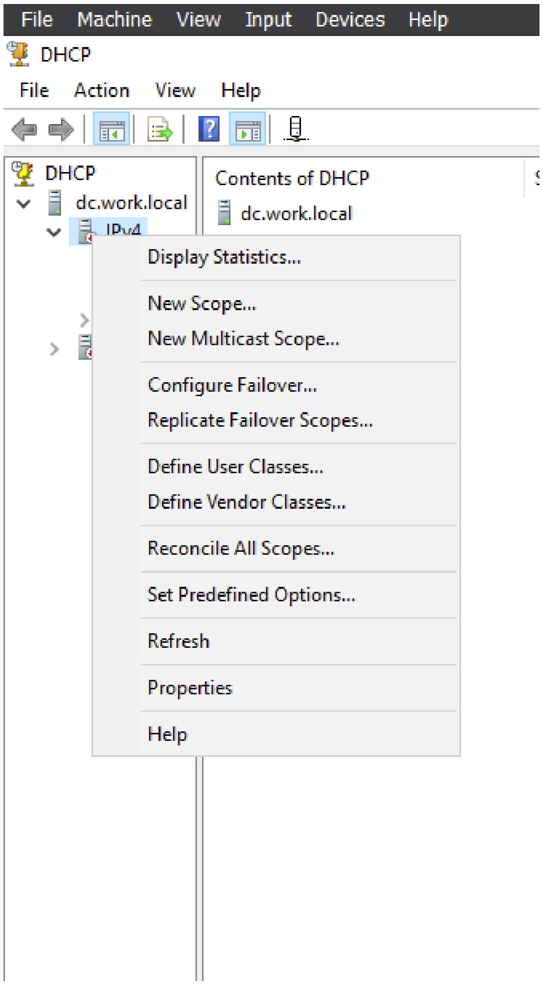
Finaly, this is website in windows that use for user:



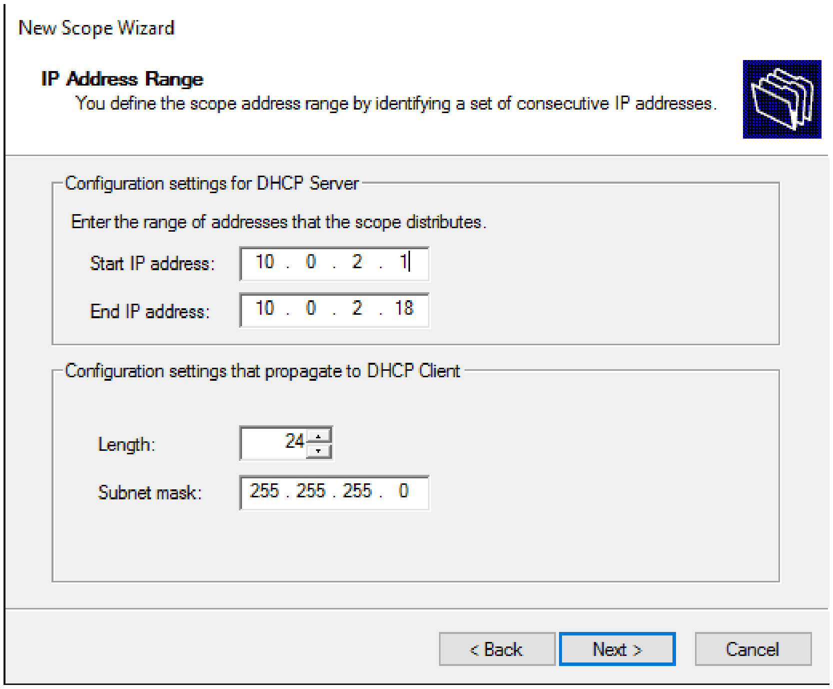
http://www.alkhushman.itct.com/
Pop HTML CSS Template
POP design
New HTML Template with pop up pages and use this layout for your website
Welcome
Our Team
Our Work
Contact
Copyright © 2025 Your Company. Design: Tooplate
7:58 PM
5/15/2025

Configure DHCP Server

After installing the DHCP server in windows server, I've Set up the DHCP Server and configure it and Create a DHCP pool with a subnet similar to the DC subnet .



I've created a new scope and set start, end IP address and subnet mask:



New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 10 . 0 . 2 . 1

End IP address: 10 . 0 . 2 . 18

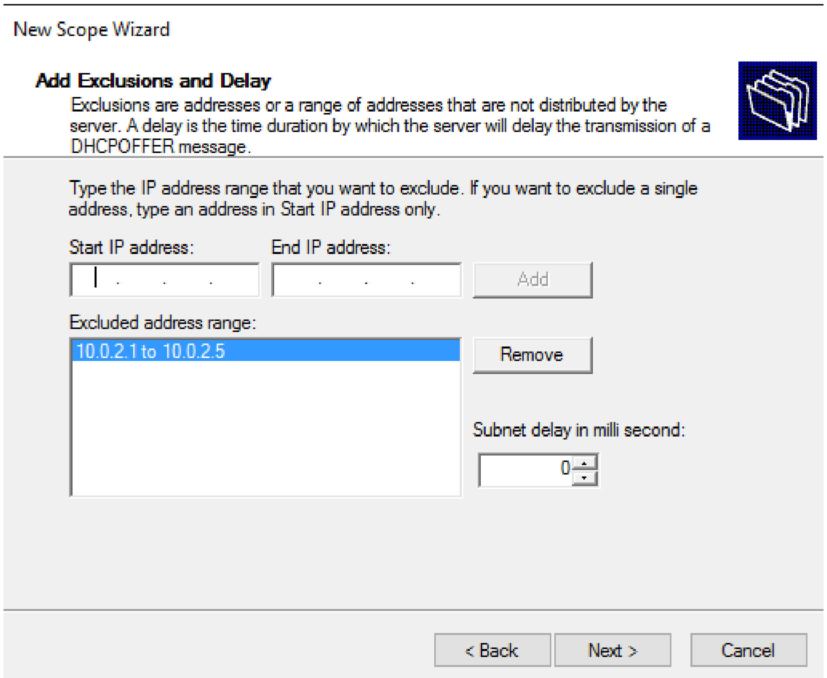
Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

Then, I've added exclusions IP's range:

Note: I've been Excluded address range for first five IP's.



New Scope Wizard

Add Exclusions and Delay

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCPOFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: . . .

End IP address: . . .

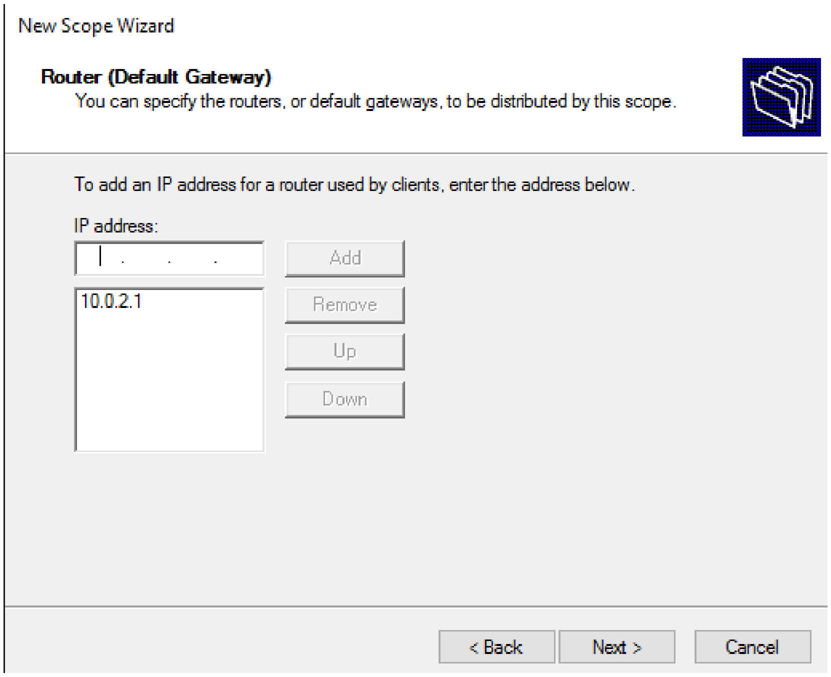
Excluded address range:

10.0.2.1 to 10.0.2.5

Subnet delay in milli second: 0

Then, added IP Address for Router(Default Gateway):

Note: this is the last step in creating a scope.



New Scope Wizard

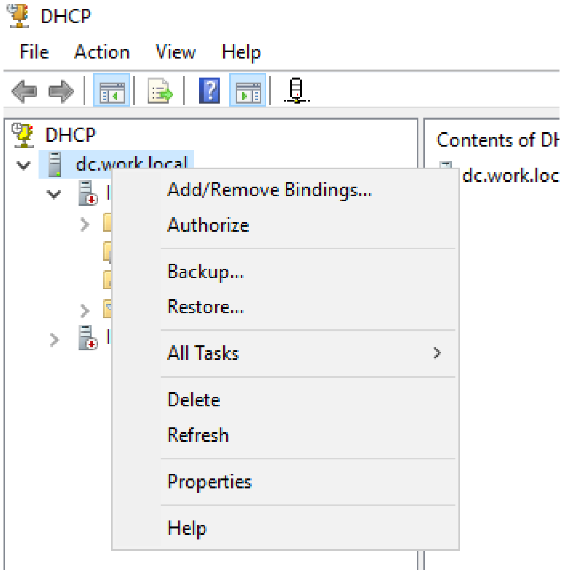
Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

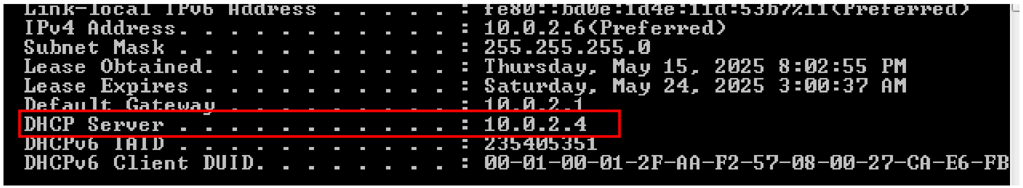
IP address:

10.0.2.1

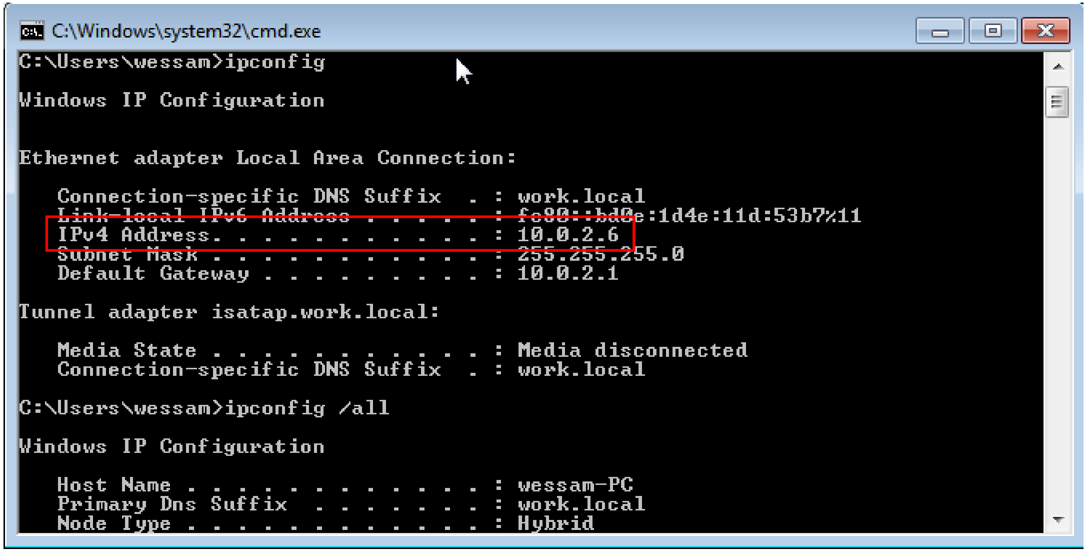
Then checked on Authorize.



Allow Windows machines (Clients) to request IP Addresses automatically:



```
   Link-local IPv6 Address . . . . . : fe80::bd0e:1d4e:11d:53b7%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.2.6(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, May 15, 2025 8:02:55 PM
   Lease Expires . . . . . . . . . . : Saturday, May 24, 2025 3:00:37 AM
   Default Gateway . . . . . . . . . : 10.0.2.1
   DHCP Server . . . . . . . . . . . : 10.0.2.4
   DHCPv6 IAID . . . . . . . . . . . : 235405351
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2F-AA-F2-57-08-00-27-CA-E6-FB
```



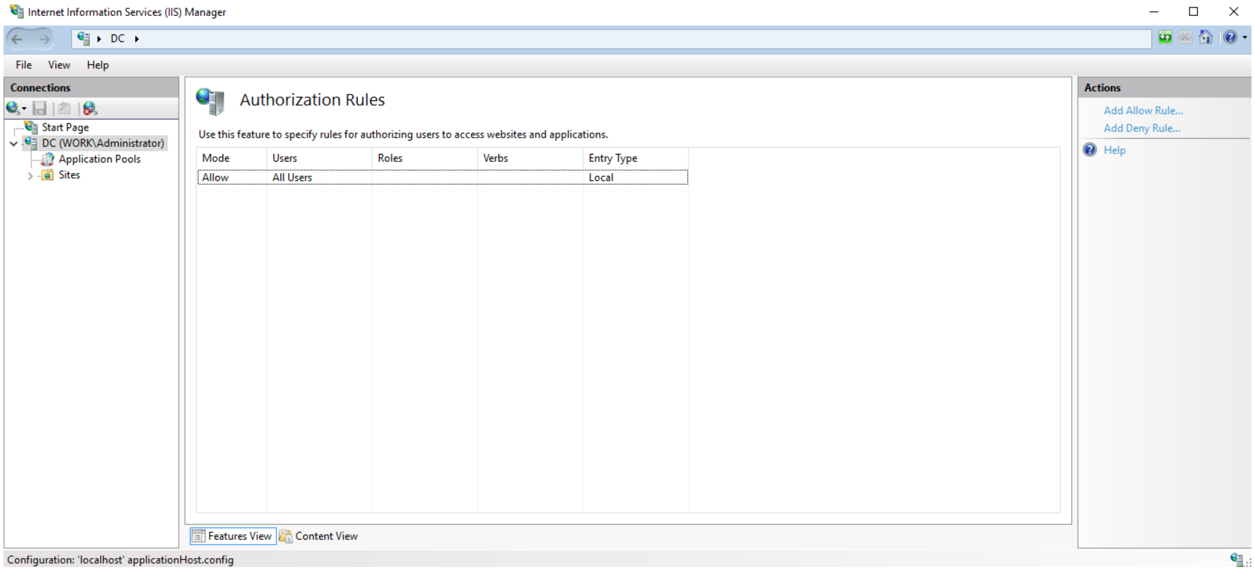
```
C:\Users\wessam>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : work.local
   Link-local IPv6 Address . . . . . : fe80::bd0e:1d4e:11d:53b7%11
   IPv4 Address. . . . . . . . . . . : 10.0.2.6
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1

Tunnel adapter isatap.work.local:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : work.local

C:\Users\wessam>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : wessam-PC
   Primary Dns Suffix  . . . . . . . : work.local
   Node Type . . . . . . . . . . . . : Hybrid
```

The machine has taken the IP Address from DHCP server.

Group Policy and Access Control

BLOCK HR EMPLOYEES FROM ACCESSING THE WEBSITE (INTENDED ONLY FOR THE TECHNICAL TEAM).

I mentioned earlier that I've added feature called "authentication" in role feature, It's time to use it



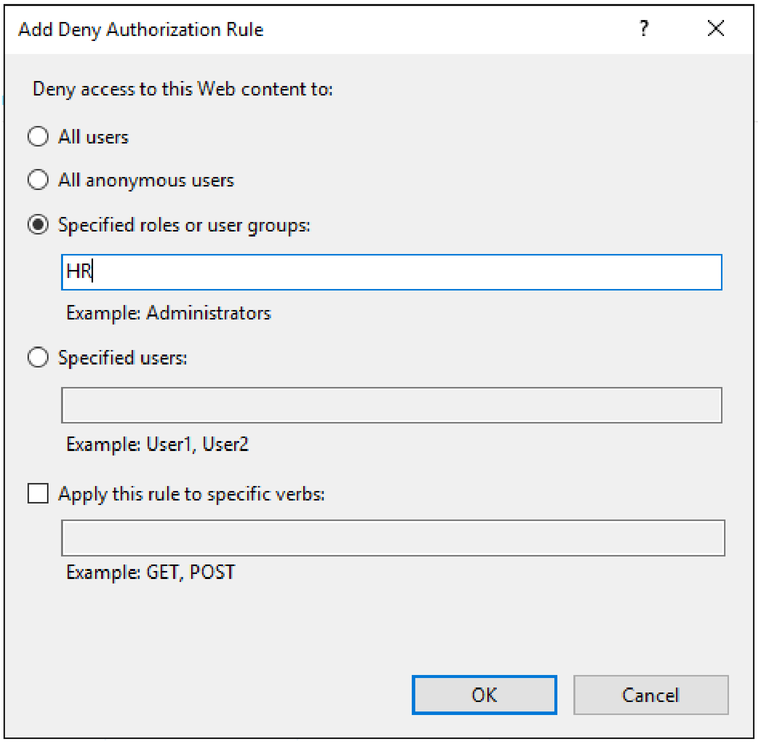
Authorization Rules

Use this feature to specify rules for authorizing users to access websites and applications.

Mode	Users	Roles	Verbs	Entry Type
Allow	All Users			Local

Configuration: 'localhost' applicationHost.config

In actions tab, I've added deny rule to prevent HR access to website:



Add Deny Authorization Rule

Deny access to this Web content to:

○ All users

○ All anonymous users

● Specified roles or user groups:

HR

Example: Administrators

○ Specified users:

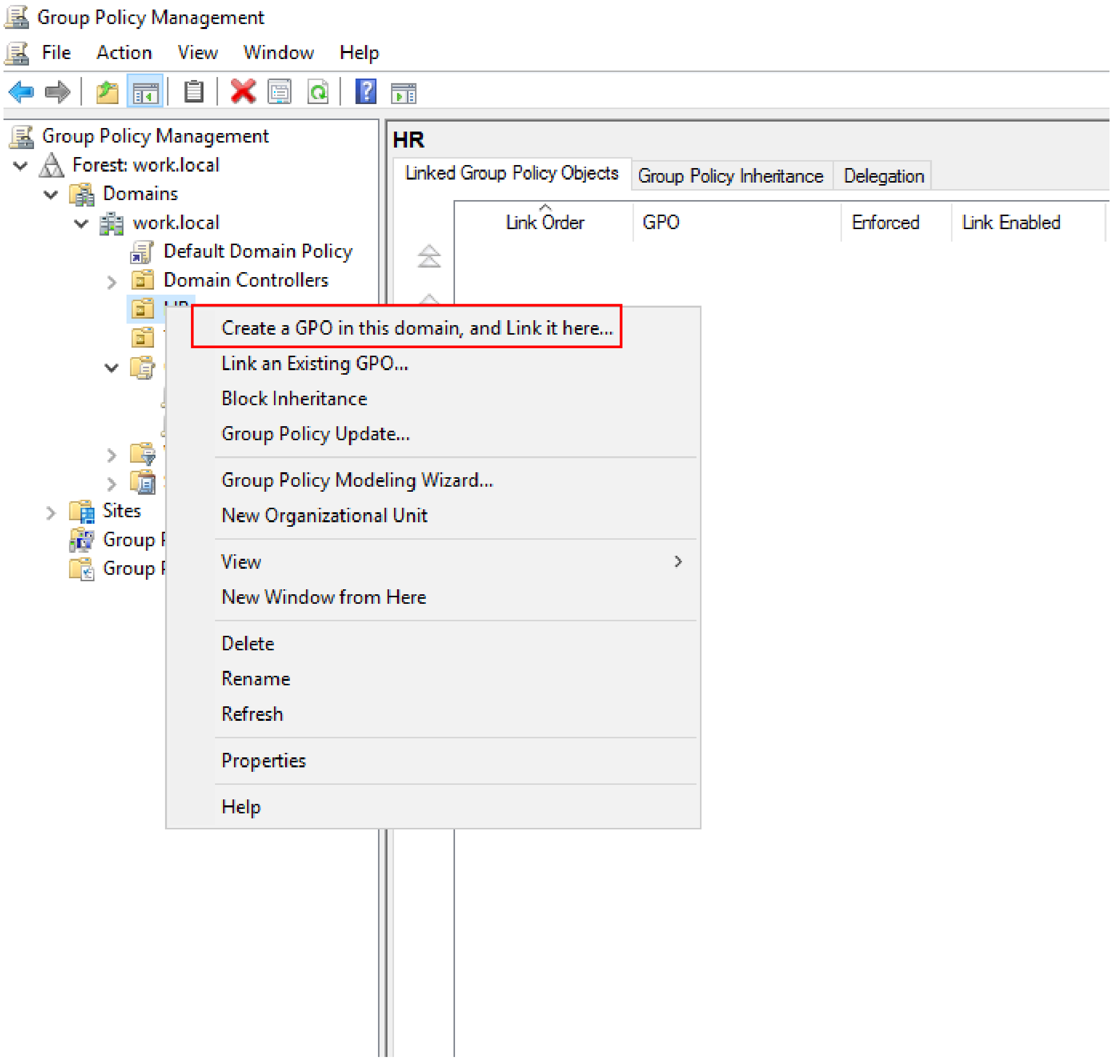
Example: User1, User2

□ Apply this rule to specific verbs:

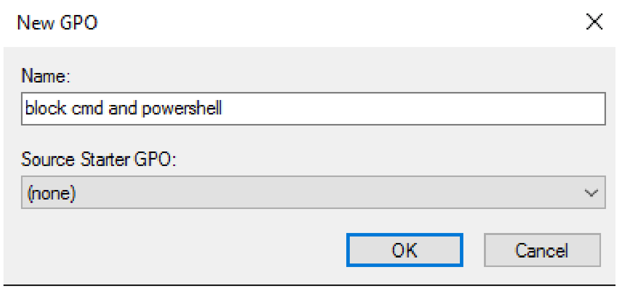
Example: GET, POST

Prevent HR employees from running PowerShell and CMD.

In Group Policy Management, I've created a GPO for HR only:



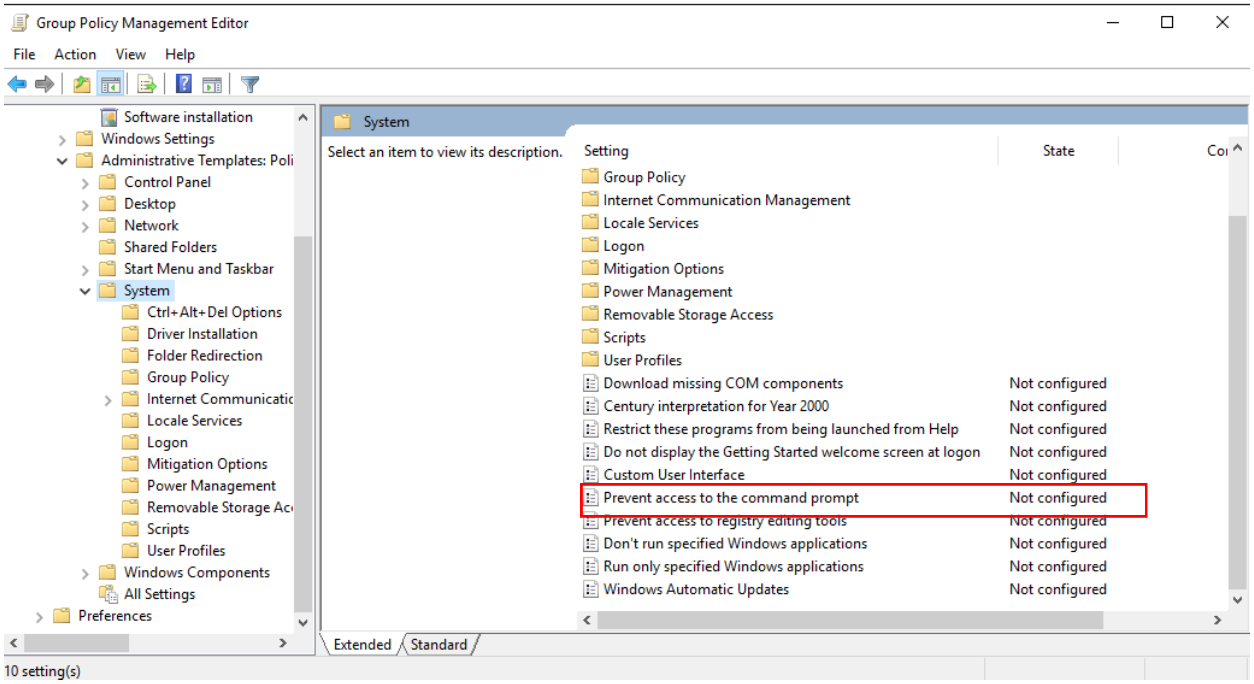
Then, set a name for it:



Name:
block cmd and powershell

Source Starter GPO:
(none)

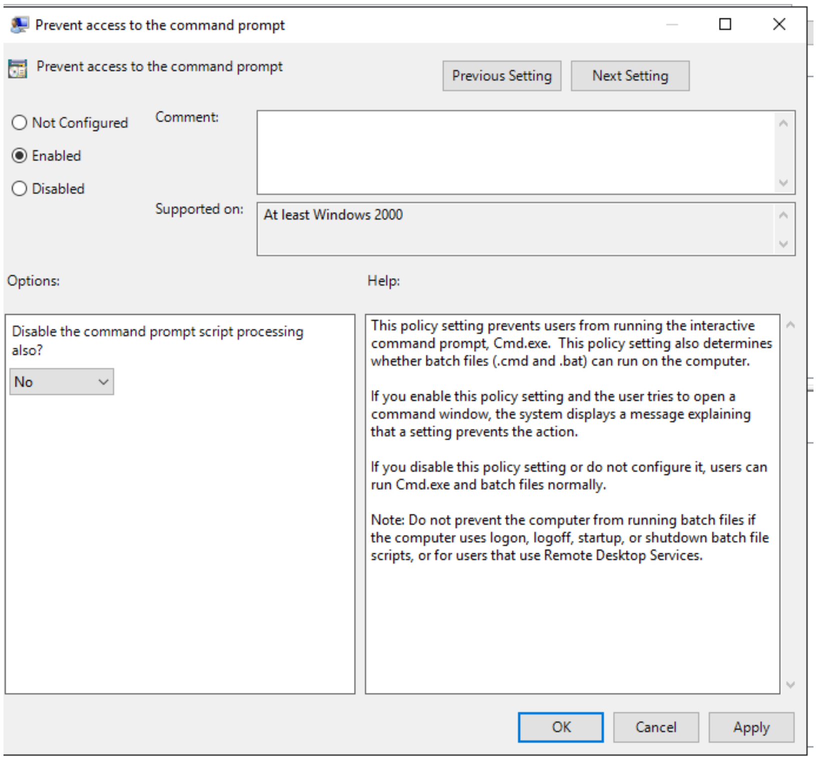
Then, I've Edit that GPO and search for the policy that prevent cmd or powrshell in user config...=>Administrative templates ...=>system



Setting	State
Group Policy	
Internet Communication Management	
Locale Services	
Logon	
Mitigation Options	
Power Management	
Removable Storage Access	
Scripts	
User Profiles	
Download missing COM components	Not configured
Century interpretation for Year 2000	Not configured
Restrict these programs from being launched from Help	Not configured
Do not display the Getting Started welcome screen at logon	Not configured
Custom User Interface	Not configured
Prevent access to the command prompt	Not configured
Prevent access to registry editing tools	Not configured
Don't run specified Windows applications	Not configured
Run only specified Windows applications	Not configured
Windows Automatic Updates	Not configured

10 setting(s)

Then, Enable it.



Prevent access to the command prompt

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 2000

Options:

Disable the command prompt script processing also? No

Help:

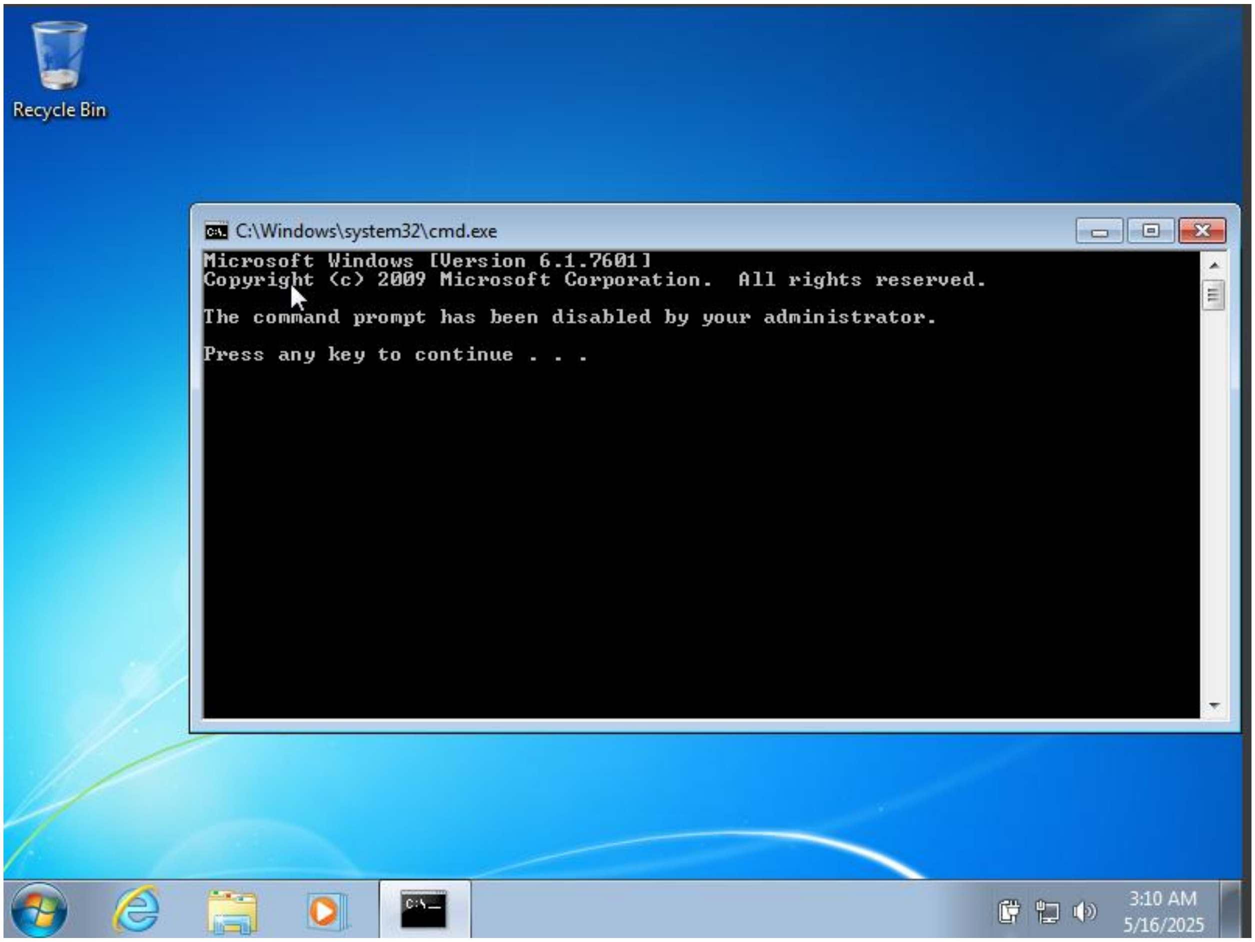
This policy setting prevents users from running the interactive command prompt, Cmd.exe. This policy setting also determines whether batch files (.cmd and .bat) can run on the computer.

If you enable this policy setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.

If you disable this policy setting or do not configure it, users can run Cmd.exe and batch files normally.

Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Remote Desktop Services.

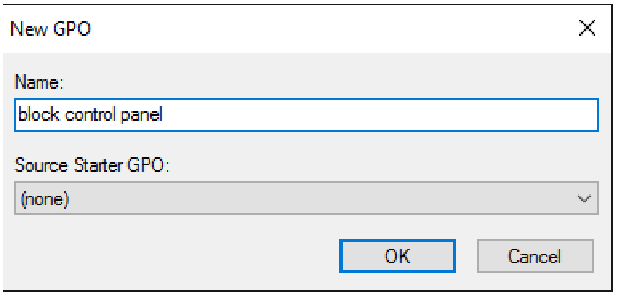
When I try to access to cmd I found this:



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

The command prompt has been disabled by your administrator.

Press any key to continue . . .
```

Prevent all employees from accessing the Control Panel.

In Group Policy Management, I've created a GPO in domain:



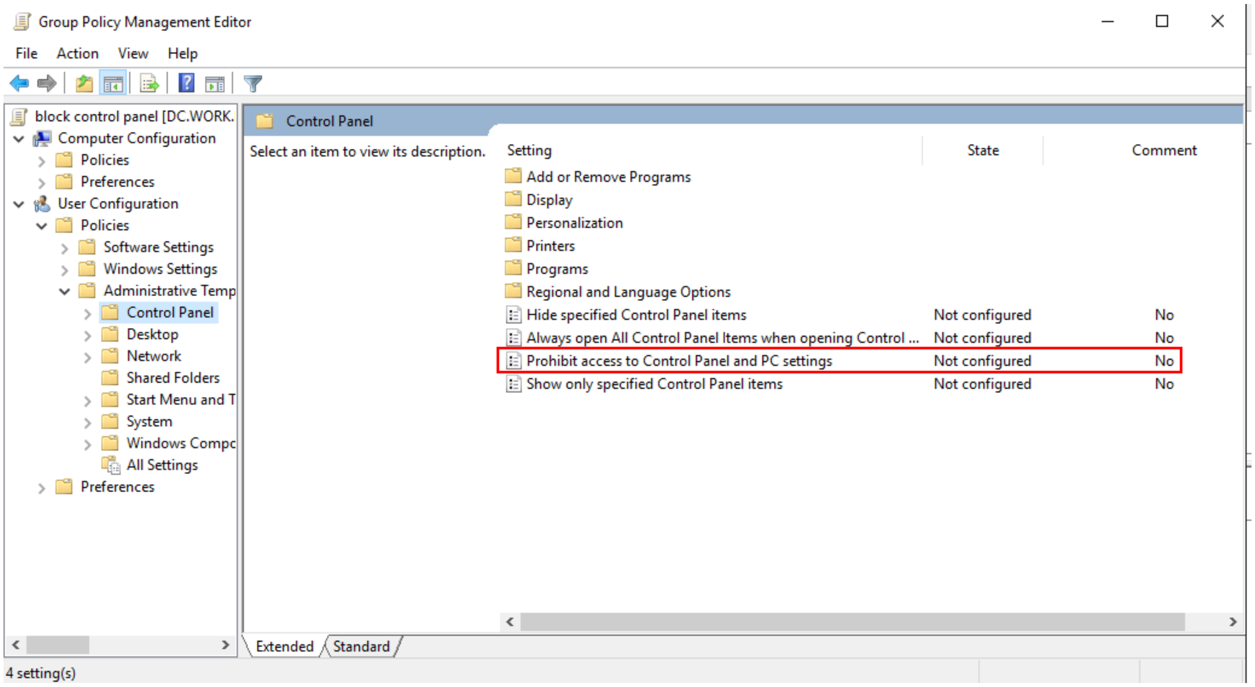
New GPO

Name: block control panel

Source Starter GPO: (none)

Then, set a name for it.

Then, I've Edit that GPO and search for the policy that prevent access to control panel in user config...=>Administrative templates ...=>Control Canel



- block control panel [DC.WORK.
  - Computer Configuration
    - Policies
    - Preferences
  - User Configuration
    - Policies
      - Software Settings
      - Windows Settings
      - Administrative Temp
        - Control Panel
        - Desktop
        - Network
        - Shared Folders
        - Start Menu and T
        - System
        - Windows Compc
        - All Settings
    - Preferences

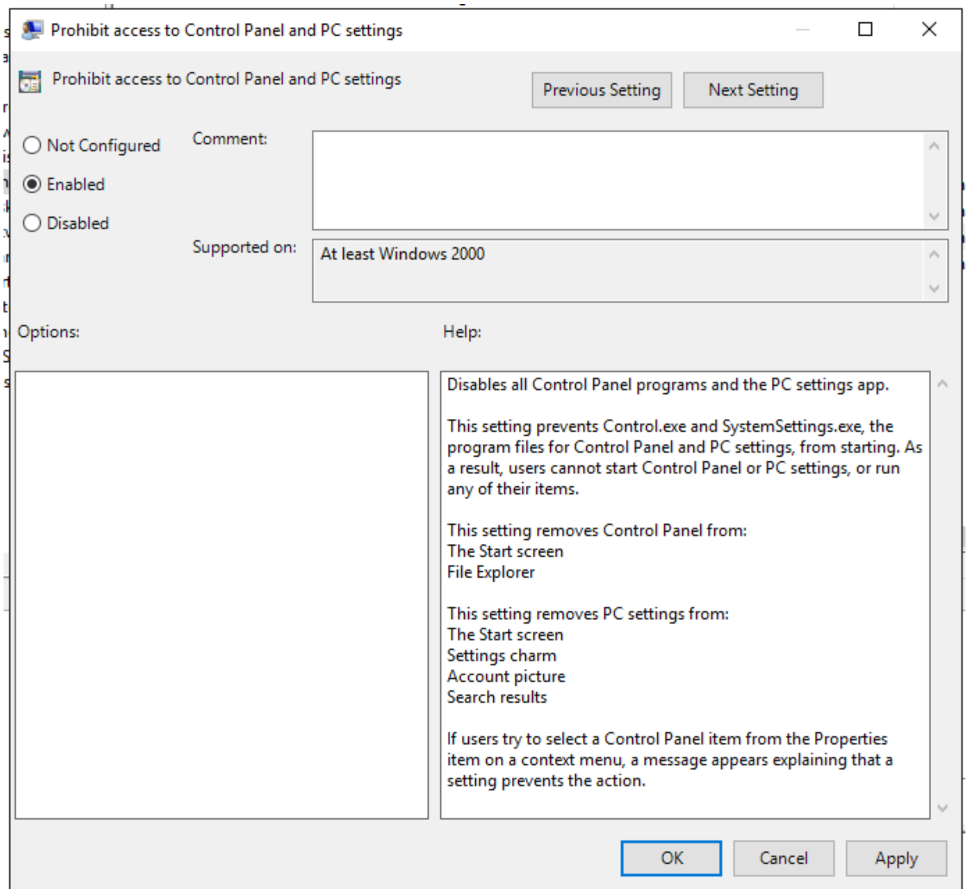
Control Panel

Select an item to view its description.

Setting	State	Comment
Add or Remove Programs		
Display		
Personalization		
Printers		
Programs		
Regional and Language Options		
Hide specified Control Panel items	Not configured	No
Always open All Control Panel Items when opening Control ...	Not configured	No
Prohibit access to Control Panel and PC settings	Not configured	No
Show only specified Control Panel items	Not configured	No

4 setting(s)

Then, Enable it:



Prohibit access to Control Panel and PC settings

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 2000

Options:

Help:

Disables all Control Panel programs and the PC settings app.

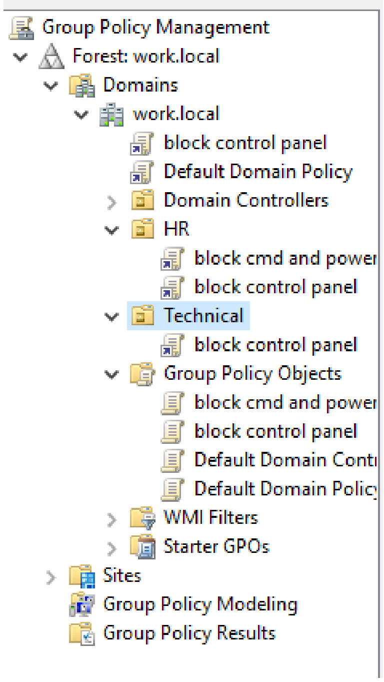
This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.

This setting removes Control Panel from:
The Start screen
File Explorer

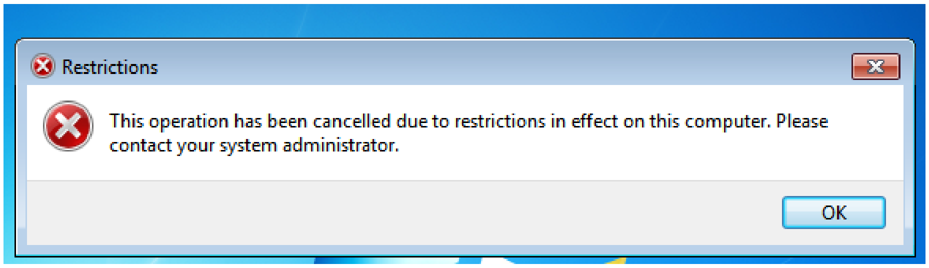
This setting removes PC settings from:
The Start screen
Settings charm
Account picture
Search results

If users try to select a Control Panel item from the Properties item on a context menu, a message appears explaining that a setting prevents the action.

Result of policy I've appley it:



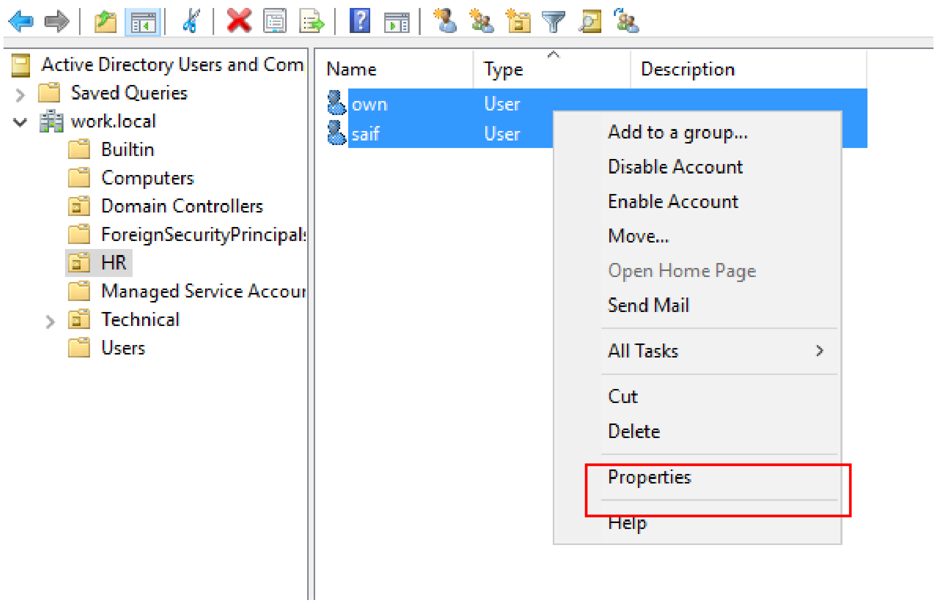
When I try to access to control panel I found this:



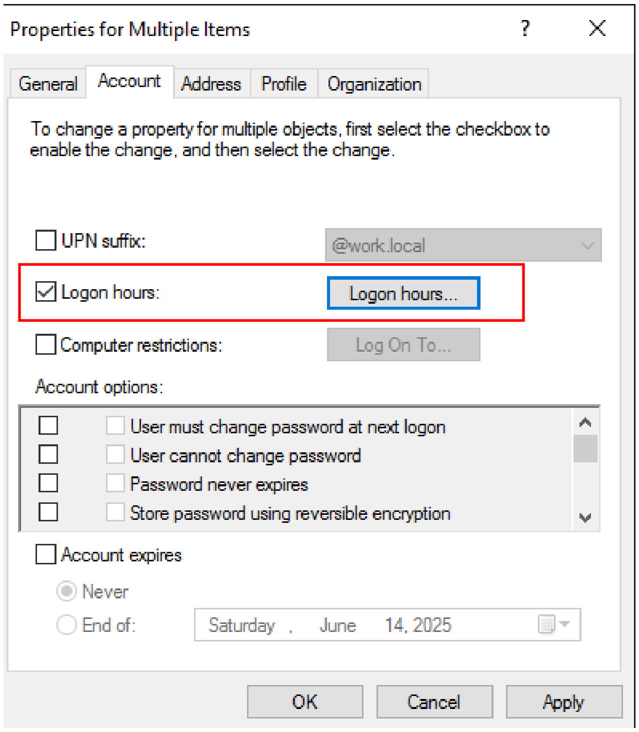
This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.

Allow all employees to login to their accounts only between 8 AM – 5 PM.

In the beginning, I've selected the users from HR and Technical and go to properties:



Then, I've went through Account tab to logon hours:


Properties for Multiple Items

General | Account | Address | Profile | Organization

To change a property for multiple objects, first select the checkbox to enable the change, and then select the change.

☐ UPN suffix: @work.local

☑ Logon hours: Logon hours...

☐ Computer restrictions: Log On To...

Account options:

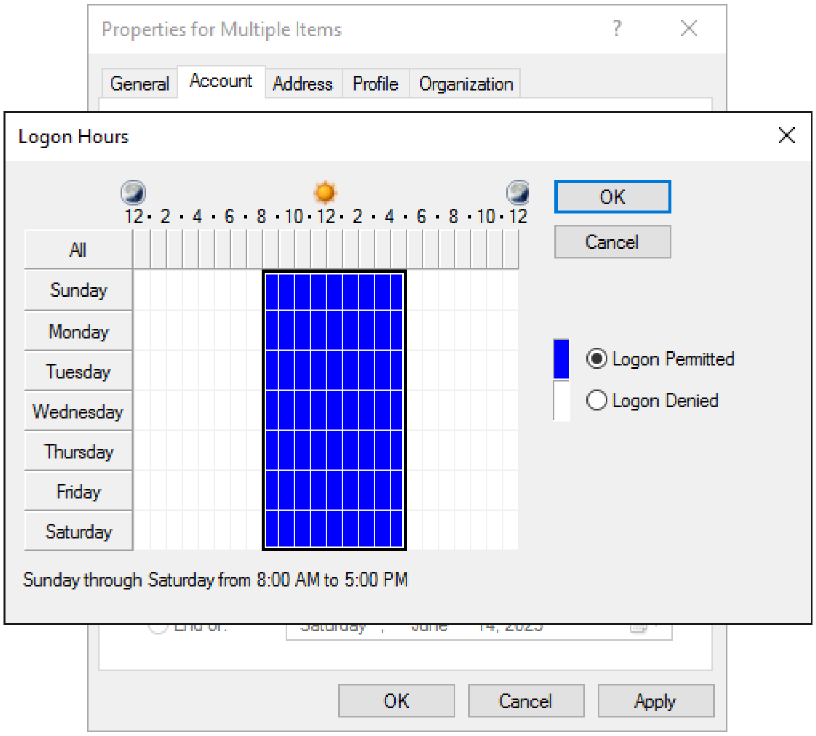
☐ ☐ User must change password at next logon
☐ ☐ User cannot change password
☐ ☐ Password never expires
☐ ☐ Store password using reversible encryption

☐ Account expires

● Never

○ End of: Saturday , June 14, 2025

Then, set a time between 8 AM to 5 PM:

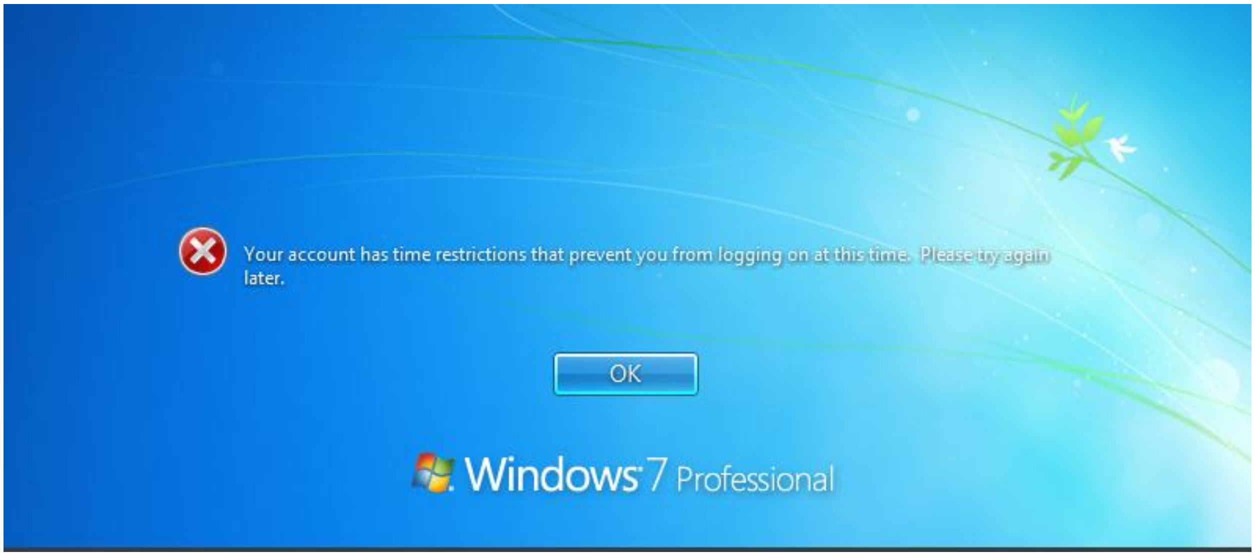


● Logon Permitted

○ Logon Denied

Sunday through Saturday from 8:00 AM to 5:00 PM

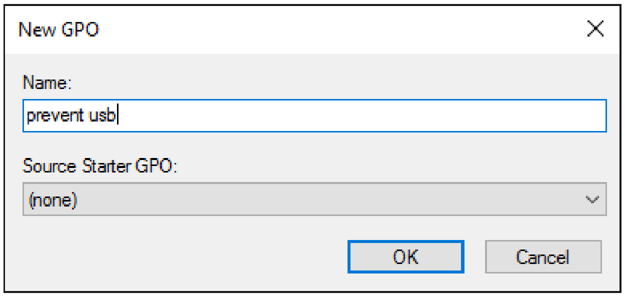
When I try to access to user account I found this :



Your account has time restrictions that prevent you from logging on at this time. Please try again later.

Prevent all employees from plugging in USB devices or any removable storage.

In Group Policy Management, I've created a GPO in domain:



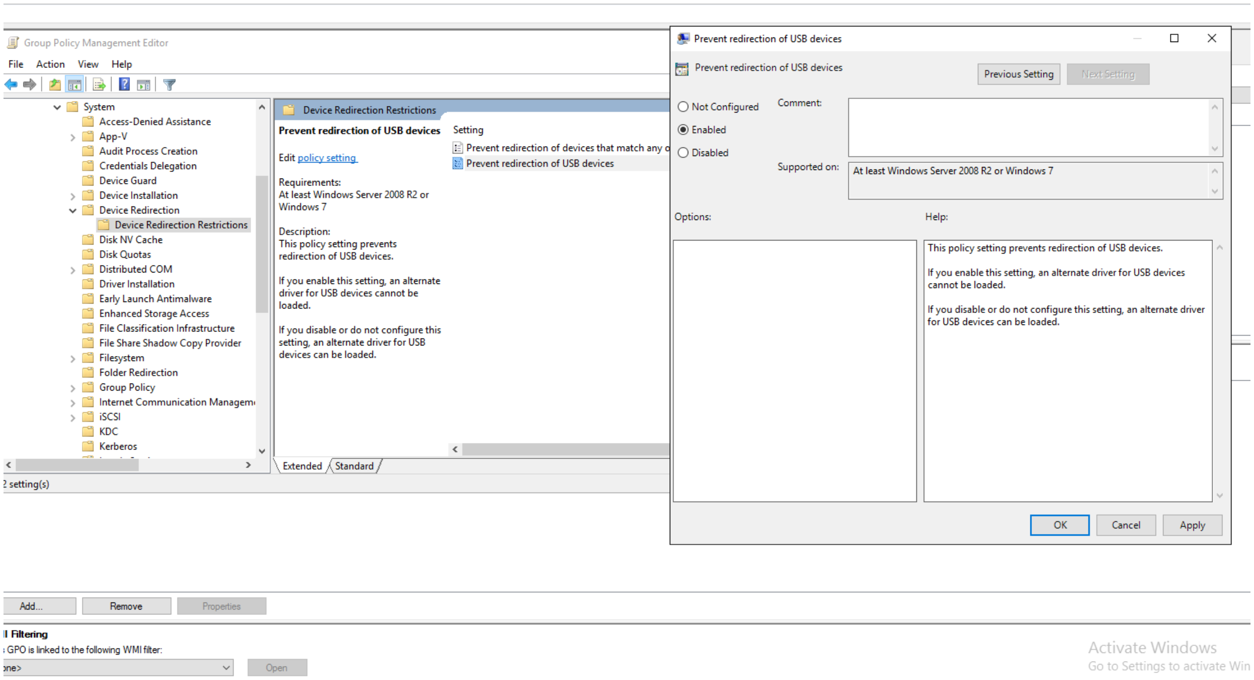
New GPO

Name: prevent usb

Source Starter GPO: (none)

Then, set a name for it.

Then, I've Edit that GPO and search for the policy that prevent USB in computer config...=>Administrative templates ...=>system=>Device Redirection Res...



Group Policy Management Editor

Device Redirection Restrictions

Prevent redirection of USB devices

Edit policy setting

Requirements:
At least Windows Server 2008 R2 or Windows 7

Description:
This policy setting prevents redirection of USB devices.

If you enable this setting, an alternate driver for USB devices cannot be loaded.

If you disable or do not configure this setting, an alternate driver for USB devices can be loaded.

Setting
- Prevent redirection of devices that match any o
- Prevent redirection of USB devices

Prevent redirection of USB devices

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2008 R2 or Windows 7

Options:

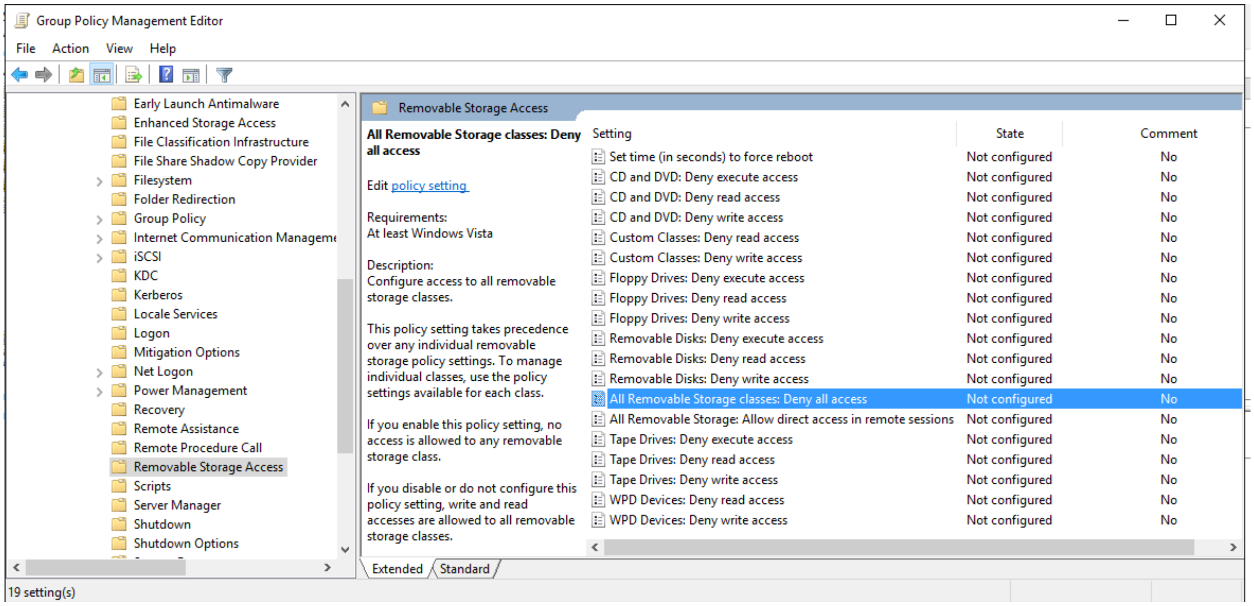
Help:
This policy setting prevents redirection of USB devices.

If you enable this setting, an alternate driver for USB devices cannot be loaded.

If you disable or do not configure this setting, an alternate driver for USB devices can be loaded.

To prevent access all removable storage go to computer config...=>Administrative templates ...=>system=> Removable Storage Access

And Enable it :



Group Policy Management Editor

Early Launch Antimalware
Enhanced Storage Access
File Classification Infrastructure
File Share Shadow Copy Provider
Filesystem
Folder Redirection
Group Policy
Internet Communication Manageme
iSCSI
KDC
Kerberos
Locale Services
Logon
Mitigation Options
Net Logon
Power Management
Recovery
Remote Assistance
Remote Procedure Call
Removable Storage Access
Scripts
Server Manager
Shutdown
Shutdown Options

Removable Storage Access

All Removable Storage classes: Deny all access

Edit policy setting

Requirements:
At least Windows Vista

Description:
Configure access to all removable storage classes.

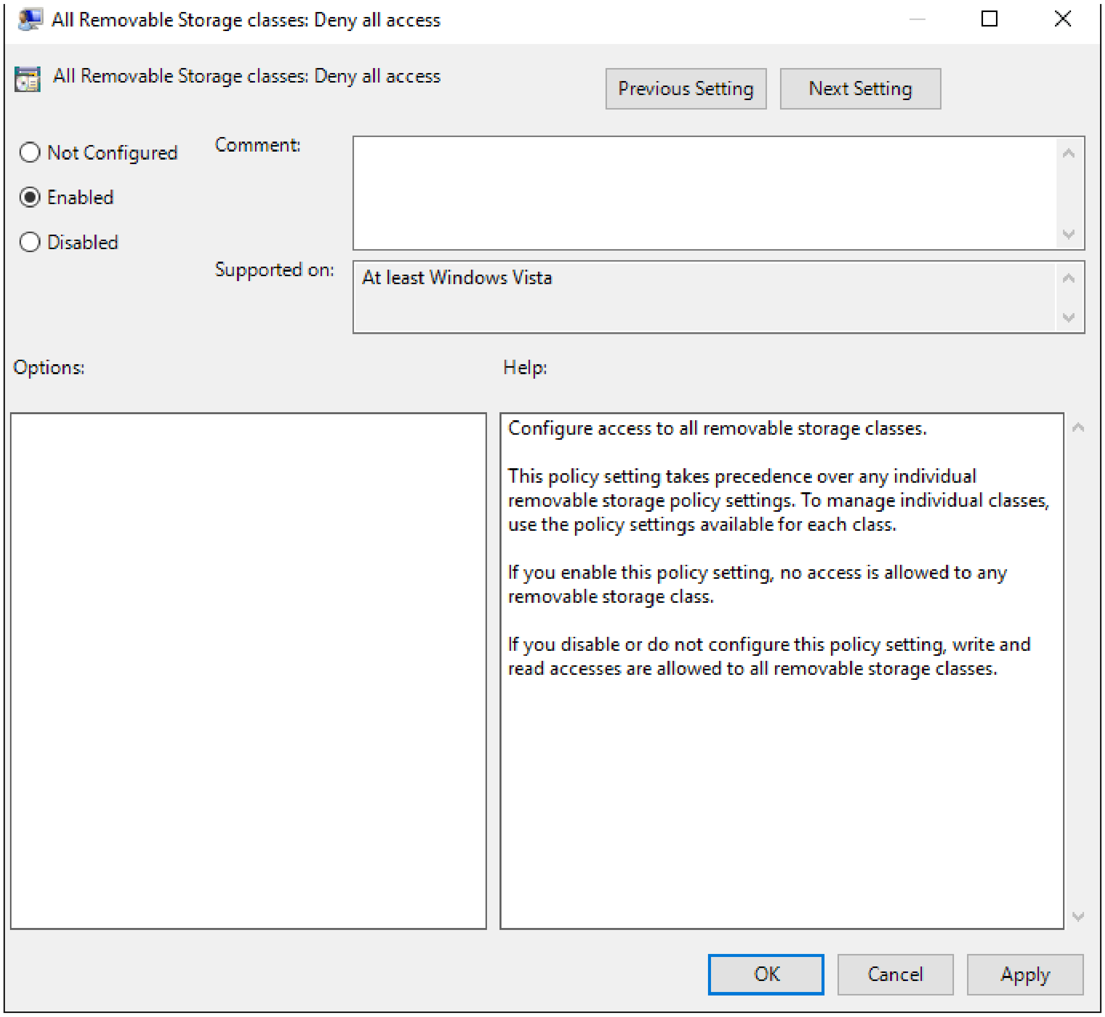
This policy setting takes precedence over any individual removable storage policy settings. To manage individual classes, use the policy settings available for each class.

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.

Setting	State	Comment
Set time (in seconds) to force reboot	Not configured	No
CD and DVD: Deny execute access	Not configured	No
CD and DVD: Deny read access	Not configured	No
CD and DVD: Deny write access	Not configured	No
Custom Classes: Deny read access	Not configured	No
Custom Classes: Deny write access	Not configured	No
Floppy Drives: Deny execute access	Not configured	No
Floppy Drives: Deny read access	Not configured	No
Floppy Drives: Deny write access	Not configured	No
Removable Disks: Deny execute access	Not configured	No
Removable Disks: Deny read access	Not configured	No
Removable Disks: Deny write access	Not configured	No
All Removable Storage classes: Deny all access	Not configured	No
All Removable Storage: Allow direct access in remote sessions	Not configured	No
Tape Drives: Deny execute access	Not configured	No
Tape Drives: Deny read access	Not configured	No
Tape Drives: Deny write access	Not configured	No
WPD Devices: Deny read access	Not configured	No
WPD Devices: Deny write access	Not configured	No

19 setting(s)



All Removable Storage classes: Deny all access

All Removable Storage classes: Deny all access

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Help:

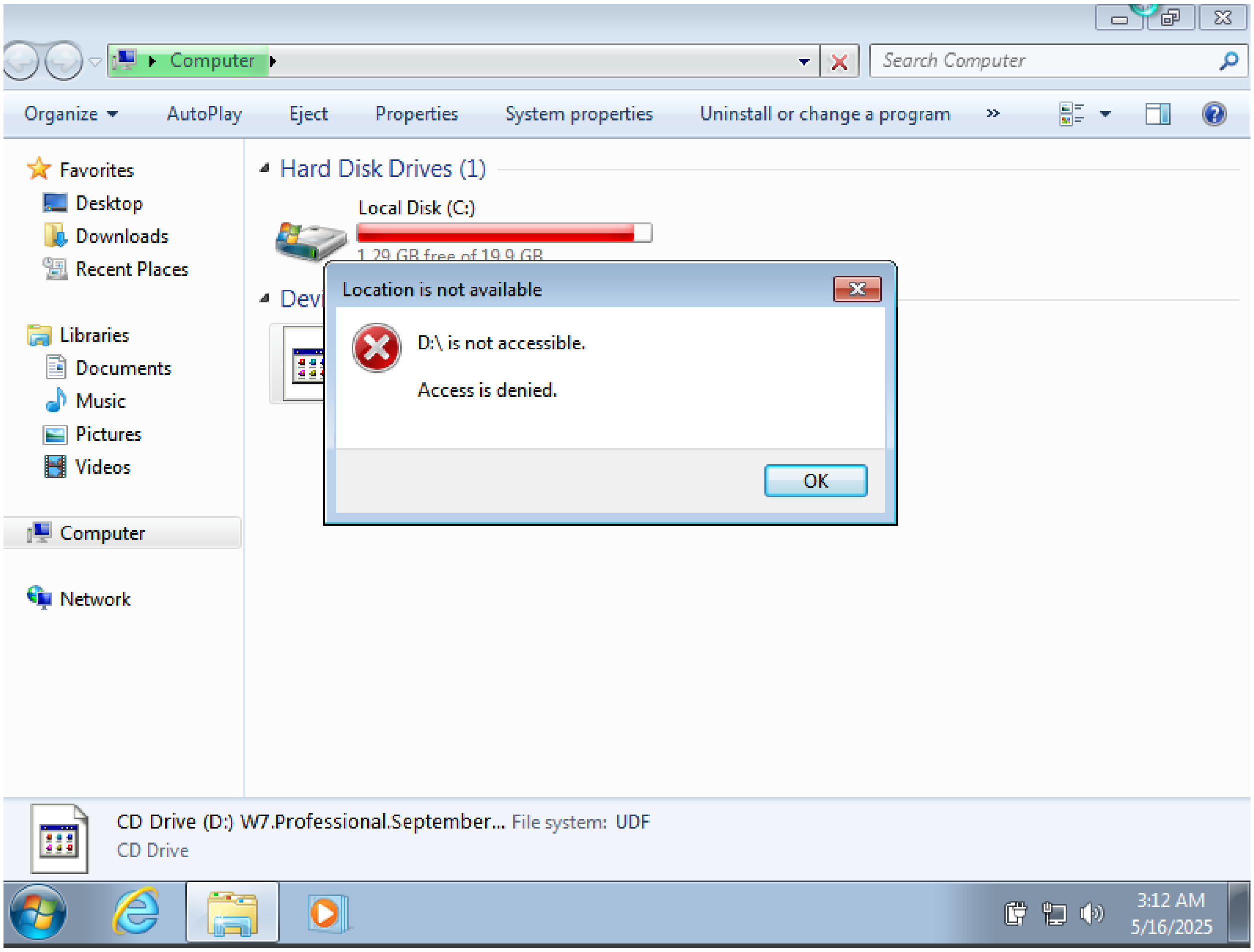
Configure access to all removable storage classes.

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.

When I try to access to USB I found this:



Location is not available

D:\ is not accessible.

Access is denied.

CD Drive (D:) W7.Professional.September... File system: UDF
CD Drive

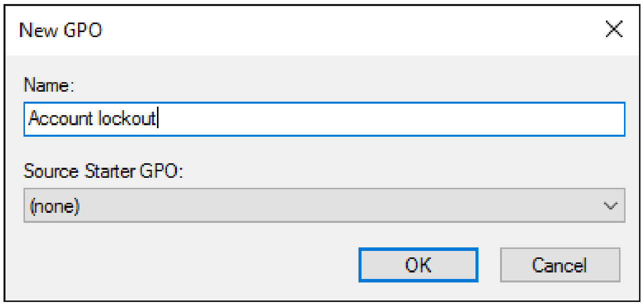
Finaly create different five policy:

Account Lockout Policy

This policy helps protect against **brute-force attacks** on user credentials. If an attacker tries to guess a password repeatedly, the account will be temporarily locked, slowing or stopping the attack.

The steps is:

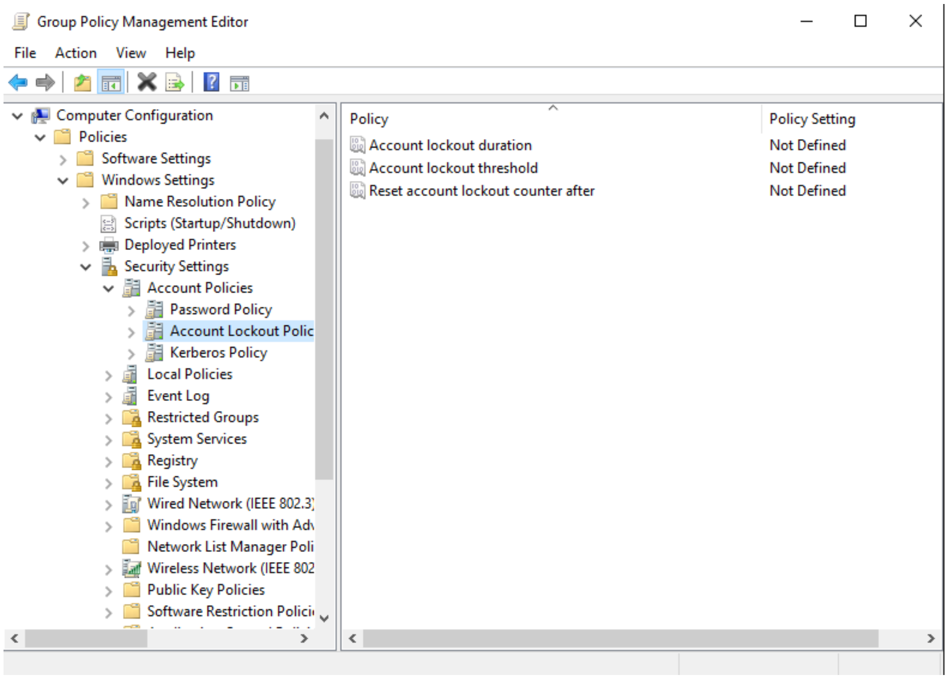
In Group Policy Management, I've created a GPO in domain:



Name: Account lockout

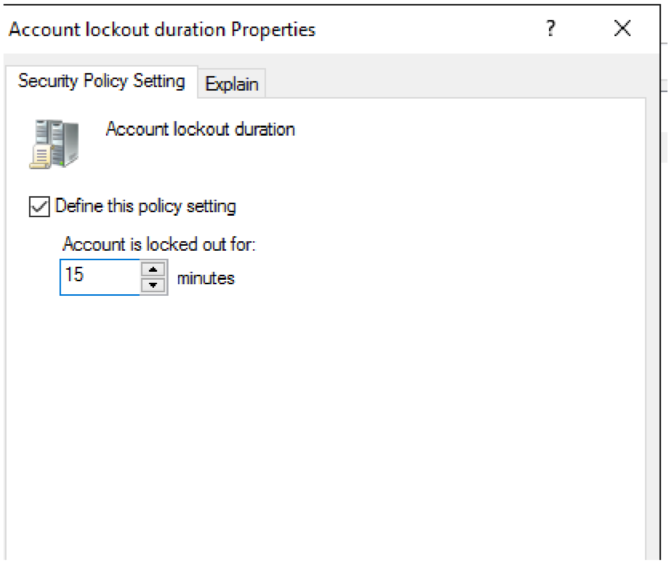
Source Starter GPO: (none)

Then, I've Edit that GPO and search for the policy in Computer Configuration → Windows Settings → Security Settings → Account Policies → Account Lockout Policy



Policy	Policy Setting
Account lockout duration	Not Defined
Account lockout threshold	Not Defined
Reset account lockout counter after	Not Defined

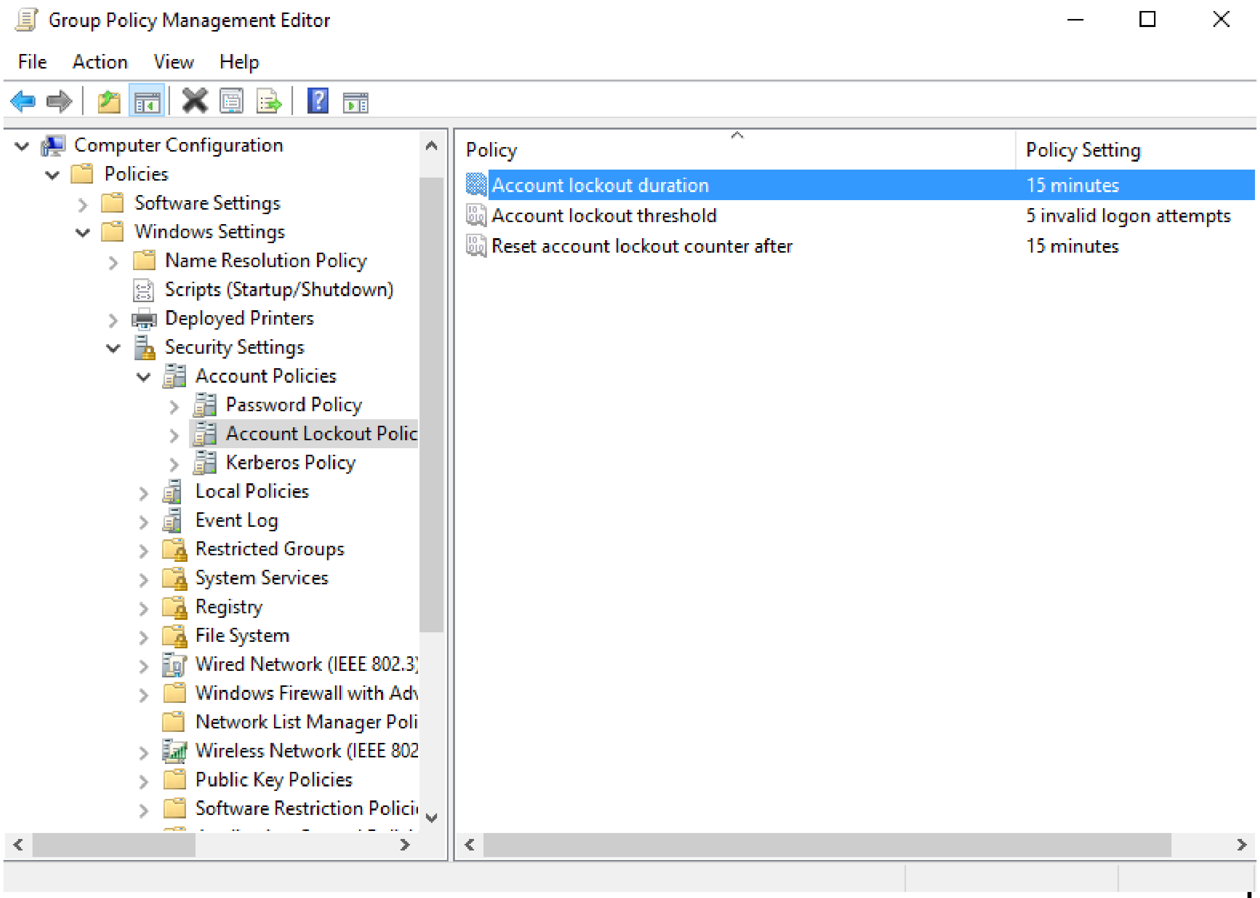
Then, set a time for lockout:



☑ Define this policy setting

Account is locked out for:

15 minutes



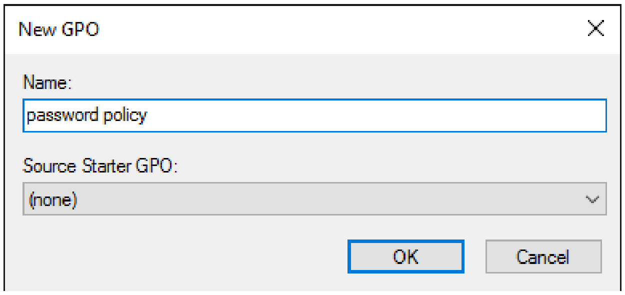
Policy	Policy Setting
Account lockout duration	15 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	15 minutes

Password Policy

Strong password policies ensure users use **complex and unique** passwords, reducing the risk of easy-to-guess or reused passwords being compromised.

The steps are:

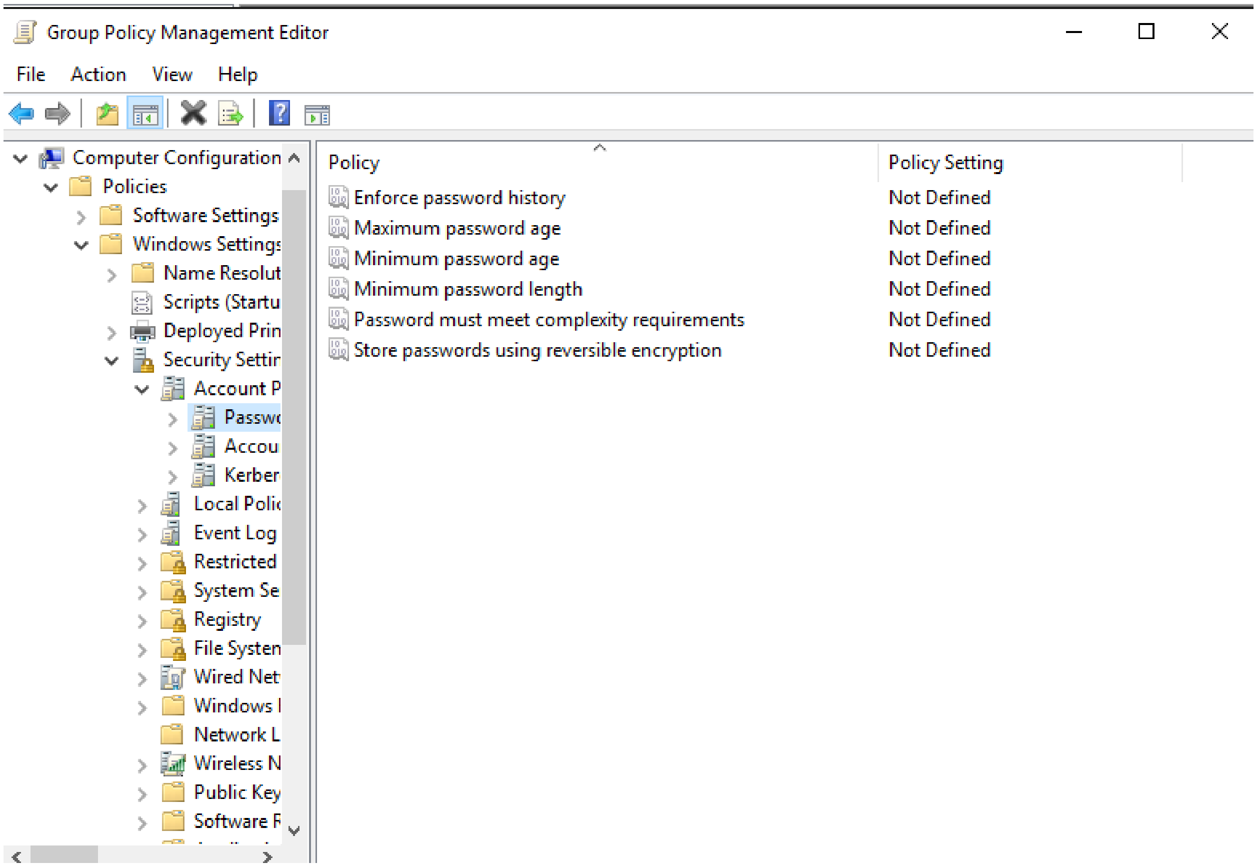
In Group Policy Management, I've created a GPO in domain:



Name: password policy

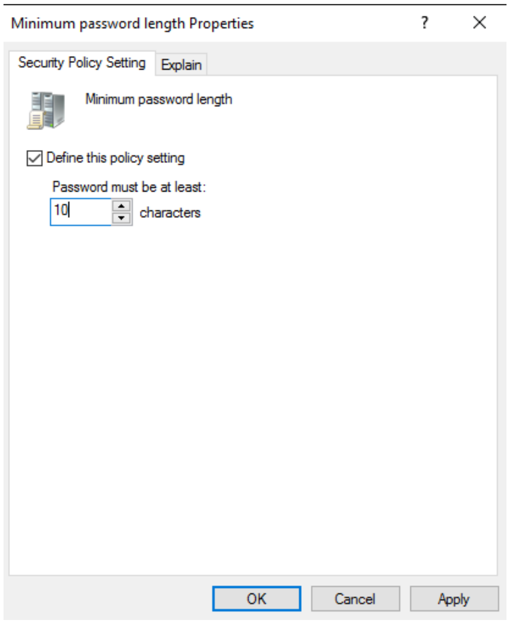
Source Starter GPO: (none)

Then, I've Edit that GPO and search for the policy in Computer Configuration → Windows Settings → Security Settings → Account Policies → Password Policy



Policy	Policy Setting
Enforce password history	Not Defined
Maximum password age	Not Defined
Minimum password age	Not Defined
Minimum password length	Not Defined
Password must meet complexity requirements	Not Defined
Store passwords using reversible encryption	Not Defined

And I've set this configuration:

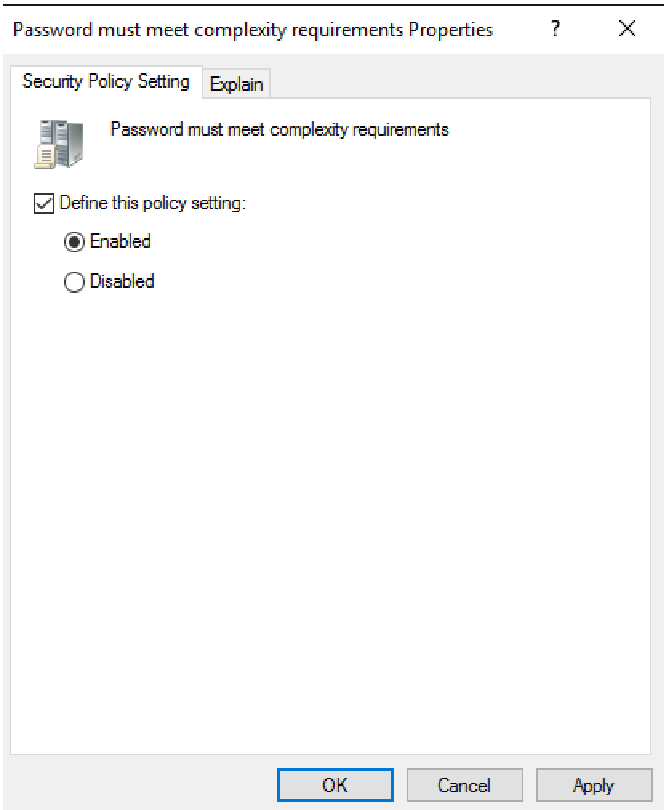


Minimum password length

☑ Define this policy setting

Password must be at least:

10 characters

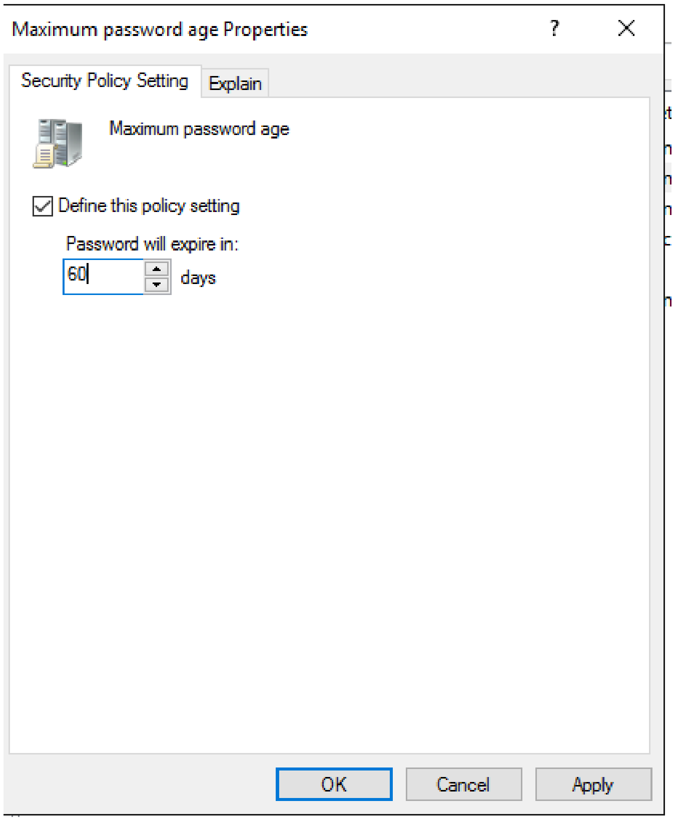

Password must meet complexity requirements Properties

Password must meet complexity requirements

☑ Define this policy setting:

● Enabled

○ Disabled

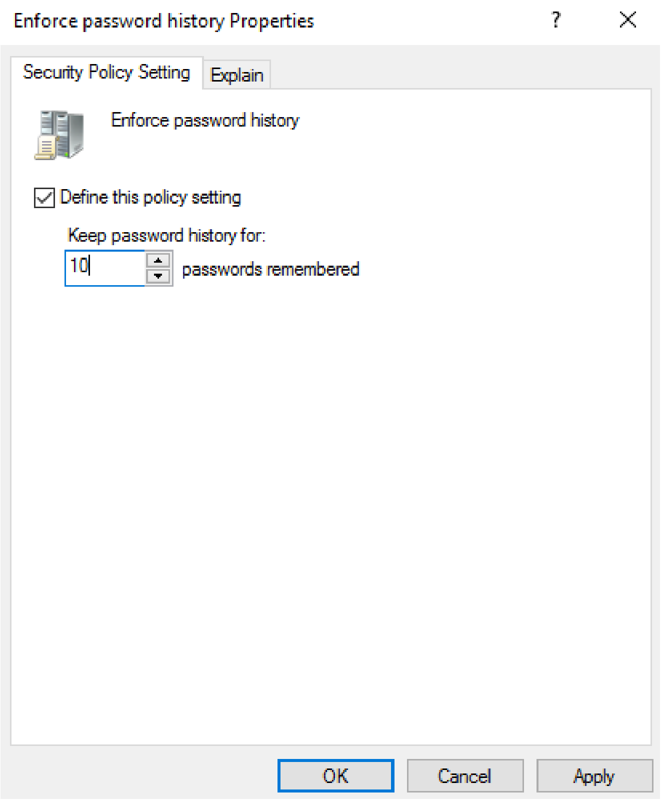

Maximum password age Properties

Maximum password age

☑ Define this policy setting

Password will expire in:

60 days



Enforce password history Properties

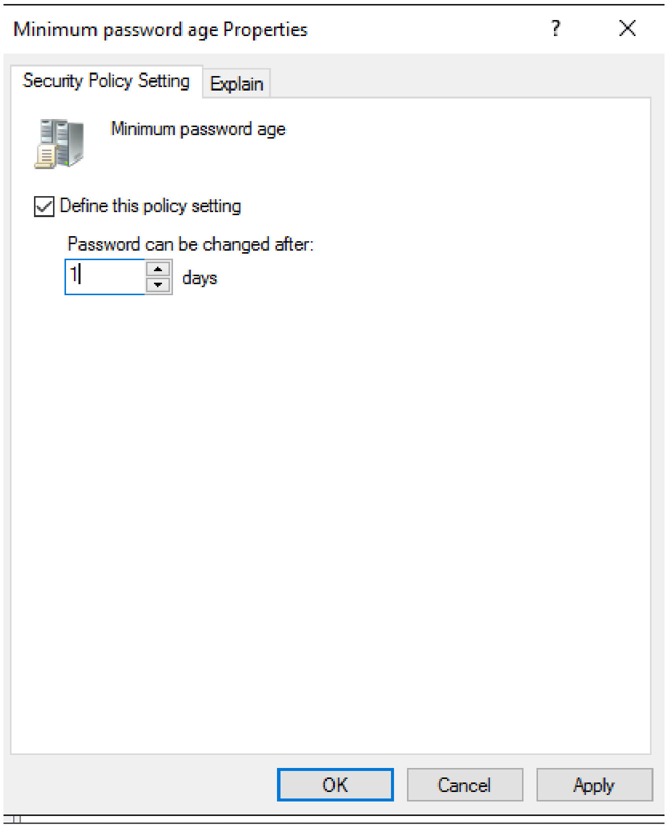
Security Policy Setting | Explain

Enforce password history

☑ Define this policy setting

Keep password history for:

10 passwords remembered



Minimum password age Properties

Security Policy Setting | Explain

Minimum password age

☑ Define this policy setting

Password can be changed after:

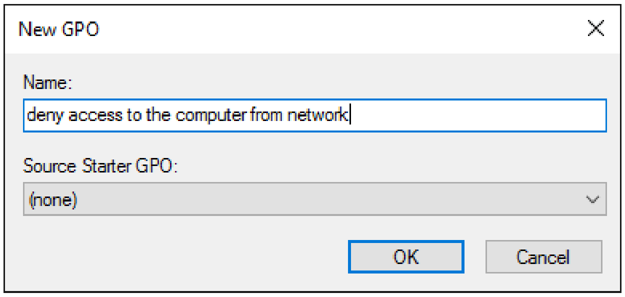
1 days

Deny Access to This Computer from the Network

Restricting network access for specific users reduces the **attack surface** and prevents lateral movement inside the network.

The steps is :

In Group Policy Management, I've created a GPO in domain:

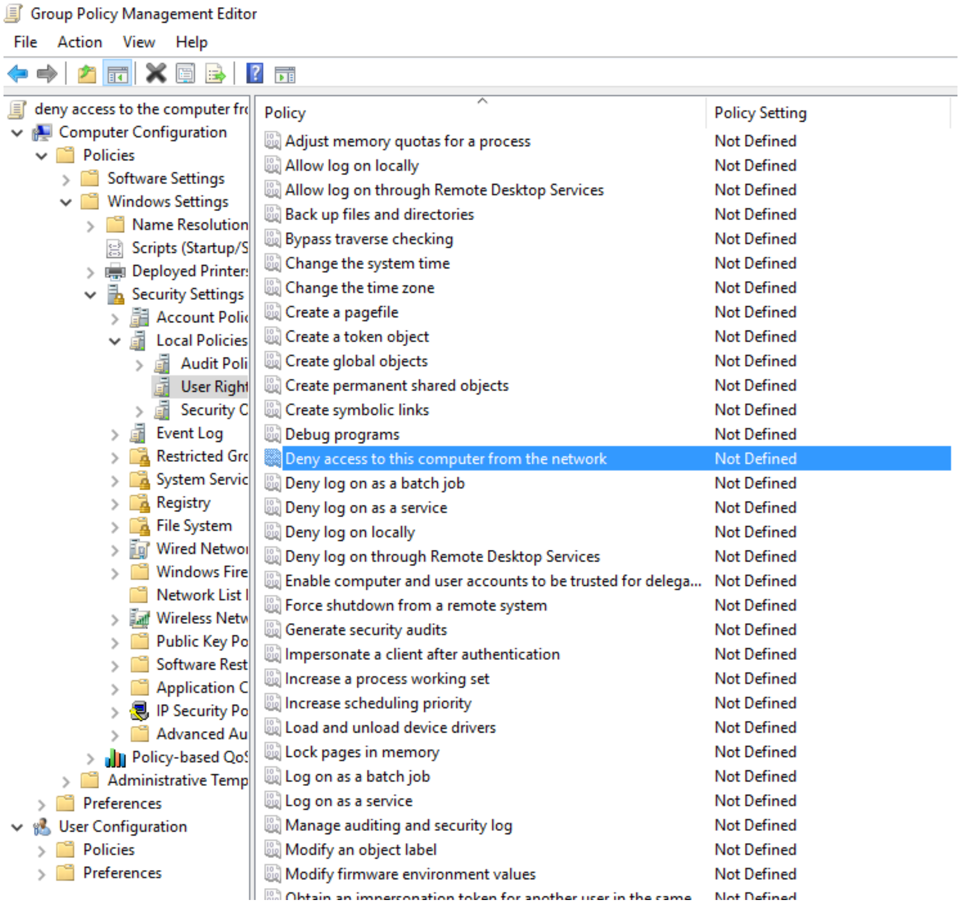


New GPO

Name: deny access to the computer from network

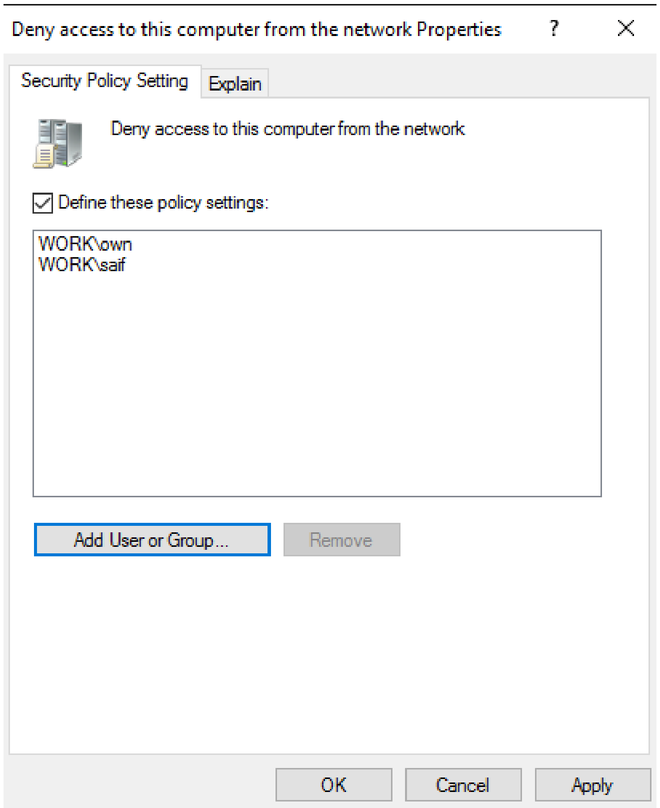
Source Starter GPO: (none)

Then, I've Edit that GPO and search for the policy in Computer Configuration → Windows Settings → Security Settings → Local Policies → User Rights Assignment



Policy	Policy Setting
Adjust memory quotas for a process	Not Defined
Allow log on locally	Not Defined
Allow log on through Remote Desktop Services	Not Defined
Back up files and directories	Not Defined
Bypass traverse checking	Not Defined
Change the system time	Not Defined
Change the time zone	Not Defined
Create a pagefile	Not Defined
Create a token object	Not Defined
Create global objects	Not Defined
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Not Defined
Deny access to this computer from the network	Not Defined
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	Not Defined
Deny log on through Remote Desktop Services	Not Defined
Enable computer and user accounts to be trusted for delega...	Not Defined
Force shutdown from a remote system	Not Defined
Generate security audits	Not Defined
Impersonate a client after authentication	Not Defined
Increase a process working set	Not Defined
Increase scheduling priority	Not Defined
Load and unload device drivers	Not Defined
Lock pages in memory	Not Defined
Log on as a batch job	Not Defined
Log on as a service	Not Defined
Manage auditing and security log	Not Defined
Modify an object label	Not Defined
Modify firmware environment values	Not Defined
Obtain an impersonation token for another user in the same	Not Defined

Then, I've added user form HR into the policy:



Deny access to this computer from the network Properties

Deny access to this computer from the network

☑ Define these policy settings:

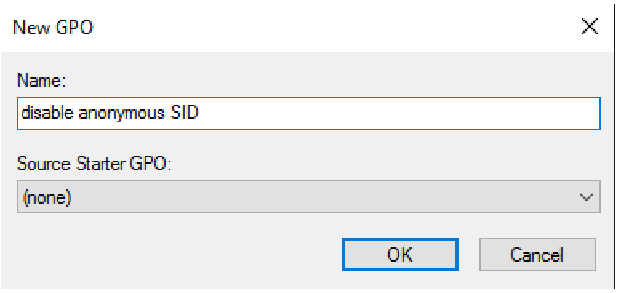
WORK\own
WORK\saif

Disable Anonymous SID Enumeration

Prevents attackers from anonymously listing **user accounts and shared resources** via SID enumeration.

The steps are:

In Group Policy Management, I've created a GPO in domain:

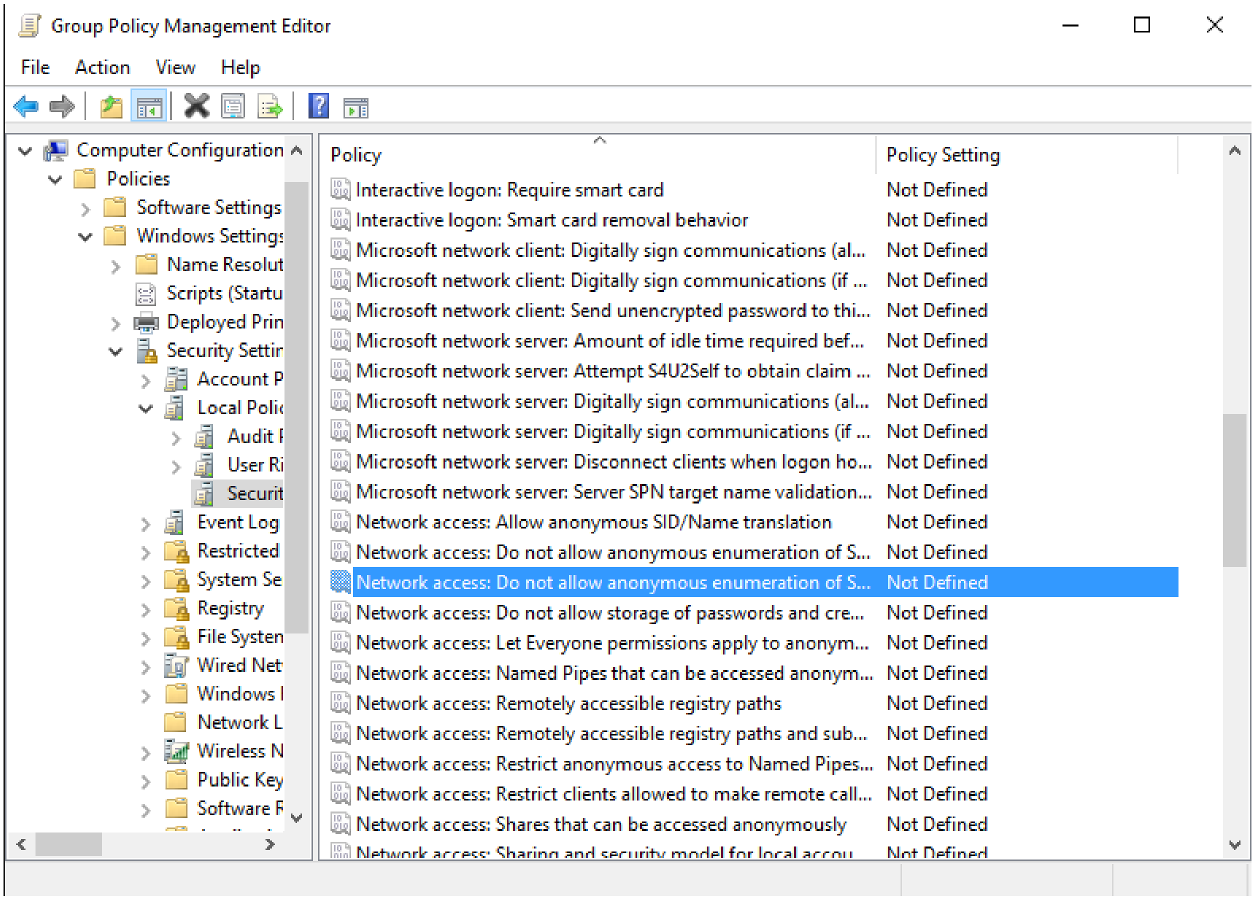


New GPO

Name: disable anonymous SID

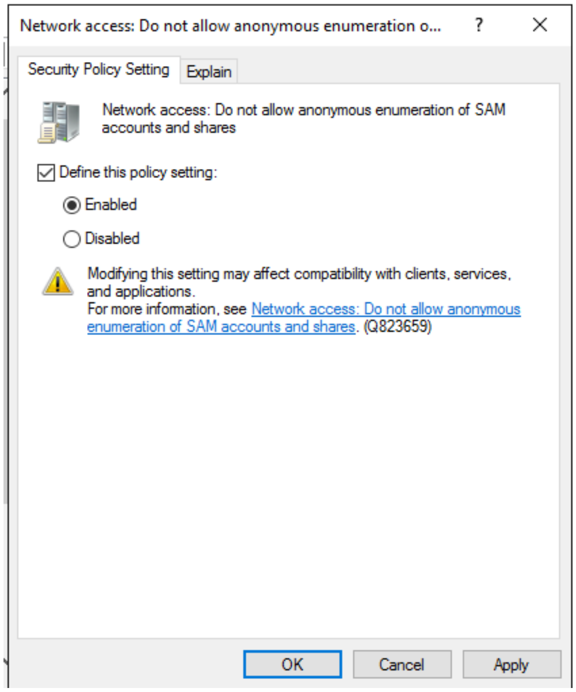
Source Starter GPO: (none)

Then, I've Edit that GPO and search for the policy in Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options



Policy	Policy Setting
Interactive logon: Require smart card	Not Defined
Interactive logon: Smart card removal behavior	Not Defined
Microsoft network client: Digitally sign communications (al...	Not Defined
Microsoft network client: Digitally sign communications (if ...	Not Defined
Microsoft network client: Send unencrypted password to thi...	Not Defined
Microsoft network server: Amount of idle time required bef...	Not Defined
Microsoft network server: Attempt S4U2Self to obtain claim ...	Not Defined
Microsoft network server: Digitally sign communications (al...	Not Defined
Microsoft network server: Digitally sign communications (if ...	Not Defined
Microsoft network server: Disconnect clients when logon ho...	Not Defined
Microsoft network server: Server SPN target name validation...	Not Defined
Network access: Allow anonymous SID/Name translation	Not Defined
Network access: Do not allow anonymous enumeration of S...	Not Defined
Network access: Do not allow anonymous enumeration of S...	Not Defined
Network access: Do not allow storage of passwords and cre...	Not Defined
Network access: Let Everyone permissions apply to anonym...	Not Defined
Network access: Named Pipes that can be accessed anonym...	Not Defined
Network access: Remotely accessible registry paths	Not Defined
Network access: Remotely accessible registry paths and sub...	Not Defined
Network access: Restrict anonymous access to Named Pipes...	Not Defined
Network access: Restrict clients allowed to make remote call...	Not Defined
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accou	Not Defined

Then, I've enabled it :



Network access: Do not allow anonymous enumeration of SAM accounts and shares

☑ Define this policy setting:

● Enabled

○ Disabled

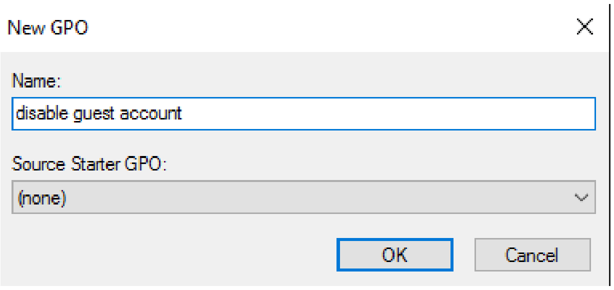
Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network access: Do not allow anonymous enumeration of SAM accounts and shares. (Q823659)

Disable Guest Account

The Guest account is a common target for attackers because it requires no password by default.

The steps is :

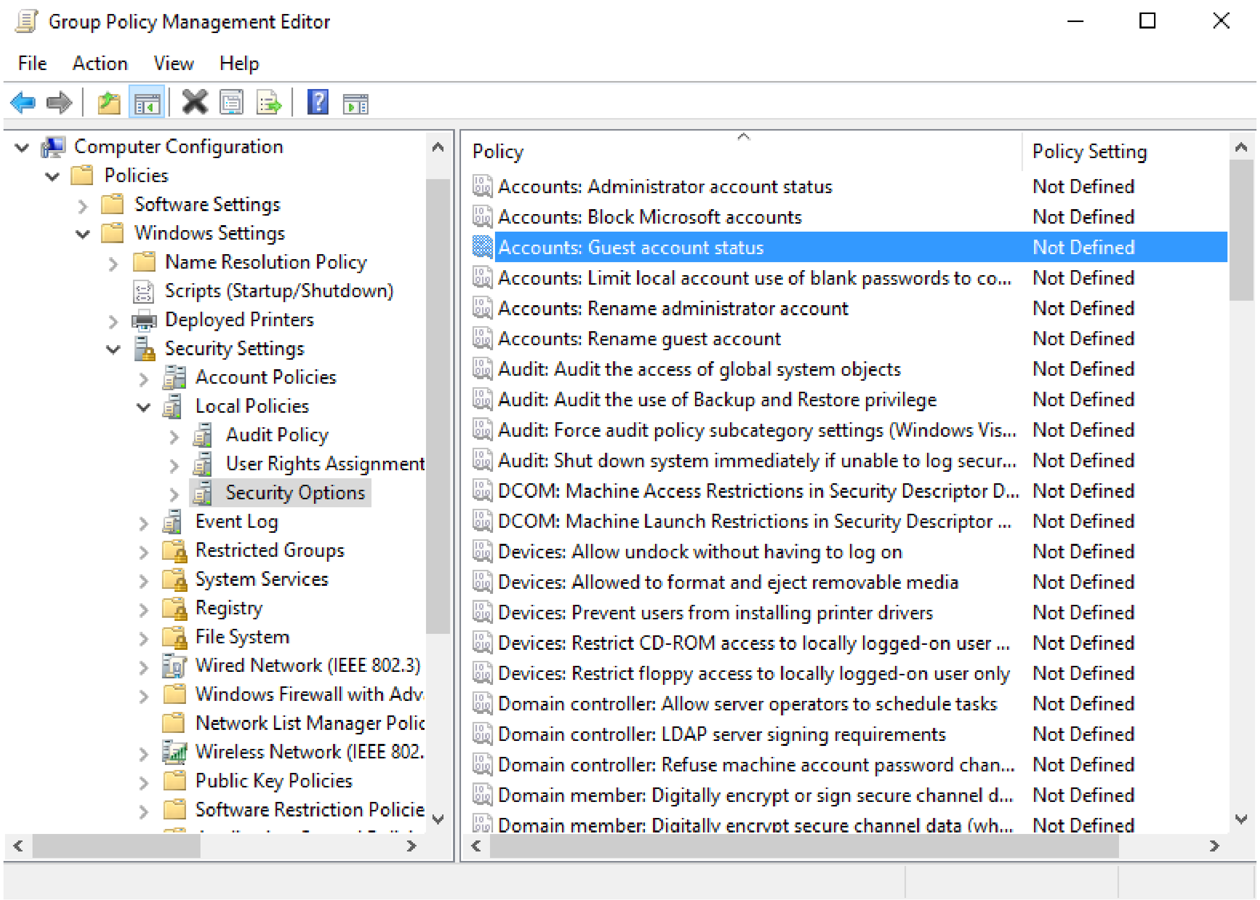
In Group Policy Management, I've created a GPO in domain:



Name: disable guest account

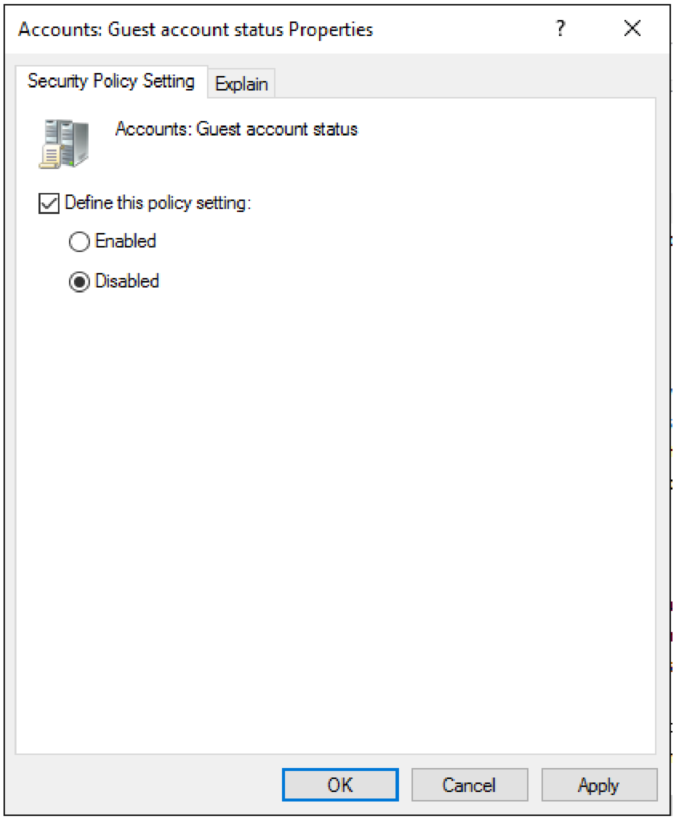
Source Starter GPO: (none)

Then, I've Edit that GPO and search for the policy in Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options



Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to co...	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Not Defined
Domain member: Digitally encrypt secure channel data (wh...	Not Defined

Then, I've disable it:



Accounts: Guest account status Properties

Security Policy Setting | Explain

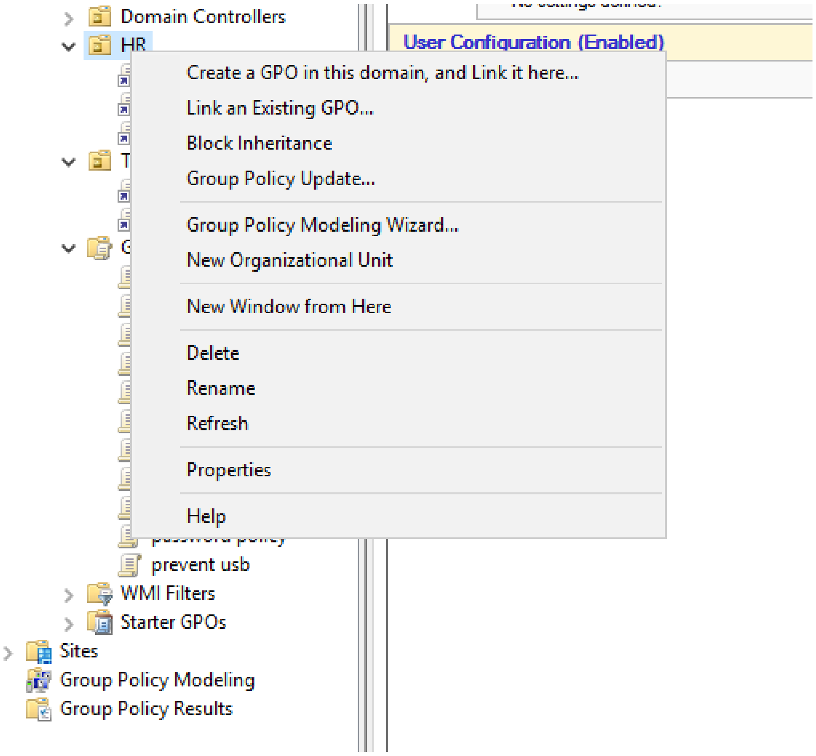
Accounts: Guest account status

☑ Define this policy setting:

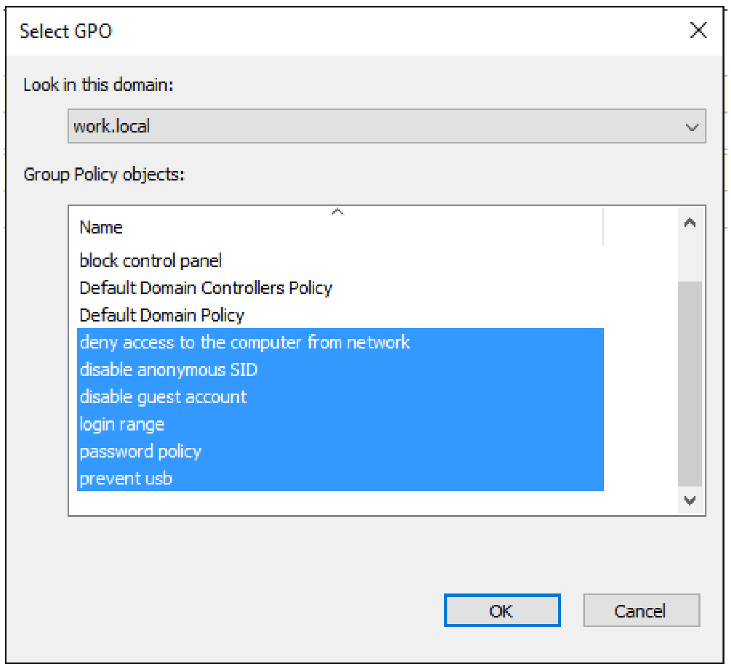
○ Enabled

● Disabled

Finaly, I've link an existing GPO of the HR Unit :



Then, I've selected the requited policy:



Select GPO

Look in this domain:

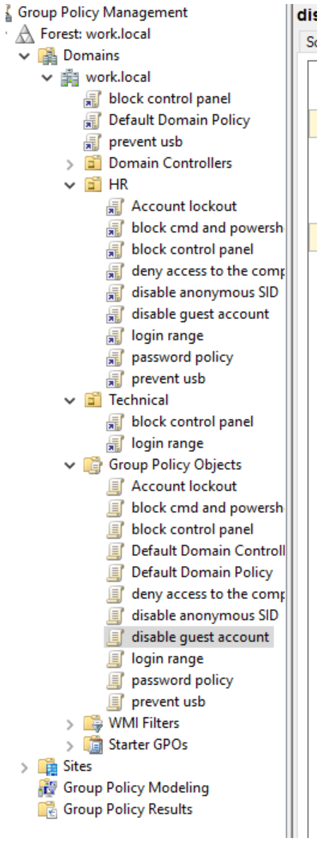
work.local

Group Policy objects:

Name

block control panel
Default Domain Controllers Policy
Default Domain Policy
deny access to the computer from network
disable anonymous SID
disable guest account
login range
password policy
prevent usb

And ,this is a list of policies that I've configured it:



Group Policy Management
- Forest: work.local
  - Domains
    - work.local
      - block control panel
      - Default Domain Policy
      - prevent usb
      - Domain Controllers
      - HR
        - Account lockout
        - block cmd and powersh
        - block control panel
        - deny access to the comp
        - disable anonymous SID
        - disable guest account
        - login range
        - password policy
        - prevent usb
      - Technical
        - block control panel
        - login range
      - Group Policy Objects
        - Account lockout
        - block cmd and powersh
        - block control panel
        - Default Domain Controll
        - Default Domain Policy
        - deny access to the comp
        - disable anonymous SID
        - disable guest account
        - login range
        - password policy
        - prevent usb
      - WMI Filters
      - Starter GPOs
  - Sites
  - Group Policy Modeling
  - Group Policy Results