Windows Server 2022 - Domain Group Policy Documentation

Explain :

This task aims to secure and manage a Windows Server 2022 domain environment (`we.local`) by applying a comprehensive set of Group Policies (GPOs). The objective is to enforce organizational security standards across users and computers within the domain.

Environment Overview :

environment was used to simulate and configure a secured Active Directory domain infrastructure:

- **Domain Name:** `we.local`
- **Server OS:** Windows Server 2022
- **Client OS:** Windows 10 (Domain-joined VM)
- **Virtualization Platform:** (VMware)

Initial Setup:

first step =>Active Directory Domain Services (AD DS) was installed on Windows Server 2022.

After installation => the server was promoted to a Domain Controller,

new domain => was created with the name: (**`we.local`**)

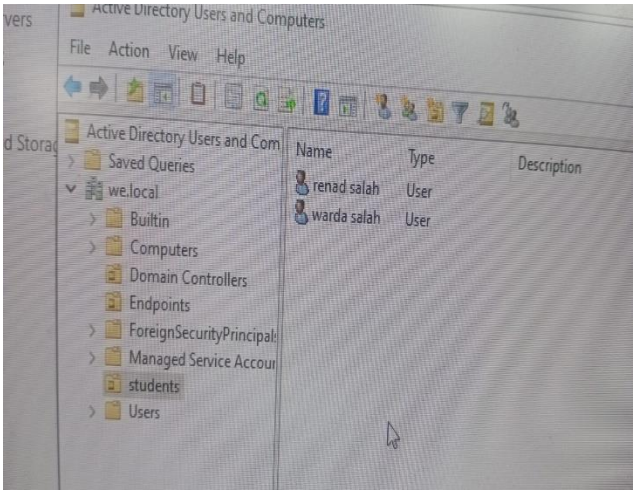
Windows Client machine(Windows 10) **=>** was set up and configured to be on the same network subnet as the server to ensure connectivity between both devices. Static IP addresses were assigned accordingly to both server and client, and successful communication was verified using the ping command

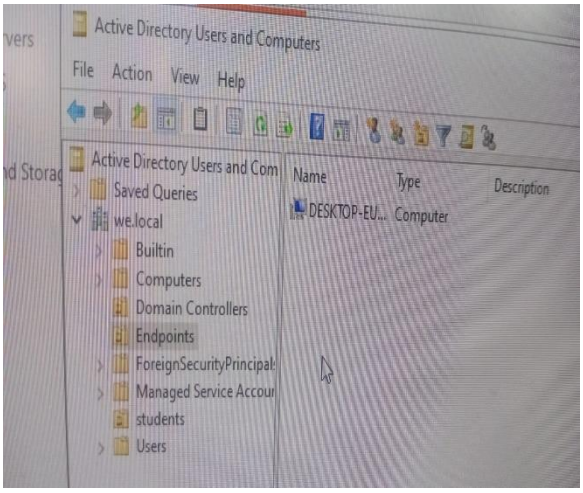
Once connectivity was confirmed, the client machine was successfully joined to the domain (`we.local`) .

Organizational Units and User Accounts

Create OU for Users and Endpoints

- Created an OU named **Students** to organize domain users.
- Created two user accounts: **Renad Salah** and **Warda Salah**, both located inside the `Students` OU.
- Created an OU named **Endpoints** to organize domain-joined machines.
- After joining the client machine to the domain, its computer object was automatically
- added to the **Endpoints** OU for policy management and organization.



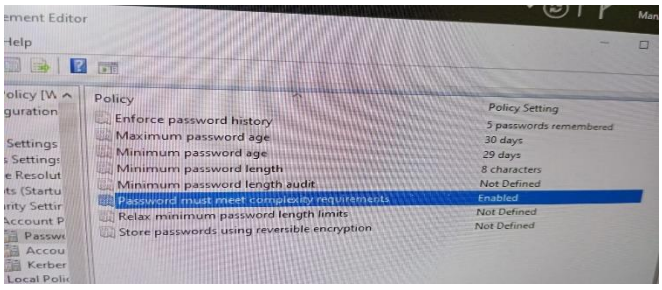


Group Policy Configuration Overview

The following section outlines the security and administrative policies applied through Group Policy Objects (GPOs) to enforce a secure and well-managed domain environment.

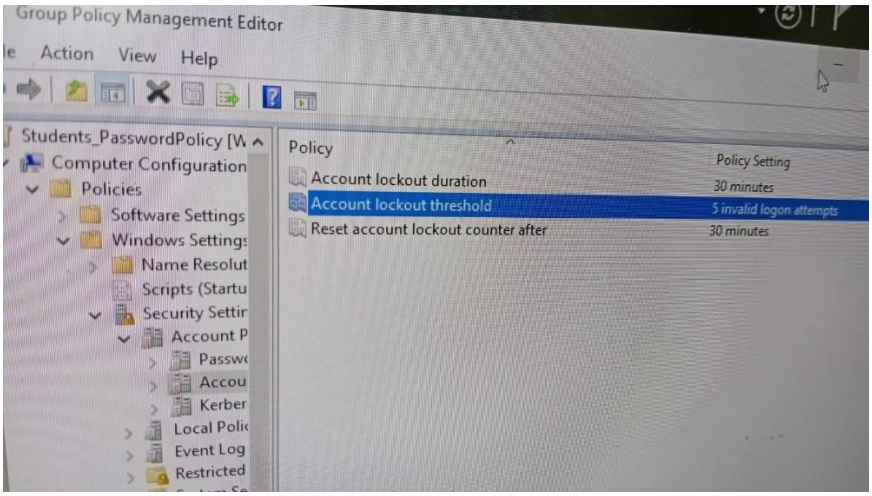
1. Apply Enforce Strong Password Policy

- **Policy Path:** Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy



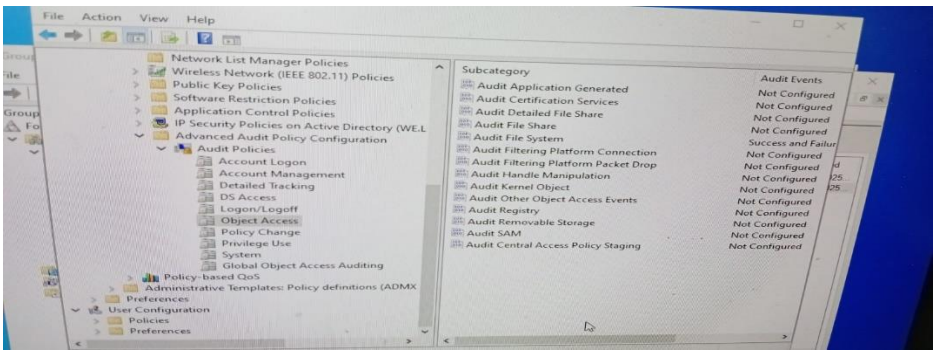
2. Account Lockout Policy

- **Path:** Computer Configuration > Windows Settings > Security Settings > Account Policies > Account Lockout Policy
- Lock account after 3 failed attempts
- Lockout duration: 30 minutes
- Reset account lockout counter after: 15 minutes



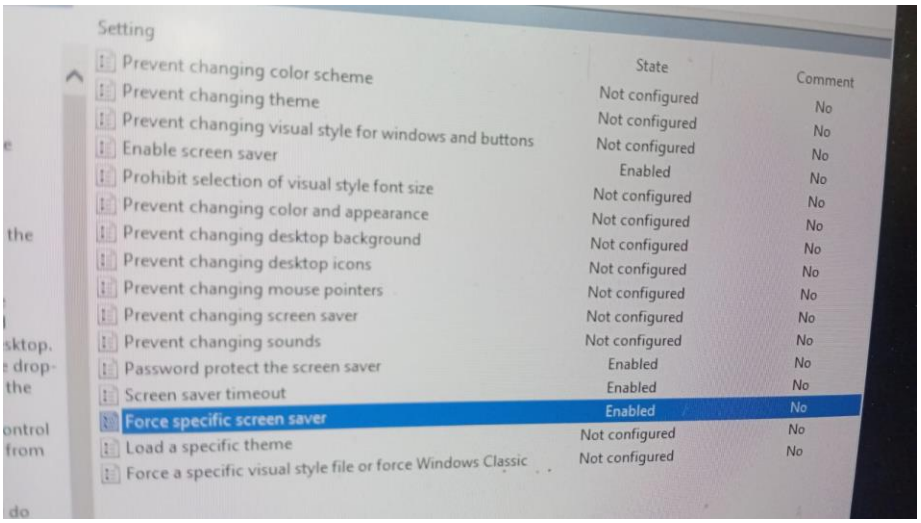
3. Audit Policies

- **Path:** Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration
- Enabled:
  - Logon events
  - Account logon
  - Object access
  - Policy change
  - Directory service access



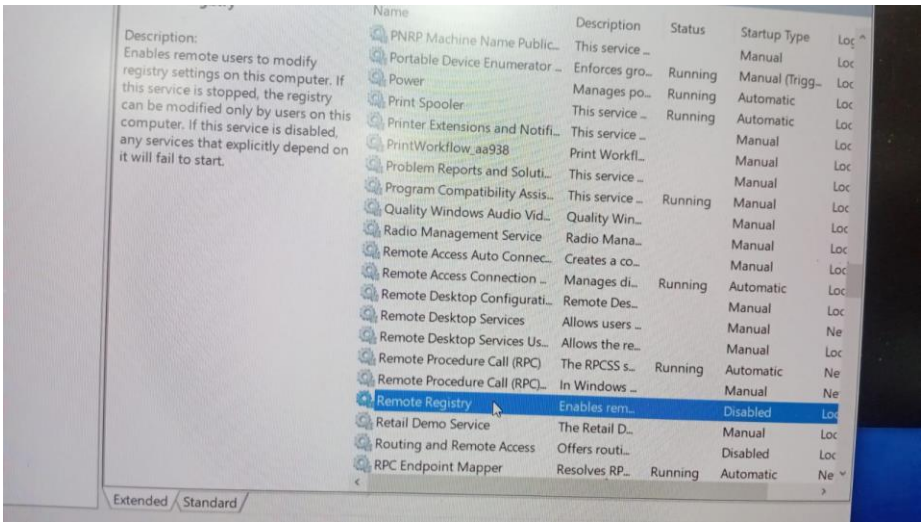
4. Screensaver Policy

- **Path:** User Configuration > Administrative Templates > Control Panel > Personalization
- Enabled screen saver
- Set timeout: 600 seconds (10 minutes)
- Enabled password protection
- Applied specific screen saver: scrnsave.scr



5. Disable Services

- Applied through Services or GPO to disable unnecessary services (Bluetooth Support, Print Spooler , remote registry on sensitive machines).



8. Firewall Rule to Block Ping to 8.8.8.8 and 8.8.4.4

- **Path:** Computer Configuration > Windows Settings > Security Settings > Windows Defender Firewall > Inbound Rules
- Created custom rule to block ICMP (ping) to those IPs.

9. Disallow Media Drives

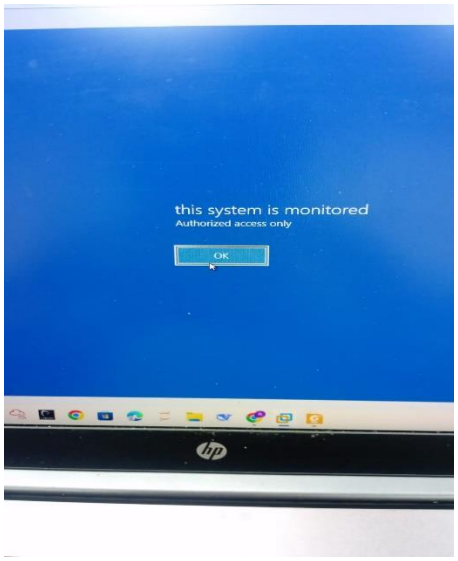
- **Path:** Computer Configuration > Administrative Templates > System > Removable Storage Access
- Deny all access to: CD/DVD, USB, and other removable drives

10. Restrict Software Installation

- **Path:** User Configuration > Administrative Templates > Windows Components > Windows Installer
- Enabled policy: "Prohibit User Installs"

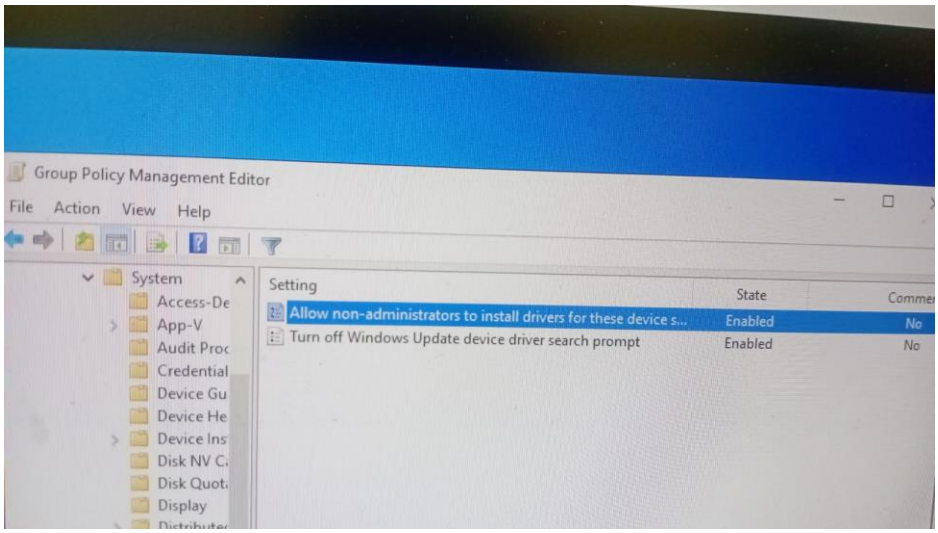
11. Set a Logon Message

- **Path:** Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options
- Set legal notice caption and text with organization security warning.



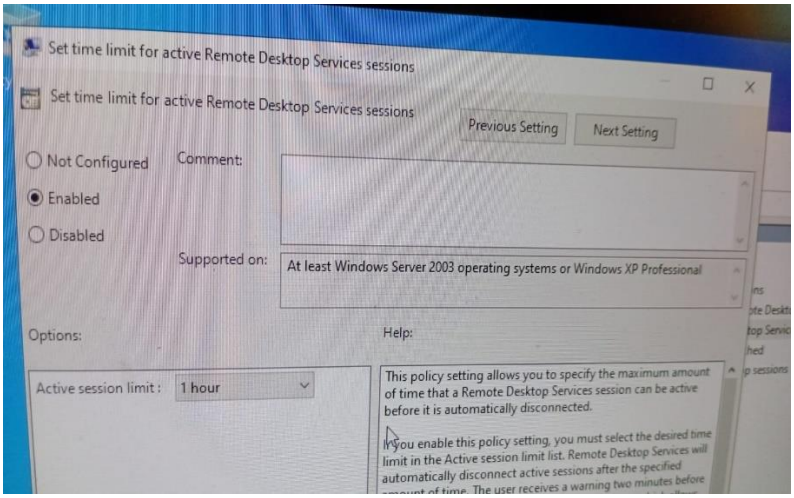
12. Disable CMD and PowerShell

- **Path:** User Configuration > Administrative Templates > System
- Disable CMD: Enabled "Prevent access to command prompt"
- Disable PowerShell: Restricted execution policies via script policies



13. RDP Restrictions

- **Path:** Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections
- Limited number of RDP connections
- Set idle session timeout to 15 minutes

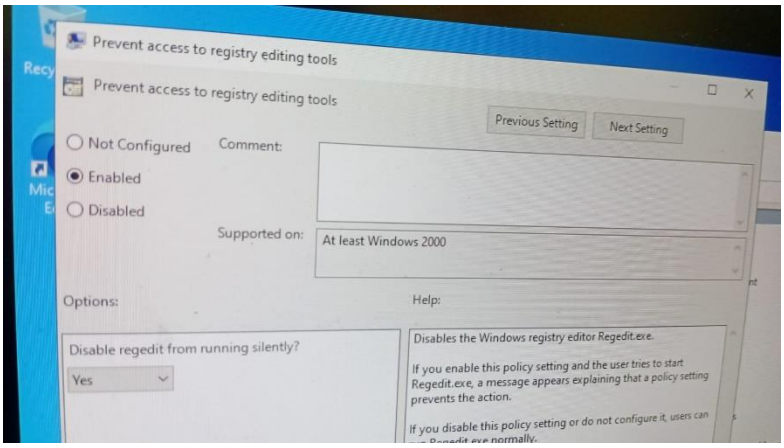


14. Microsoft Edge - Disable InPrivate Mode

- **Path:** User Configuration > Administrative Templates > Microsoft Edge
- Enabled: "InPrivate mode availability" → Set to Disabled

15. Disable Registry Editor

- **Path:** User Configuration > Administrative Templates > System
- Enabled policy: "Prevent access to registry editing tools"



14. Microsoft Edge - Disable InPrivate Mode

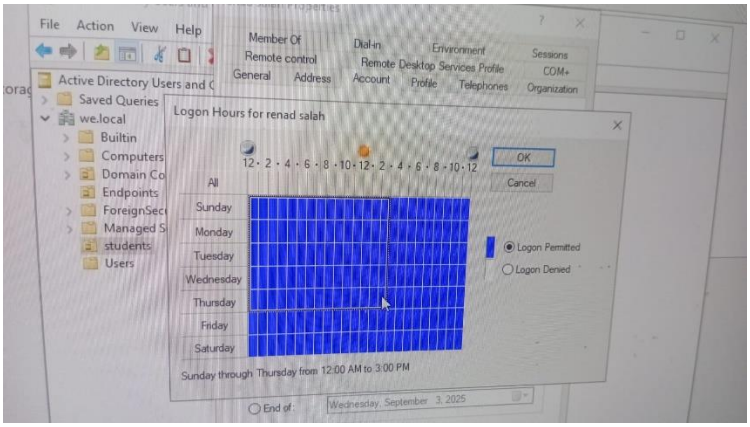
- **Path:** User Configuration > Administrative Templates > Microsoft Edge
- Enabled: "InPrivate mode availability" → Set to Disabled

16. Prevent Installation of Printer Drivers

- **Path:** Computer Configuration > Administrative Templates > System > Driver Installation
- Enabled: "Prevent users from installing printer drivers"

19. Restrict Time of Day Logon

- Set through Active Directory Users and Computers
- User Properties > Account > Logon Hours...
- Allowed login from 08:00 to 16:00, Sunday to Thursday



21. Windows Defender - Scan Downloads and Attachments

- **Path:** Same as above
- Enabled: "Scan all downloaded files and attachments"

22. Enforce BitLocker Encryption

- **Path:** Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption
- Enforced encryption on OS, fixed, and removable drives
- Required recovery keys to be stored in Active Directory
- Enabled TPM and additional authentication