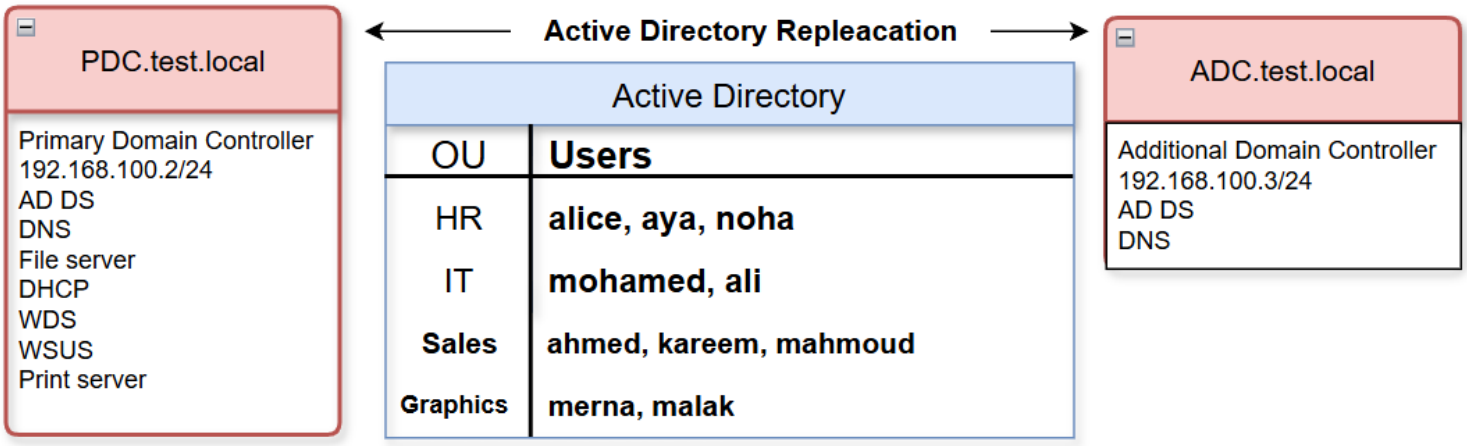
SUMMARY

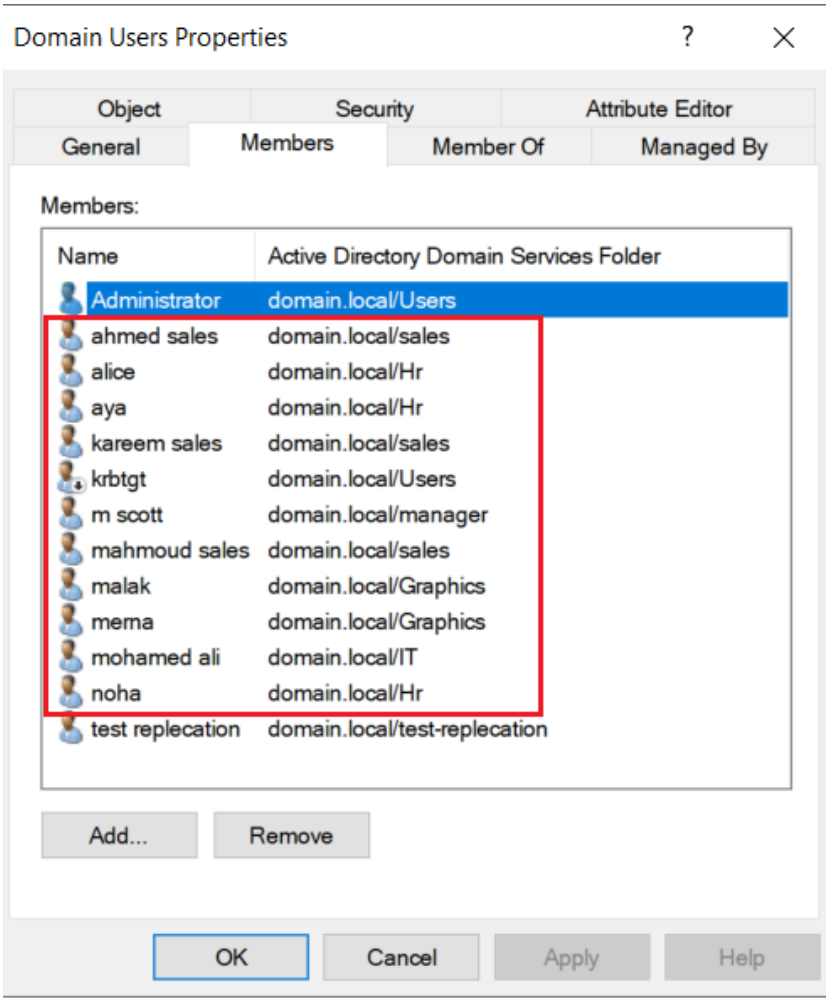
This Windows Server project implements key services such as AD DS for centralized domain management, network sharing with roaming profiles, FSRM for quotas and file control, and essential infrastructure like DHCP, DNS, and WDS. It also includes configuring RDP for remote access, drive mapping for shared resources, and policies for managing user logon times.

Mahmoud Ahmed Elsawah

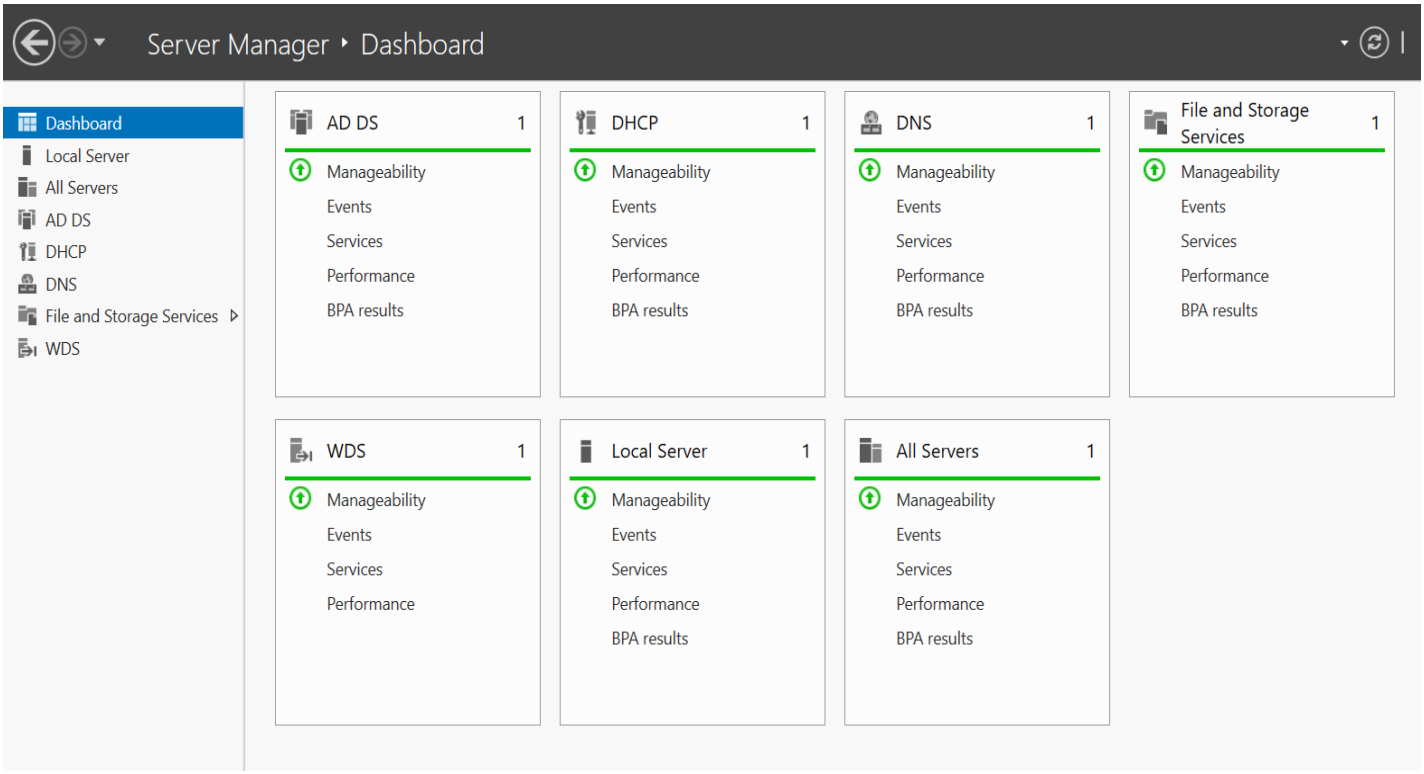
Windows Server Project Configuration Plan



Domain Users and Their Ous

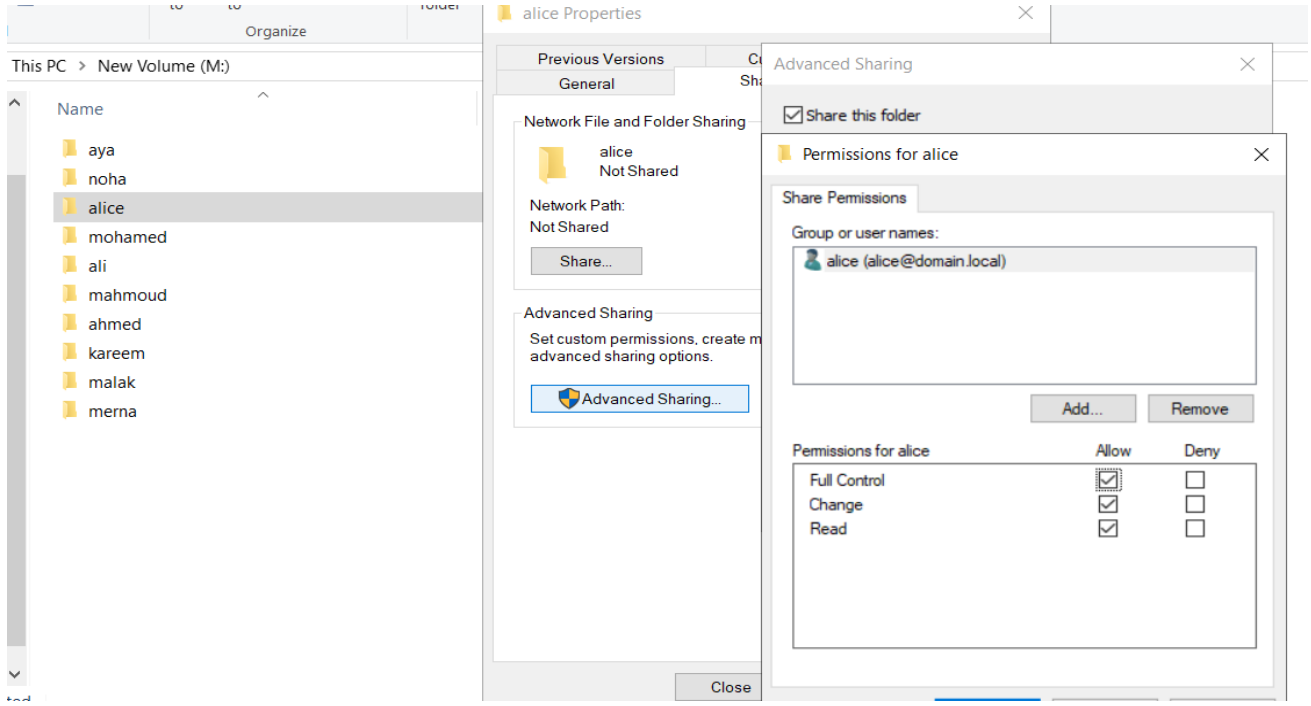


Services Installed on the PDC

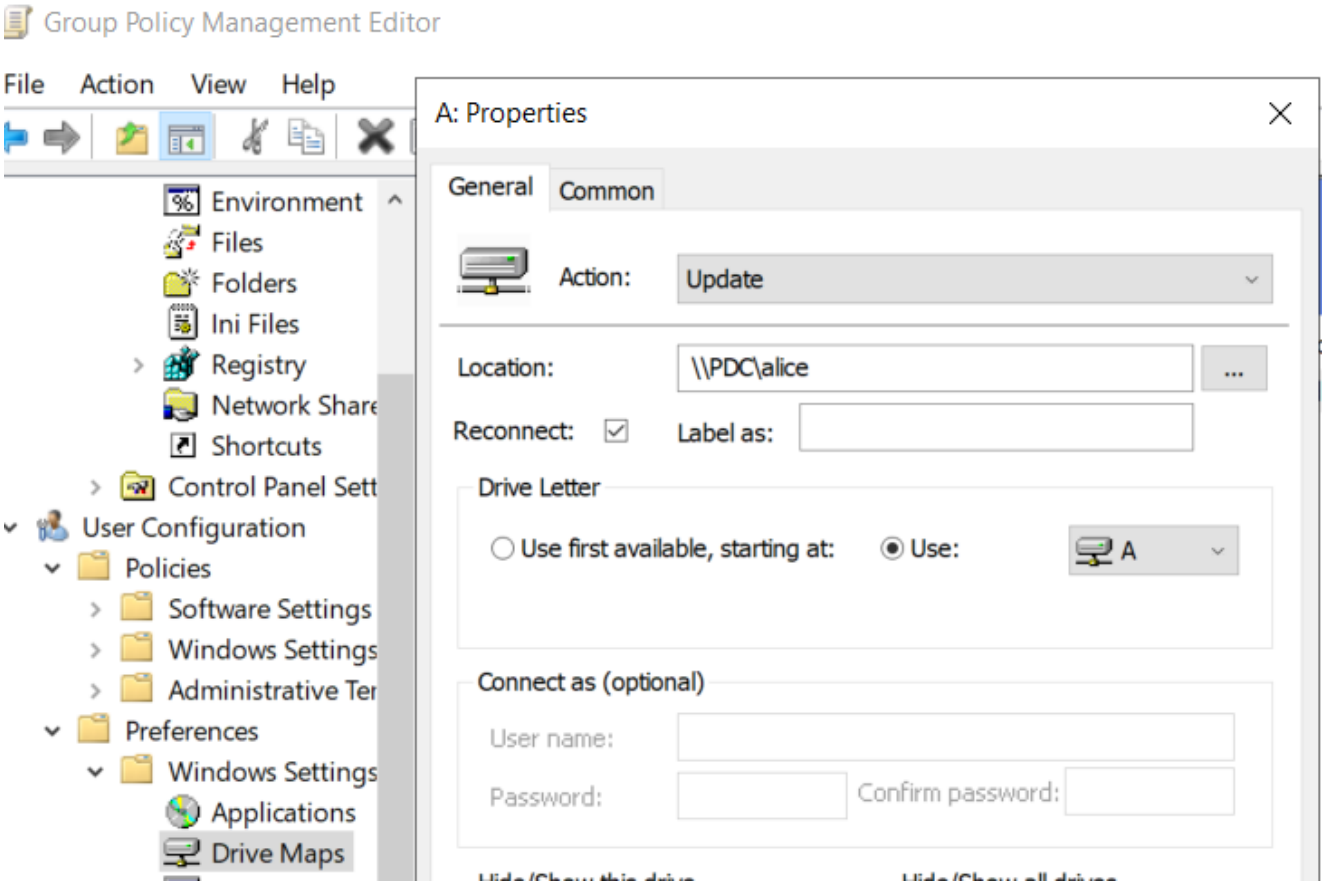


1. User Home Directories

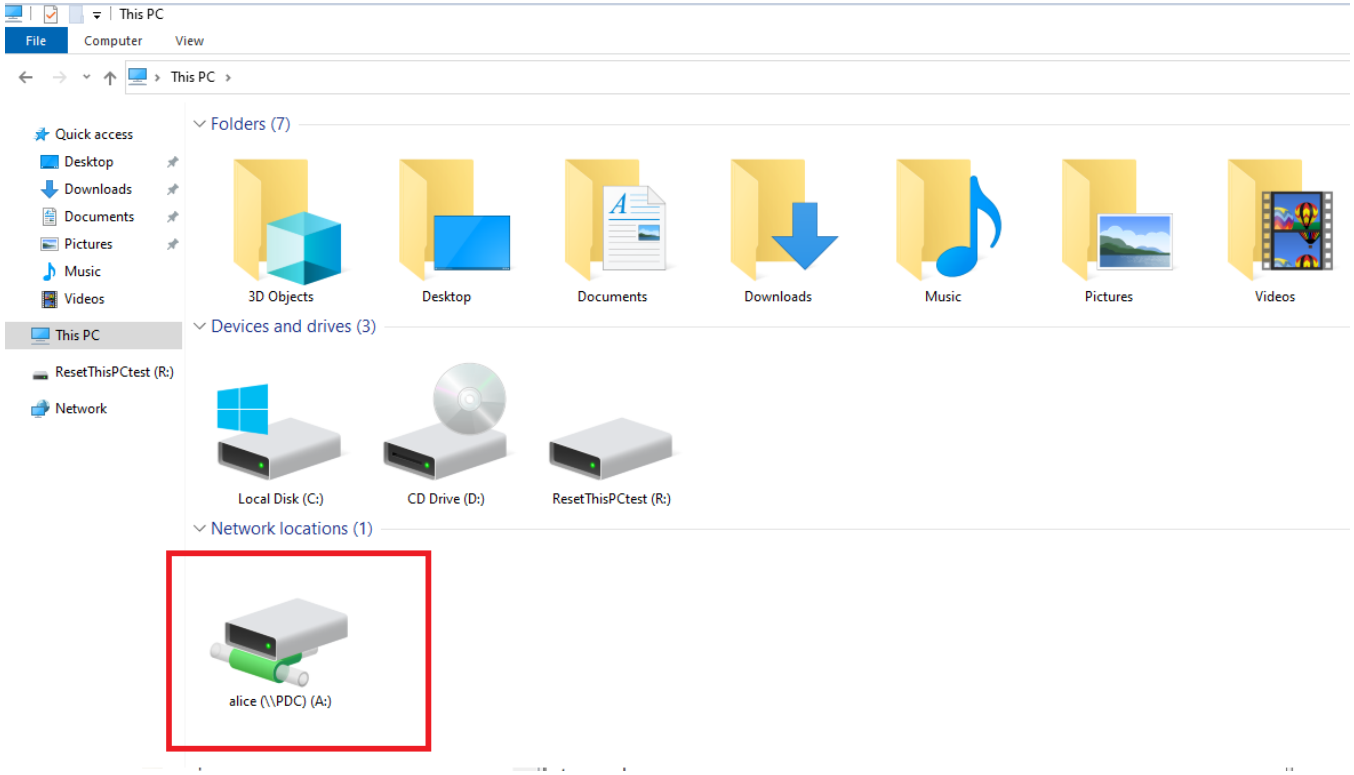
Each domain user has a dedicated home directory. For example, alice has a shared folder with full control permissions (could be restricted using NTFS permissions).



A mapped network drive is assigned to access the home directory.



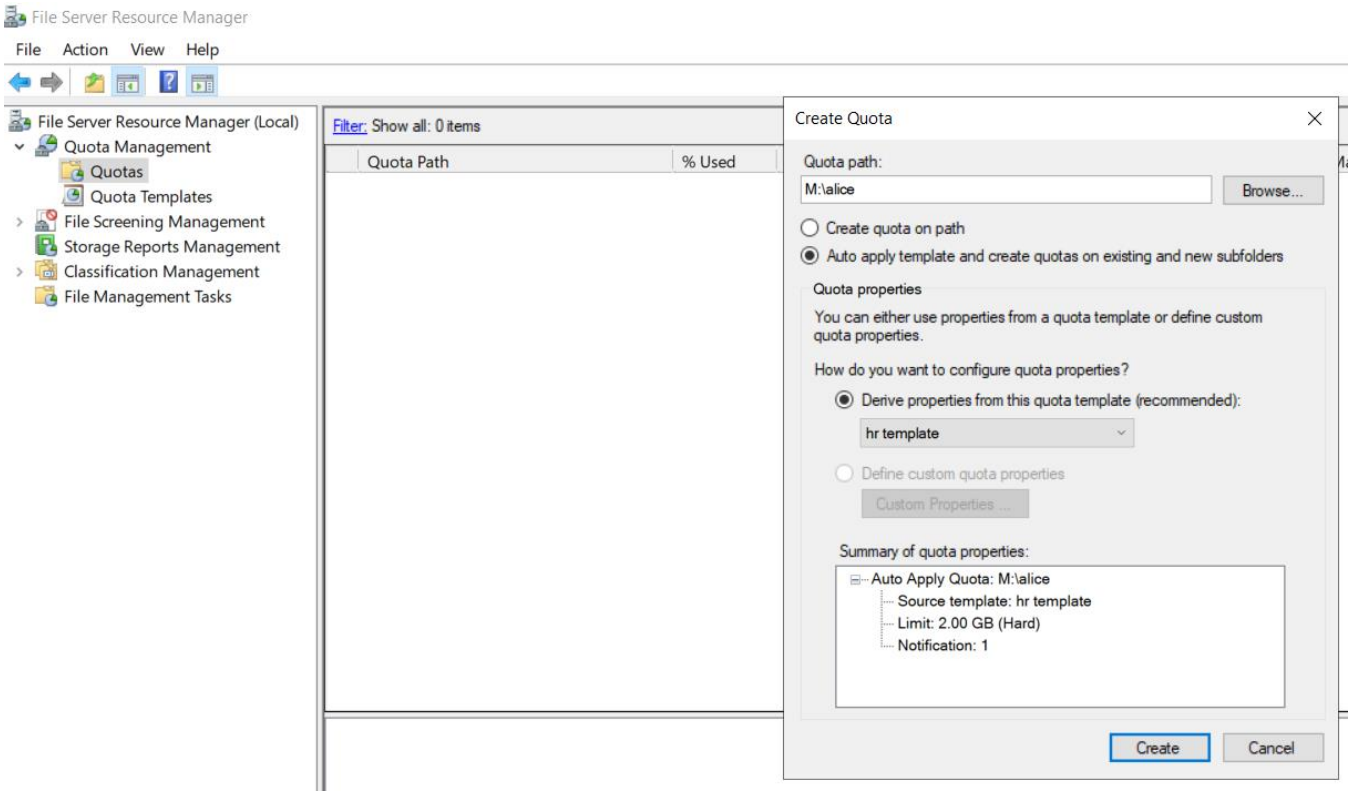
Now you can see the shared file mapped in Alice's account.

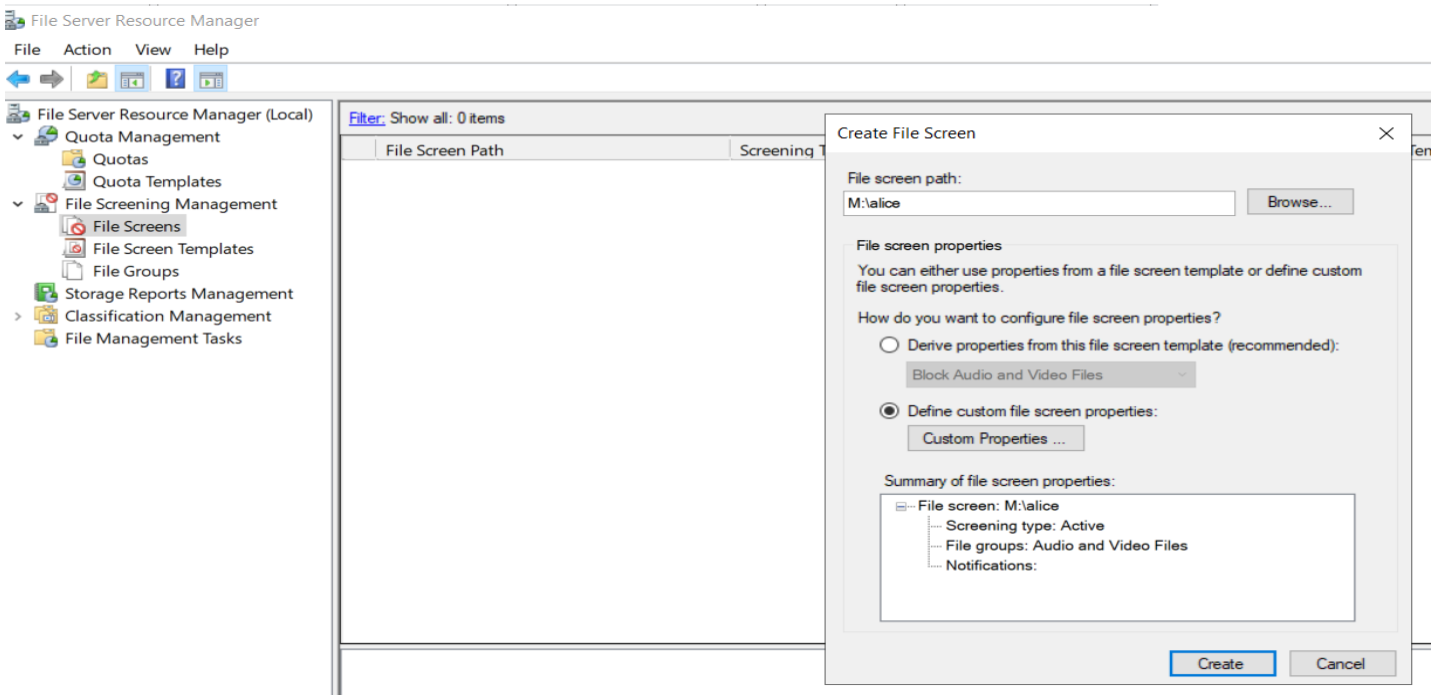


2. Storage Quotas and File Restrictions (Per OU)

Organizational Unit (OU)	Quota Limit	File Restrictions
HR	2 GB	MP4 files not allowed
Graphics	10 GB	No file type restrictions
IT	5 GB	MP4 files not allowed
Sales	4 GB	No file type restrictions

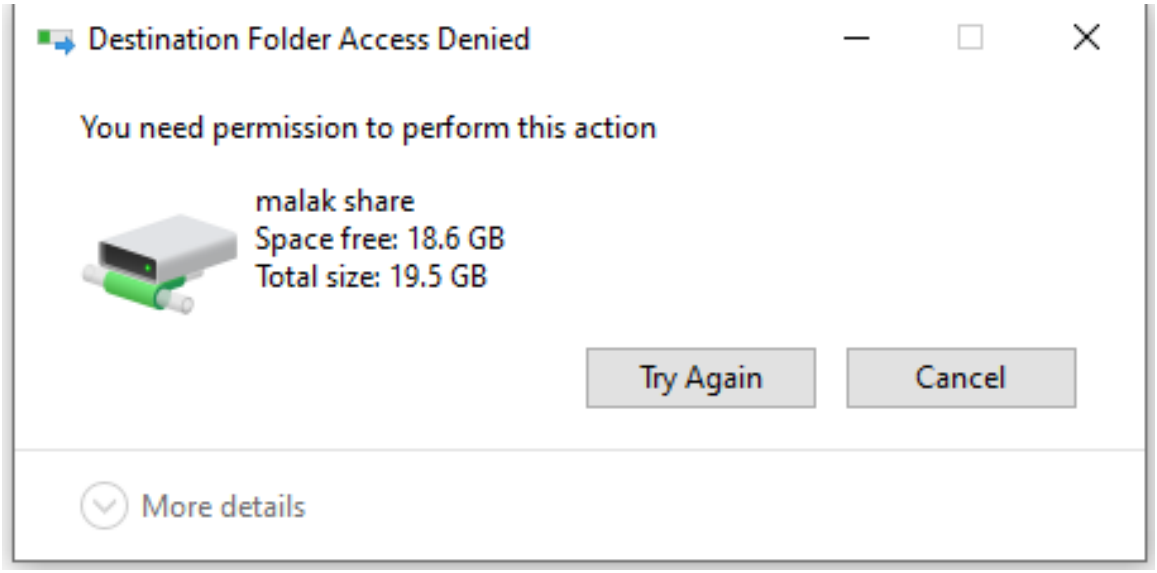
Using FSRM, a custom quota template for HR with 2 GB was created and assigned to Alice's folder.





after screening, Alice and HR users can't upload videos to their folders.

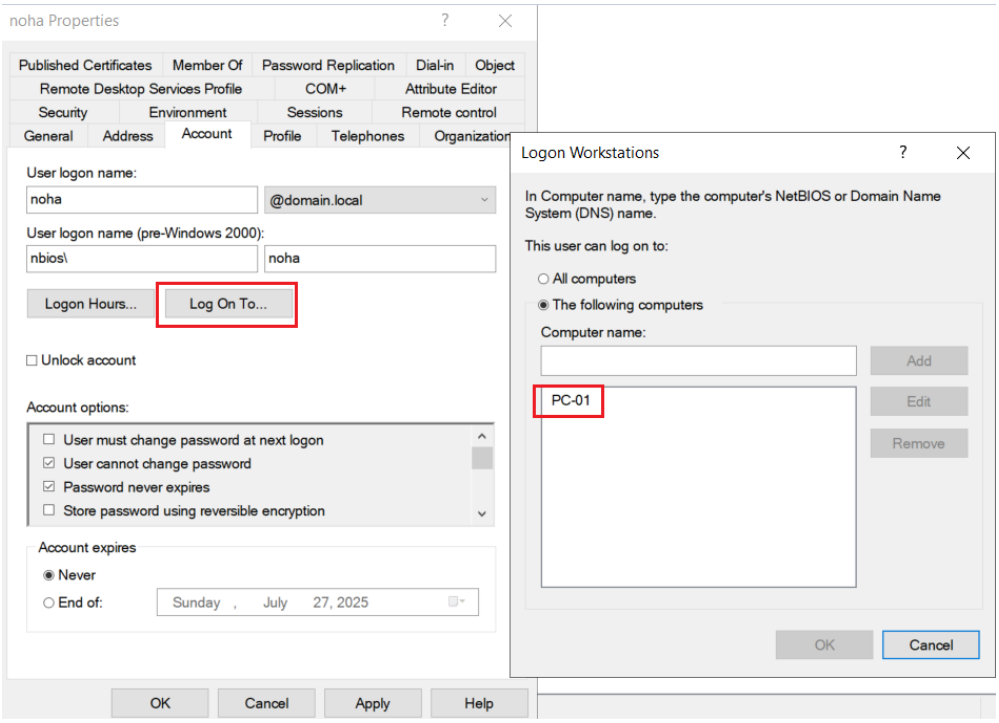
attaching video after screening:-



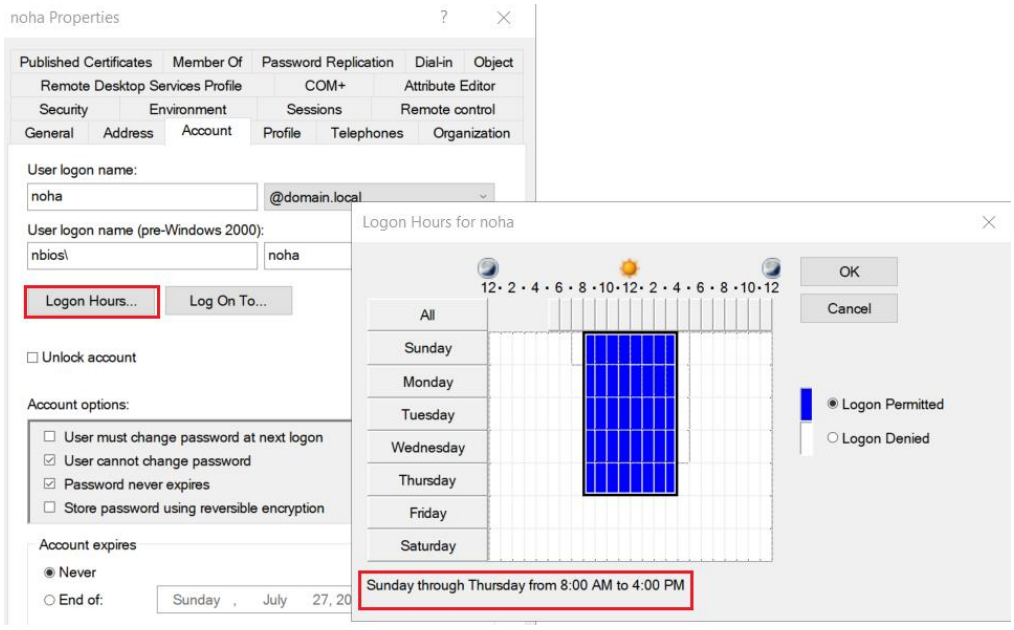
3. Logon Restrictions

All users (except IT) can log on from one assigned PC only, e.g., Noha from HR can log on only to PC-01. They can log in only between 8:00 AM and 4:00 PM, Sunday to Thursday.

a)allowed log in PCs



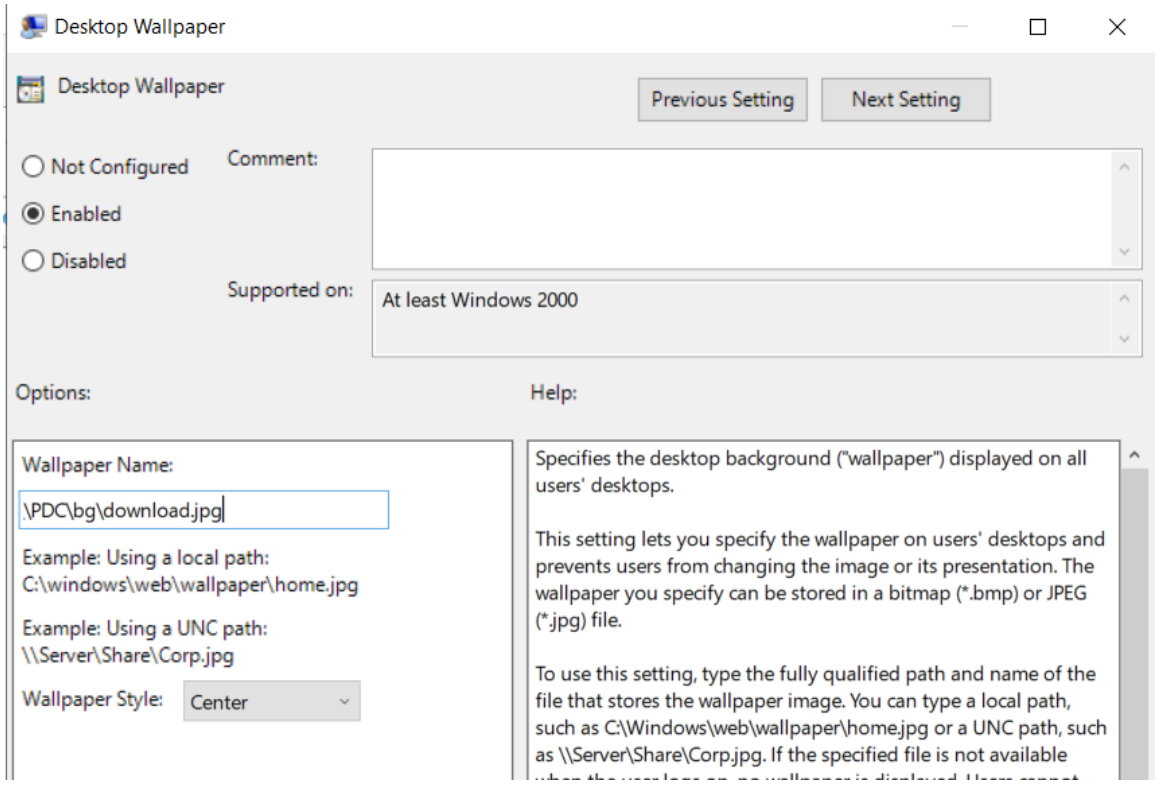
b)allowed log in hours

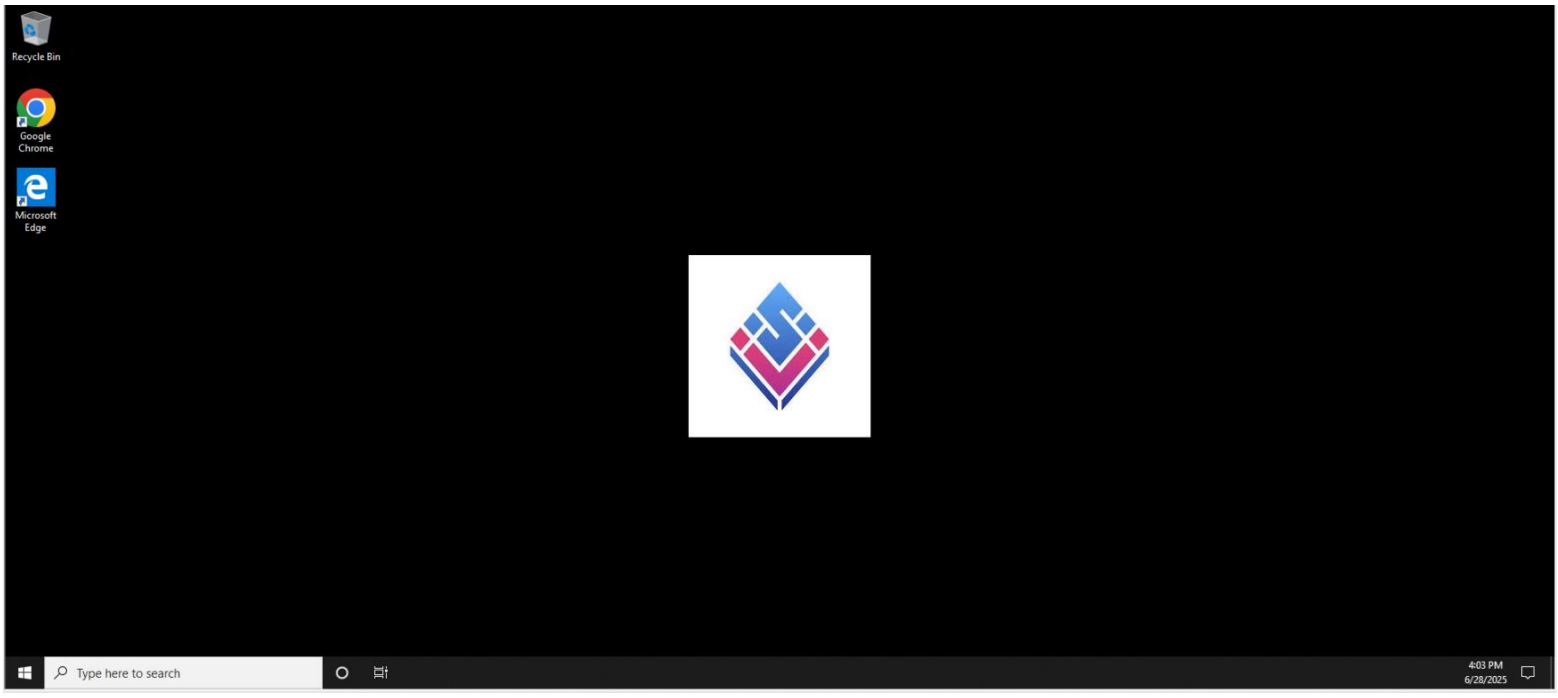


IT users can log on from any PC without time restrictions.

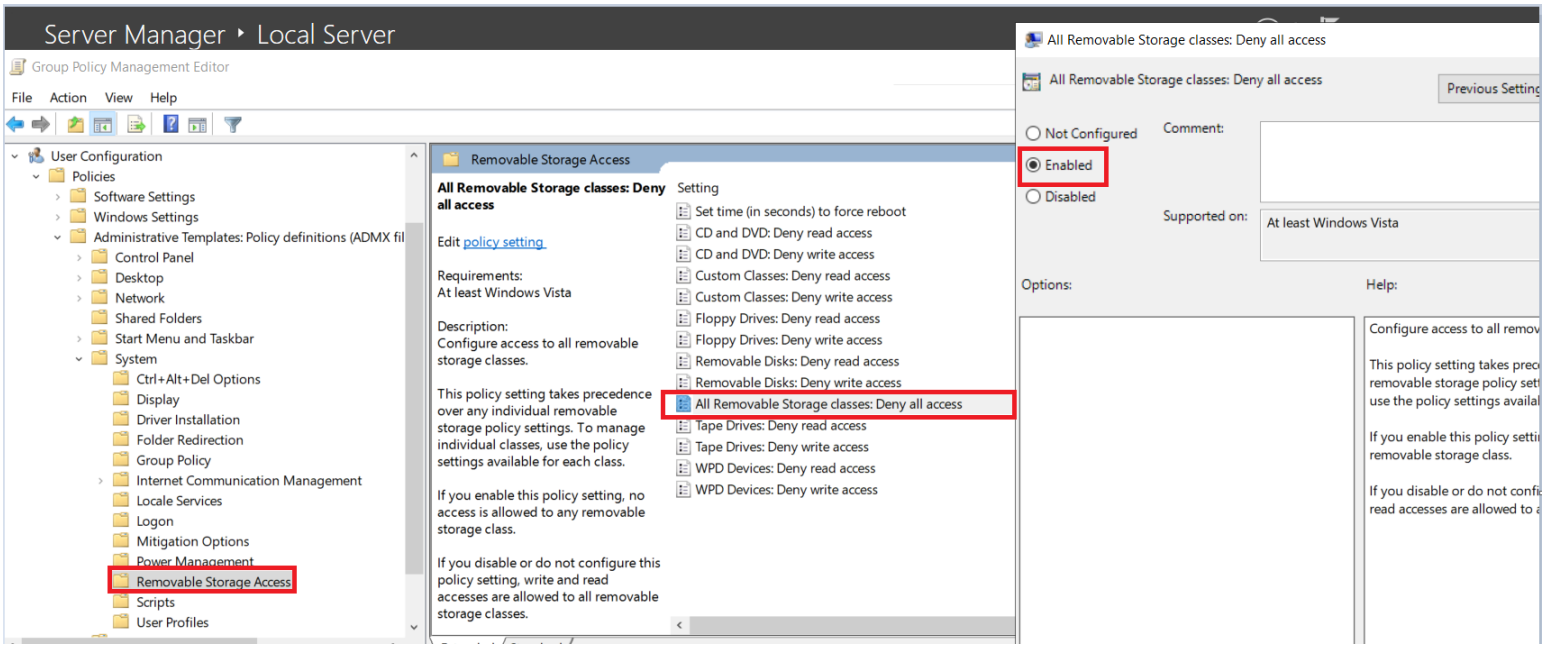
4. Group Policies and Desktop Environment

All domain PCs have a standard desktop background via GPO.



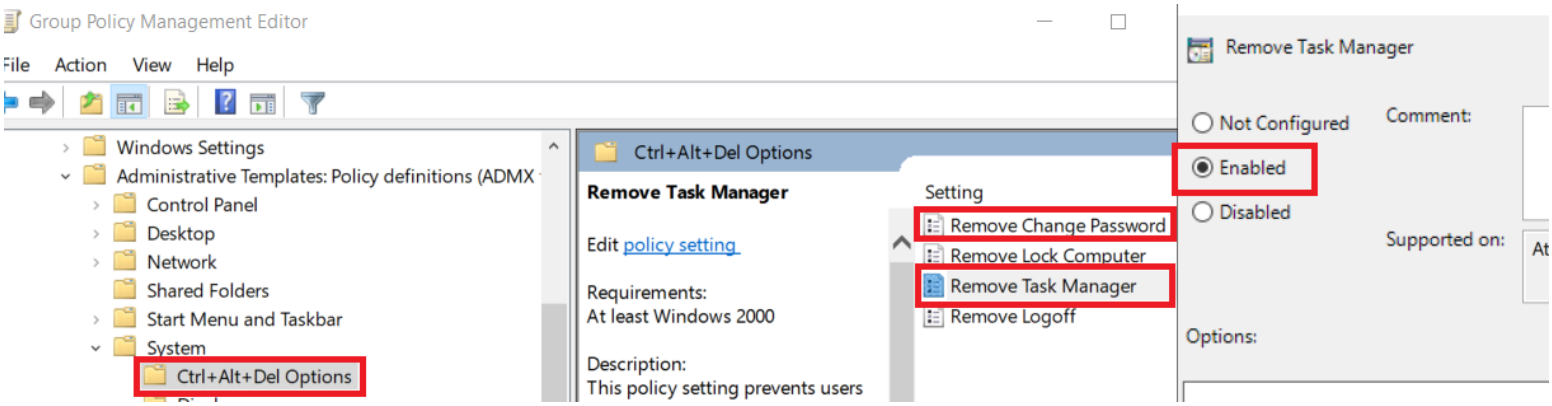


USB and Phone Access: Only IT users can use USB drives and transfer data to/from phones. Other users are blocked via:
User Configuration → Admin Templates → System → All Removable Storage Deny Access (Enabled)

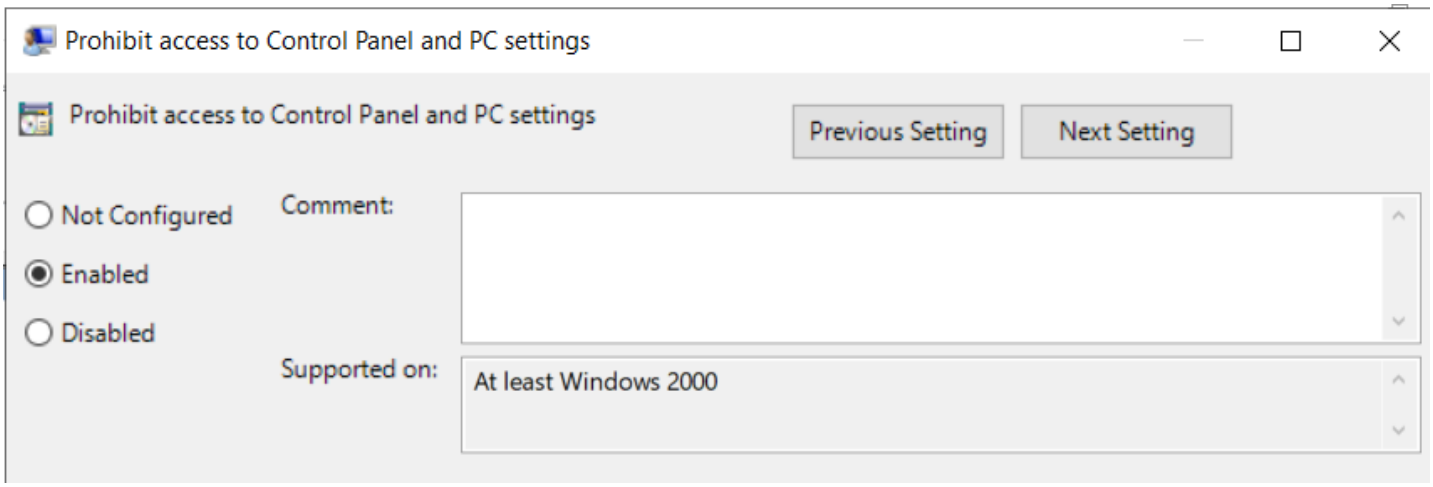


Phone access:
- WPD devices: Deny read access (Enabled)
- WPD devices: Deny write access (Enabled)

Task Manager, password changes, and Control Panel are prohibited for all except IT users via:



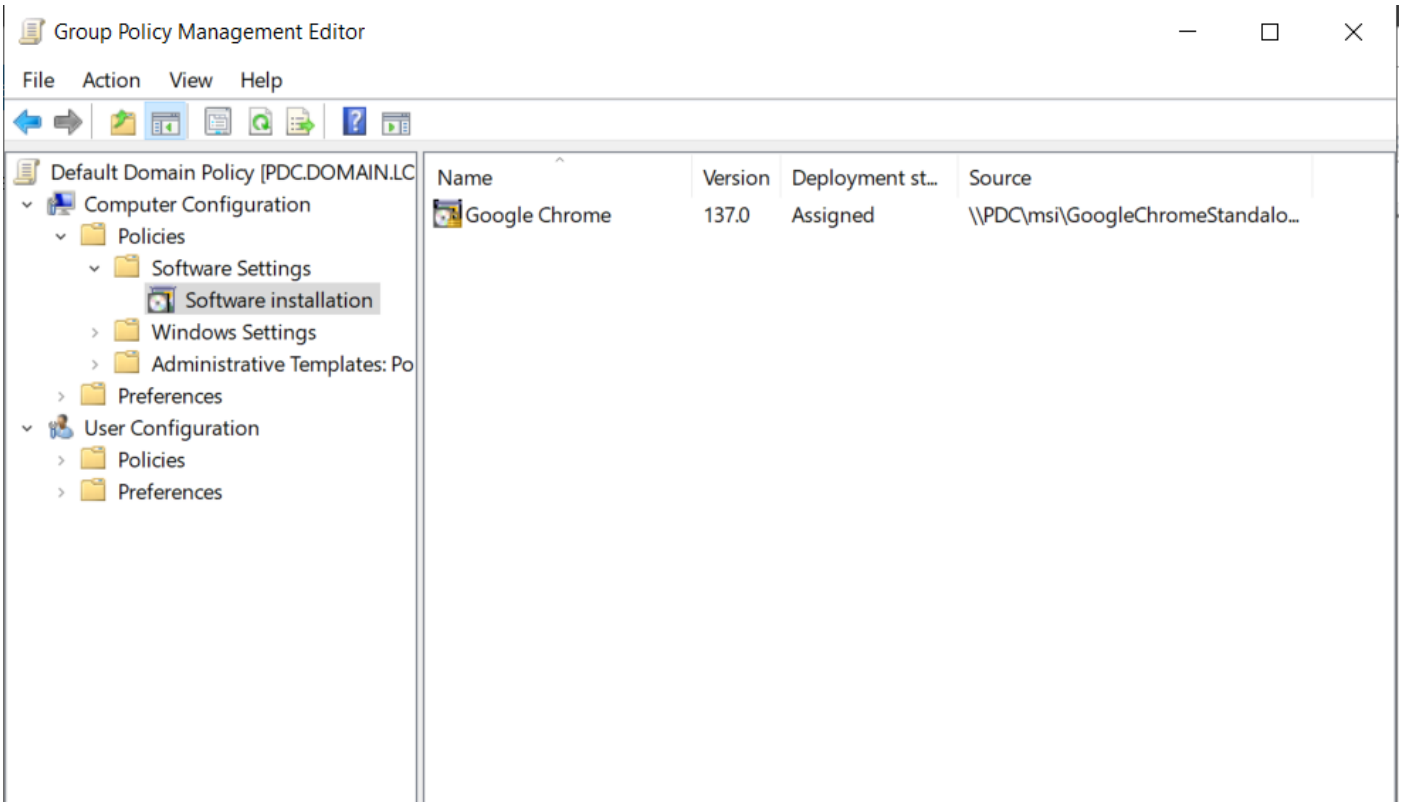
User Configuration → Admin Templates → Control Panel → Prohibit Access to Control Panel and PC Settings (Enabled).



Now the users with this policy applied can't access control panel

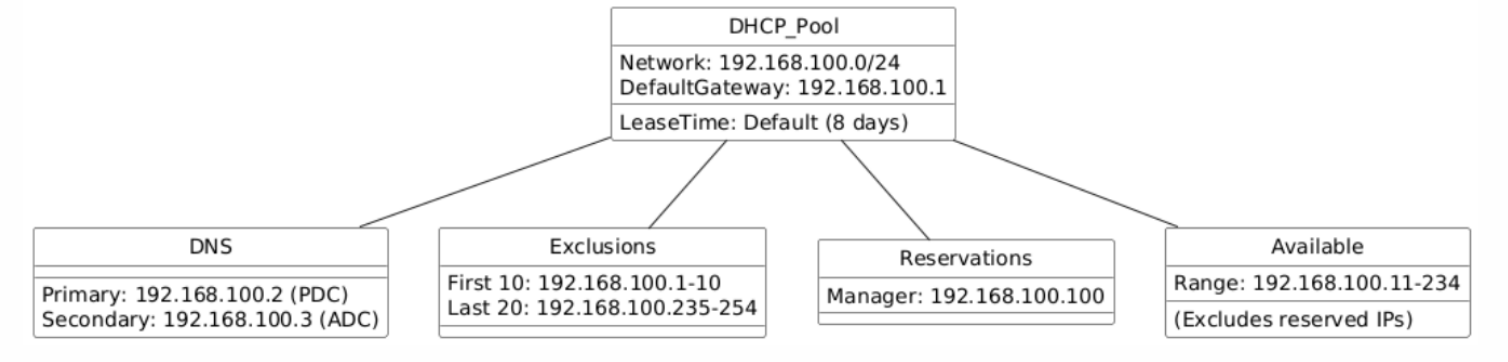
5. Software Deployment

All PCs joining the domain automatically get Google Chrome installed via GPO:
GPO → Computer Configuration → Policies → Software Settings → Software Installation → New Package.



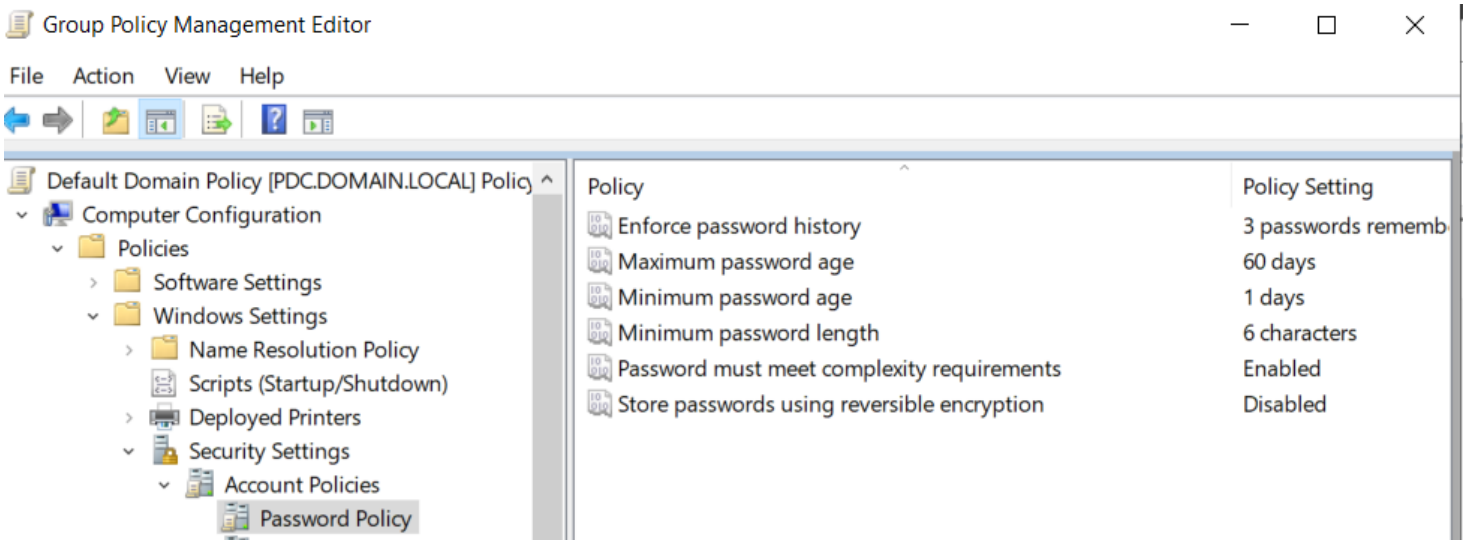
6. DHCP Scope

Configured DHCP scope on the server.



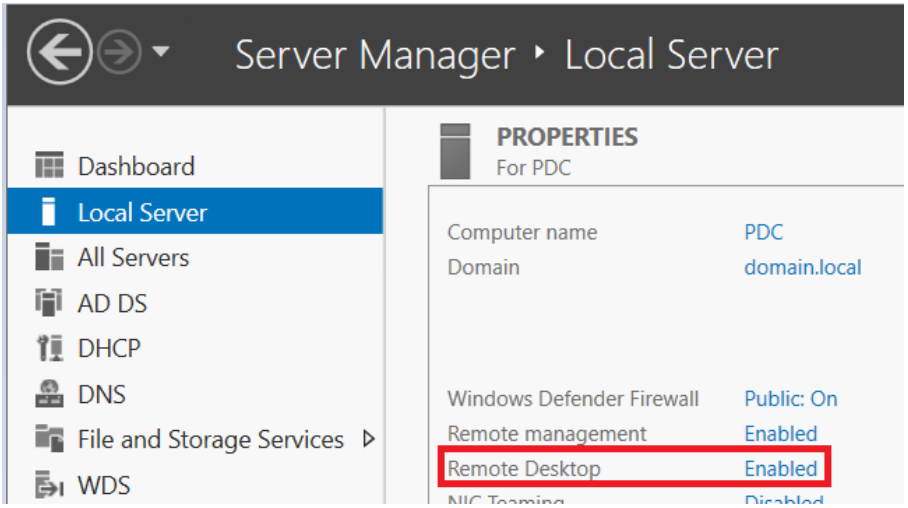
7. Password Policy

Passwords must change every 60 days, have a minimum length of 6 characters with complexity, and remember the last 3 passwords.
Configured via: Computer Configuration → Windows Settings → Security → Account Policies → Password Policy.



8. Enabling Remote Desktop

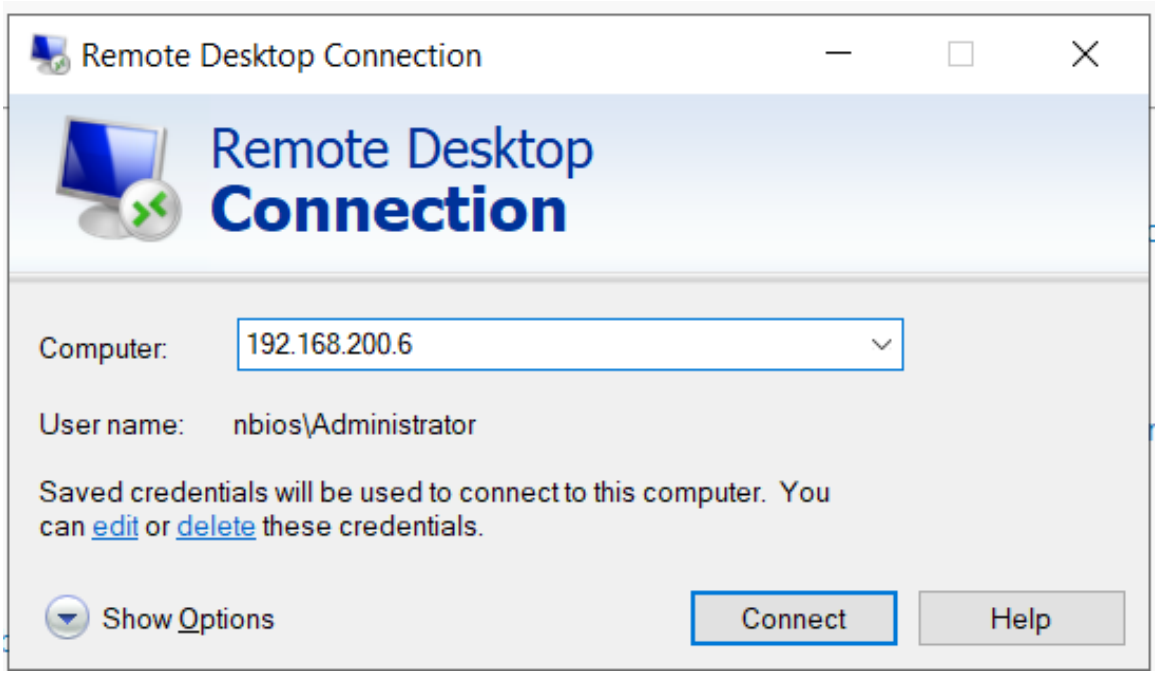
On server: Local Server → Remote Desktop → Enable



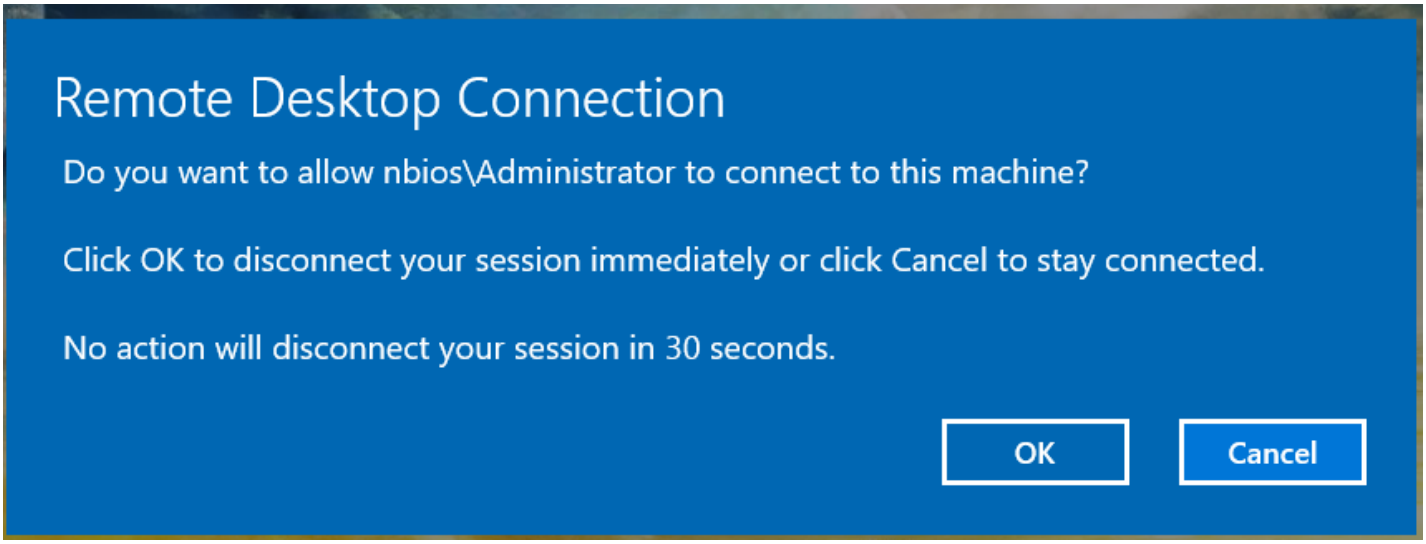
On clients via GPO:
- Allow users to connect remotely (Enabled)
- Require user authentication (Disabled)

Firewall: Added inbound rule for Remote Desktop.

Connected remotely to 192.168.200.6 (PC-01).

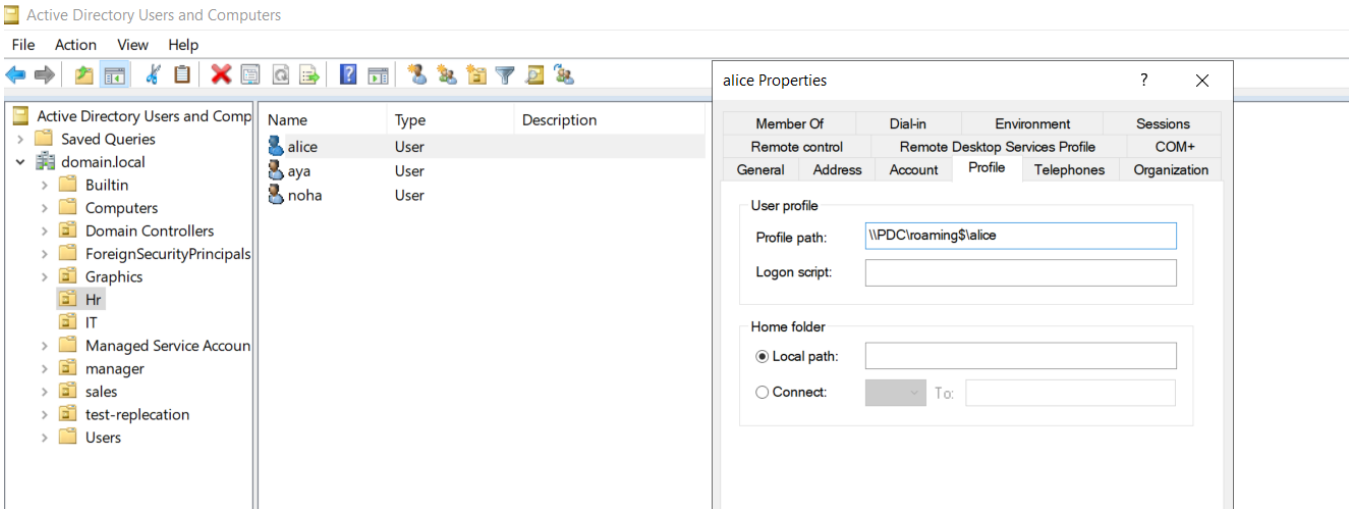


If another user is logged in, he will receive this message



After that the connection will be completed and I will be logged as the user administrator

9. Roaming Profiles



Created a hidden shared folder ($) and set the profile path in user properties.

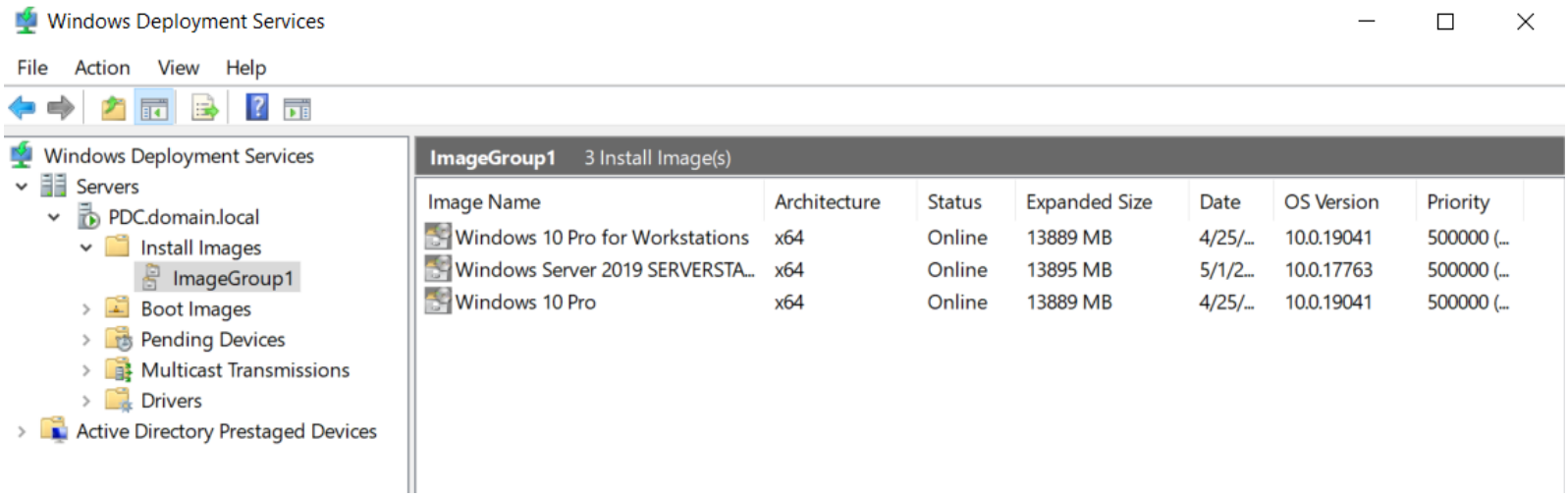
Now when Alice logs in from any PC, her profile follows her.

10. Windows Deployment Service (WDS)

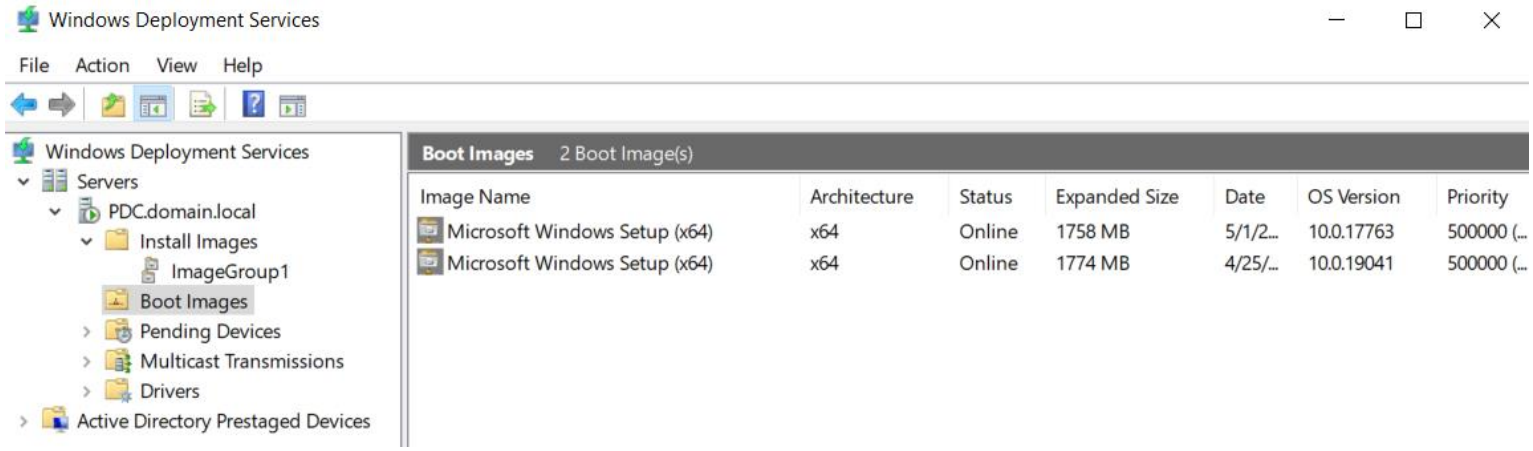
Installed and configured AD DS, DHCP, DNS, with WDS image store on NTFS. Installed WDS, added install.wim under Install Images and boot.wim under Boot Images. Clients boot via PXE to install Windows.

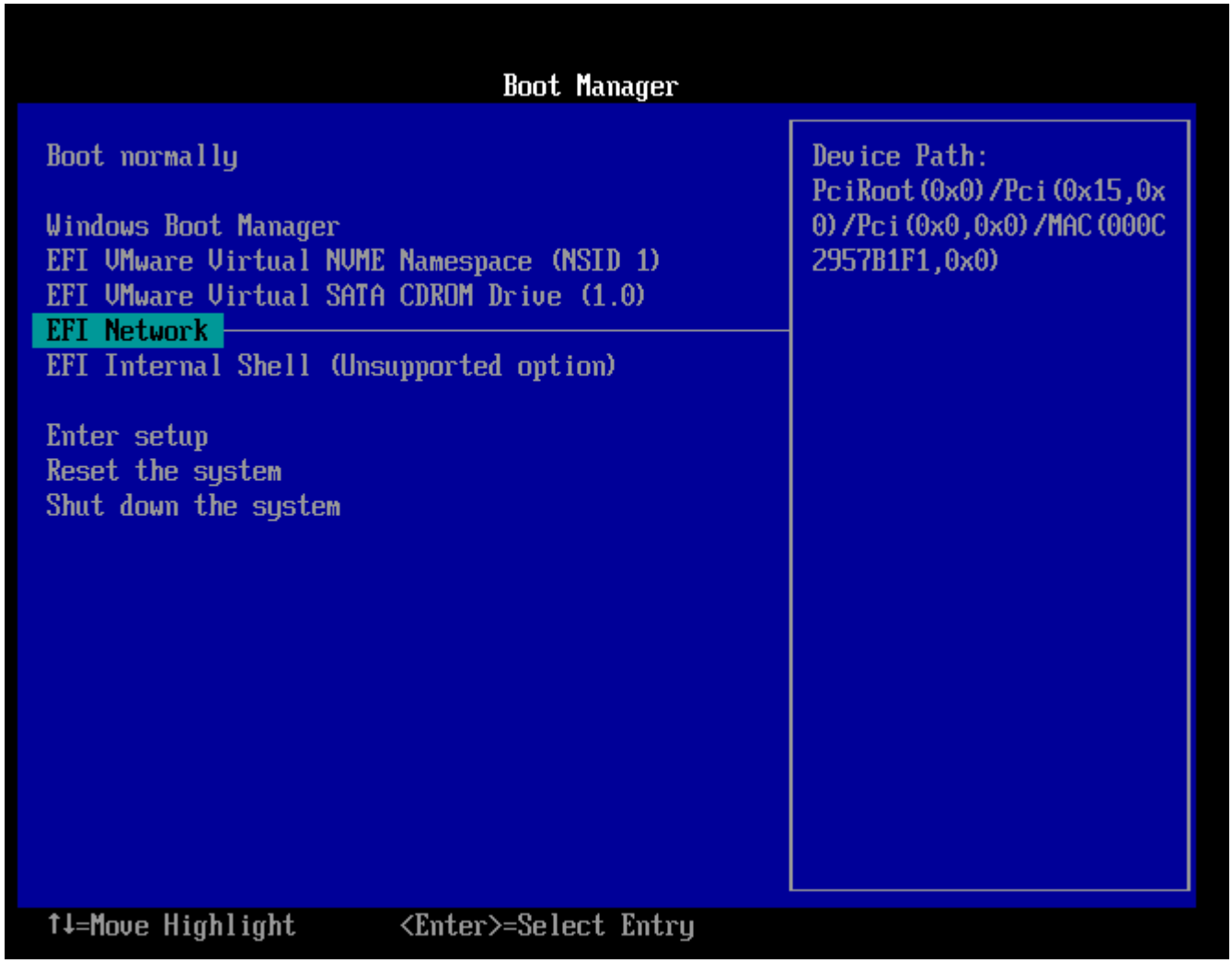
Install WDS and start the service(right click on the domain name>>all tasks >> start)

Right click on install images and add the **install.wim** file



Right click on boot images and add the **boot.wim** file





The client can boot from the Network from the boot menu and continue setting up the windows normally