

ACTIVE DIRECTORY HOME LAB

◆ Pre-Requisites for Active Directory Home Lab

1 Windows Server ISO (Domain Controller)

- **Windows Server 2019 or Windows Server 2022**
- Standard or Datacenter edition
- Used to configure:
 - Active Directory Domain Services (AD DS)
 - DHCP Server
 - DNS Server
 - RAS/NAT
- Minimum 4 GB RAM recommended (8 GB preferred)
- 2 Network Adapters (Internet + Internal)

This machine acts as the **Domain Controller (DC)**.

2 Windows Client ISO

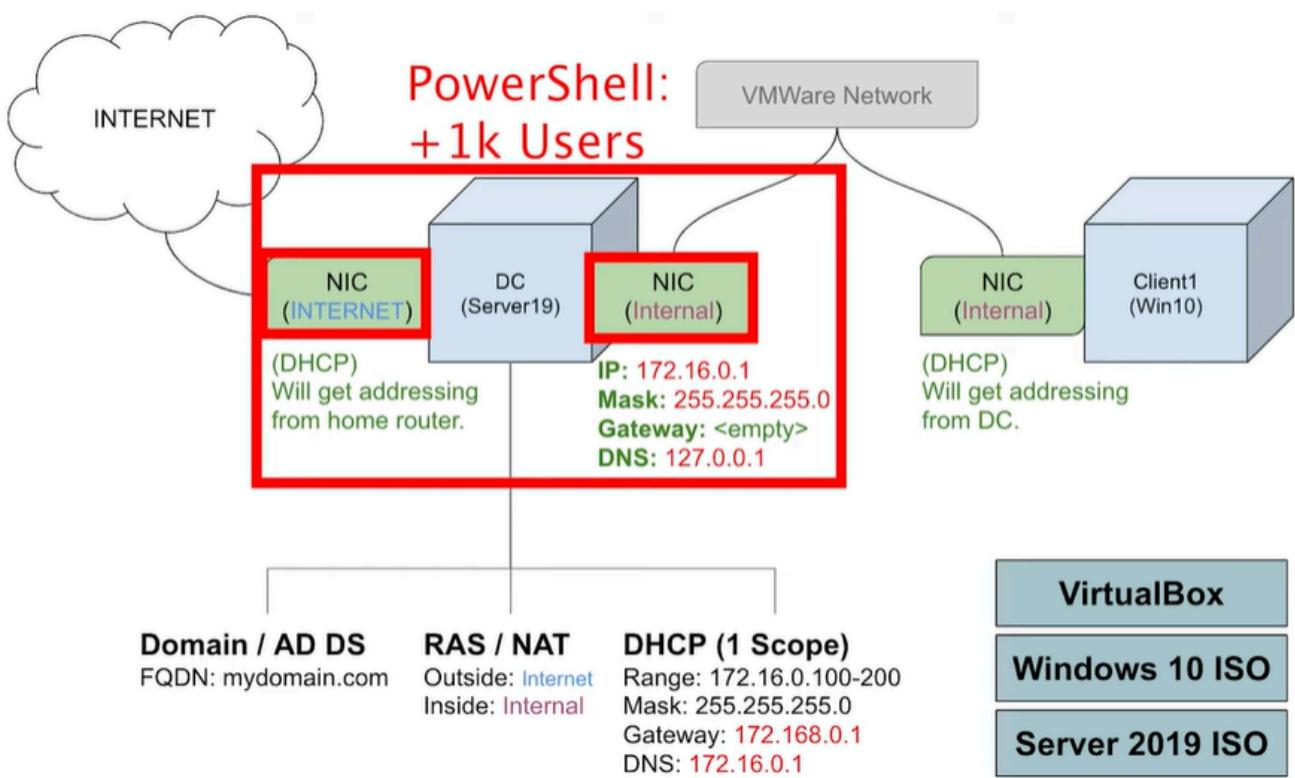
- **Windows 10 Enterprise / Professional**
or
- **Windows 11 Enterprise / Professional**
- Used as domain client machine
- Must support domain join feature
- Minimum 4 GB RAM recommended

This system is used to:

- Join the Active Directory domain
- Test GPOs
- Access shared folders
- Validate security configurations

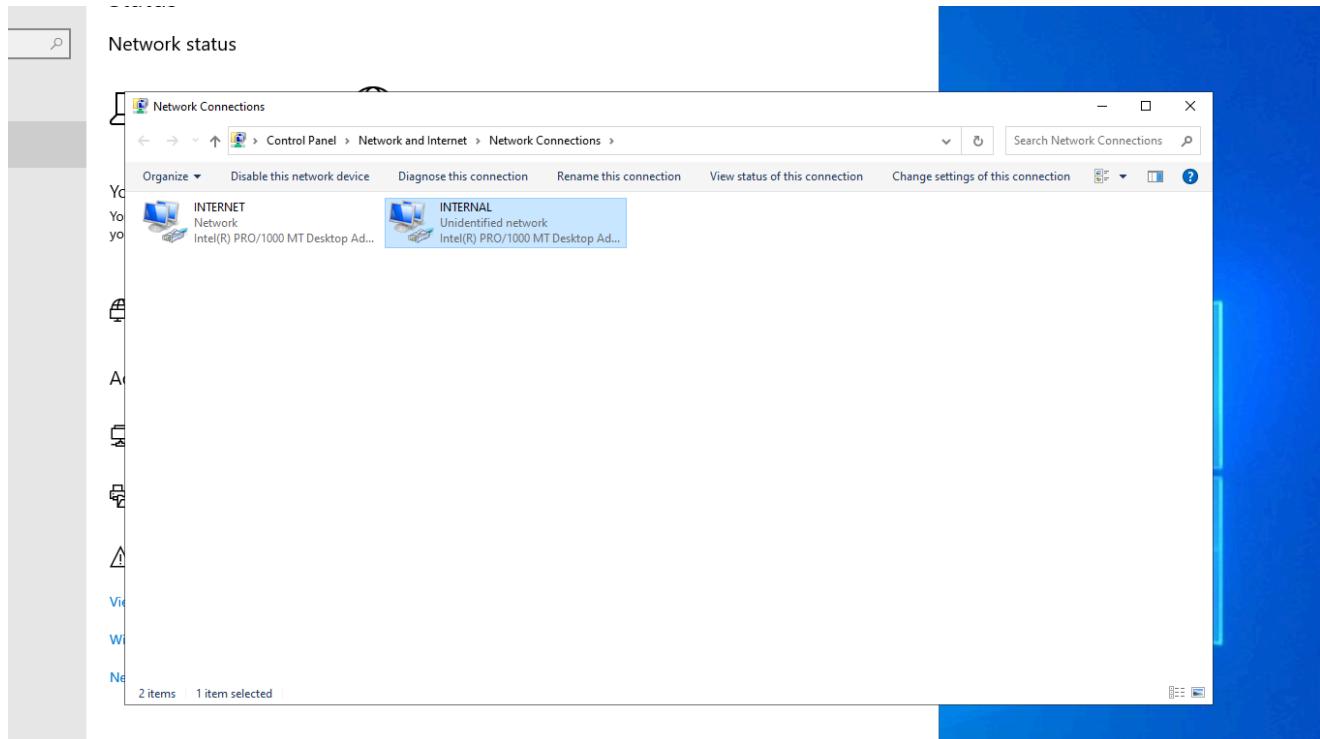
3 Virtualization Software

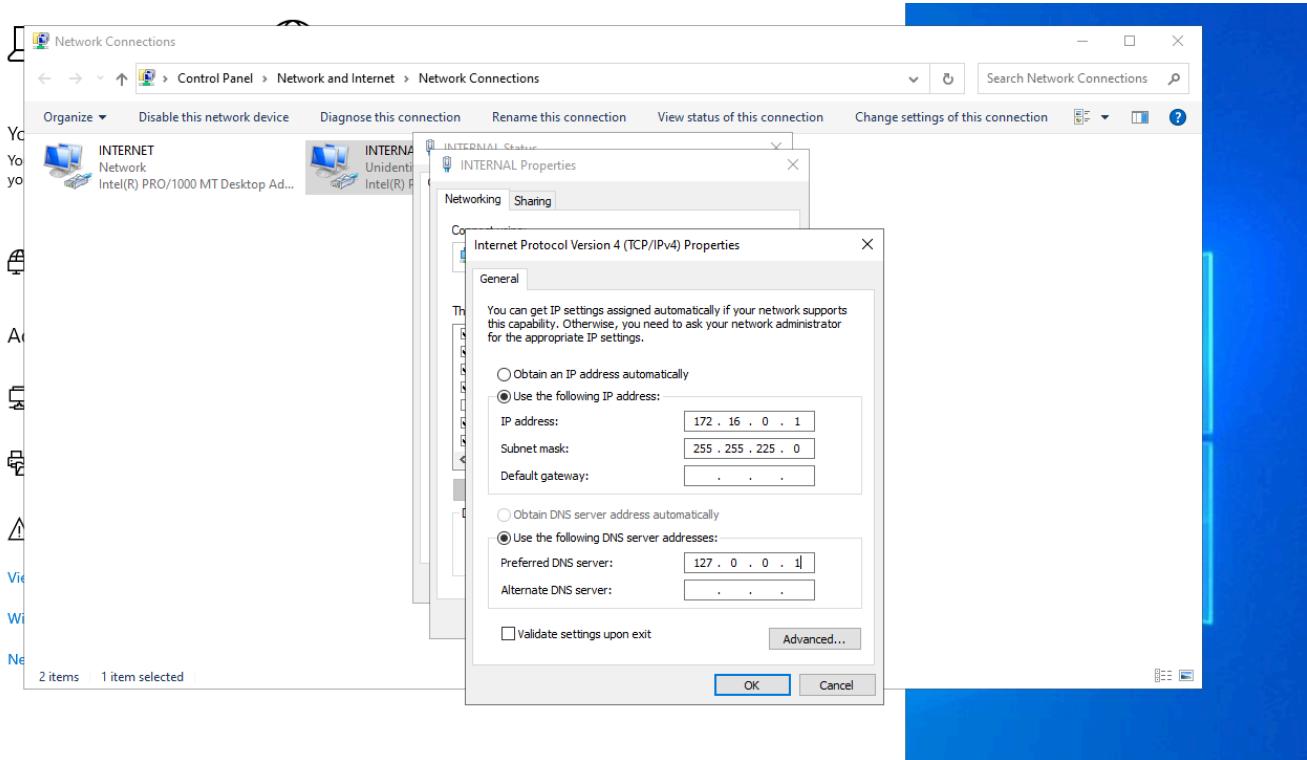
- **VirtualBox or VMware Workstation**
- Used to create:
 - 1 Domain Controller VM
 - 1 or more Client VMs
- Supports multiple network adapters (Internal + NAT/Bridged)



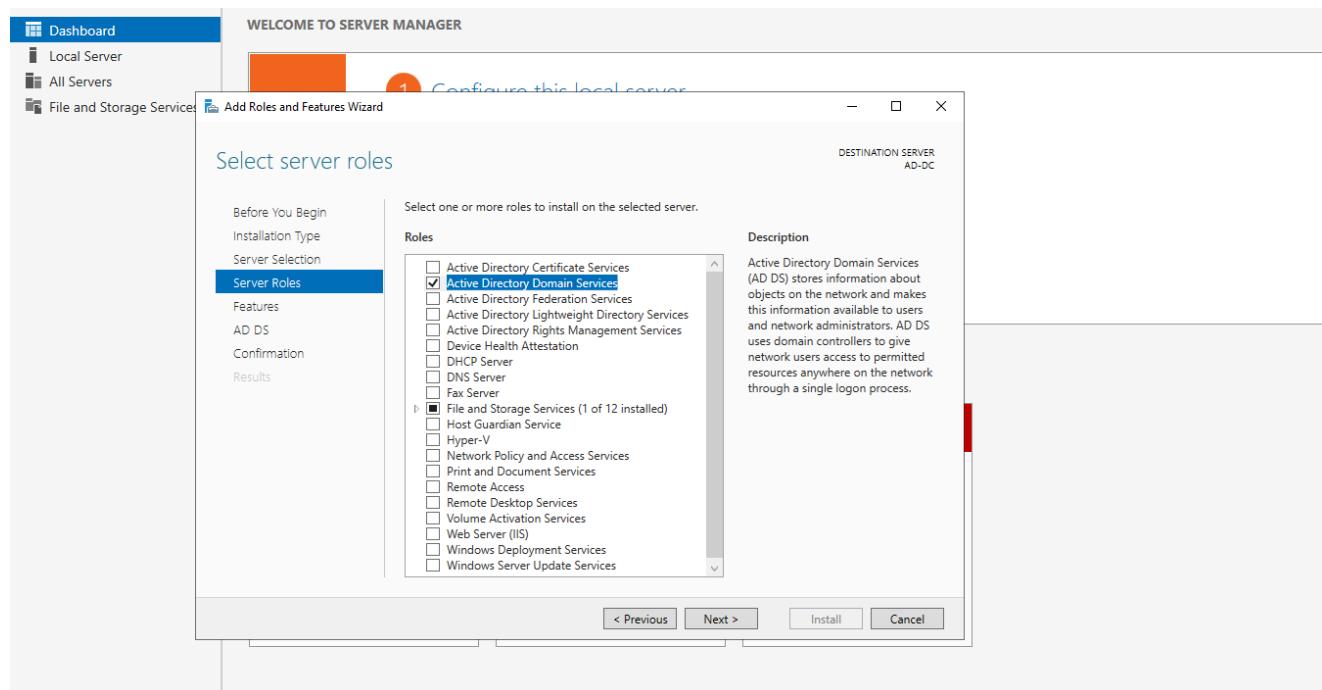
Network Connections window showing two configured adapters named INTERNET and INTERNAL. This setup separates external internet access from the internal domain network.

The INTERNAL adapter was configured with static IP address 172.16.0.1 and subnet mask 255.255.255.0. This IP acts as the gateway for client machines inside the domain network.

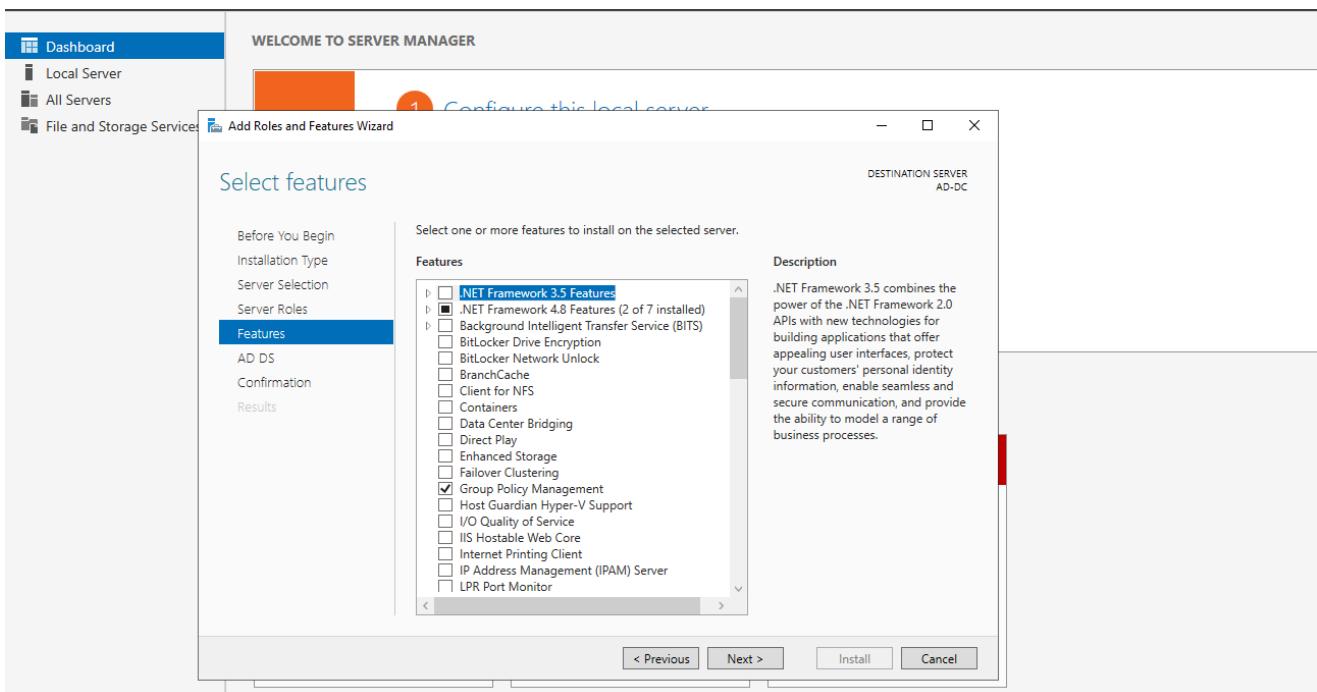




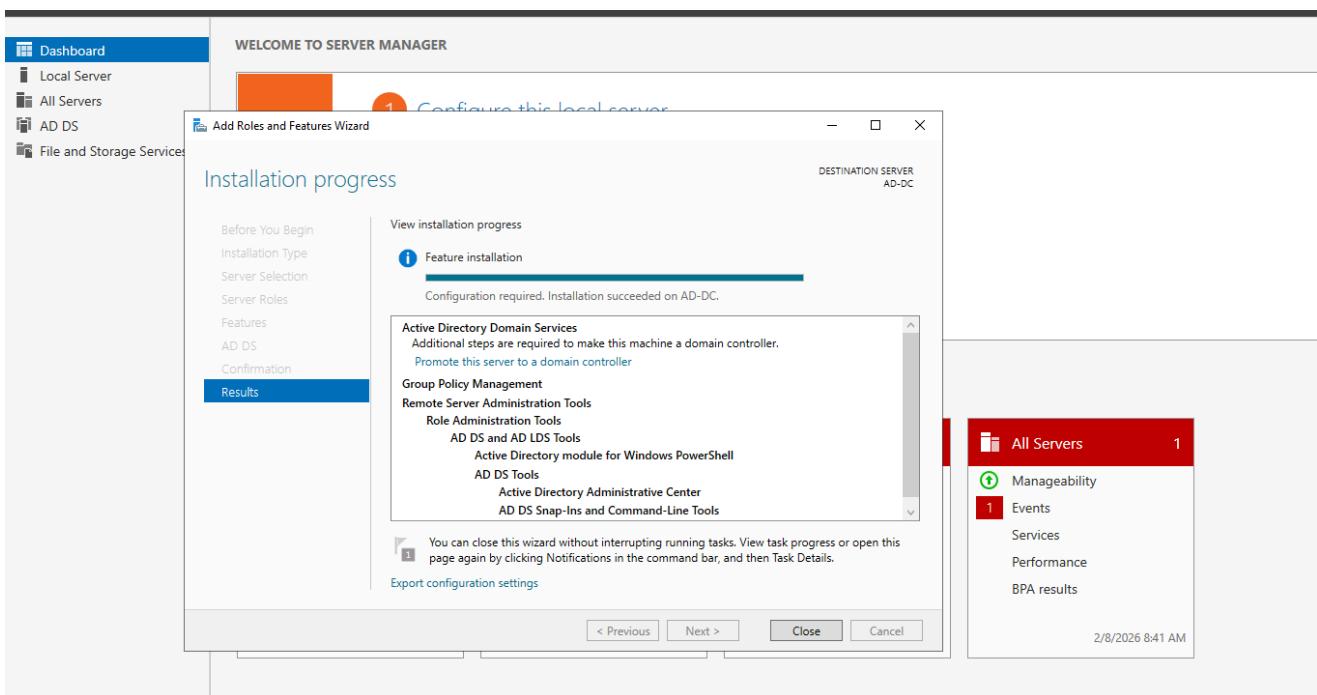
Add Roles and Features Wizard was opened to install server roles. Active Directory Domain Services (AD DS) role was selected for domain configuration.



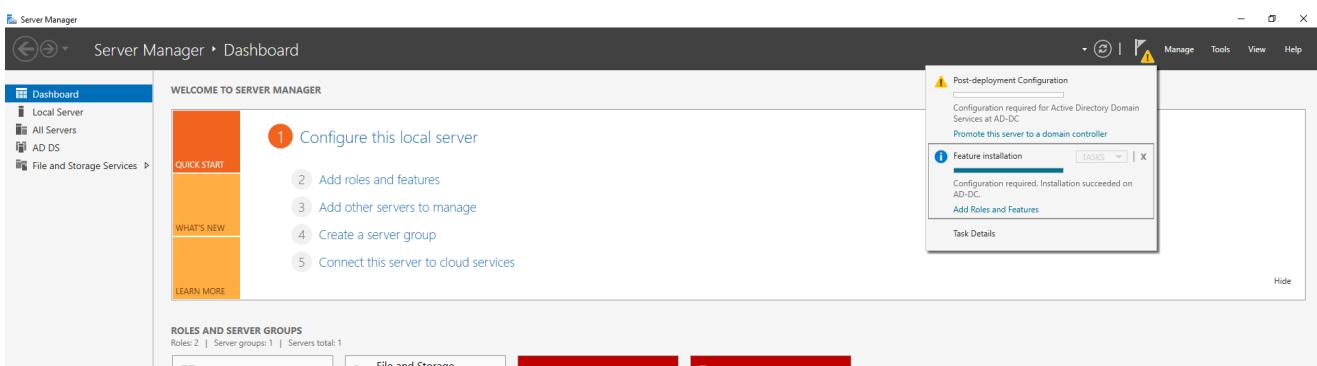
Required features and management tools were selected to support AD DS installation. This ensures proper administration and management of the domain.



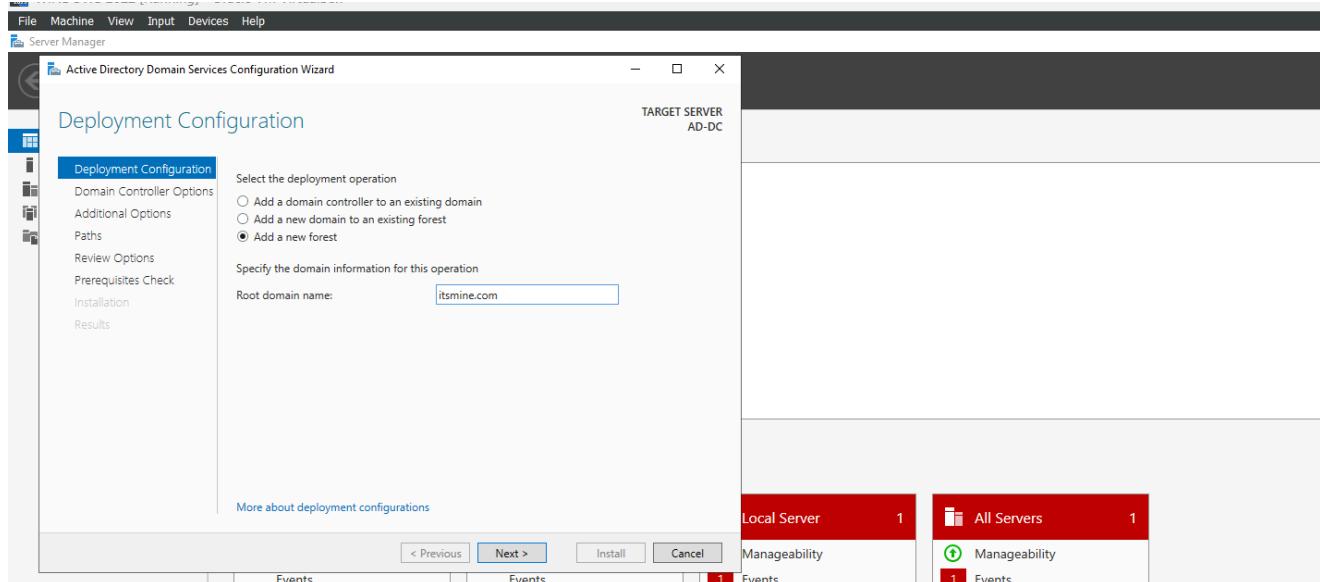
Active Directory Domain Services role installation was completed successfully. The server was prepared to be promoted as a Domain Controller



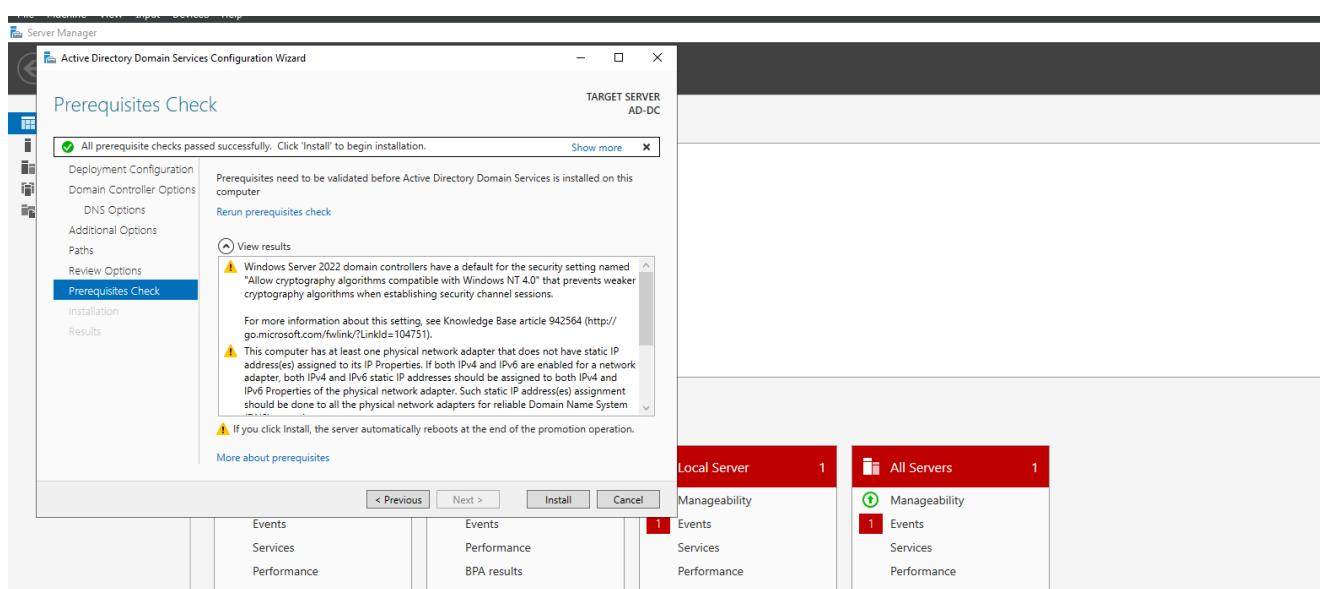
The option “Promote this server to a domain controller” was selected from Server Manager. This begins the domain creation process.



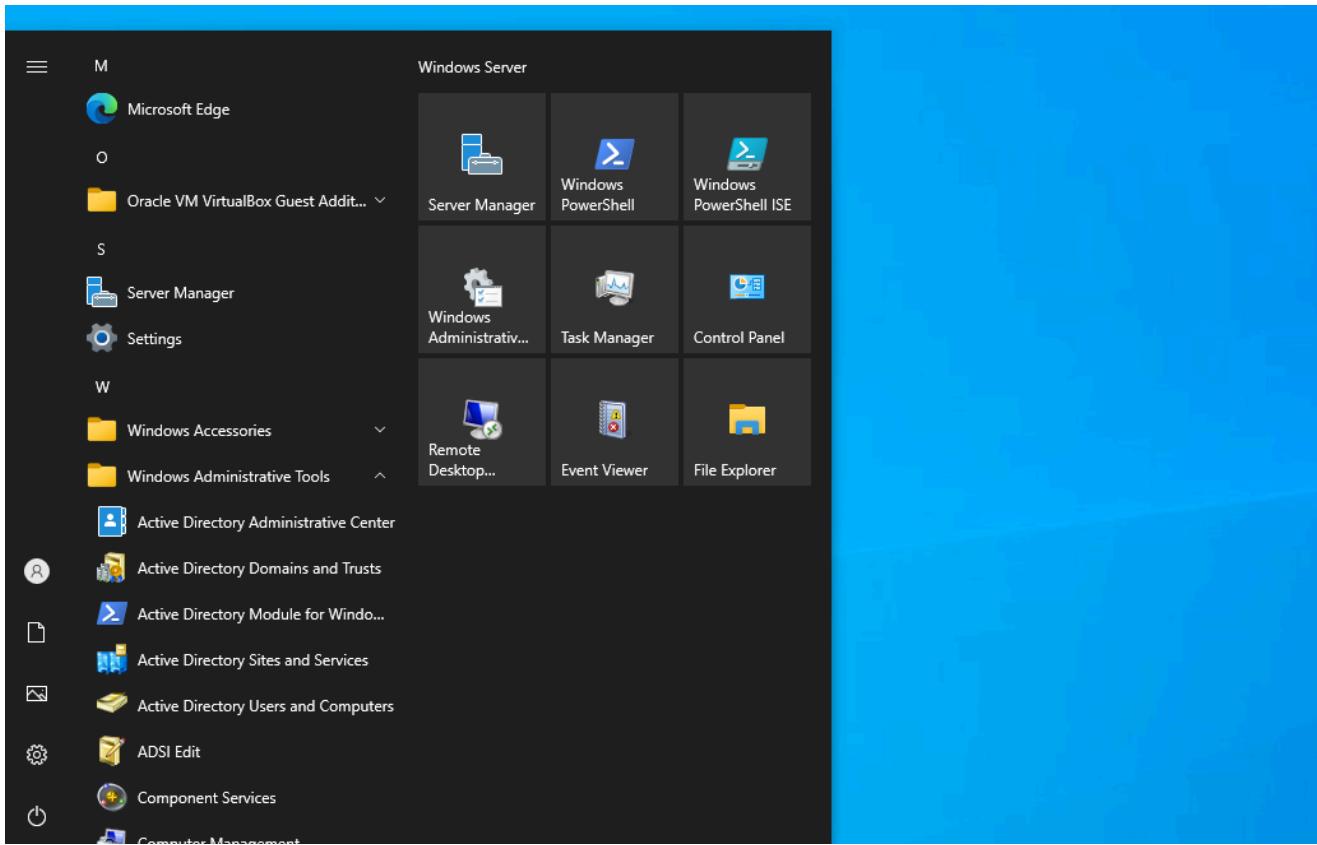
A new forest was created with the root domain name itsmine.com. This establishes the primary Active Directory domain environment.



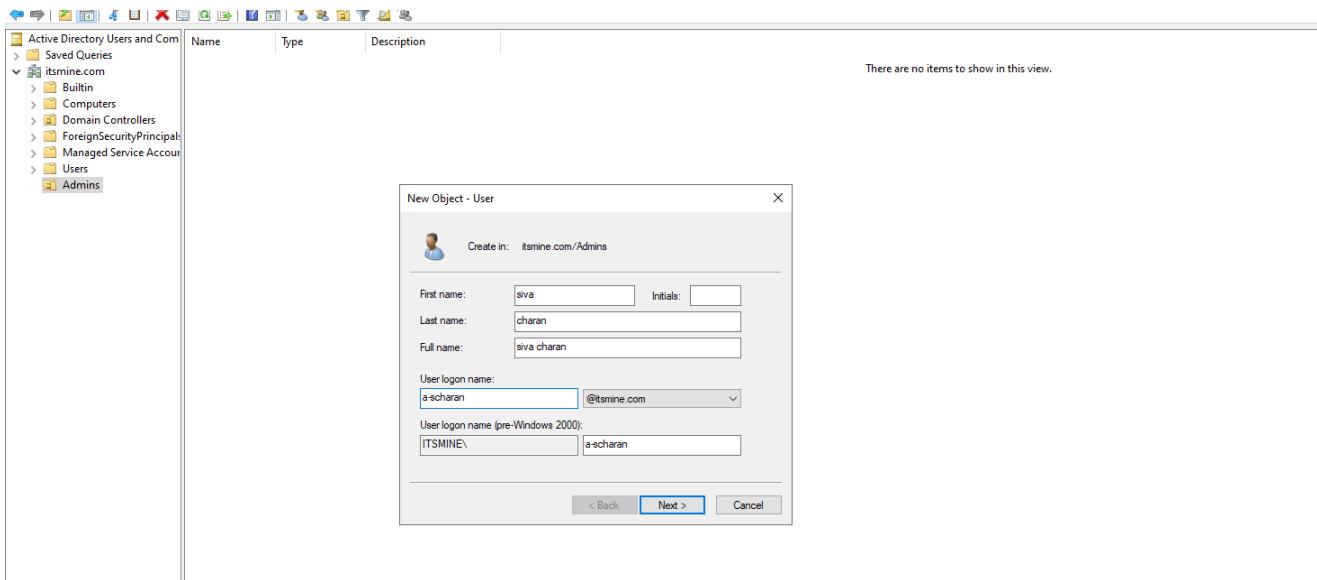
Prerequisite checks were completed before finalizing the Domain Controller promotion. The server was validated for AD DS configuration.



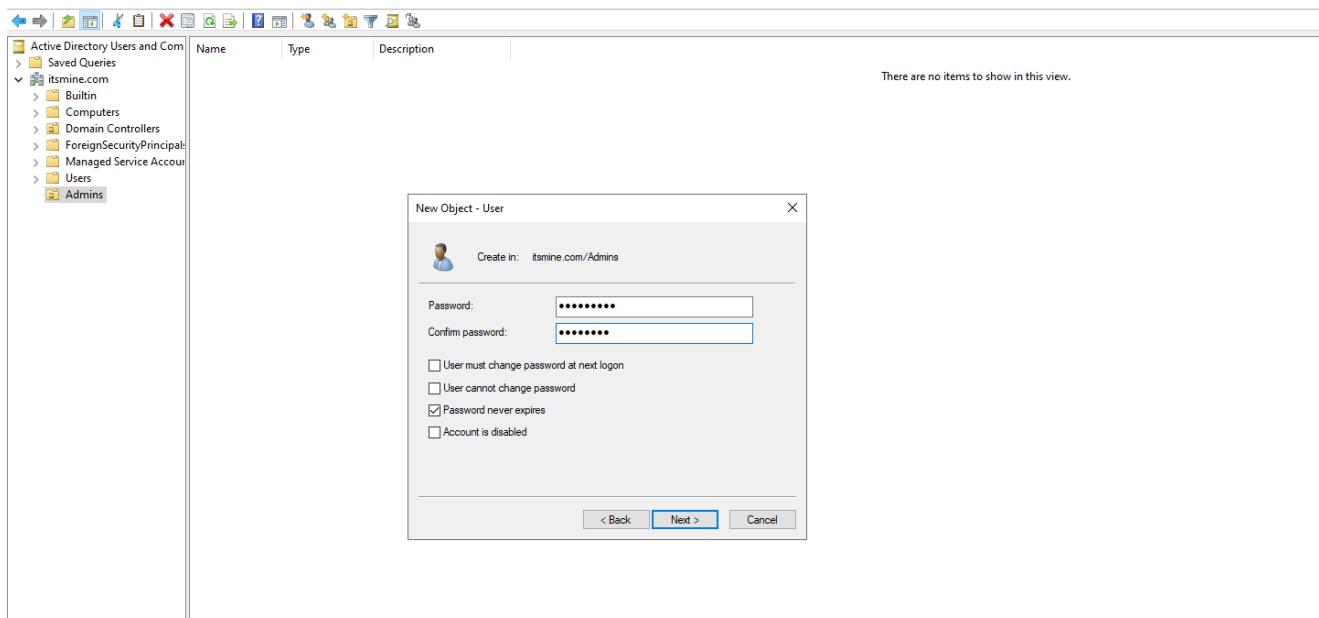
After restarting, Active Directory administrative tools were verified from the Start menu. This confirms successful installation of AD services.



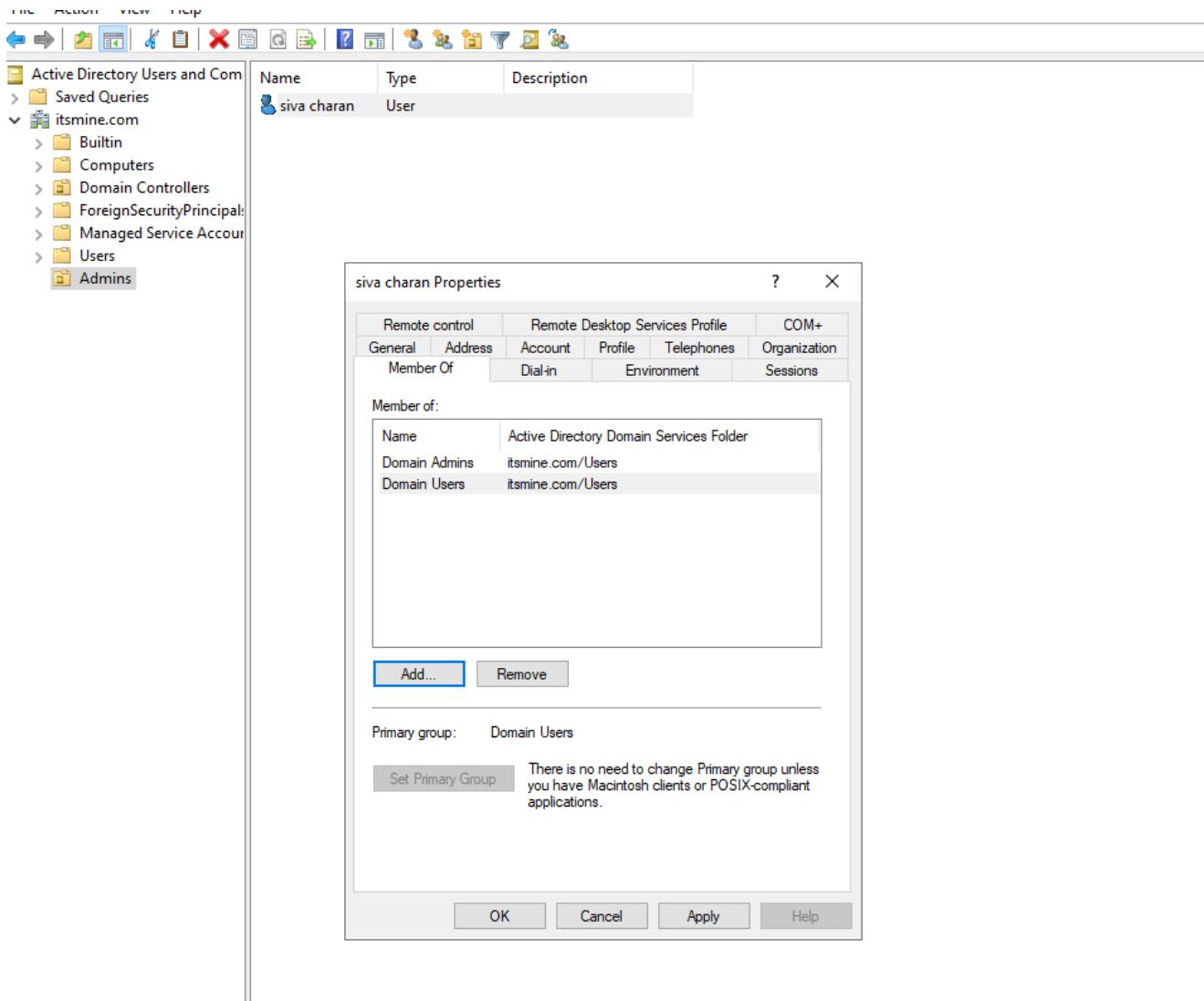
Active Directory Users and Computers console was opened to begin user account management. A new domain user creation process was initiated.



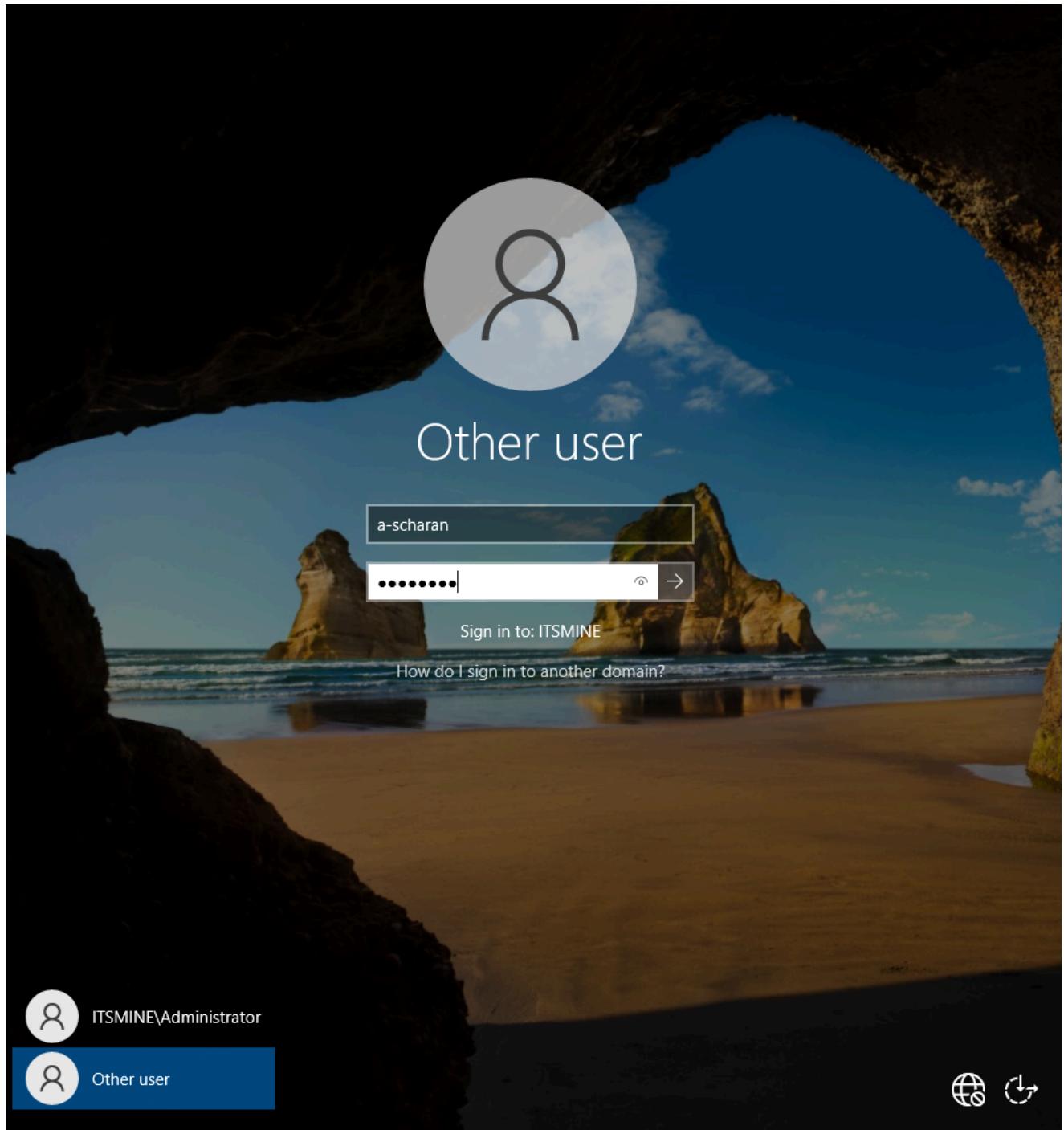
User account details such as first name, last name, and logon name were entered. This step creates a new domain user object in Active Directory.



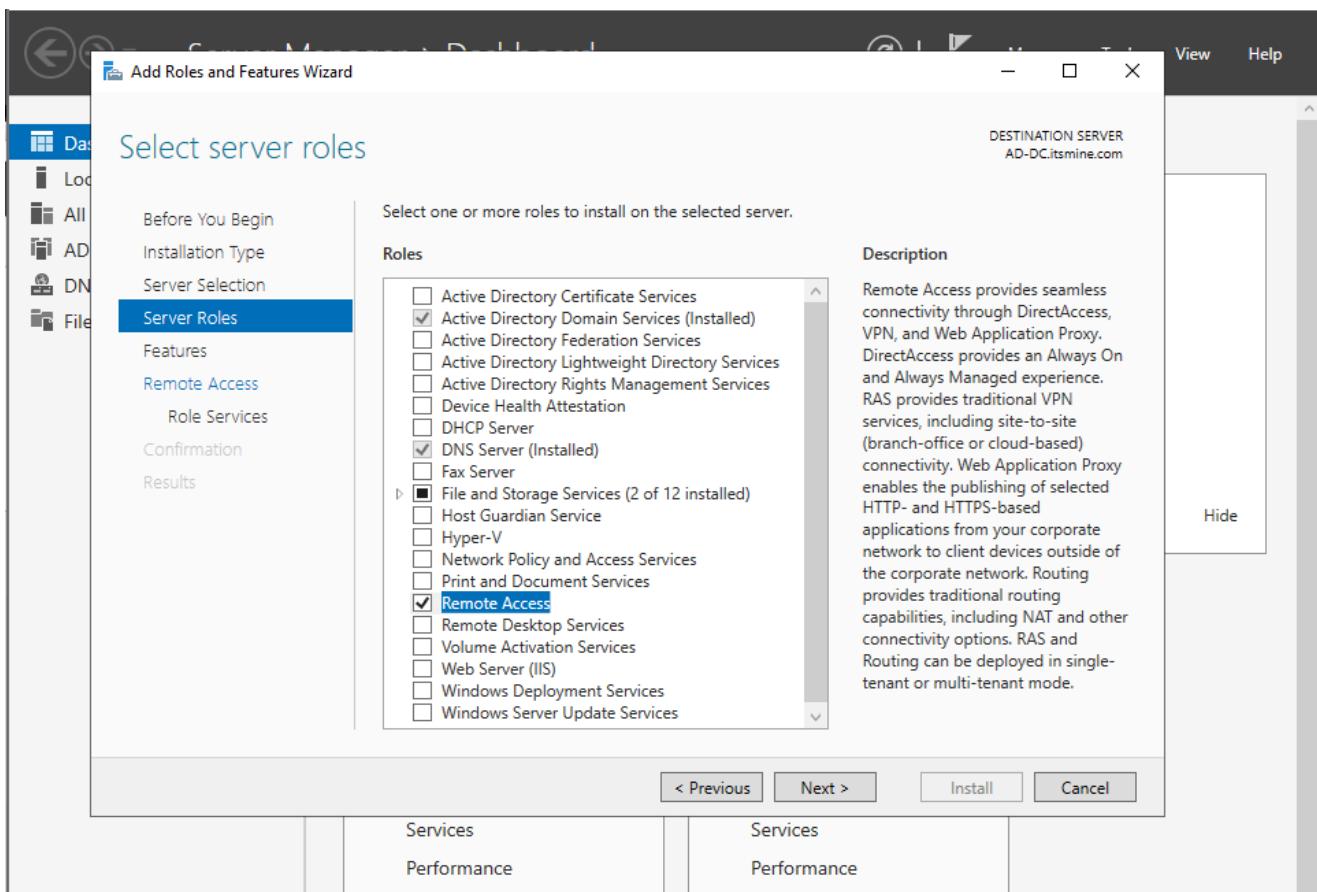
A secure password was assigned to the user account and the account was enabled. Group membership was reviewed under the Member Of tab



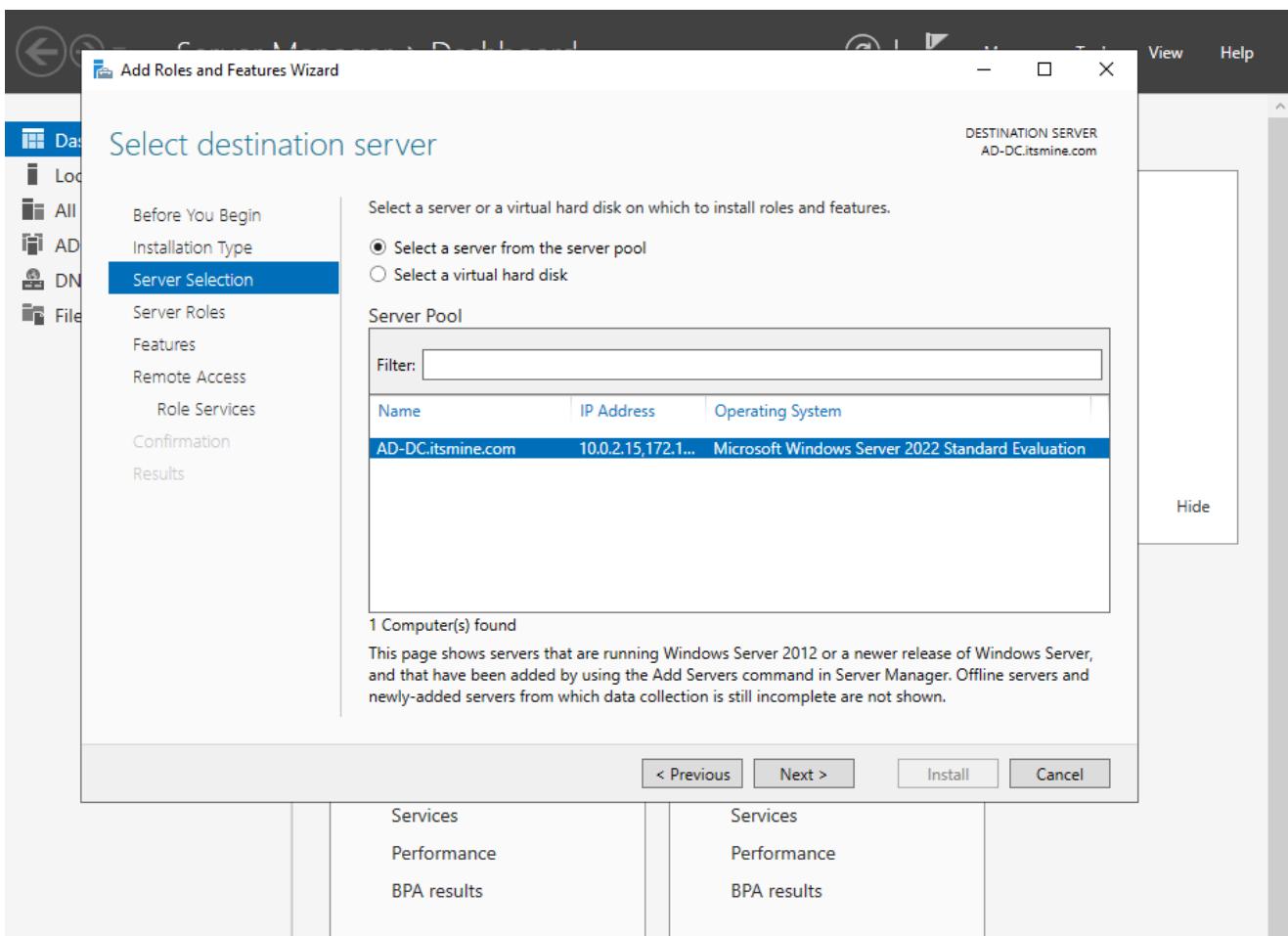
Windows login screen displaying domain user authentication. Successful login confirms proper domain connectivity and authentication services.



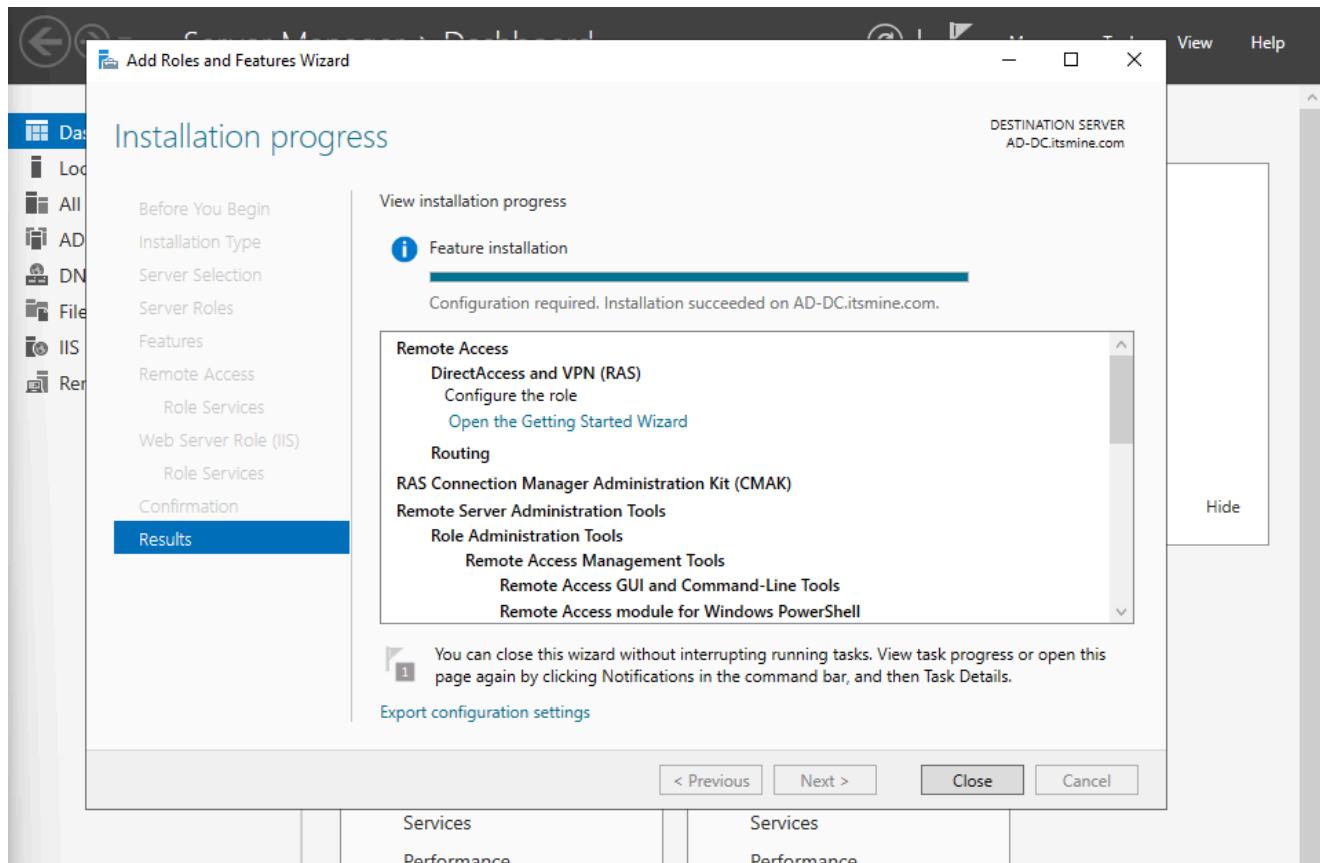
Add Roles and Features Wizard was used again to install the Remote Access role. This role is required for routing and NAT configuration.



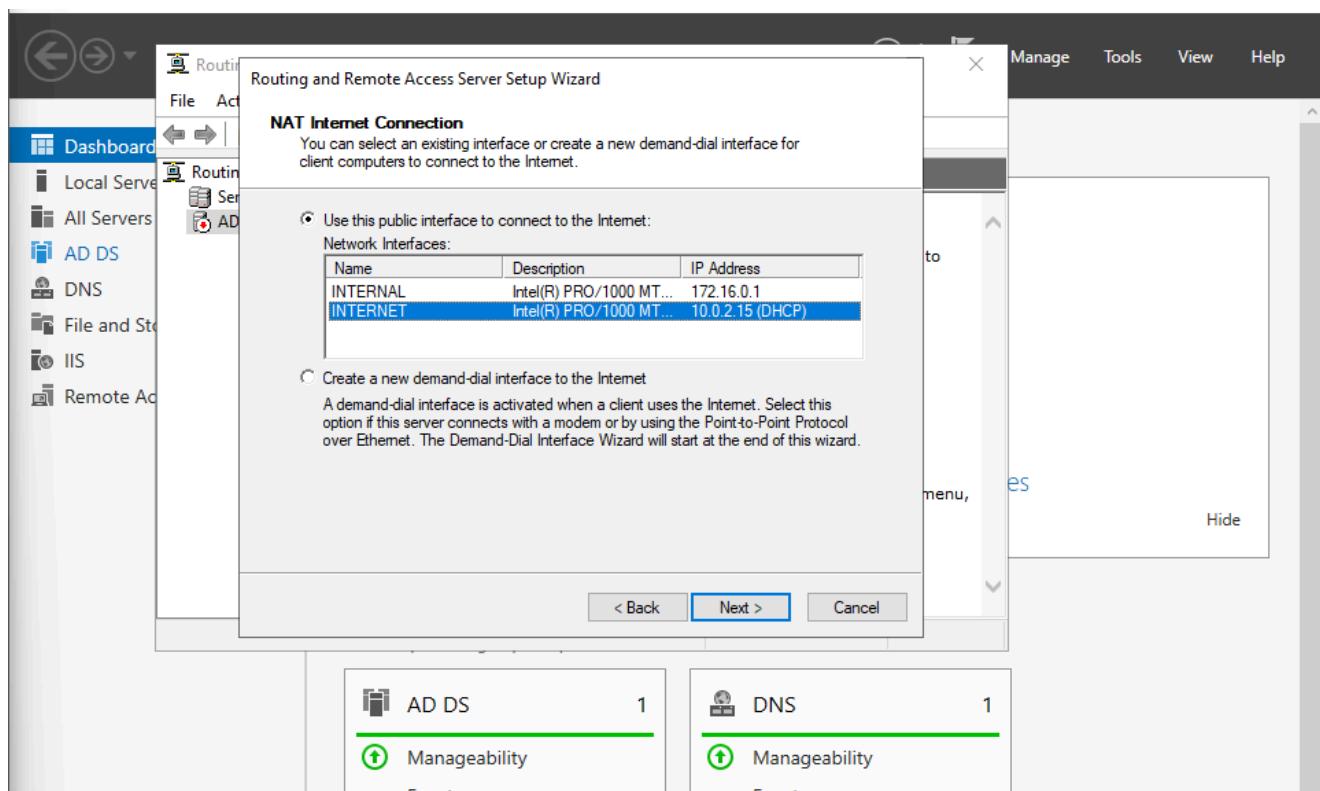
The destination server was confirmed before proceeding with installation. Remote Access role installation was initiated.



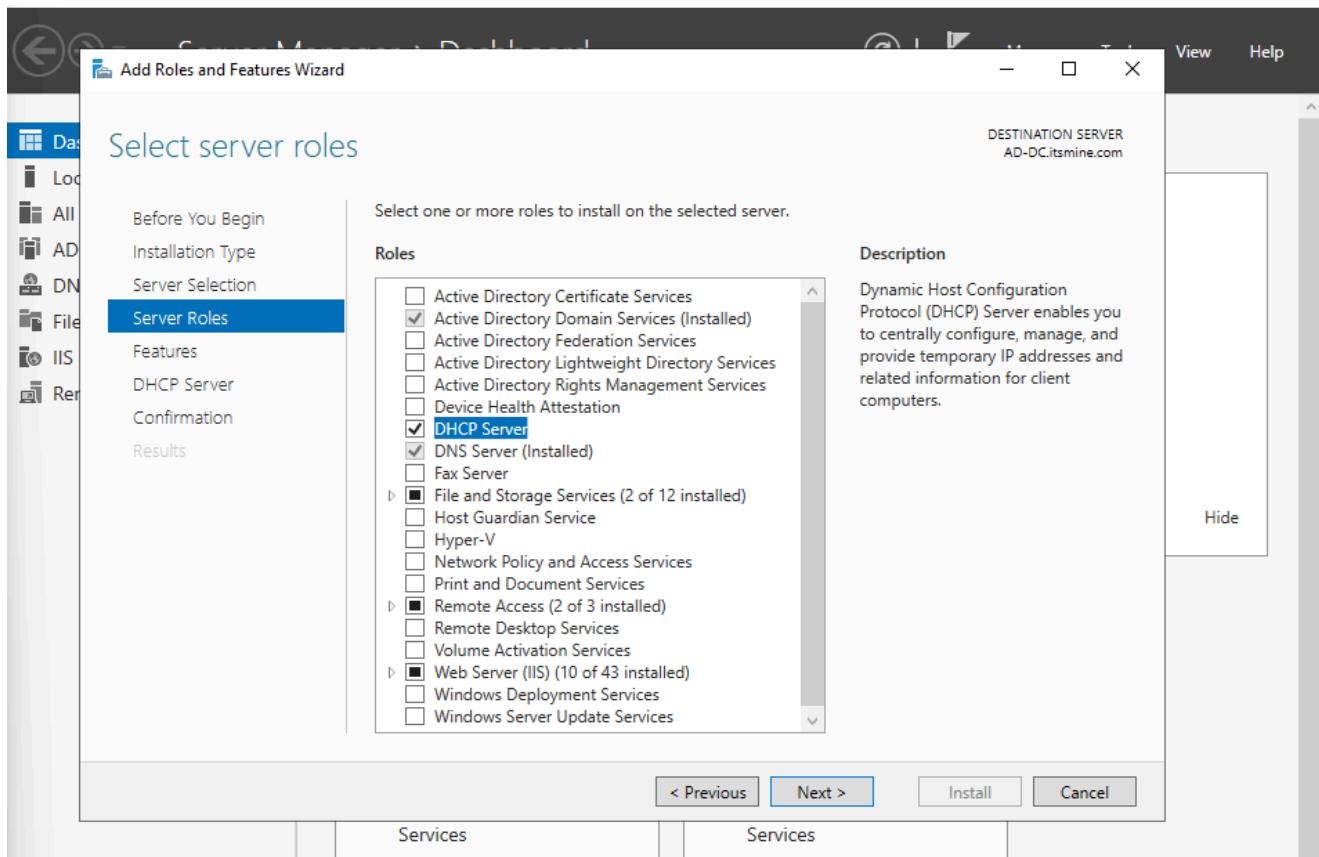
Remote Access role installation was completed successfully. The server is now capable of handling routing services.



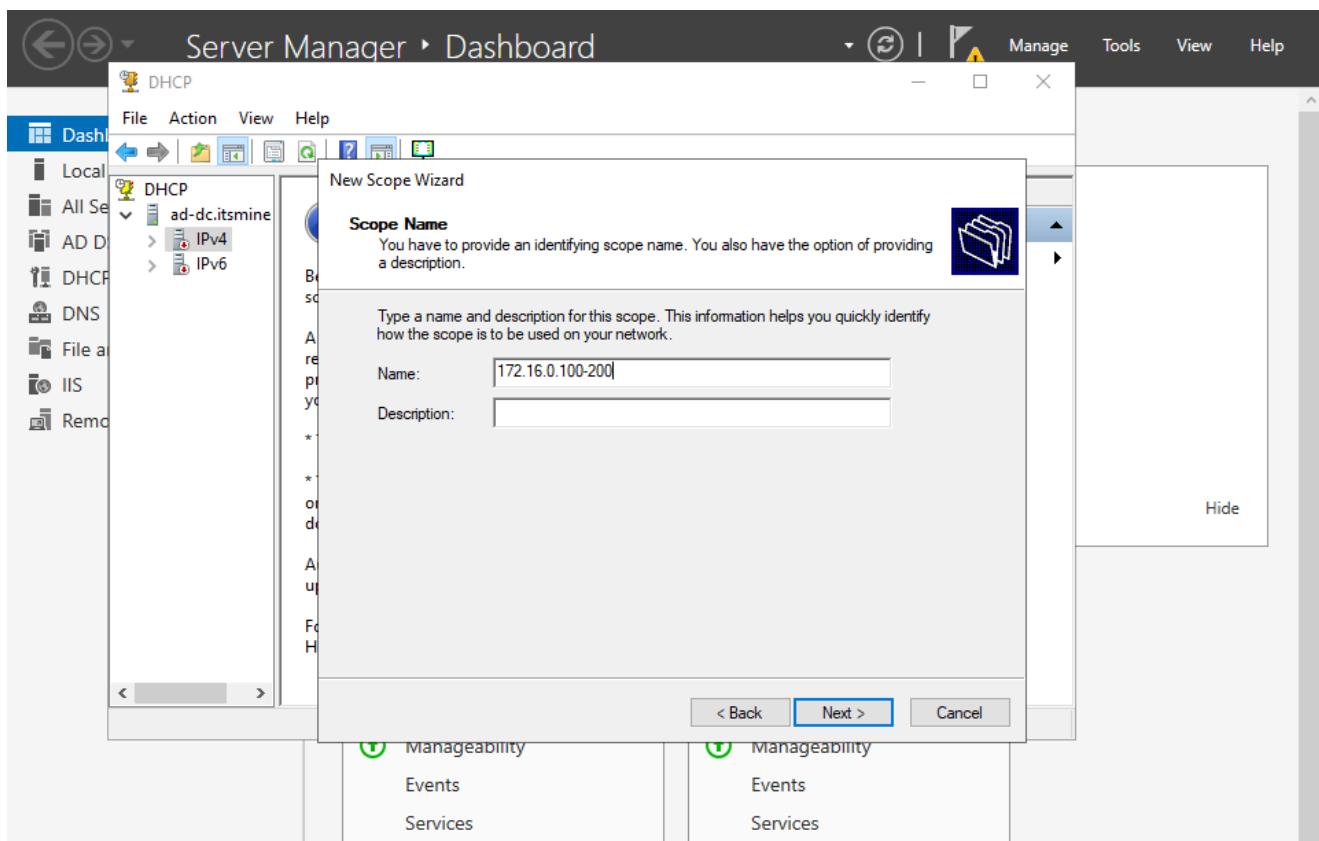
Routing and Remote Access setup wizard was used to configure NAT. The INTERNAL interface was selected as the private network interface.



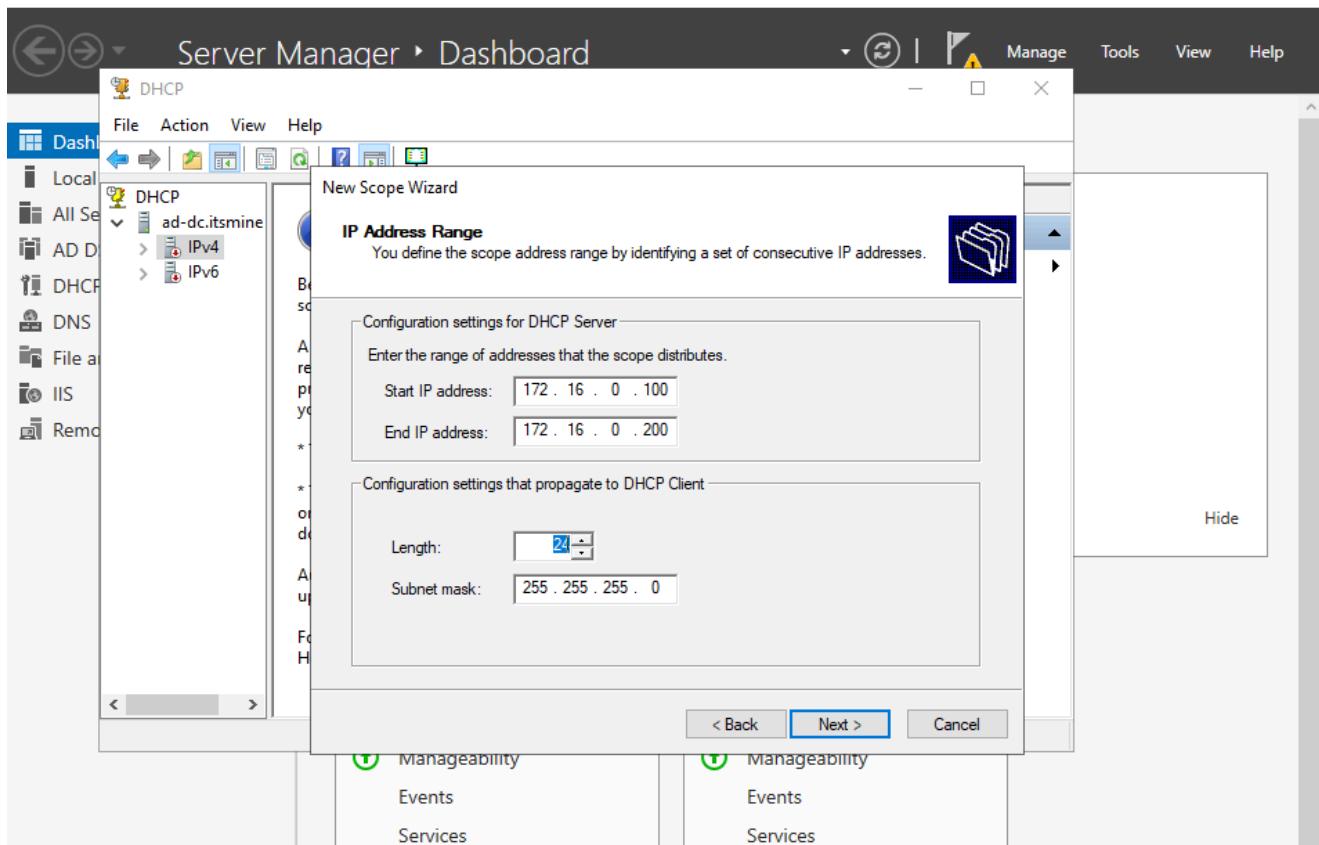
DHCP Server role was selected and installed from Server Manager. This allows automatic IP address assignment for client machines.



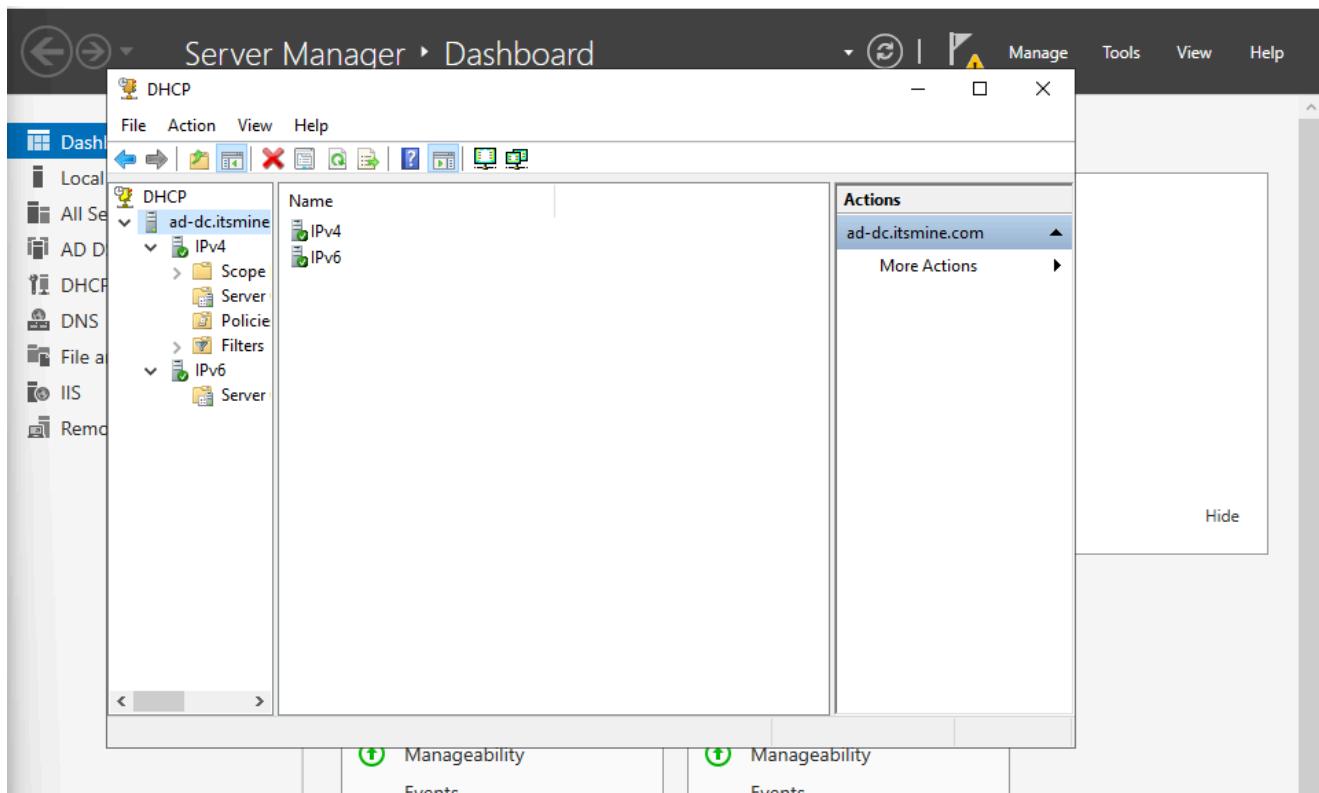
New Scope Wizard was opened in the DHCP console. A scope was created for the IP range 172.16.0.100–200.



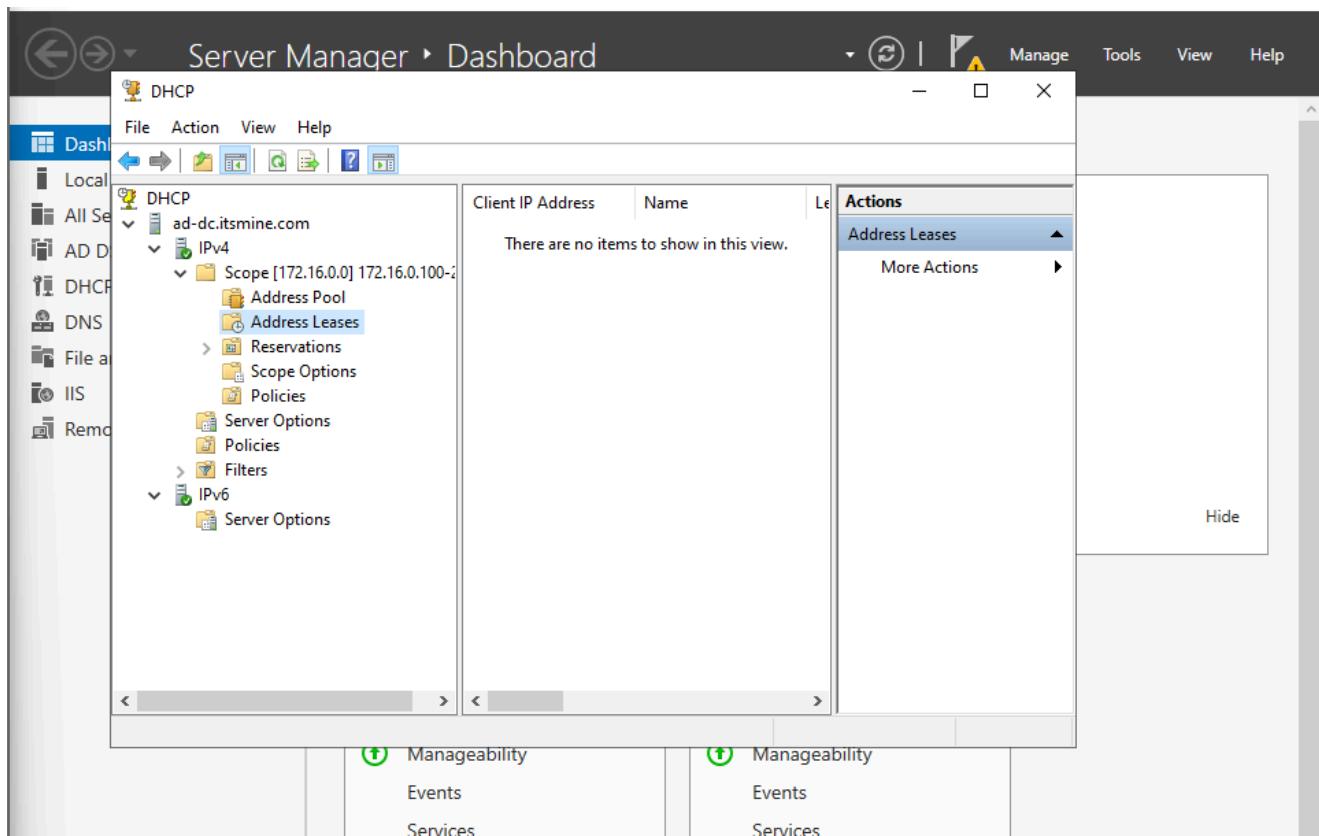
DHCP scope was configured with start IP 172.16.0.100 and end IP 172.16.0.200. Subnet mask 255.255.255.0 was defined for the network



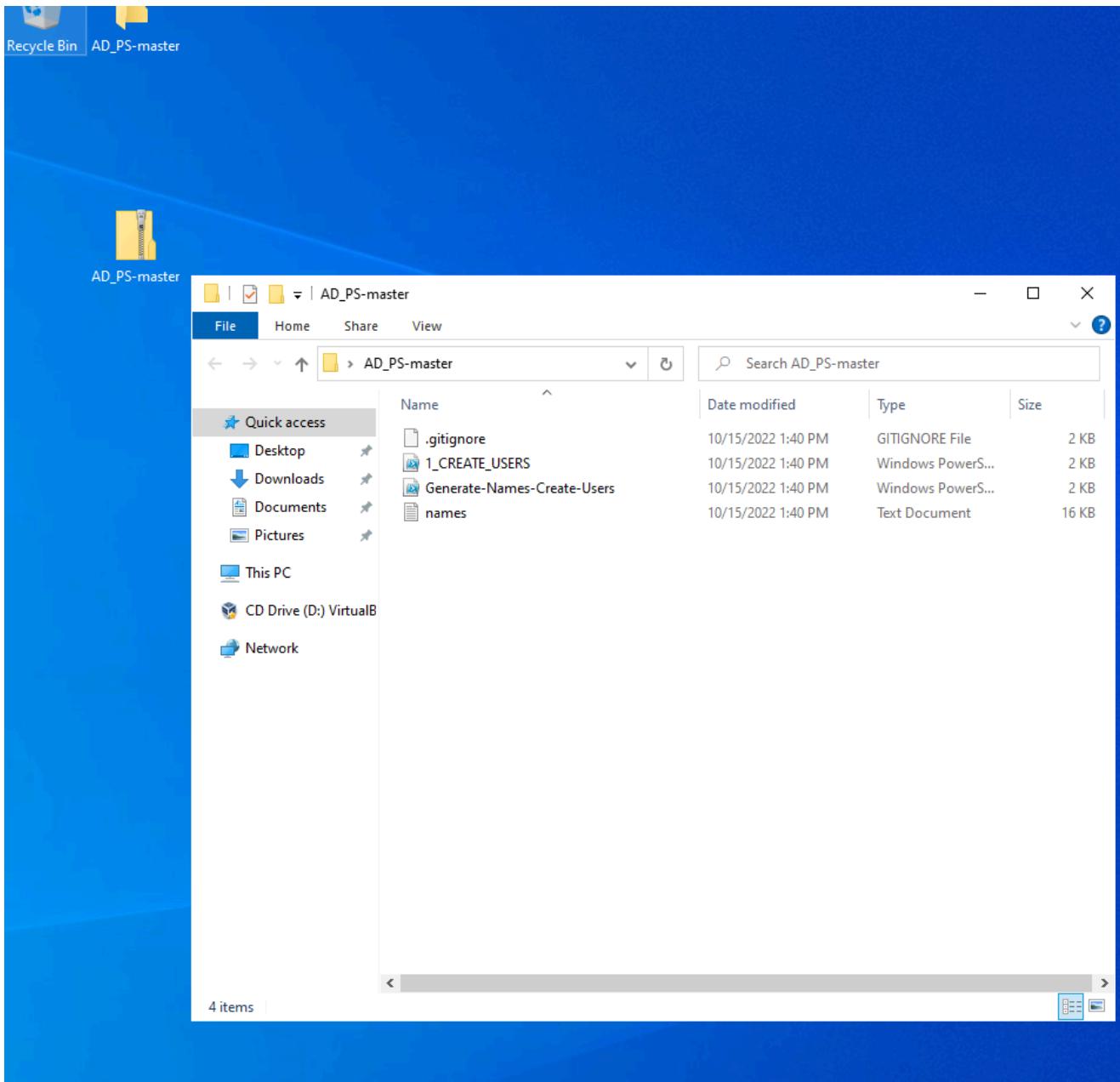
The DHCP scope was successfully created under IPv4. The server is ready to distribute IP addresses to domain clients.



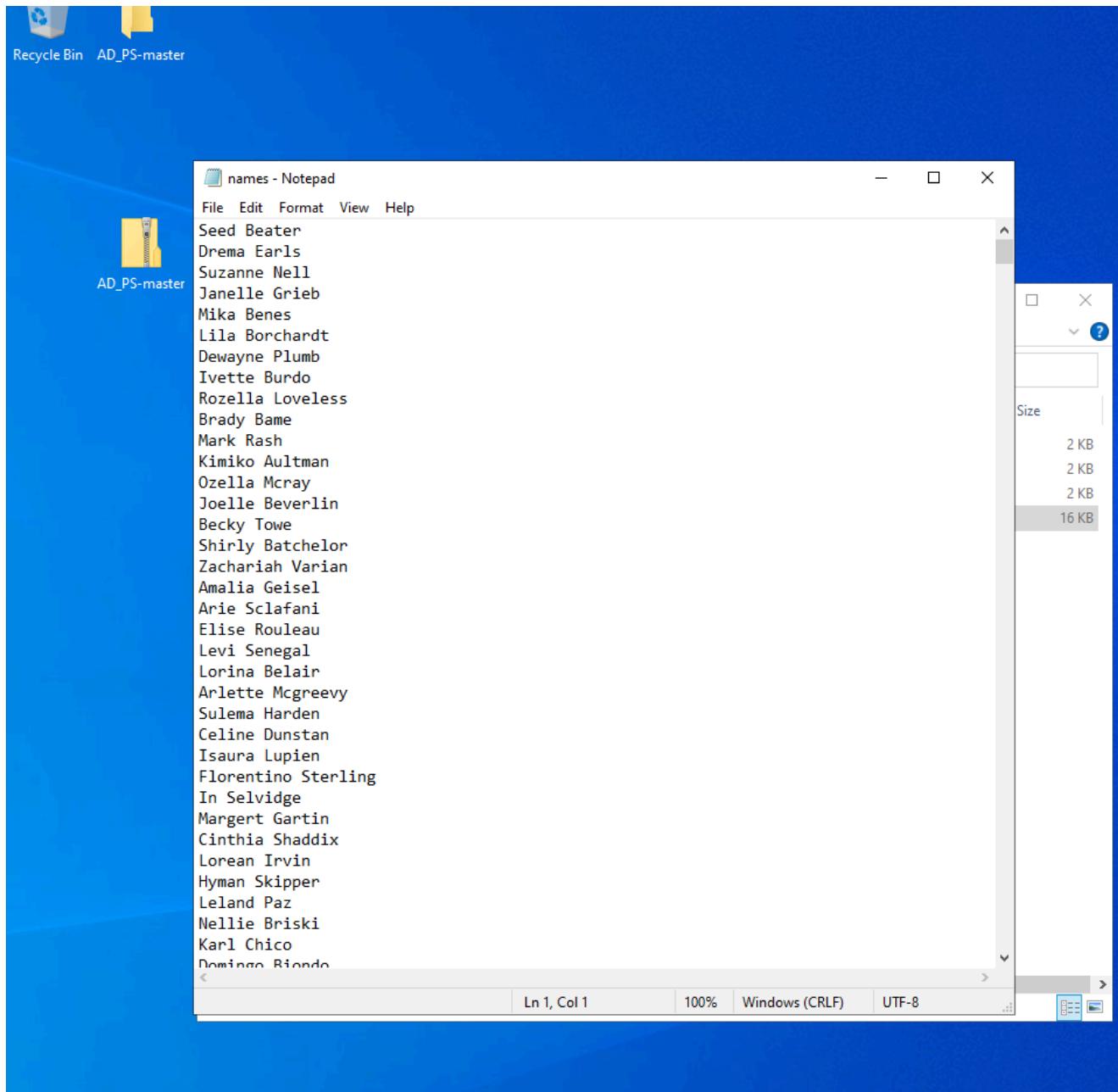
Address Leases section in DHCP console was opened. This area displays IP addresses assigned to client systems



A folder named `AD_PS-master` was created to store automation scripts. It contains the PowerShell script and user list file for bulk user creation.



The names.txt file was created containing multiple user names. This file will be used as input for automated user creation.



PowerShell ISE was used to write a script utilizing the New-ADUser command. The script reads usernames from the text file and assigns a default password.

The screenshot shows the Windows PowerShell ISE interface. The title bar reads "Administrator: Windows PowerShell ISE". The menu bar includes File, Edit, View, Tools, Debug, Add-ons, and Help. Below the menu is a toolbar with various icons. A code editor window titled "1_CREATE_USERS.ps1" is open, displaying a PowerShell script. The script starts by defining variables: \$PASSWORD_FOR_USERS ("Password1") and \$USER_FIRST_LAST_LIST (contents of "names.txt"). It then creates a new organizational unit named "_USERS" with the "ProtectedFromAccidentalDeletion" flag set to \$false. A foreach loop iterates over each line in \$USER_FIRST_LAST_LIST, splitting it into \$first and \$last, and creating a new user (\$username) with the first name as given name and the last name as surname. The user is assigned a password from \$PASSWORD_FOR_USERS, has "EmployeeID" set to \$username, and "Path" set to "ou=_USERS,\$([ADSI]::Get("").distinguishedName)". The "Enabled" parameter is set to \$true. The PowerShell window below shows the command PS C:\Windows\system32>.

```
1 # ----- Edit these Variables for your own Use Case ----- #
2 $PASSWORD_FOR_USERS = "Password1"
3 $USER_FIRST_LAST_LIST = Get-Content .\names.txt
4 # -----
5
6 $password = ConvertTo-SecureString $PASSWORD_FOR_USERS -AsPlainText -Force
7 New-ADOrganizationalUnit -Name _USERS -ProtectedFromAccidentalDeletion $false
8
9 foreach ($n in $USER_FIRST_LAST_LIST) {
10     $first = $n.Split(" ")[0].ToLower()
11     $last = $n.Split(" ")[1].ToLower()
12     $username = $($first.Substring(0,1))$($last).ToLower()
13     Write-Host "Creating user: $($username)" -BackgroundColor Black -ForegroundColor Cyan
14
15     New-AdUser -AccountPassword $password ` 
16                 -GivenName $first ` 
17                 -Surname $last ` 
18                 -DisplayName $username ` 
19                 -Name $username ` 
20                 -EmployeeID $username ` 
21                 -PasswordNeverExpires $true ` 
22                 -Path "ou=_USERS,$([ADSI]::Get("").distinguishedName)" ` 
23                 -Enabled $true
24 }
```

Execution policy was set to Unrestricted to allow script execution. The script directory was verified before running the automation.

The screenshot shows the Windows PowerShell ISE interface. The top window displays the script file `1_CREATE_USERS.ps1` with the following content:

```
1 # ----- Edit these Variables for your own Use Case ----- #
2 $PASSWORD_FOR_USERS = "Password1"
3 $USER_FIRST_LAST_LIST = Get-Content .\names.txt
4 # -----
5
6 $password = ConvertTo-SecureString $PASSWORD_FOR_USERS -AsPlainText -Force
7 New-ADOrganizationalUnit -Name _USERS -ProtectedFromAccidentalDeletion $false
8
9 foreach ($n in $USER_FIRST_LAST_LIST) {
10     $first = $n.Split(" ")[0].ToLower()
11     $last = $n.Split(" ")[1].ToLower()
12     $username = "$($first.Substring(0,1))$($last)".ToLower()
13     Write-Host "Creating user: $($username)" -BackgroundColor Black -ForegroundColor Cyan
14
15     New-AdUser -AccountPassword $password ` 
16             -GivenName $first ` 
17             -Surname $last ` 
18             -DisplayName $username ` 
19             -Name $username ` 
20             -EmployeeID $username ` 
21             -PasswordNeverExpires $true ` 
22             -Path "ou=_USERS,$([ADSI]::Get(")).distinguishedName" ` 
23             -Enabled $true
24 }
```

The bottom window shows the PowerShell command history and output:

```
PS C:\Windows\system32> Set-ExecutionPolicy Unrestricted
PS C:\Windows\system32> Set-ExecutionPolicy Unrestricted
PS C:\Windows\system32> cd C:\users\a-scharan\Desktop\AD_PS-master
PS C:\users\a-scharan\Desktop\AD_PS-master> ls

    Directory: C:\users\a-scharan\Desktop\AD_PS-master

Mode                LastWriteTime         Length Name
----                -----
--              10/15/2022  1:40 PM        1811 .gitignore
--              10/15/2022  1:40 PM        1025 1_CREATE_USERS.ps1
--              10/15/2022  1:40 PM        1532 Generate-Names-Create-Users.ps1
-a---            2/8/2026   9:30 AM       15581 names.txt

PS C:\users\a-scharan\Desktop\AD_PS-master> |
```

The status bar at the bottom indicates "Completed" and shows "Ln 22 Col 45" and "100%".

The PowerShell script was executed to automatically create multiple domain user accounts. The console output confirms successful user creation.

The screenshot shows a Windows PowerShell ISE window with the title "Administrator: Windows PowerShell ISE". The script file is named "1_CREATE_USERS.ps1". The code creates users in Active Directory based on a list of names. The output window shows the progress of user creation, listing over 30 users being created.

```
1 # ----- Edit these Variables for your own Use Case ----- #
2 $PASSWORD_FOR_USERS = "Password1"
3 $USER_FIRST_LAST_LIST = Get-Content .\names.txt
4 #
5
6 $password = ConvertTo-SecureString $PASSWORD_FOR_USERS -AsPlainText -Force
7 New-ADOrganizationalUnit -Name _USERS -ProtectedFromAccidentalDeletion $false
8
9 foreach ($n in $USER_FIRST_LAST_LIST) {
10     $first = $n.Split(" ")[0].ToLower()
11     $last = $n.Split(" ")[1].ToLower()
12     $username = "$($first.Substring(0,1))$($last)".ToLower()
13     Write-Host "Creating user: $($username)" -BackgroundColor Black -ForegroundColor Cyan
14
15     New-AdUser -AccountPassword $password `
16                 -GivenName $first `
17                 -Surname $last `
18                 -DisplayName $username `
19                 -Name $username `
20                 -EmployeeID $username `
21                 -PasswordNeverExpires $true `
22                 -Path "ou=_USERS,$([ADSI]'').distinguishedName" `
23                 -Enabled $true
24 }
```

```
Creating user: nbriski
Creating user: kchico
Creating user: dbiondo
Creating user: crinaldi
Creating user: cibarra
Creating user: ttaitt
Creating user: cansari
Creating user: tstaller
Creating user: sbaxley
Creating user: agoltz
Creating user: jdonati
Creating user: tnocera
Creating user: tgoggans
Creating user: vafleur
Creating user: dbanda
Creating user: abirk
Creating user: imccusker
Creating user: rhellums
Creating user: klarose
Creating user: esandor
Creating user: mravenscroft
Creating user: dedgington
Creating user: rcrocker
Creating user: astrout
Creating user: eservais
Creating user: mnicholes
Creating user: iloden
```

Running script / selection. Press Ctrl+Break to stop. Press Ctrl+B to break into debugger. | Ln 84 Col 1 | 100%

Active Directory Users and Computers console displays newly created bulk users. This verifies successful automation.

The screenshot shows the Windows Server Manager interface. On the left, the navigation pane is visible with options like Dashboard, Local Server, All Servers, AD DS, DHCP, DNS, File and Storage, IIS, and Remote. The main area displays the 'Active Directory Users and Computers' snap-in. It shows a tree view under 'itsmine.com' with nodes for _Schemas, _SYSTEM, Admins, Builtin, Computers, Domain Controllers, ForeignSecurityPrincipals, Managed Service Accounts, and Users. Below this is a table of users with columns for Name, Type, and Description. A separate table below shows the 'System Log' with columns for Server Name, ID, Severity, Source, Log, and Date and Time.

	Server Name	ID	Severity	Source	Log	Date and Time
	AD-DC	6008	Error	EventLog	System	2/8/2026 9:58:49 PM
	AD-DC	41	Critical	Microsoft-Windows-Kernel-Power	System	2/8/2026 9:58:42 PM
	AD-DC	10149	Warning	Microsoft-Windows-Windows Remote Management	System	2/8/2026 9:49:48 PM
	AD-DC	134	Warning	Microsoft-Windows-Time-Service	System	2/8/2026 9:49:05 PM
	AD-DC	134	Warning	Microsoft-Windows-Time-Service	System	2/8/2026 9:49:04 PM
	AD-DC	7023	Error	Microsoft-Windows-Service Control Manager	System	2/8/2026 9:49:03 PM

ipconfig command was executed on the client machine. The client received an IP address within the configured DHCP range.

The screenshot shows a Command Prompt window titled 'Command Prompt'. The user has run the 'ipconfig' command, which displays network configuration details. The output includes sections for 'Ethernet adapter Ethernet' and 'Tunnel adapter isatap.itsmine.com'. In the 'Ethernet adapter Ethernet' section, it shows the connection-specific DNS suffix as 'itsmine.com', the link-local IPv6 address as 'fe80::7d77:8d2f:7dec:77aa%4', the IPv4 address as '172.16.0.100', the subnet mask as '255.255.255.0', and the default gateway as '172.16.0.1'. The 'Tunnel adapter isatap.itsmine.com' section shows the media state as 'Media disconnected' and the connection-specific DNS suffix as 'itsmine.com'. The prompt at the bottom indicates the user is still in the command line.

```
'ipconfig' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\user 1>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix  . : itsmine.com
  Link-local IPv6 Address . . . . . : fe80::7d77:8d2f:7dec:77aa%4
  IPv4 Address . . . . . : 172.16.0.100
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 172.16.0.1

Tunnel adapter isatap.itsmine.com:

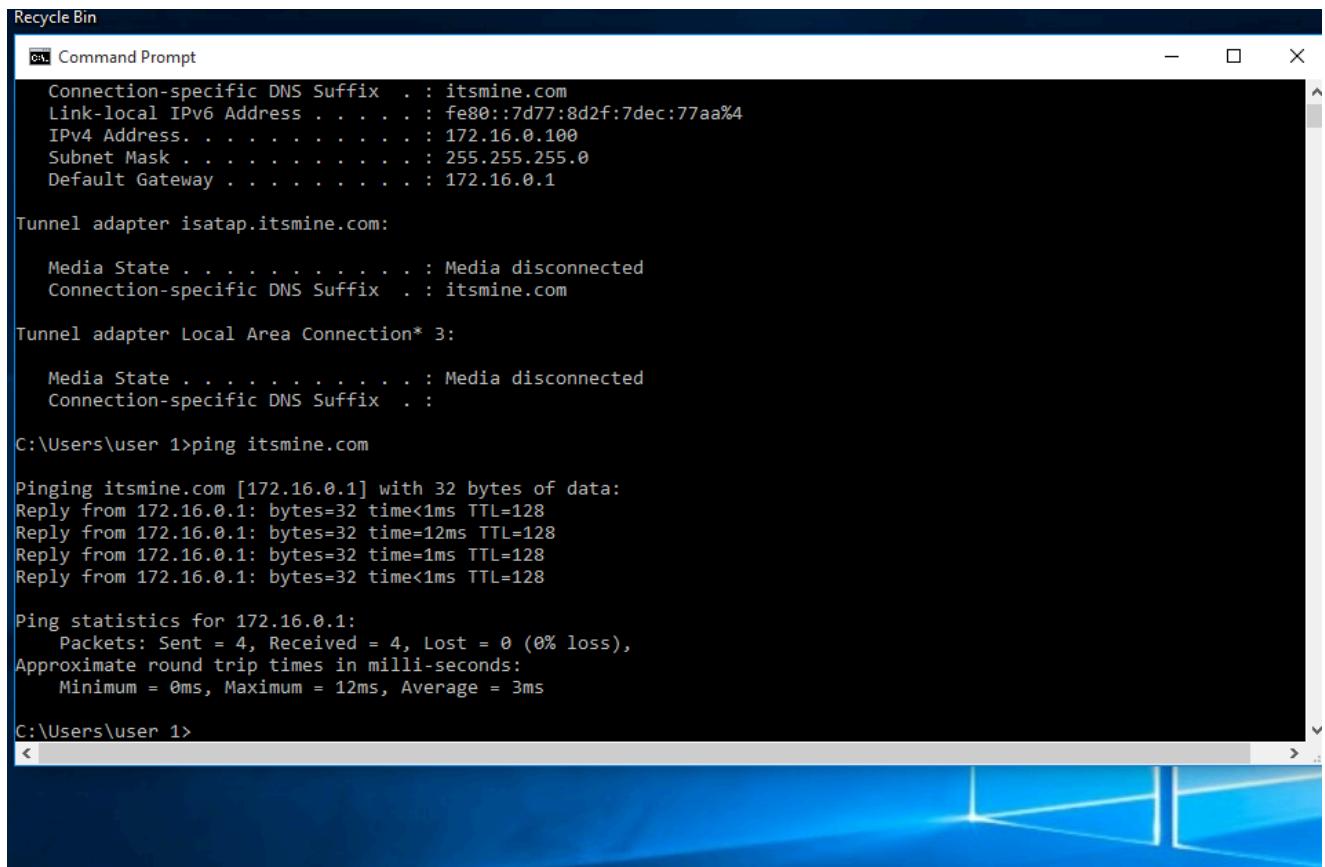
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix  . : itsmine.com

Tunnel adapter Local Area Connection* 3:

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

C:\Users\user 1>
```

Ping test to itsmine.com was performed from the client machine. Successful replies confirm DNS resolution and network connectivity.



```
Recycle Bin
Command Prompt
Connection-specific DNS Suffix . : itsmine.com
Link-local IPv6 Address . . . . . : fe80::7d77:8d2f:7dec:77aa%4
IPv4 Address . . . . . : 172.16.0.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.16.0.1

Tunnel adapter isatap.itsmine.com:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : itsmine.com

Tunnel adapter Local Area Connection* 3:

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

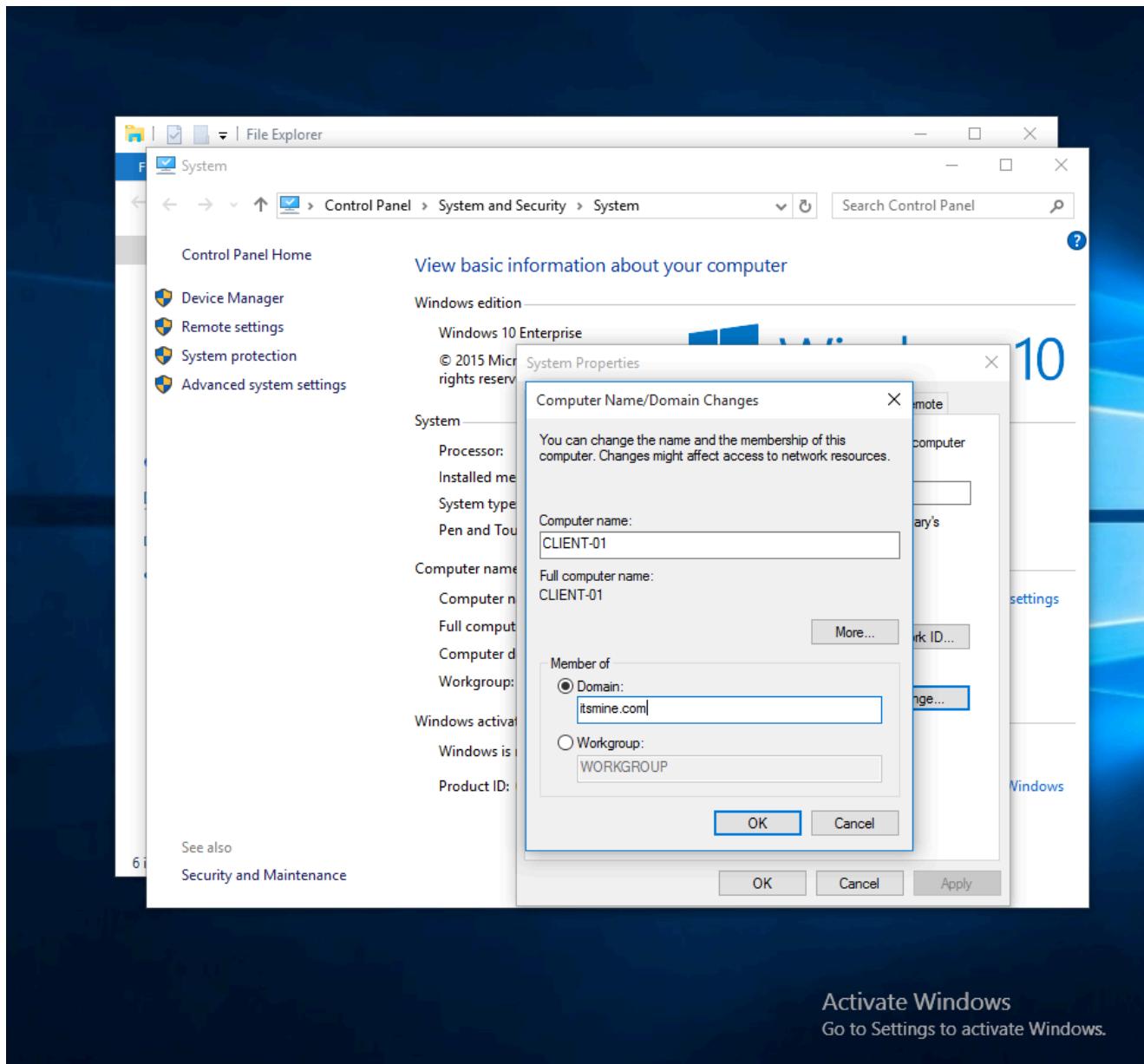
C:\Users\user 1>ping itsmine.com

Pinging itsmine.com [172.16.0.1] with 32 bytes of data:
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128
Reply from 172.16.0.1: bytes=32 time=12ms TTL=128
Reply from 172.16.0.1: bytes=32 time=1ms TTL=128
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128

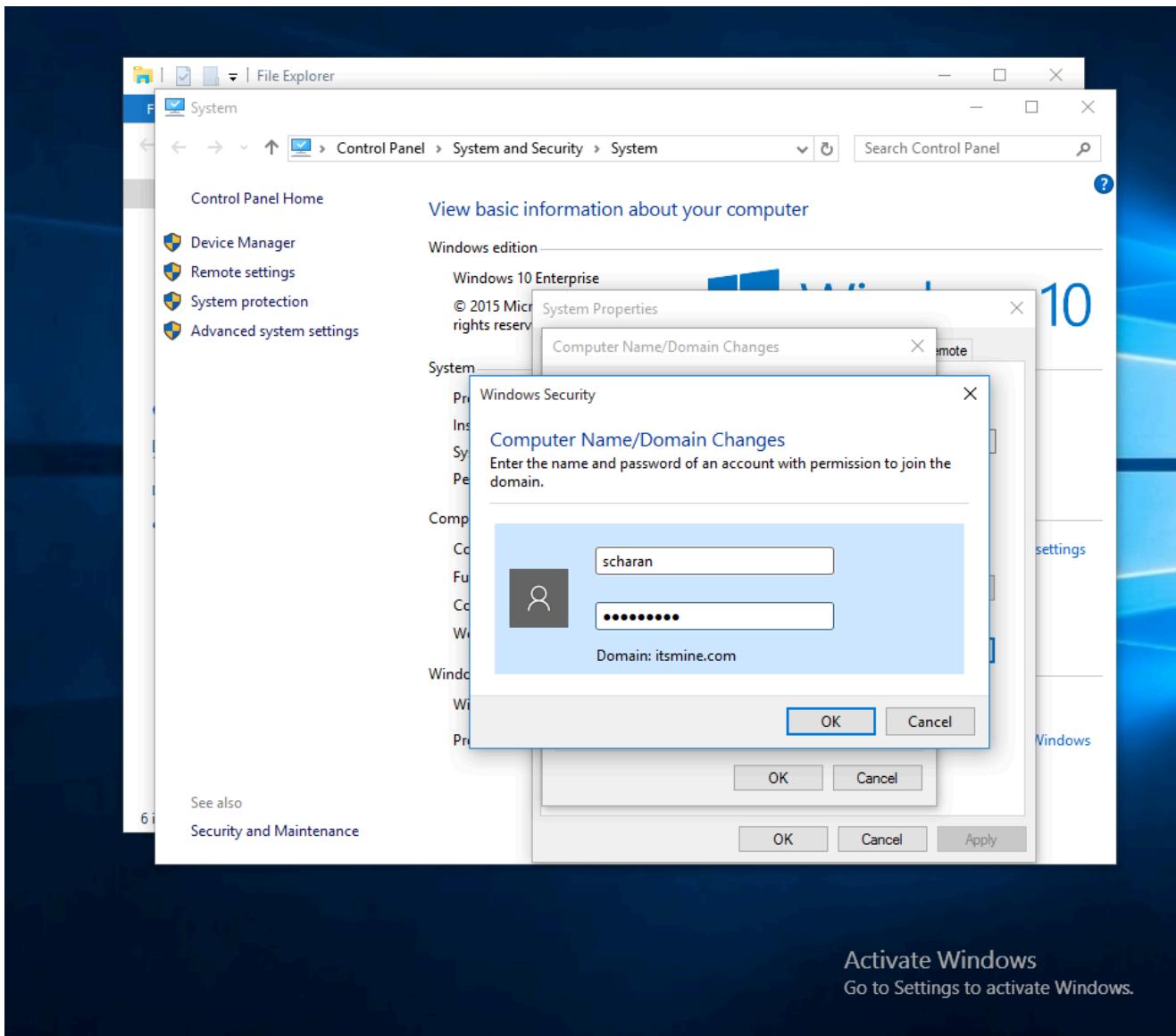
Ping statistics for 172.16.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 3ms

C:\Users\user 1>
```

System Properties were opened to join the Windows 10 machine to the itsmine.com domain. Domain membership option was selected.



Domain administrator credentials were entered to authenticate domain join. The client machine was successfully added to the domain.

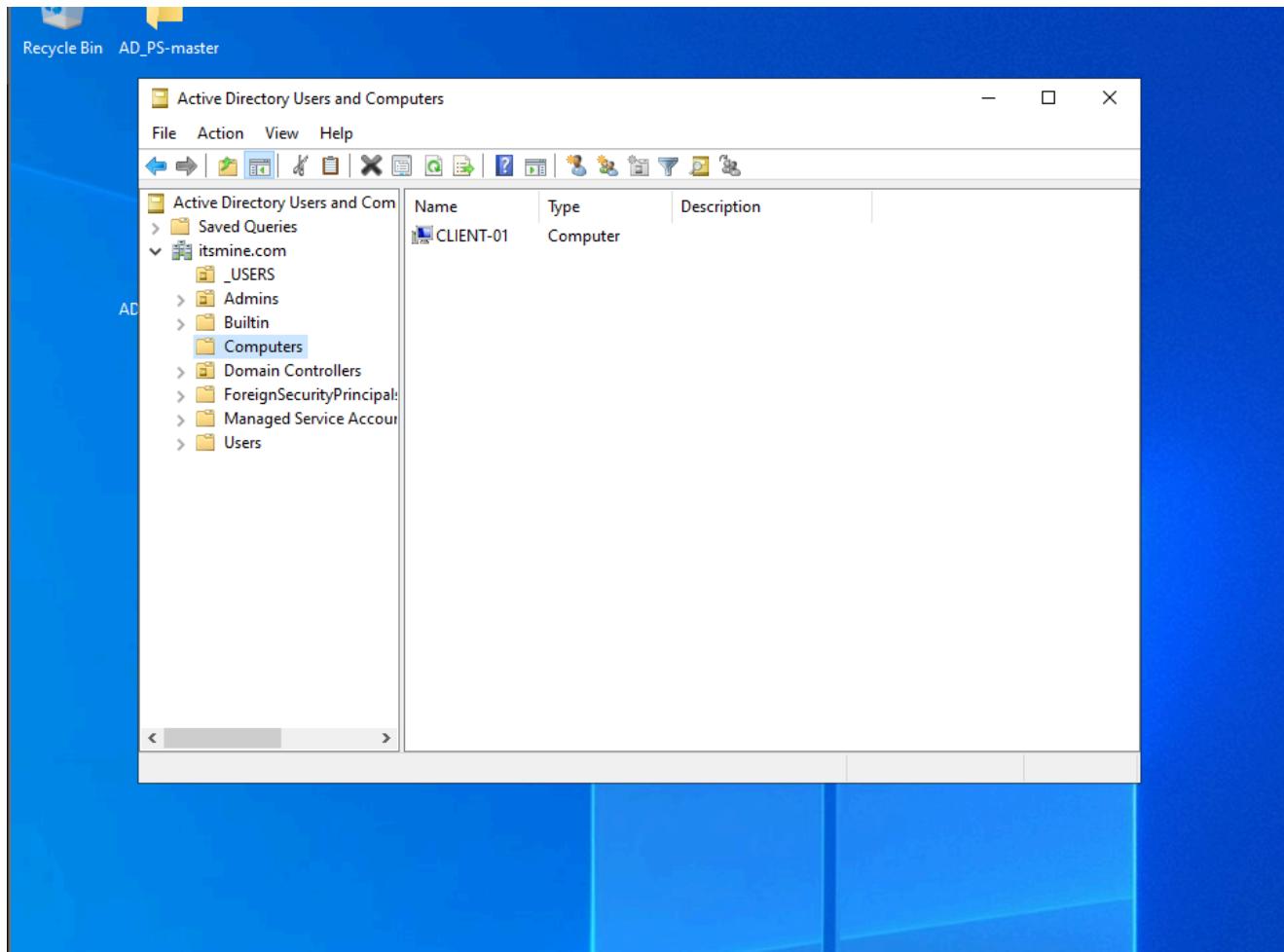


DHCP console shows an active lease assigned to the client machine. This confirms proper IP allocation from the DHCP server.

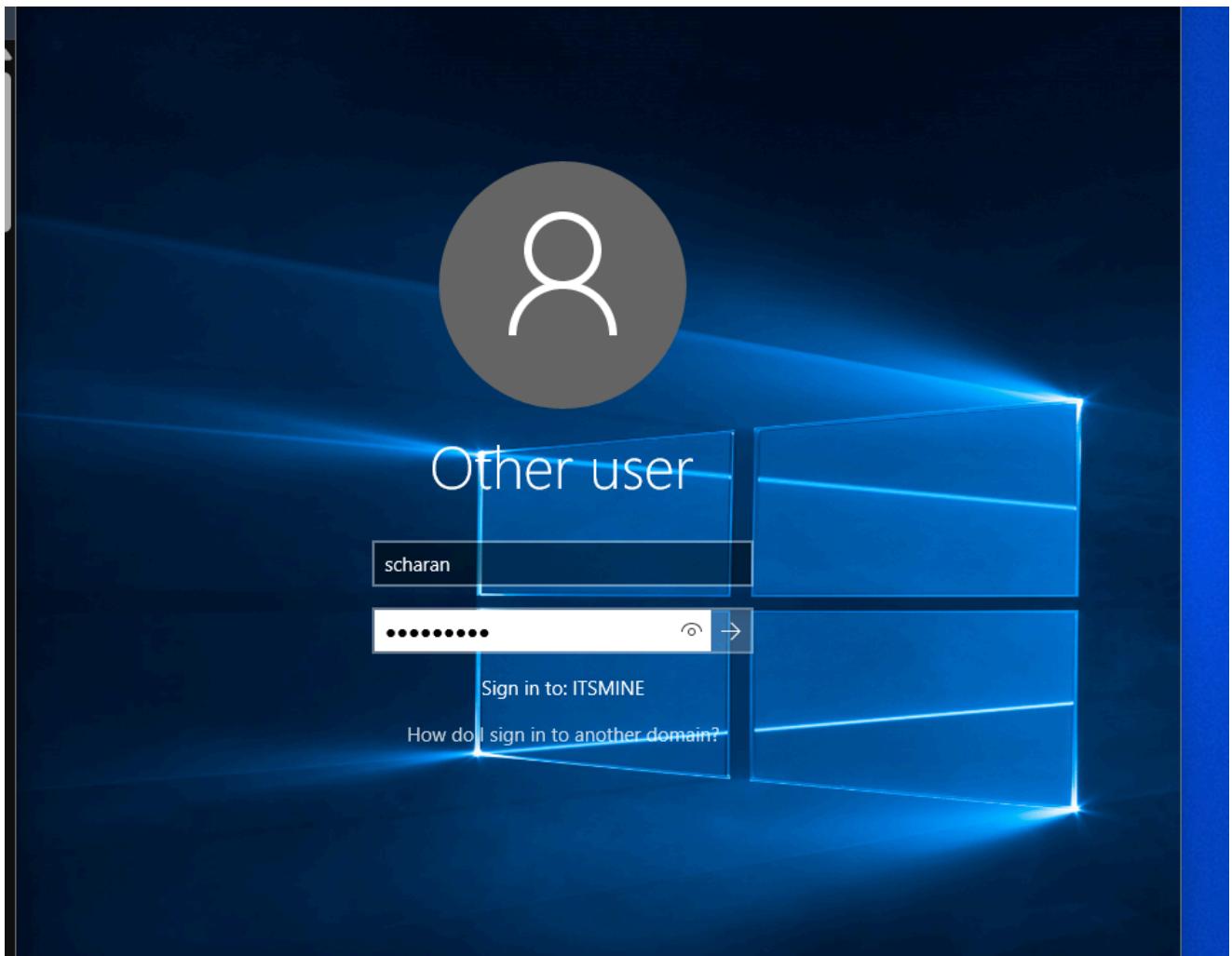
A screenshot of the Microsoft DHCP Management Console. The left pane shows a tree view of DHCP configurations under 'ad-dc.itsmine.com'. The right pane displays a table of active leases. One lease is highlighted for the client 'CLIENT-01.itsmine.com' with the IP address '172.16.0.100'. The 'Actions' column on the far right includes options like 'Address Leases' and 'More Action...'.

Client IP Address	Name	Lease Expiration	Type
172.16.0.100	CLIENT-01.itsmine...	2/16/2026 10:15:22 AM	DHCP

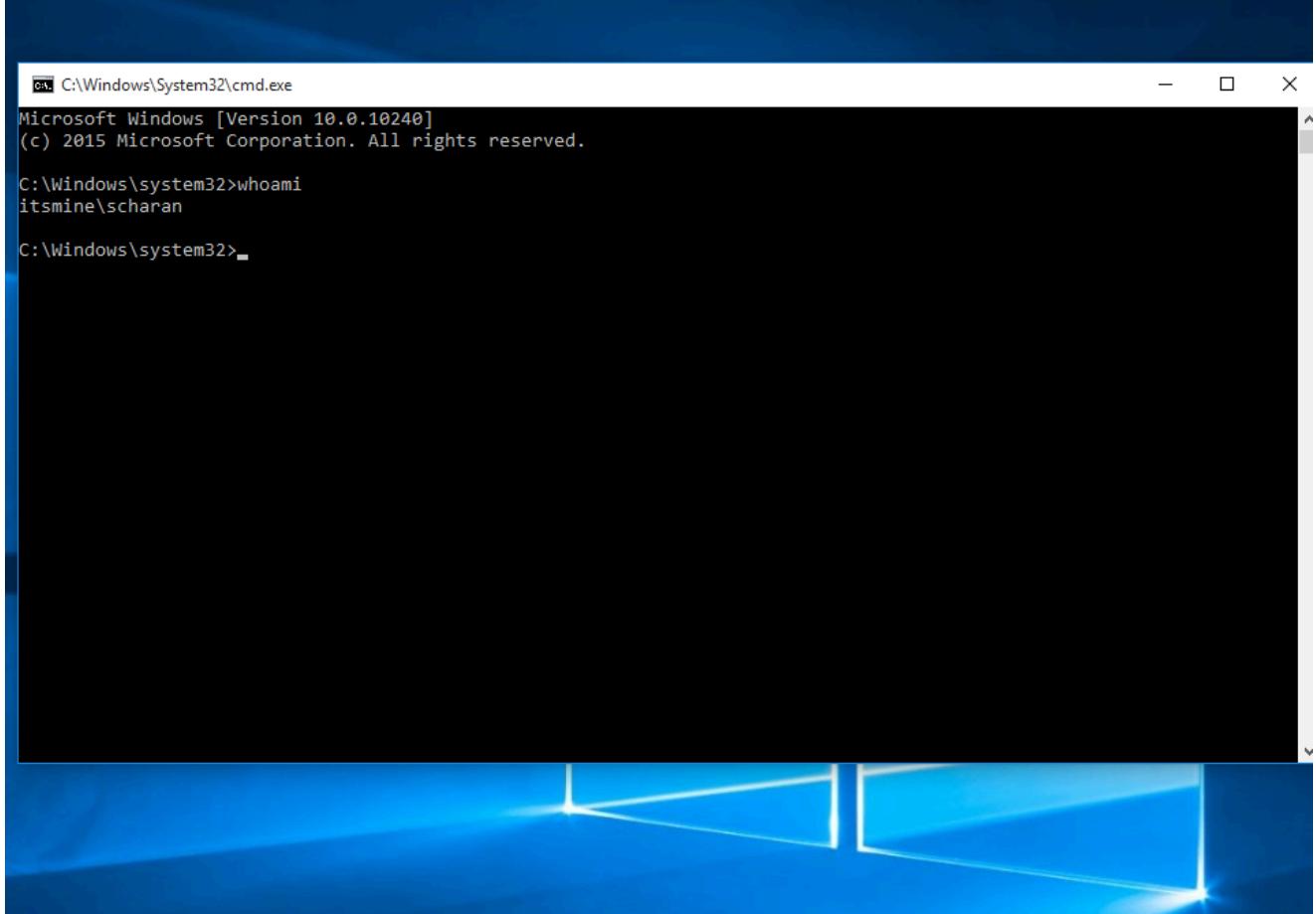
After joining the client system to the domain, the computer account (CLIENT-01) was automatically created inside Active Directory. This confirms successful domain integration of the Windows 10 machine.



Domain user login was tested on the client machine to verify authentication through Active Directory. This confirms that the client system is properly communicating with the Domain Controller.



Command Prompt access after login confirms that the user session is active and functioning under domain credentials.



A screenshot of a Windows 10 desktop. In the top-left corner, there is a small window titled "C:\Windows\System32\cmd.exe" showing a command prompt session. The session starts with "Microsoft Windows [Version 10.0.10240]" and "(c) 2015 Microsoft Corporation. All rights reserved." followed by the command "whoami" which returns "itsmine\scharan". The rest of the screen is a standard Windows 10 desktop environment.

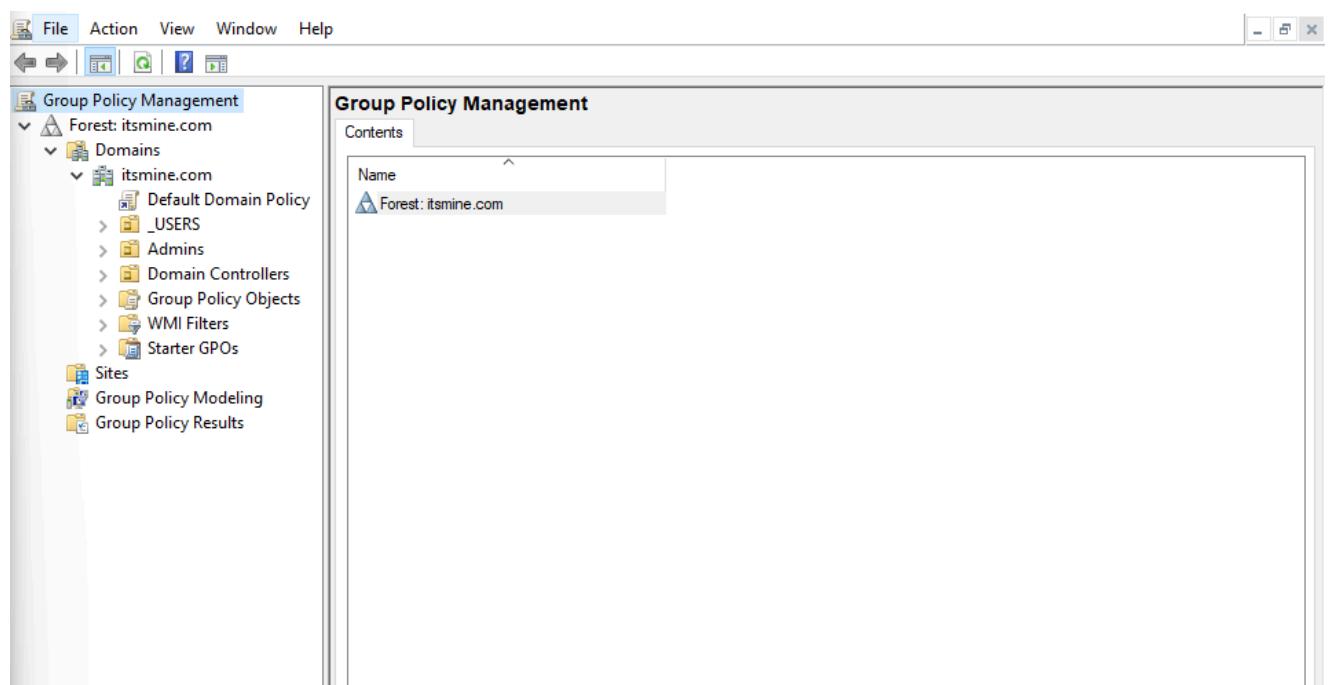
```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
itsmine\scharan

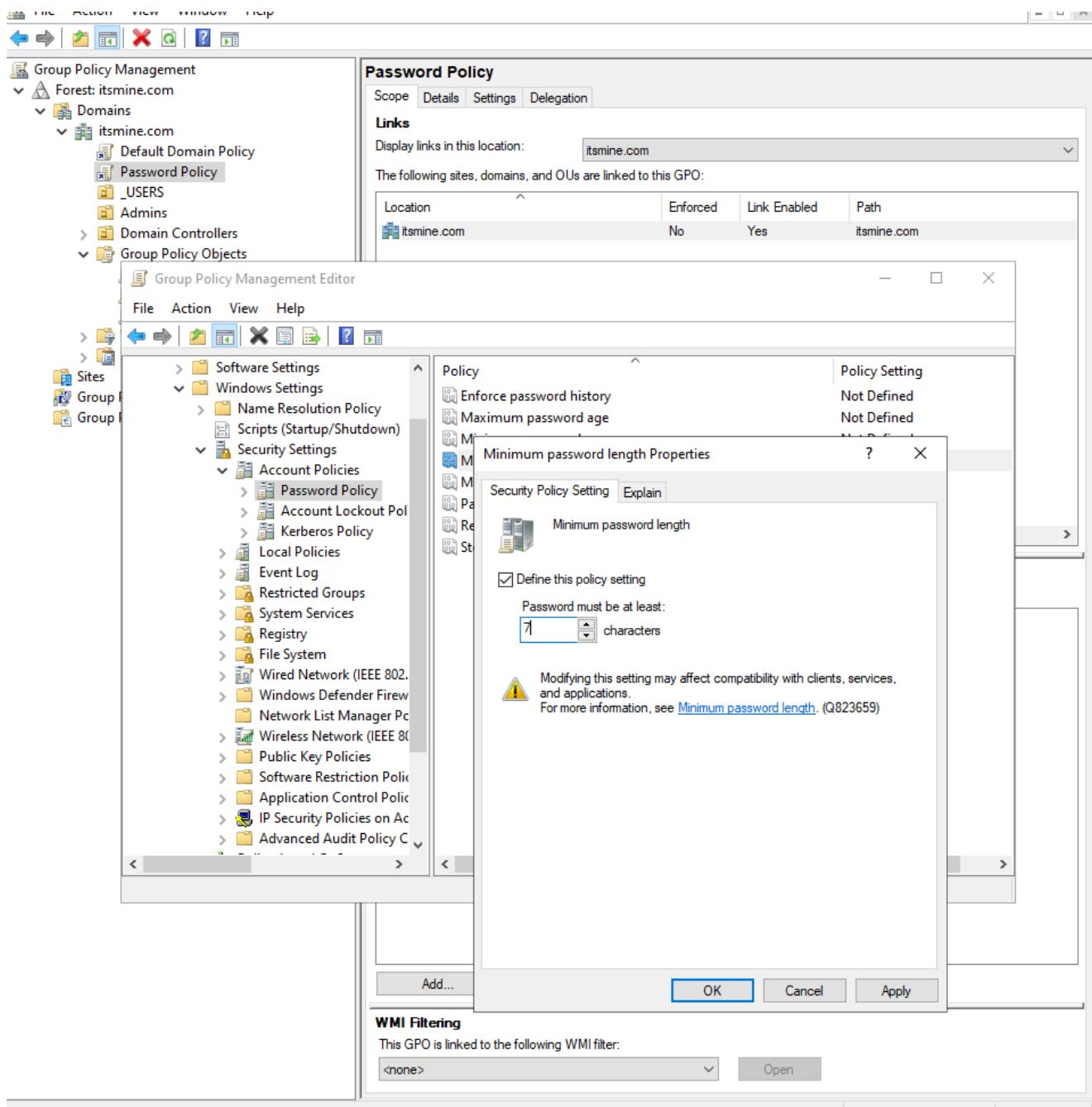
C:\Windows\system32>
```

GROUP POLICY MANAGEMENT :

A Password Policy GPO was created in Group Policy Management to enforce strong password standards across the domain. This ensures centralized control of authentication security.



Minimum password length was configured to 7 characters to prevent weak credentials. This strengthens user account protection.

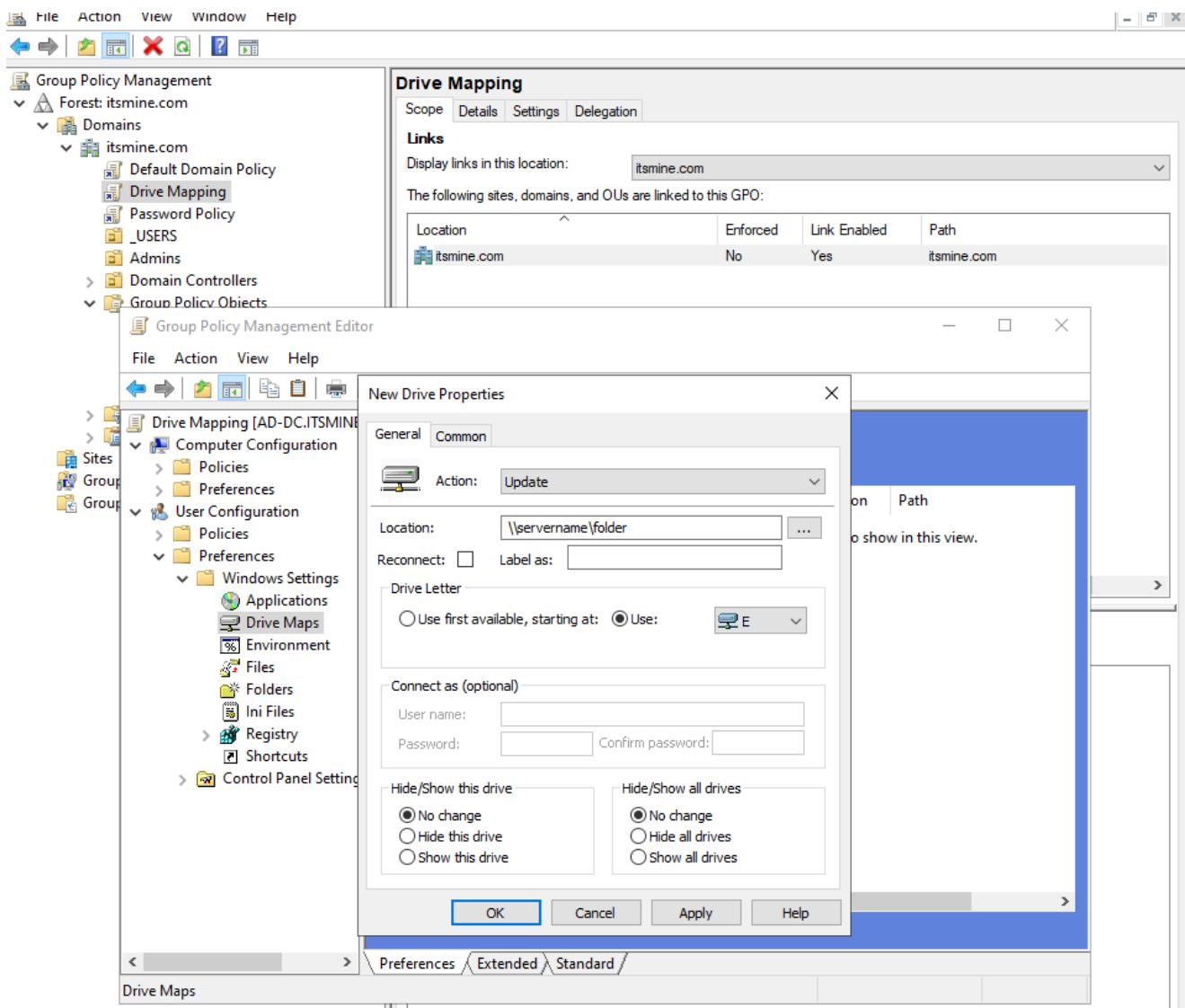


The Password Policy GPO was linked at the domain level to ensure it applies to all domain users. This guarantees uniform password enforcement. Password settings such as length and complexity were defined under Security Settings. These configurations prevent simple and predictable passwords.

The screenshot shows the Group Policy Management Editor window. In the left navigation pane, under 'Group Policy Objects', 'Default Domain Policy' is selected. In the main pane, the 'Password Policy' tab is active. The 'Scope' section shows 'Display links in this location: itsmine.com'. Below it, a table lists 'The following sites, domains, and OUs are linked to this GPO:' with one entry: 'itsmine.com' (Location: itsmine.com, Enforced: No, Link Enabled: Yes, Path: itsmine.com). The 'Policy' table on the right shows various password-related settings:

Policy	Policy Setting
Enforce password history	Not Defined
Maximum password age	Not Defined
Minimum password age	Not Defined
Minimum password length	7 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Not Defined
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Not Defined

A Drive Mapping policy was created under User Configuration to automatically connect users to a shared network drive. This provides centralized access to shared resources. The shared folder path and drive letter were configured so that users receive the mapped drive during login. This eliminates the need for manual mapping.



A Desktop Wallpaper policy was implemented to standardize the desktop background for domain users. This enforces consistent visual configuration across systems. The wallpaper setting was enabled and linked to the domain, ensuring automatic application after policy refresh.

The screenshot shows the Group Policy Management Editor interface. On the left, the navigation pane displays a tree structure under 'Group Policy Management' for the 'Forest: itsmine.com' and 'Domains' section, with 'itsmine.com' expanded to show 'Default Domain Policy', 'Desktop Wallpaper', 'Drive Mapping', and 'Password Policy'. The main pane is titled 'Desktop Wallpaper' and shows the 'Scope' tab selected. It displays the 'Links' section with 'itsmine.com' listed and a table of linked sites, domains, and OUs. The 'Edit policy setting' section for 'Desktop Wallpaper' is open, showing requirements ('At least Windows 2000') and a detailed description of what the policy does. A table lists various policy settings with their current state: 'Enable Active Desktop', 'Disable Active Desktop', 'Prohibit changes', 'Desktop Wallpaper' (which is 'Enabled'), 'Prohibit adding items', 'Prohibit closing items', 'Prohibit deleting items', 'Prohibit editing items', 'Disable all items', 'Add/Delete items', and 'Allow only bitmapped wallpaper'. At the bottom, it says '11 setting(s)'.

A Restrict Policy was configured to limit access to certain system features. This helps prevent unauthorized system modifications. Control Panel and PC settings access were disabled using Group Policy. This restricts users from altering important configurations.

The screenshot shows the Group Policy Management Editor interface. On the left, the navigation pane displays a tree structure under 'Forest: itsmine.com' with 'Domains' expanded, showing 'itsmine.com' and its policies. A 'Restrict policy' node is selected. The main pane, titled 'Restrict policy', shows the 'Scope' tab selected. It lists 'Display links in this location: itsmine.com' and 'The following sites, domains, and OUs are linked to this GPO: itsmine.com'. Below this is a table:

Location	Enforced	Link Enabled	Path
itsmine.com	No	Yes	itsmine.com

The 'Action' menu is open, showing options like File, Action, View, Help, and a toolbar with icons for New, Open, Save, Print, and Exit.

In the center, the 'Control Panel' settings are shown. The 'Prohibit access to Control Panel and PC settings' setting is listed as 'Enabled'. Other settings include 'Add or Remove Programs', 'Display', 'Personalization', 'Printers', 'Programs', 'Regional and Language Options', 'Hide specified Control Panel items', 'Always open All Control Panel Items wh...', 'Show only specified Control Panel items', and 'Settings Page Visibility'. Most settings are marked as 'Not configured'.

At the bottom, there are buttons for 'Add...', 'Remove', and 'Properties'. A 'WMI Filtering' section indicates 'This GPO is linked to the following WMI filter: <none>' with an 'Open' button.

A removable storage restriction policy was implemented to enhance endpoint security. This controls the use of external storage devices. All USB storage access was blocked by enabling the “Deny all access” option. This prevents potential data exfiltration through USB devices.

The screenshot shows the Group Policy Management console. On the left, the navigation pane includes 'Group Policy Management', 'Forest: itsmine.com', 'Domains', and 'itsmine.com'. Under 'itsmine.com', several policies are listed: 'Default Domain Policy', 'Desktop Wallpaper', 'Disable USB devices', 'Drive Mapping', 'Password Policy', and 'Restrict policy'. The 'Disable USB devices' policy is selected, and its properties are displayed in the main pane.

Disable USB devices

Scope Details Settings Delegation

Links

Display links in this location: itsmine.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
itsmine.com	No	Yes	itsmine.com

All Removable Storage classes: Deny all access

Previous Setting Next Setting

Enabled Comment:

Not Configured Disabled

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.

OK Cancel Apply

WMI Filtering

This GPO is linked to the following WMI filter:

An Account Lockout Policy was configured to defend against brute-force login attempts. This ensures account protection after repeated failed logins. Lockout threshold and duration values were defined so accounts automatically lock after multiple invalid attempts.

The screenshot shows the Group Policy Management Editor interface. On the left, the navigation pane displays the Group Policy Management tree under 'Forest: itsmine.com' and 'Domains'. A specific GPO named 'Account lockout policy' is selected. The main pane, titled 'Account lockout policy', shows the 'Scope' tab selected. It lists 'Display links in this location: itsmine.com' and 'The following sites, domains, and OUs are linked to this GPO:'. A table shows one link: 'itsmine.com' with 'Enforced: No', 'Link Enabled: Yes', and 'Path: itsmine.com'. Below this, the 'Group Policy Management Editor' window is open, showing the 'Account lockout policy [AD-DC.ITSMINE.C...' node under 'Computer Configuration / Policies / Windows Settings / Security Settings / Account Policies / Password Policy / Account Lockout Pol...'. The 'Properties' tab of the GPO editor is visible at the bottom.

Location	Enforced	Link Enabled	Path
itsmine.com	No	Yes	itsmine.com

Policy Setting

Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes

All configured GPOs were reviewed to confirm proper linking and enforcement at the domain level. This verifies that security policies are actively applied.

The screenshot shows the Group Policy Management console interface. On the left, a tree view displays the Group Policy Management structure under 'Forest: itsmine.com'. Key nodes include 'Domains' (with 'itsmine.com' expanded), 'Group Policy Objects' (also expanded), and other administrative categories like 'COM', 'WMI Filters', 'Starter GPOs', 'Sites', 'Group Policy Modeling', and 'Group Policy Results'. The right pane is titled 'itsmine.com' and contains a 'Status' tab. It provides a summary of Active Directory and SYSVOL replication status. A message states: 'This page shows the status of Active Directory and SYSVOL (DFSR) replication for this domain as it relates to Group Policy.' Below this, 'Status Details' show: 'AD-DC.itsmine.com is the baseline domain controller for this domain.' (with a 'Change' link), '0 Domain controller(s) with replication in progress' (indicated by a red question mark icon), and '0 Domain controller(s) with replication in sync' (indicated by a green checkmark icon).

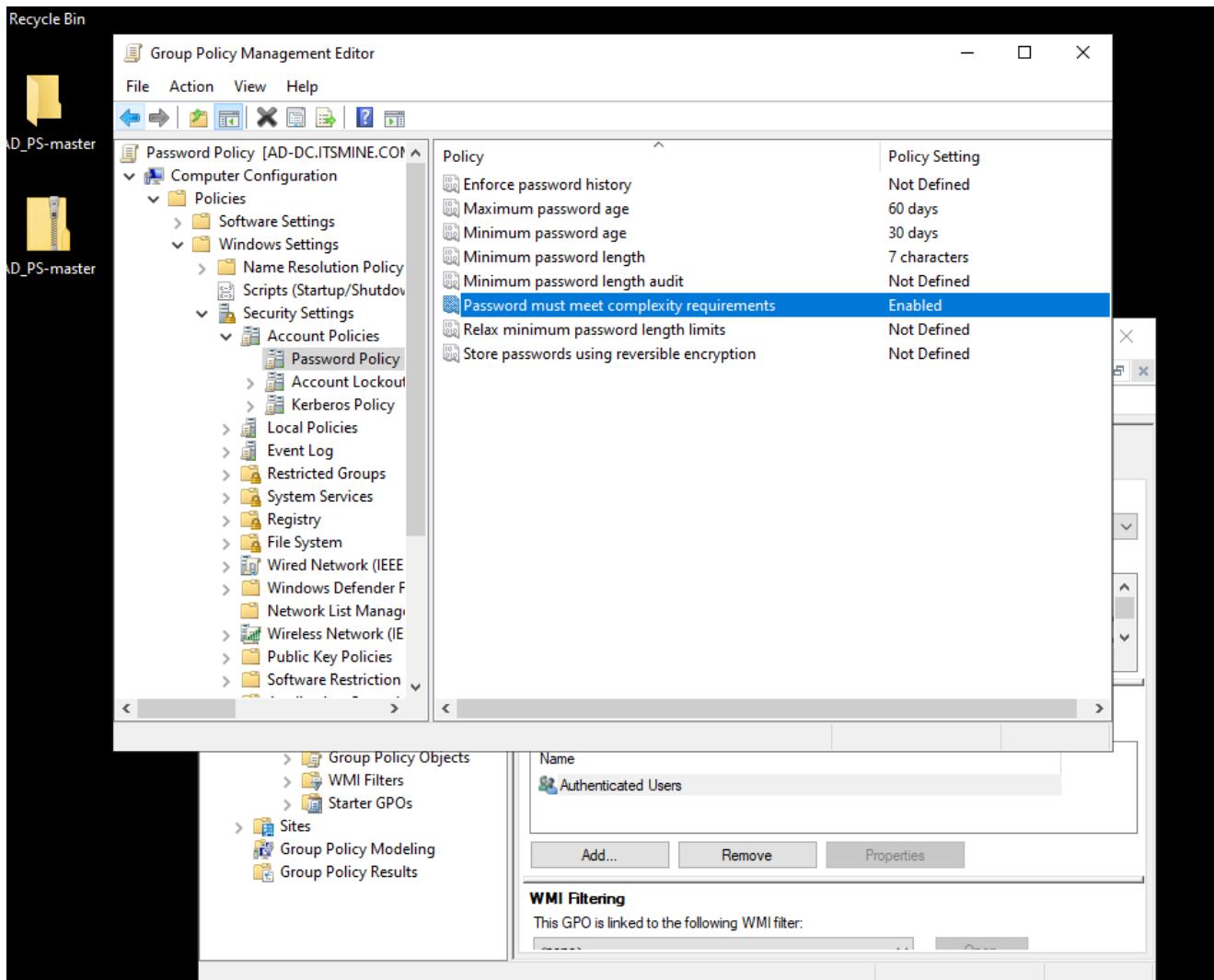
SECURITY POLICY (TESTING) :

Security policy implementation section introduces the importance of enforcing strong domain-level security configurations.

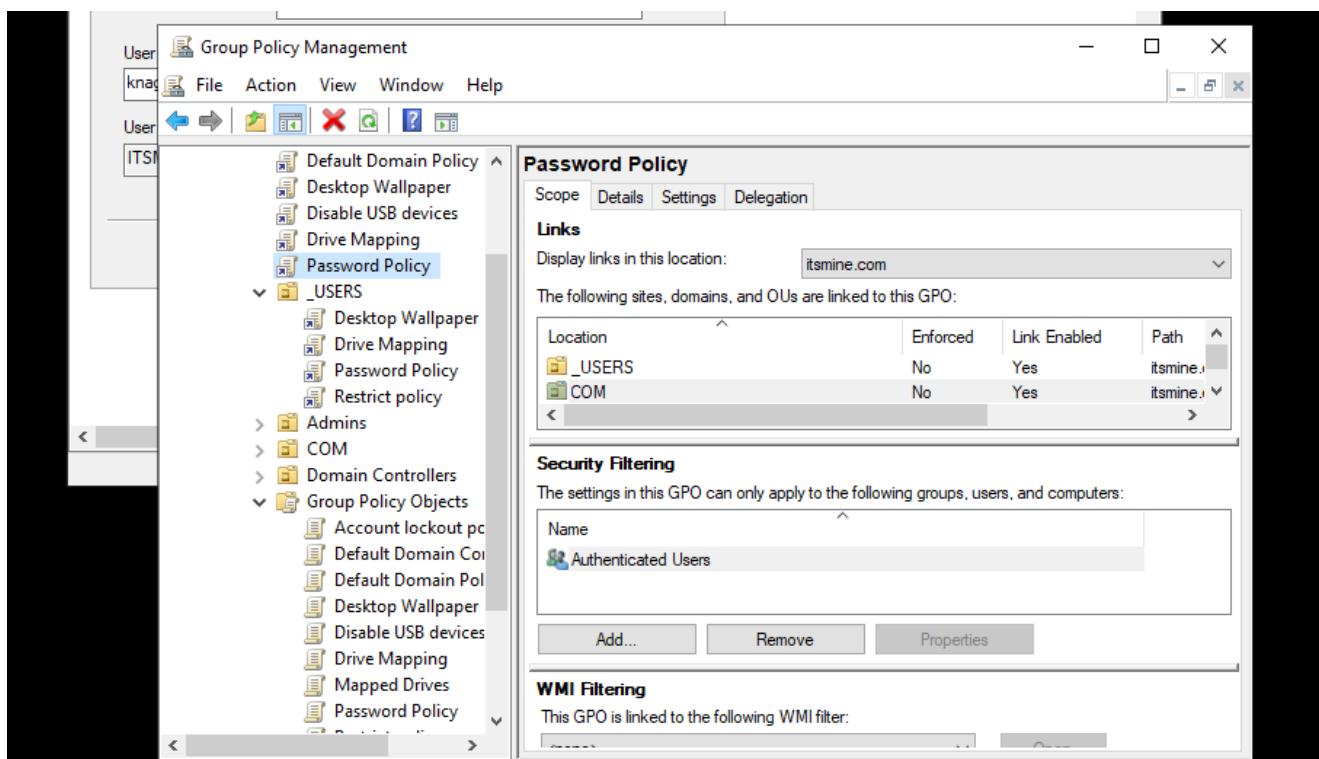
Activity 1: Password Policy Configuration

Configure and enforce a strong password policy for AD users.

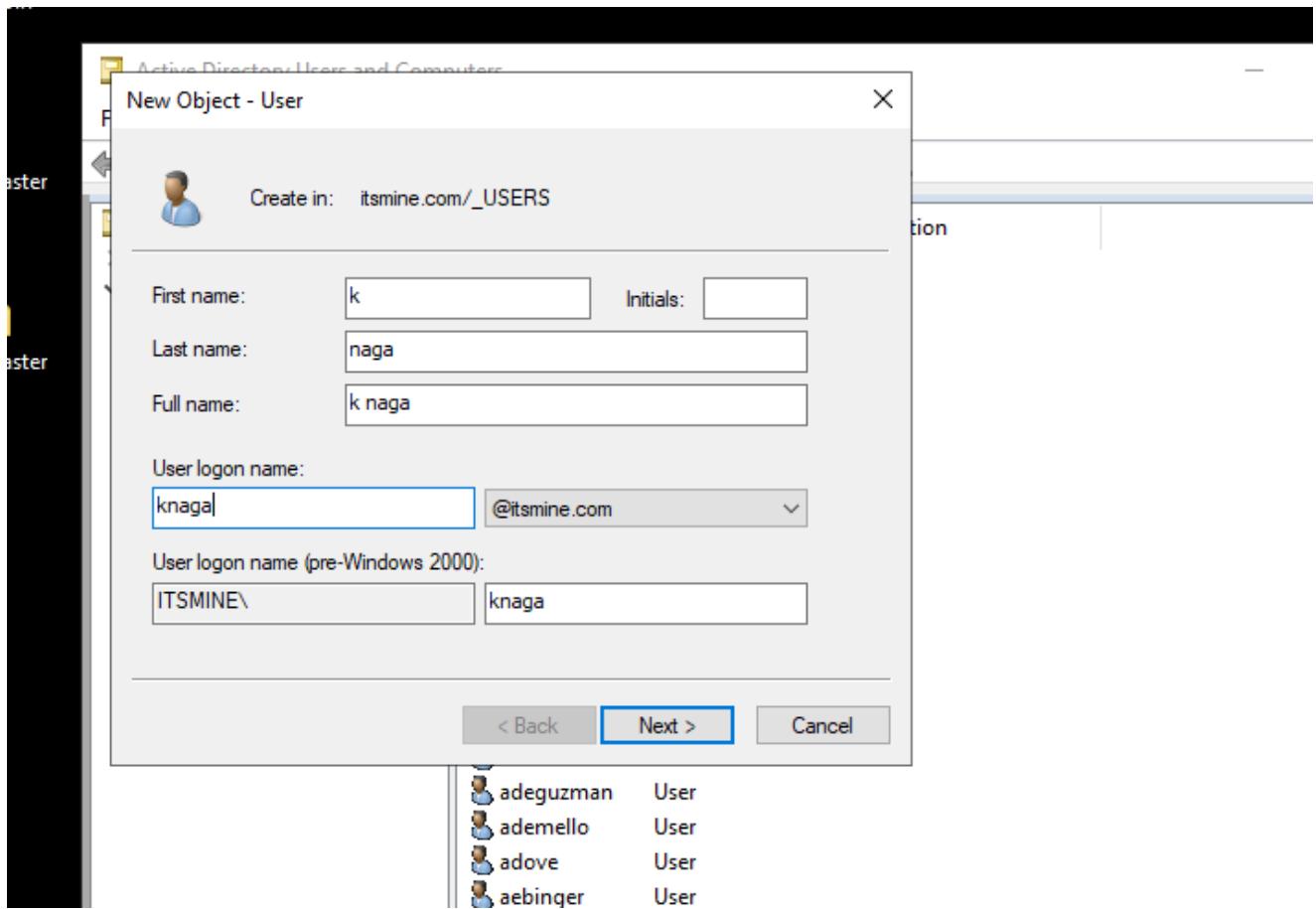
Password Policy settings were reviewed again to validate configuration values such as minimum length and complexity enforcement.



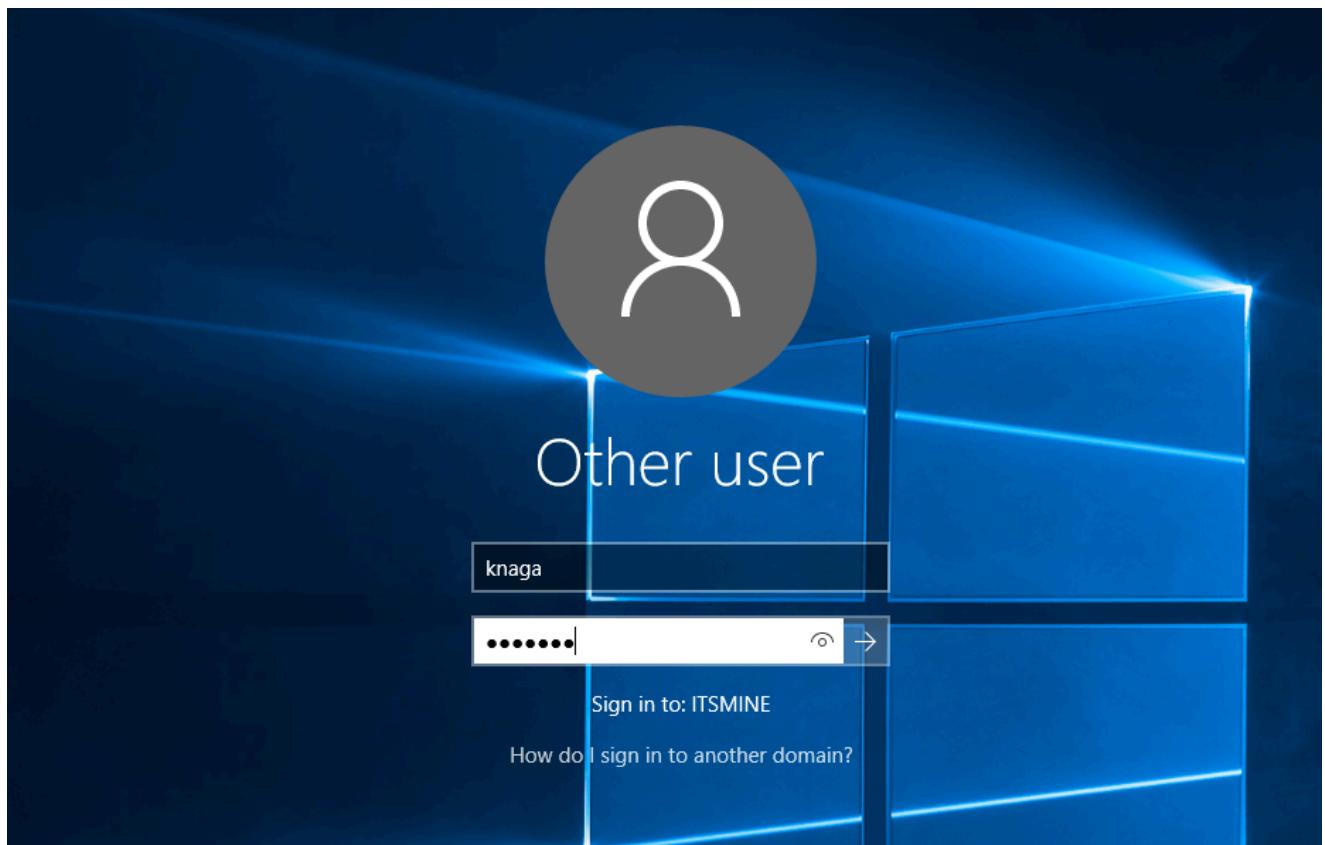
The Password Policy GPO was linked to the required Organizational Unit to ensure it applies to selected users.



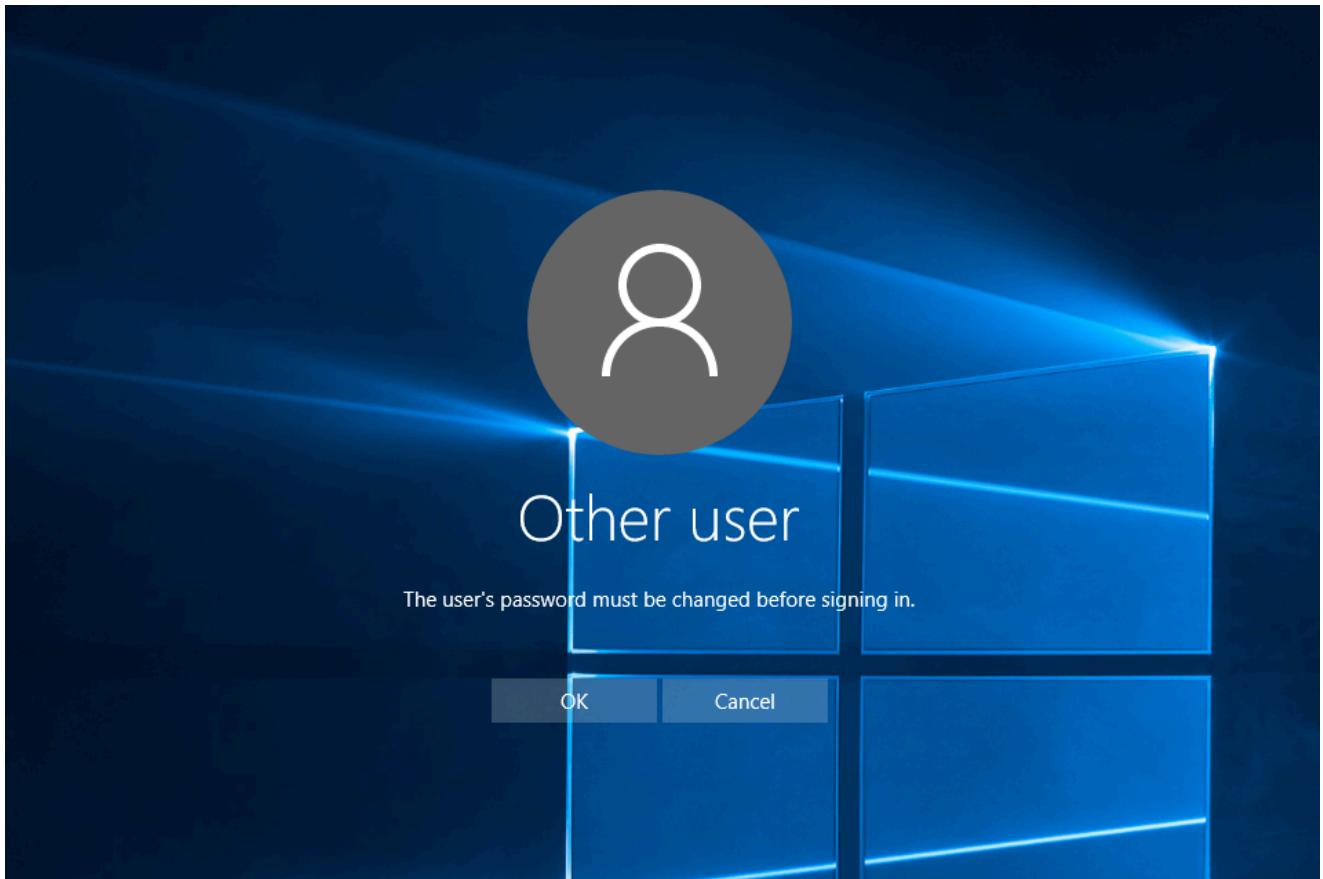
A new test user account was created to validate the password policy behavior under real login conditions.



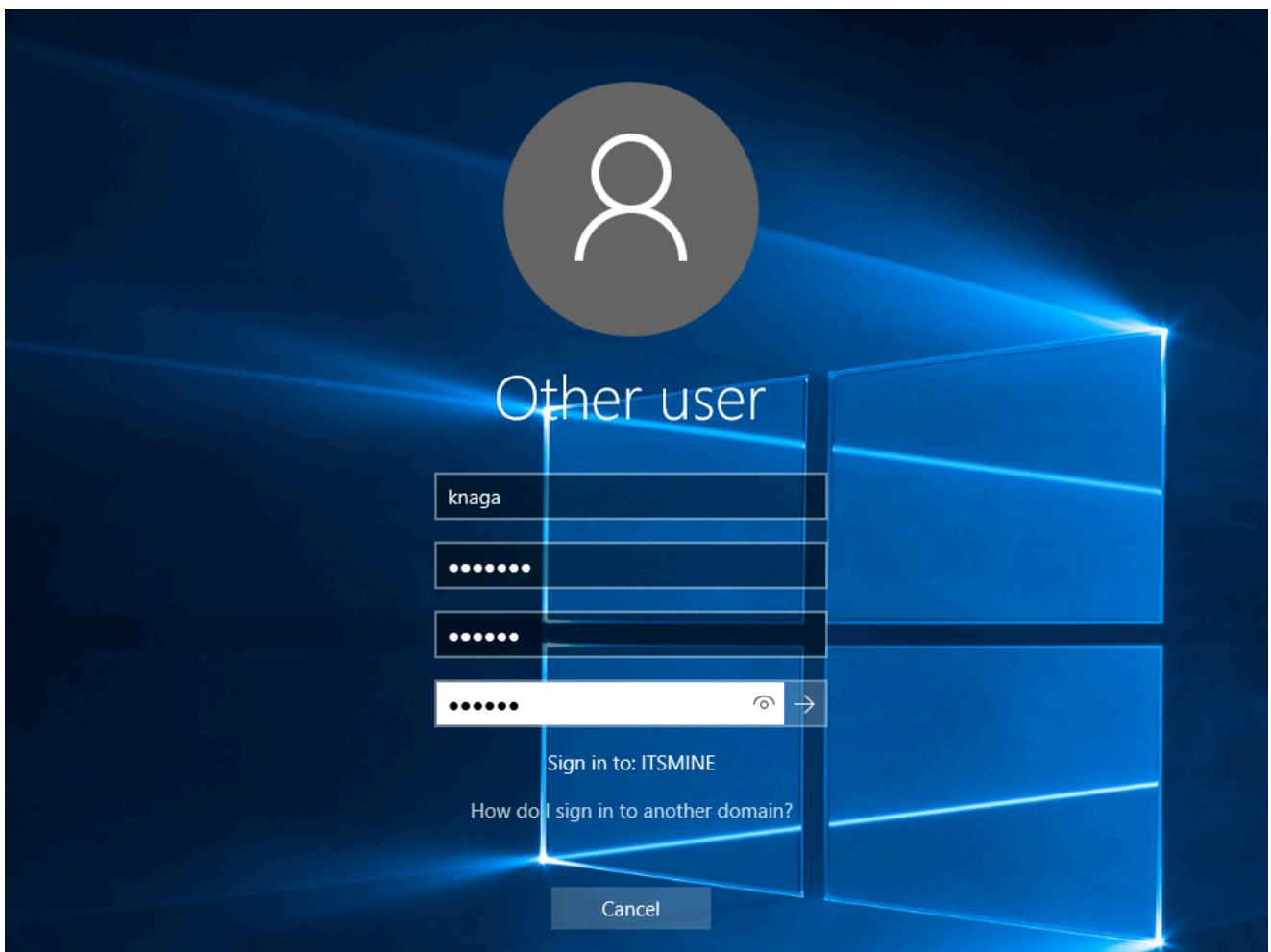
The newly created user attempted login for the first time, triggering a mandatory password change requirement.



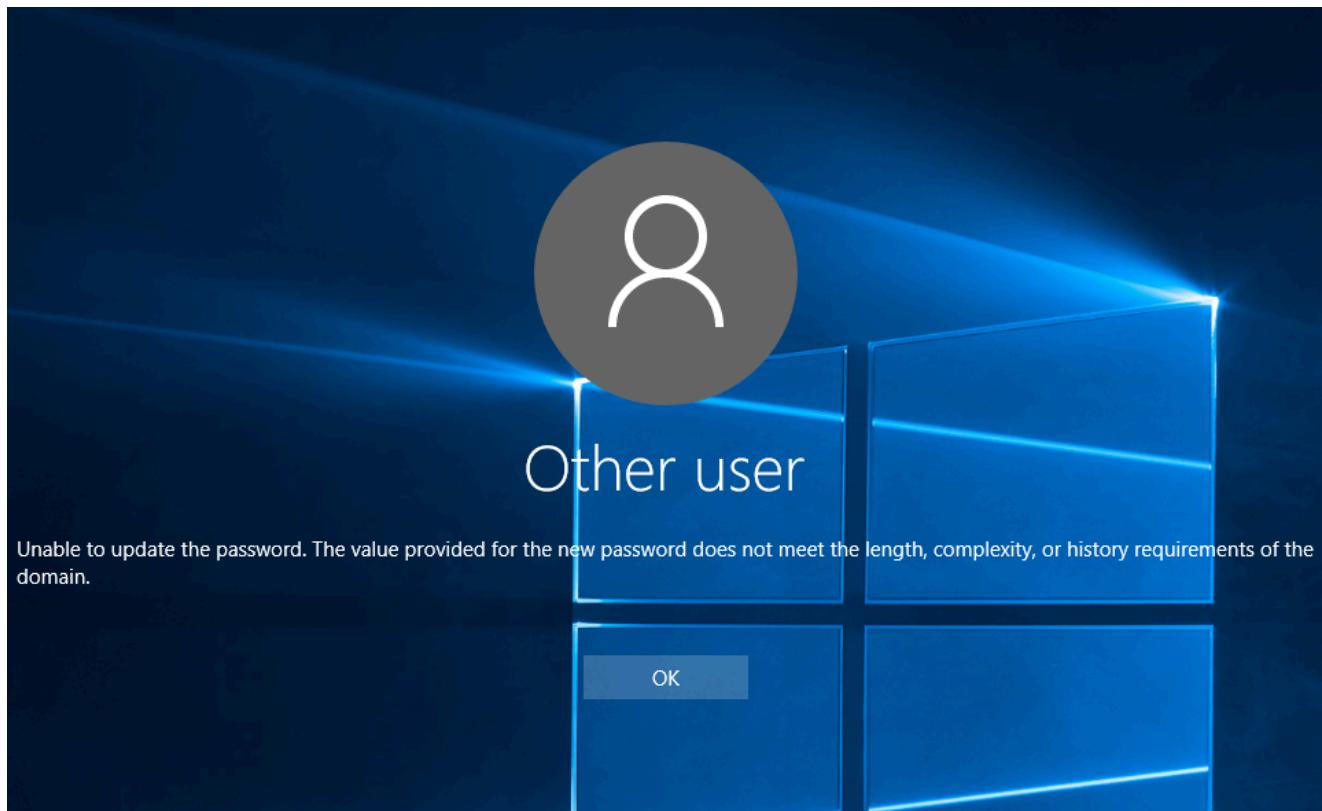
The system enforced password change before granting access, confirming correct policy application.



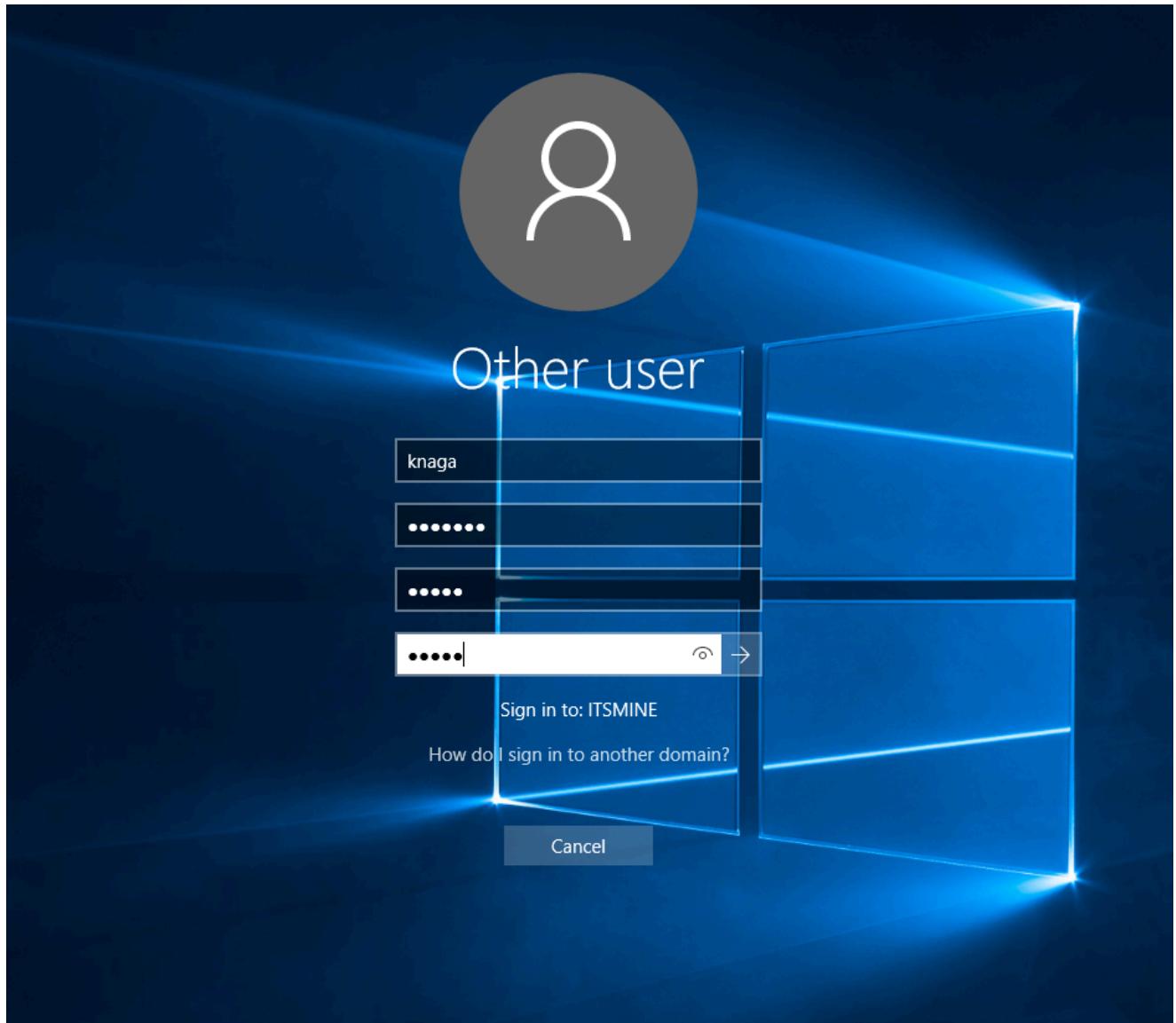
An attempt was made to set a weak password that does not meet policy requirements.



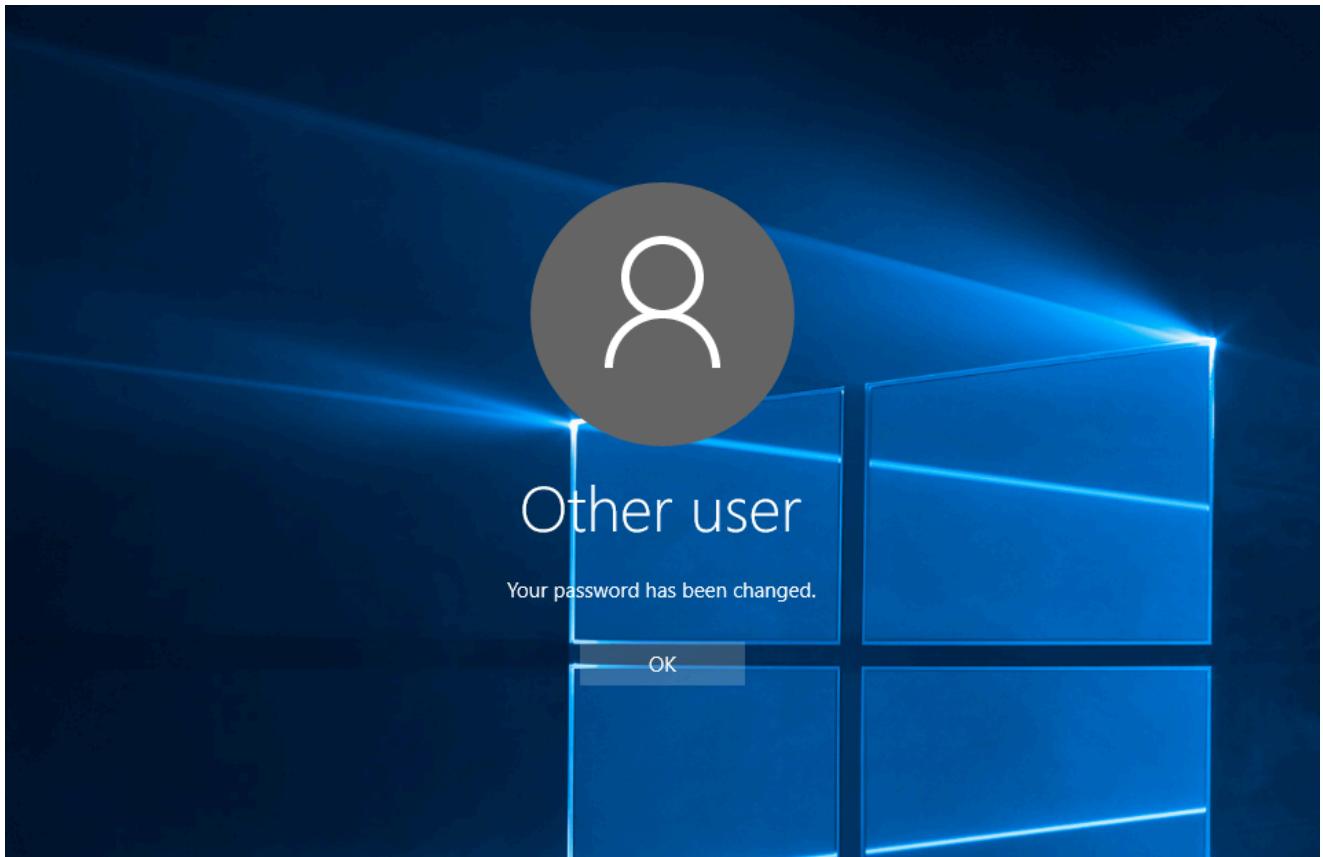
The system rejected the password due to length and complexity restrictions, confirming enforcement of the configured policy.



A compliant password meeting domain security requirements was entered.



Password change was successfully completed, confirming proper policy validation.

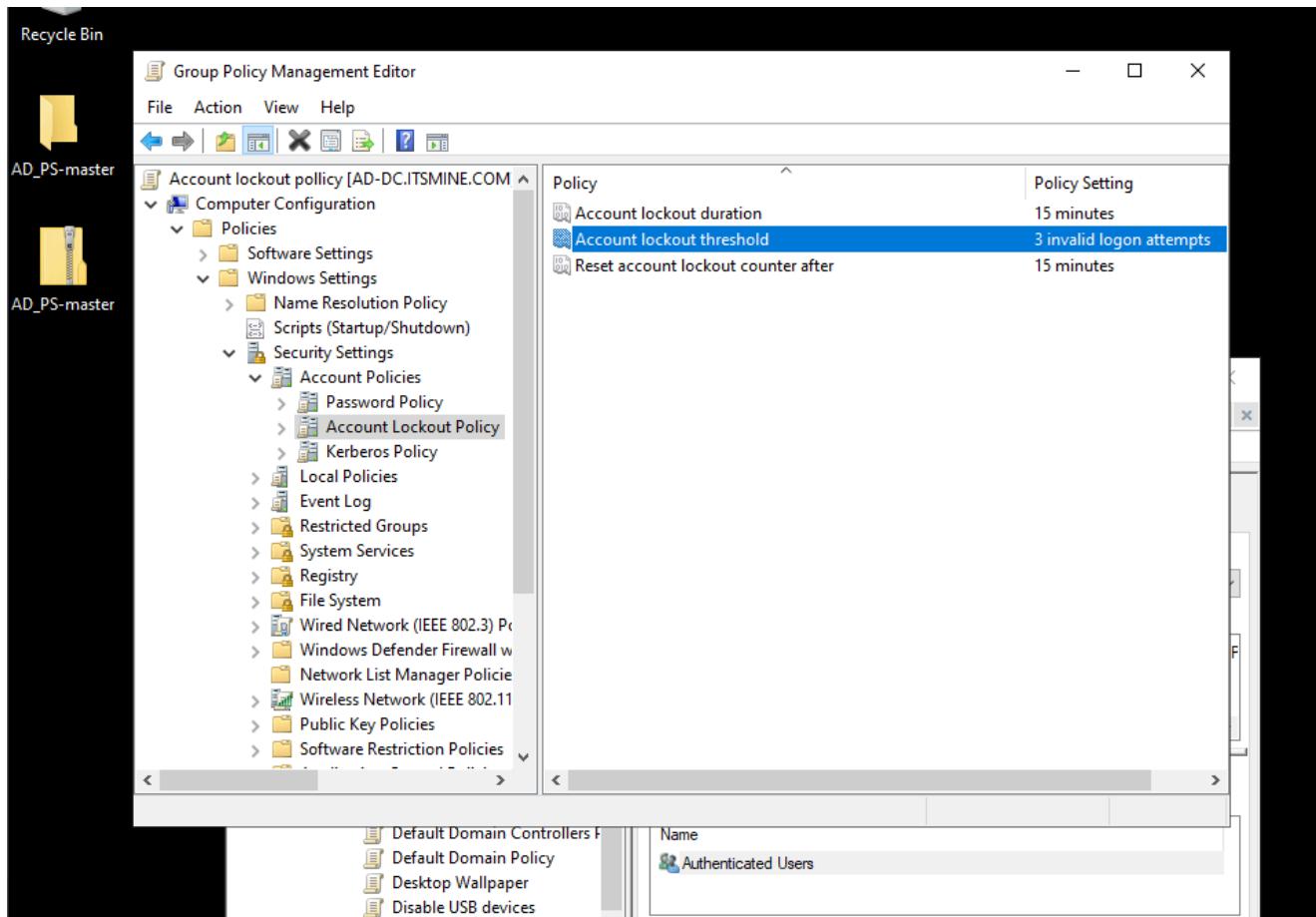


Account Lockout Policy configuration was reviewed to confirm threshold and duration settings for failed login attempts.

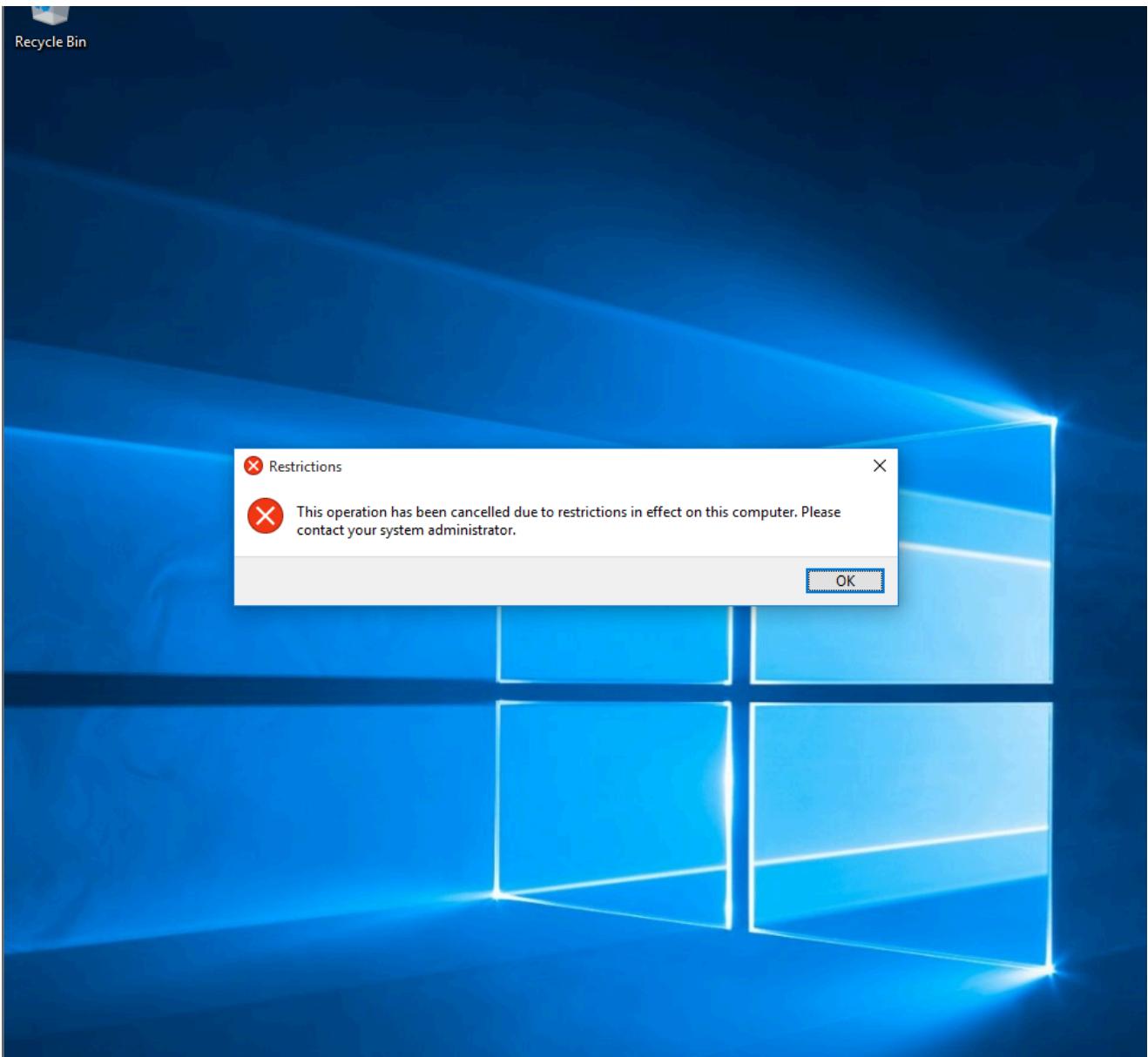
Activity 2: Account Lockout Policy Configuration

Configure an account lockout policy to protect against brute-force attacks.

password threshold



A restriction message appeared when attempting a blocked action, confirming that Control Panel restriction policy is active.



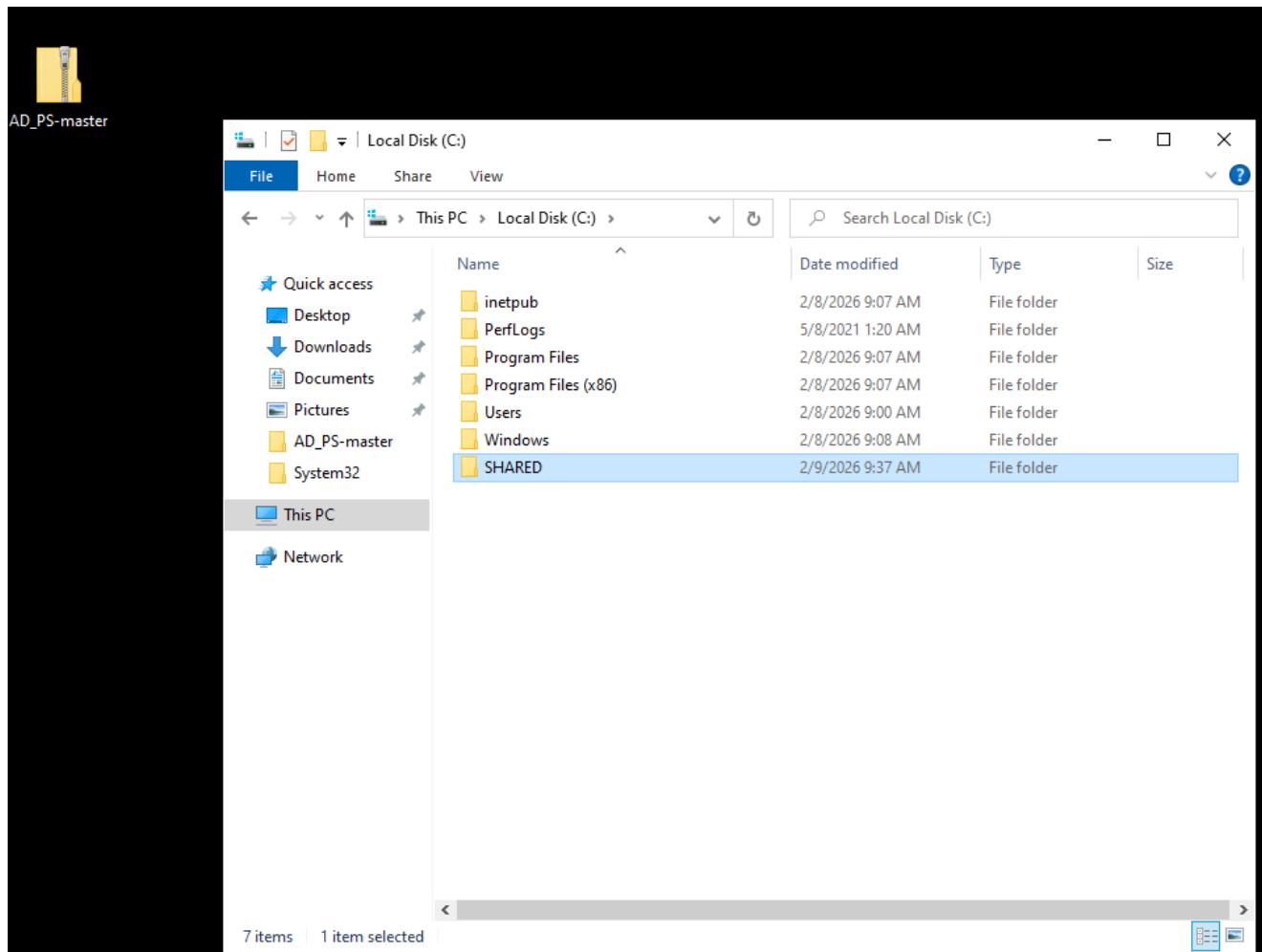
FILE SERVICES (SETTING UP NETWOKR SHARING):

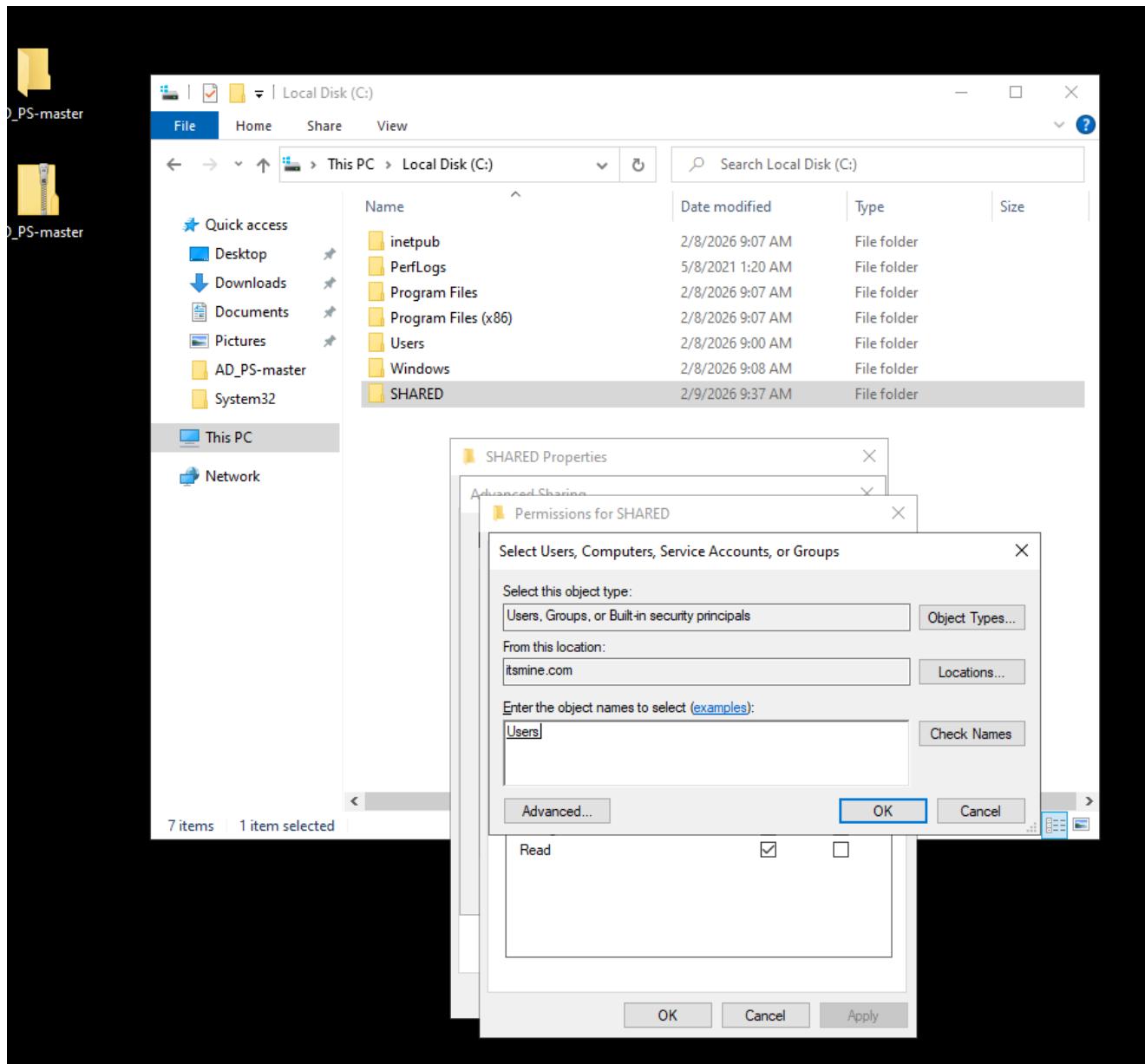
Activity 1: Set Up a File Sharing

Configure File Sharing

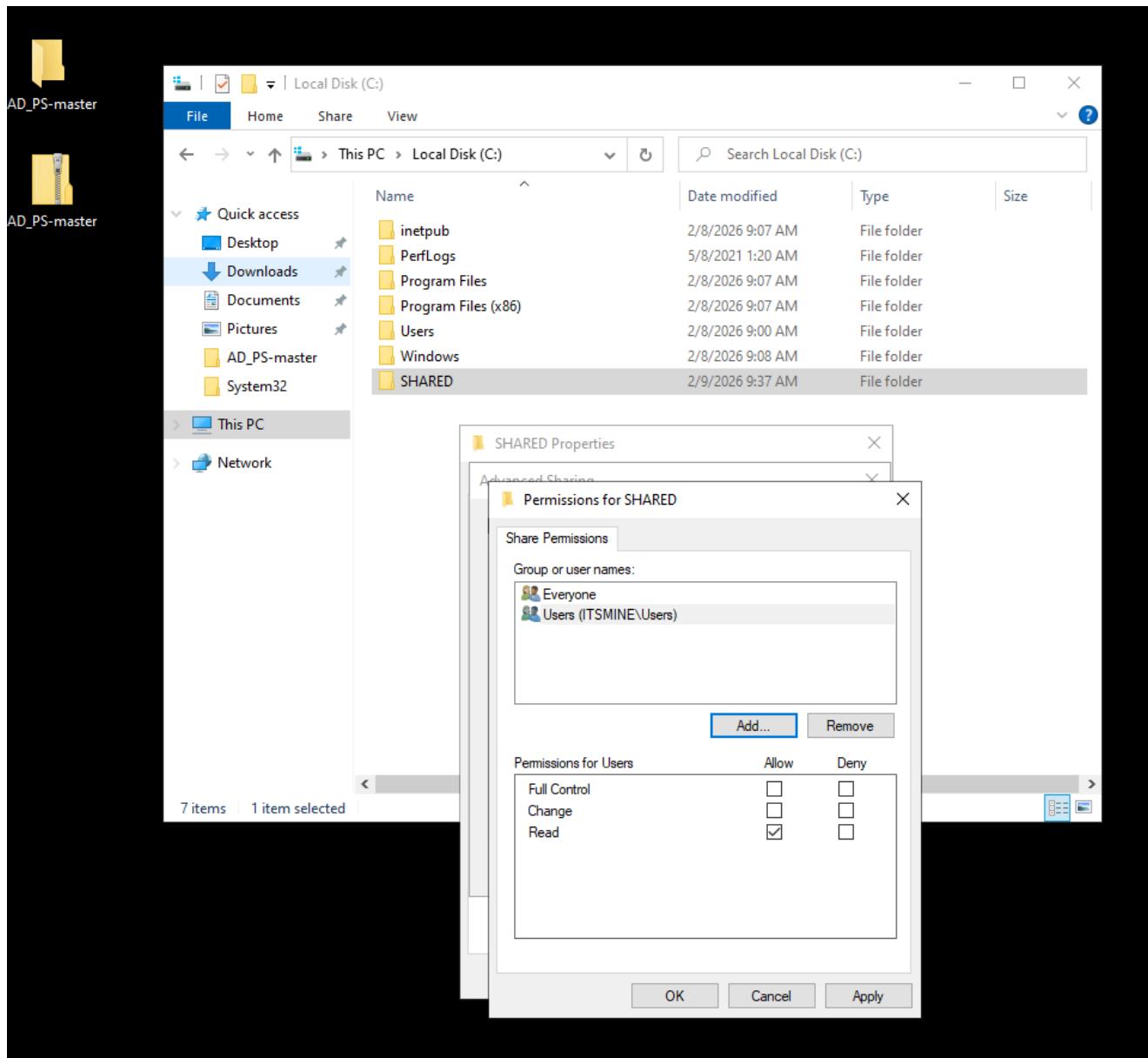
- Create shared folders with appropriate permissions.
- Set NTFS and share permissions to allow domain users access.

A shared folder named SHARED was created on the server to provide centralized file access to domain users

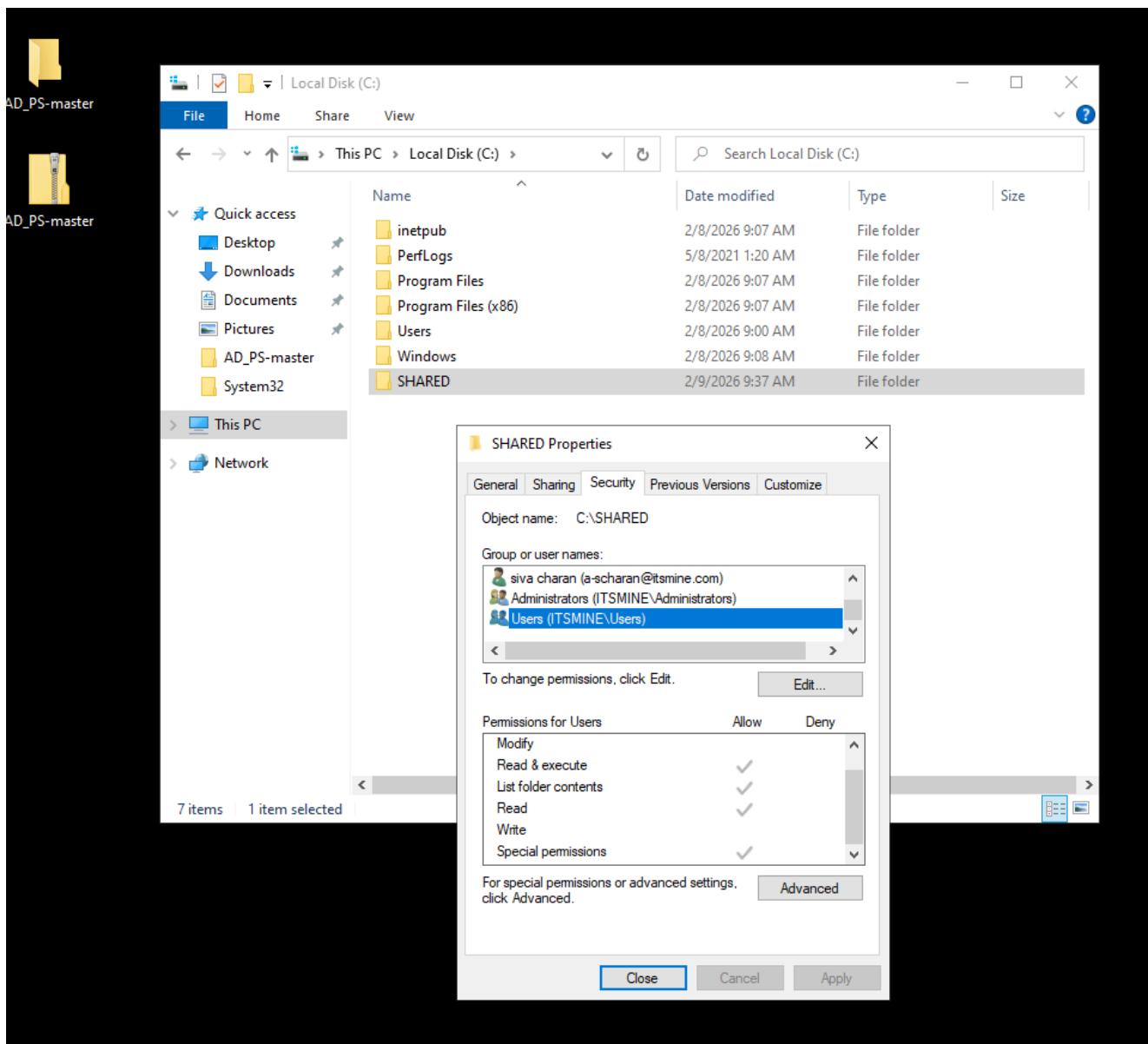




Share permissions were configured for the SHARED folder, granting access to domain users for file sharing within the network.



NTFS permissions were configured for the SHARED folder to control user-level access within the domain.

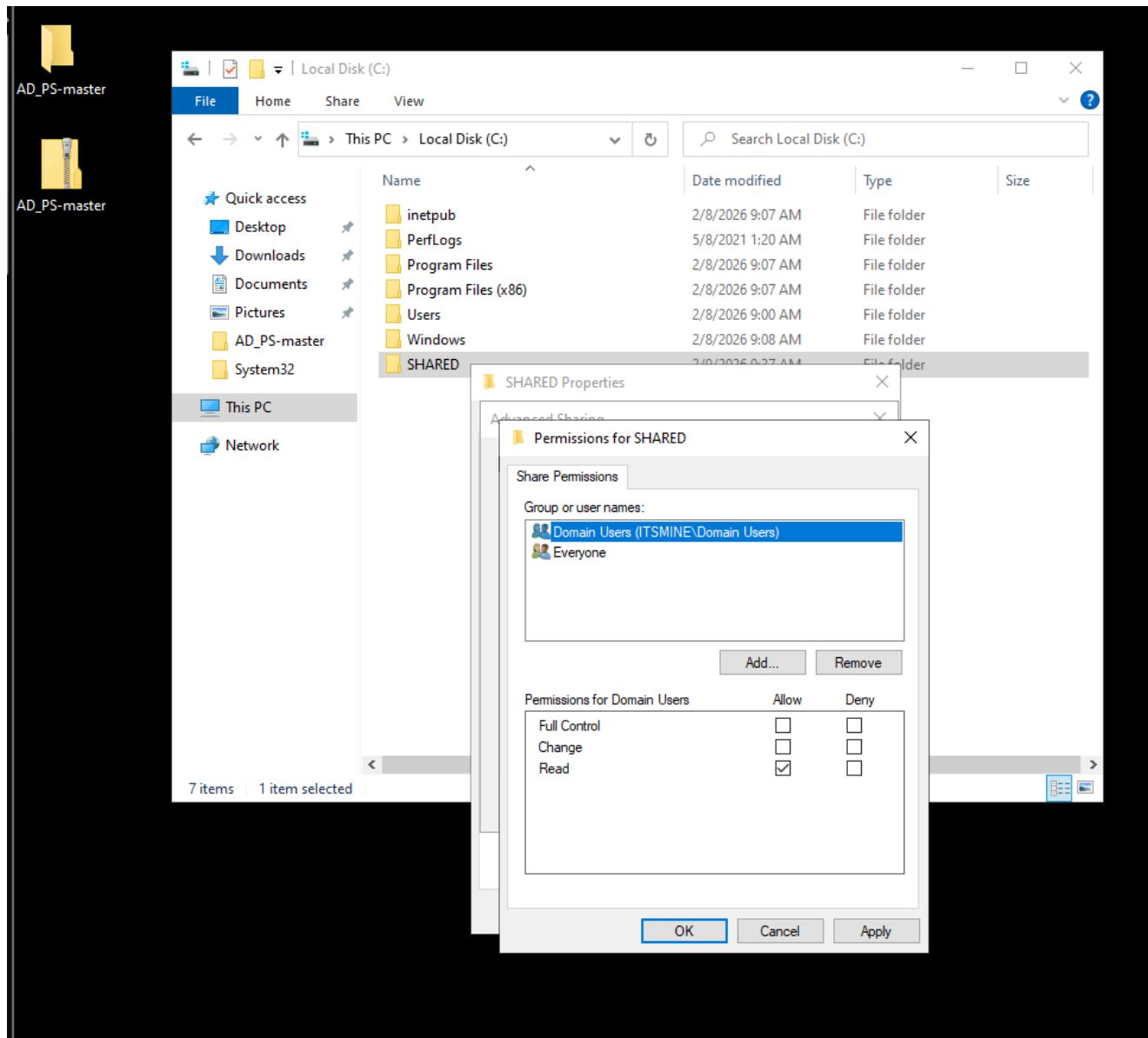


Activity 2: Set Up Client Machines

Access Shared Resources

- Log in to the client machines using domain user accounts.
 - Map network drives to access shared folders.

Share permissions were adjusted to allow Domain Users access to the SHARED folder. This enables domain-based file access from client systems.

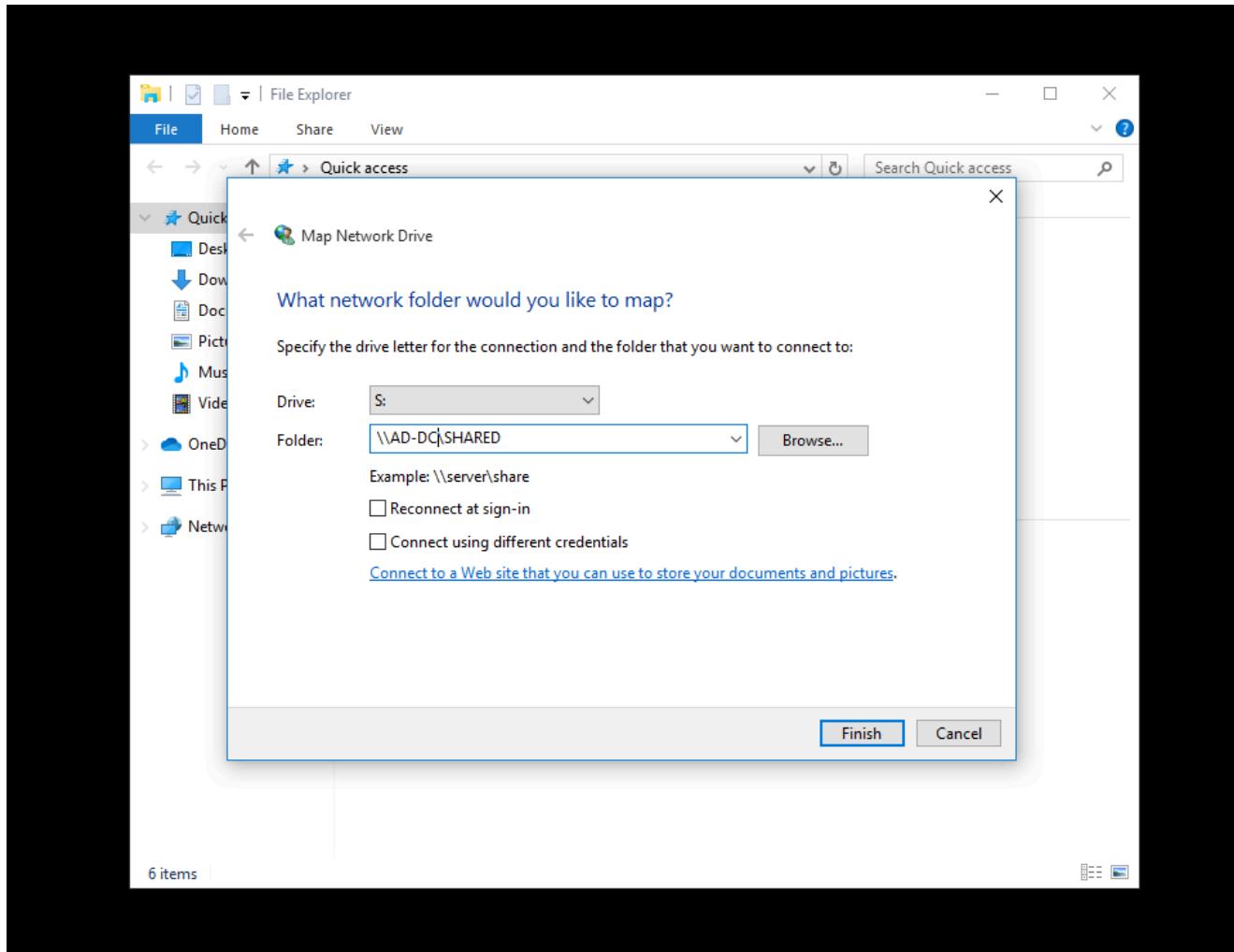


```
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

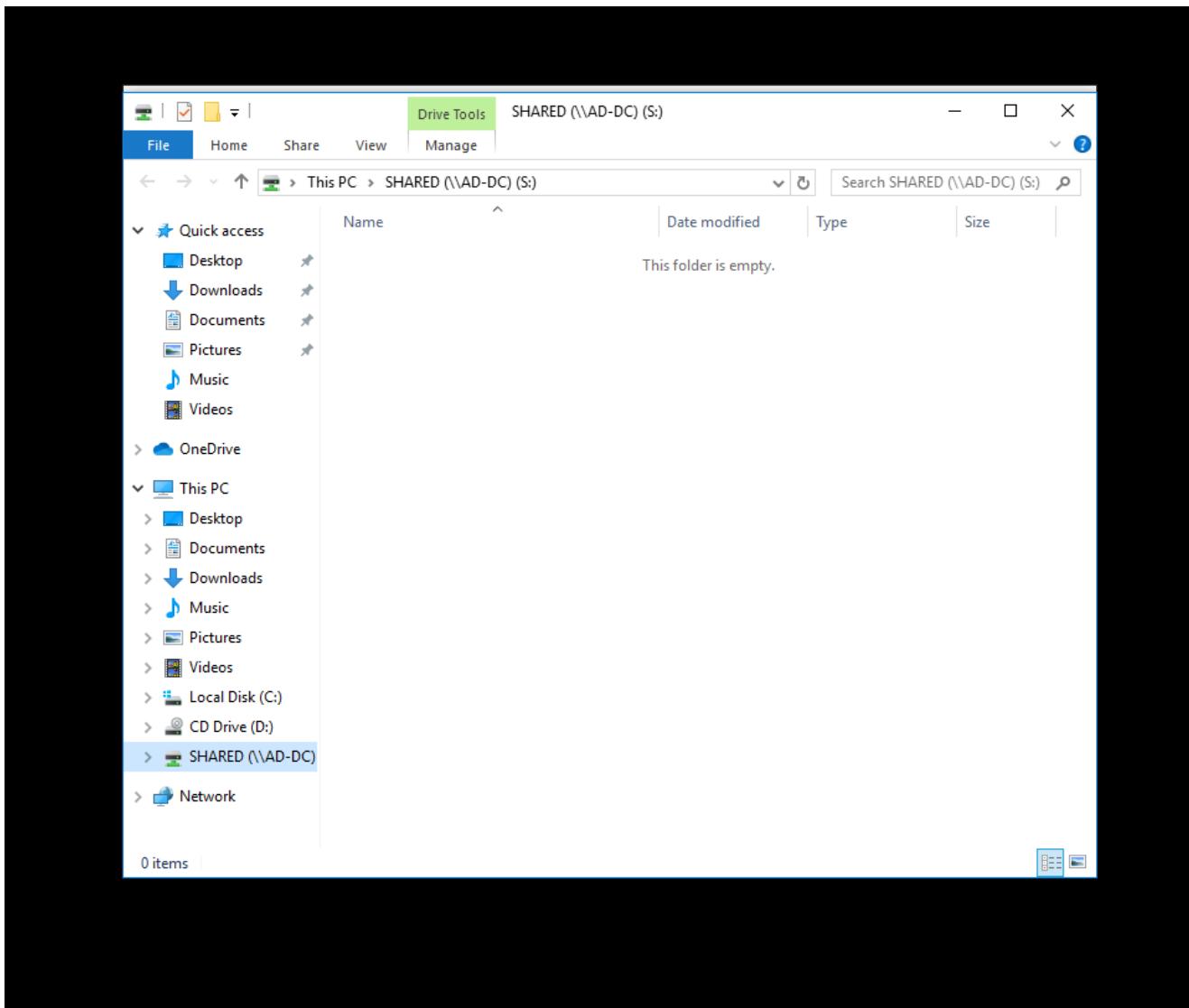
C:\Users\ascharan>hostname
AD-DC

C:\Users\ascharan>
```

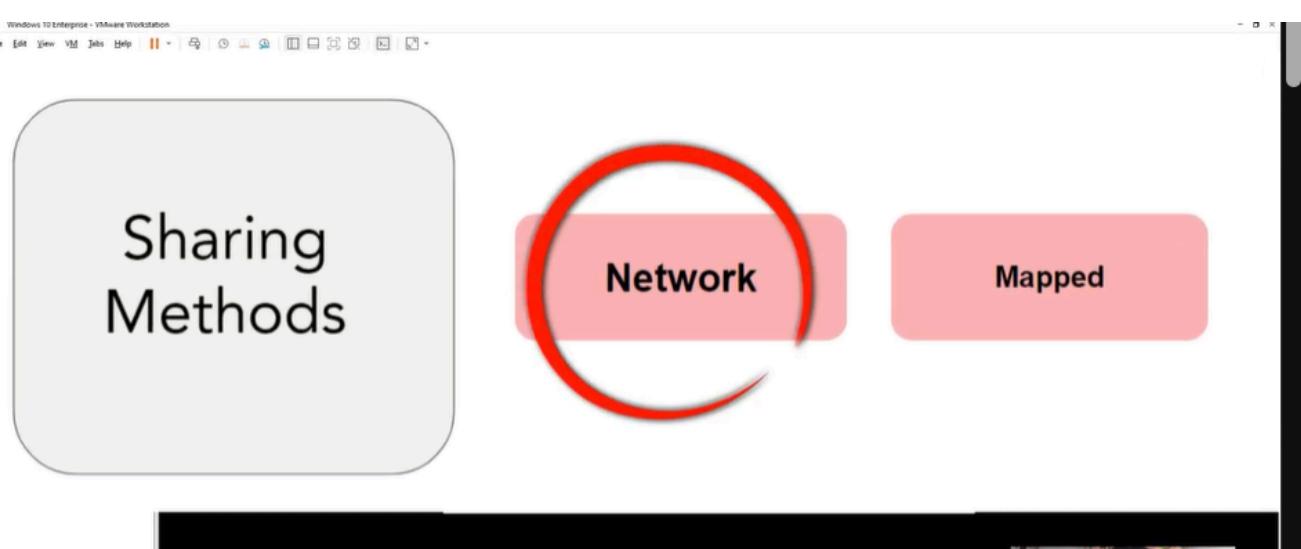
The shared folder was mapped using the network path (\AD-DC\SHARED). This allows users to access the shared folder as a local drive.



The mapped SHARED drive is visible on the client system. This confirms successful network drive connection.



Different sharing methods such as direct network access and mapped drives are illustrated for resource accessibility.

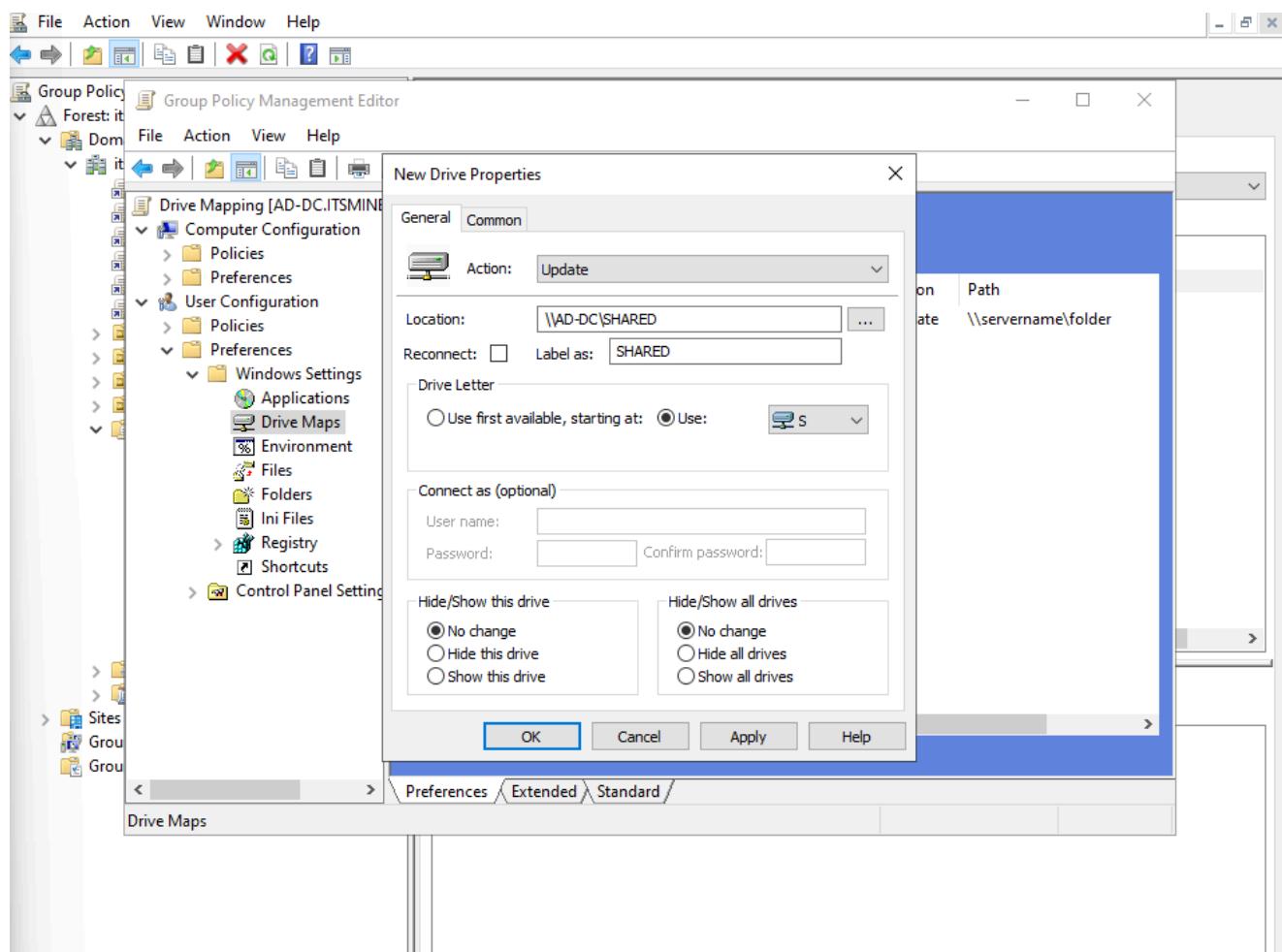


Activity 3: GPO Configuration

A

Configure Group Policy Objects (GPOs) to automatically map network drives for users.

A Drive Mapping GPO was configured with the shared folder path and assigned drive letter. This ensures automatic mapping at user login.



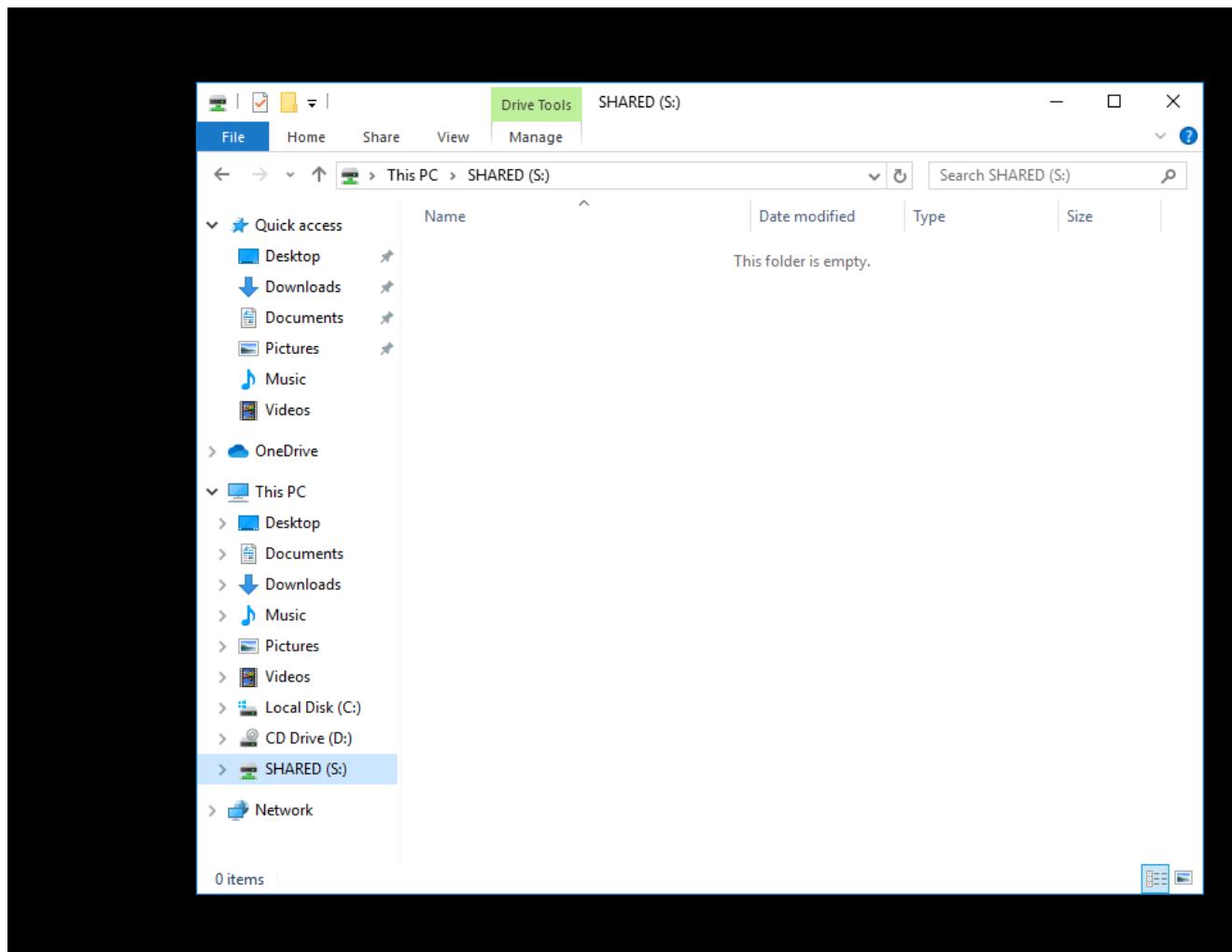
The Drive Mapping GPO was linked to the relevant Organizational Unit to apply automatically to selected users

The screenshot shows the 'Drive Mapping' section of the Group Policy Management console. The left pane displays a tree structure of Group Policies under 'Forest: itsmine.com'. The 'itsmine.com' policy is expanded, showing various GPOs like 'Account lockout policy', 'Default Domain Policy', etc., and a 'Drives' folder which contains 'Drive Mapping'. The right pane is titled 'Drive Mapping' and contains four tabs: Scope, Details, Settings, Delegation, and Status. The 'Scope' tab is selected. It shows a table of links:

Location	Enforced	Link Enabled	Path
_USERS	No	Yes	itsmine.com/_USERS
itsmine.com	No	Yes	itsmine.com

Below the table is a 'Security Filtering' section with a list of groups: 'Authenticated Users'.

The SHARED drive appears automatically on the client machine after policy refresh, confirming successful GPO deployment.

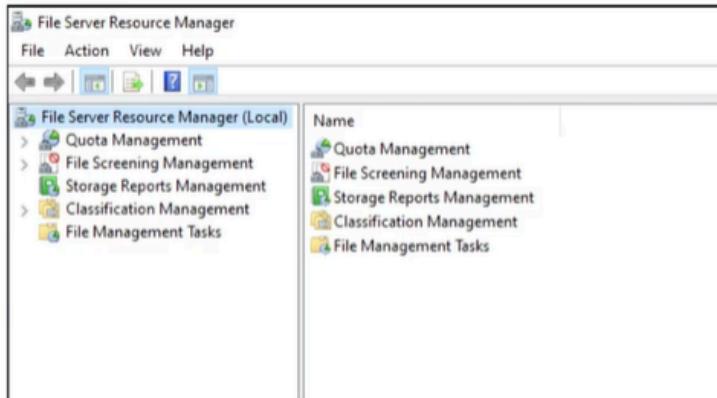


Activity 4: Implement quotas and file screening using File Server Resource Manager (FSRM).

Configure FSRM to create Quota Template and File Screen Template to effectively manage File Storage in your organization

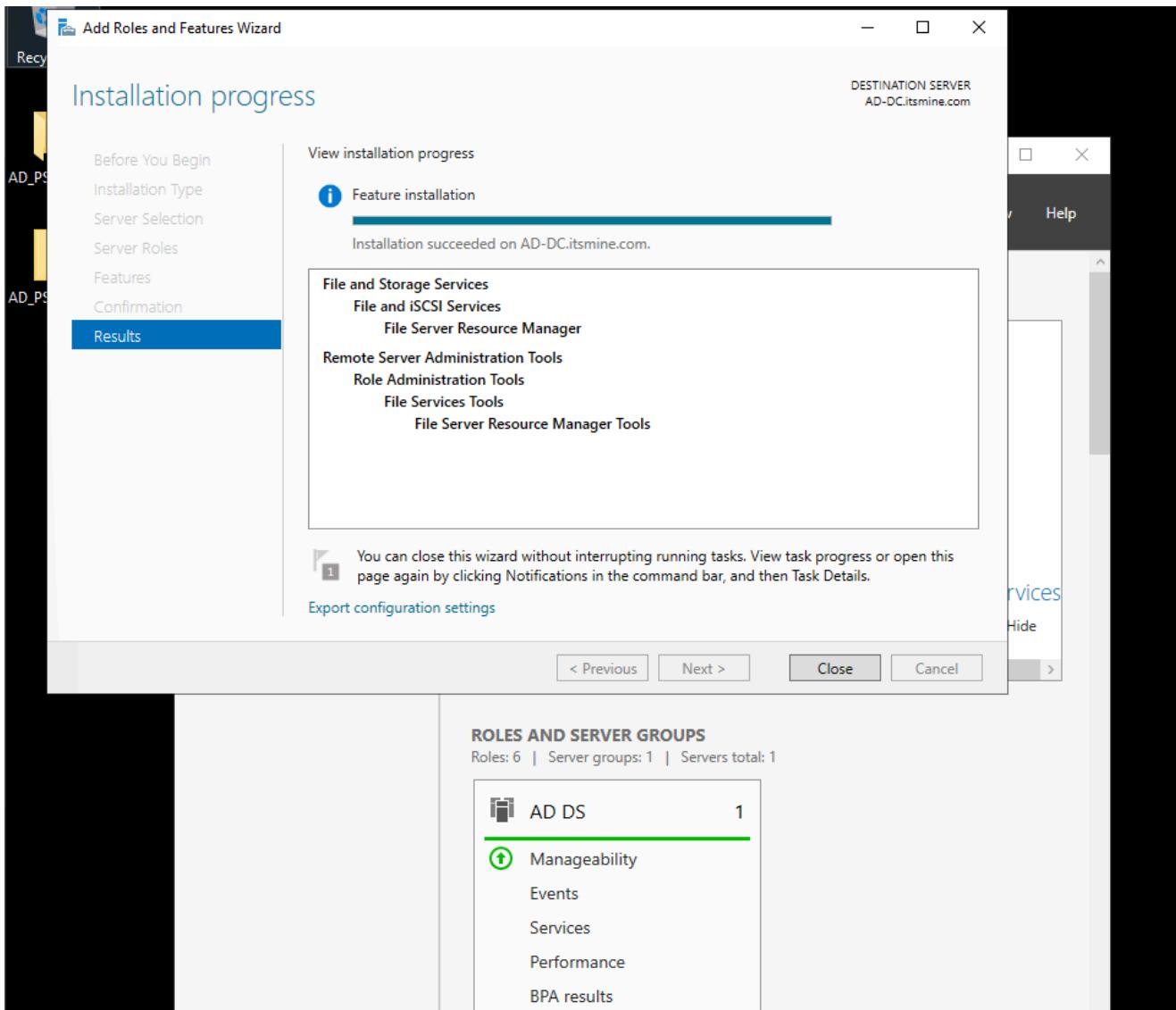
FSRM console displays tools such as Quota Management and File Screening Management for advanced file server control.

File Server Resource Manager (FSRM)

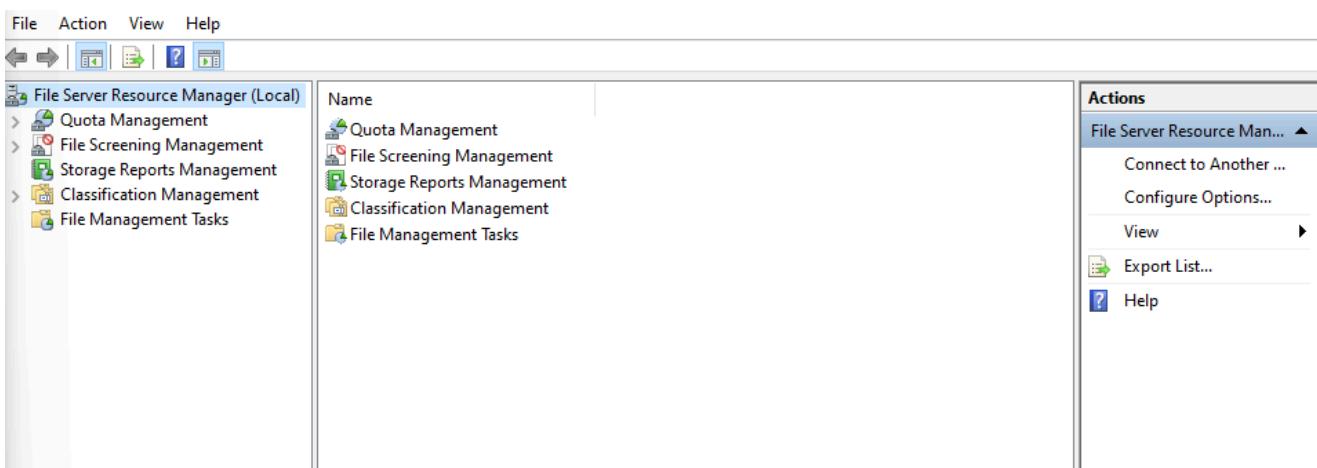


suite of tools provided by Microsoft to help you manage and classify data stored on file servers.

File Server Resource Manager role service was installed under File and Storage Services to enable quota and screening features.



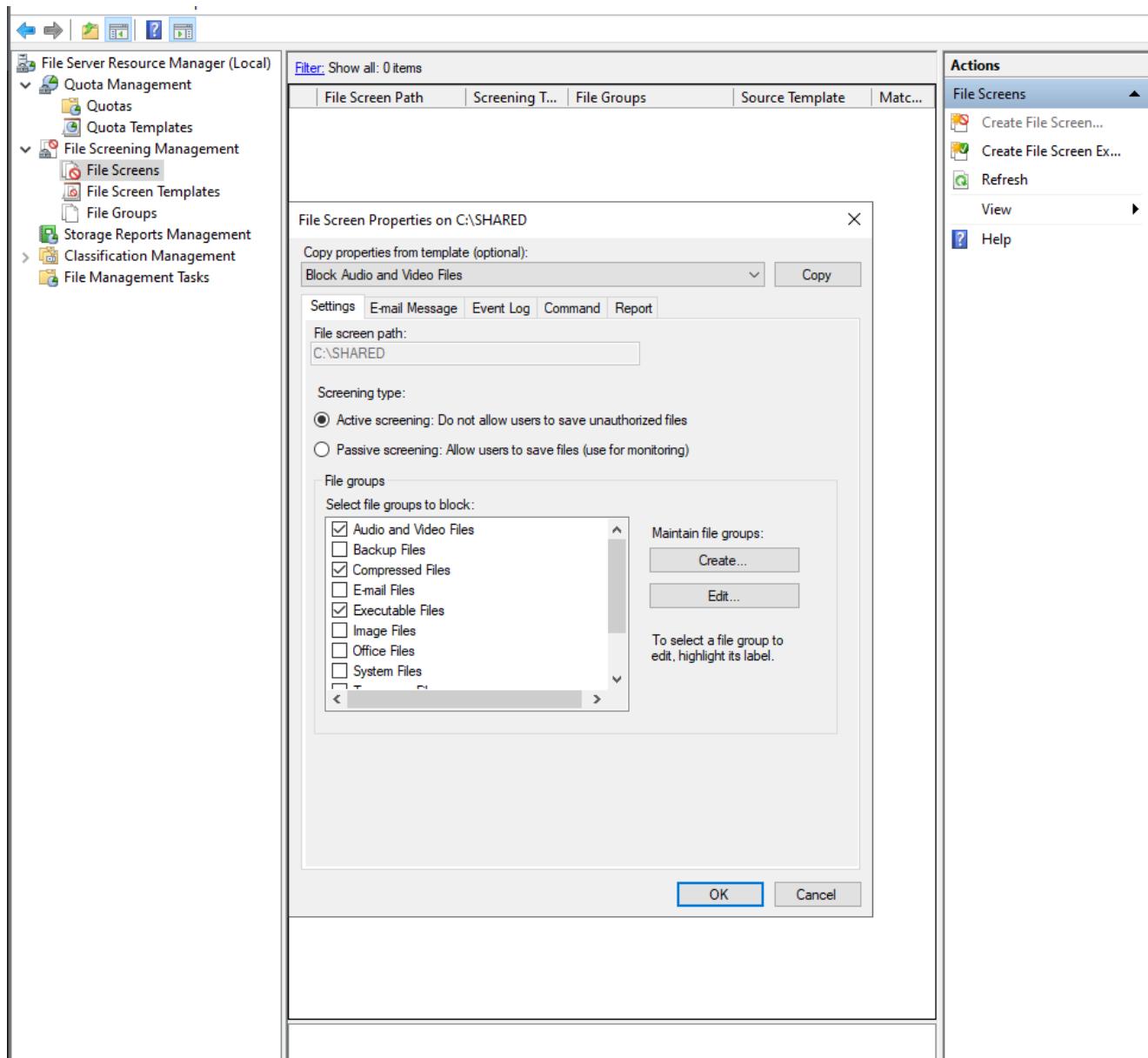
FSRM management interface shows available configuration sections including quotas and file screens.



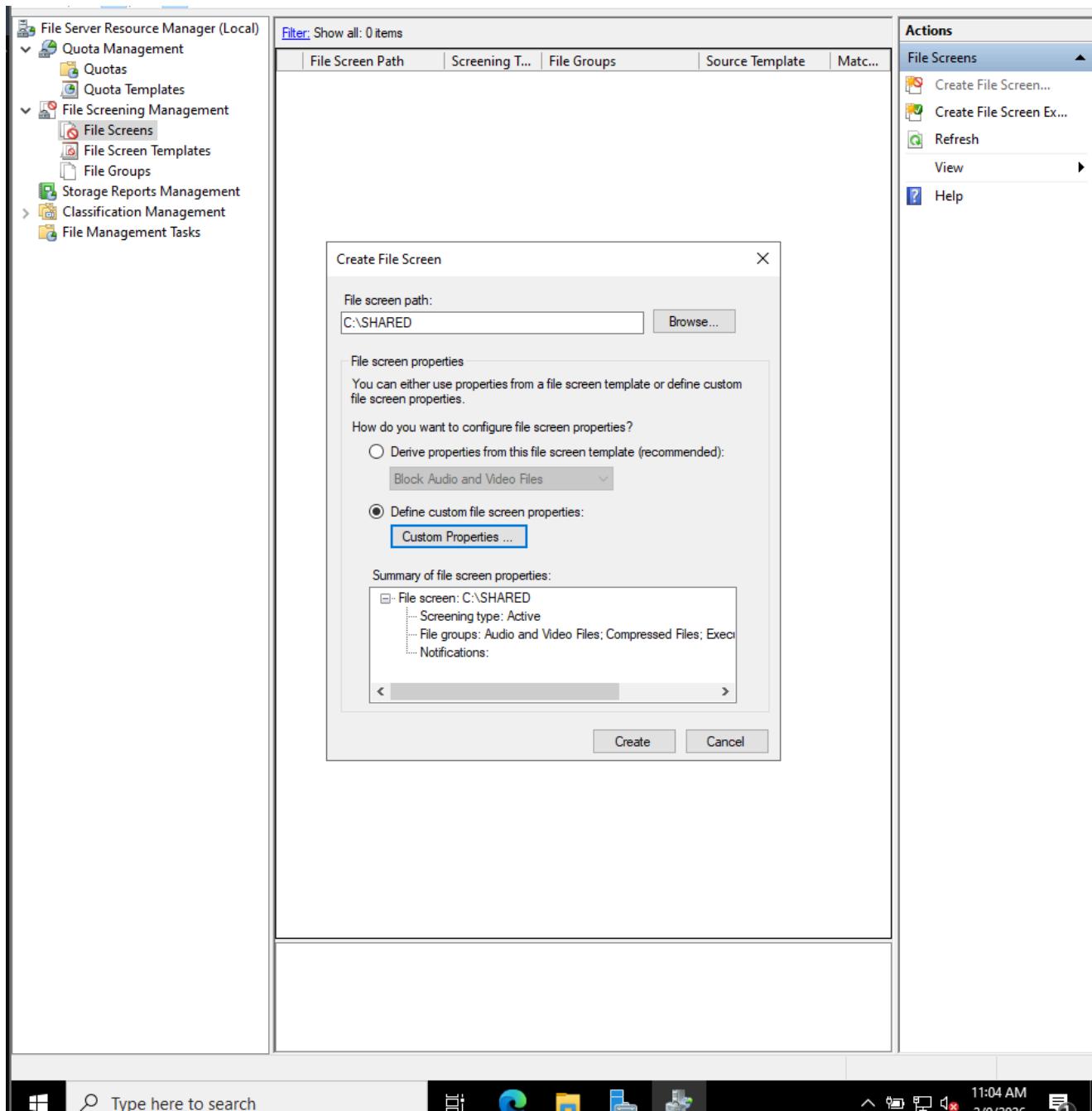
A quota was created for the SHARED folder to limit storage usage. The limit was defined to restrict excessive disk consumption.

The screenshot shows the Windows File Server Resource Manager (Local) interface. The left navigation pane includes links for Quota Management (selected), Quotas, Quota Templates, File Screening Management, Storage Reports Management, Classification Management, and File Management Tasks. The main pane displays the 'Quota Properties of C:\SHARED' dialog box. This dialog includes fields for 'Copy properties from quota template (optional)', 'Quota path' (set to C:\SHARED), 'Description (optional)', 'Space limit' (set to 100.000 MB, Hard quota selected), 'Notification thresholds' (empty table), and a 'Disable quota' checkbox. The right pane shows an 'Actions' menu with options for Quotas (selected), Create Quota..., Refresh, View, and Help.

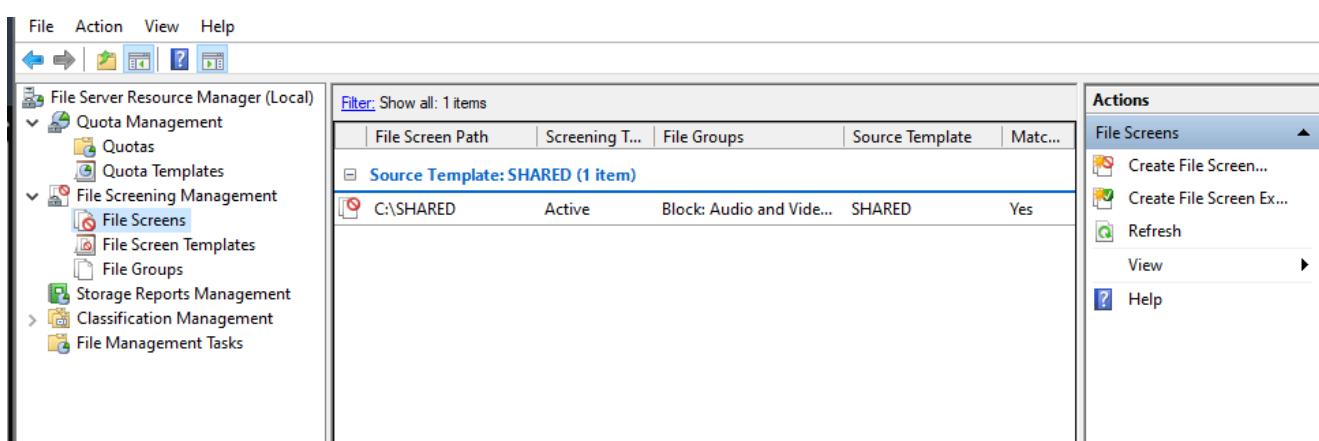
A File Screen was configured on the SHARED folder to block specific file types such as audio and video files. This prevents unauthorized storage of restricted content.



A custom file screen template was applied to the SHARED folder. This enforces file-type restrictions directly on the storage path.



The file screen appears active under the SHARED path, confirming successful configuration.



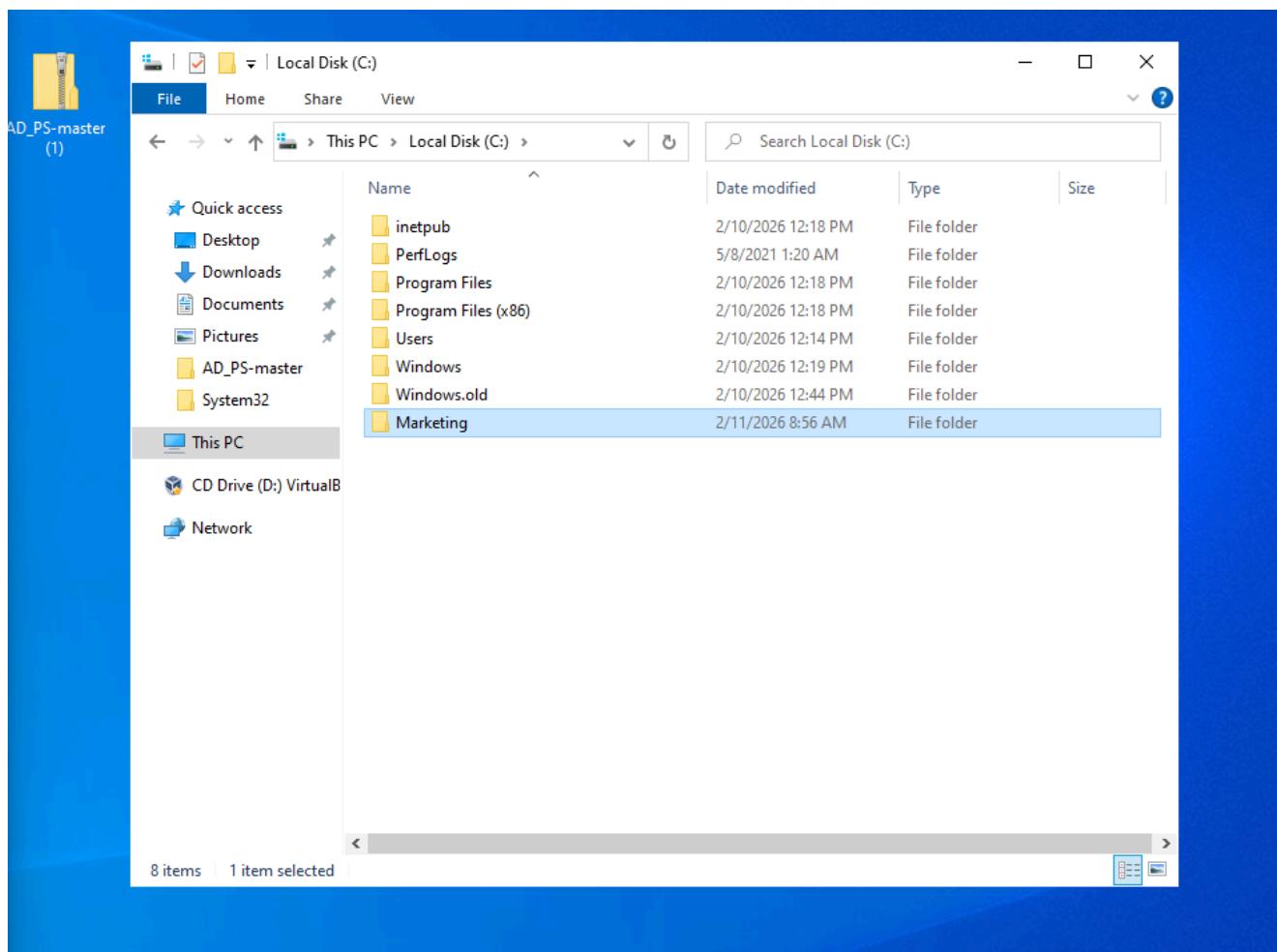
NTFS vs SHARED (HOW TO ASSIGN FOLDER PERMISSIONS) :

Activity 1

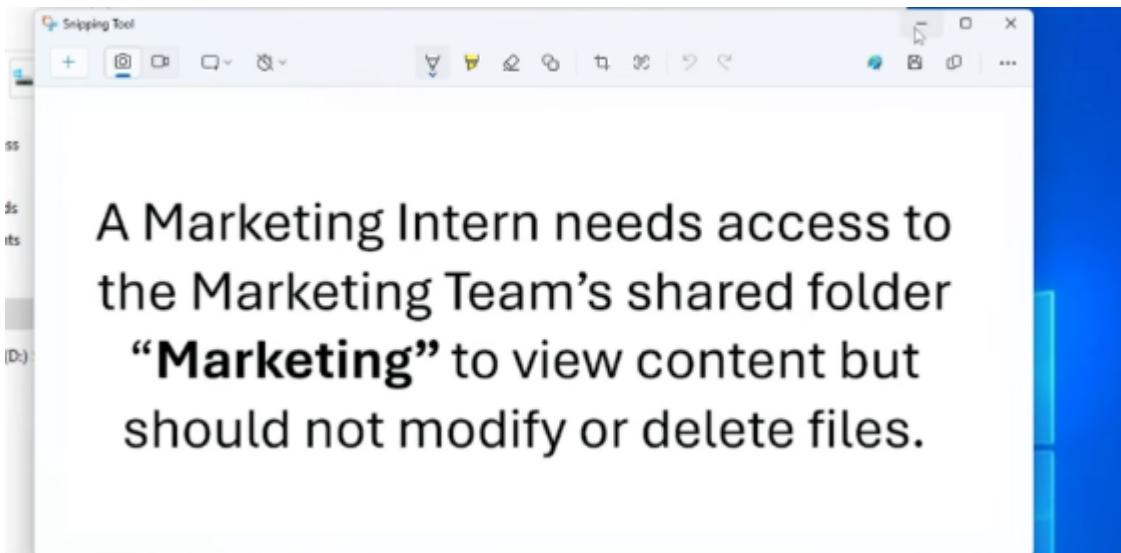


A Marketing Intern needs access to the Marketing Team's shared folder **“Marketing”** to view content but should not modify or delete files.

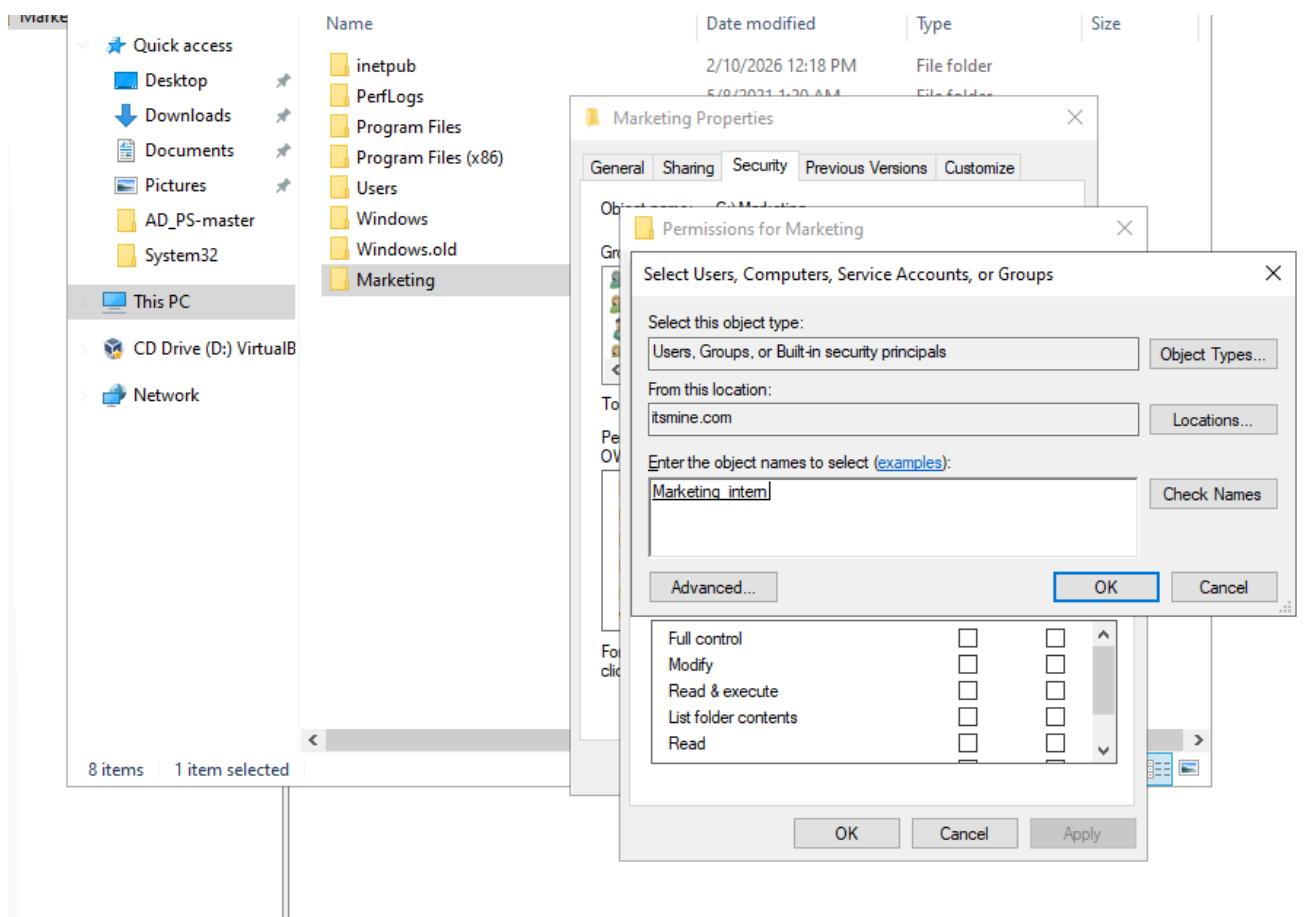
A Marketing folder was created to implement role-based access control for departmental file sharing.



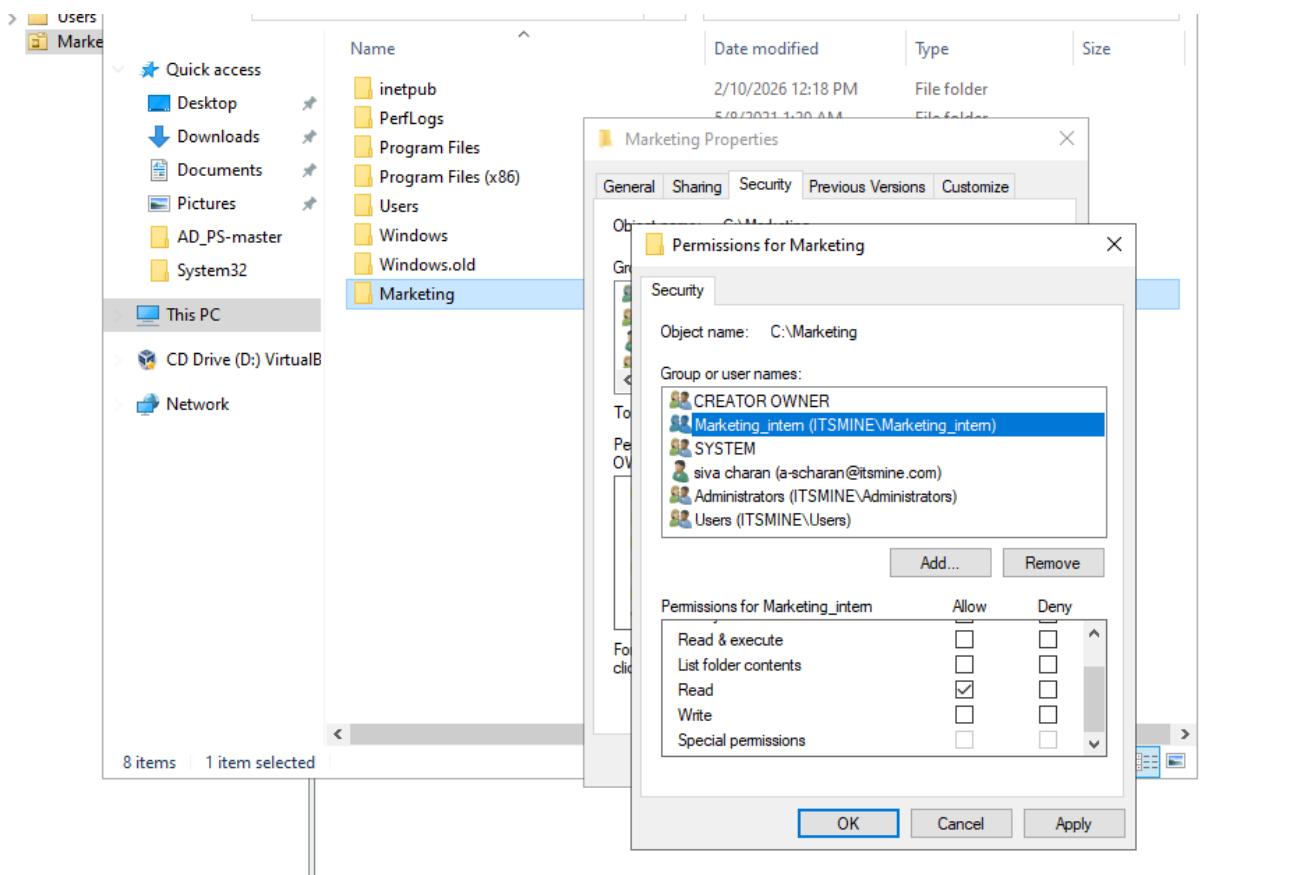
The requirement specifies that the intern should only view content without modification rights.



NTFS permissions were configured to grant Read access only to the Marketing Intern group.



Marketing folder permissions were reviewed to confirm restricted access settings.

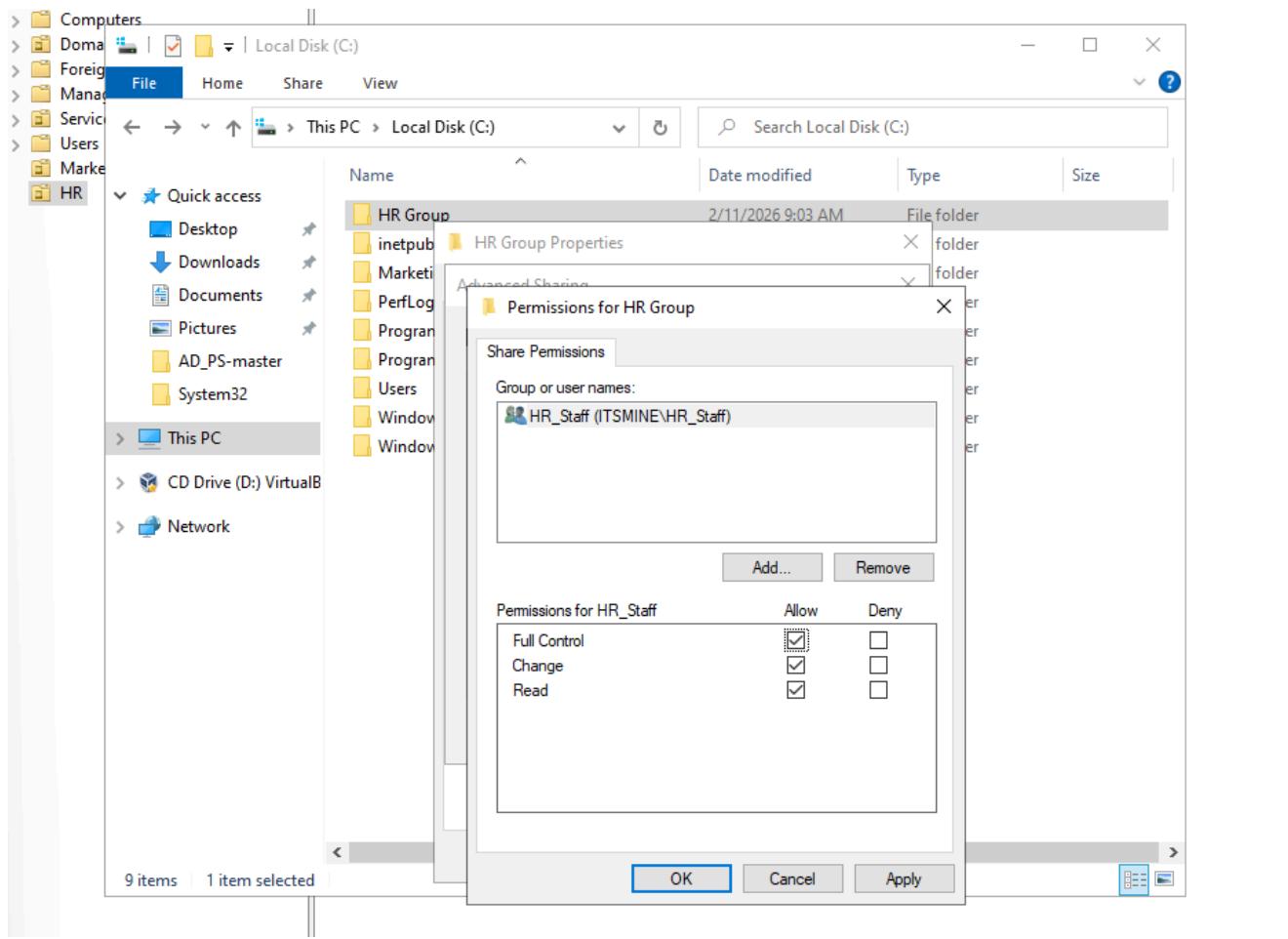


Activity 2

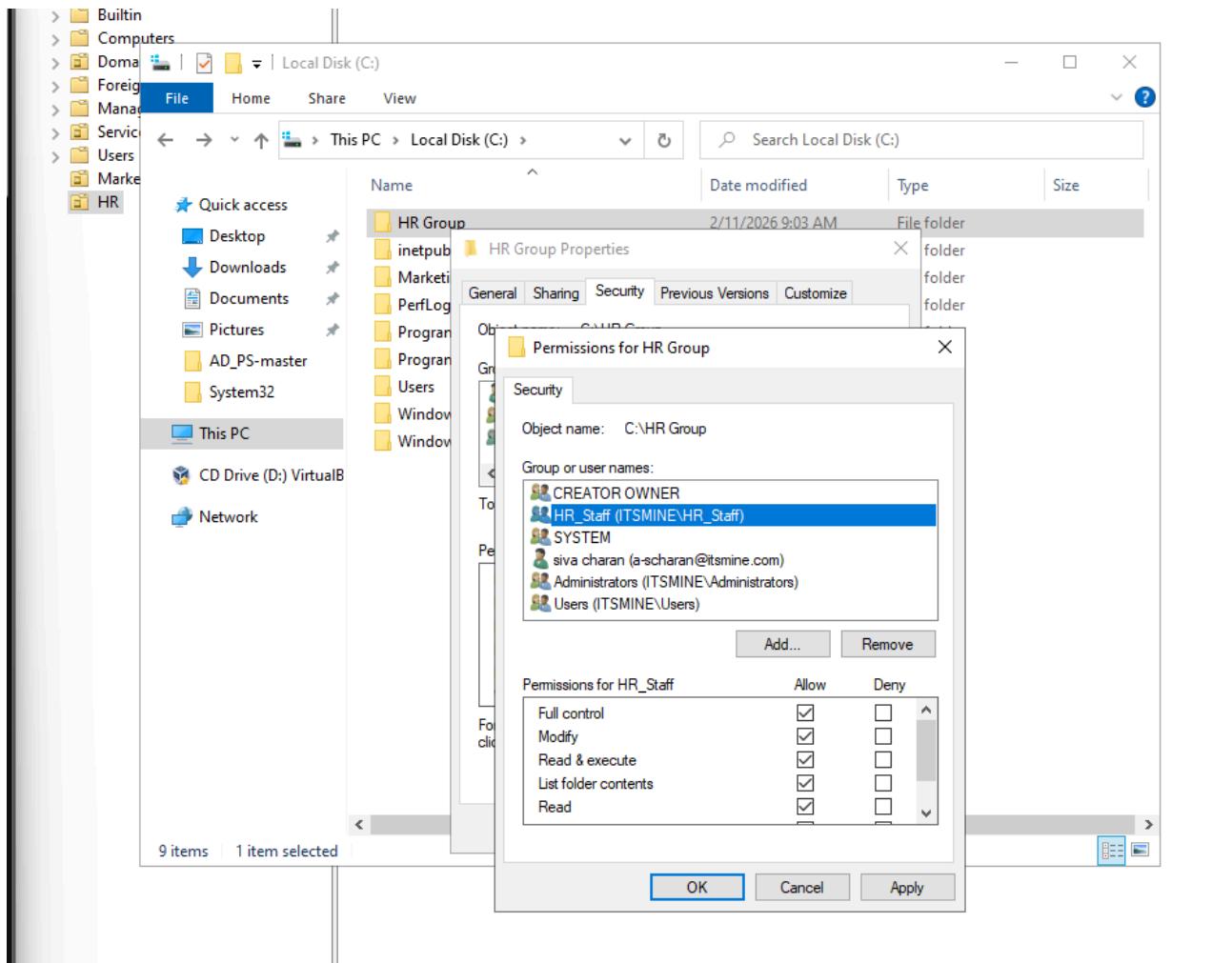


The HR Department needs a secure folder **HRGroup** that only HR staff can access. Other employees should not see the folder at all.

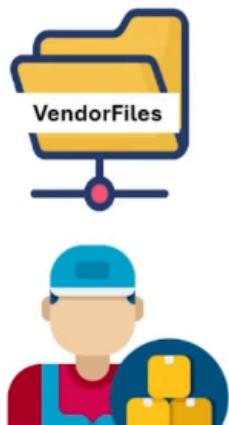
Share permissions were configured to allow access exclusively to the HR Staff group.



NTFS permissions were set to ensure only HR users have full control, while others have no access

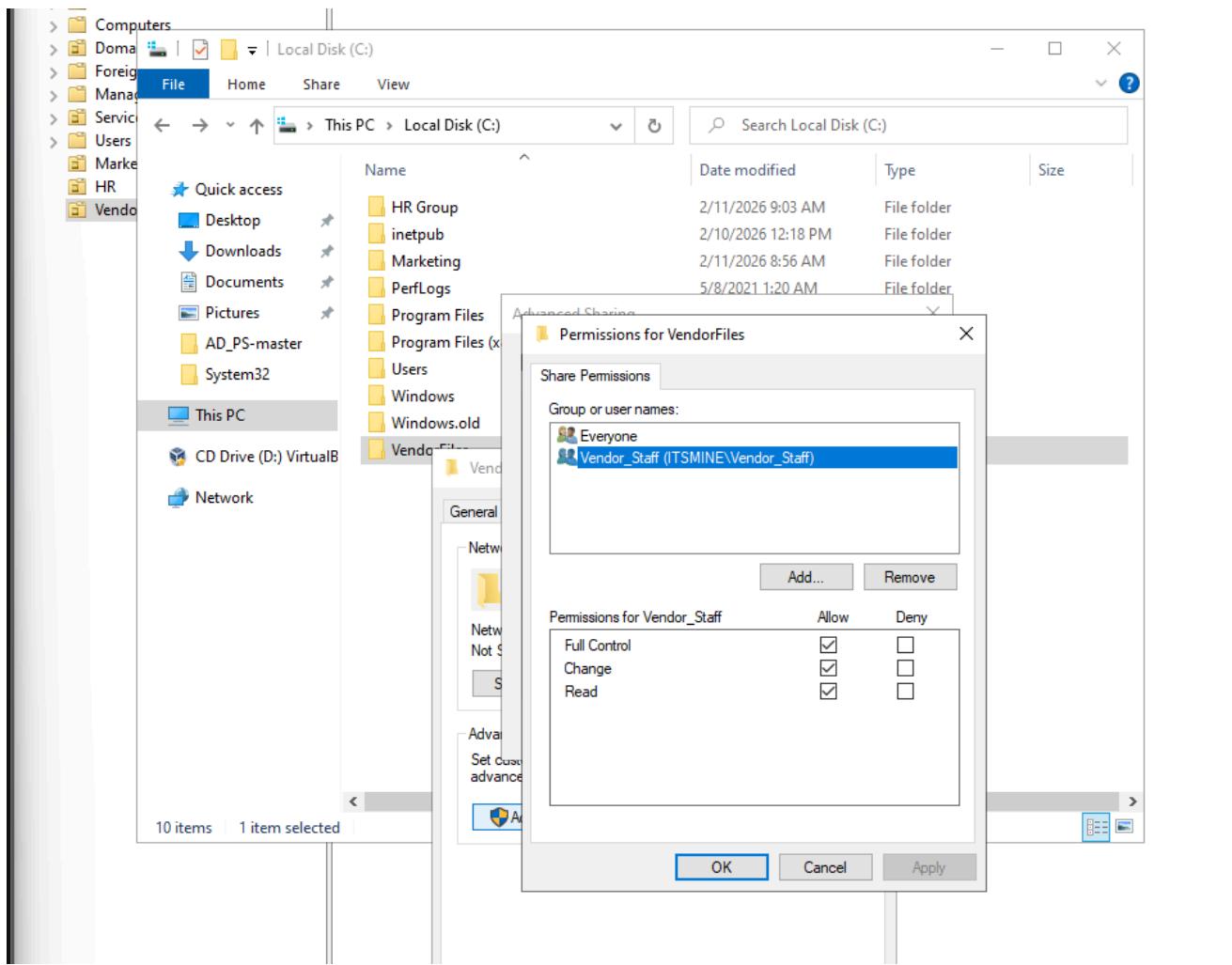


Activity 3

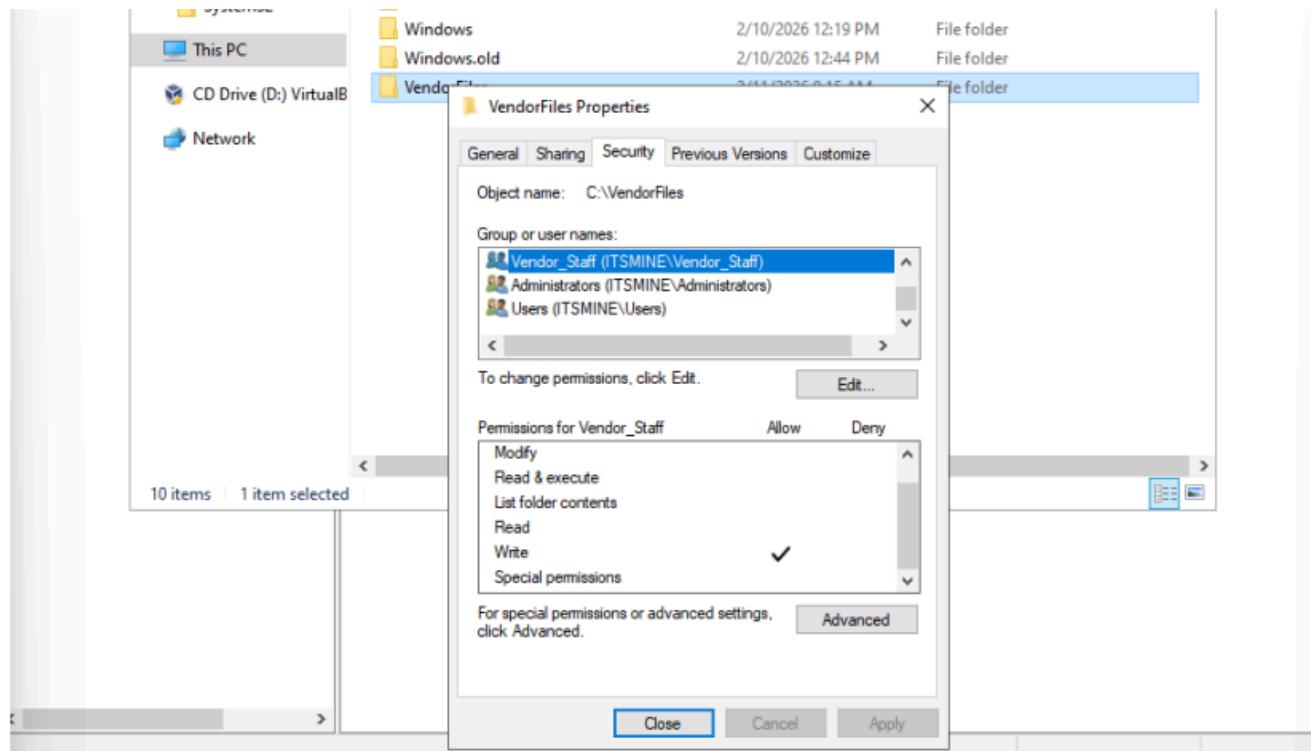


A third-party vendor needs access to a temporary folder **VendorFiles** to upload reports but should not see other files.

Share permissions were configured to allow the Vendor group appropriate access for report uploads.



NTFS permissions were adjusted to allow write access without exposing other sensitive files

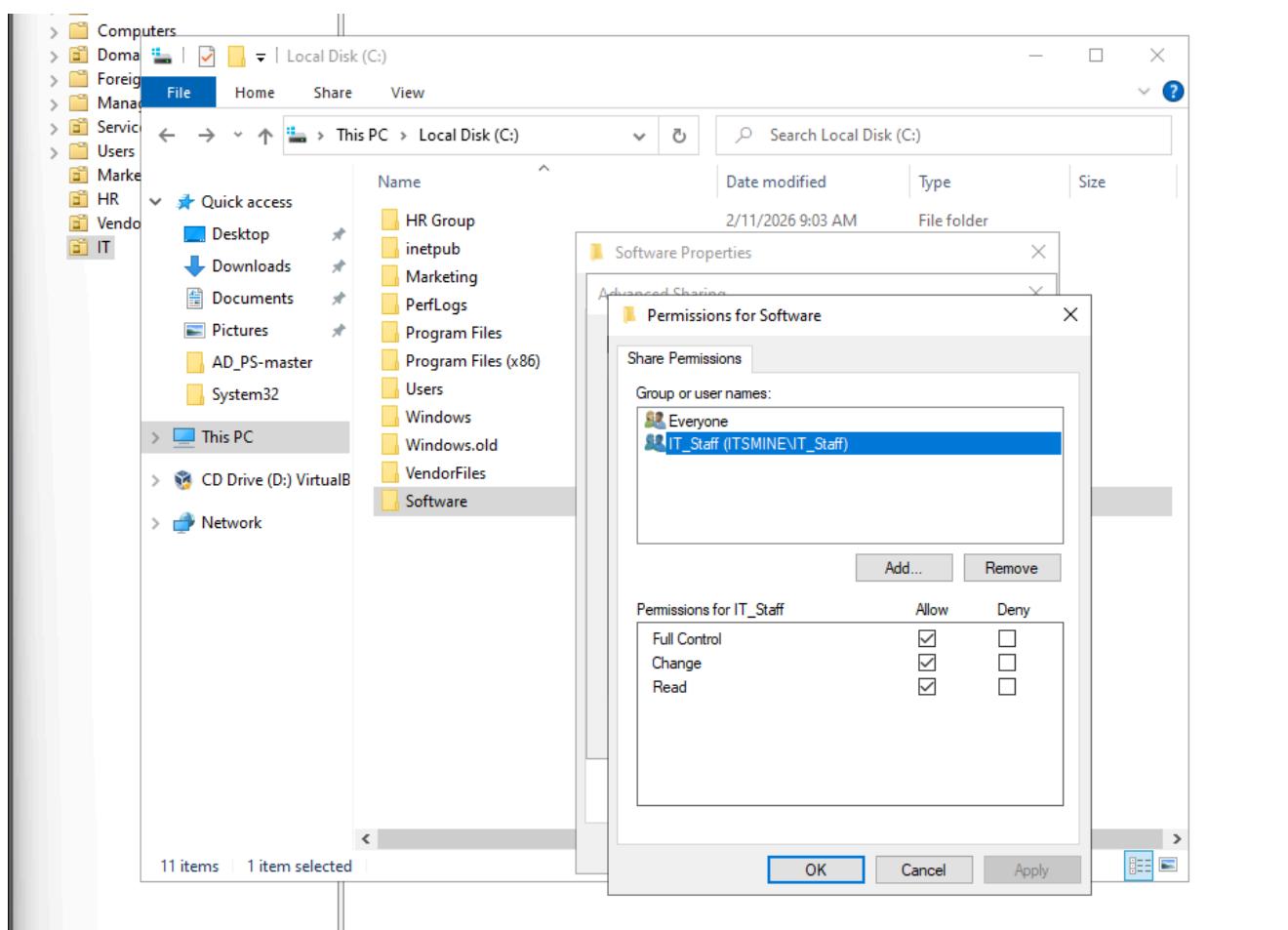


Activity 4

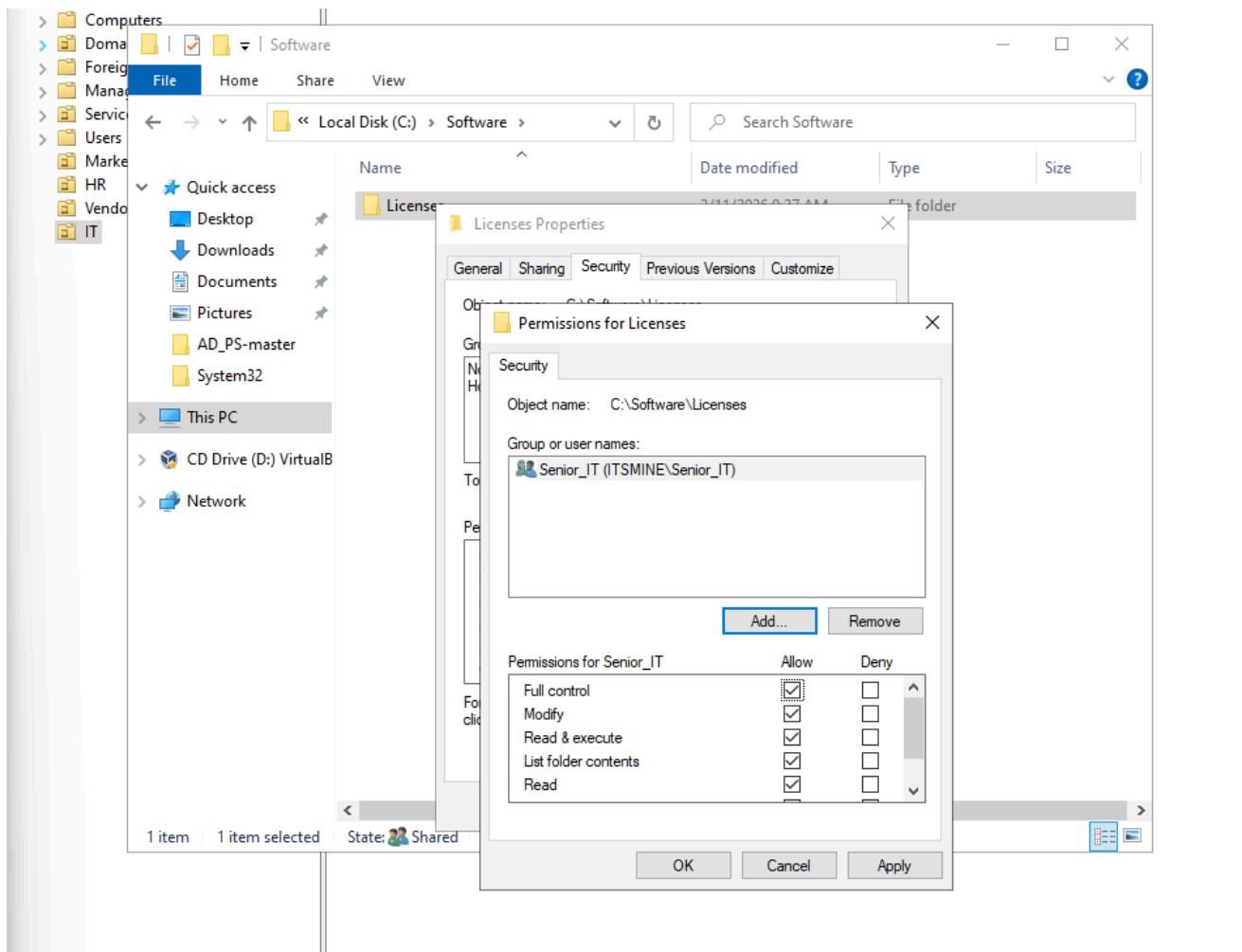


In the IT Department, all techs need access to the Software Repository **Software** but only senior IT staff should be able to access the "Licenses" subfolder

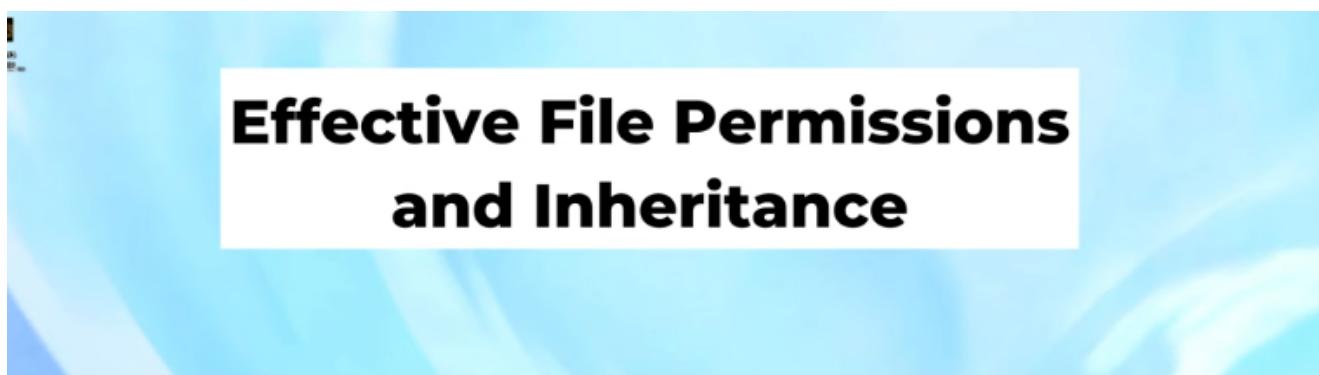
Software repository permissions were configured to allow IT staff access.



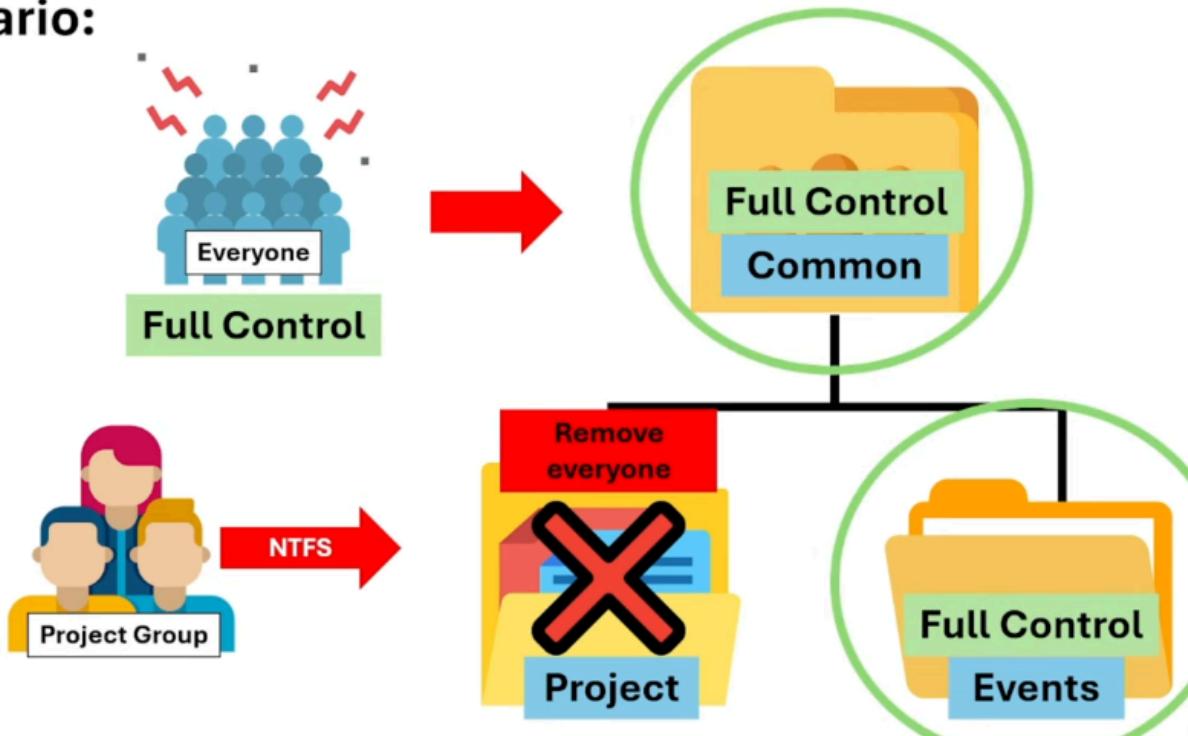
Additional NTFS restrictions were applied so that only Senior IT staff can access the Licenses folder.



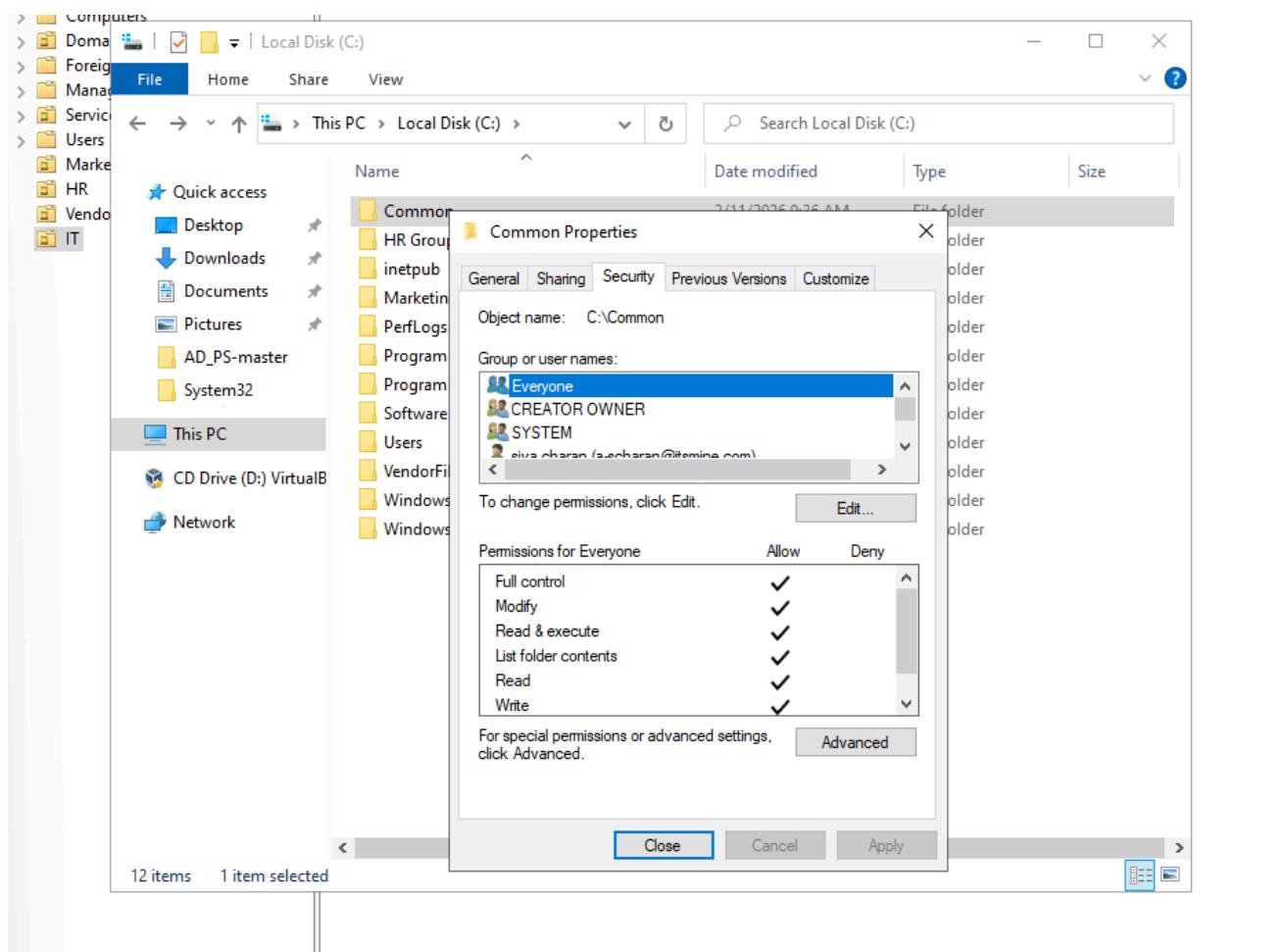
EFFECTIVE FILE PERMISSION AND INHERITANCE :



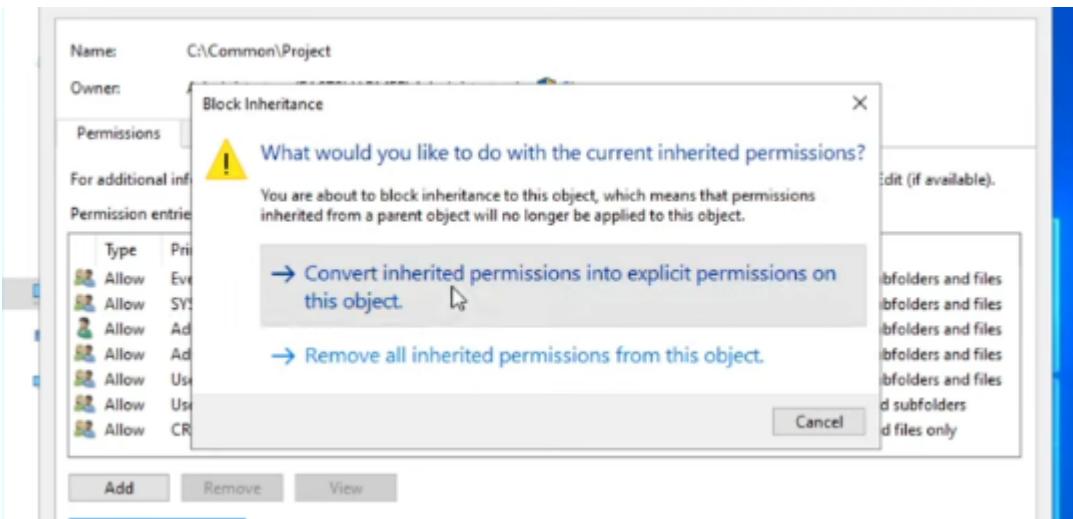
Scenario:



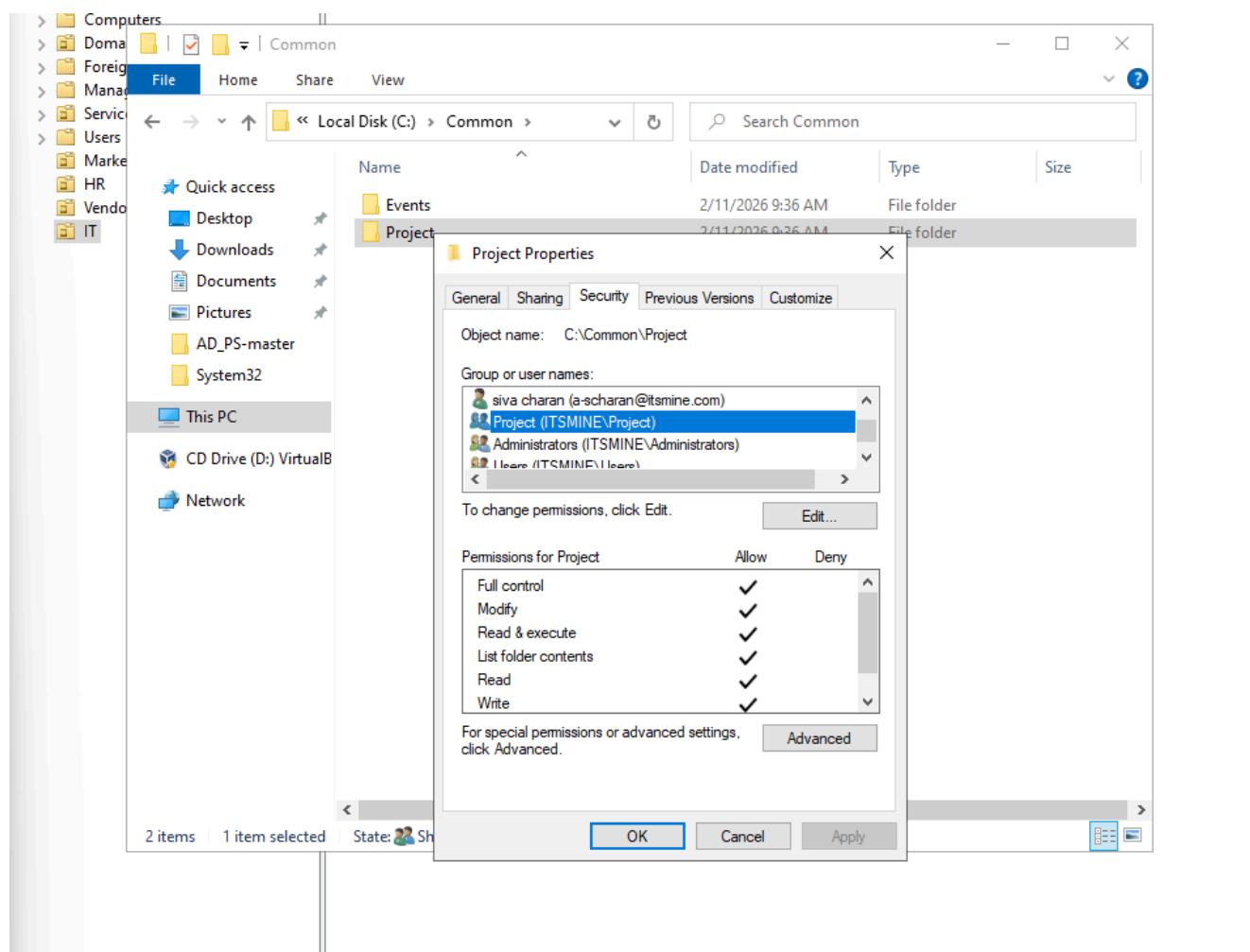
Permissions for the Common folder were reviewed to analyze inherited access entries.



Inheritance was blocked on a subfolder to convert inherited permissions into explicit permissions. This allows fine-grained control over folder access.



Permissions for the Project folder were configured to control access at a granular level. Specific users and groups were assigned appropriate rights to manage folder security.



SCENARIO

Effective Permissions and Inheritance for File Permissions

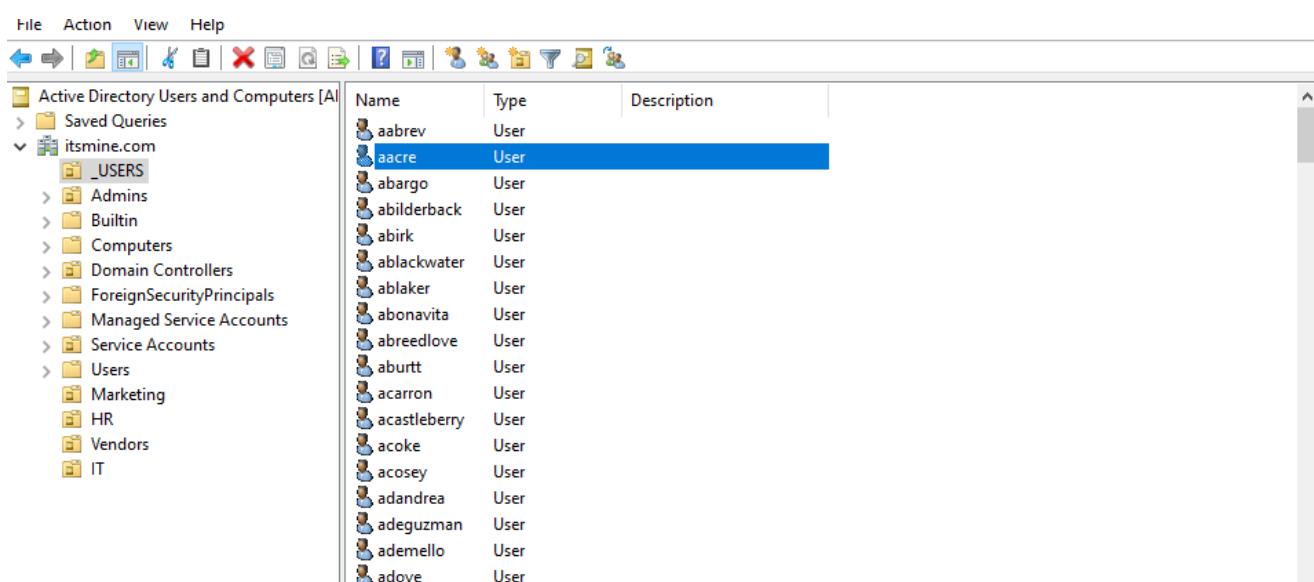
Explicit Deny



**Deny
Confidential
Folder**

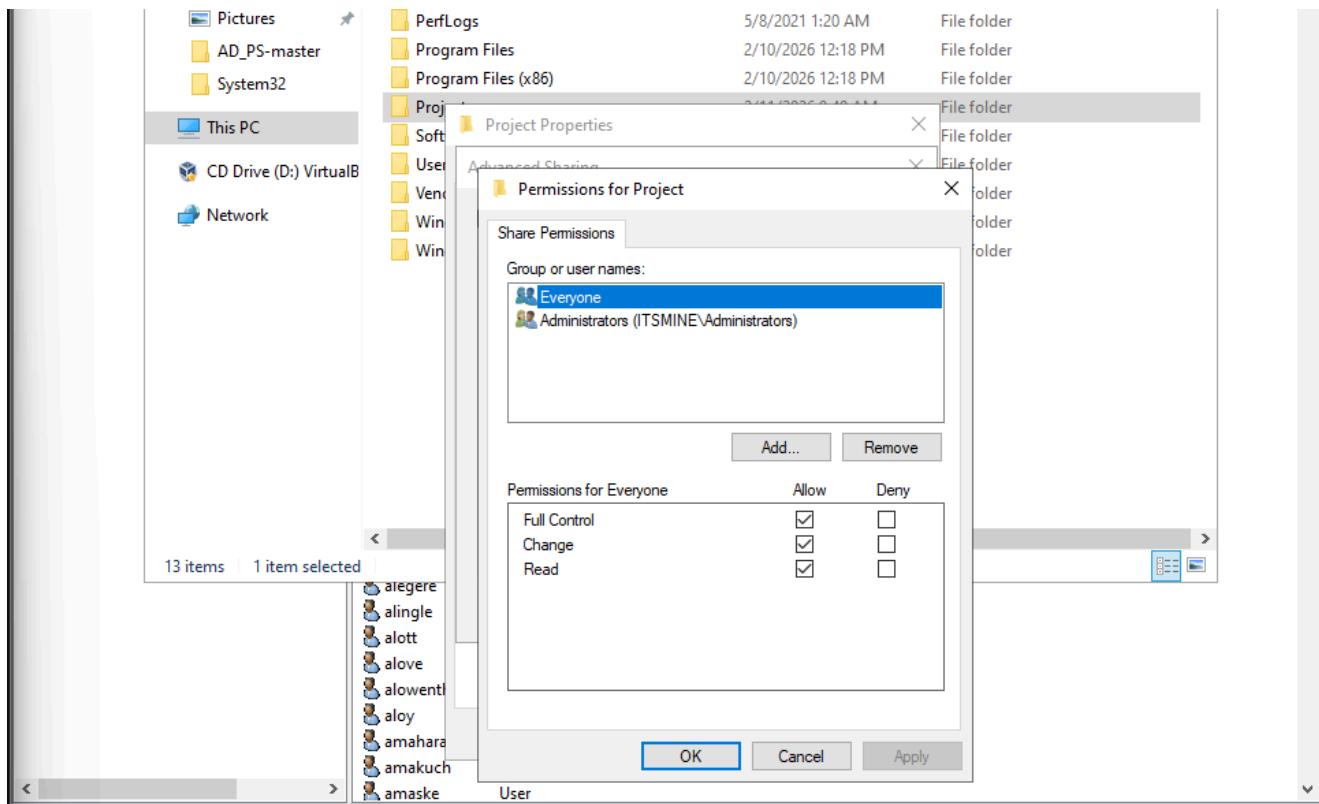


User accounts were reviewed in Active Directory to identify members involved in the permission configuration.

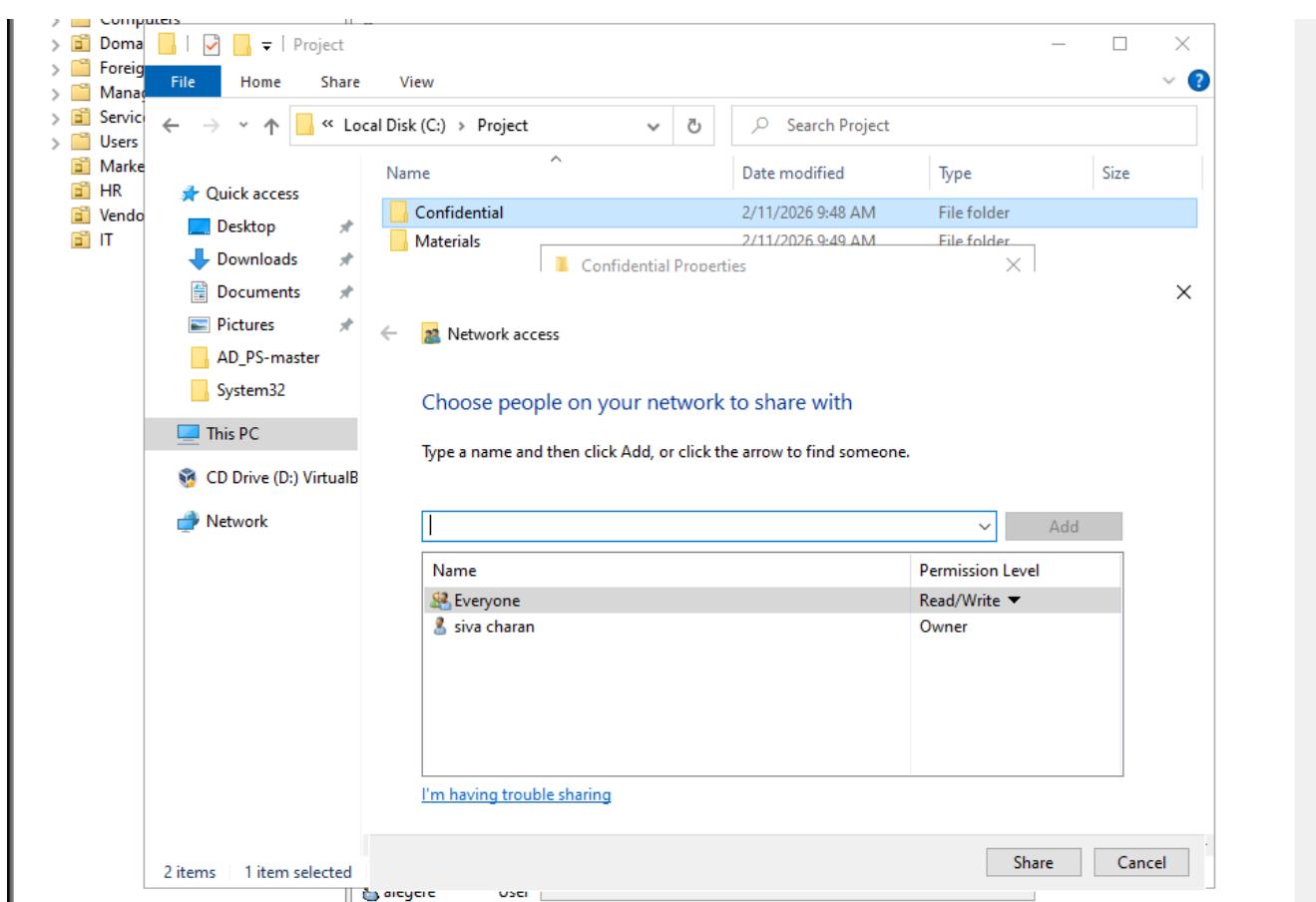


Name	Type
aabrev	User
aacre	User
abargo	User
abildeback	User
abirk	User
ablackwater	User
ablaker	User
abonavita	User
abreedlove	User
aburtt	User
acarron	User
acastleberry	User
acoke	User
acosey	User
adandrea	User
adeguzman	User
ademello	User
adove	User

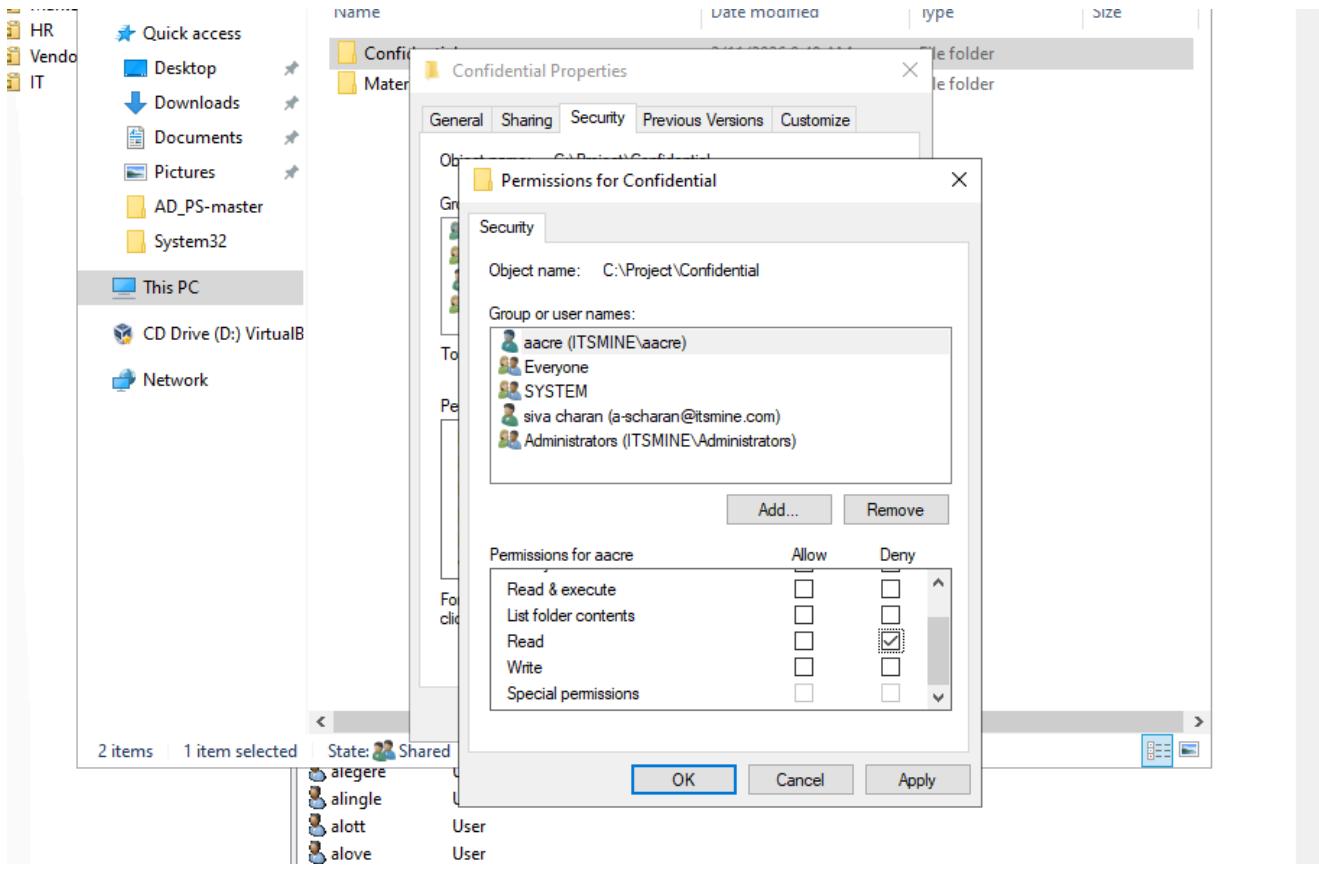
Share permissions were configured to define network-level access to the Project folder. Access was restricted based on defined user groups.



The Confidential subfolder was configured with restricted sharing settings to limit access to authorized users only.



NTFS permissions were adjusted to remove unnecessary access and ensure only specific users could read or modify content.



ACCESS BASED ENUMERATION :



Access- Based Enumeration (ABE)

User membership in the Senior_IT group was verified to ensure correct access assignment

The screenshot shows the Active Directory Users and Computers interface. On the left, the navigation pane lists various objects like Saved Queries, itsmine.com, and IT. The IT folder is expanded, showing sub-folders such as _USERS, Admins, Builtin, Computers, Domain Controllers, ForeignSecurityPrincipals, Managed Service Accounts, Service Accounts, Users, Marketing, HR, Vendors, and IT. The 'IT' folder is selected. On the right, a list of security groups is displayed:

Name	Type	Description
IT_Staff	Security Group...	
k naga	User	
Project	Security Group...	
Senior_IT	Security Group...	

A detailed view of the 'Senior_IT' security group is shown in a modal window titled 'Senior_IT Properties'. The 'Members' tab is selected, displaying the following members:

Name	Description
k naga	itsmine.com/IT

Buttons at the bottom of the modal include 'Add...', 'Remove', 'OK', 'Cancel', and 'Apply'.

The Senior_HR security group was reviewed and validated for correct user membership.

The screenshot shows the Active Directory Users and Computers interface. The navigation pane is identical to the previous one, with the 'IT' folder selected. On the right, a list of security groups is displayed:

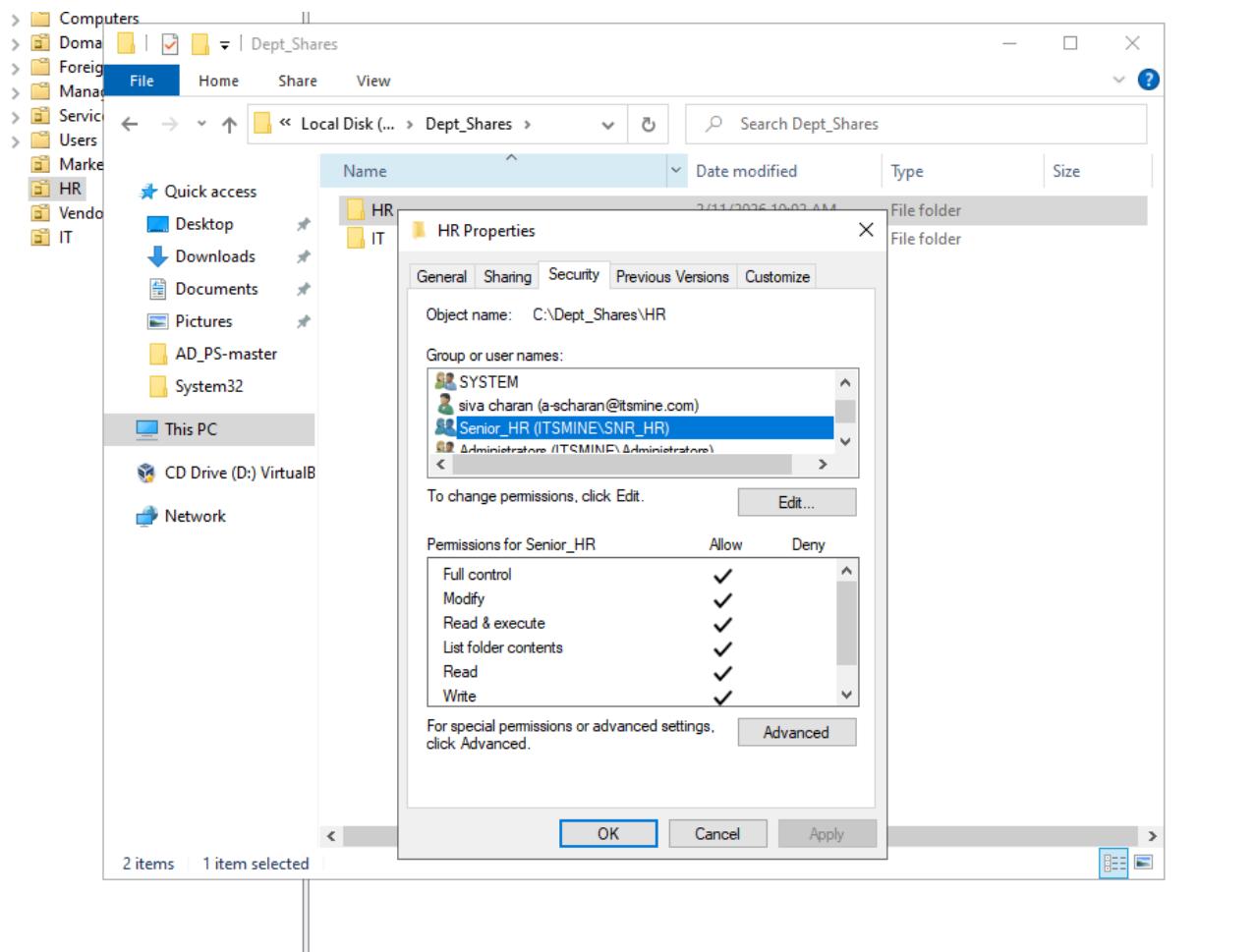
Name	Type	Description
HR_Staff	Security Group...	
Senior_HR	Security Group...	
u bavesh	User	

A detailed view of the 'Senior_HR' security group is shown in a modal window titled 'Senior_HR Properties'. The 'Members' tab is selected, displaying the following members:

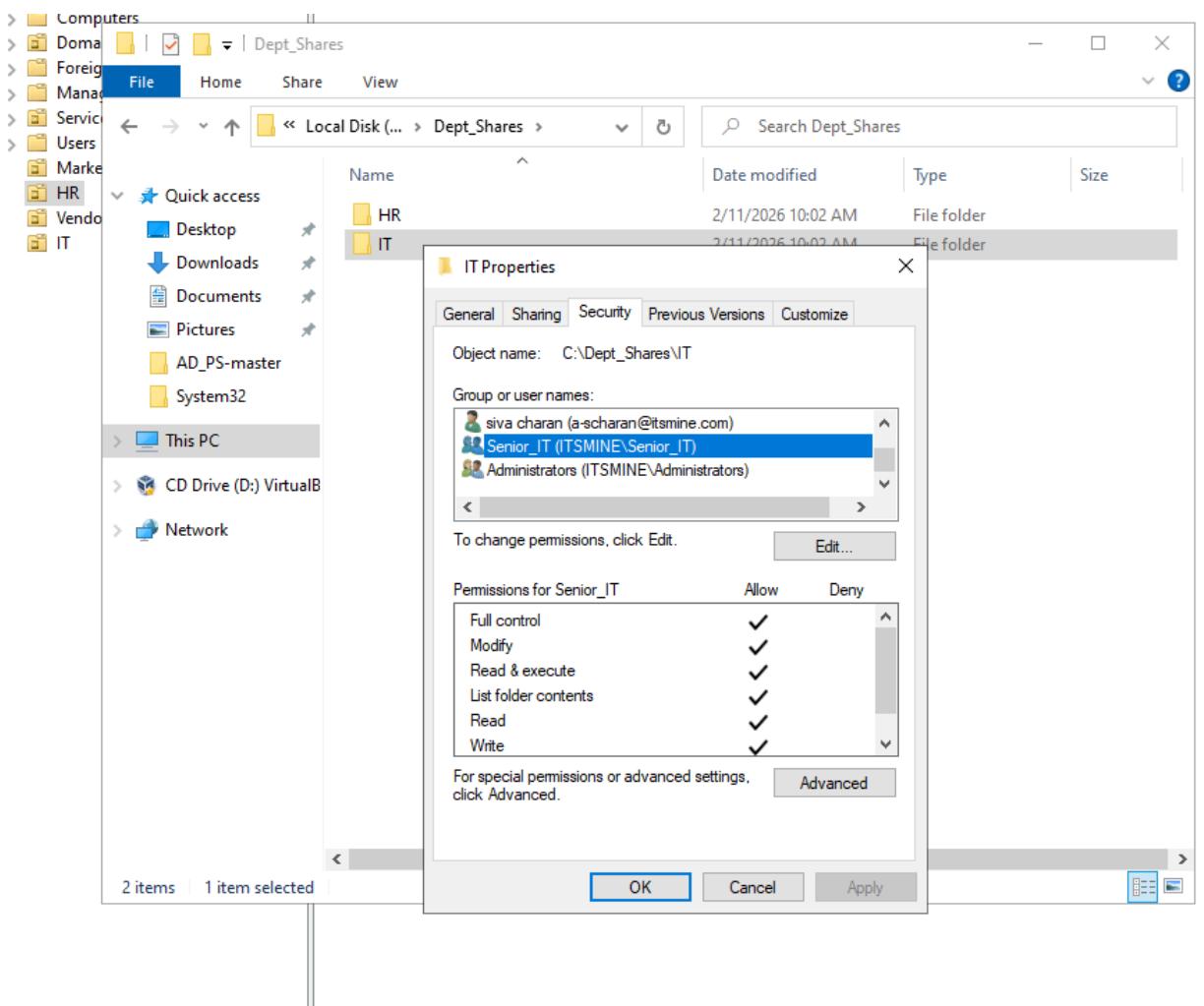
Name	Description
u bavesh	itsmine.com/HR

Buttons at the bottom of the modal include 'Add...', 'Remove', 'OK', 'Cancel', and 'Apply'.

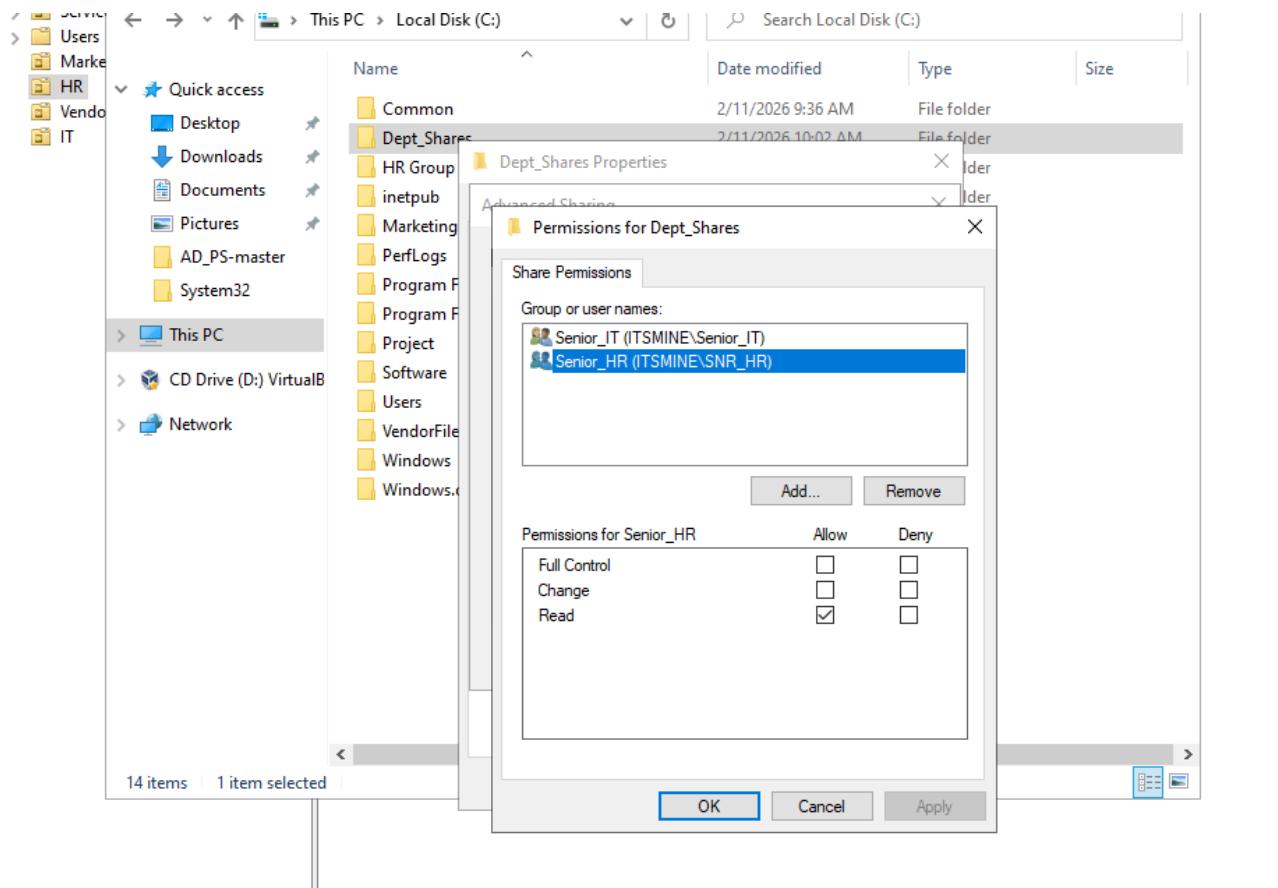
Permissions for the HR folder were configured to allow access only to authorized HR staff members.



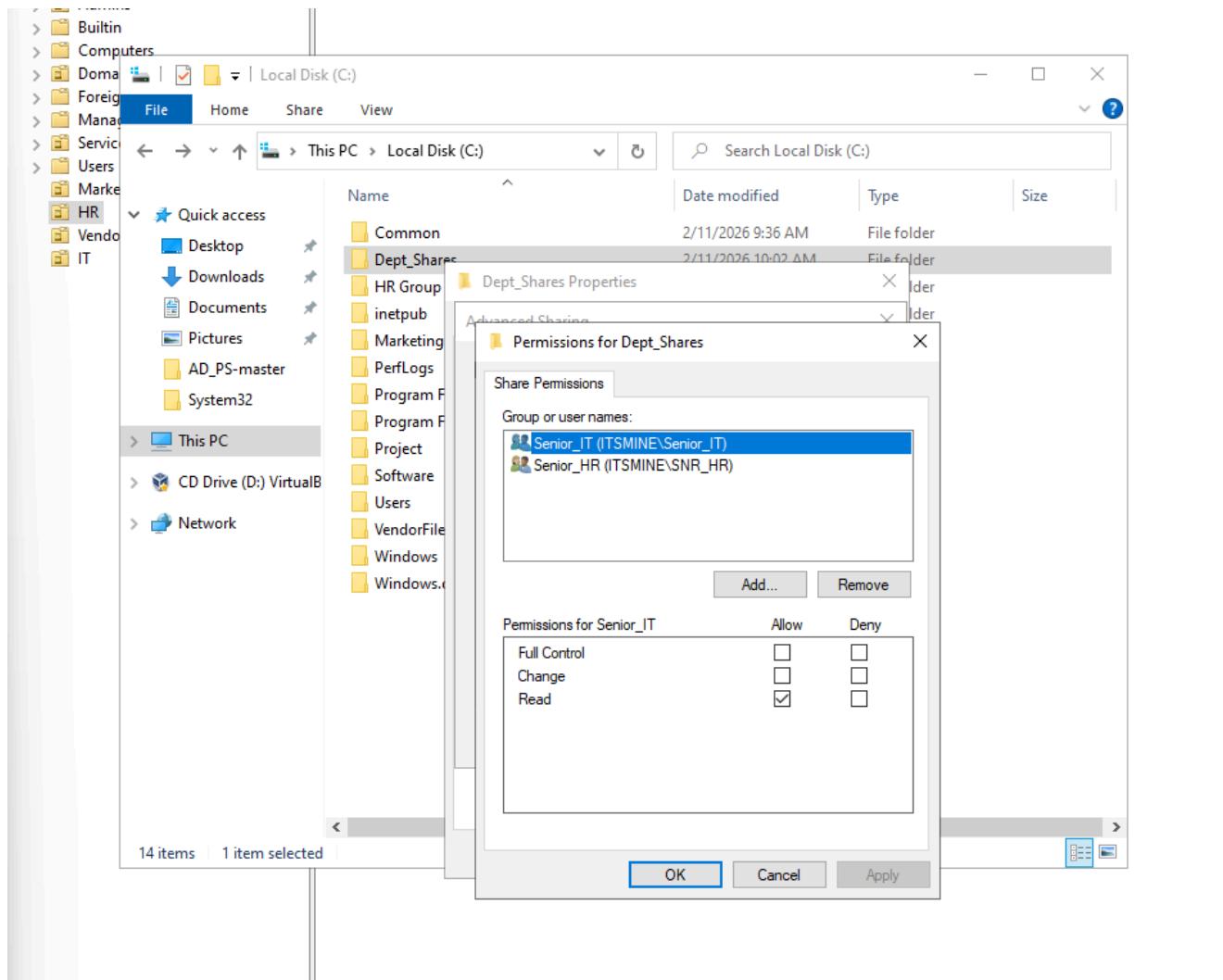
NTFS permissions were configured for the IT folder to grant access only to designated IT users.



Share permissions for Dept_Shares were defined to restrict access based on group roles.



Specific security groups such as Senior_IT and Senior_HR were granted controlled access to the shared folder.



Access-Based Enumeration was enabled in the share settings. This ensures users can only see folders for which they have permissions.

The screenshot shows the Windows Server File and Storage Services interface. On the left, a navigation pane lists: Servers, Volumes, Disks, Storage Pools, Shares (selected), iSCSI, Work Folders. The main area has two tabs: SHARES and VOLUME.

SHARES Tab:

- Header: SHARES, All shares | 9 total, TASKS
- Table:
 - Share: AD-DC (9)
 - Common: C:\Common
 - Dept_Shares**: C:\Dept_Shares (selected)
 - HR Group: C:\HR Group

VOLUME Tab:

- Header: VOLUME, Dept_Shares on AD-DC, TASKS
- (C): Capacity: 19.9 GB
- 67.4% Used: 13.4 GB Used Space, 6.49 GB Free Space

Dept_Shares Properties Dialog:

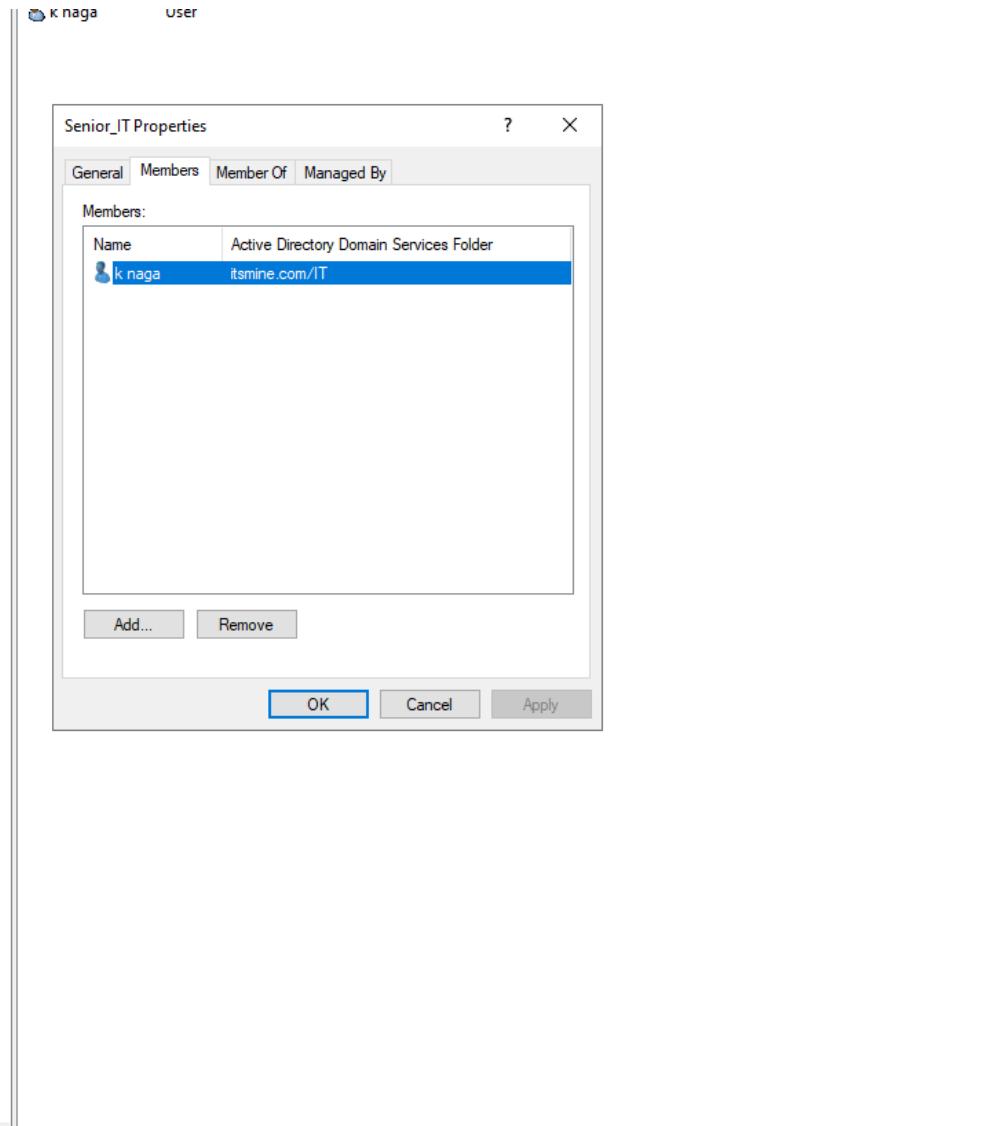
- Title: Dept_Shares Properties
- General Settings:
 - Show All
 - General
 - Permissions
 - Settings** (selected)
- Settings:
 - Enable access-based enumeration
 - Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.
 - Allow caching of share
 - Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.
 - Enable BranchCache on the file share
 - BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.
 - Encrypt data access
 - When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.

Buttons: OK, Cancel, Apply

Last refreshed on 2/11/2026 10:10:31 AM

Group membership for Senior_IT was reviewed again to confirm access-based filtering will apply correctly.

- > Builtin
- > Computers
- > Domain Controllers
- > ForeignSecurityPrincipals
- > Managed Service Accounts
- > Service Accounts
- > Users
 - Marketing
 - HR
 - Vendors
 - IT



Senior_HR group membership was verified to ensure only authorized HR personnel can access restricted folders.

File Action View Help

Active Directory Users and Computers [AI]

Saved Queries

itsmine.com

- _USERS
- Admins
- Builtin
- Computers
- Domain Controllers
- ForeignSecurityPrincipals
- Managed Service Accounts
- Service Accounts
- Users
- Marketing
- HR
- Vendors
- IT

Name	Type	Description
HR_Staff	Security Group...	
Senior_HR	Security Group...	
u bavesh	User	

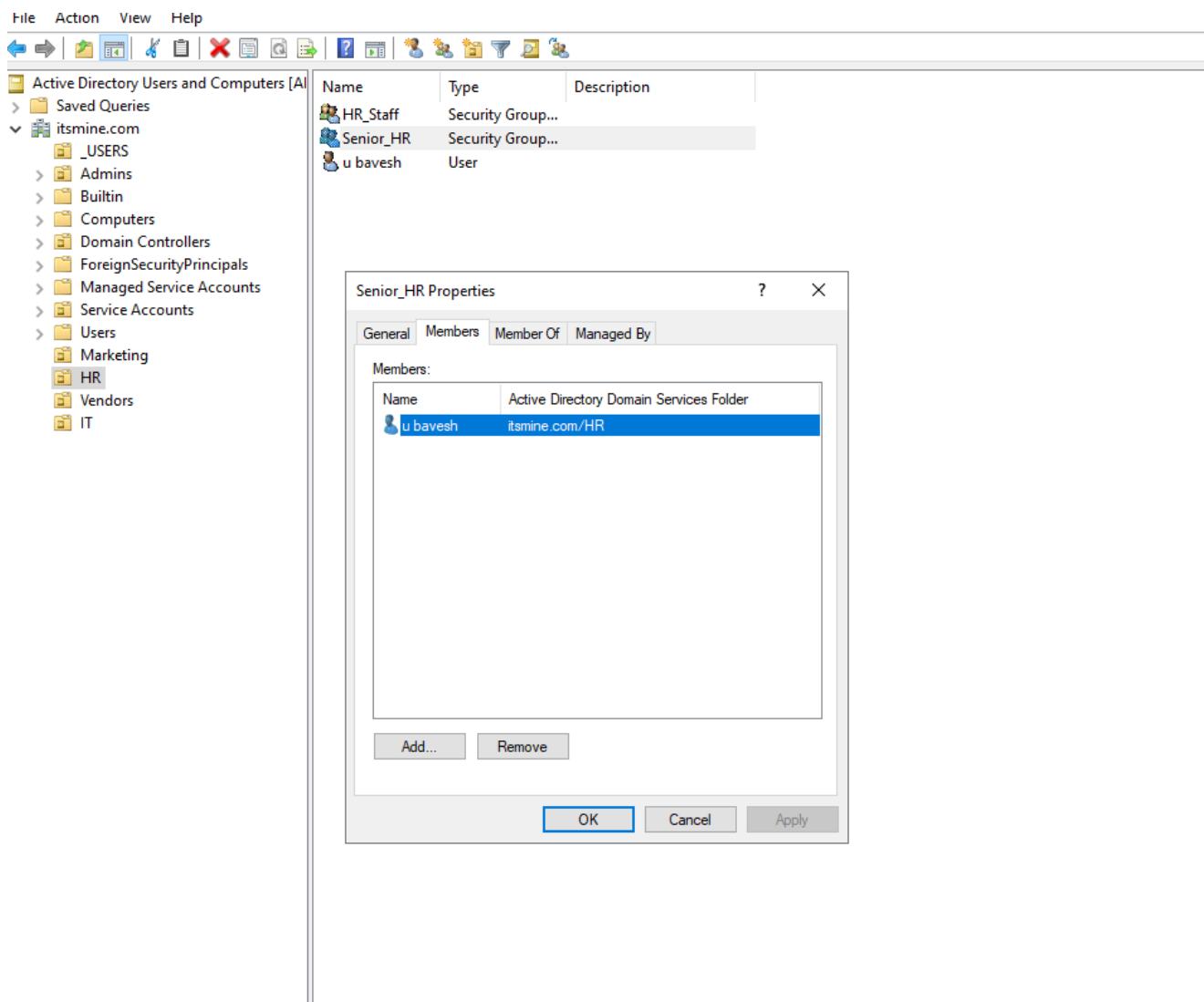
Senior_HR Properties

General Members Member Of Managed By

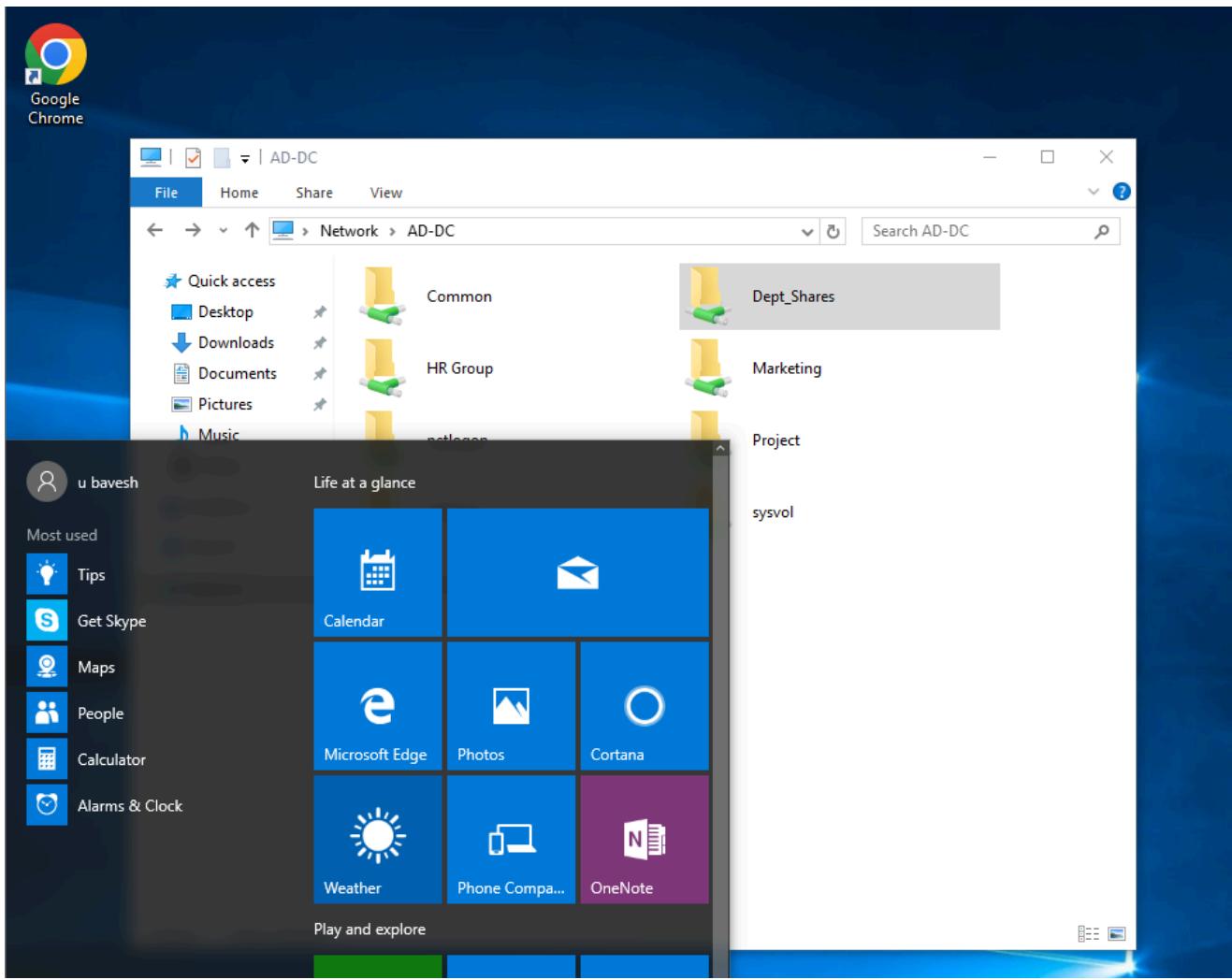
Members:

Name	Active Directory Domain Services Folder
u bavesh	itsmine.com/HR

Add... Remove OK Cancel Apply

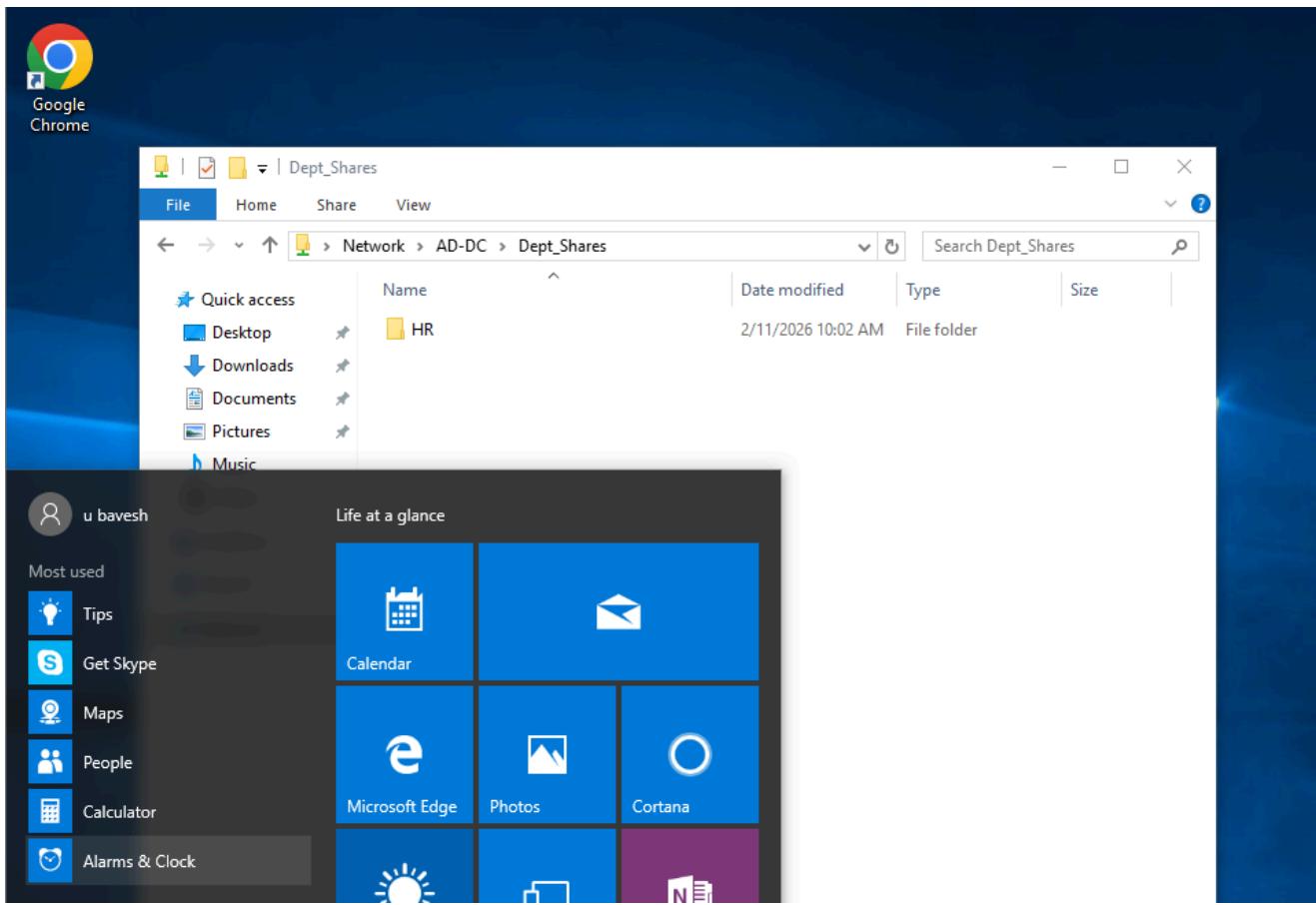


When logged in as an HR user, only permitted folders such as HR-related shares are visible.

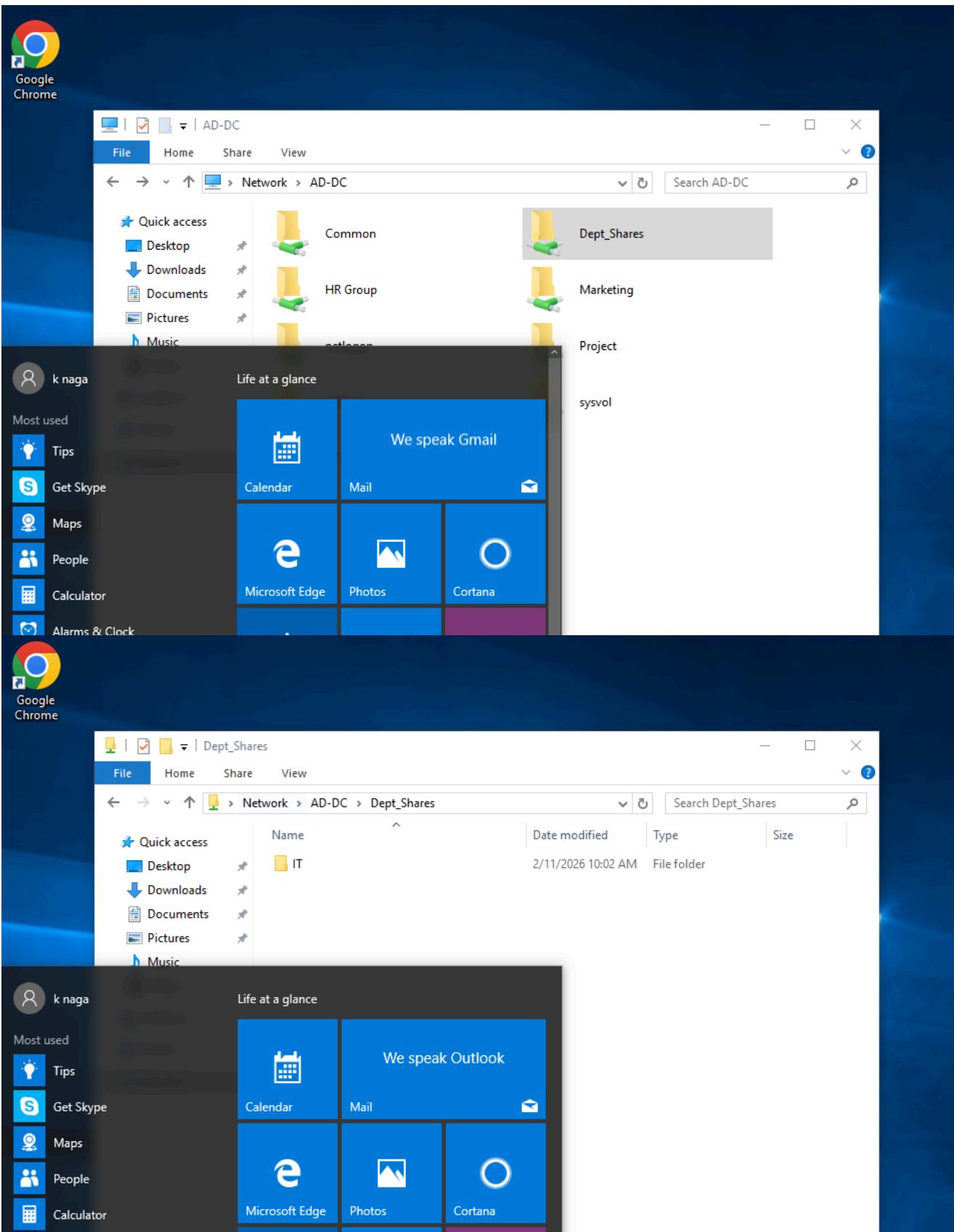


The Dept_Shares folder shows only the subfolders allowed for the logged-in user, confirming ABE functionality.

Restricted folders are hidden from users without permissions, validating ABE enforcement.



An IT user login confirms access to IT-related folders while others remain hidden.



SERVICE ACCOUNT :

The next activity introduces implementing a service account on a single-purpose computer. A configuration plan was defined for setting up a system that auto-logs in using a service account.

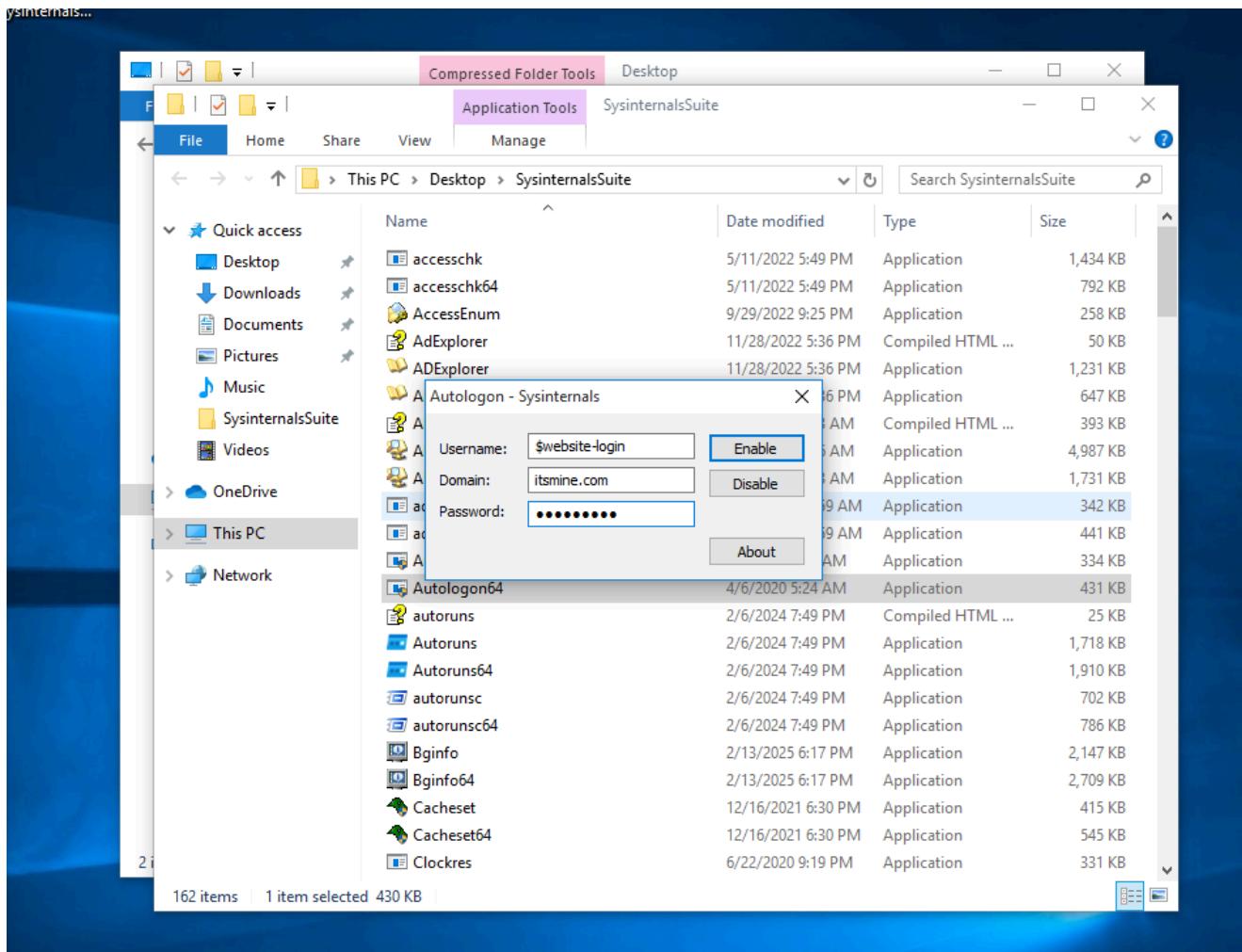
A dedicated service account (Website Login) was created in Active Directory for automated login usage.

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, the navigation pane displays the tree structure of the domain: Active Directory Users and Computers > Saved Queries > itsmine.com > _USERS > Admins > Builtin > Computers > Domain Controllers > ForeignSecurityPrincipal > Managed Service Accounts > Users > COM > Service Accounts. A new entry, "Website Login", has been added under the "Service Accounts" folder. The main pane shows a table with columns: Name, Type, and Description. The "Website Login" entry is listed with a User type and no description.

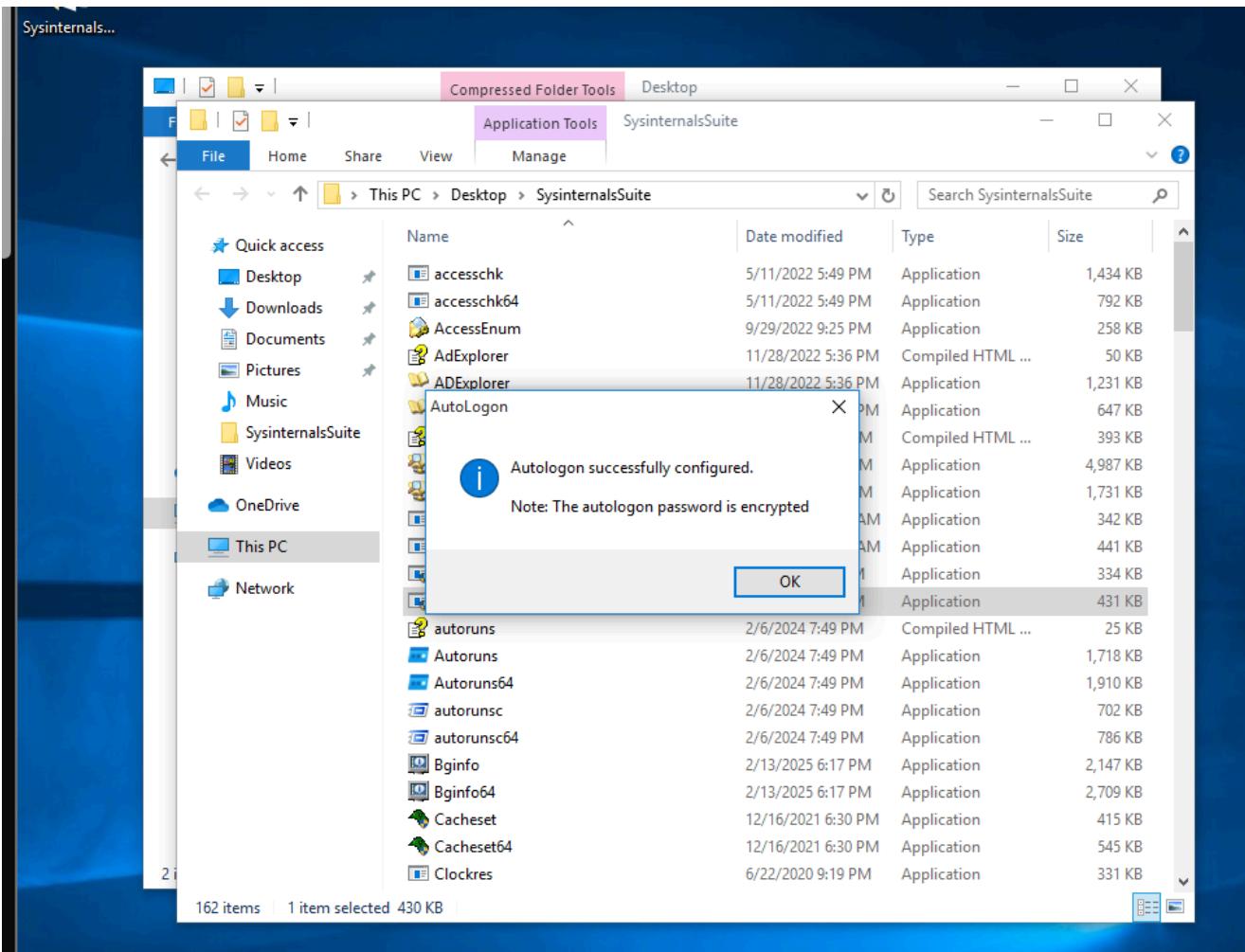
The service account properties were configured to prevent password expiration and allow automated login functionality.

The screenshot shows the "Website Login Properties" dialog box overlaid on the Active Directory Users and Computers window. In the dialog box, the "General" tab is selected. The "User logon name:" field contains "\$website-login" and the "Domain" dropdown shows "@itsmine.com". The "User logon name (pre-Windows 2000):" field contains "ITSMINE\" and the "Logon Name" dropdown shows "\$website-login". The "Unlock account" checkbox is checked. Under "Account options:", the "Password never expires" checkbox is checked, while "User must change password at next logon", "User cannot change password", and "Store password using reversible encryption" are unchecked. Under "Account expires:", the "Never" radio button is selected. At the bottom, there are "OK", "Cancel", "Apply", and "Help" buttons.

The Autologon tool was configured with service account credentials to enable automatic login on system startup.



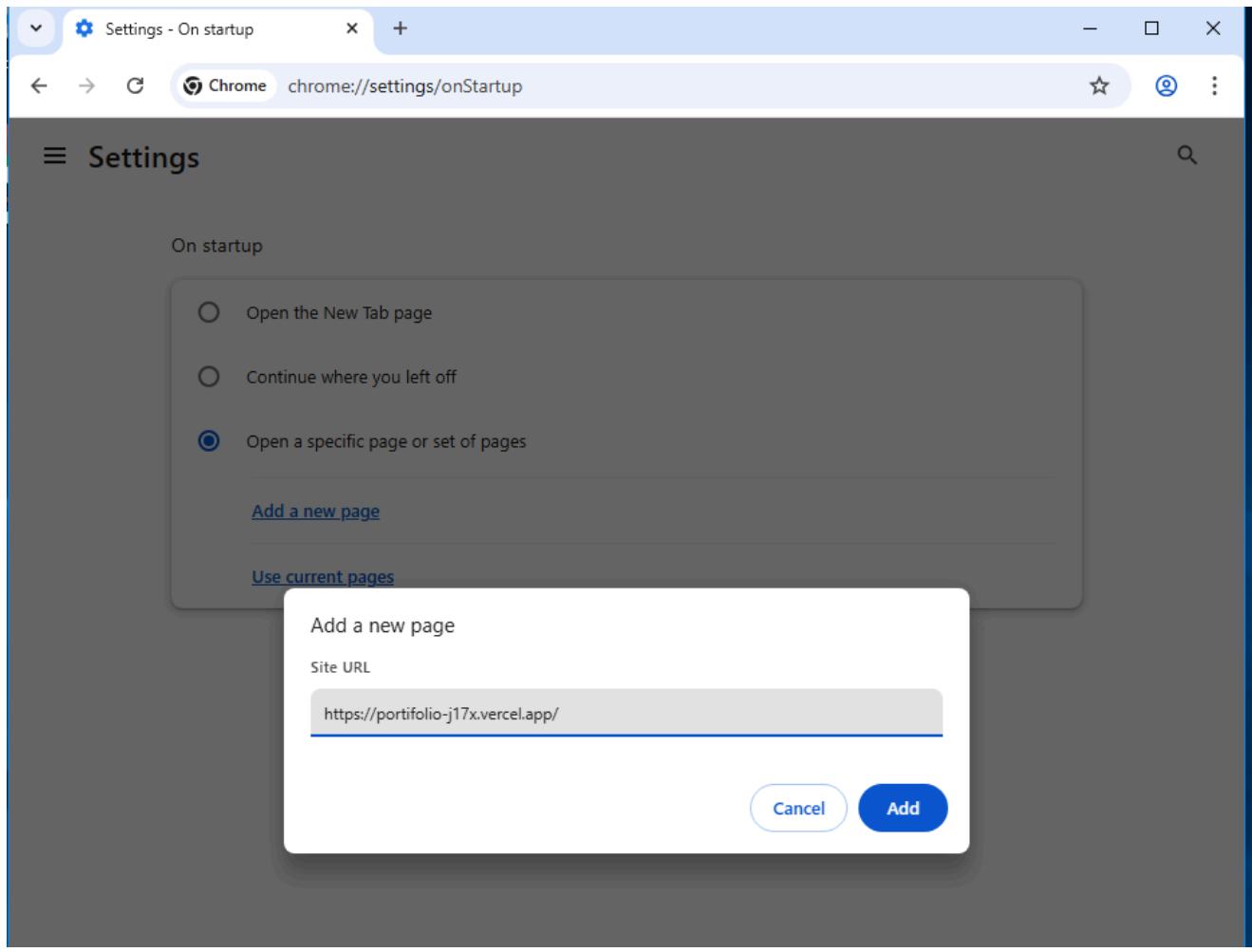
Successful autologon configuration was confirmed, ensuring the system logs in automatically after reboot.



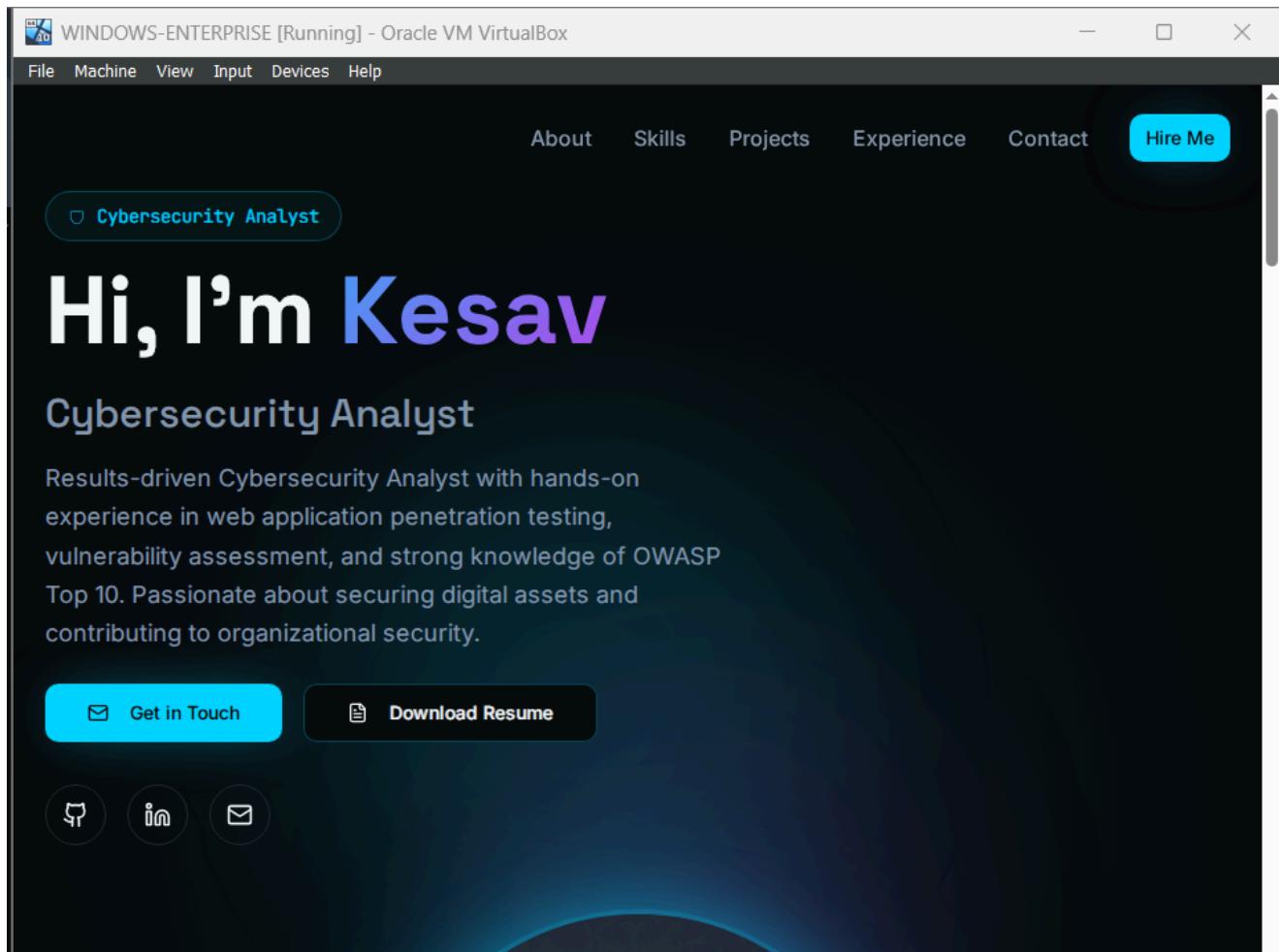
The system successfully logs in using the Website Login service account without manual input.



Browser startup configuration step was introduced to automatically launch a specific webpage.



Google Chrome was configured to open a specific webpage during startup. The configured webpage loads automatically, confirming correct startup browser configuration.



Google Chrome shortcut was added to the Windows Startup folder to ensure the browser launches automatically after login.

