ACTIVE DIRECTORY HOME LAB

🔹 Pre-Requisites for Active Directory Home Lab

1️⃣ 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)**.

2️⃣ Windows Client ISO

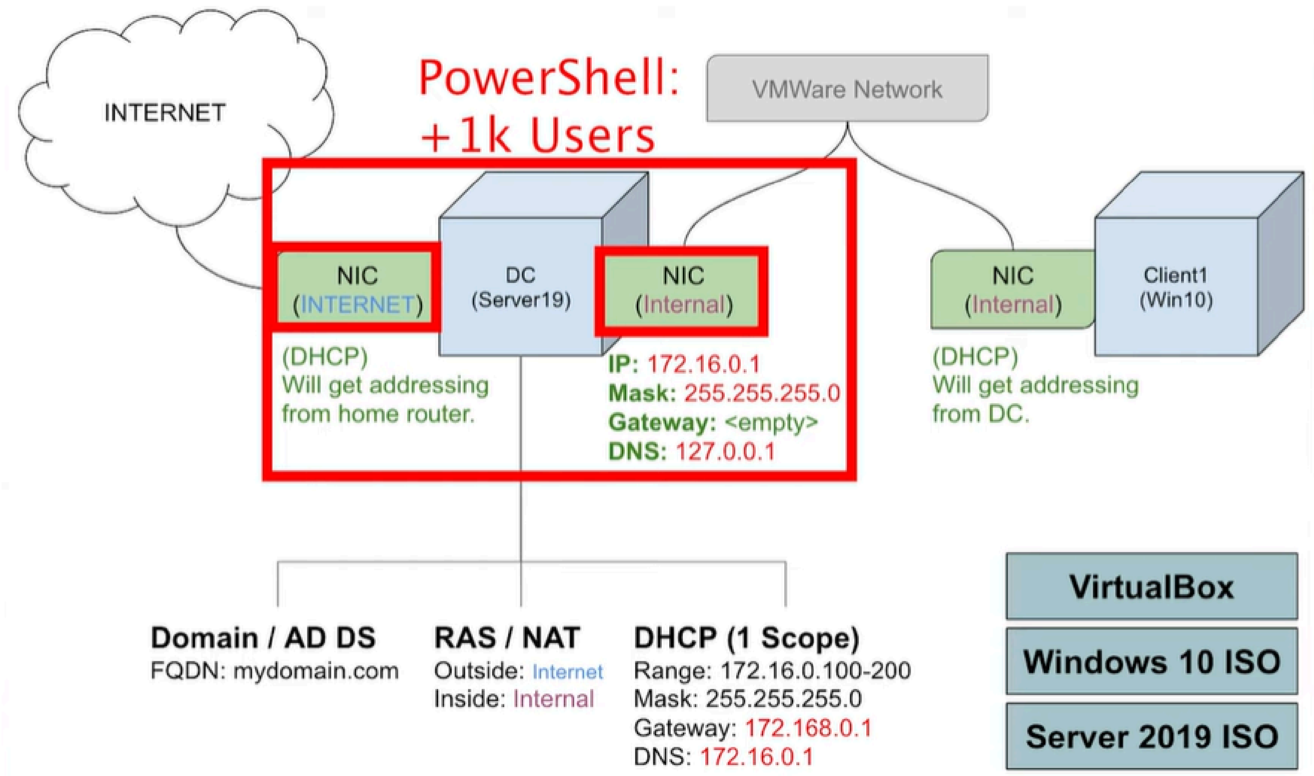
- **Windows 10 Enterprise / Professional**
  or
- **Windows 11 Enterprise / Professional**
- Used as domain client machine
- Must support domain join feature
- Minimum 4 GB RAM recommended

This system is used to:

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

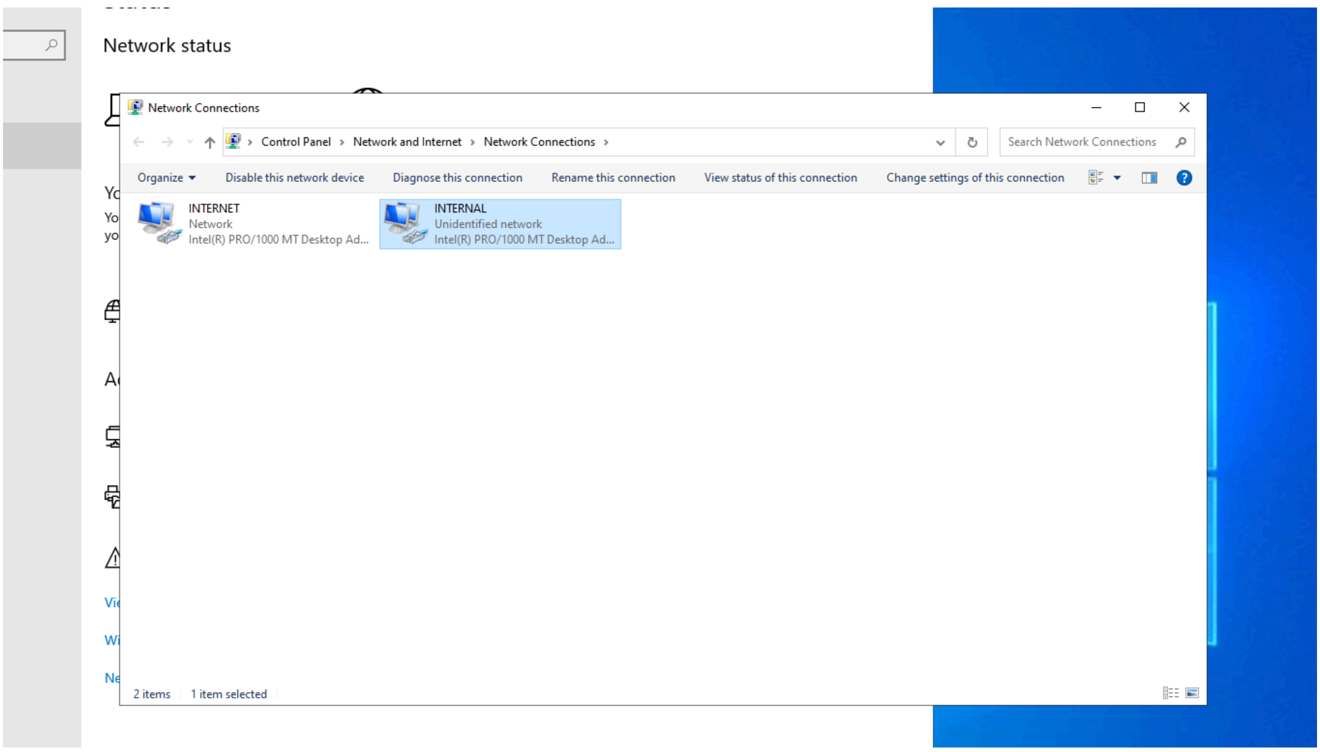
3️⃣ Virtualization Software

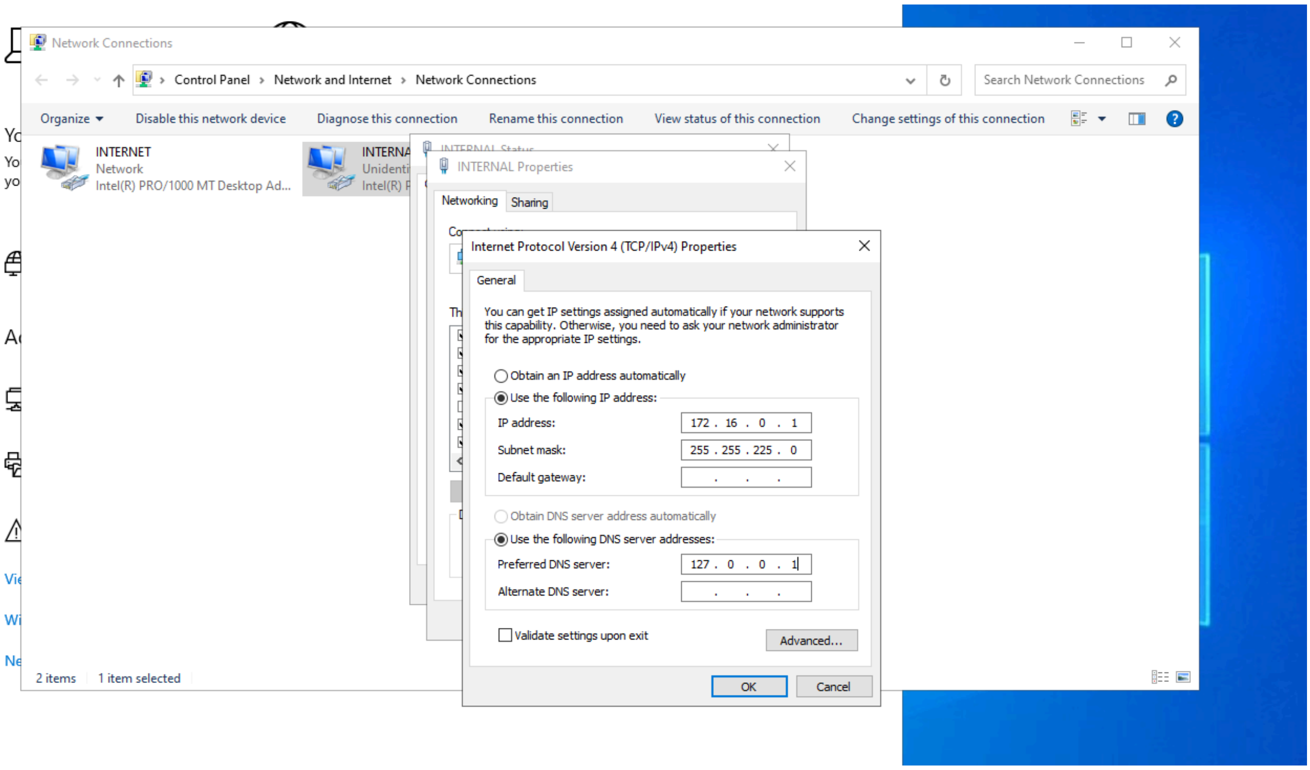
- **VirtualBox** or **VMware Workstation**
- Used to create:
  - 1 Domain Controller VM
  - 1 or more Client VMs
- Supports multiple network adapters (Internal + NAT/Bridged)



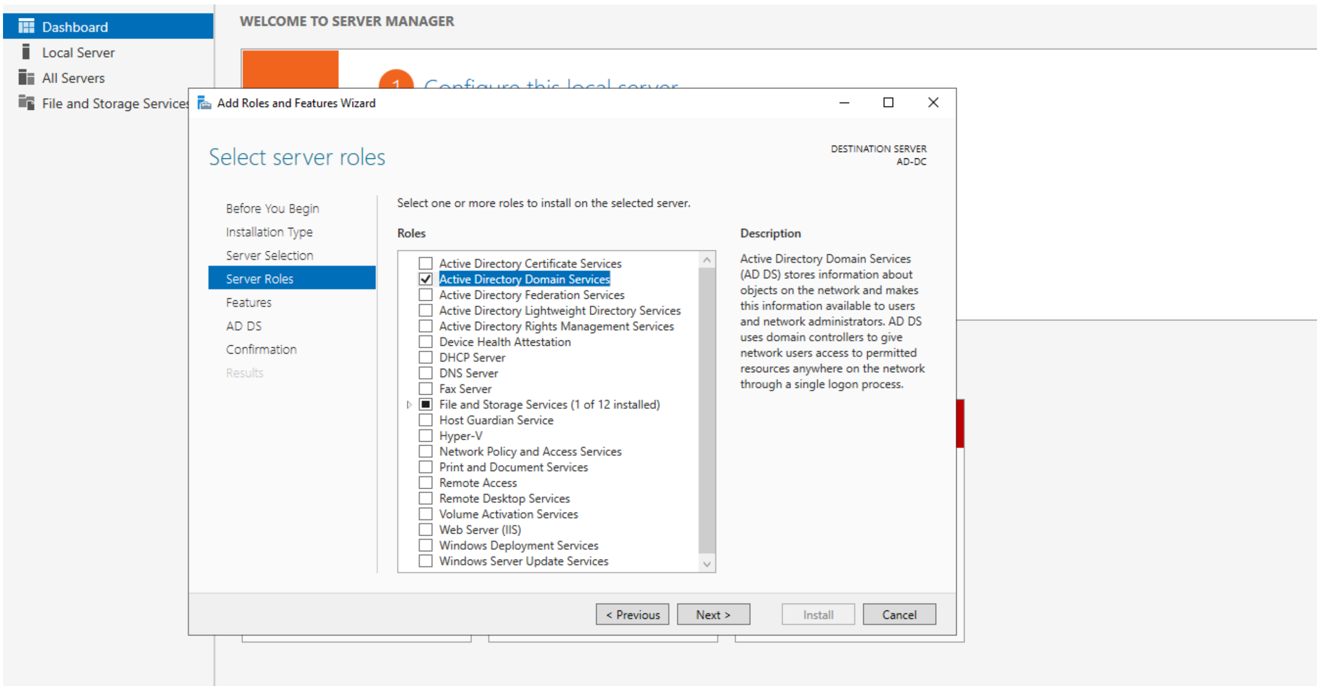
Network Connections window showing two configured adapters named INTERNET and INTERNAL. This setup separates external internet access from the internal domain network.

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.

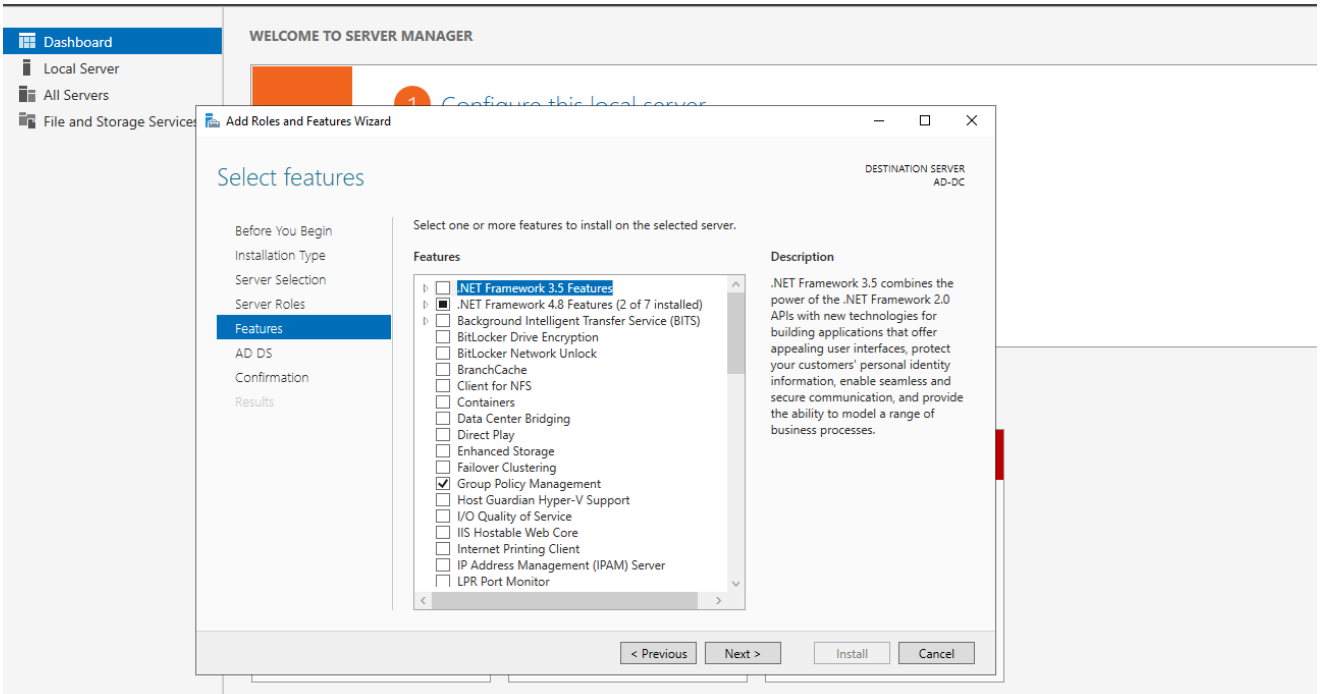




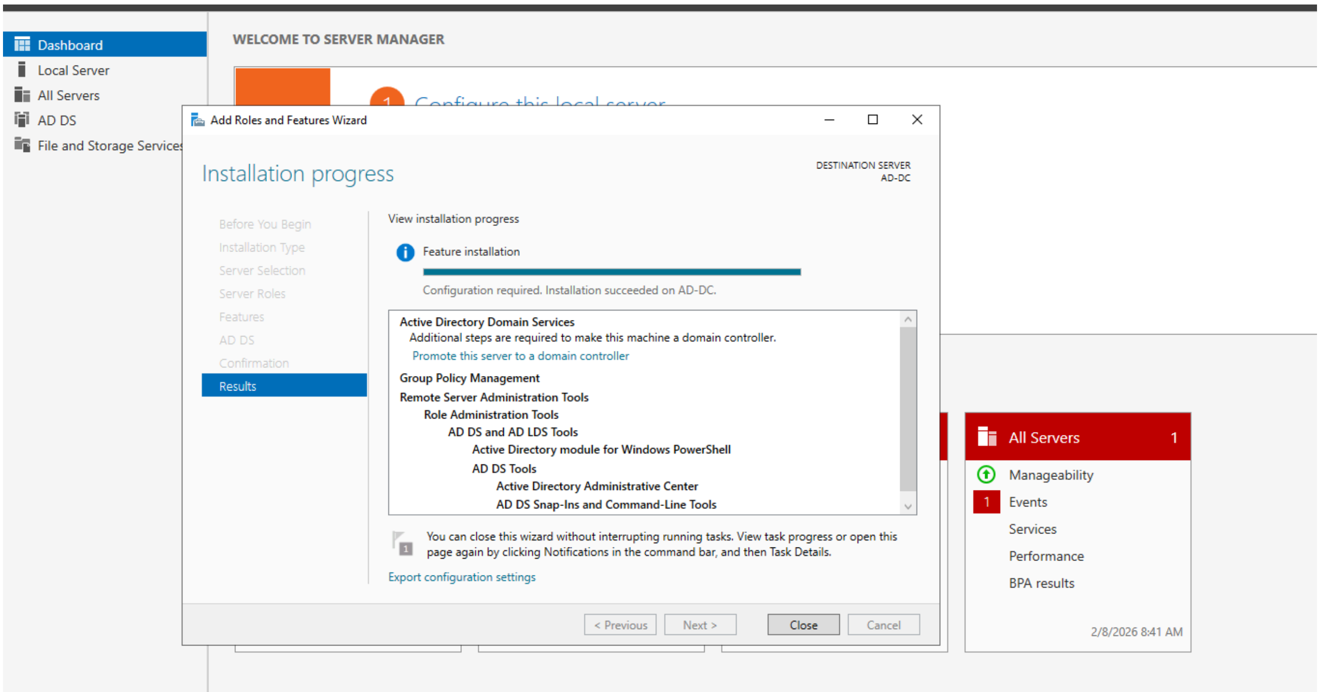
Add Roles and Features Wizard was opened to install server roles. Active Directory Domain Services (AD DS) role was selected for domain configuration.



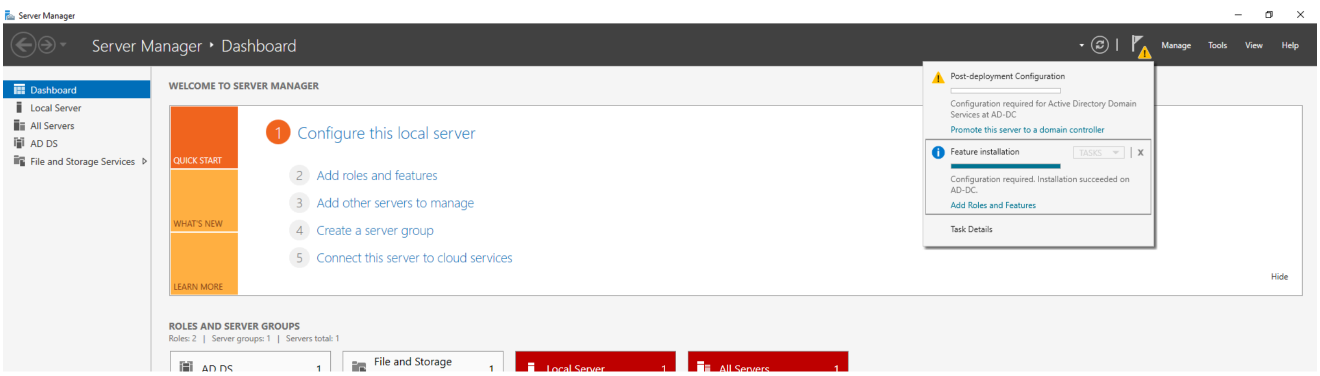
Required features and management tools were selected to support AD DS installation. This ensures proper administration and management of the domain.



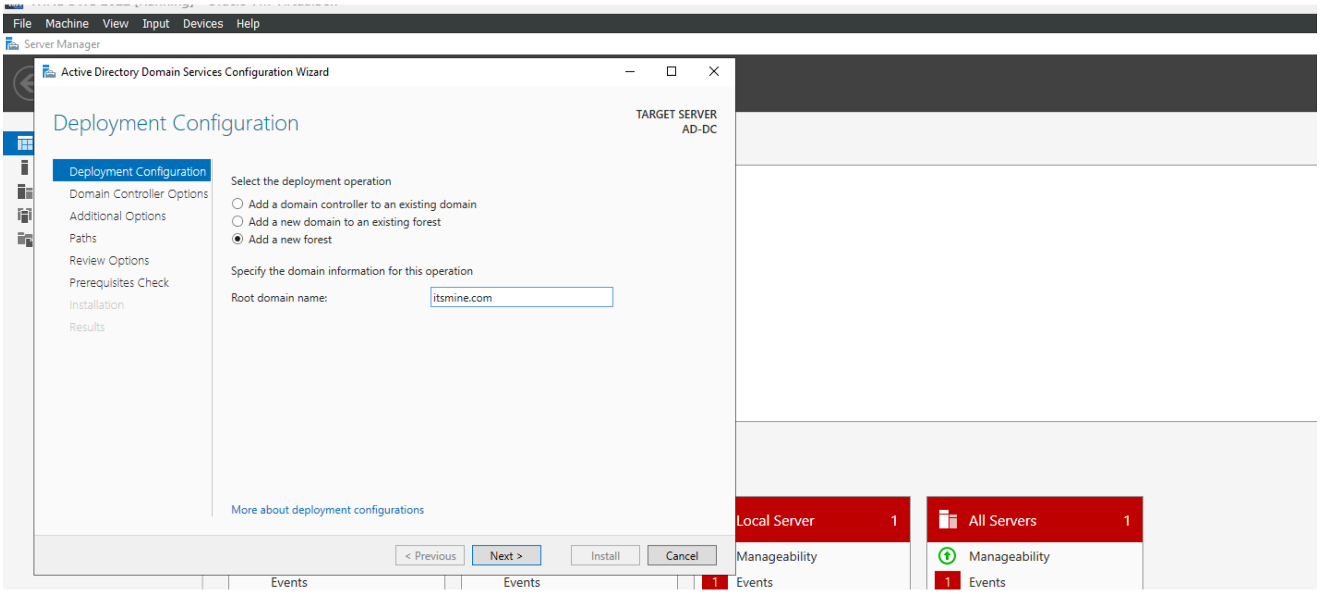
Active Directory Domain Services role installation was completed successfully. The server was prepared to be promoted as a Domain Controller



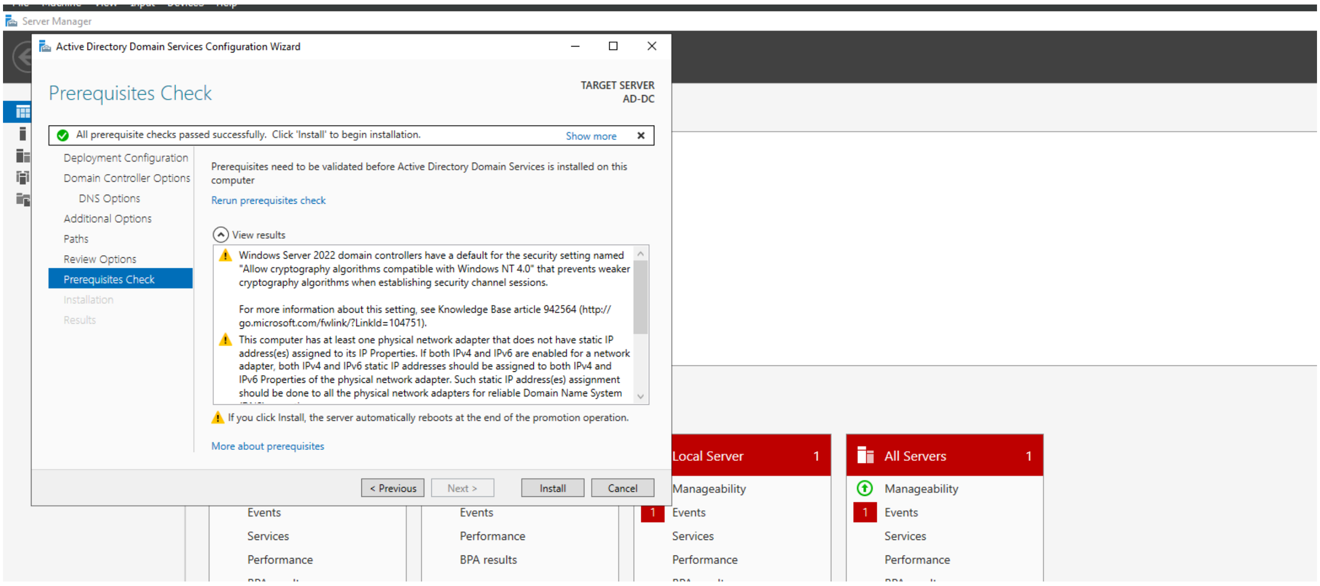
The option “Promote this server to a domain controller” was selected from Server Manager. This begins the domain creation process.



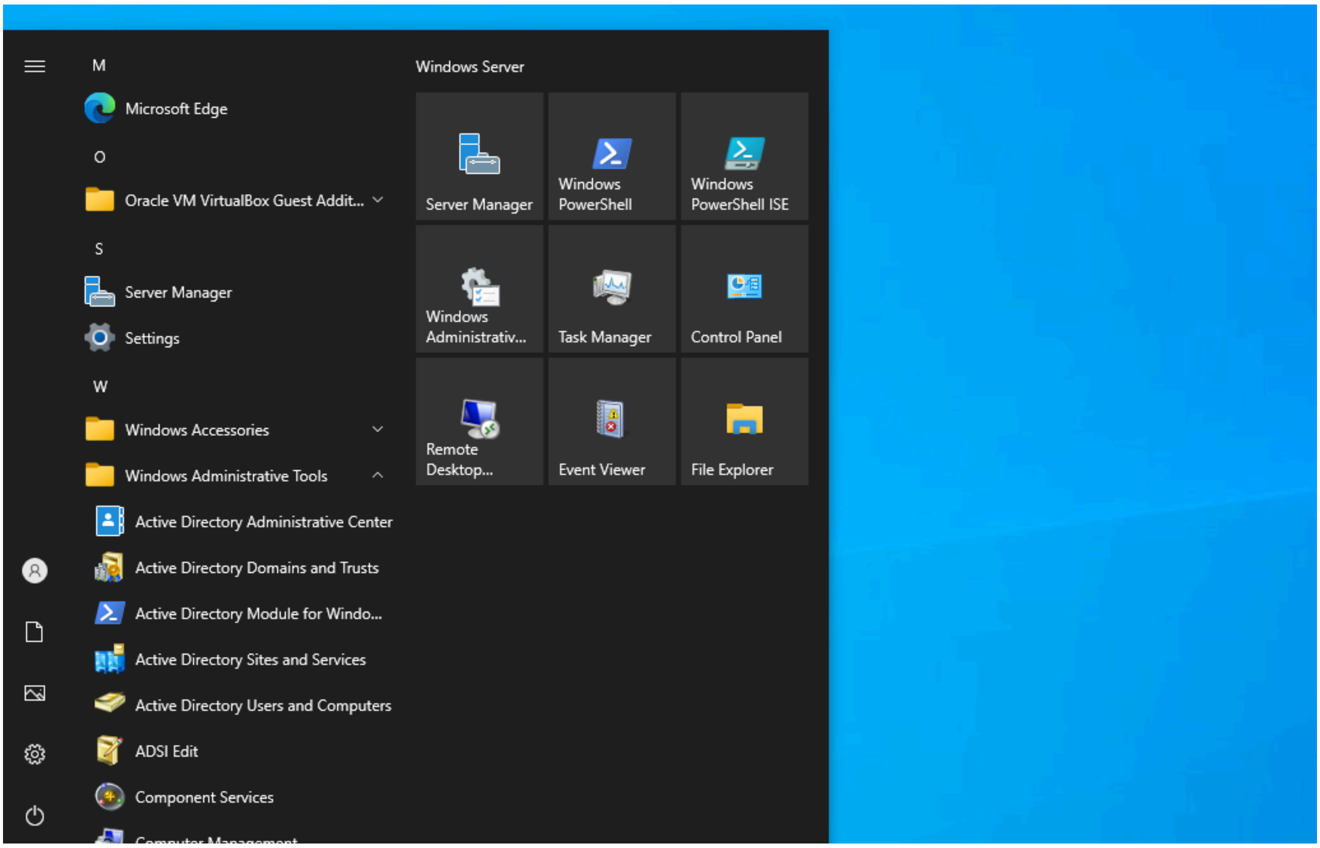
A new forest was created with the root domain name itsmine.com. This establishes the primary Active Directory domain environment.



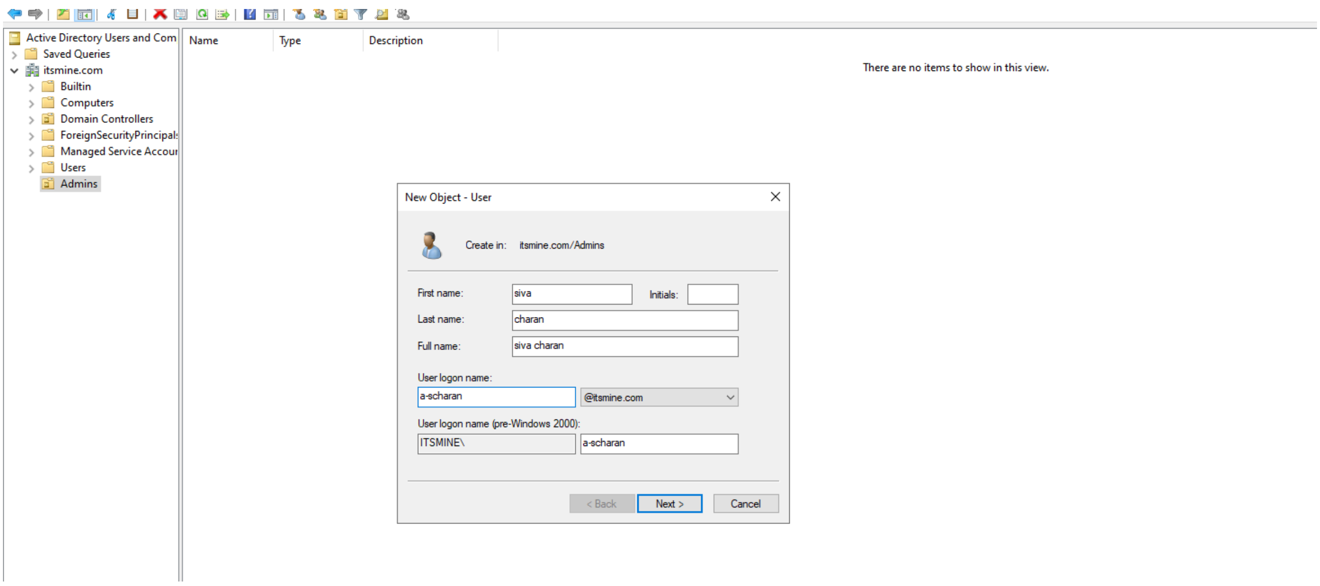
Prerequisite checks were completed before finalizing the Domain Controller promotion. The server was validated for AD DS configuration.



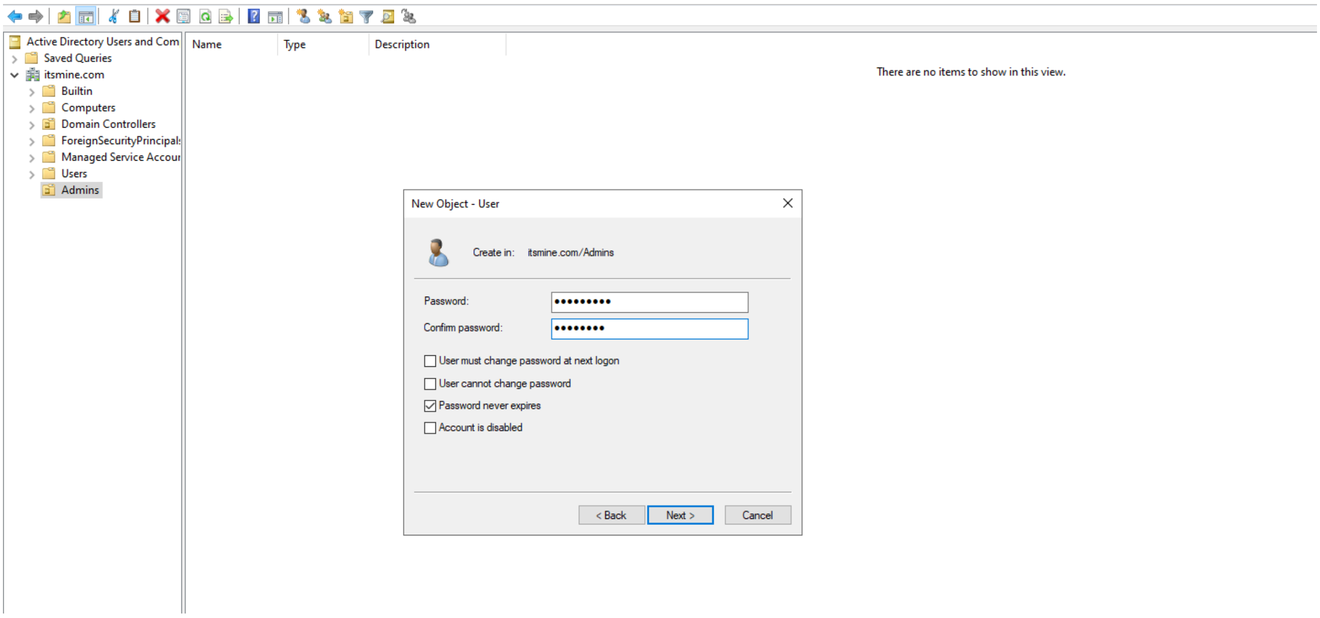
After restarting, Active Directory administrative tools were verified from the Start menu. This confirms successful installation of AD services.



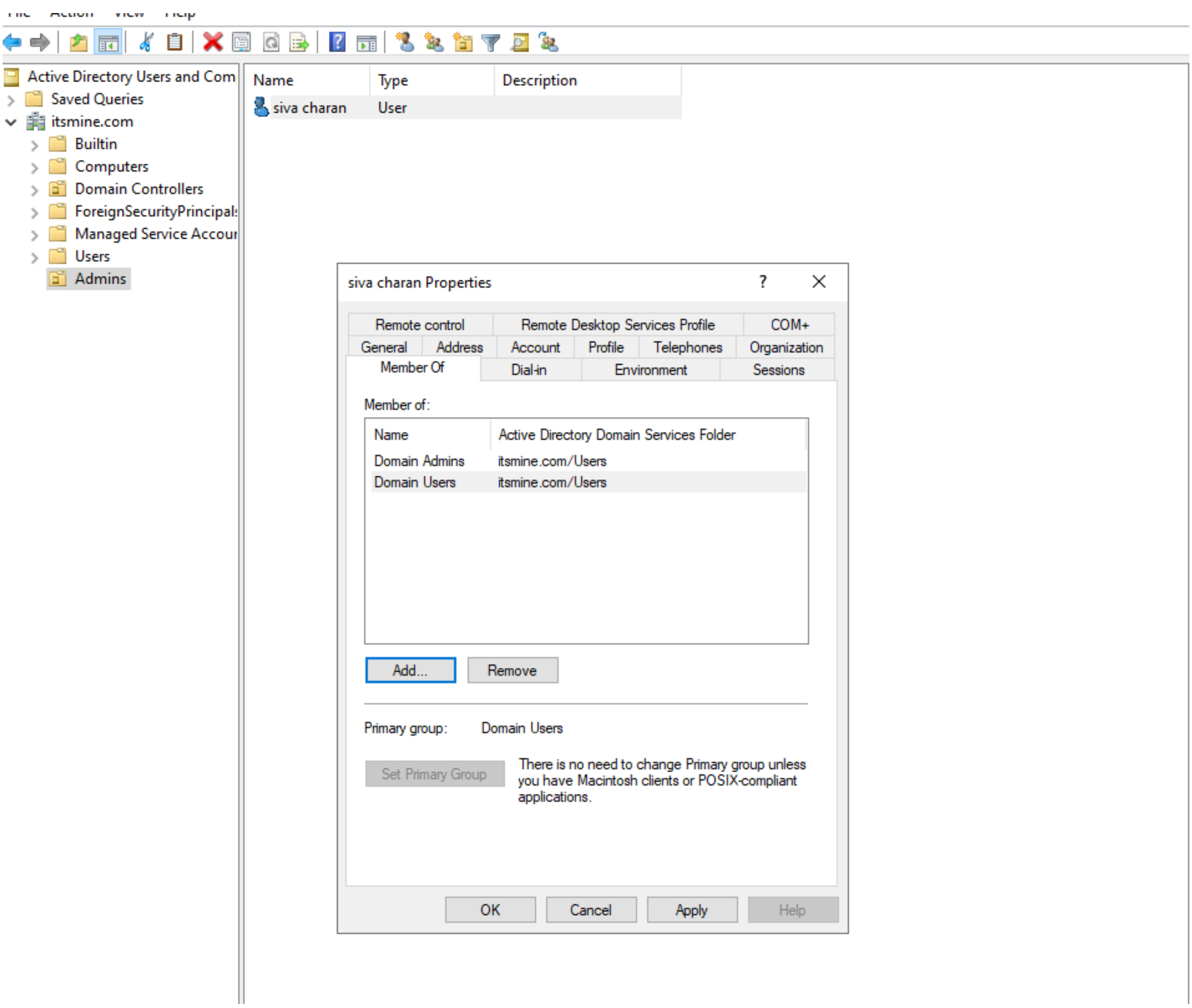
Active Directory Users and Computers console was opened to begin user account management. A new domain user creation process was initiated.



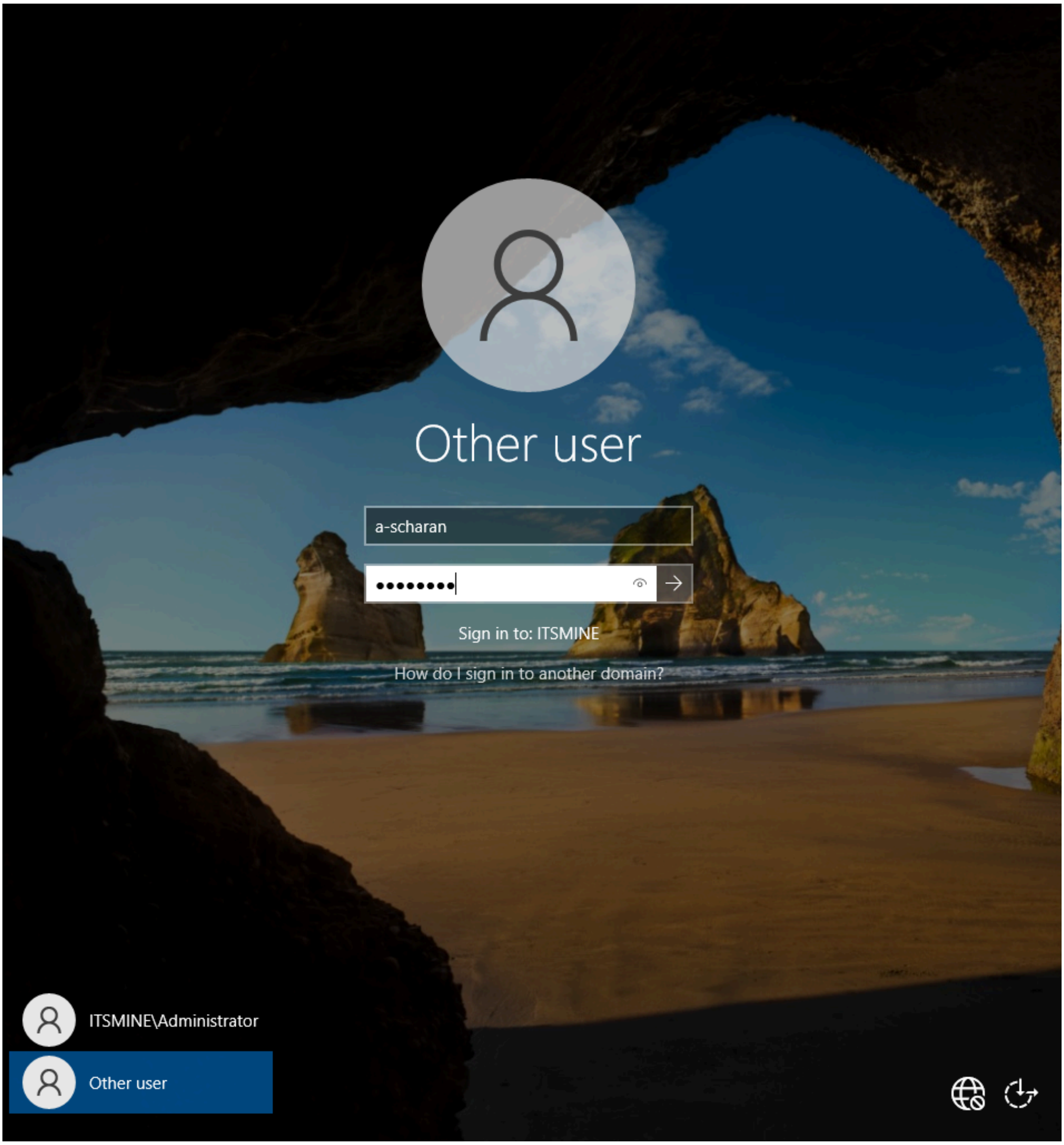
User account details such as first name, last name, and logon name were entered. This step creates a new domain user object in Active Directory.



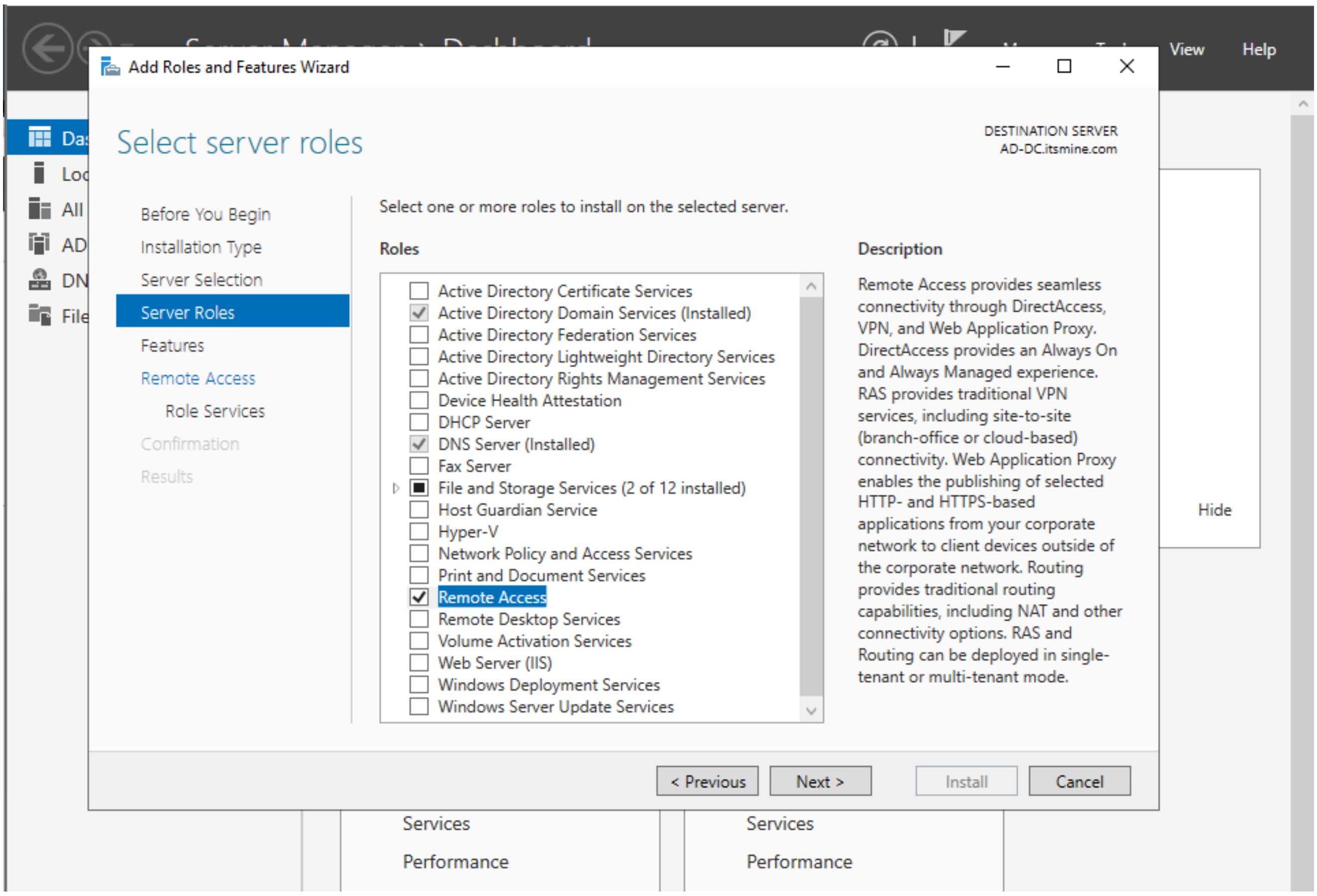
A secure password was assigned to the user account and the account was enabled. Group membership was reviewed under the Member Of tab



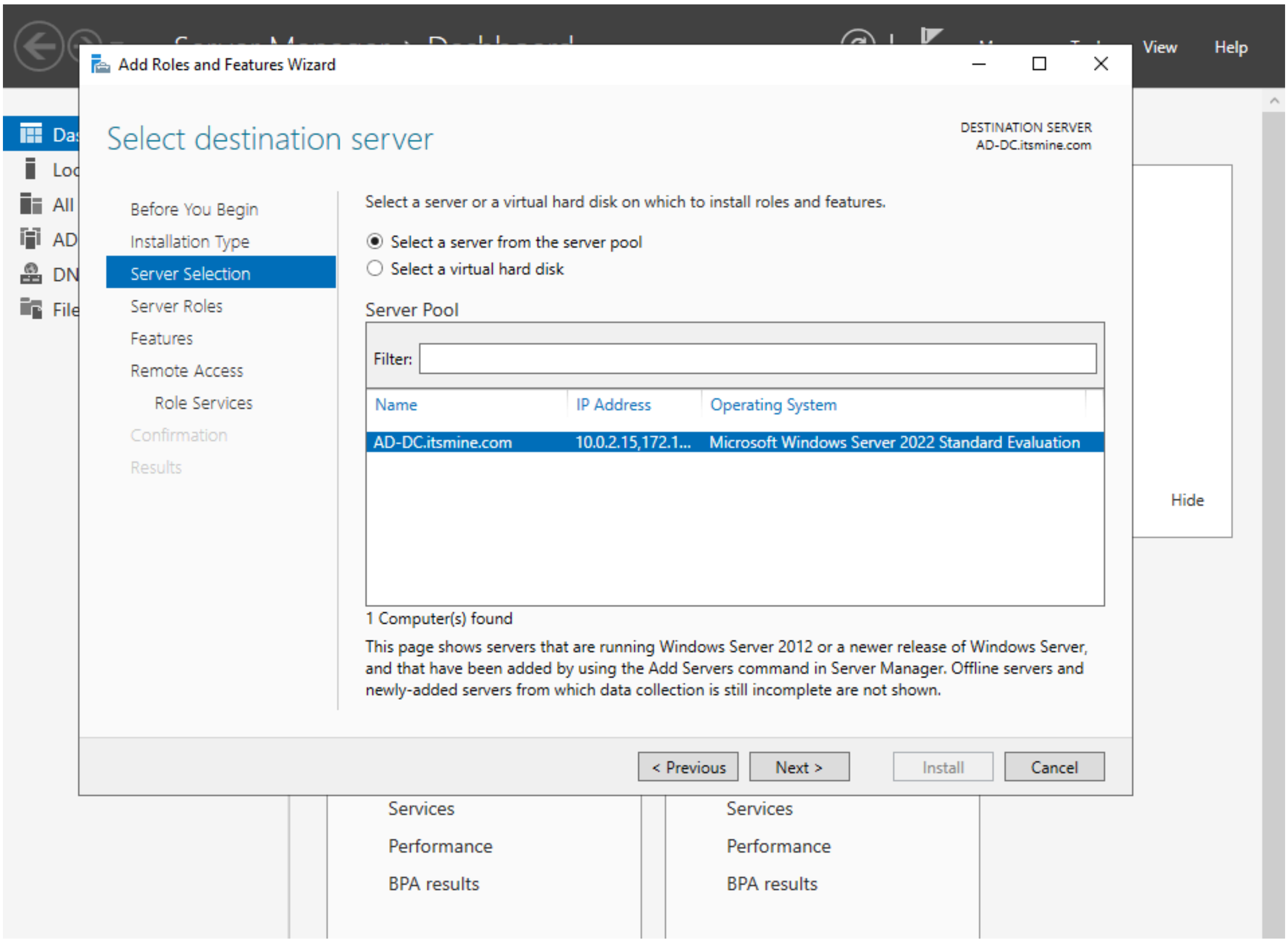
Windows login screen displaying domain user authentication. Successful login confirms proper domain connectivity and authentication services.



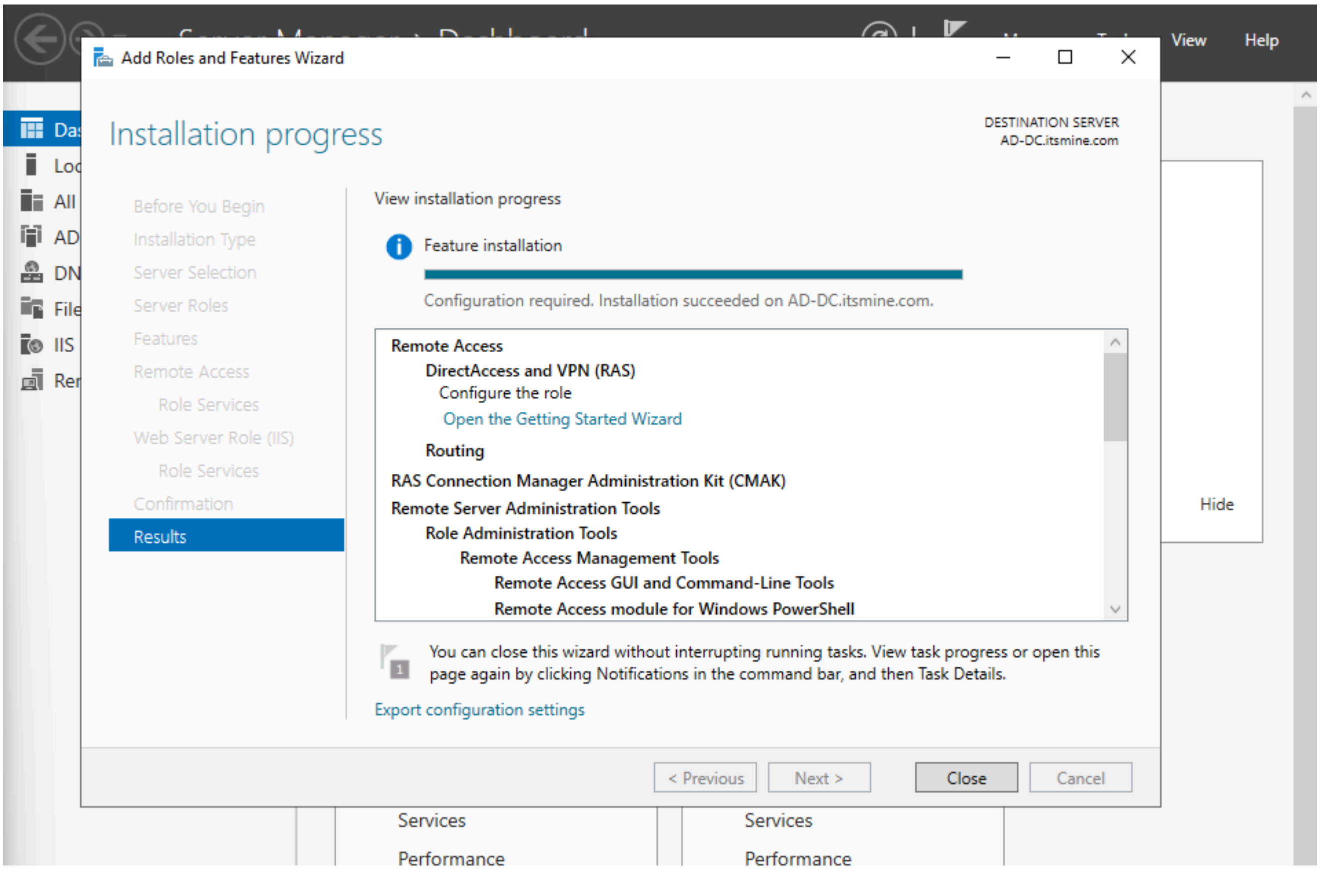
Add Roles and Features Wizard was used again to install the Remote Access role. This role is required for routing and NAT configuration.



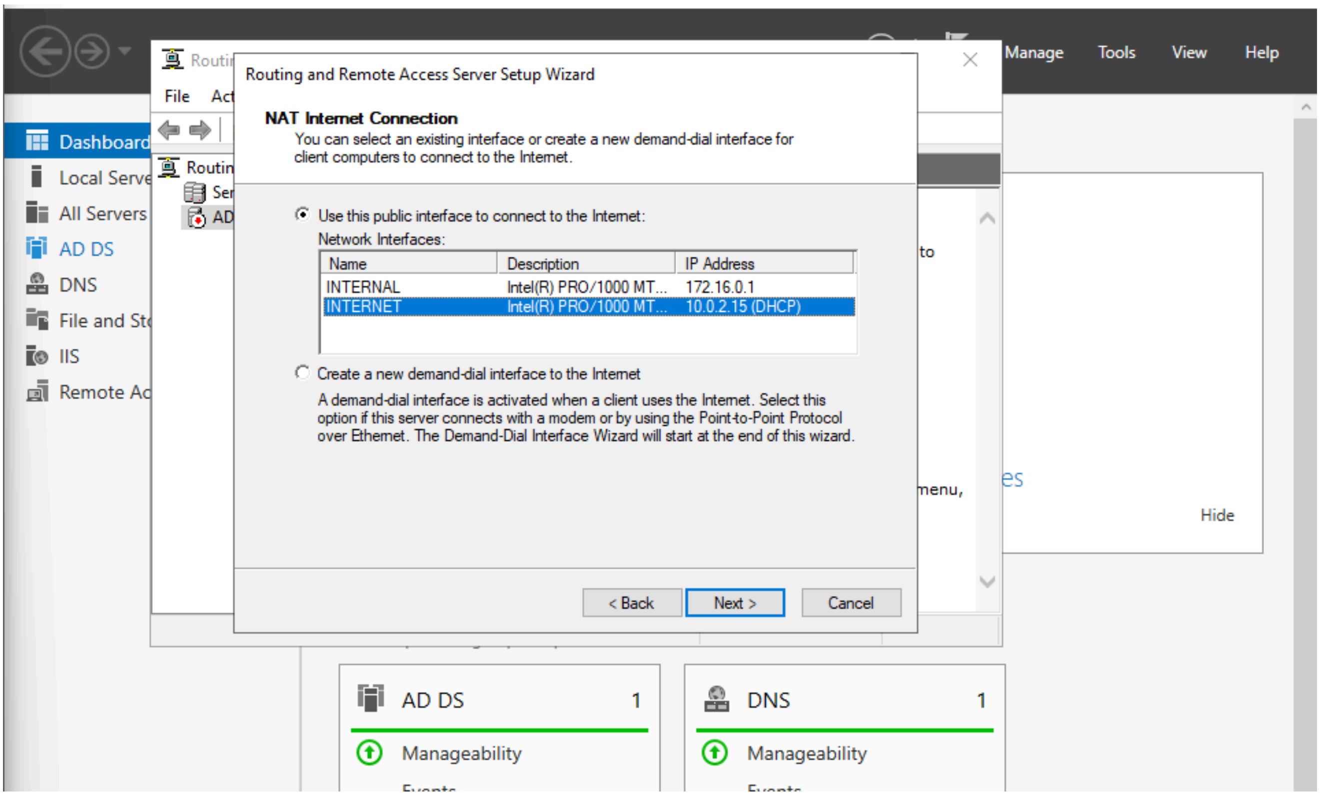
The destination server was confirmed before proceeding with installation. Remote Access role installation was initiated.



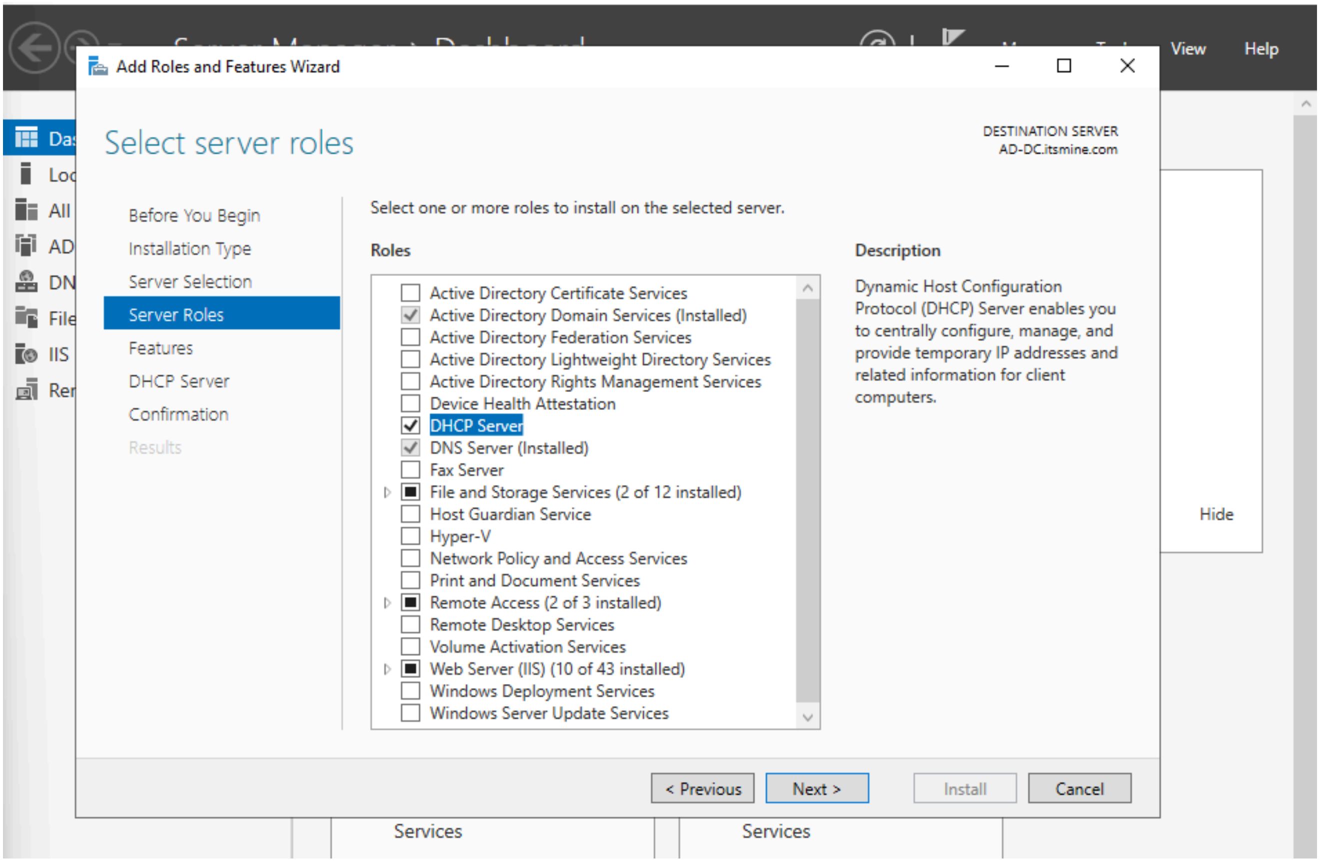
Remote Access role installation was completed successfully. The server is now capable of handling routing services.



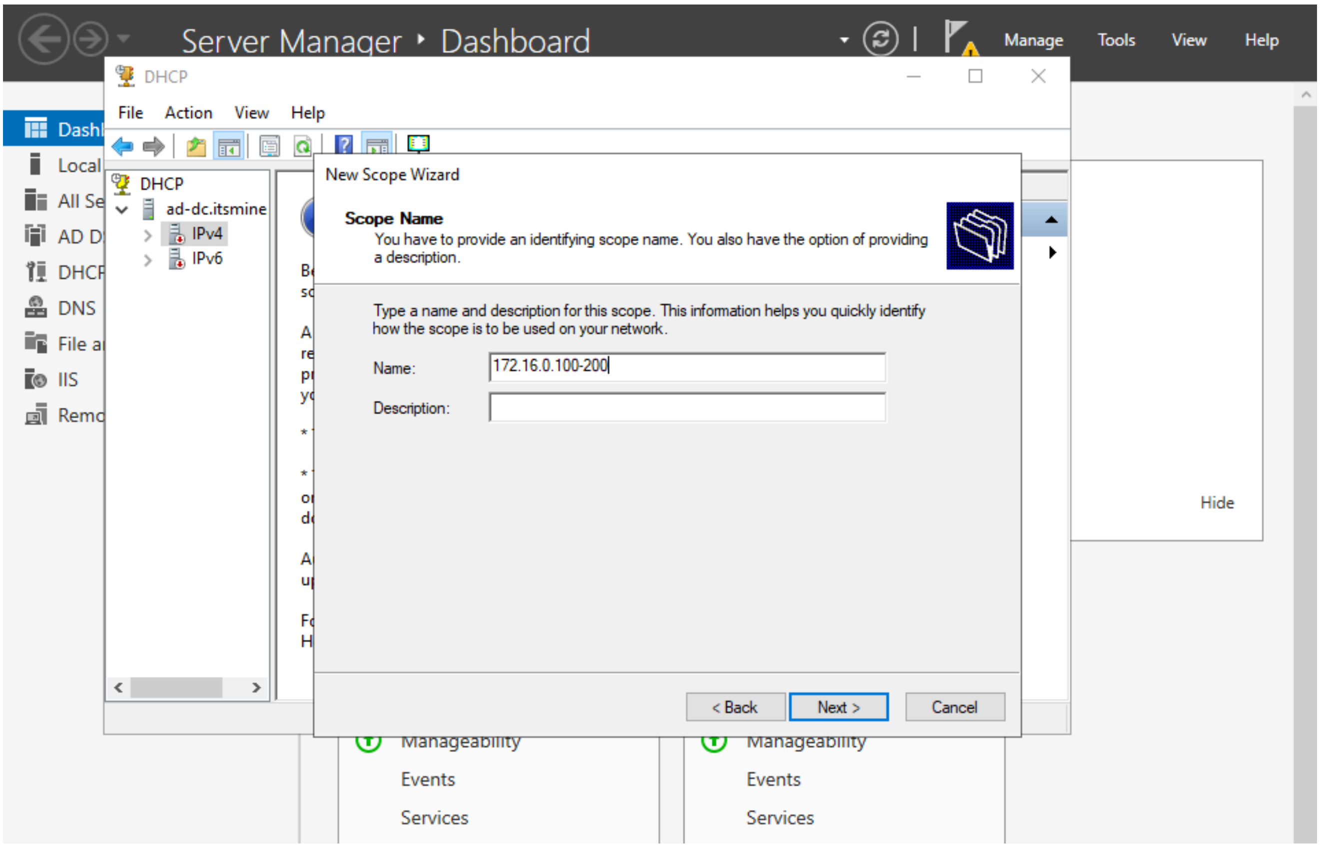
Routing and Remote Access setup wizard was used to configure NAT. The INTERNAL interface was selected as the private network interface.



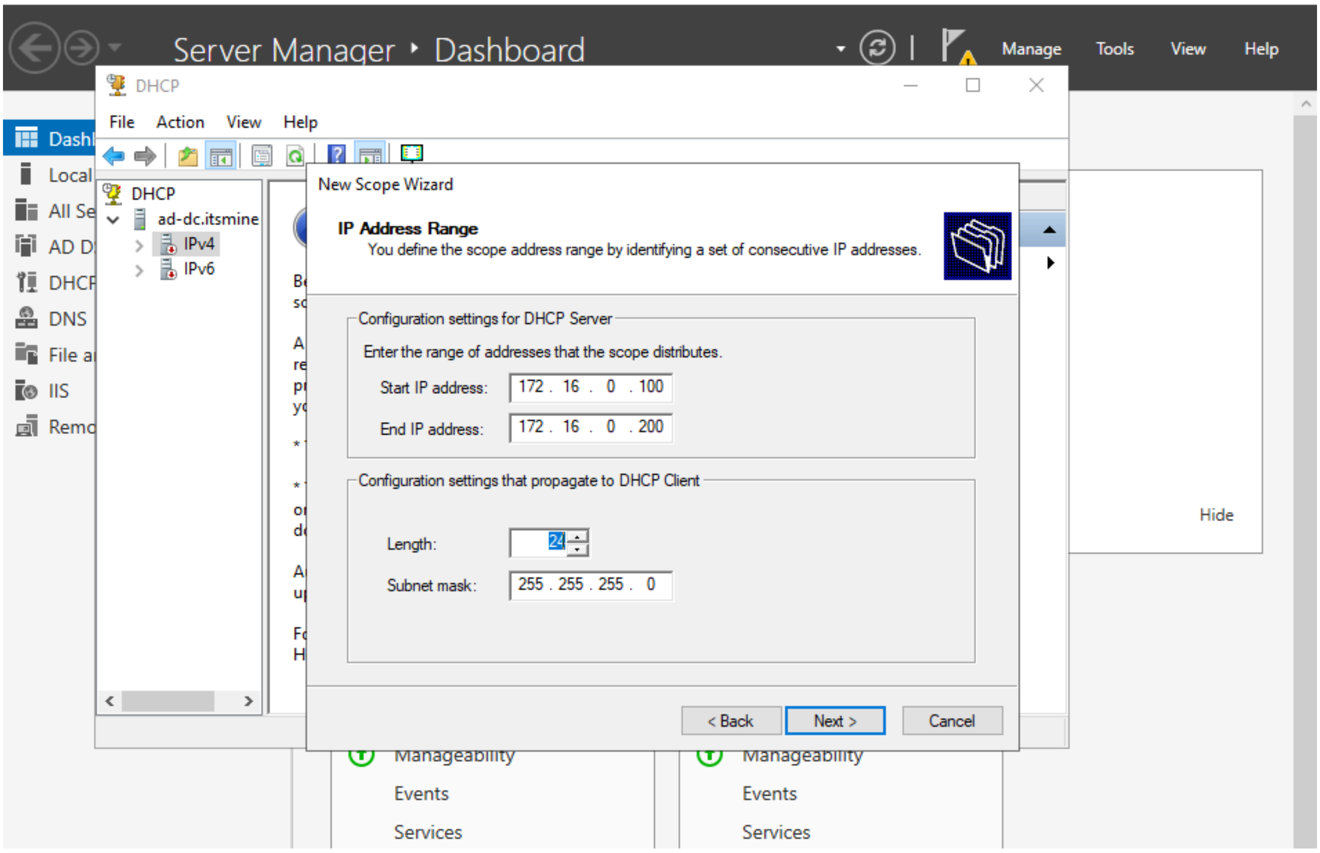
DHCP Server role was selected and installed from Server Manager. This allows automatic IP address assignment for client machines.



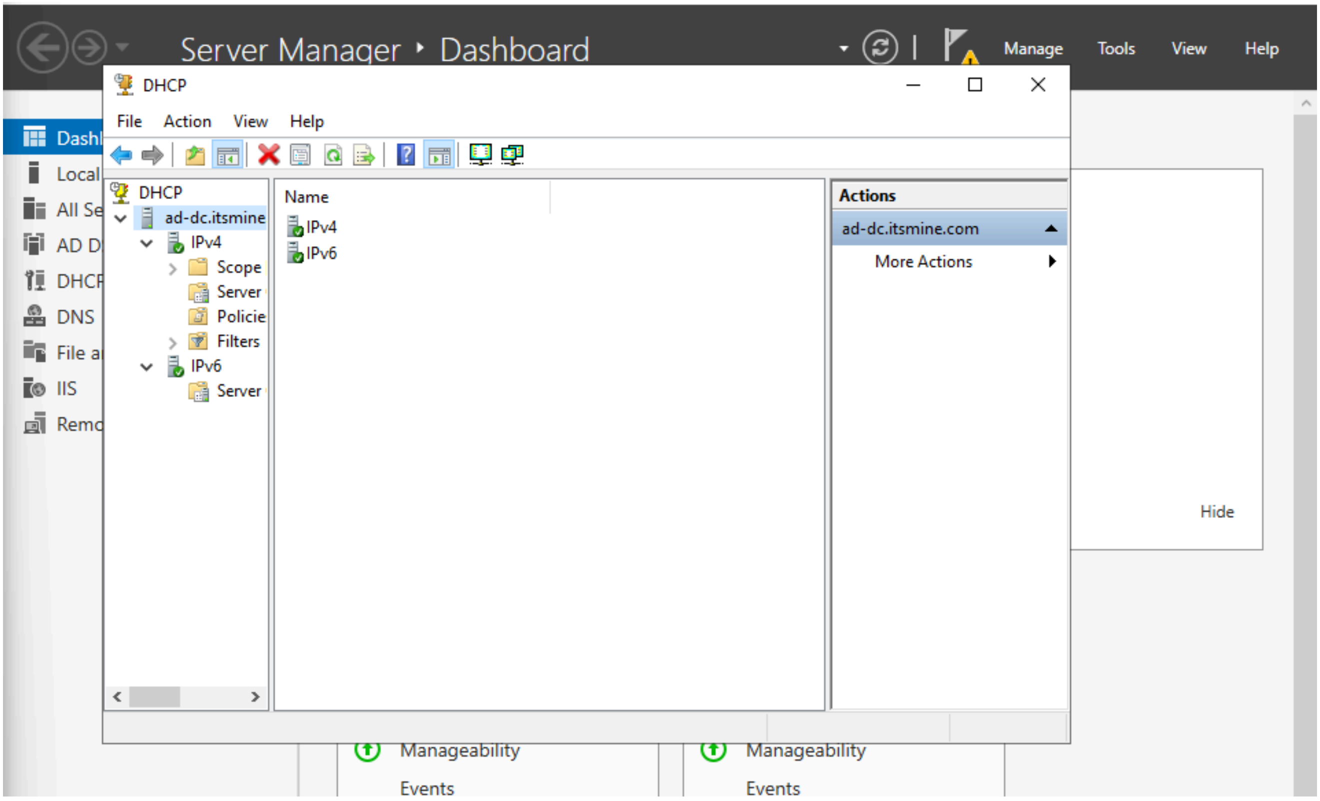
New Scope Wizard was opened in the DHCP console. A scope was created for the IP range 172.16.0.100–200.



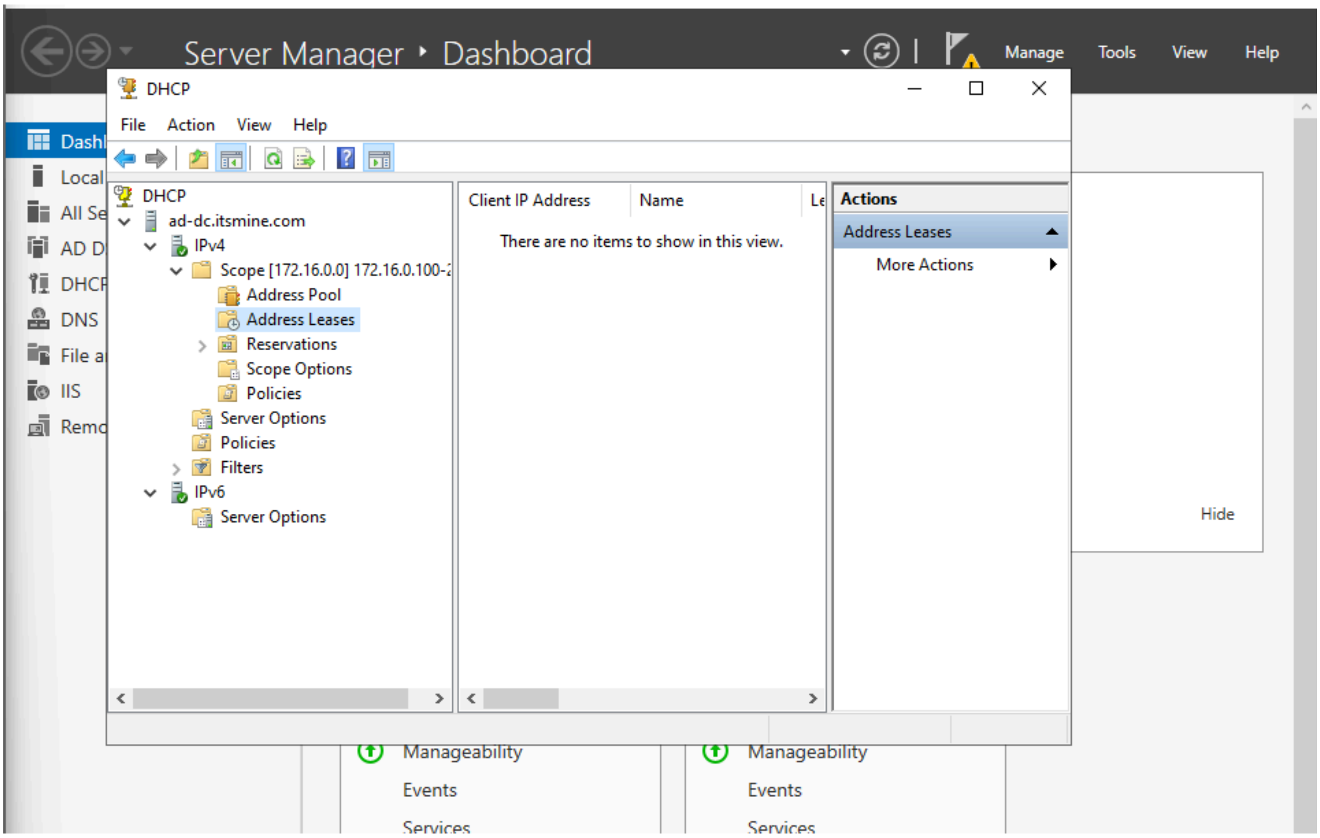
DHCP scope was configured with start IP 172.16.0.100 and end IP 172.16.0.200. Subnet mask 255.255.255.0 was defined for the network



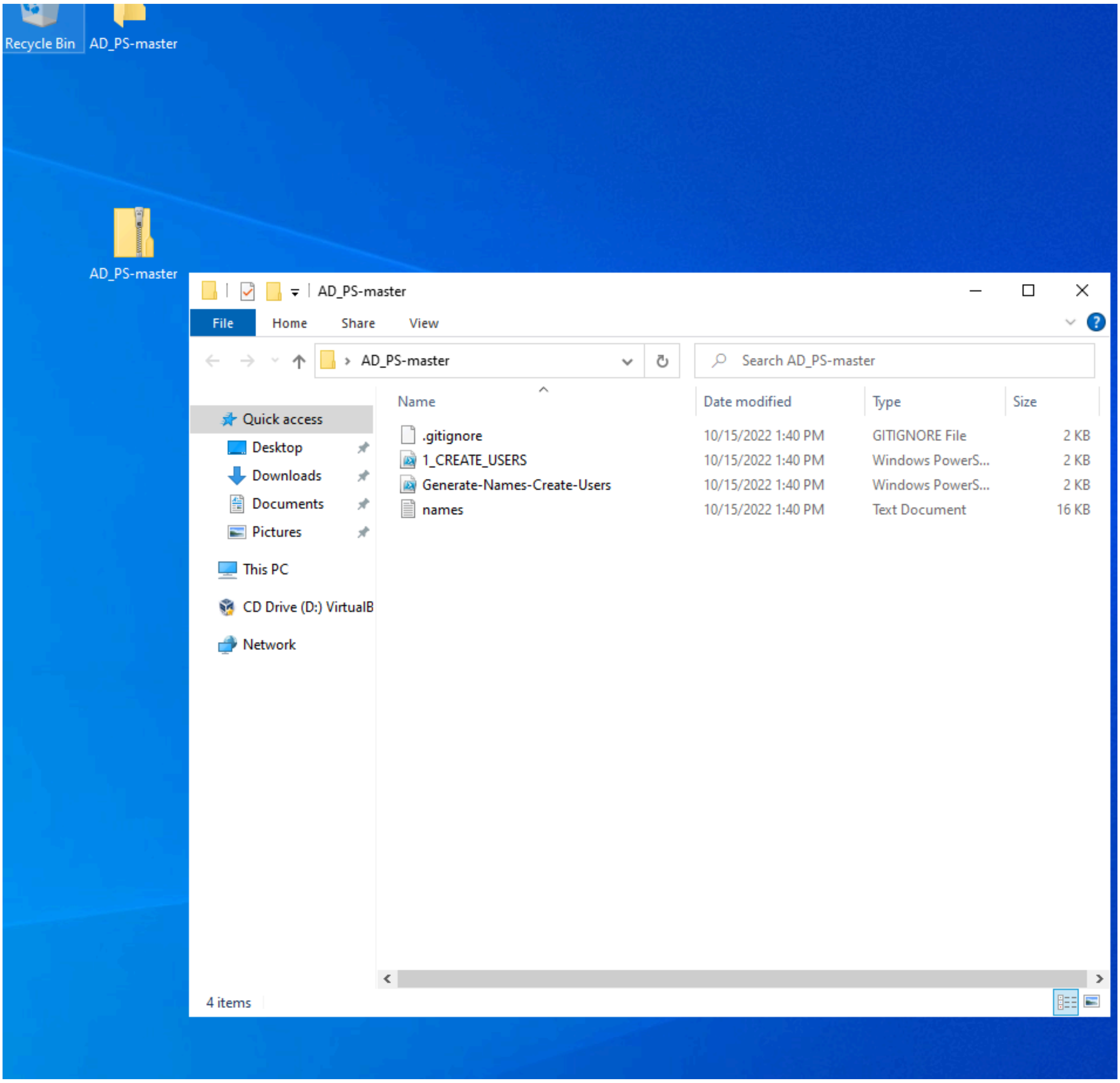
The DHCP scope was successfully created under IPv4. The server is ready to distribute IP addresses to domain clients.



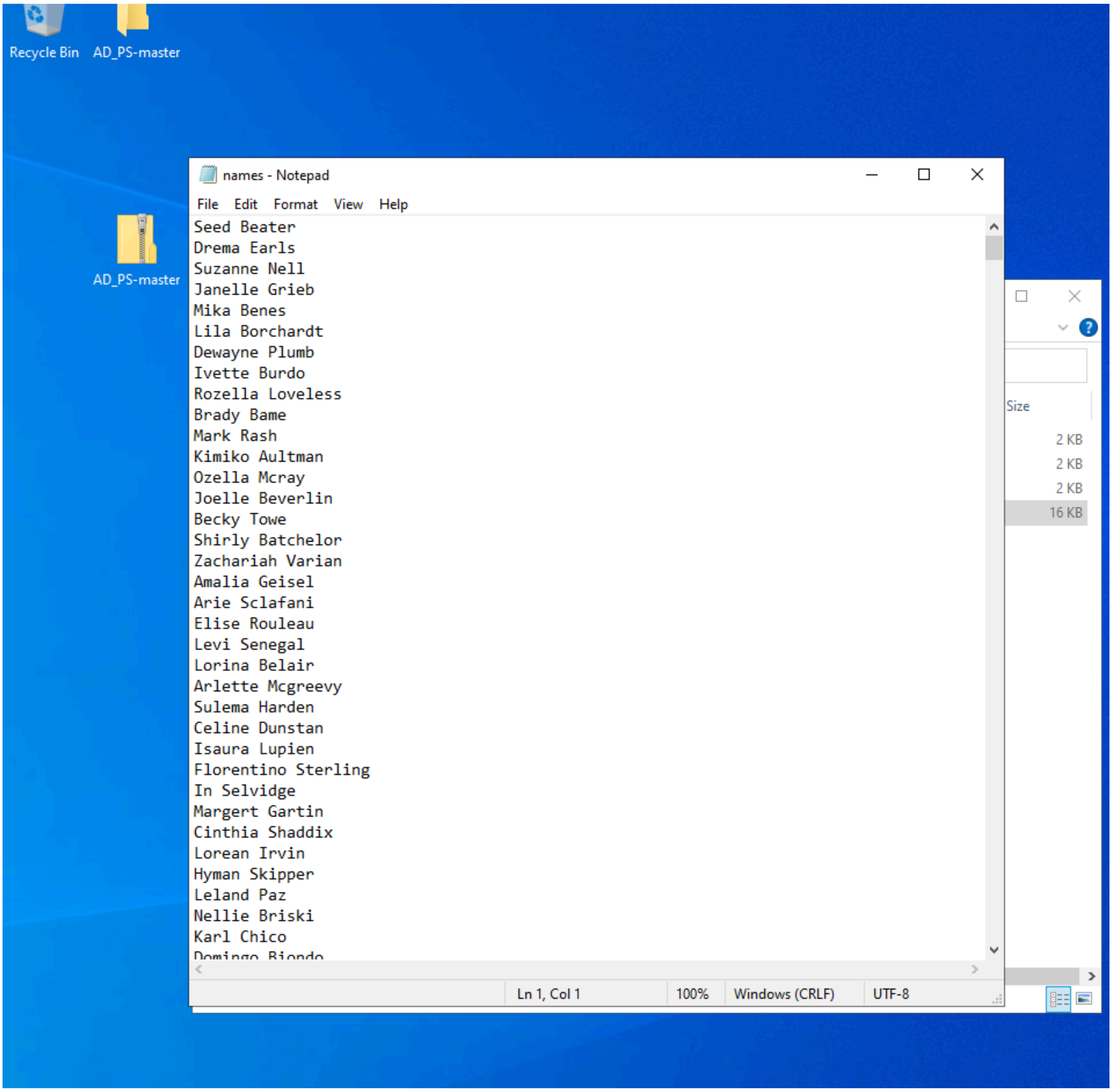
Address Leases section in DHCP console was opened. This area displays IP addresses assigned to client systems



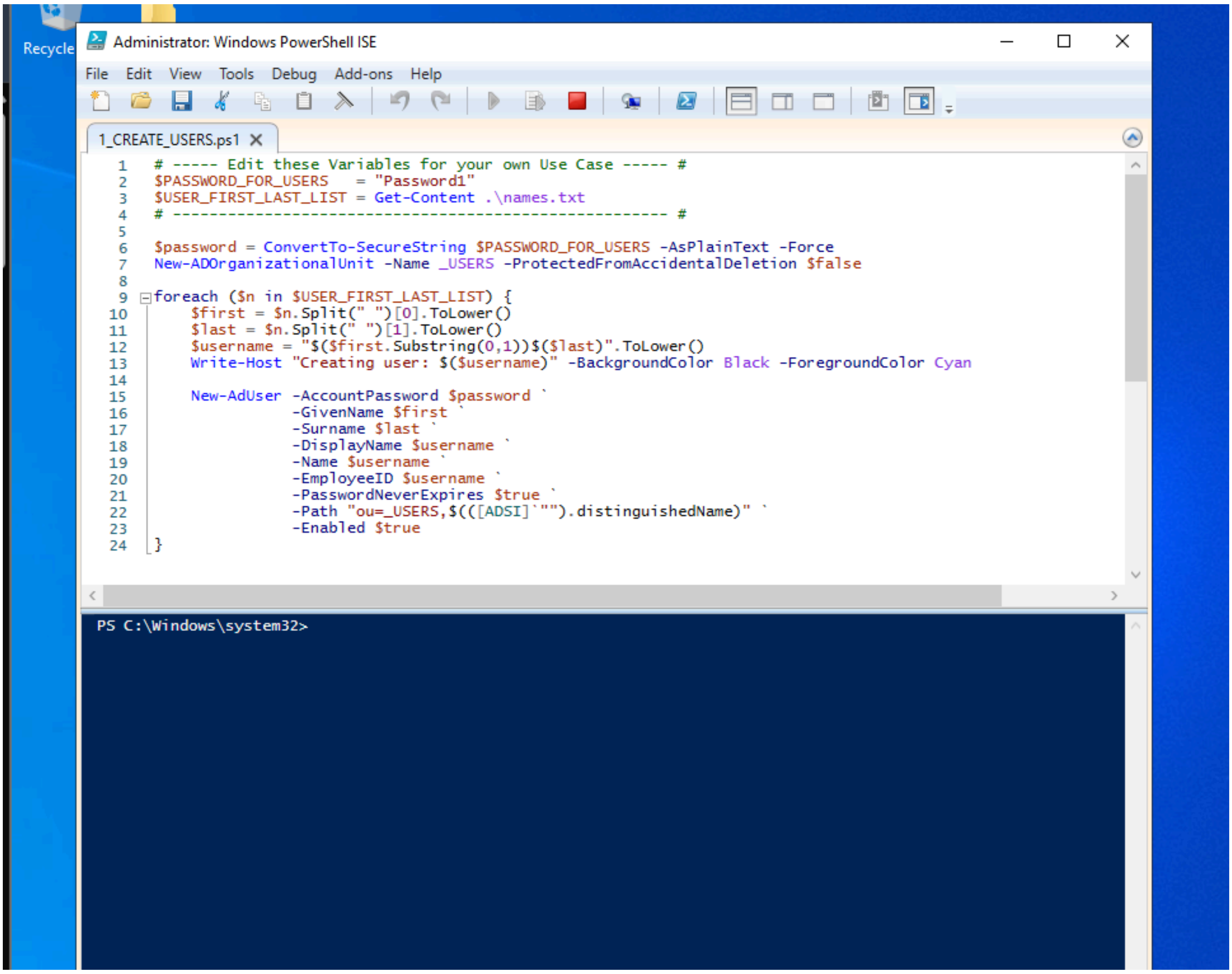
A folder named AD_PS-master was created to store automation scripts. It contains the PowerShell script and user list file for bulk user creation.



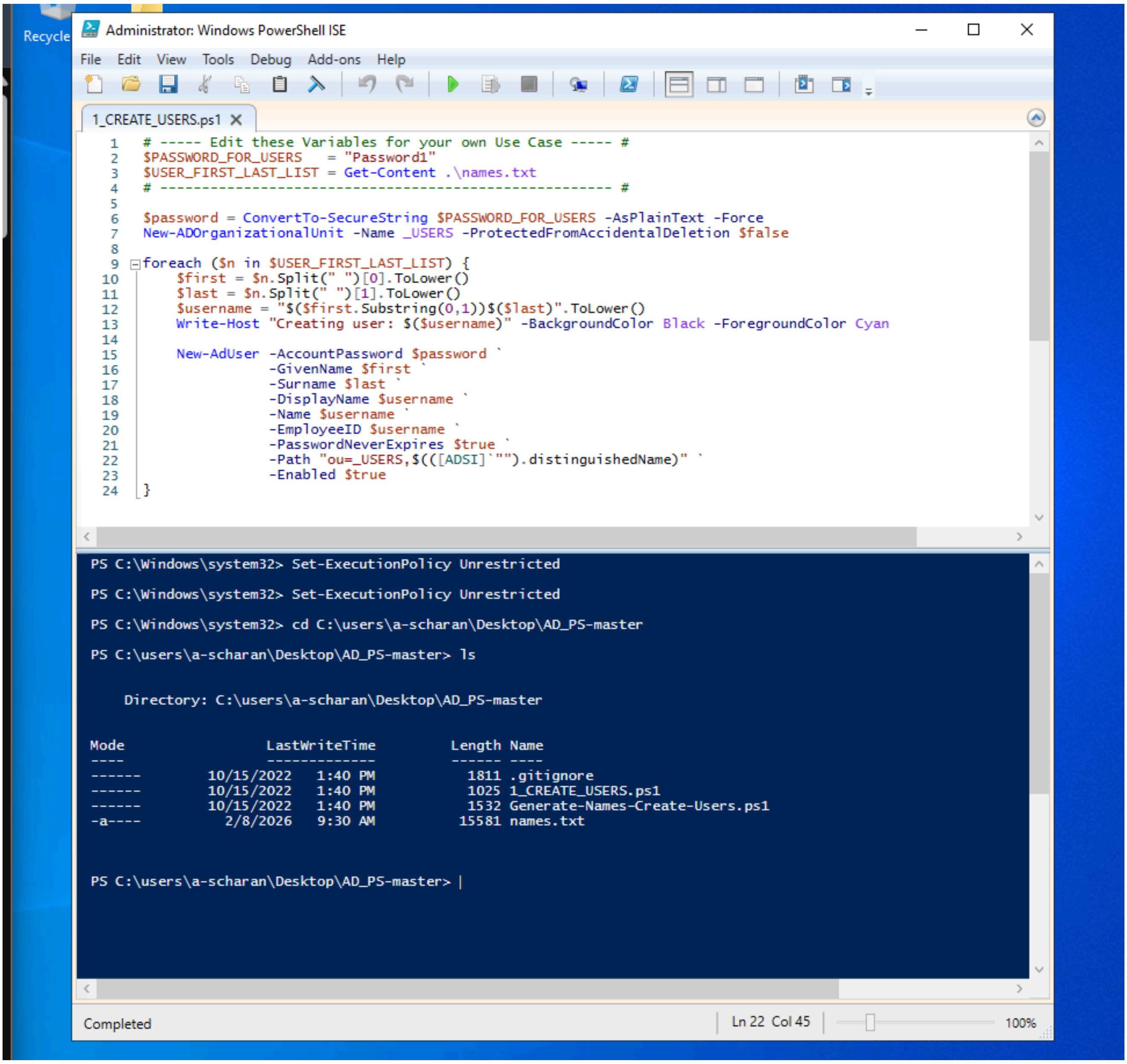
The names.txt file was created containing multiple user names. This file will be used as input for automated user creation.



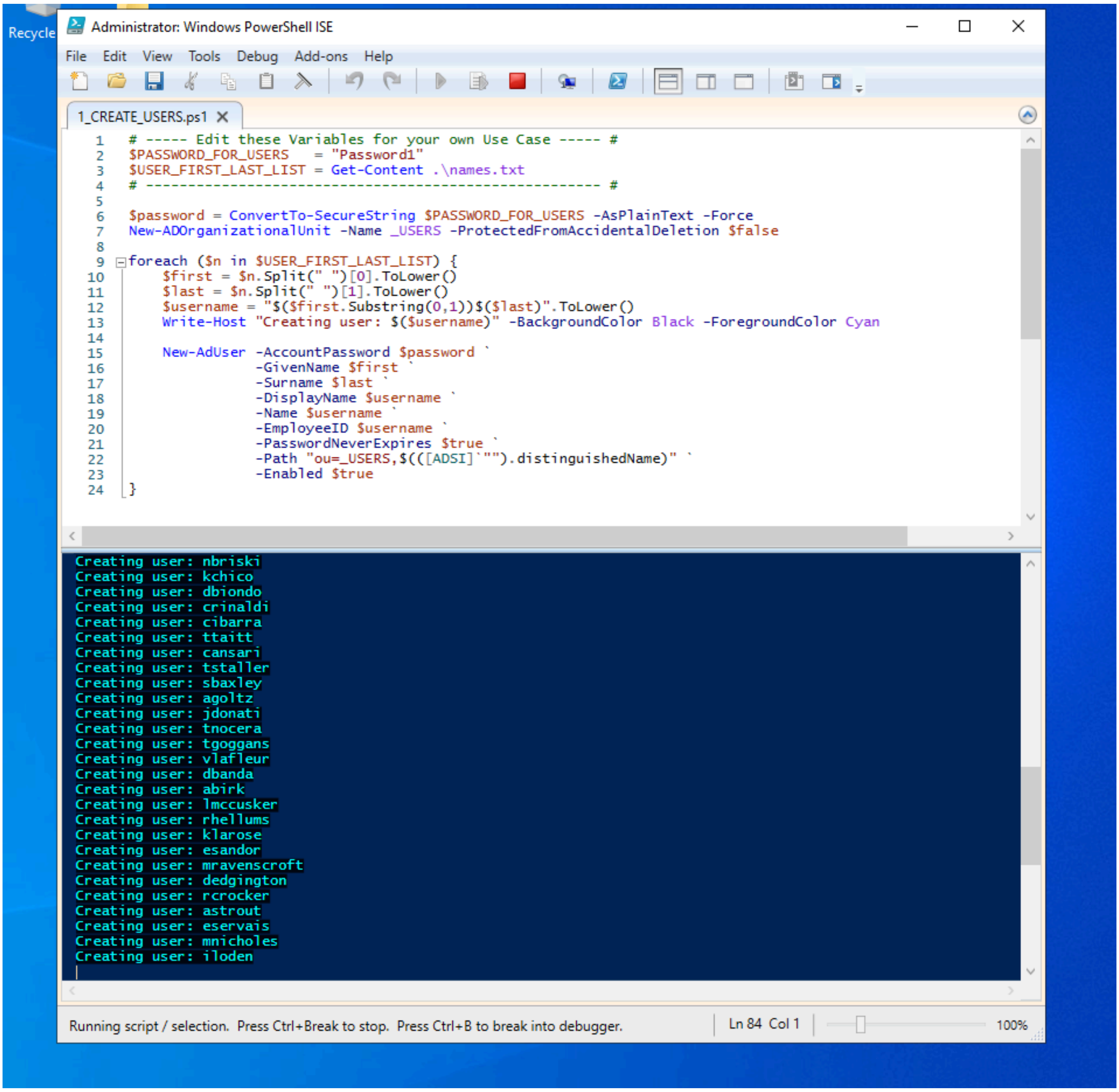
PowerShell ISE was used to write a script utilizing the New-ADUser command. The script reads usernames from the text file and assigns a default password.



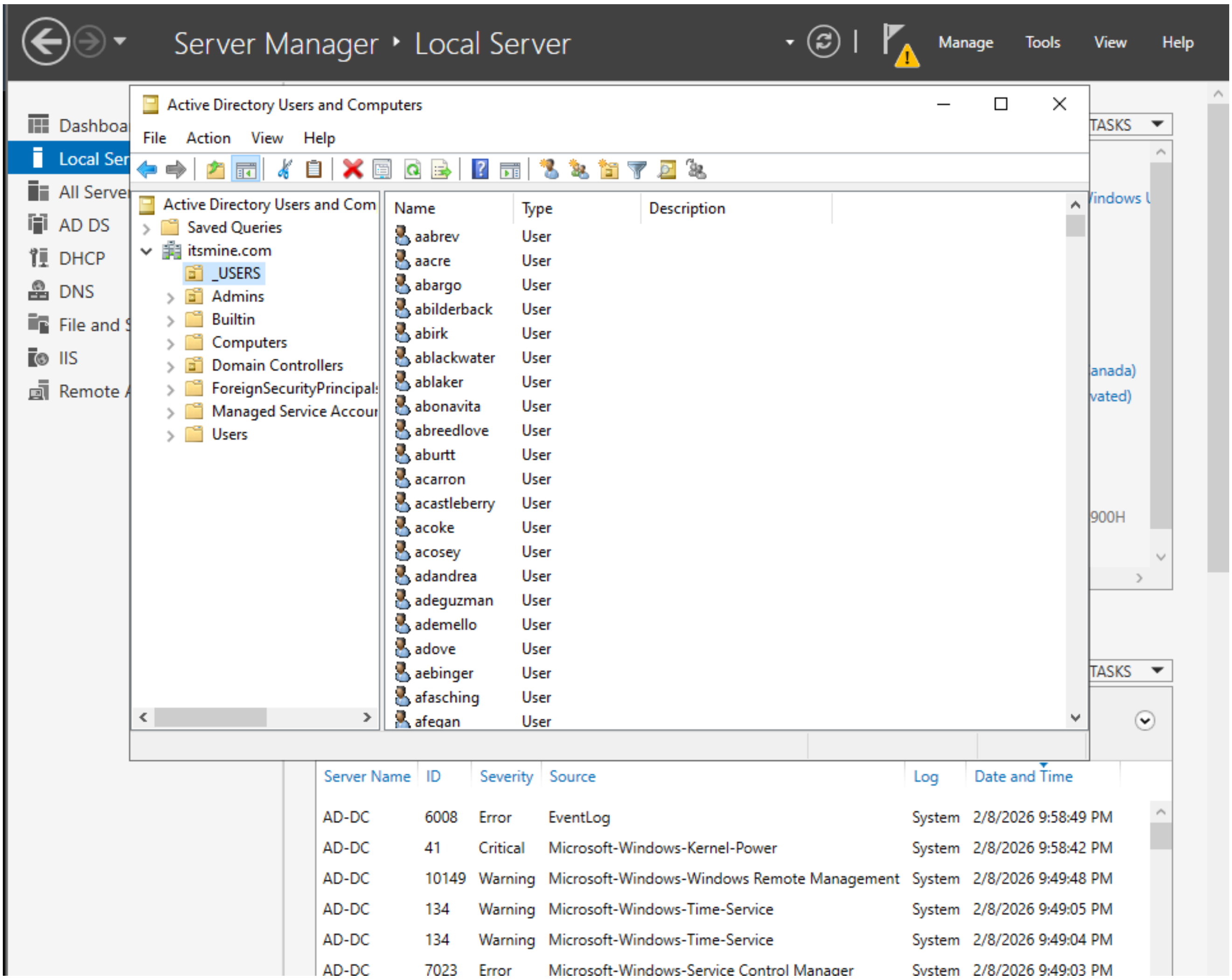
Execution policy was set to Unrestricted to allow script execution. The script directory was verified before running the automation.



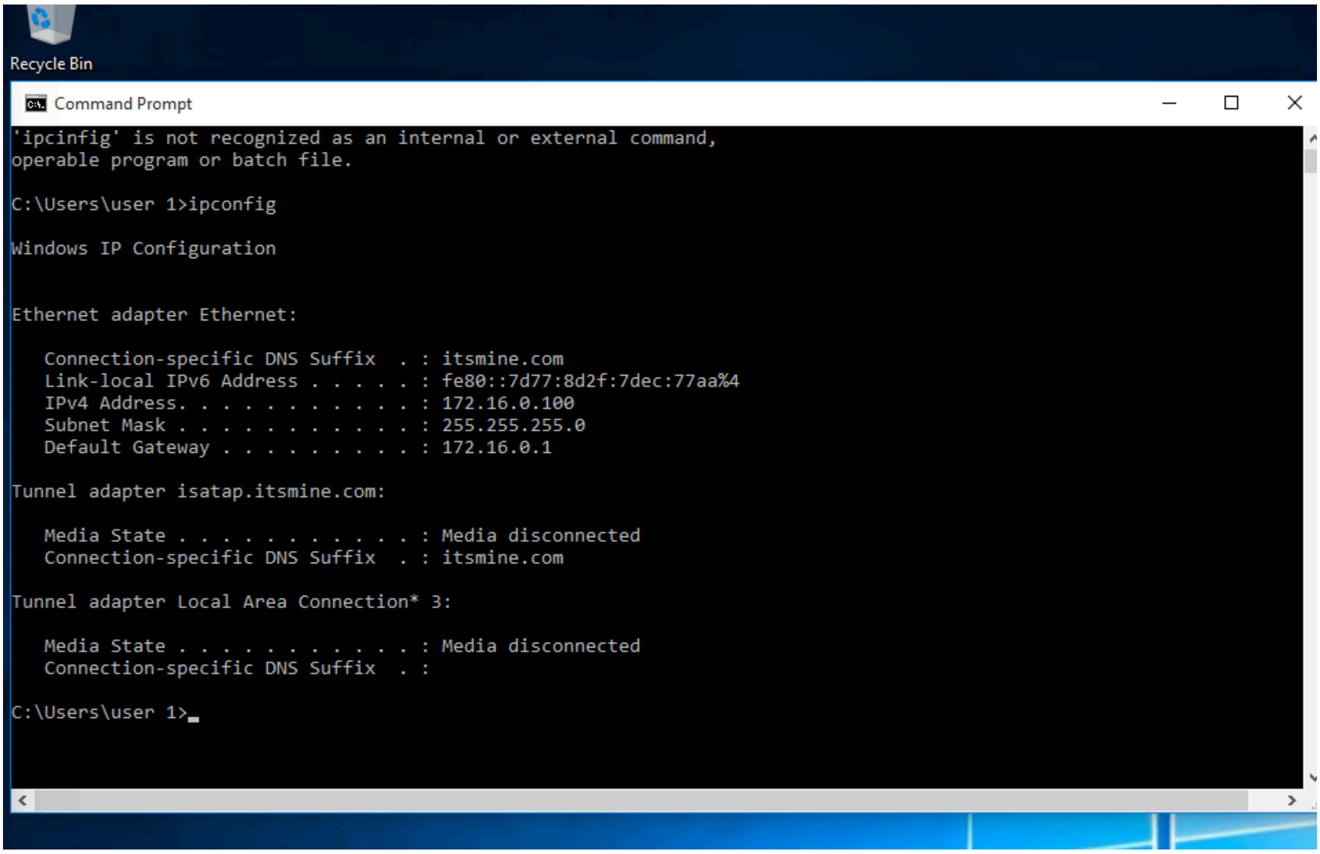
The PowerShell script was executed to automatically create multiple domain user accounts. The console output confirms successful user creation.



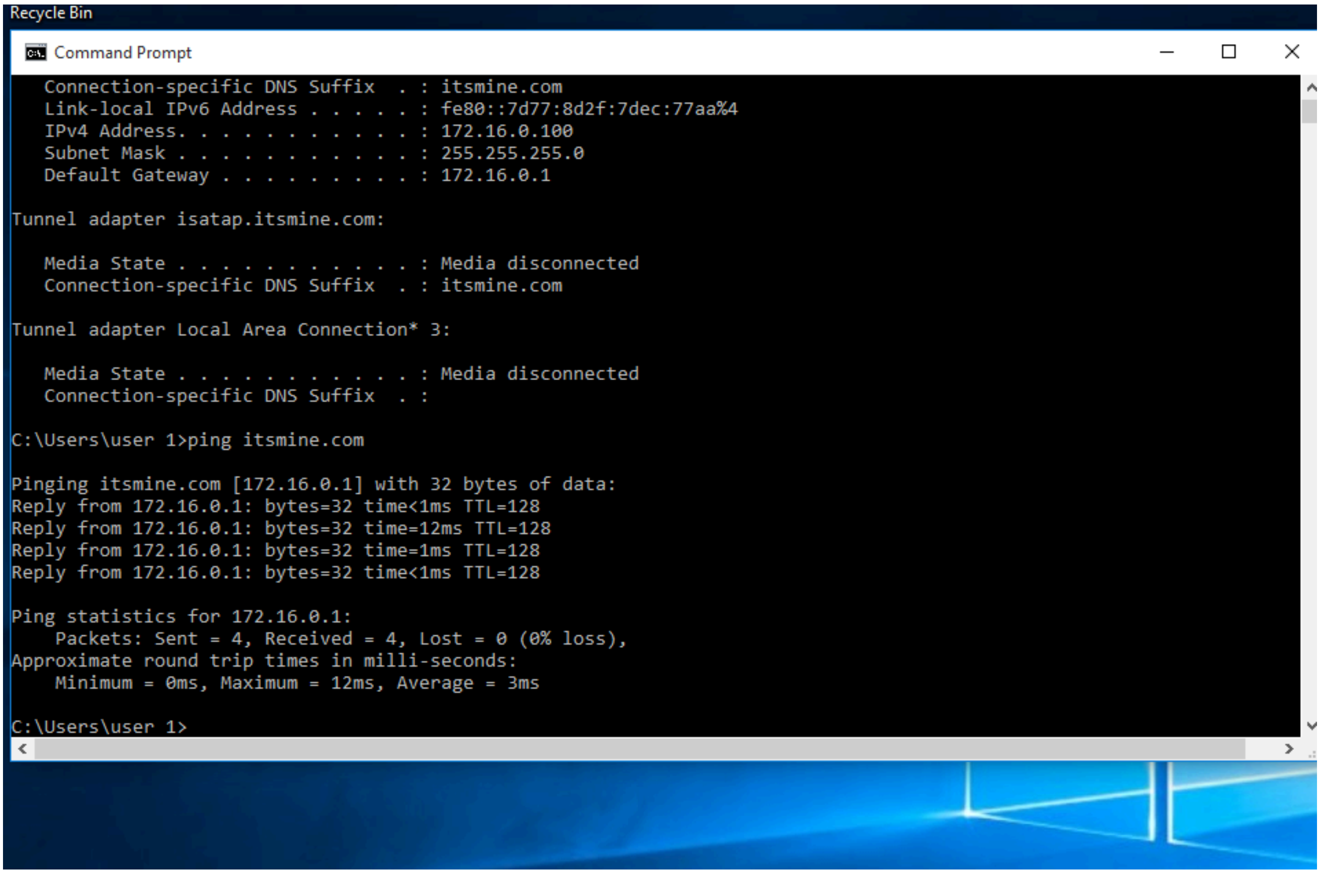
Active Directory Users and Computers console displays newly created bulk users. This verifies successful automation.



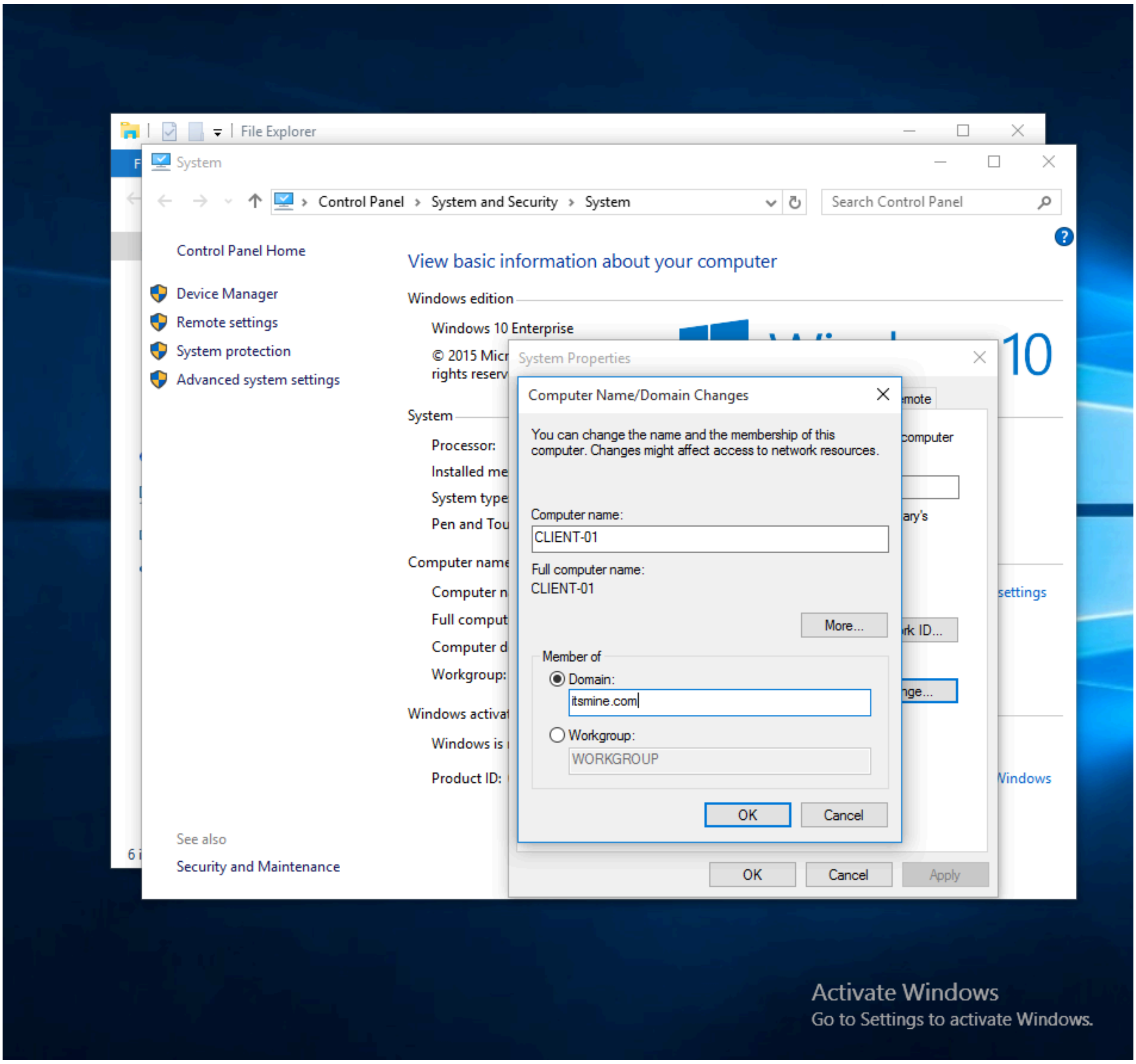
ipconfig command was executed on the client machine. The client received an IP address within the configured DHCP range.



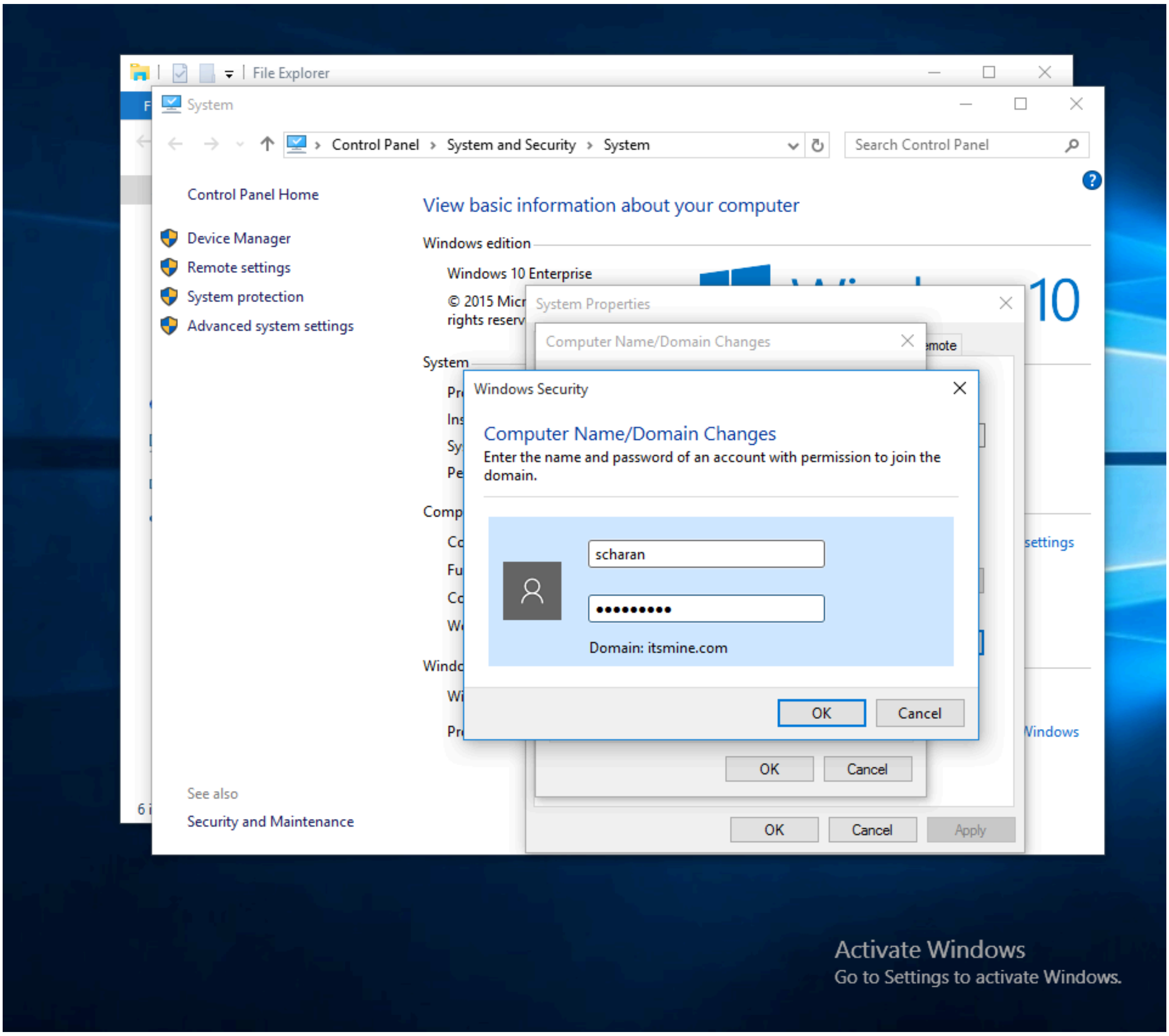
Ping test to itsmine.com was performed from the client machine. Successful replies confirm DNS resolution and network connectivity.



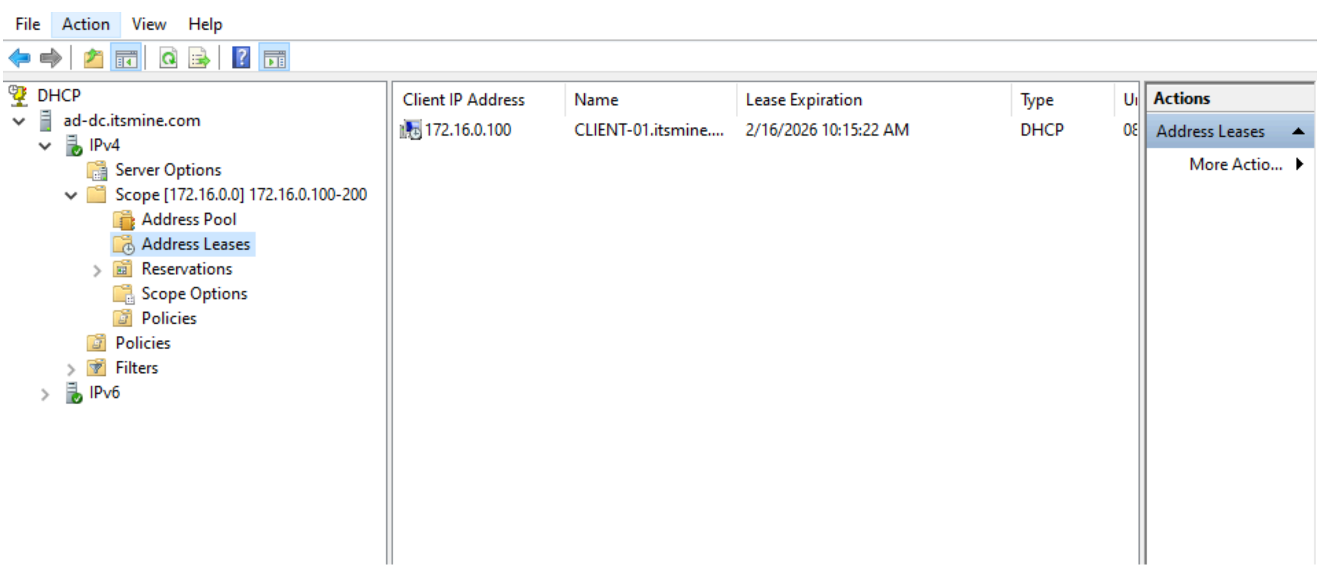
System Properties were opened to join the Windows 10 machine to the itsmine.com domain. Domain membership option was selected.



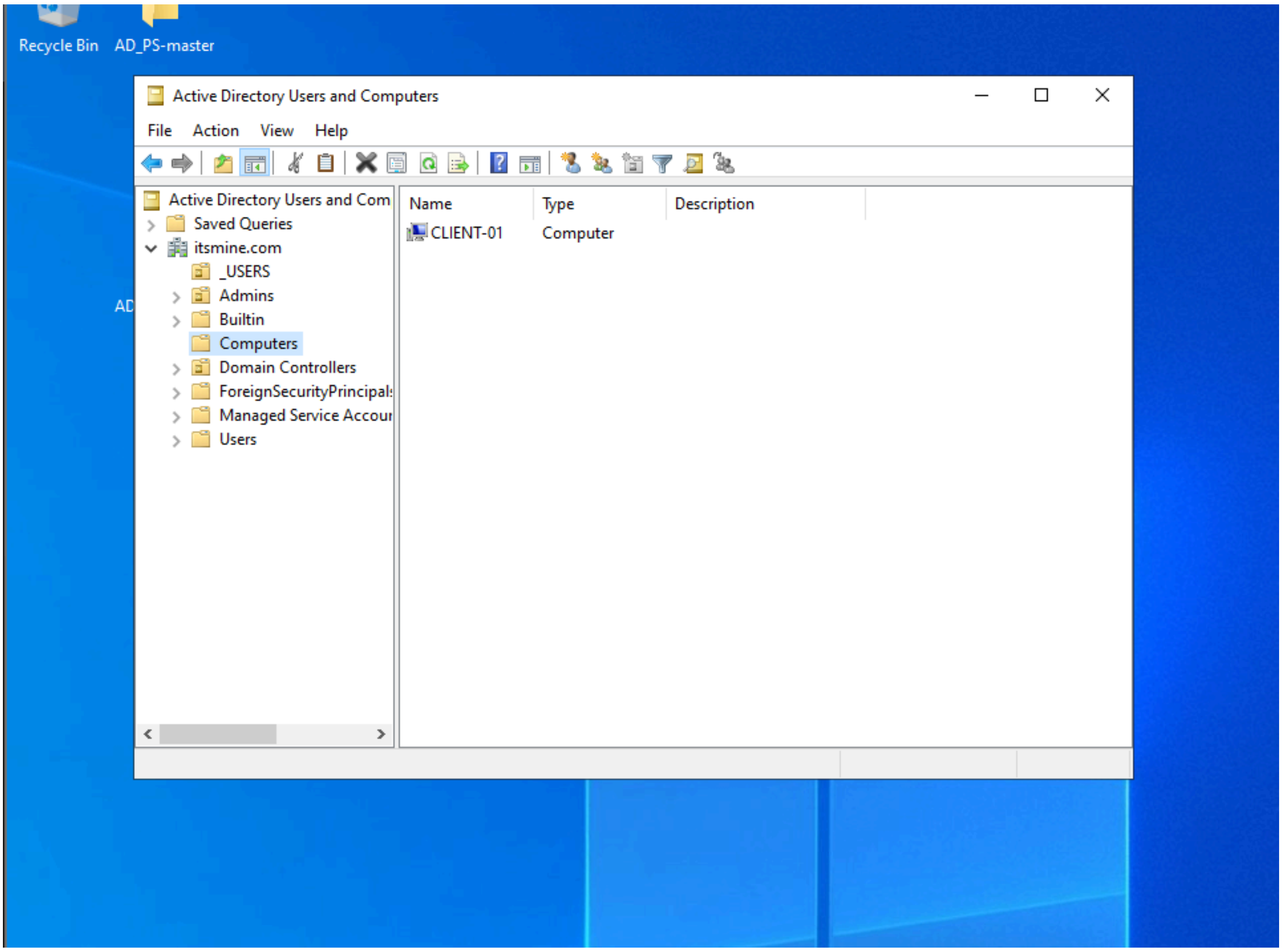
Domain administrator credentials were entered to authenticate domain join. The client machine was successfully added to the domain.



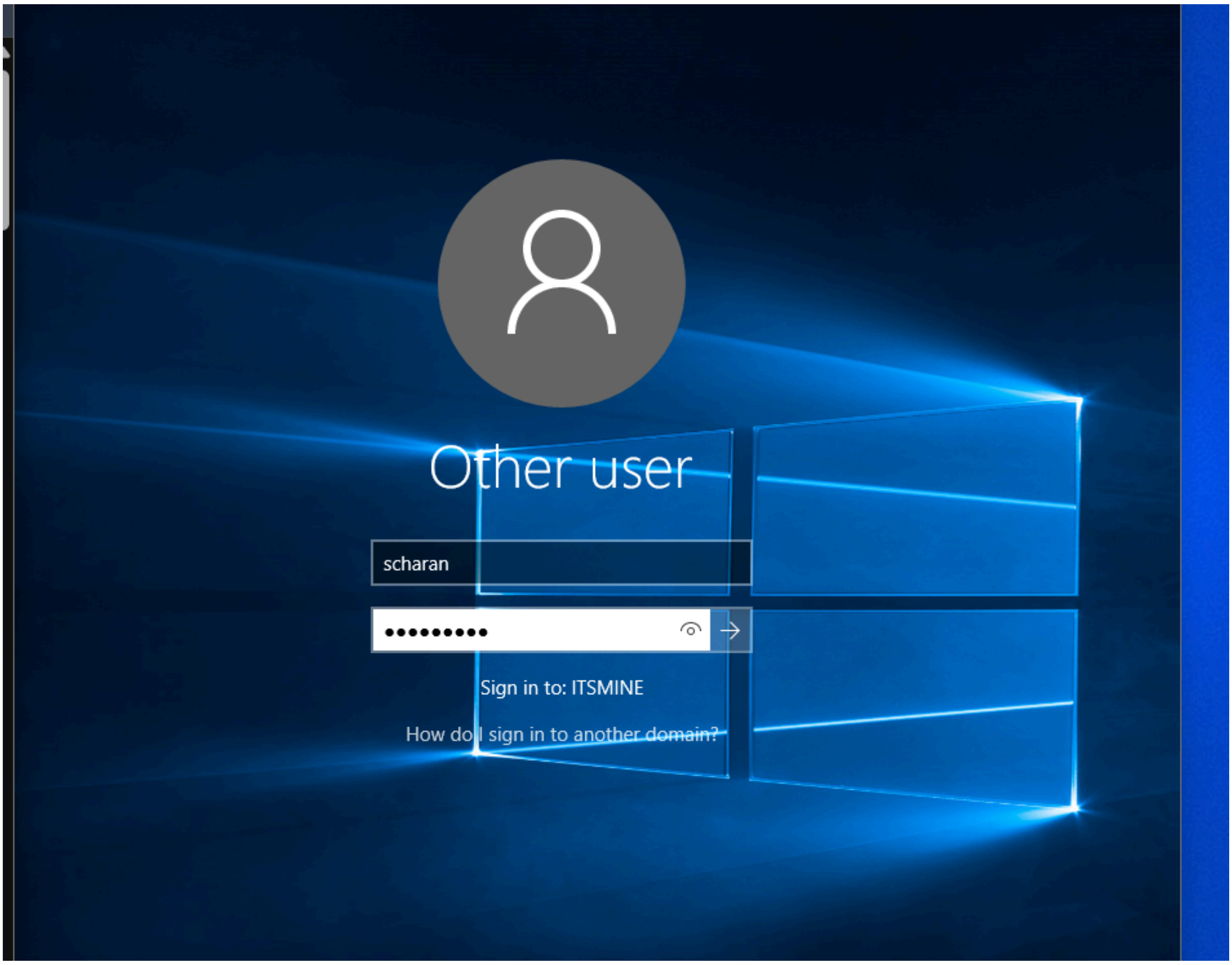
DHCP console shows an active lease assigned to the client machine. This confirms proper IP allocation from the DHCP server.



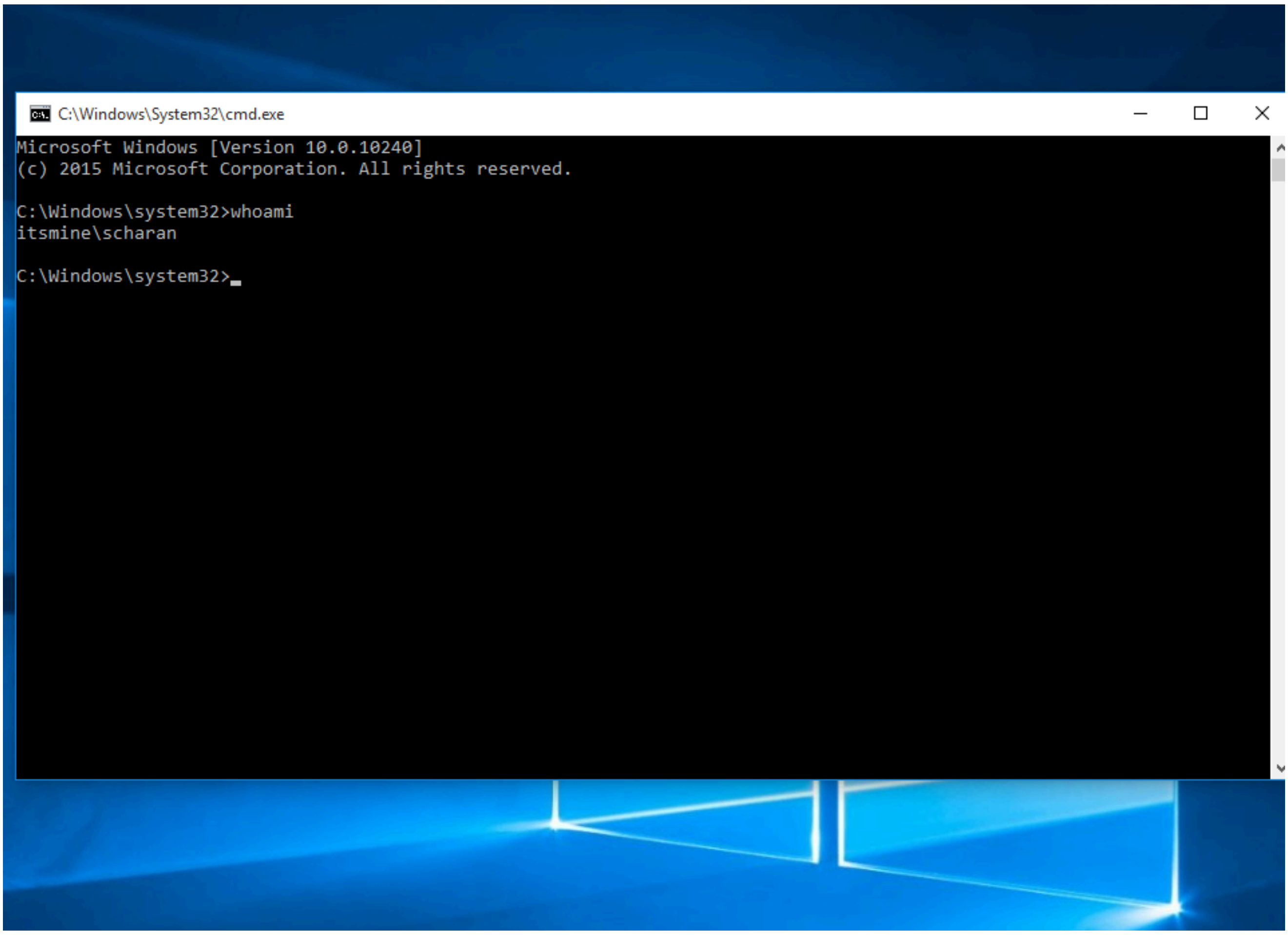
After joining the client system to the domain, the computer account (CLIENT-01) was automatically created inside Active Directory. This confirms successful domain integration of the Windows 10 machine.



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.

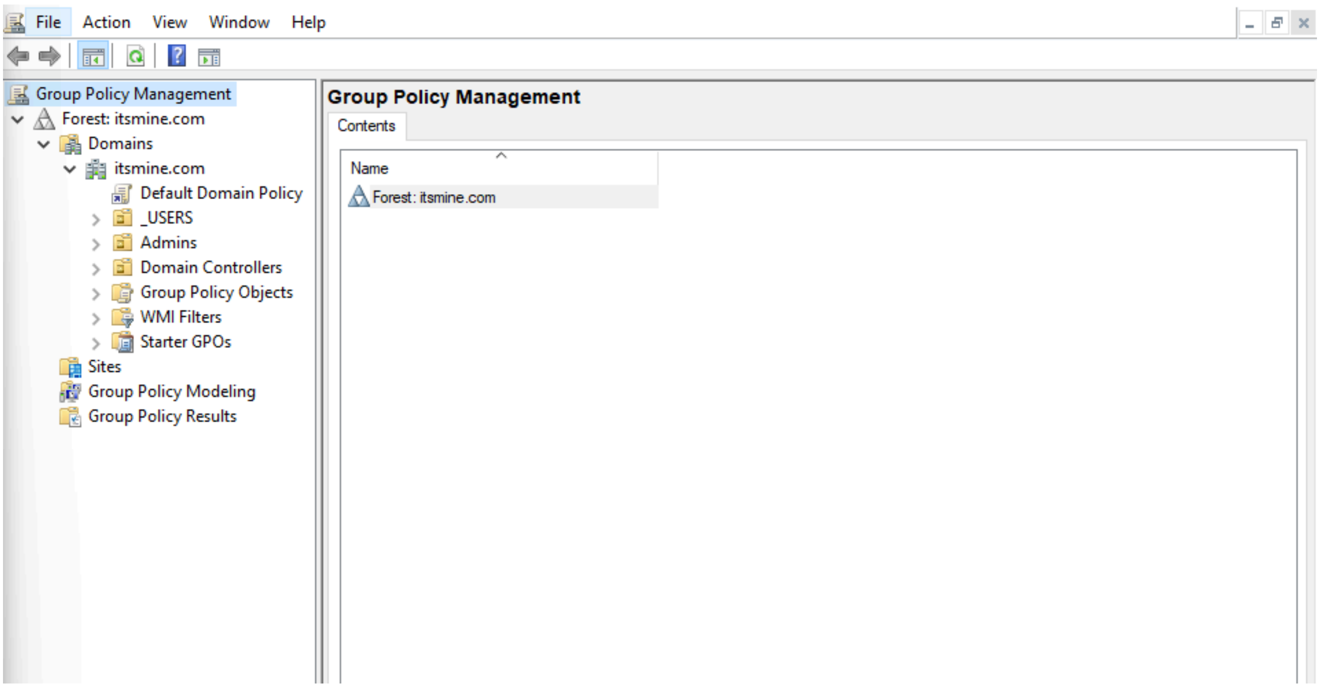


Command Prompt access after login confirms that the user session is active and functioning under domain credentials.

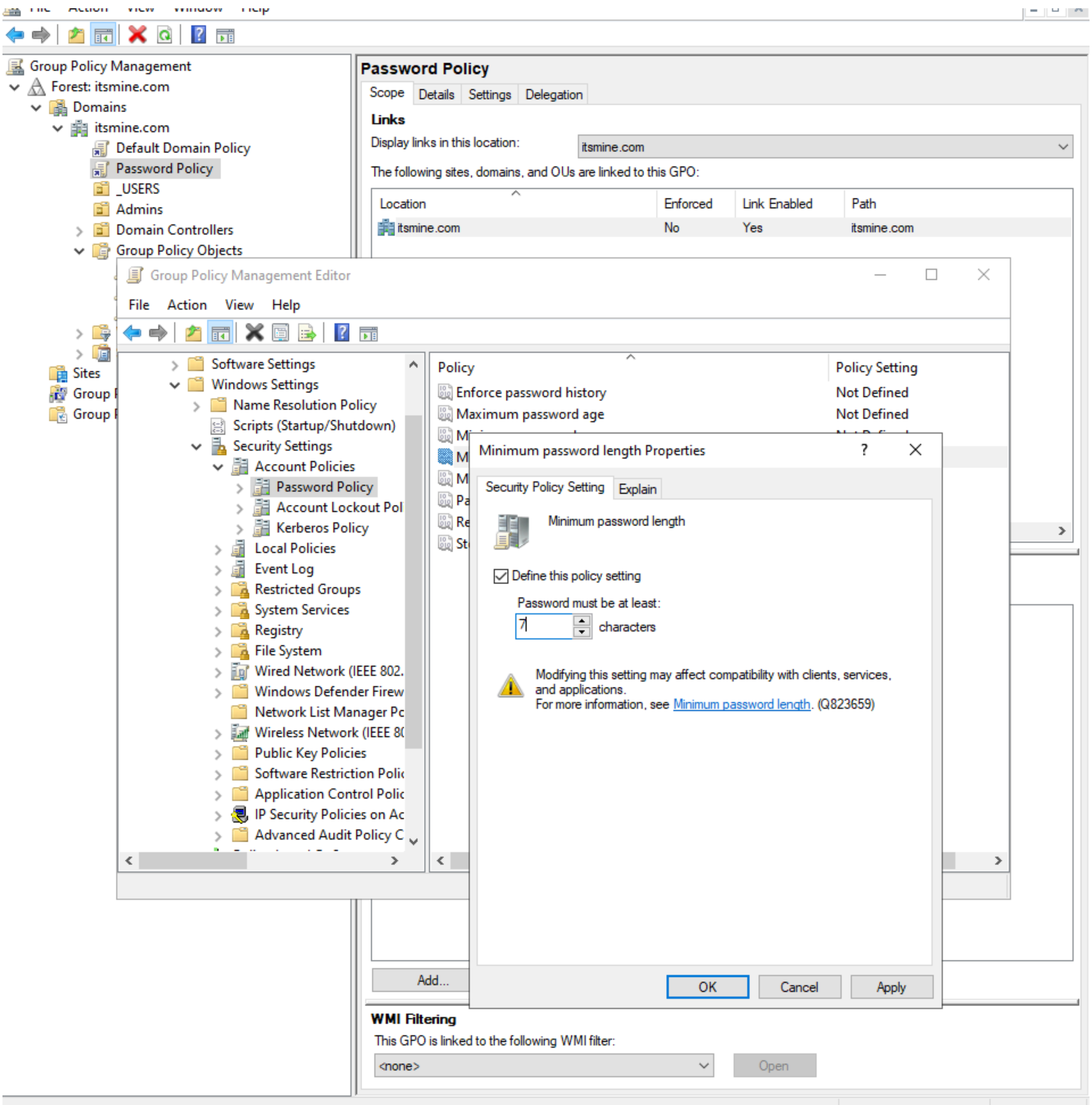


GROUP POLICY MANAGEMENT :

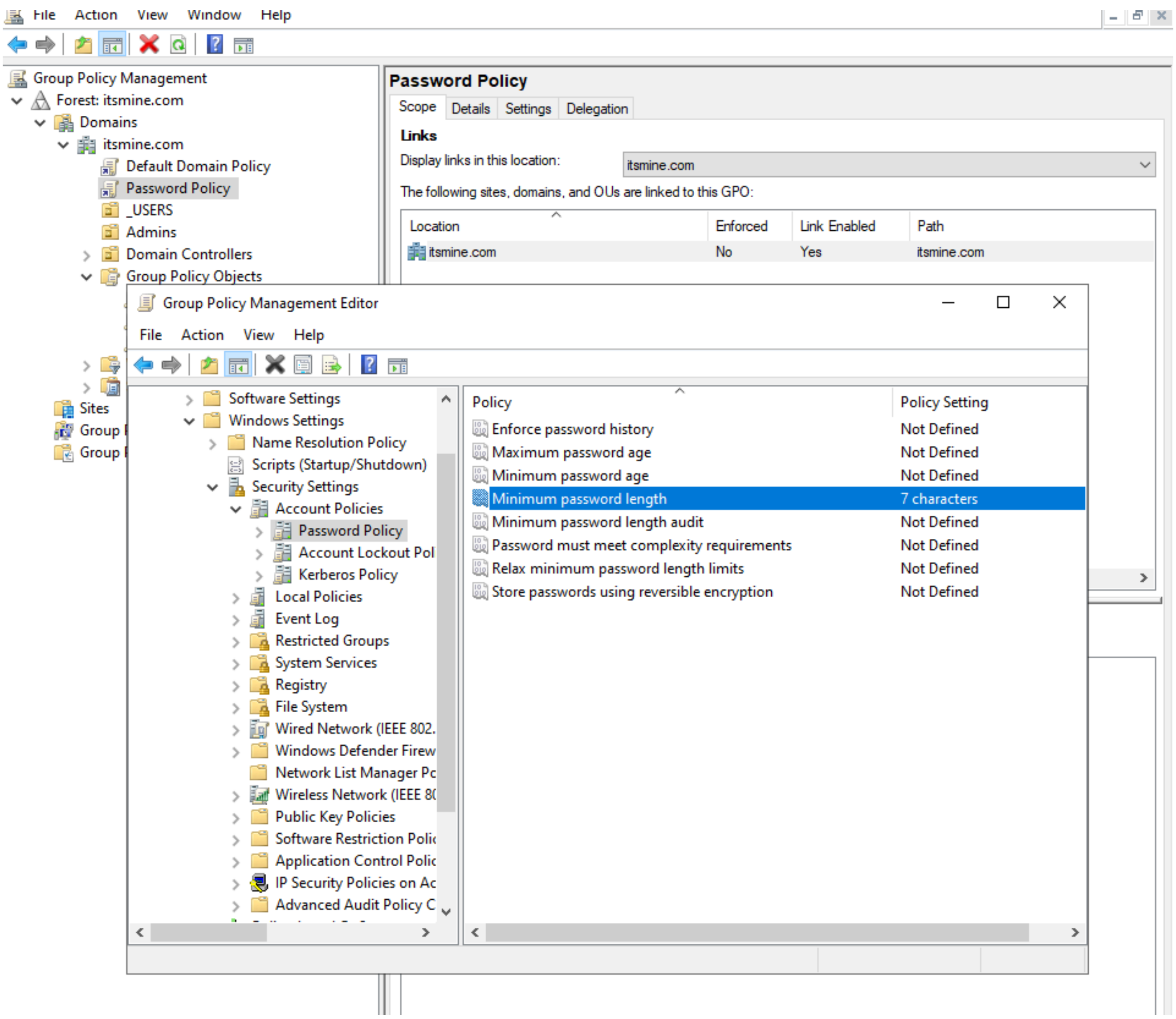
A Password Policy GPO was created in Group Policy Management to enforce strong password standards across the domain. This ensures centralized control of authentication security.



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

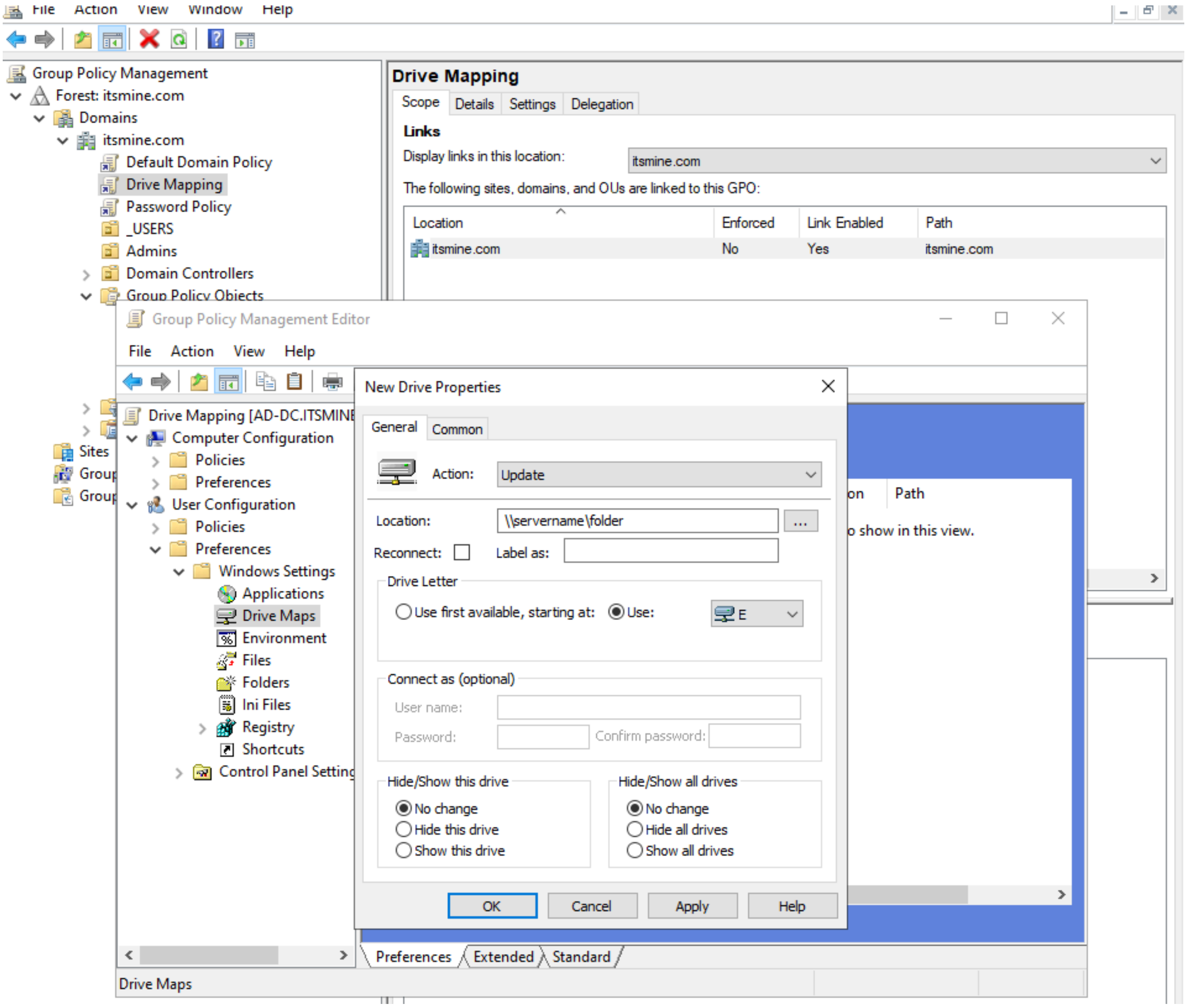


The Password Policy GPO was linked at the domain level to ensure it applies to all domain users. This guarantees uniform password enforcement.Password settings such as length and complexity were defined under Security Settings. These configurations prevent simple and predictable passwords

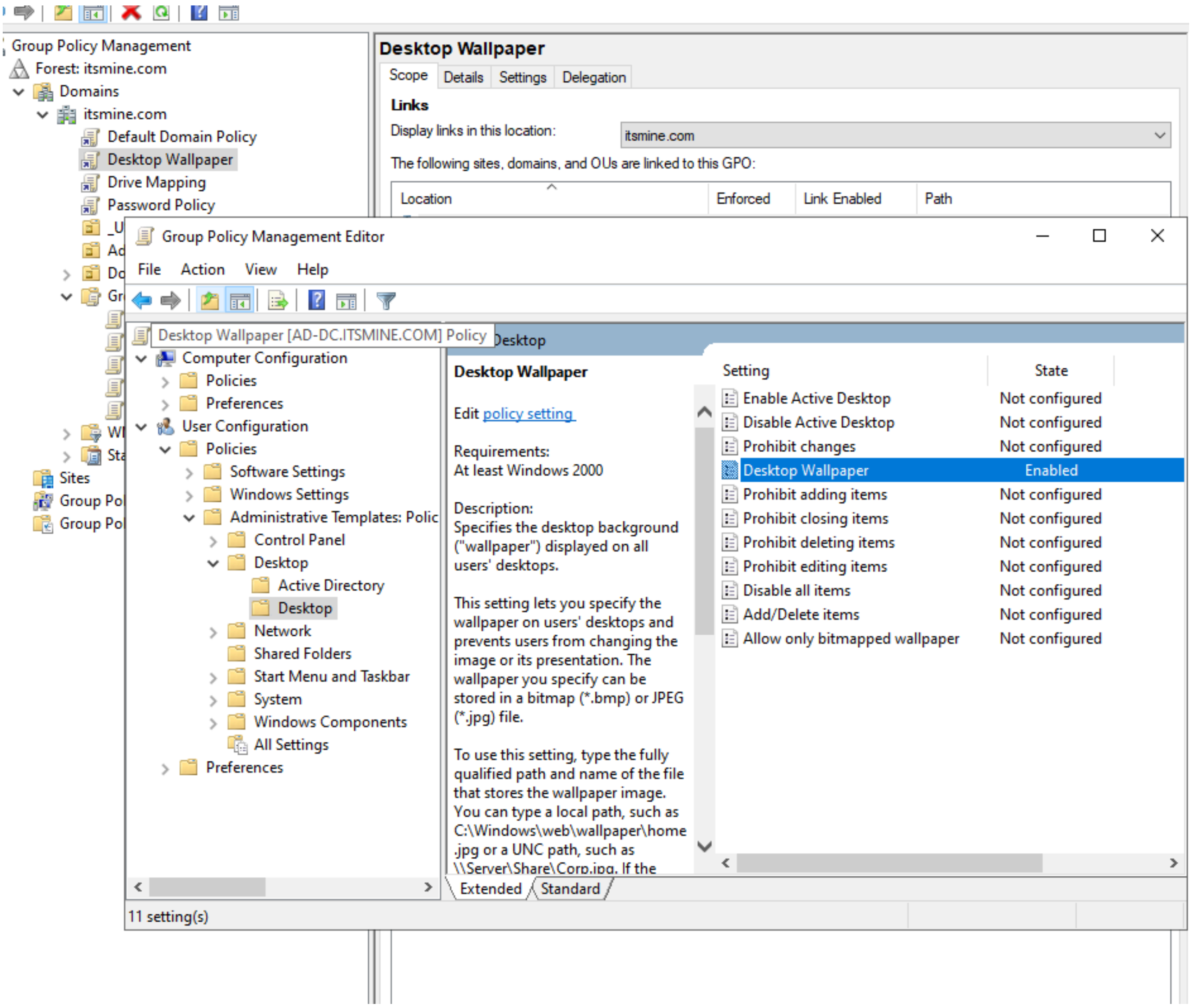


A Drive Mapping policy was created under User Configuration to automatically connect users to a shared network drive. This provides centralized access to shared resources.

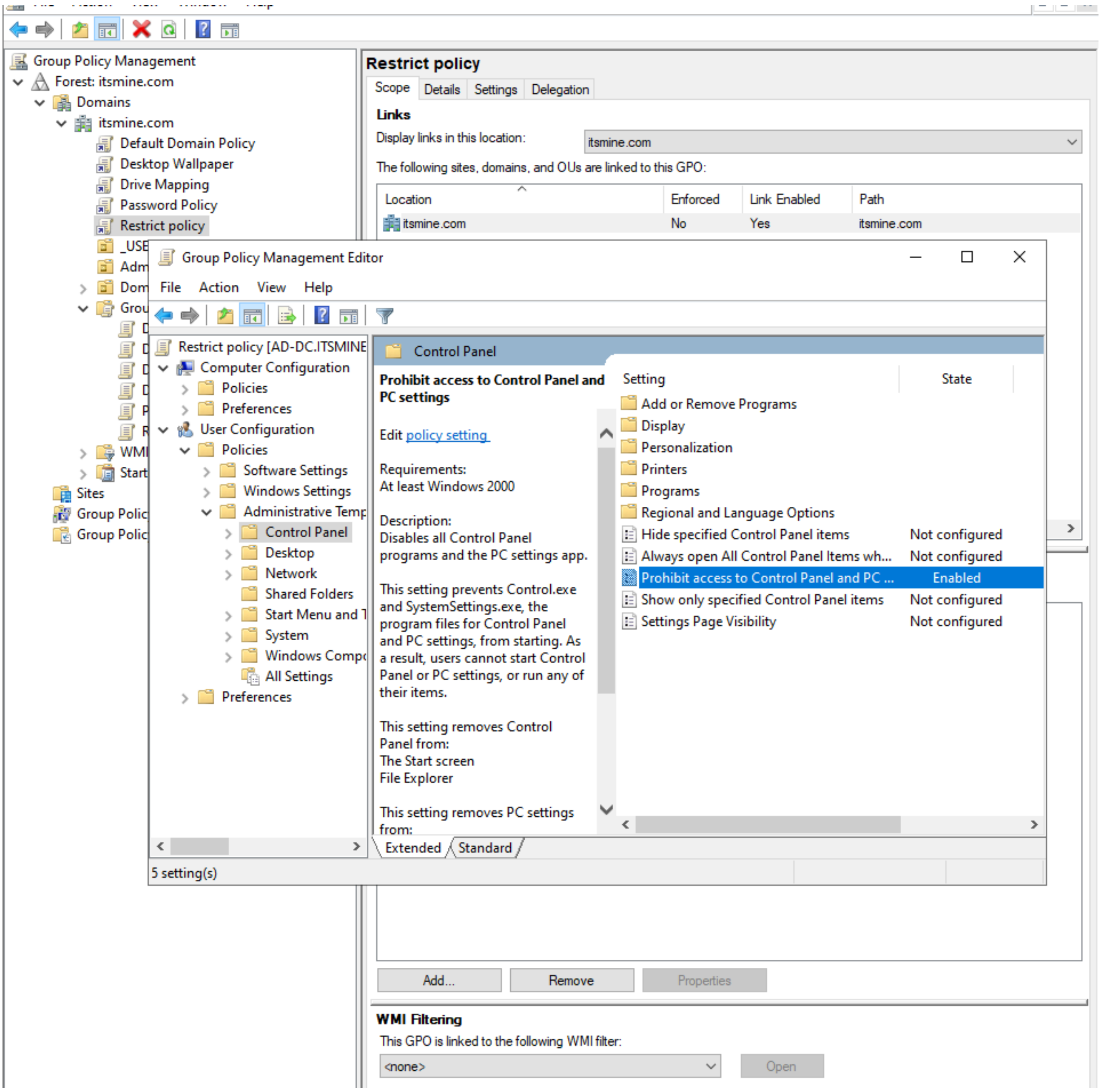
The shared folder path and drive letter were configured so that users receive the mapped drive during login. This eliminates the need for manual mapping.



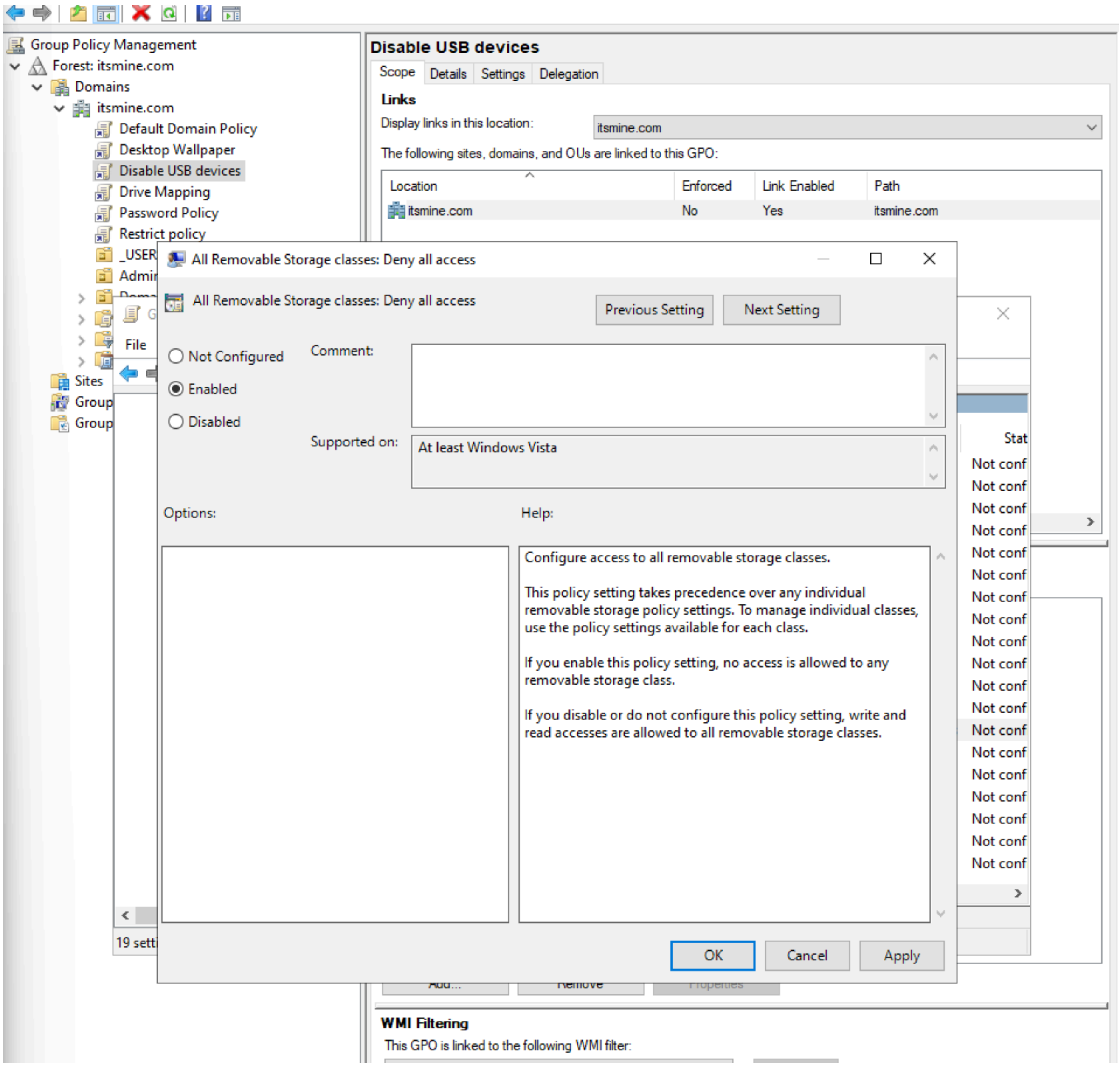
A Desktop Wallpaper policy was implemented to standardize the desktop background for domain users. This enforces consistent visual configuration across systems.The wallpaper setting was enabled and linked to the domain, ensuring automatic application after policy refresh.



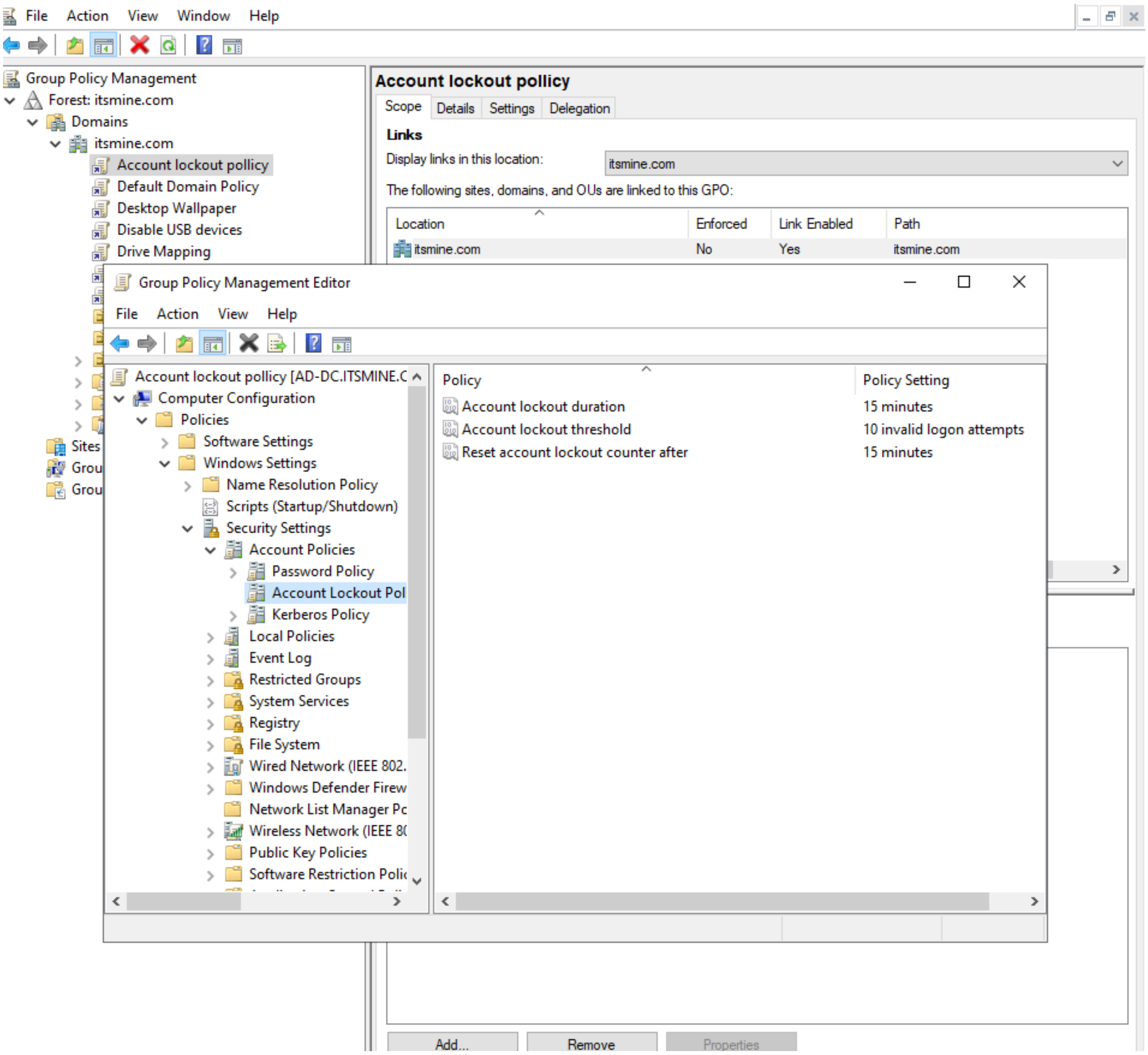
A Restrict Policy was configured to limit access to certain system features. This helps prevent unauthorized system modifications.Control Panel and PC settings access were disabled using Group Policy. This restricts users from altering important configurations.



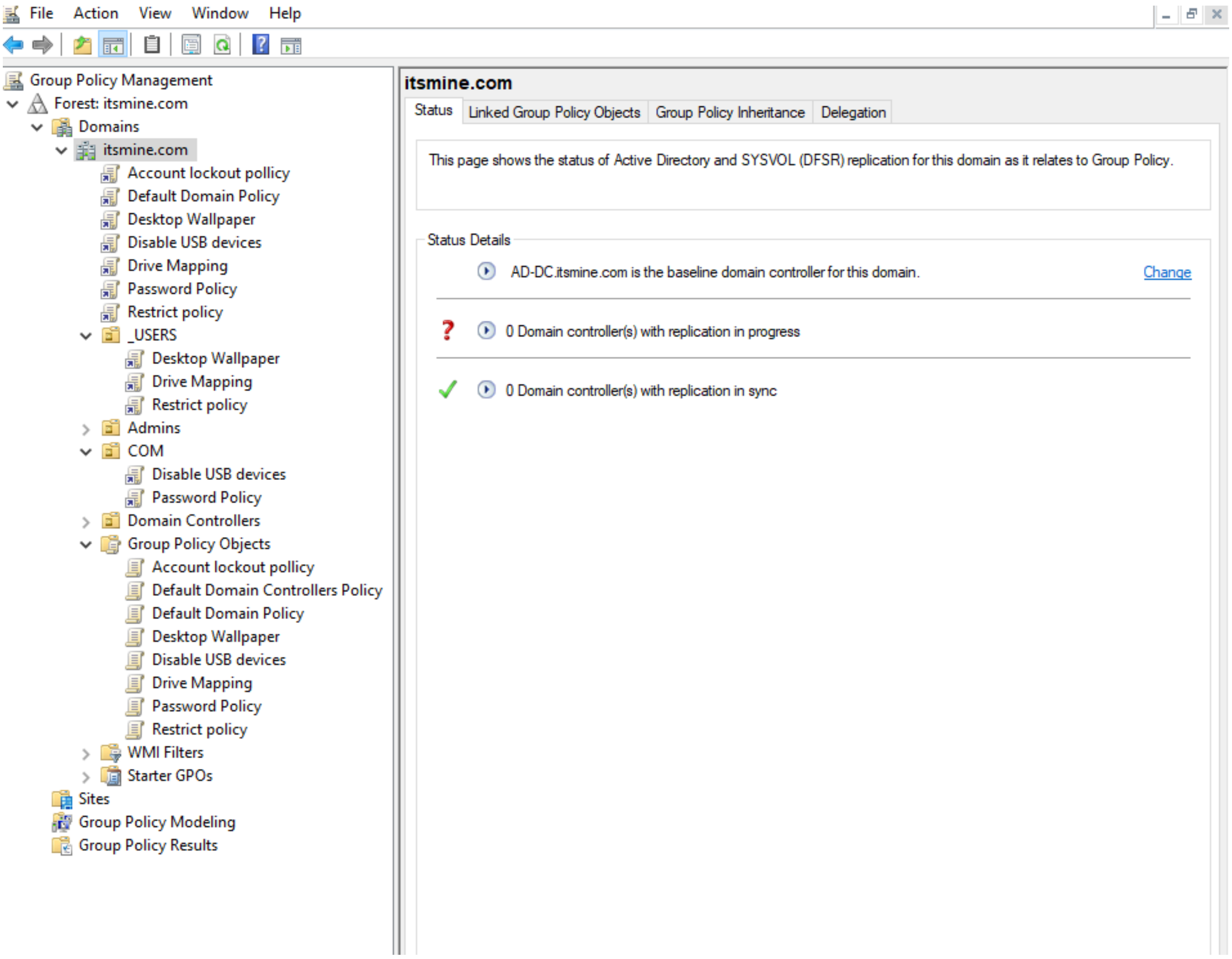
A removable storage restriction policy was implemented to enhance endpoint security. This controls the use of external storage devices. All USB storage access was blocked by enabling the “Deny all access” option. This prevents potential data exfiltration through USB devices.



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.



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



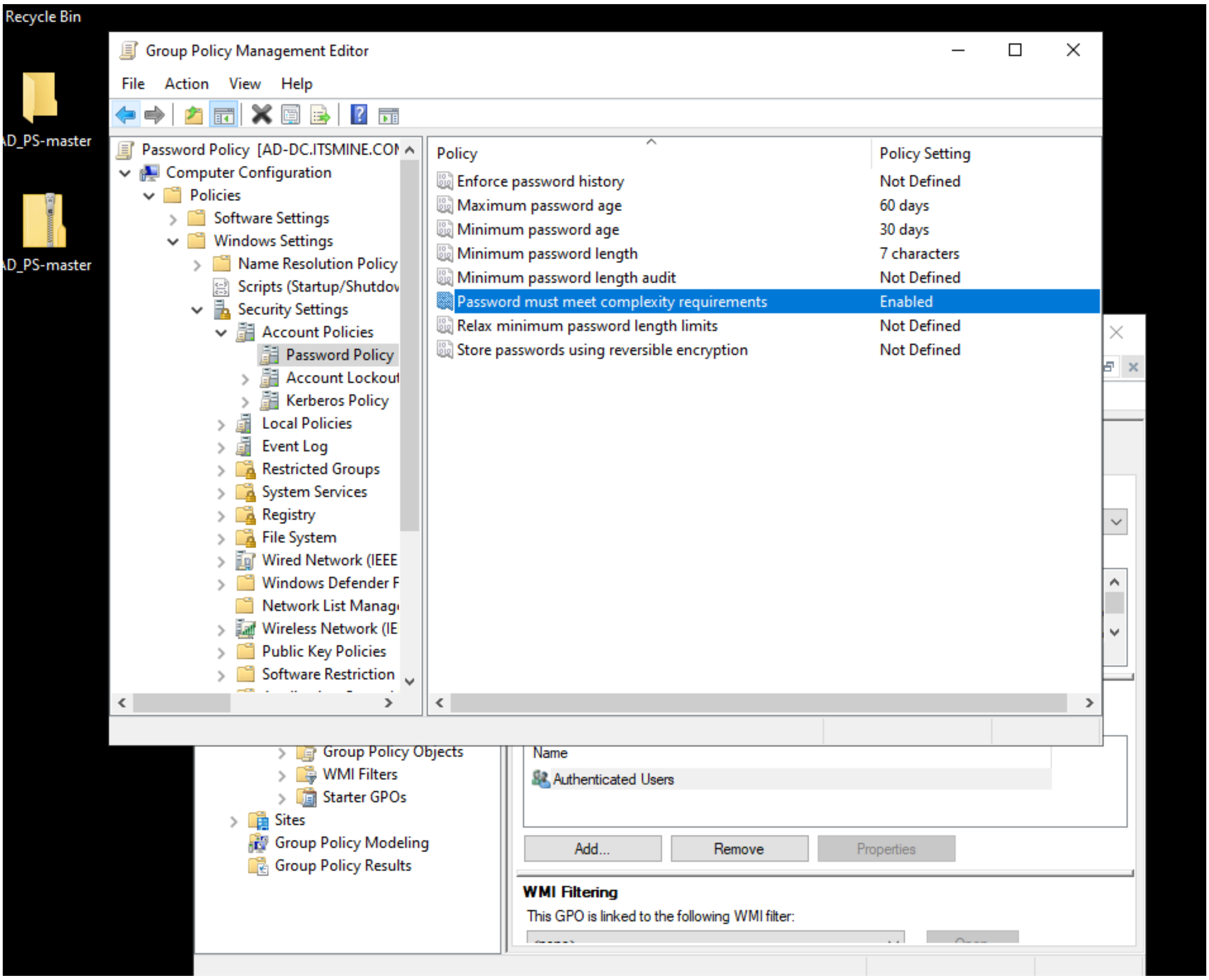
SECURITY POLICY (TESTING) :

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

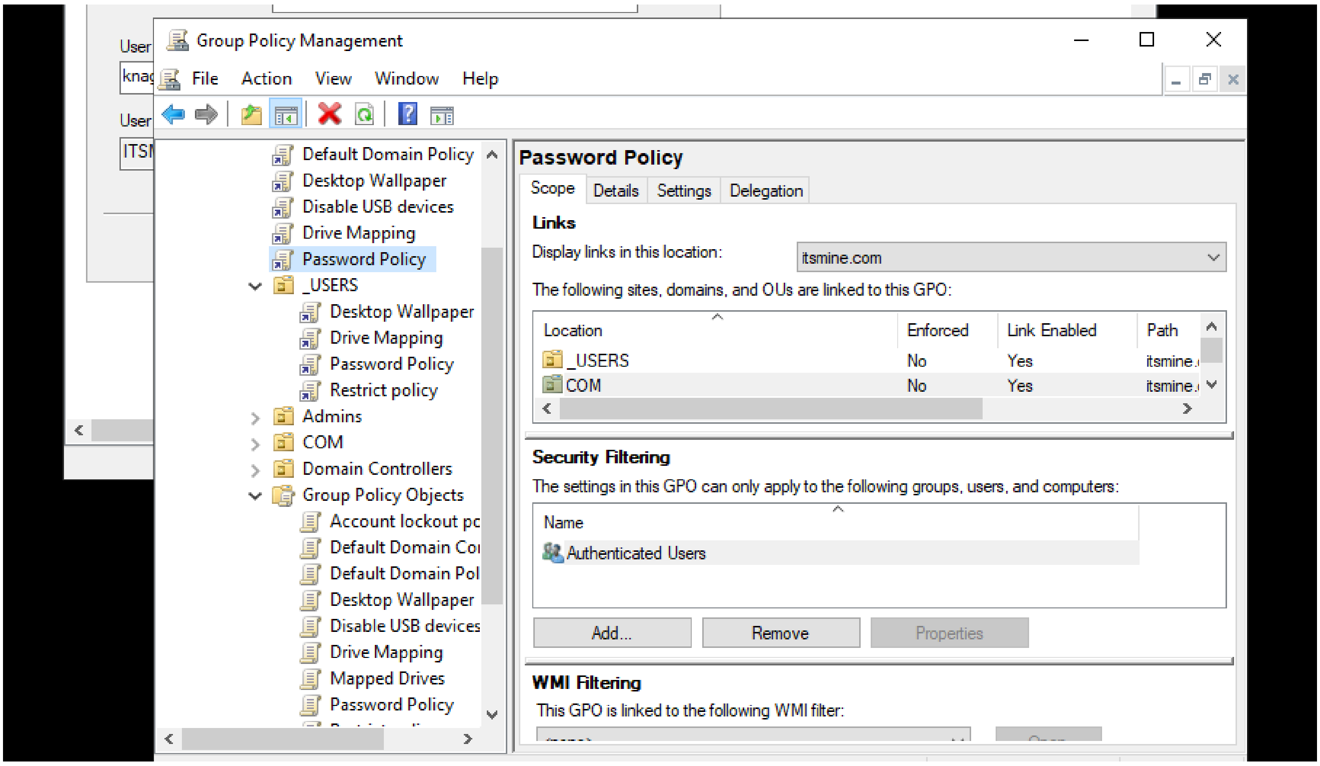
Activity 1: Password Policy Configuration

Configure and enforce a strong password policy for AD users.

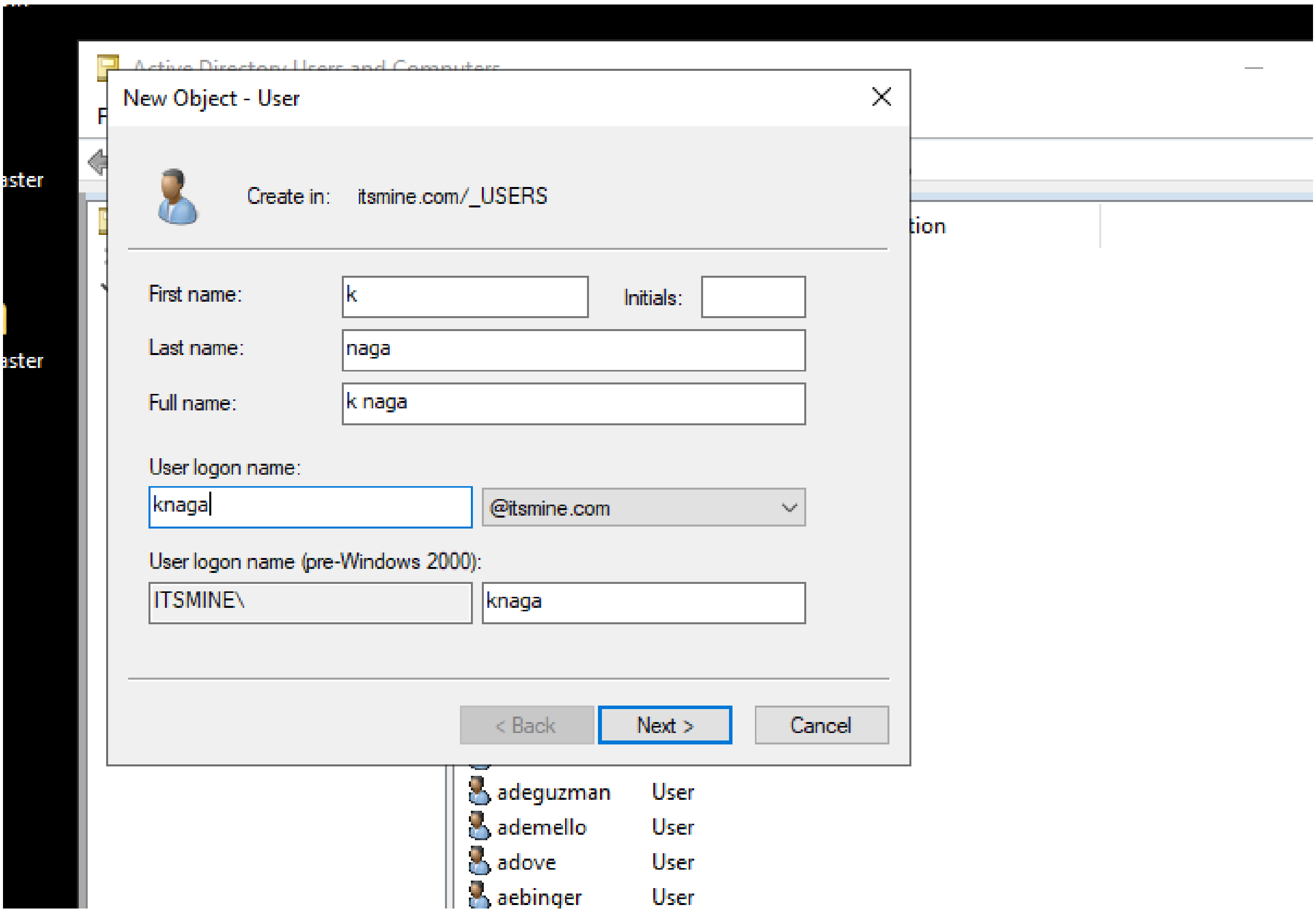
Password Policy settings were reviewed again to validate configuration values such as minimum length and complexity enforcement.



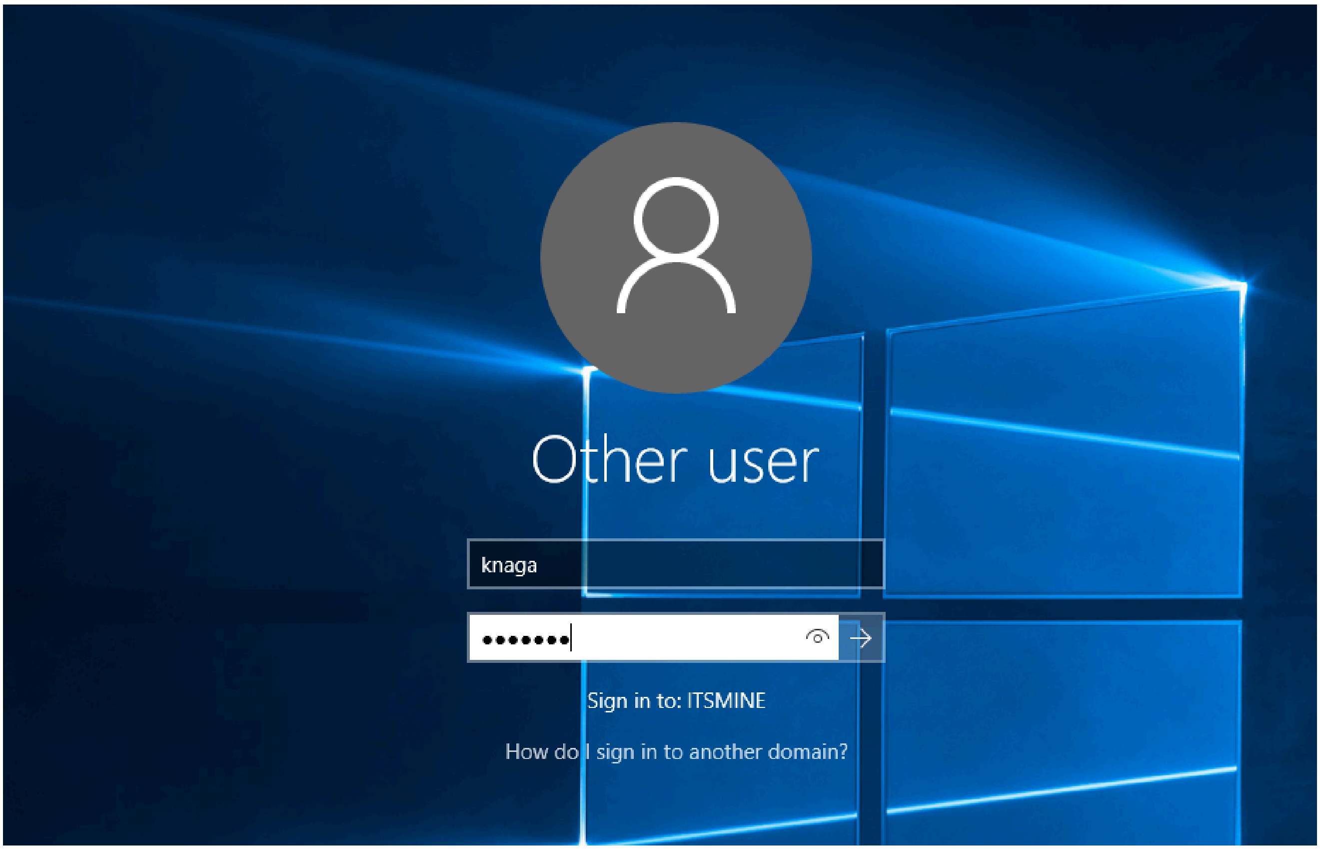
The Password Policy GPO was linked to the required Organizational Unit to ensure it applies to selected users.



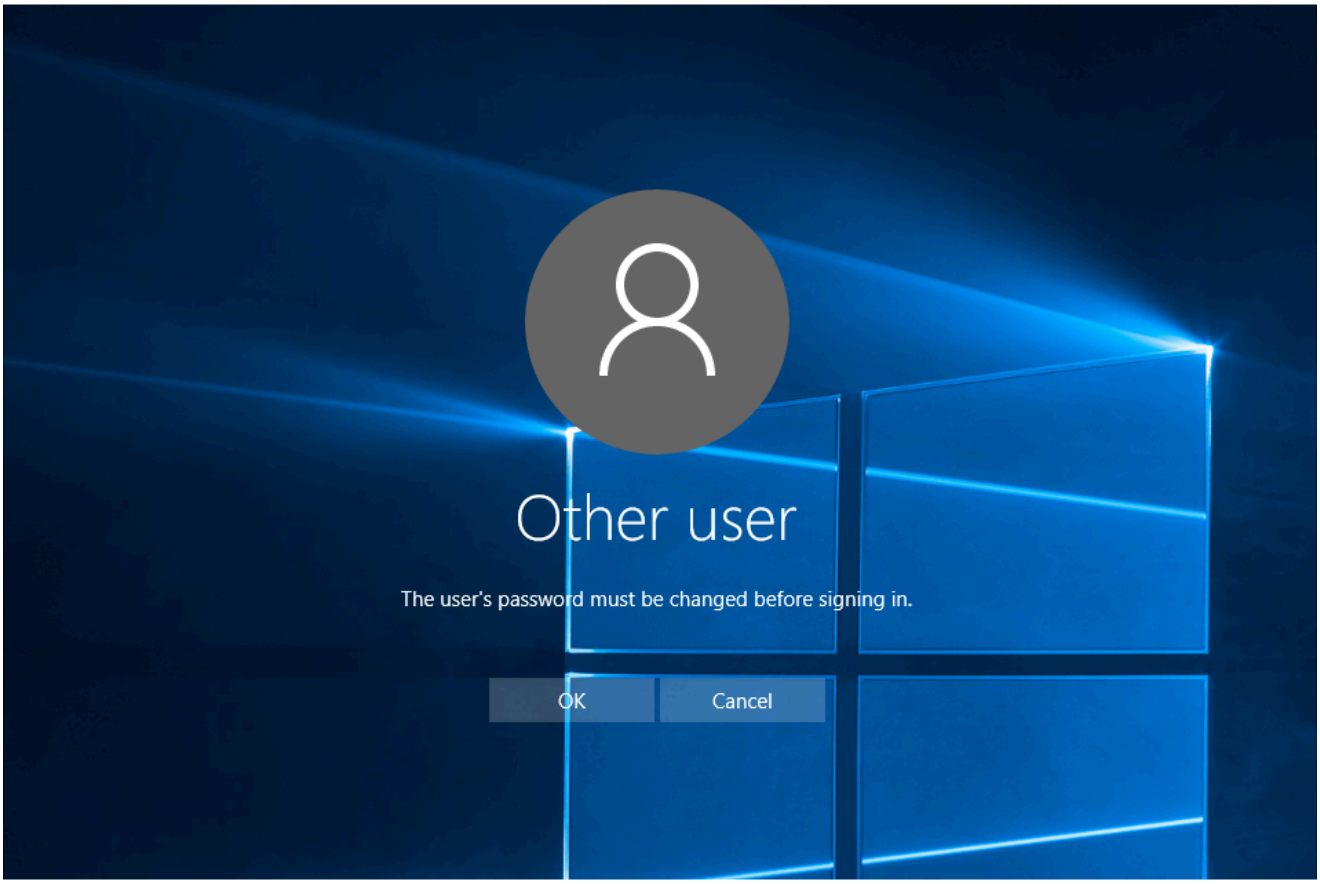
A new test user account was created to validate the password policy behavior under real login conditions.



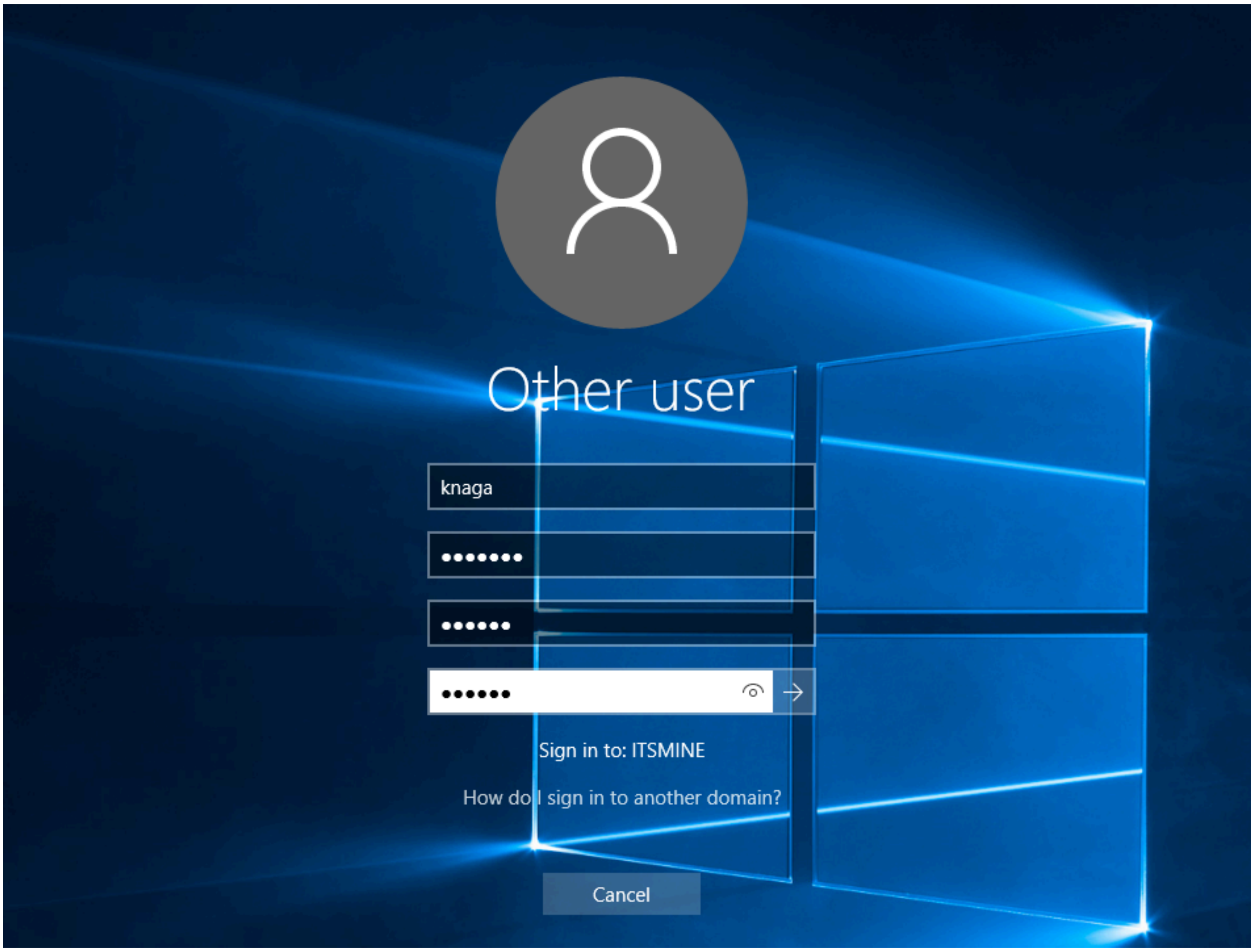
The newly created user attempted login for the first time, triggering a mandatory password change requirement.



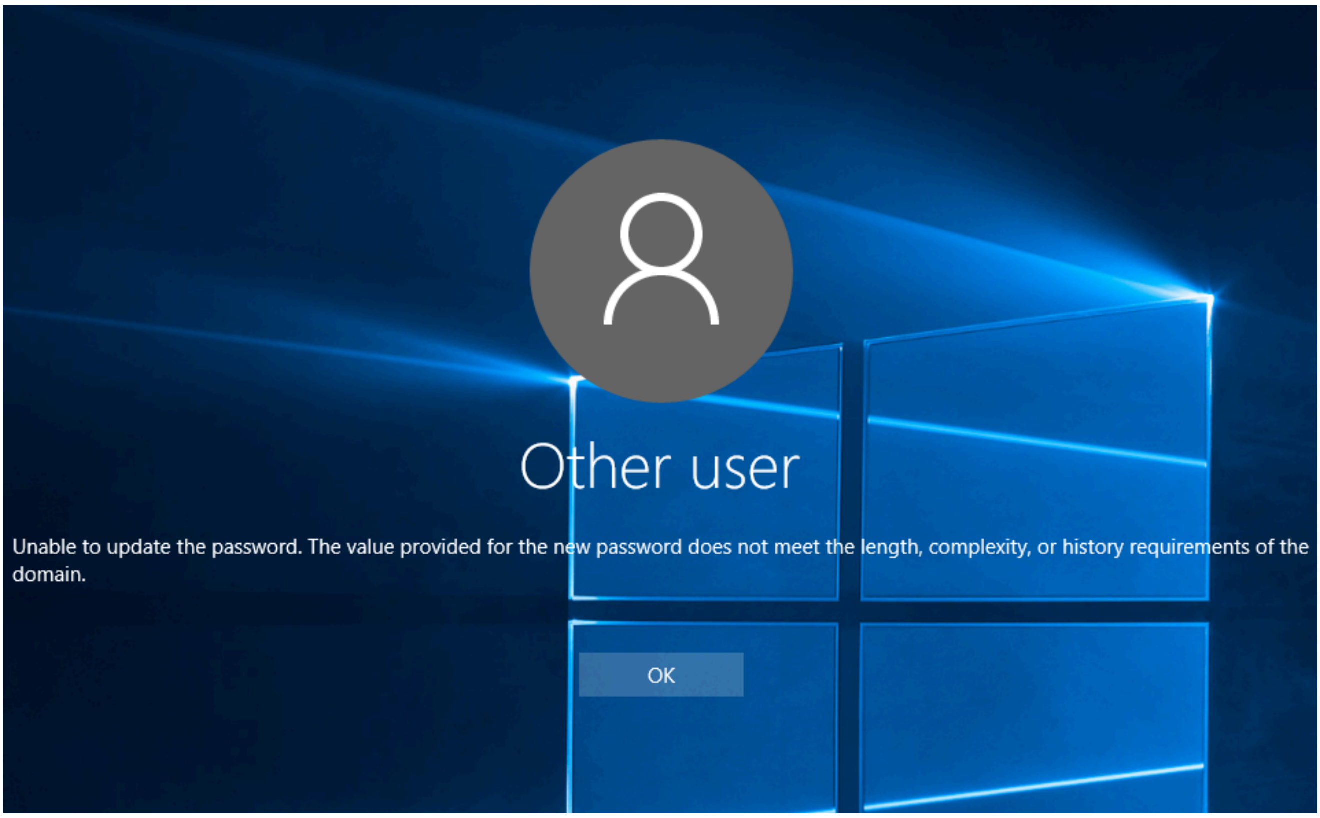
The system enforced password change before granting access, confirming correct policy application.



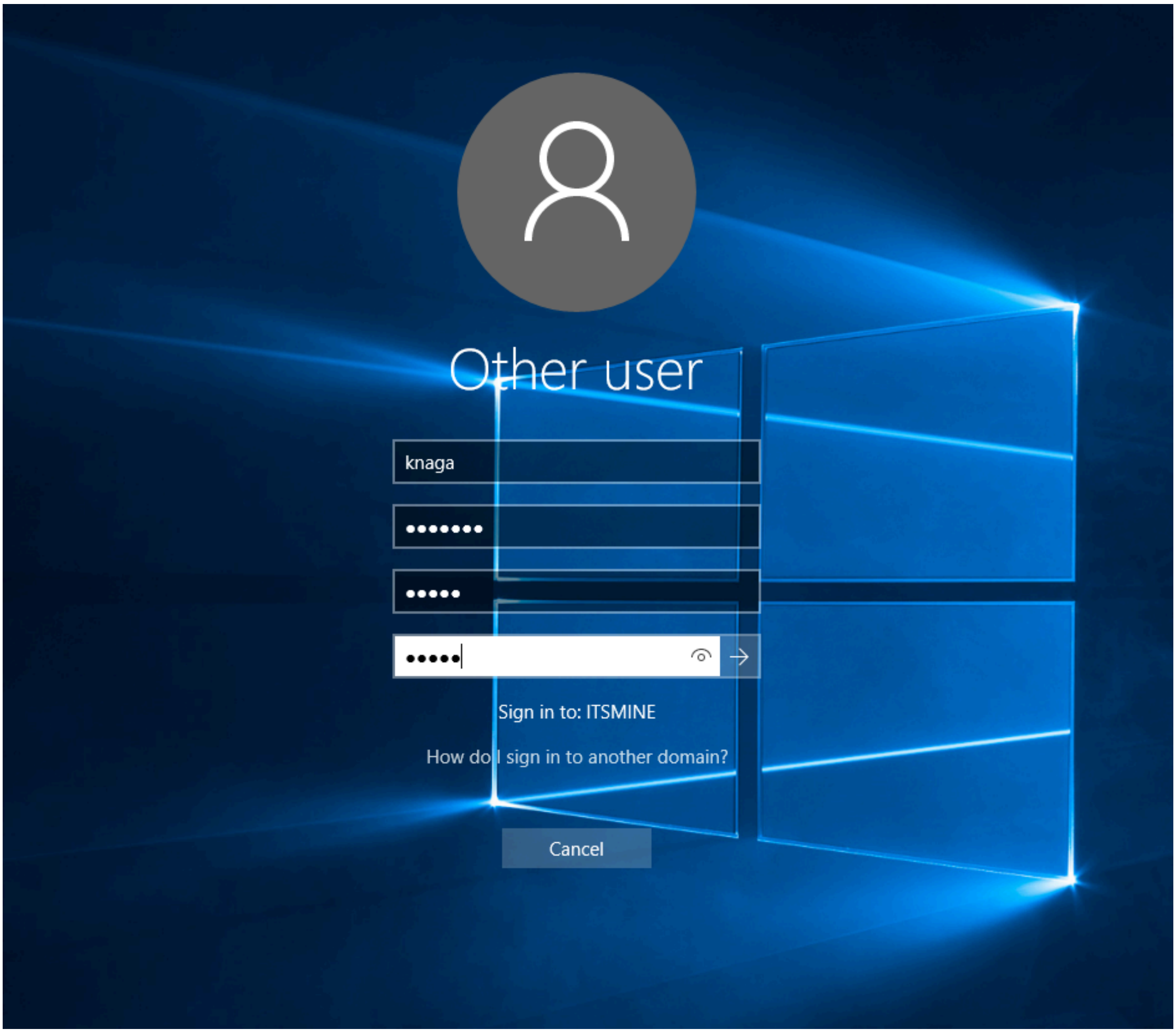
An attempt was made to set a weak password that does not meet policy requirements.



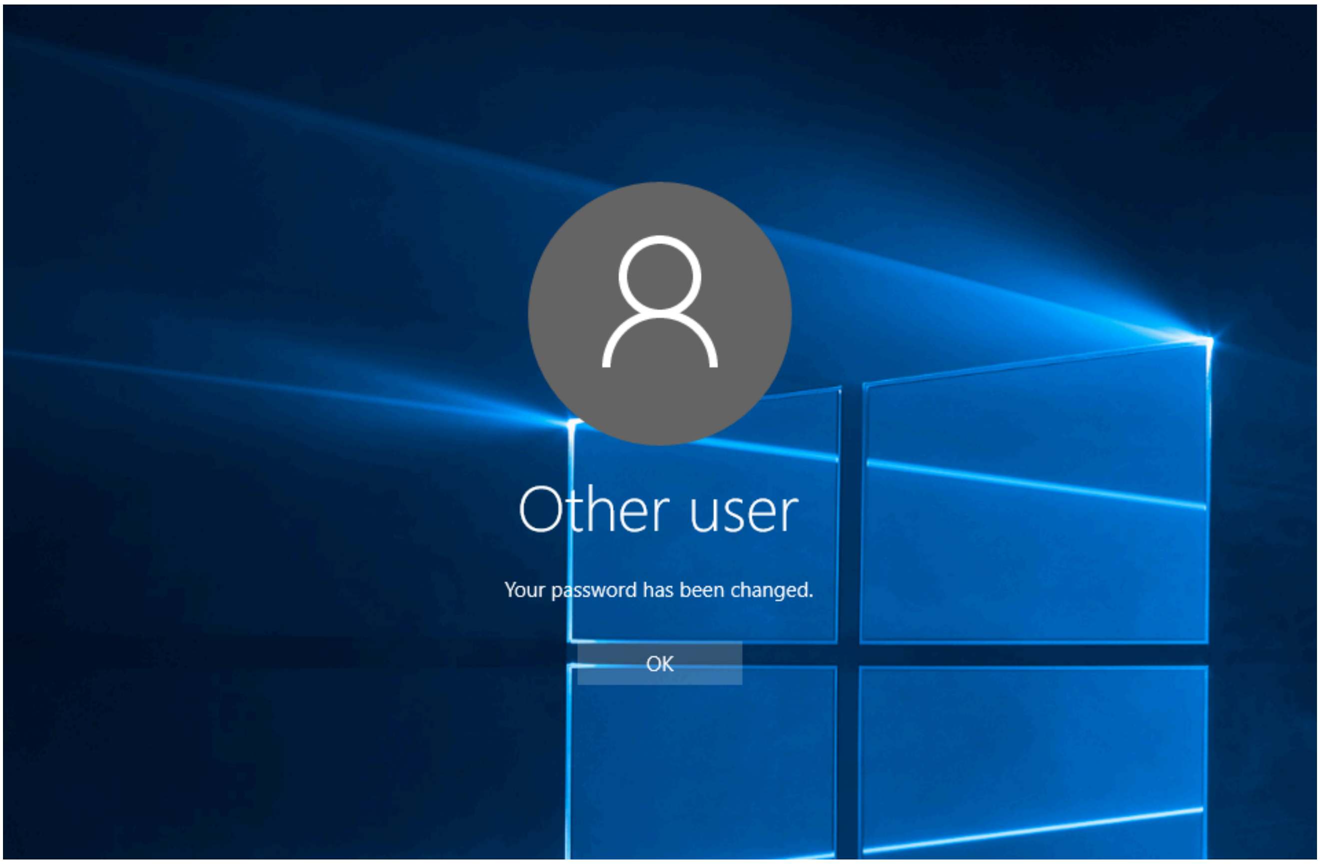
The system rejected the password due to length and complexity restrictions, confirming enforcement of the configured policy.



A compliant password meeting domain security requirements was entered.



Password change was successfully completed, confirming proper policy validation.

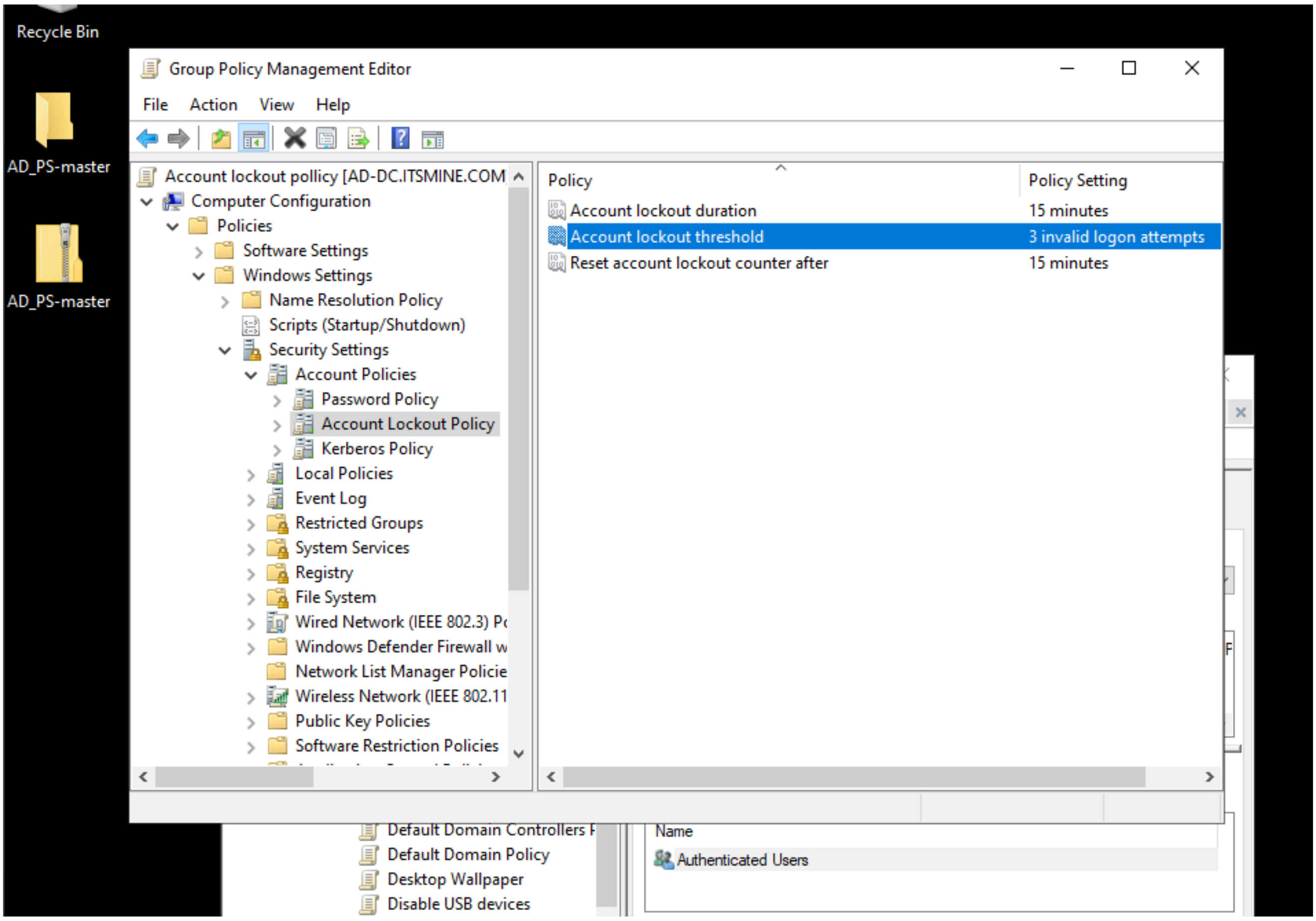


Account Lockout Policy configuration was reviewed to confirm threshold and duration settings for failed login attempts.

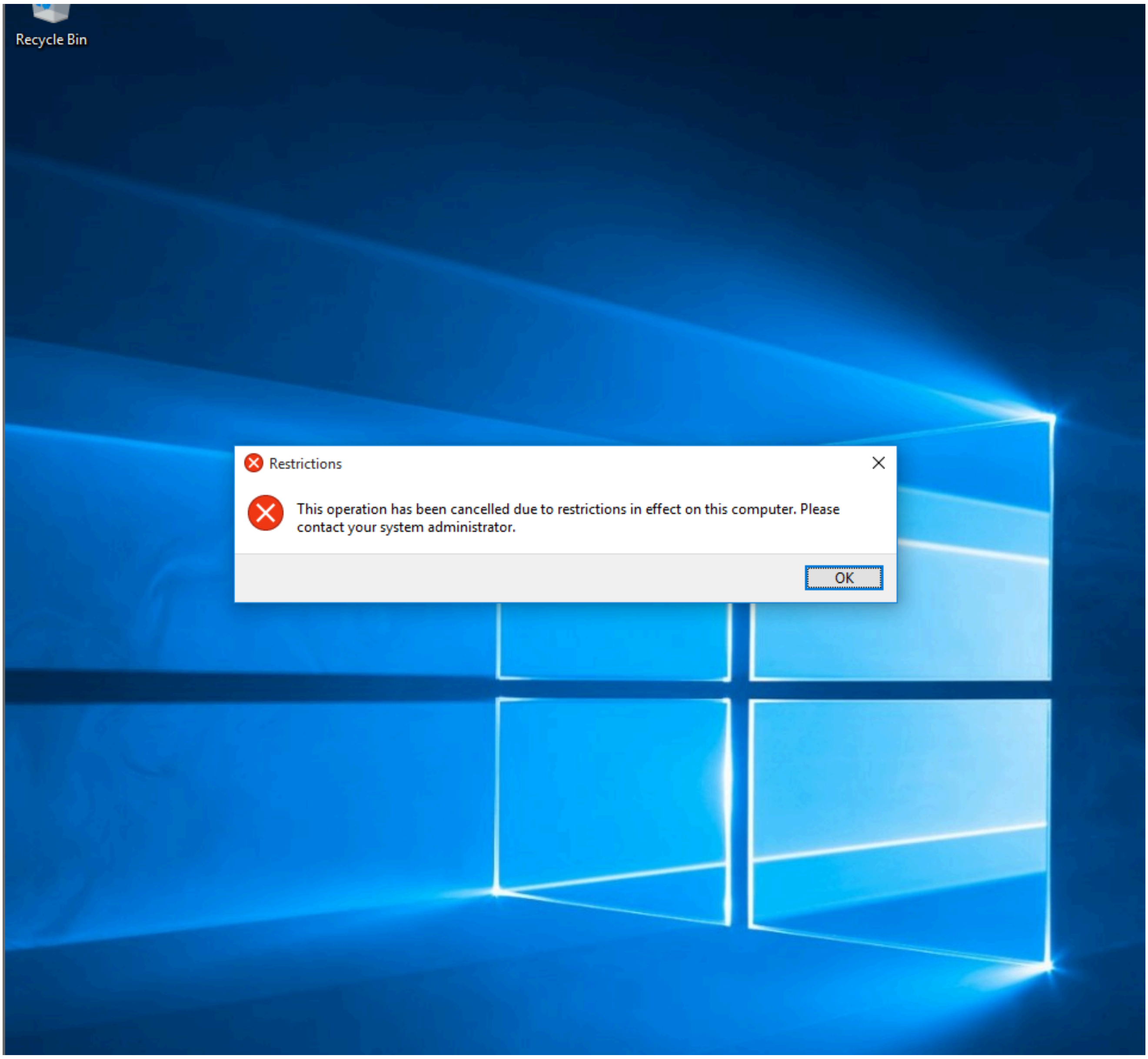
Activity 2: Account Lockout Policy Configuration

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.



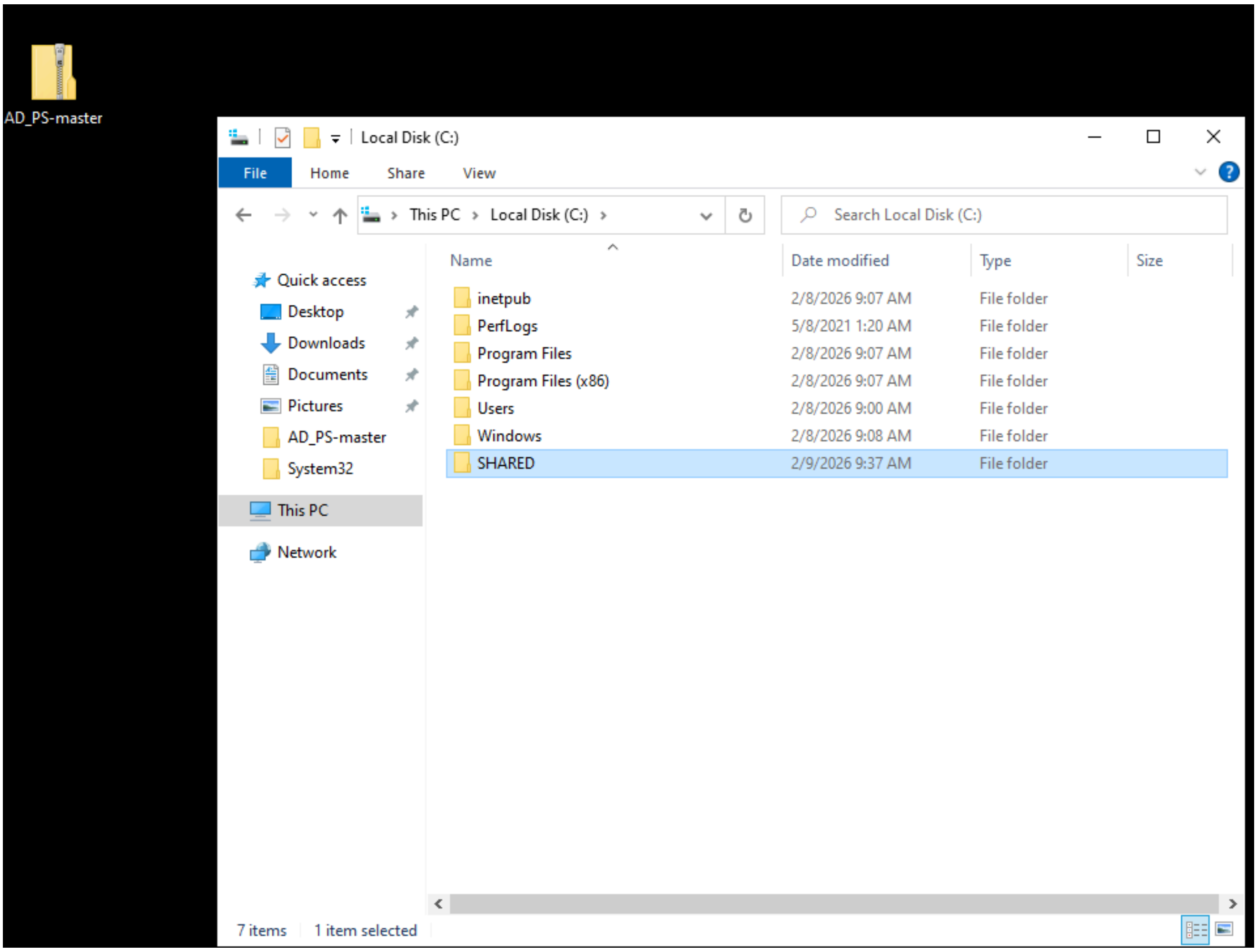
FILE SERVICES (SETTING UP NETWOKR SHARING):

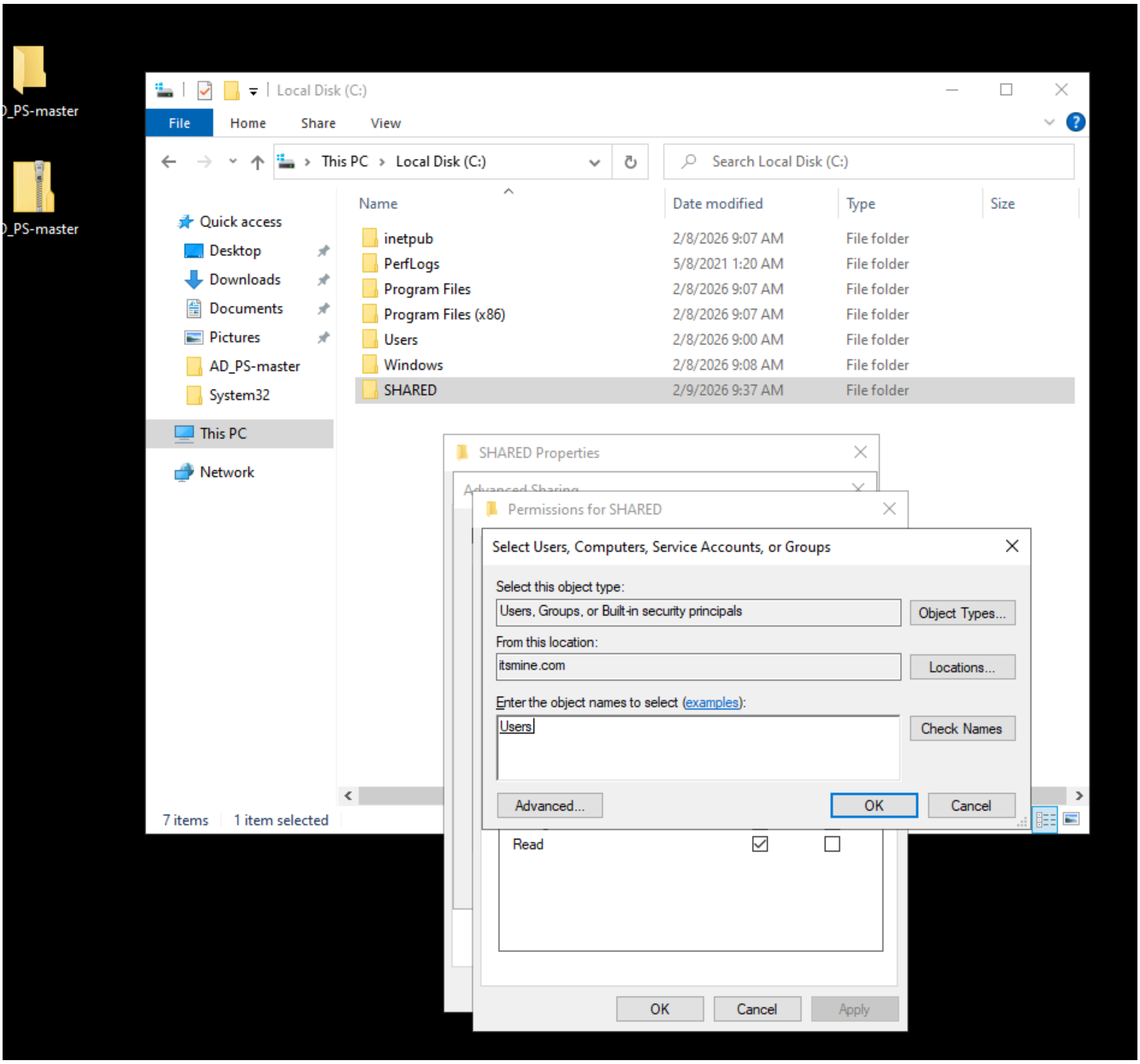
Activity 1: Set Up a File Sharing

Configure File Sharing

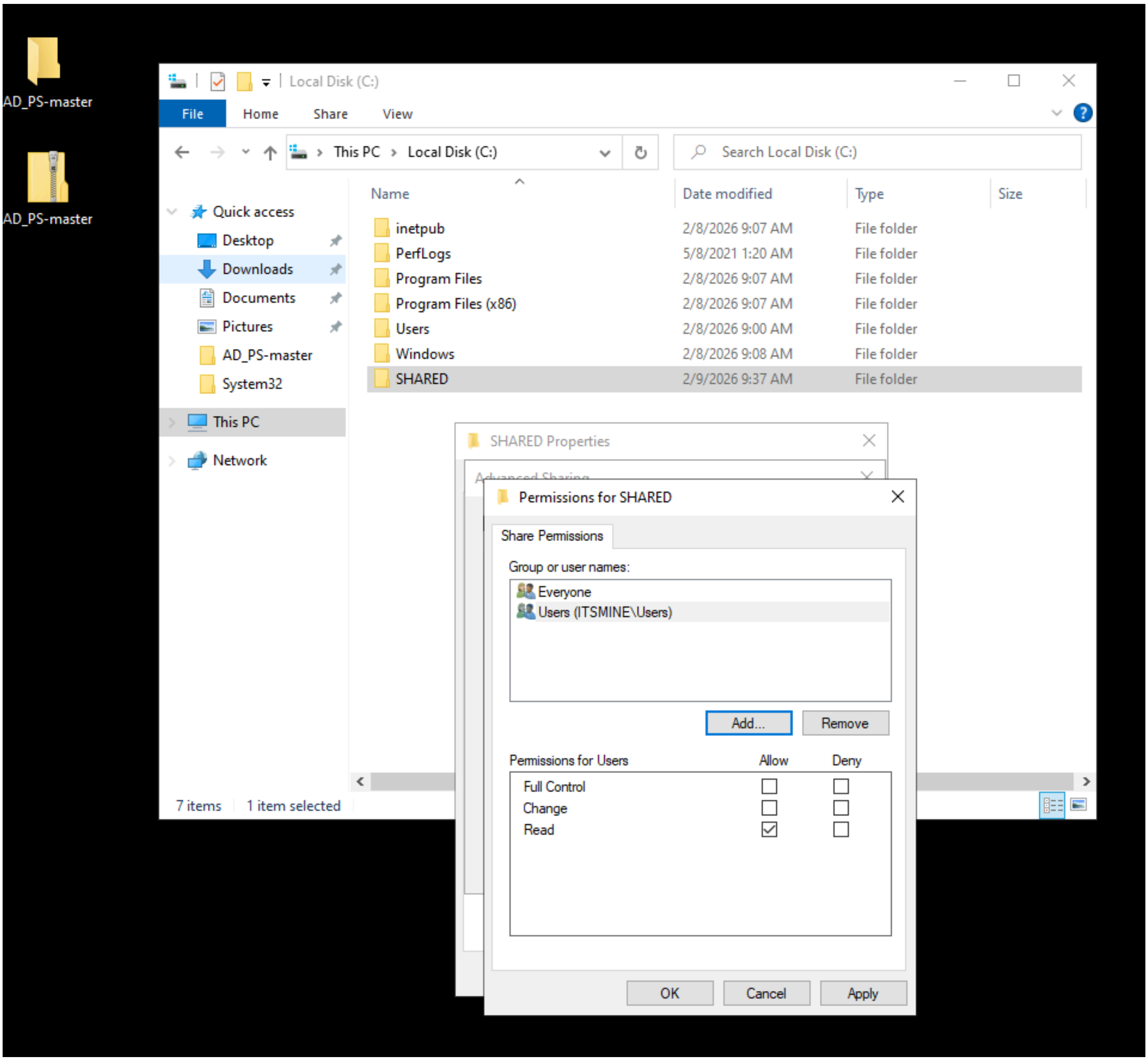
- Create shared folders with appropriate permissions.
- Set NTFS and share permissions to allow domain users access.

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

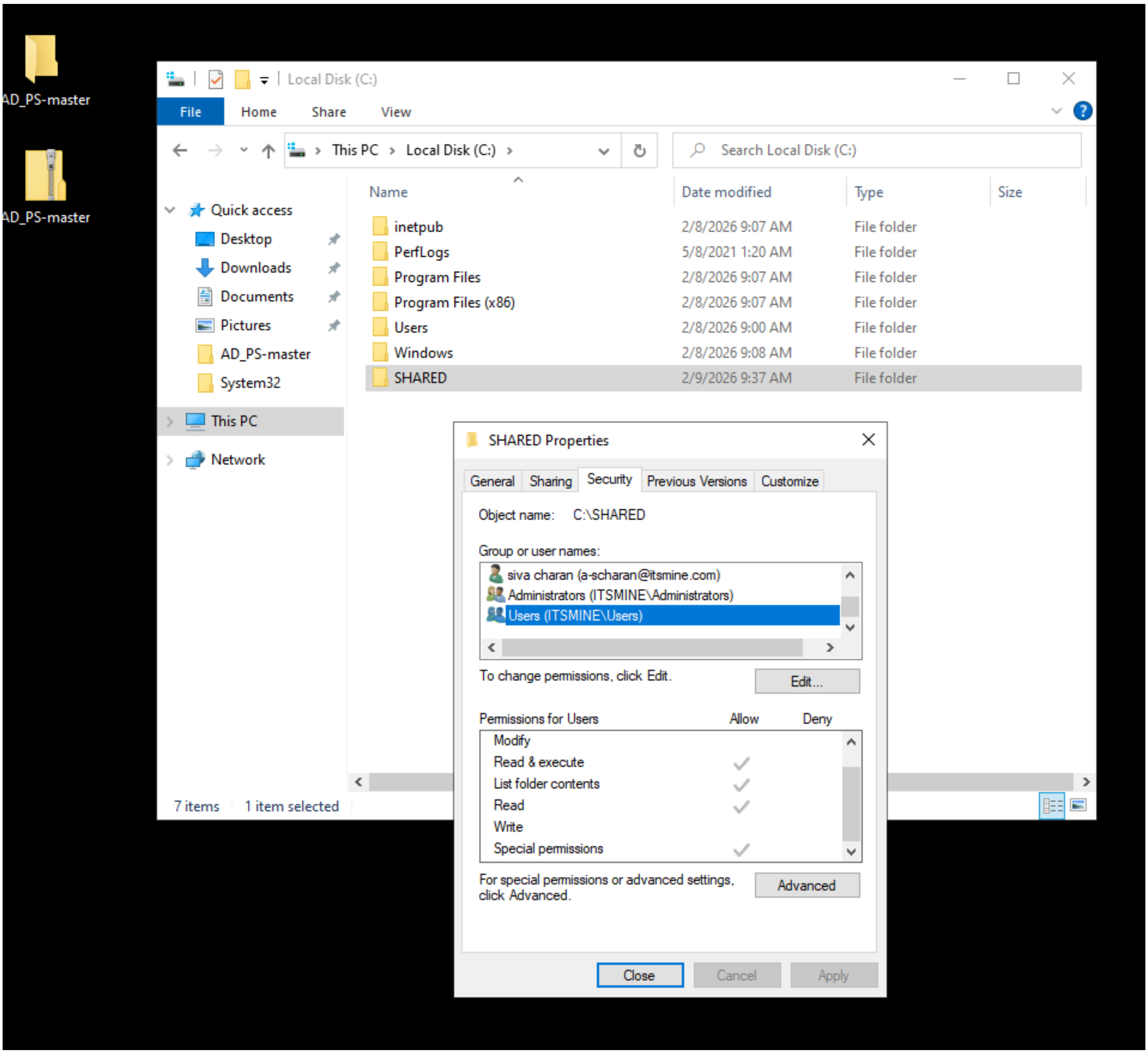

AD_PS-master
Local Disk (C:)
File
Home
Share
View
This PC > Local Disk (C:) >
Search Local Disk (C:)
Name
Date modified
Type
Size
Quick access
Desktop
Downloads
Documents
Pictures
AD_PS-master
System32
This PC
Network
inetpub 2/8/2026 9:07 AM File folder
PerfLogs 5/8/2021 1:20 AM File folder
Program Files 2/8/2026 9:07 AM File folder
Program Files (x86) 2/8/2026 9:07 AM File folder
Users 2/8/2026 9:00 AM File folder
Windows 2/8/2026 9:08 AM File folder
SHARED 2/9/2026 9:37 AM File folder
7 items
1 item selected

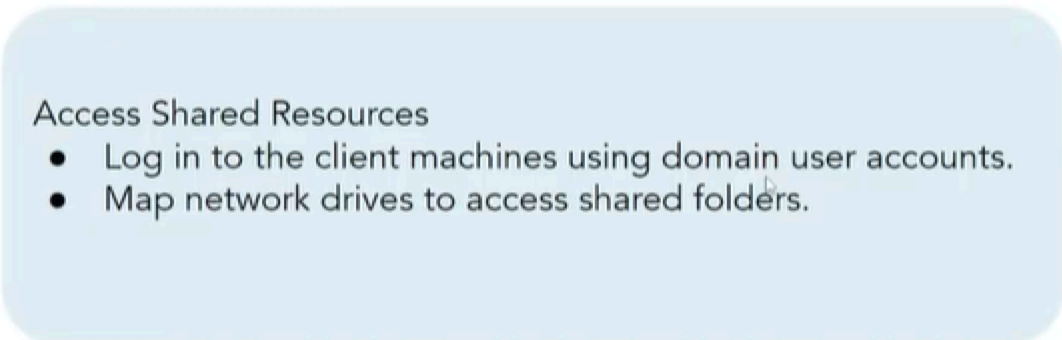


Share permissions were configured for the SHARED folder, granting access to domain users for file sharing within the network.

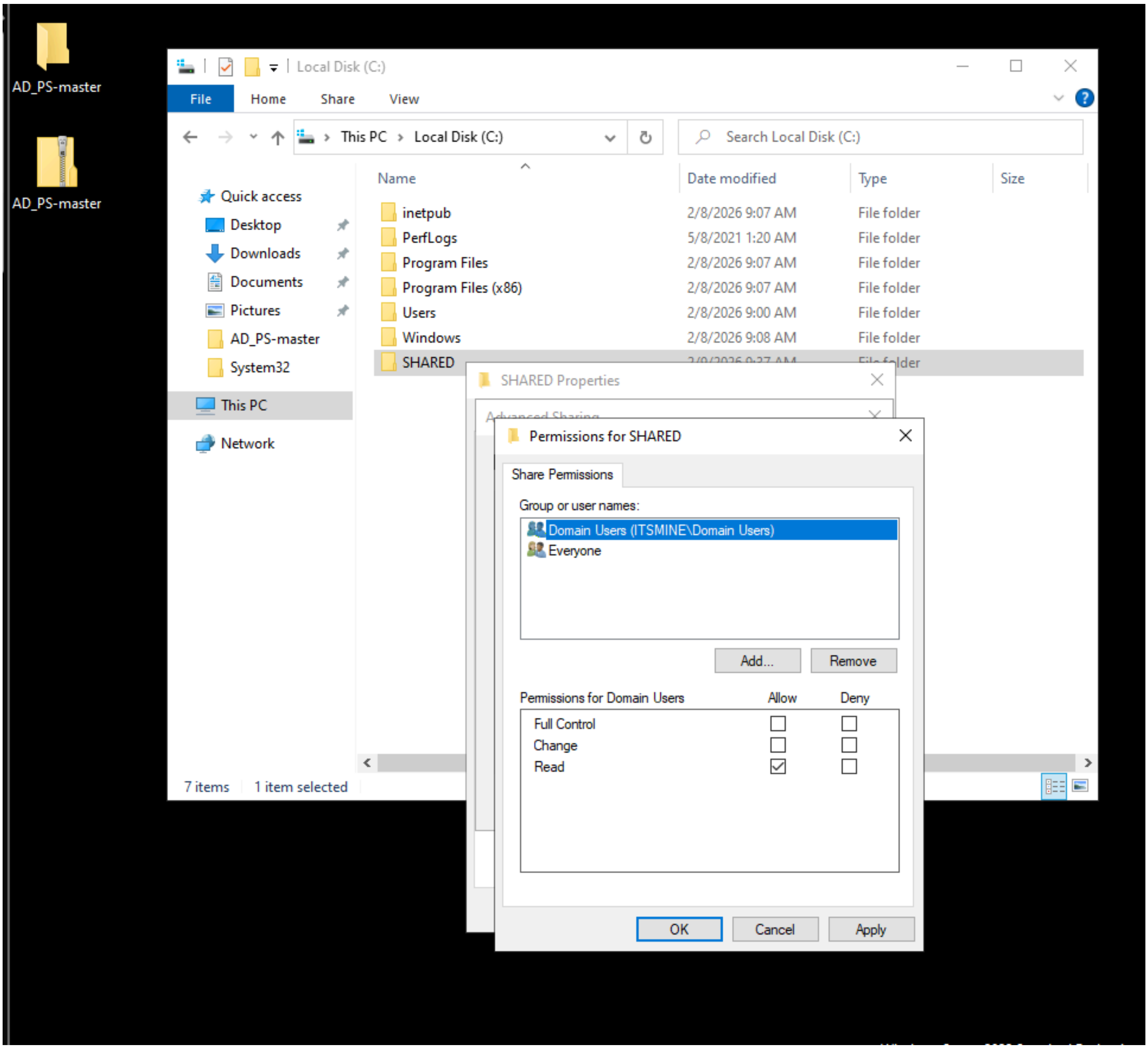


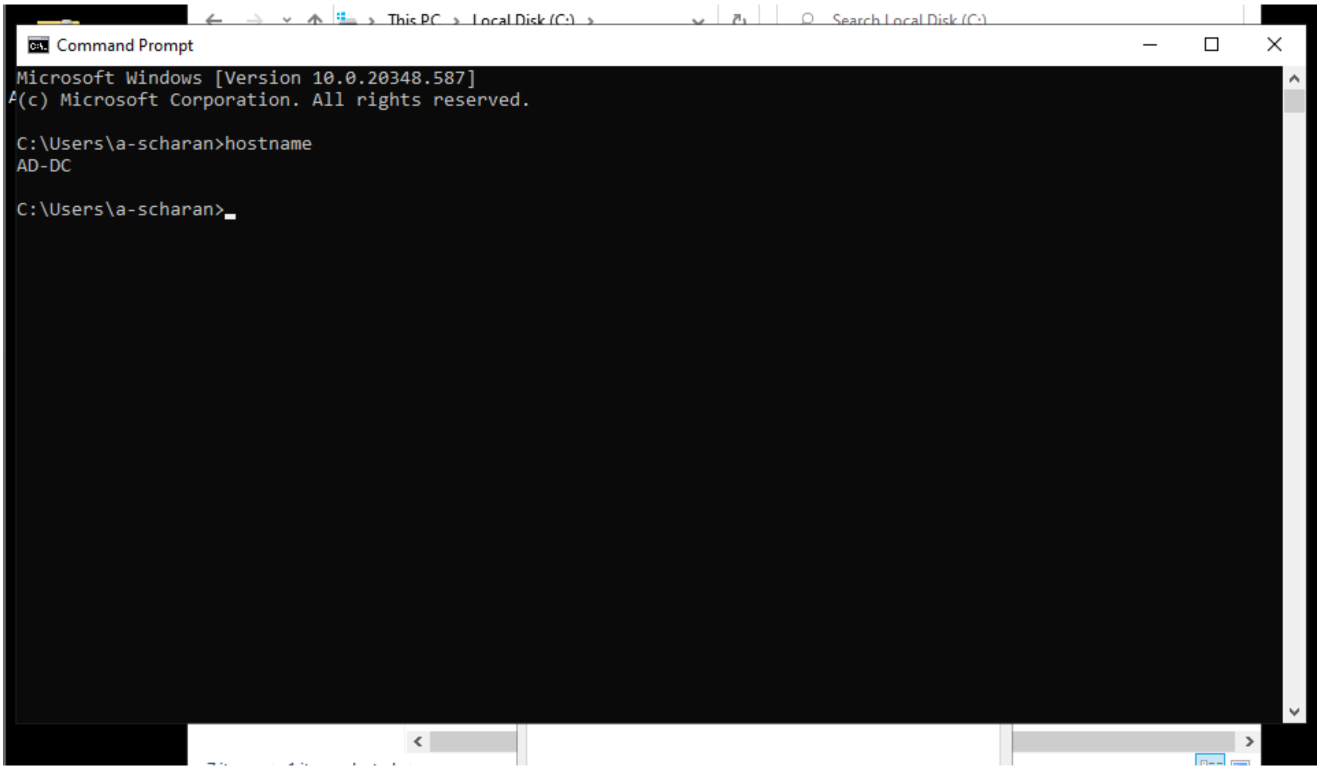
NTFS permissions were configured for the SHARED folder to control user-level access within the domain.



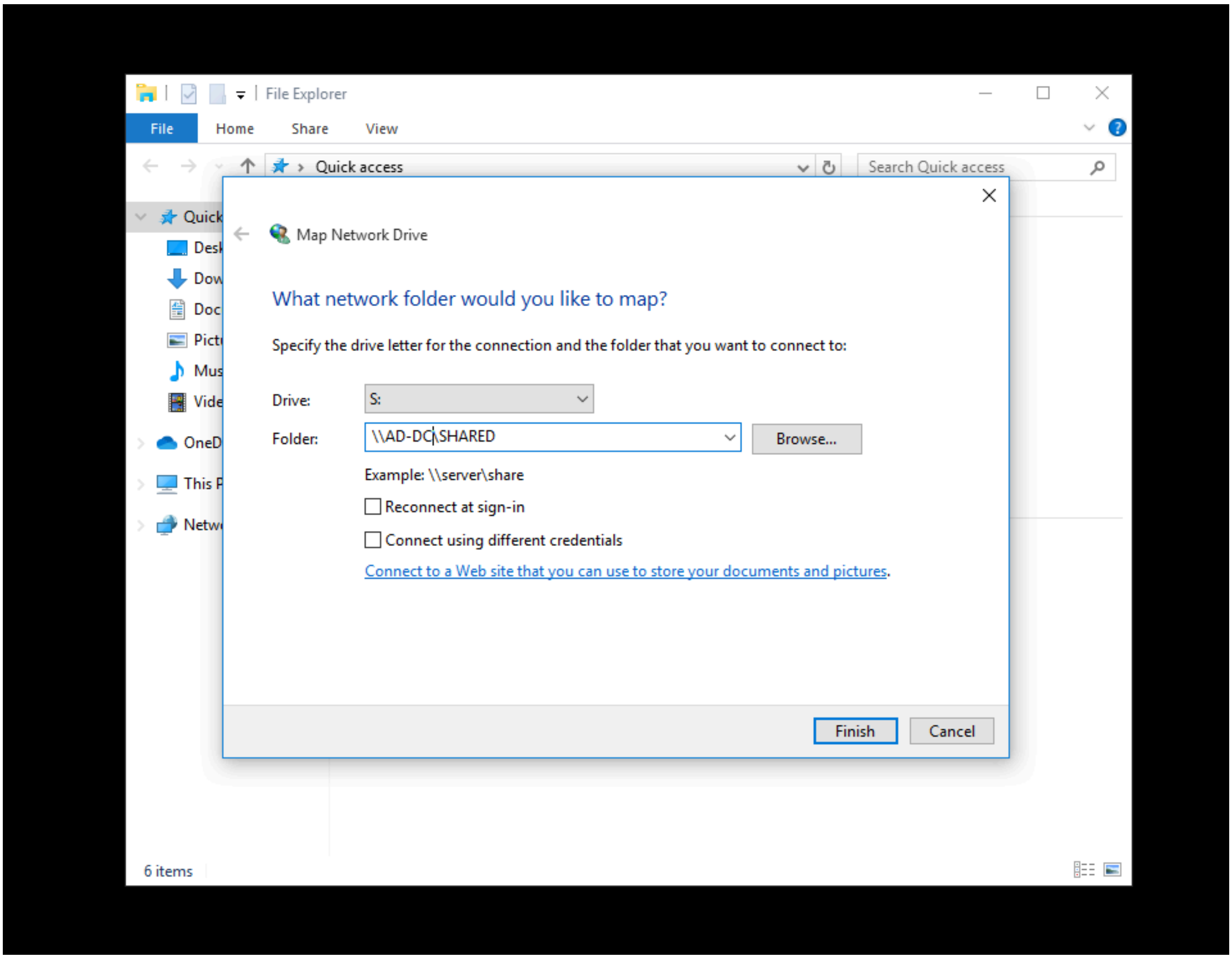


Share permissions were adjusted to allow Domain Users access to the SHARED folder. This enables domain-based file access from client systems.

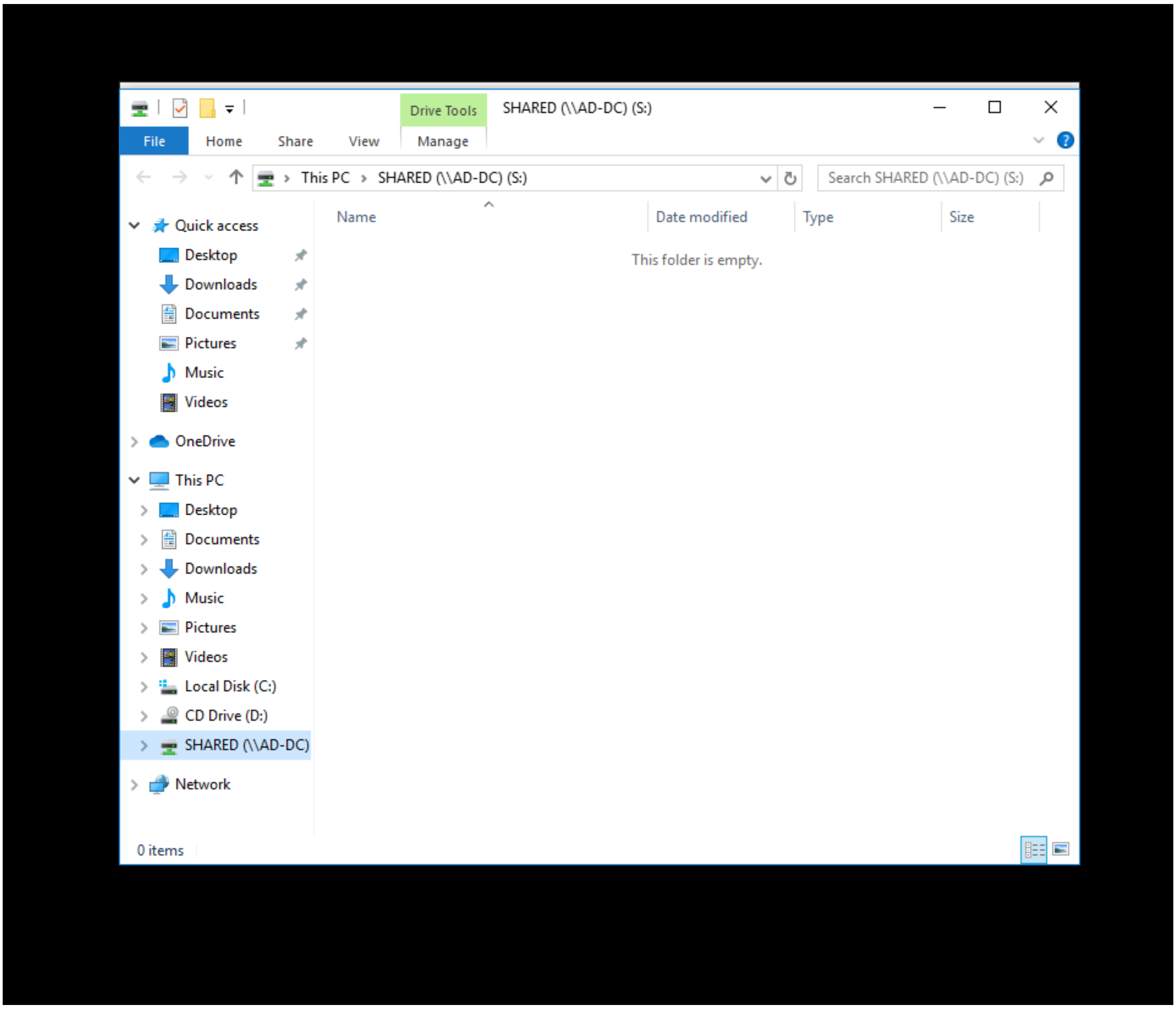

AD_PS-master
AD_PS-master
Local Disk (C:)
File
Home
Share
View
This PC › Local Disk (C:)
Search Local Disk (C:)
Quick access
Desktop
Downloads
Documents
Pictures
AD_PS-master
System32
This PC
Network
Name
Date modified
Type
Size
inpub 2/8/2026 9:07 AM File folder
PerfLogs 5/8/2021 1:20 AM File folder
Program Files 2/8/2026 9:07 AM File folder
Program Files (x86) 2/8/2026 9:07 AM File folder
Users 2/8/2026 9:00 AM File folder
Windows 2/8/2026 9:08 AM File folder
SHARED
SHARED Properties
Permissions for SHARED
Share Permissions
Group or user names:
Domain Users (ITSMINE\Domain Users)
Everyone
Add...
Remove
Permissions for Domain Users
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply
7 items
1 item selected


Command Prompt
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.
C:\Users\a-scharan>hostname
AD-DC
C:\Users\a-scharan>_

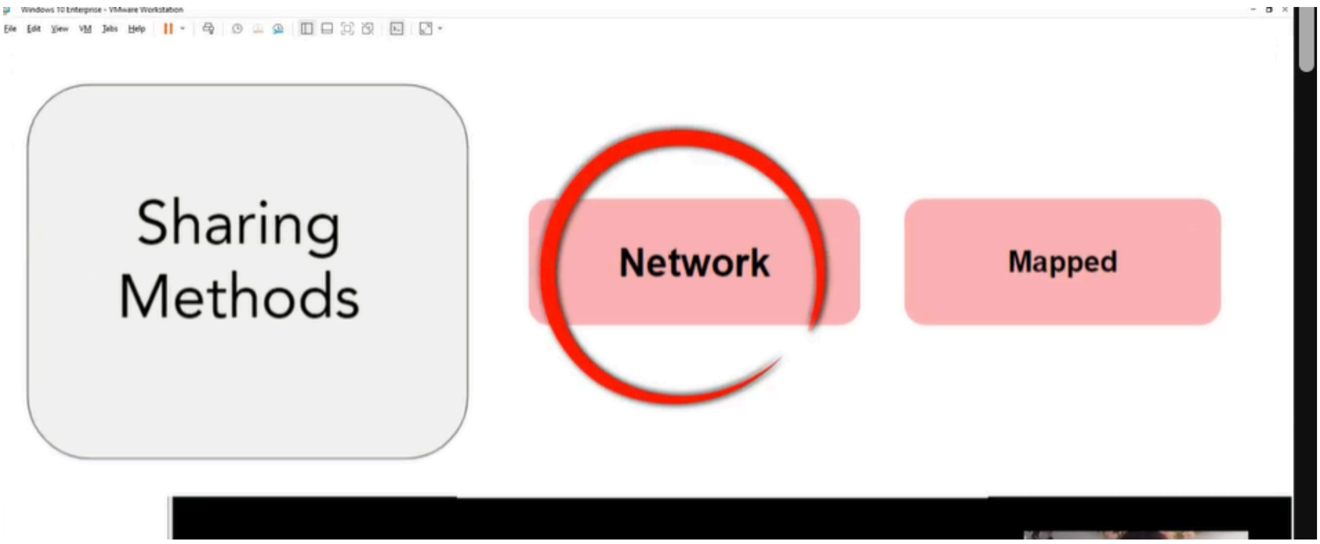
The shared folder was mapped using the network path (\AD-DC\SHARED). This allows users to access the shared folder as a local drive.



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



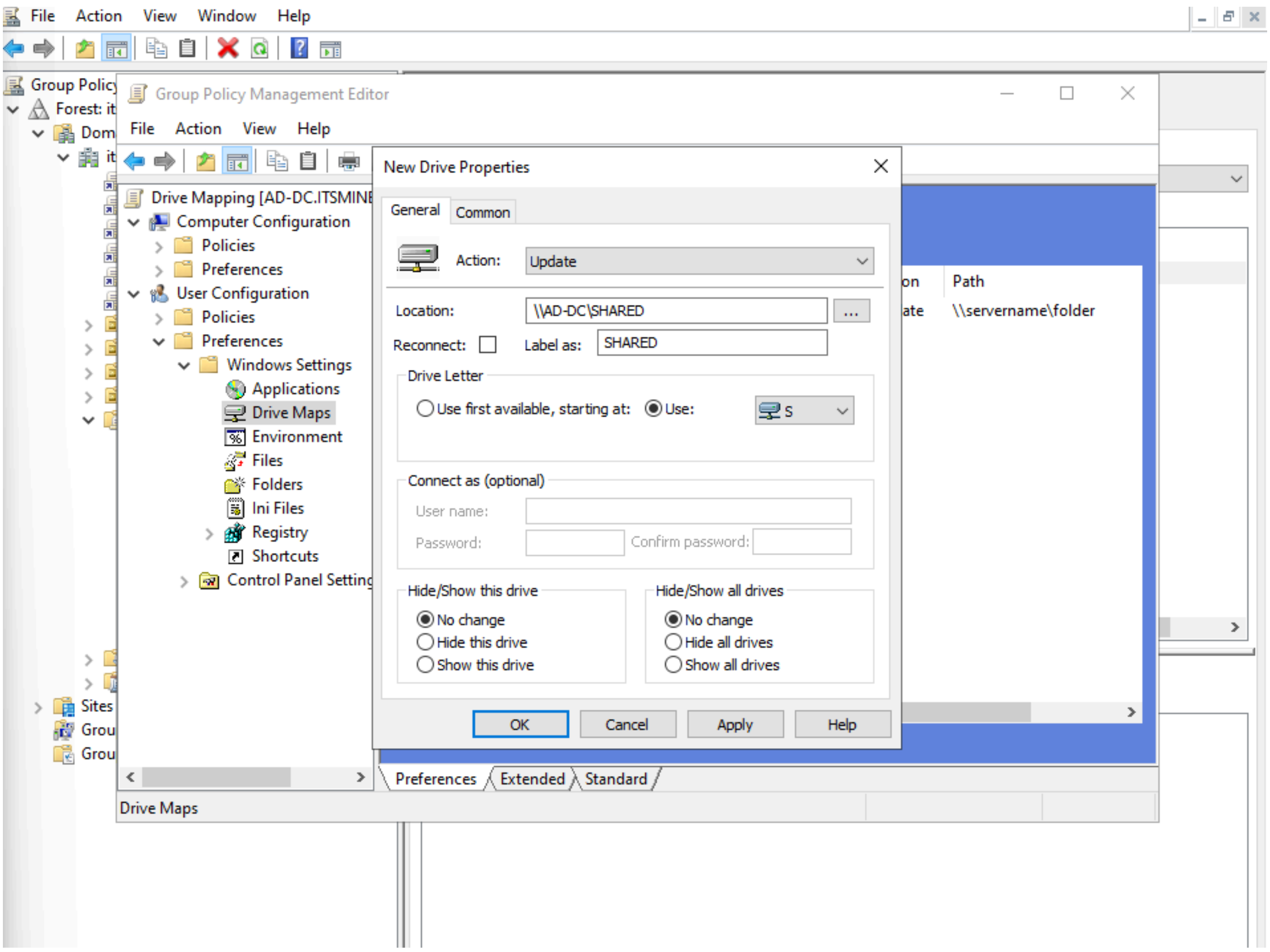
Different sharing methods such as direct network access and mapped drives are illustrated for resource accessibility.



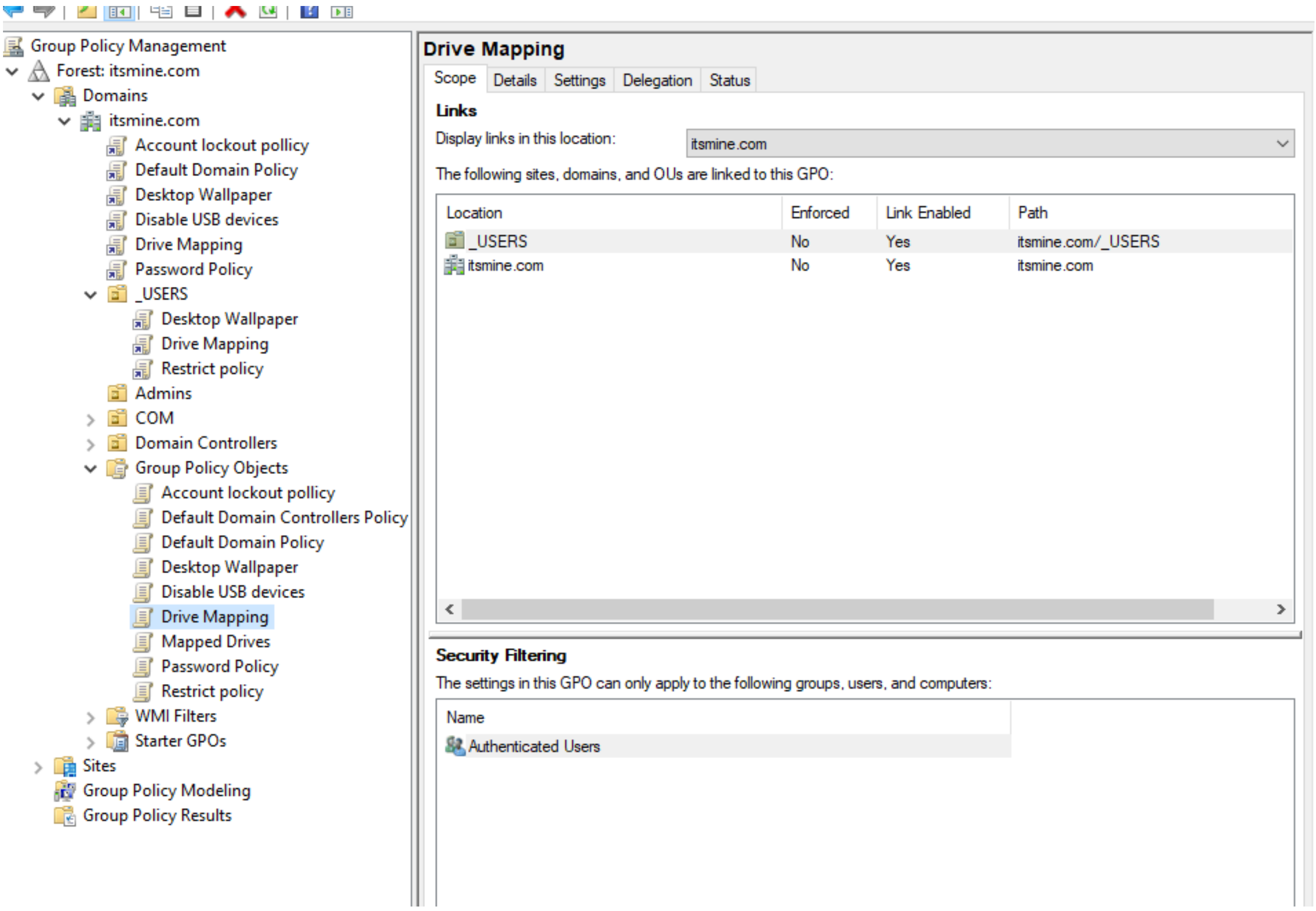
Activity 3: GPO Configuration

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

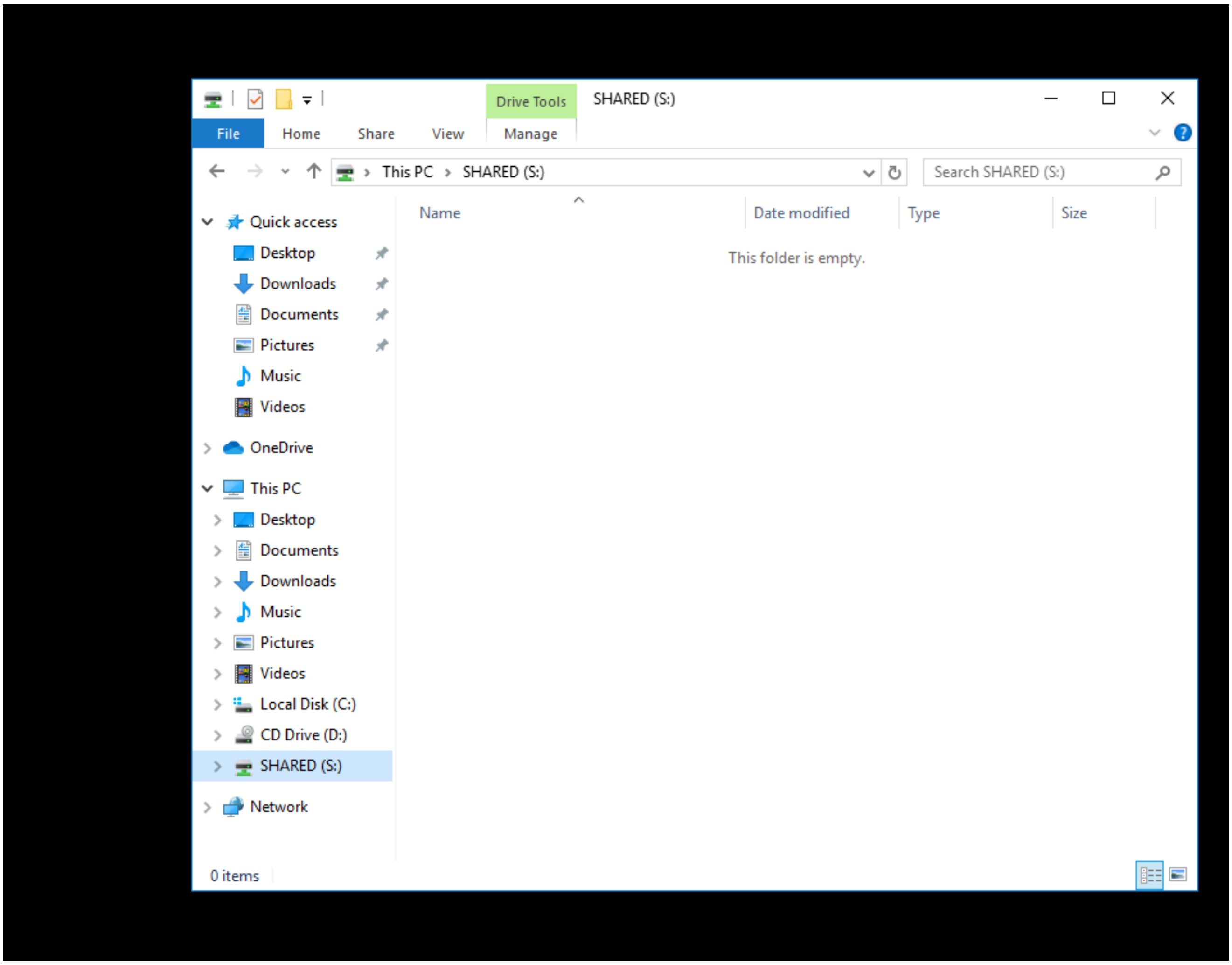
A Drive Mapping GPO was configured with the shared folder path and assigned drive letter. This ensures automatic mapping at user login.



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



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

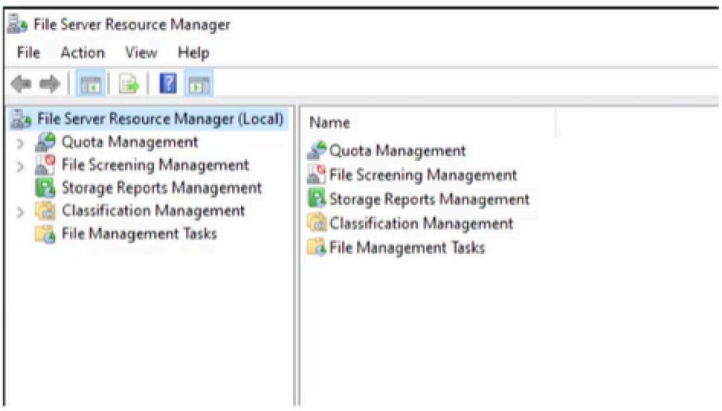


Activity 4: Implement quotas and file screening using File Server Resource Manager (FSRM).

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

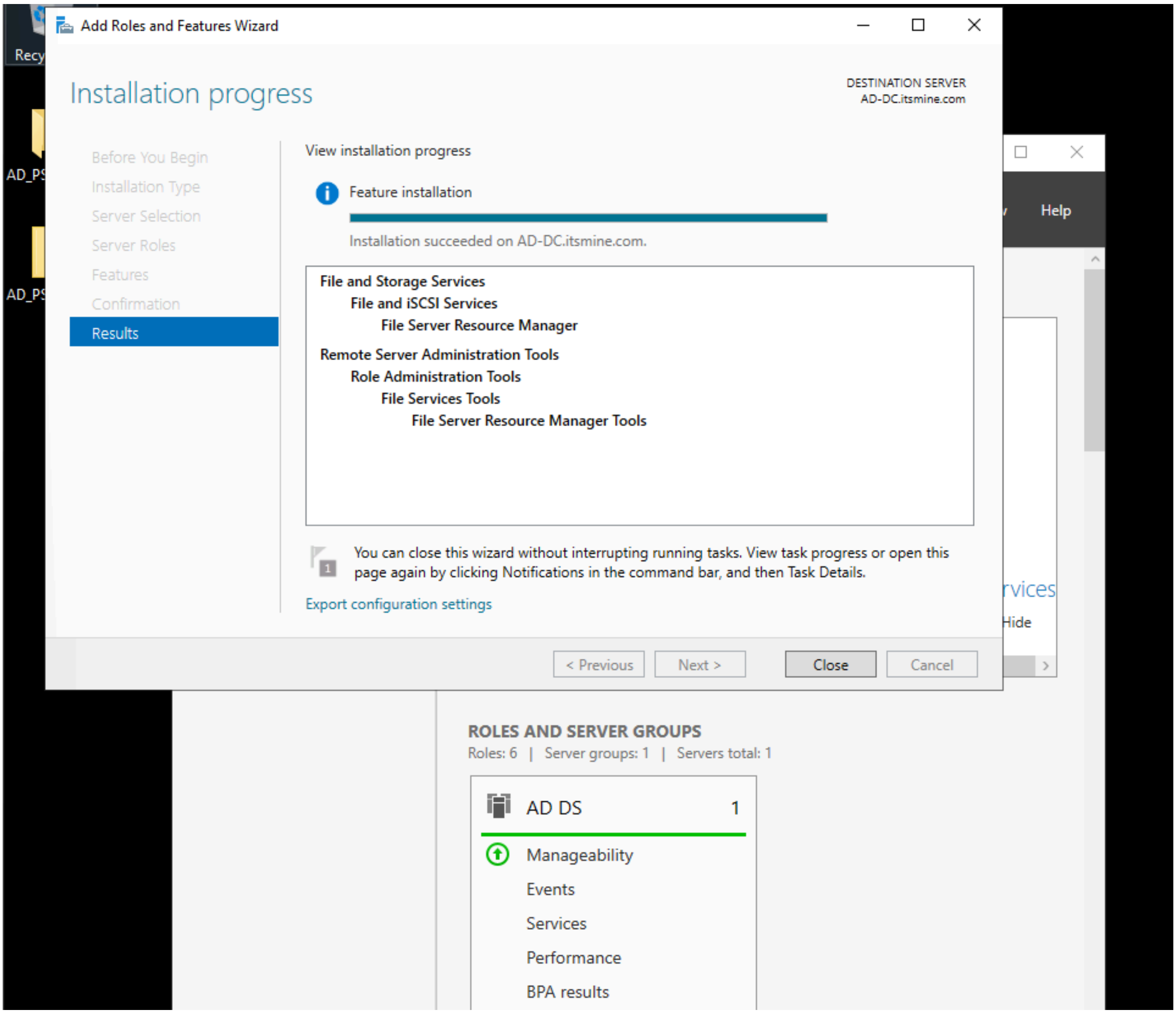
FSRM console displays tools such as Quota Management and File Screening Management for advanced file server control.

File Server Resource Manager (FSRM)

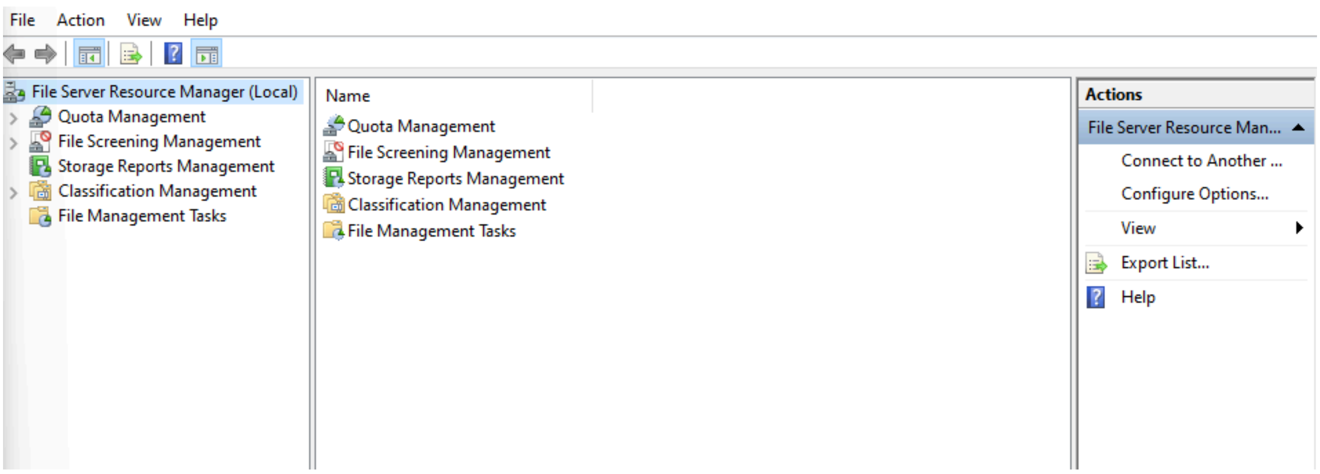


suite of tools provided by Microsoft to help you manage and classify data stored on file servers.

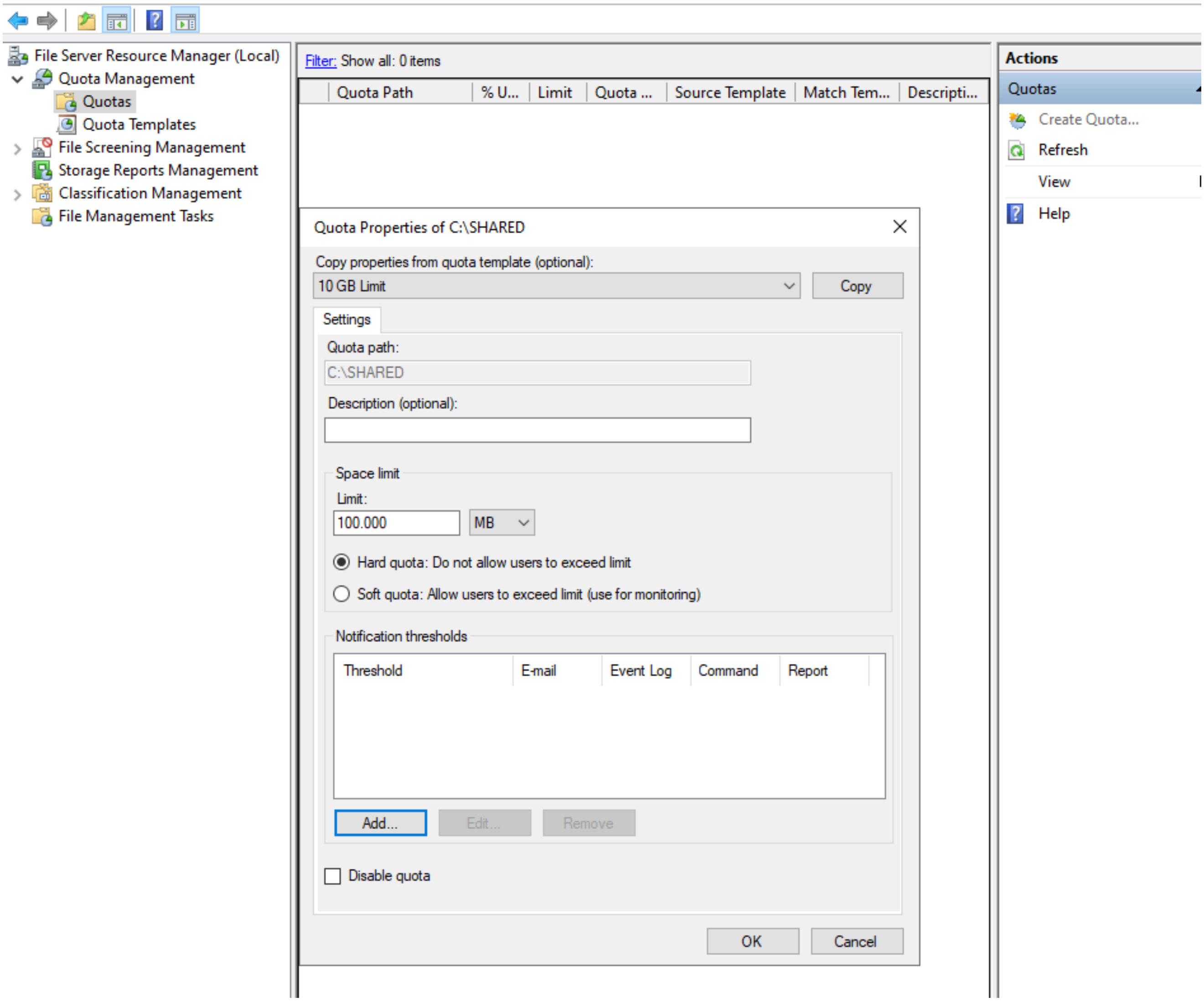
File Server Resource Manager role service was installed under File and Storage Services to enable quota and screening features.



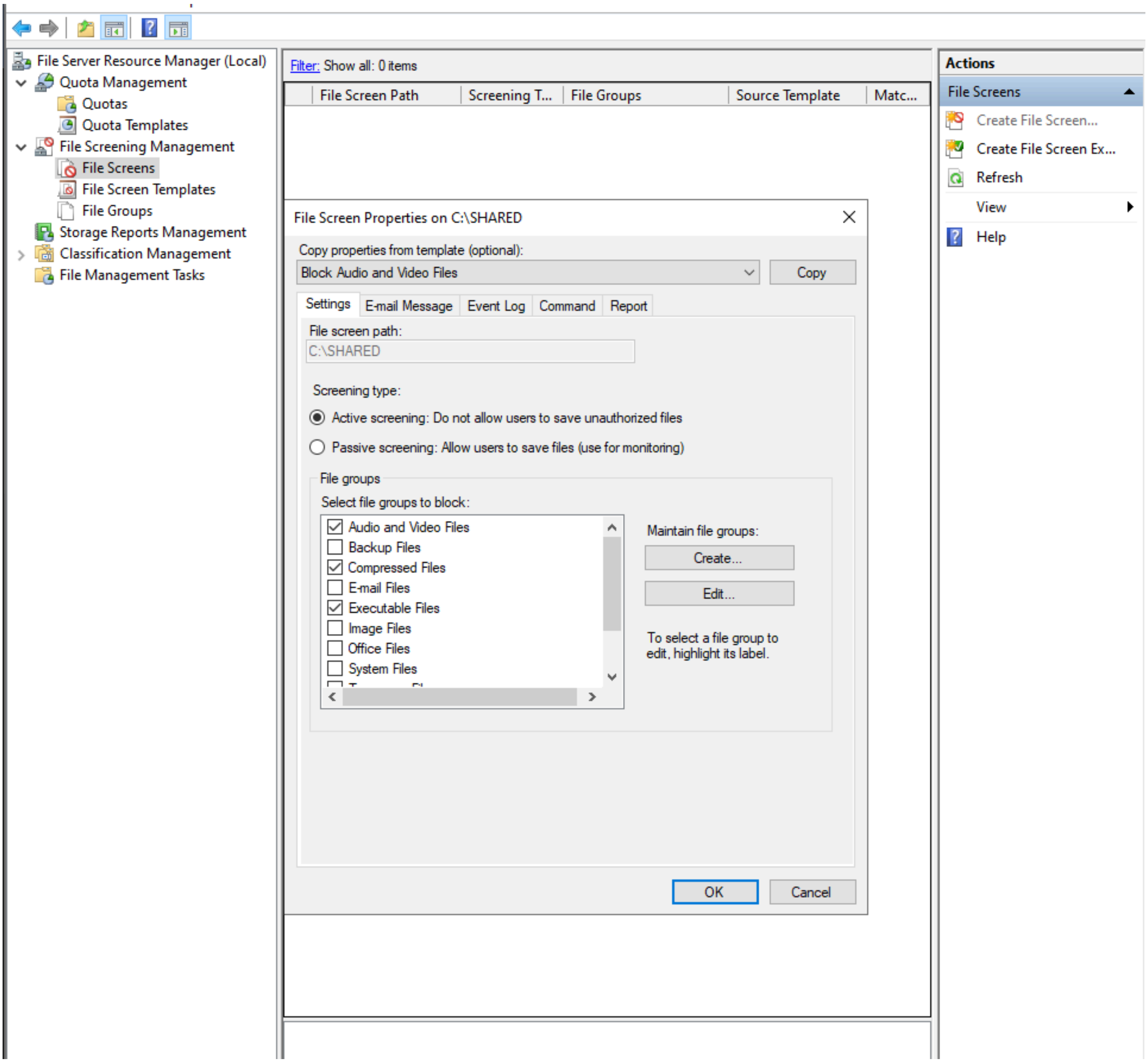
FSRM management interface shows available configuration sections including quotas and file screens.



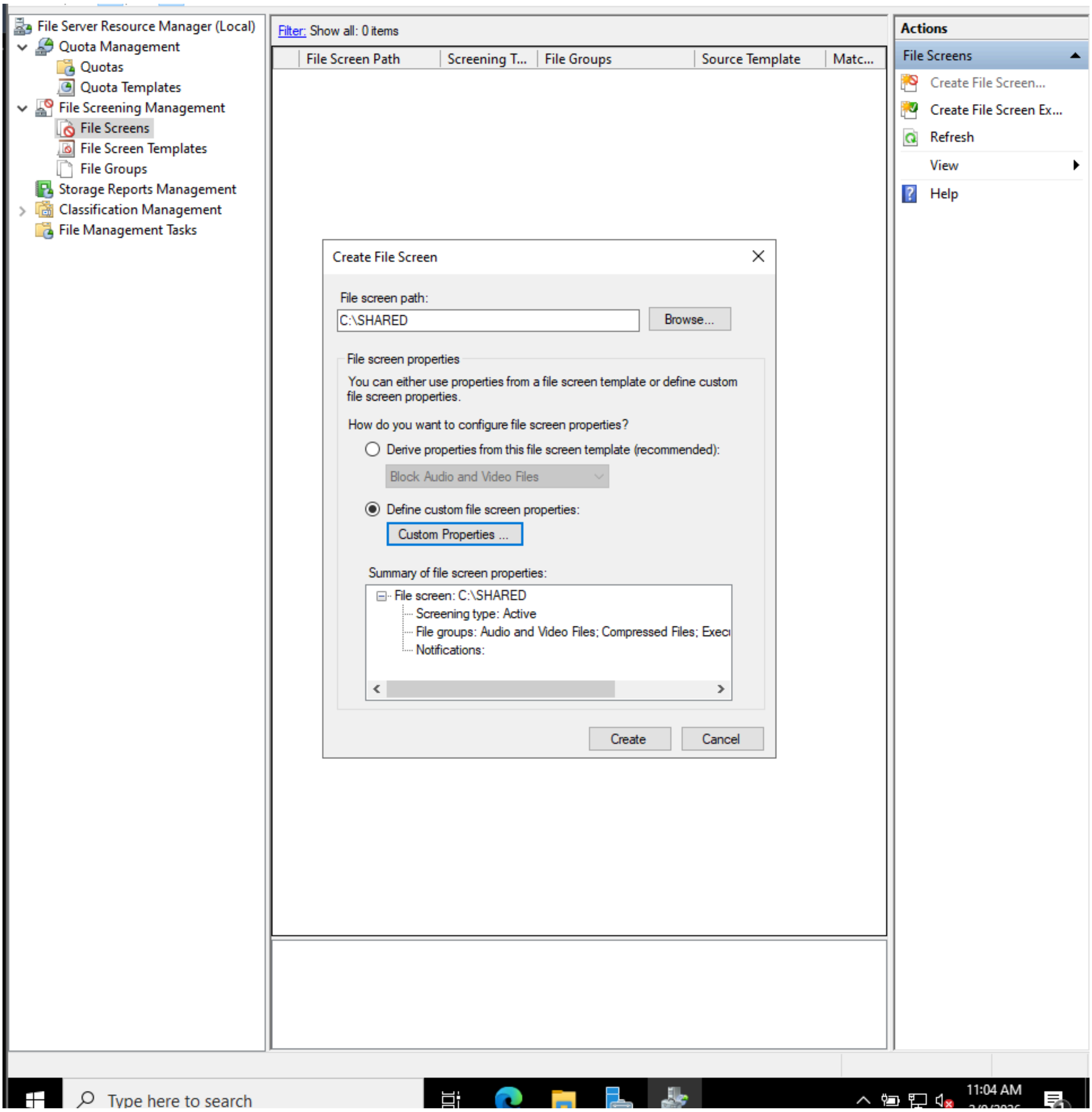
A quota was created for the SHARED folder to limit storage usage. The limit was defined to restrict excessive disk consumption.



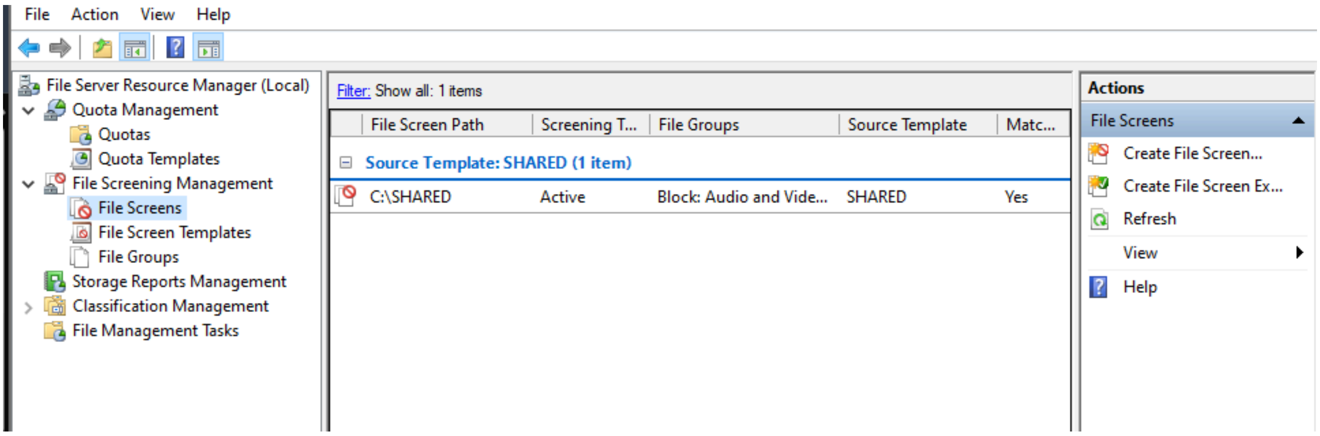
A File Screen was configured on the SHARED folder to block specific file types such as audio and video files. This prevents unauthorized storage of restricted content.



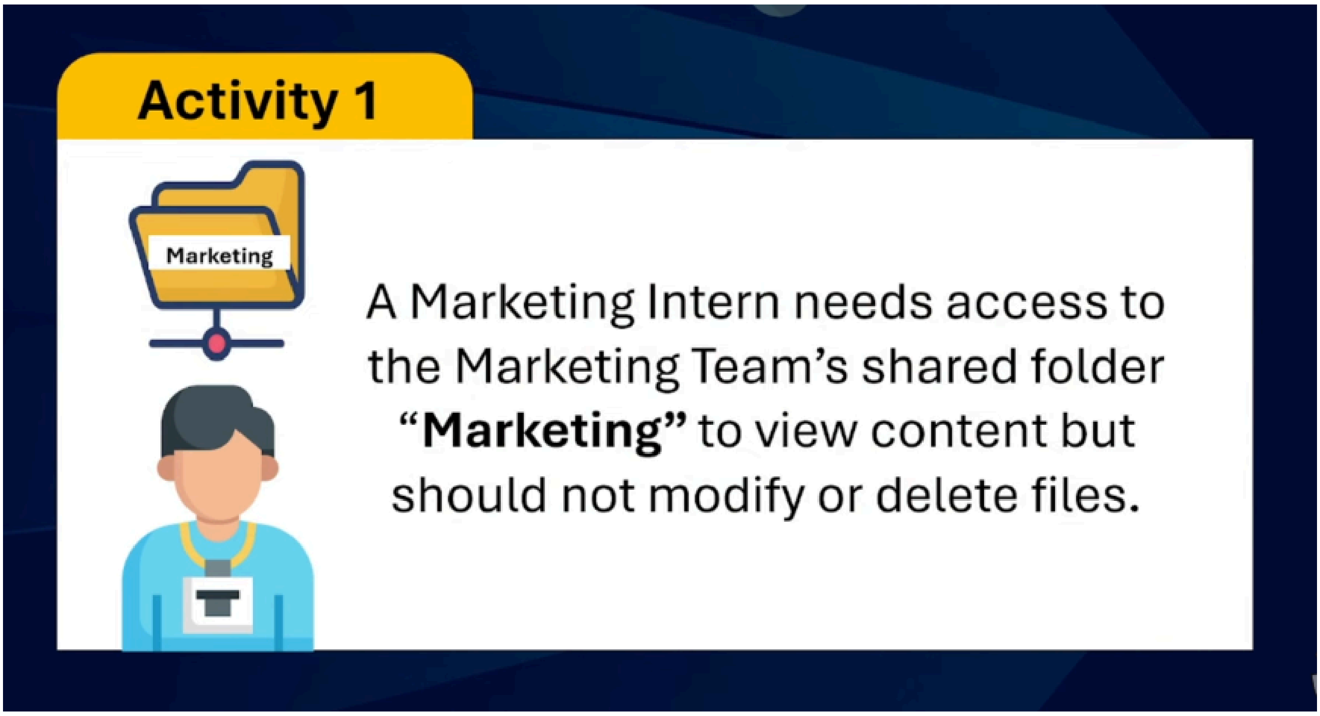
A custom file screen template was applied to the SHARED folder. This enforces file-type restrictions directly on the storage path.



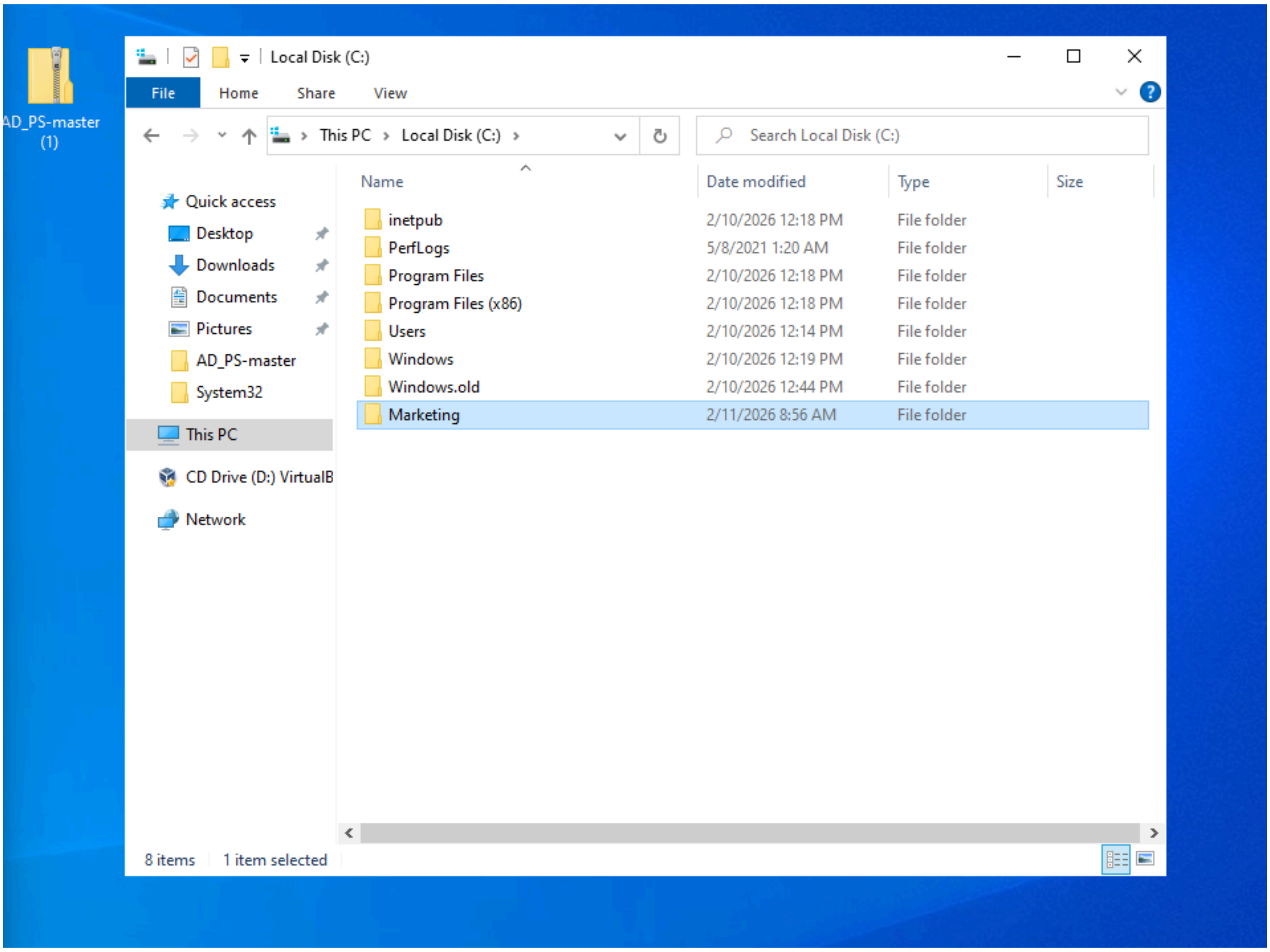
The file screen appears active under the SHARED path, confirming successful configuration.



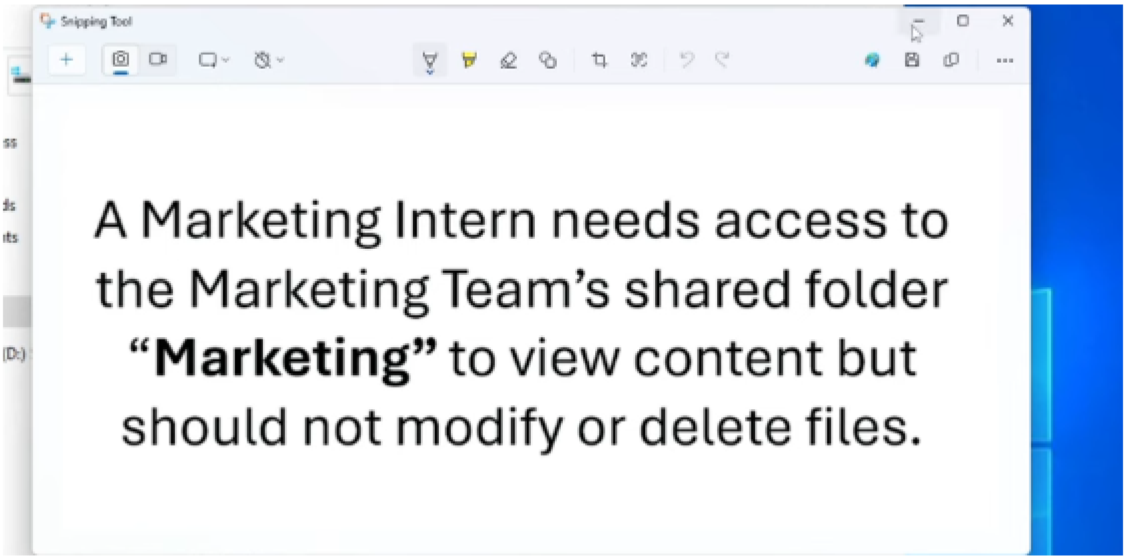
NTFS vs SHARED (HOW TO ASSIGN FOLDER PERMISSIONS) :



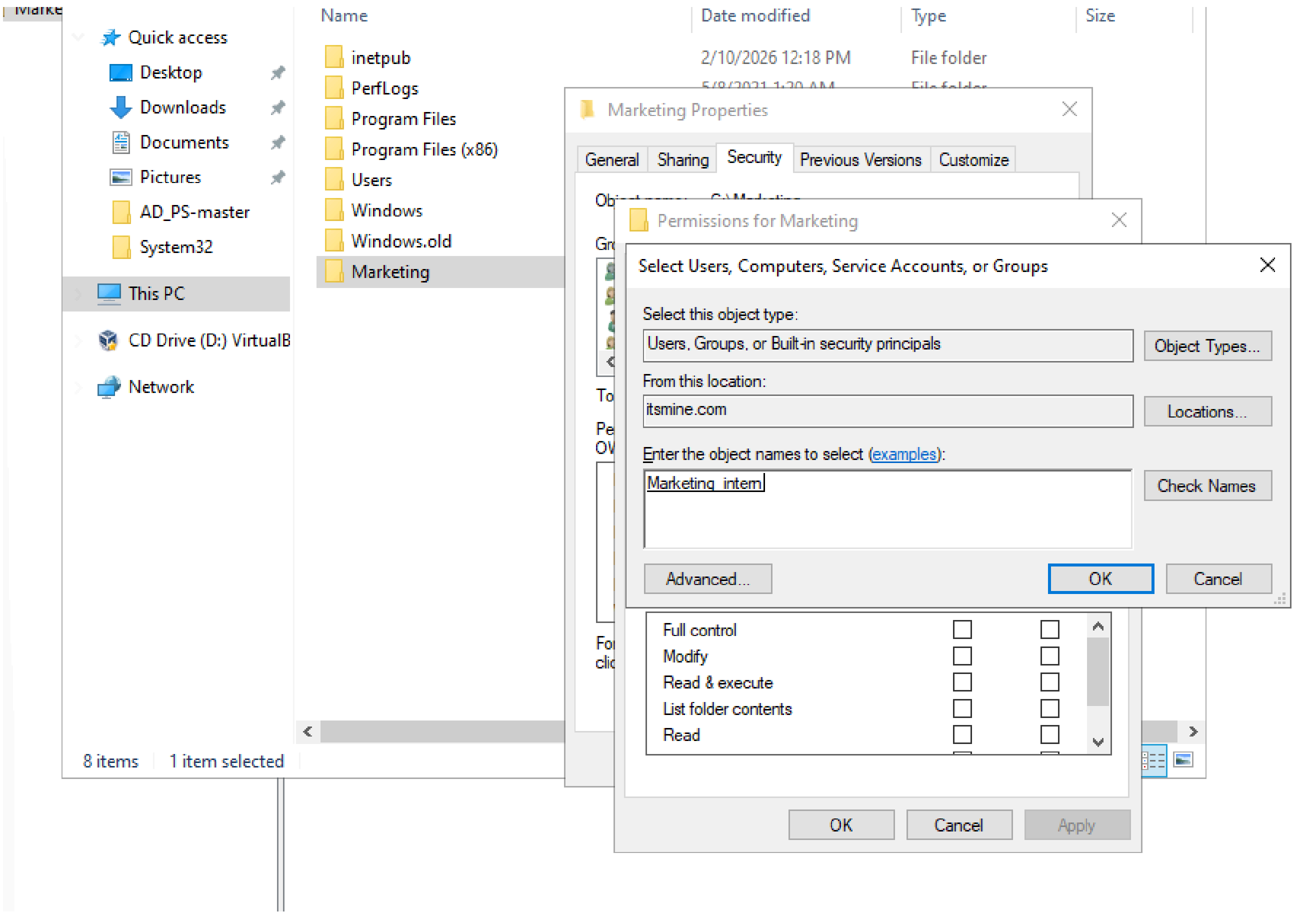
A Marketing folder was created to implement role-based access control for departmental file sharing.



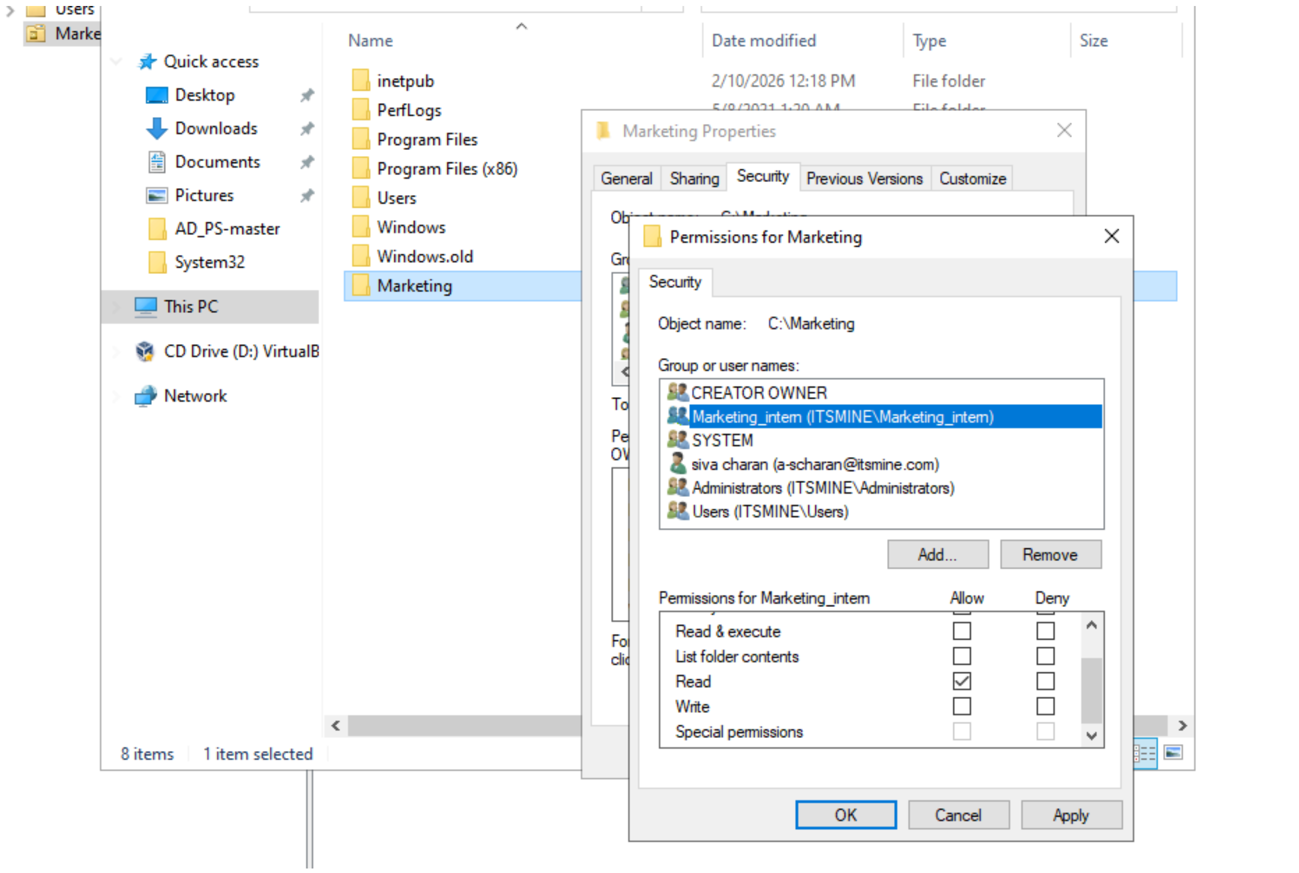
The requirement specifies that the intern should only view content without modification rights.

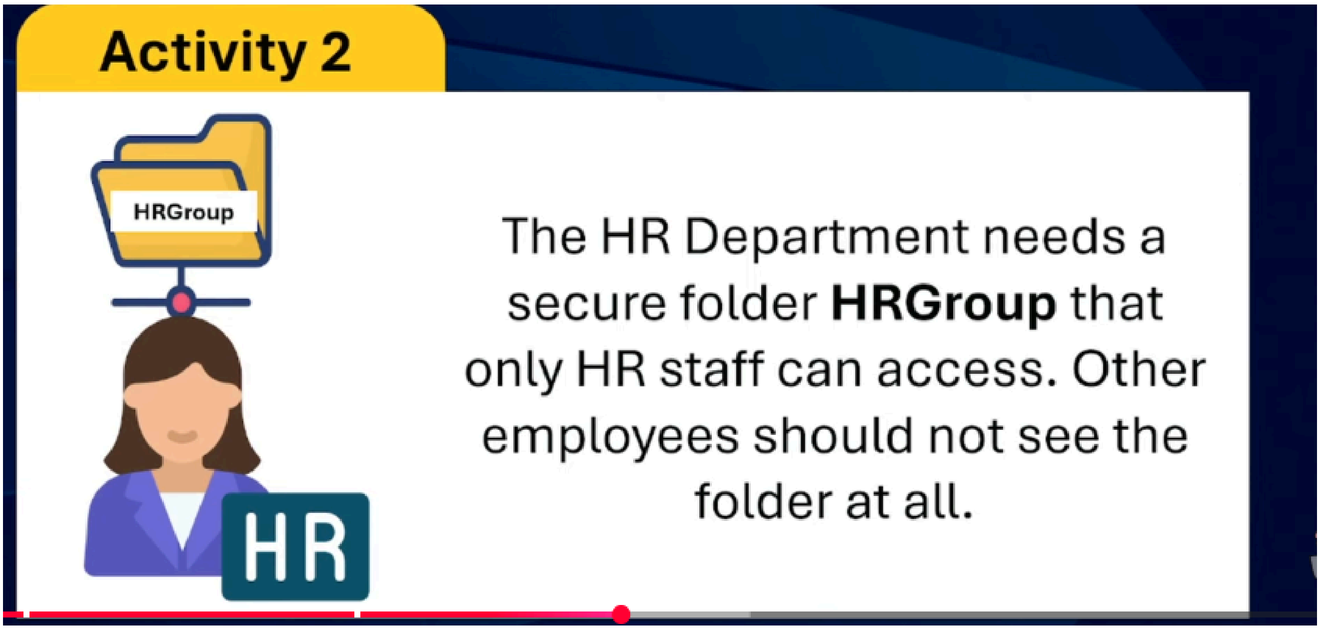


NTFS permissions were configured to grant Read access only to the Marketing Intern group.

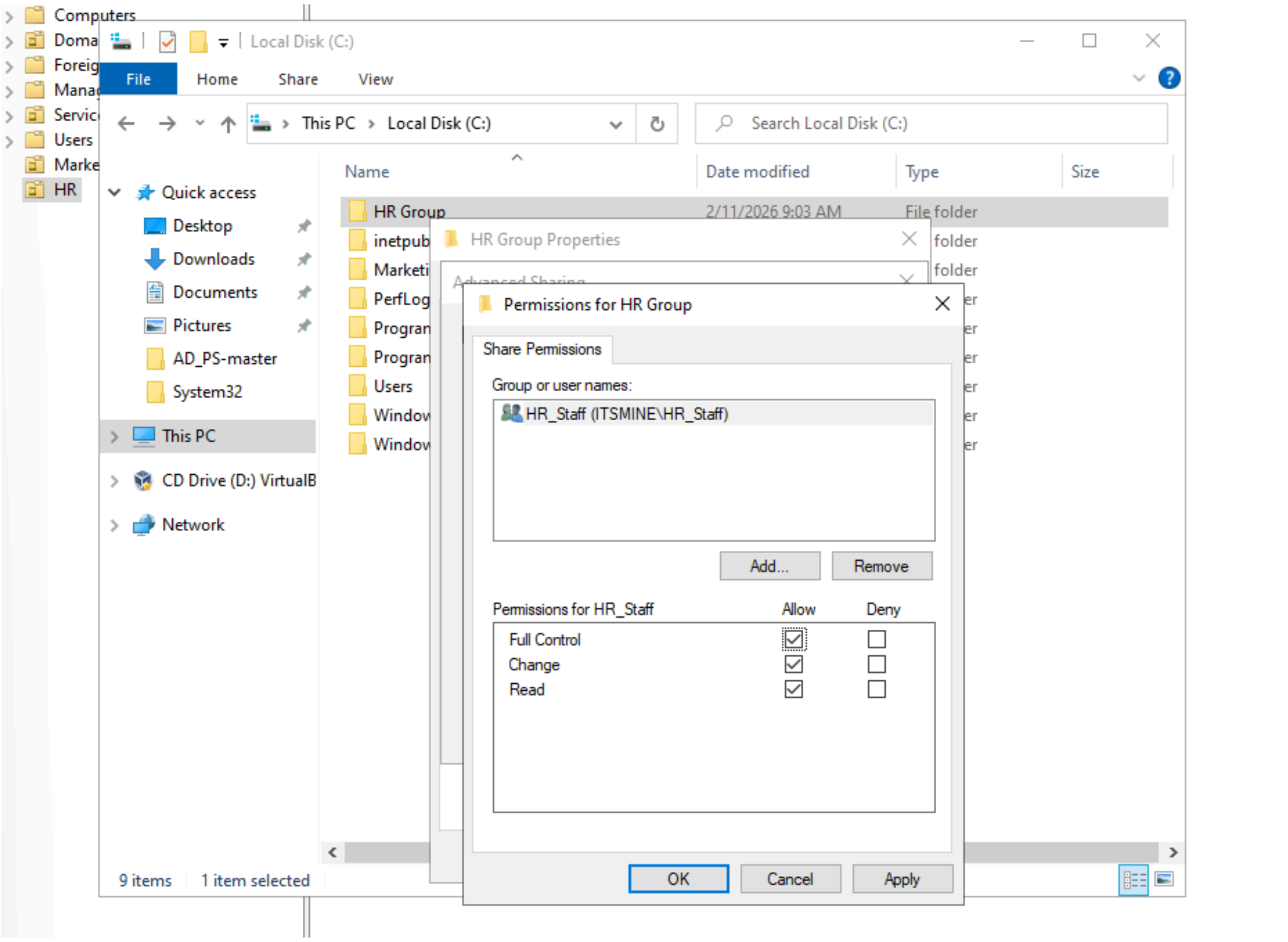


Marketing folder permissions were reviewed to confirm restricted access settings.

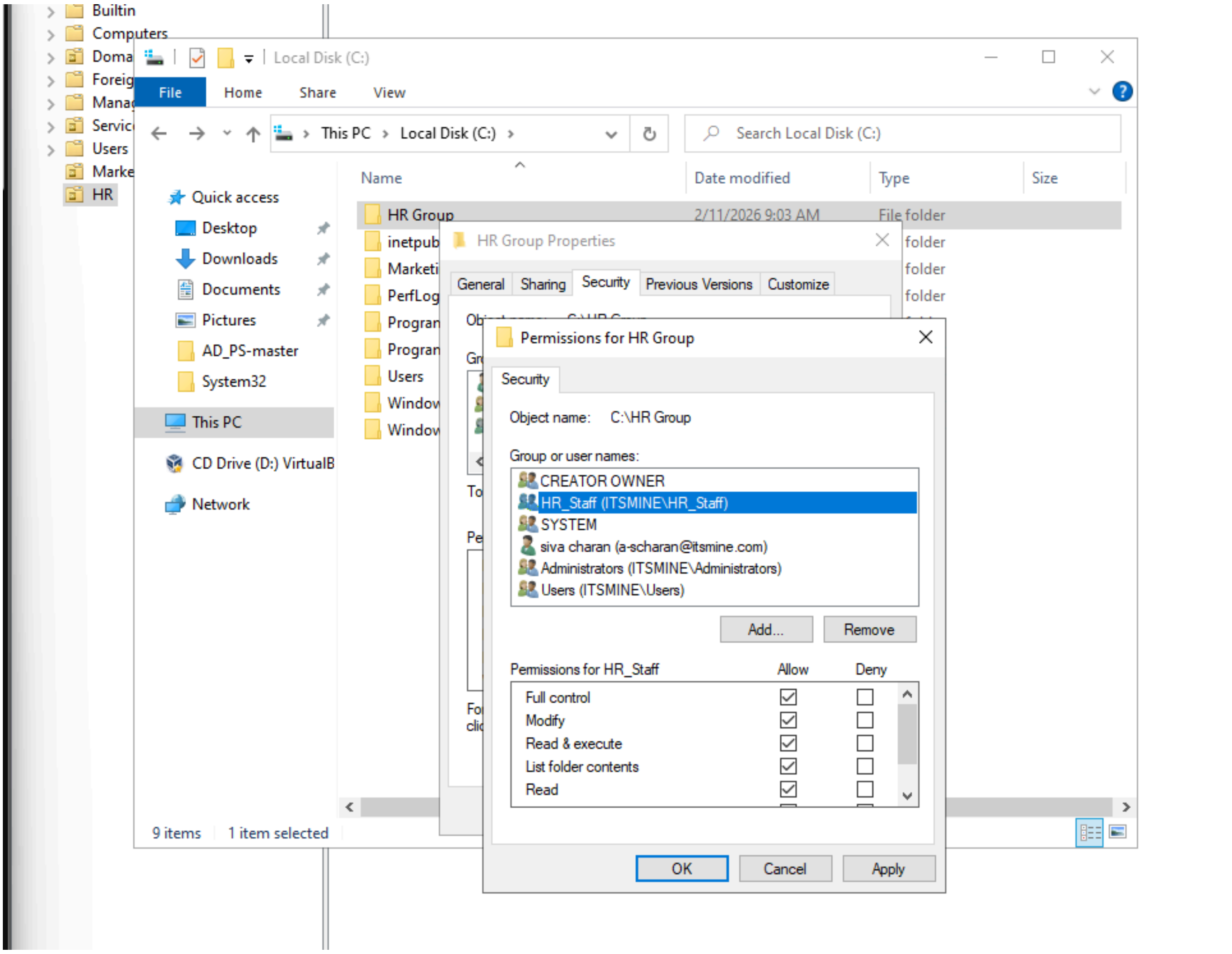


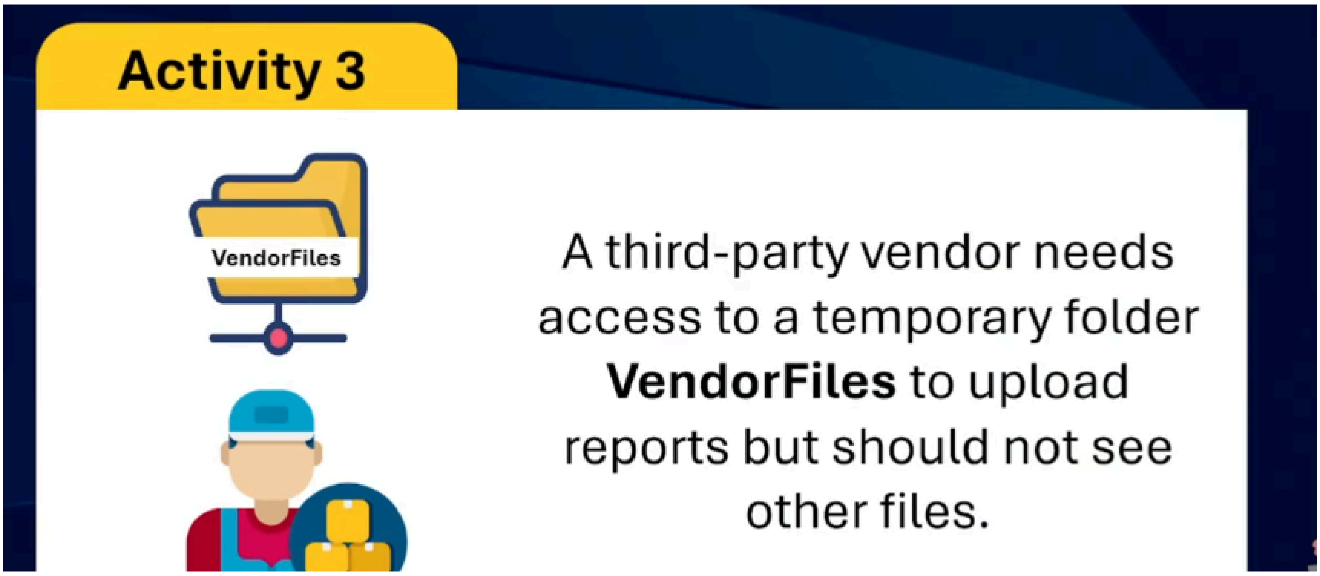


Share permissions were configured to allow access exclusively to the HR Staff group.

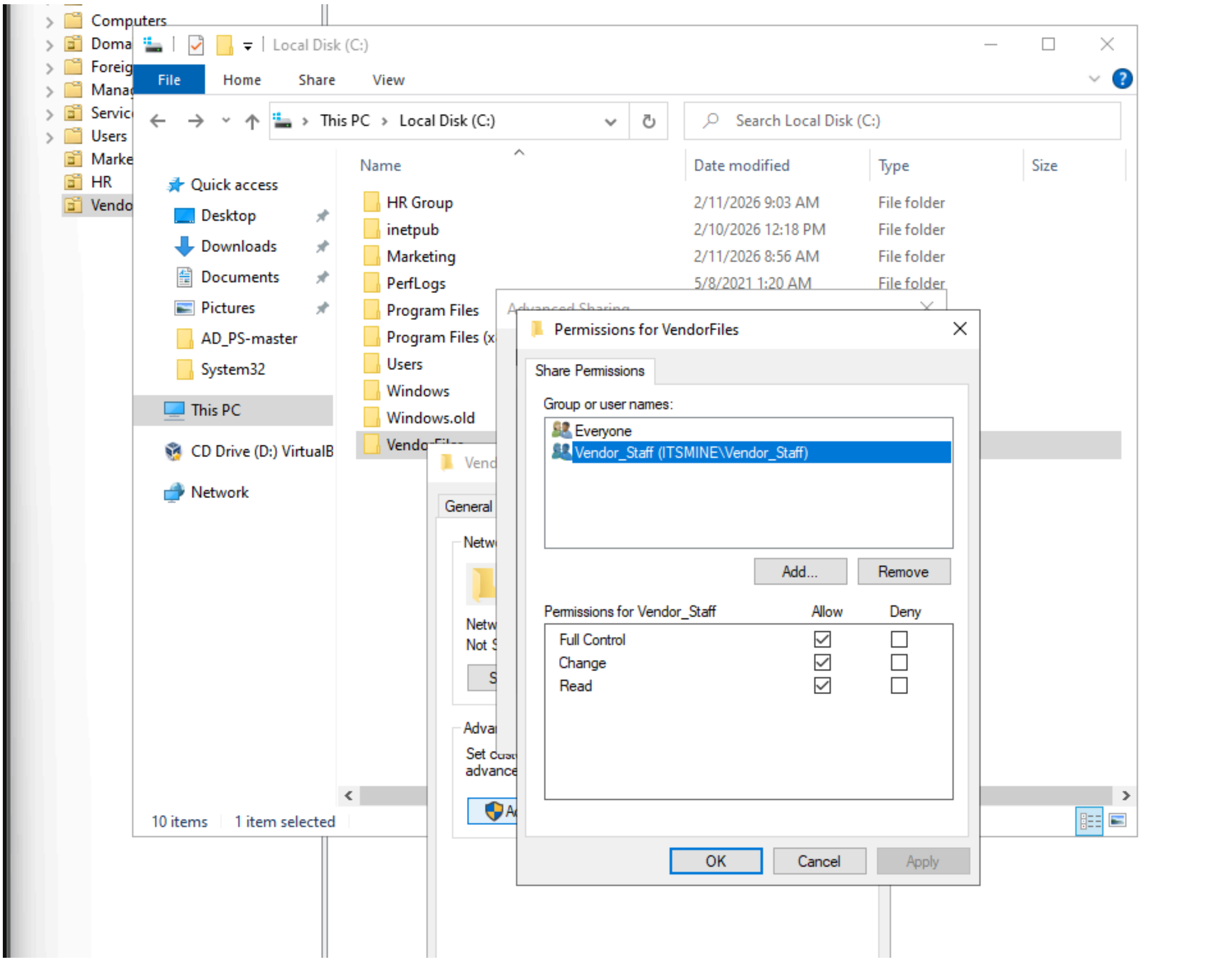


NTFS permissions were set to ensure only HR users have full control, while others have no access

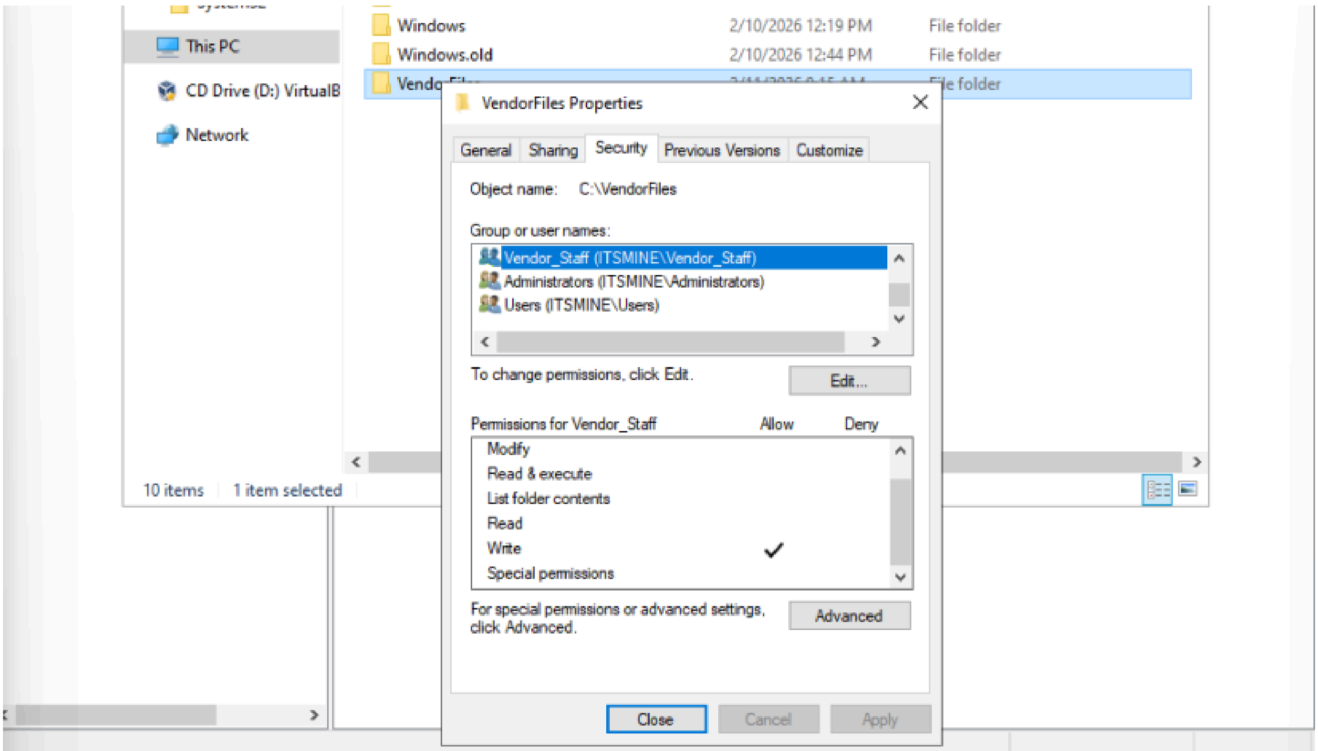


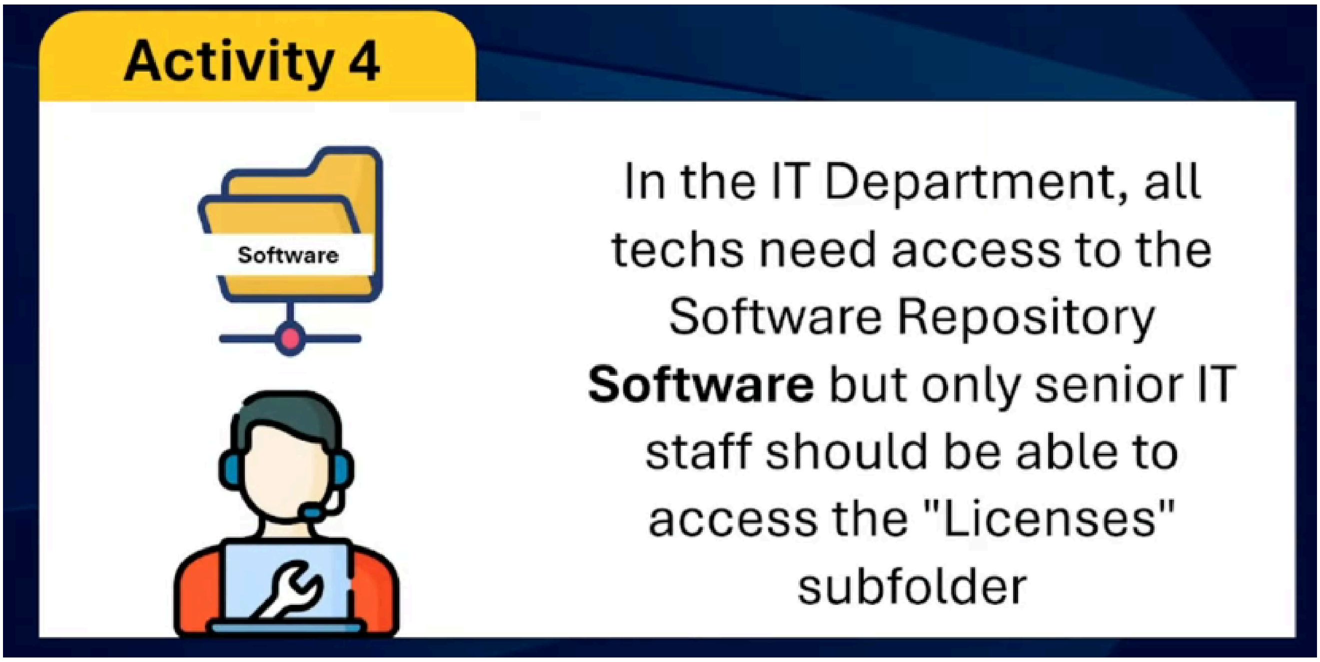


Share permissions were configured to allow the Vendor group appropriate access for report uploads.

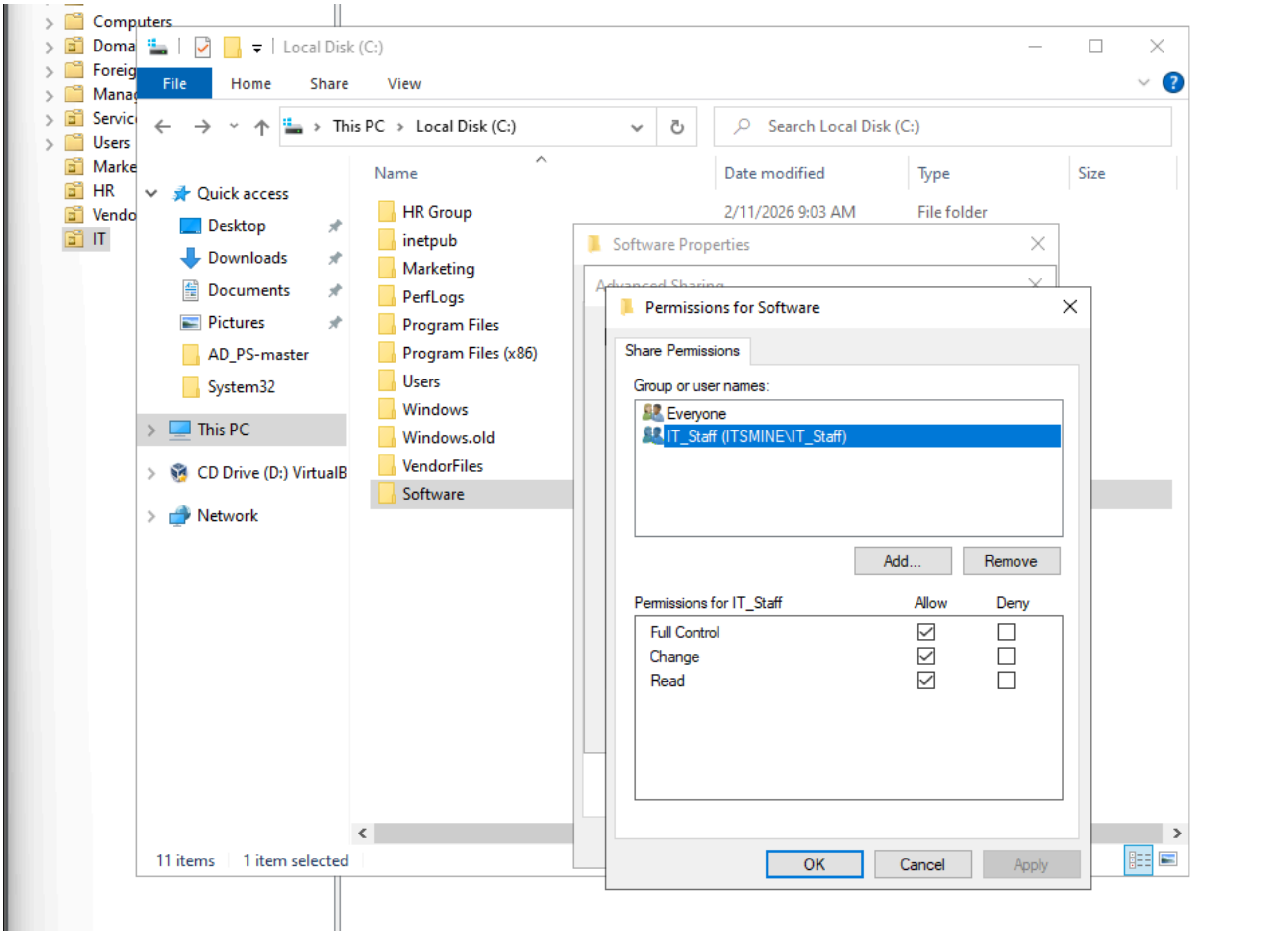


NTFS permissions were adjusted to allow write access without exposing other sensitive files

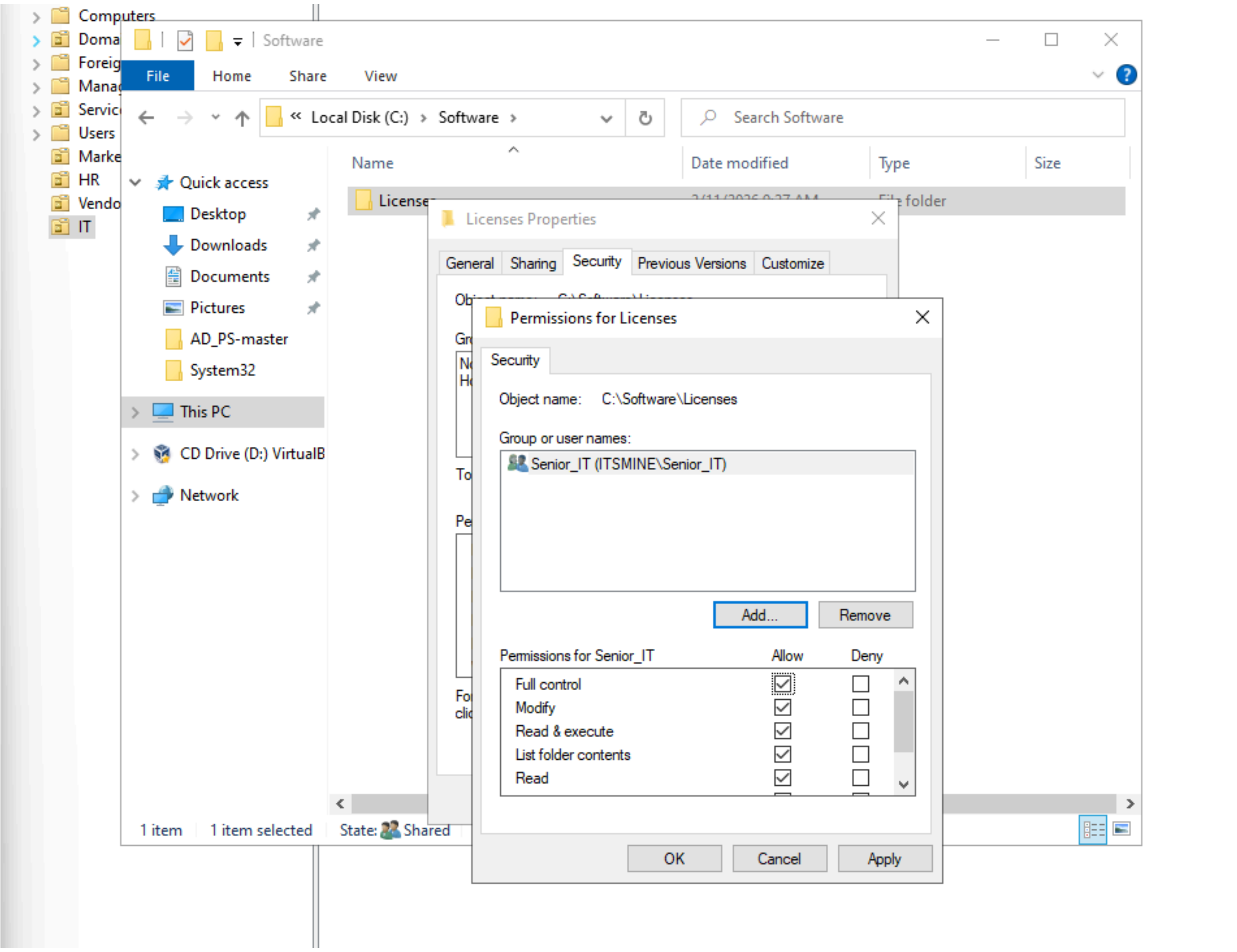




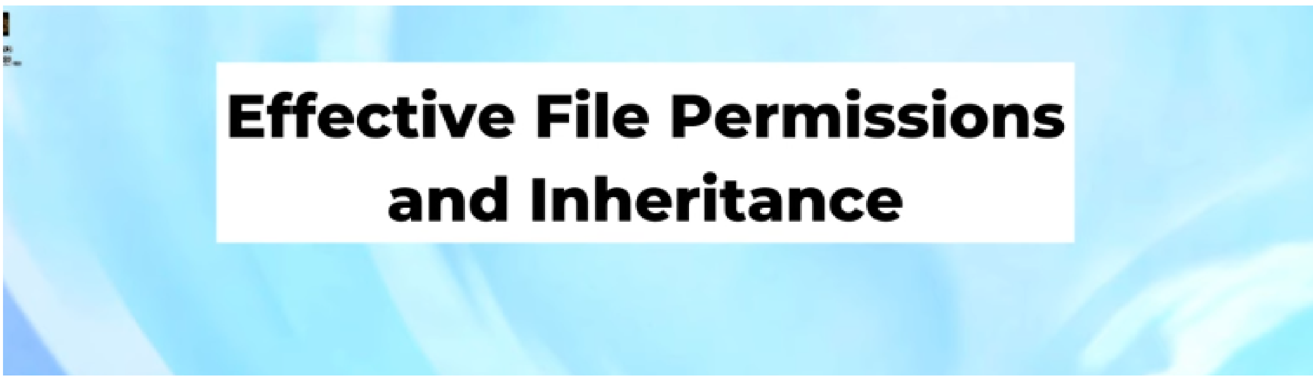
Software repository permissions were configured to allow IT staff access.



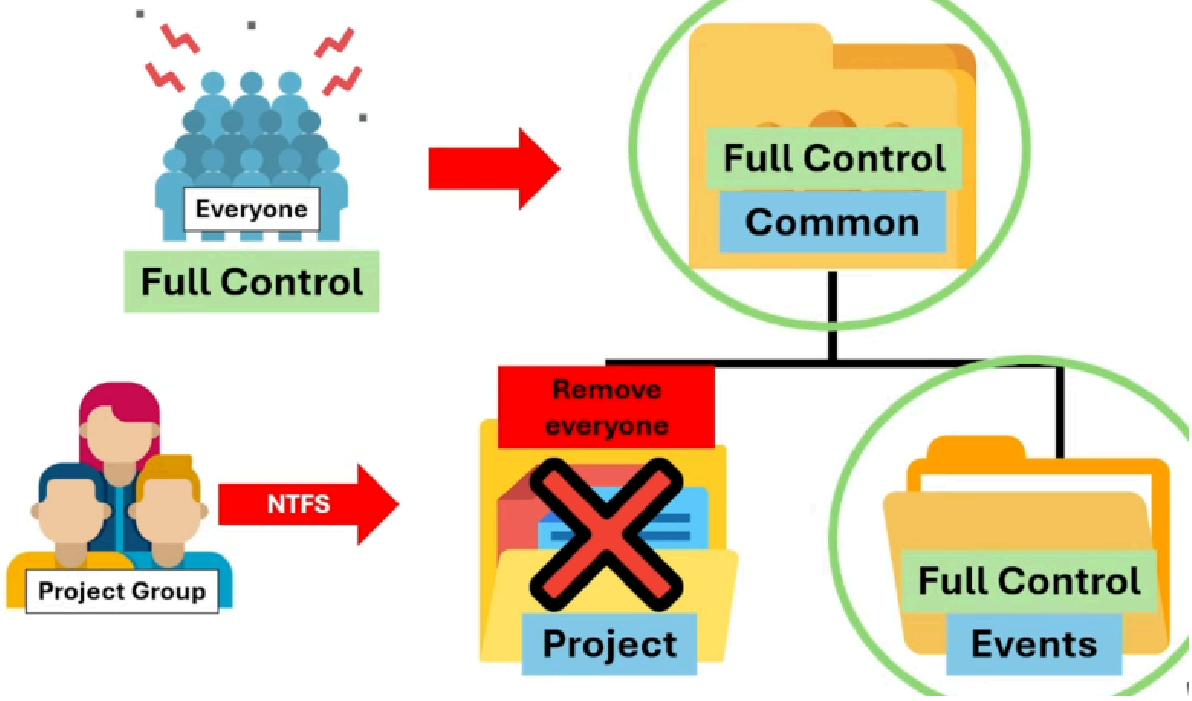
Additional NTFS restrictions were applied so that only Senior IT staff can access the Licenses folder.



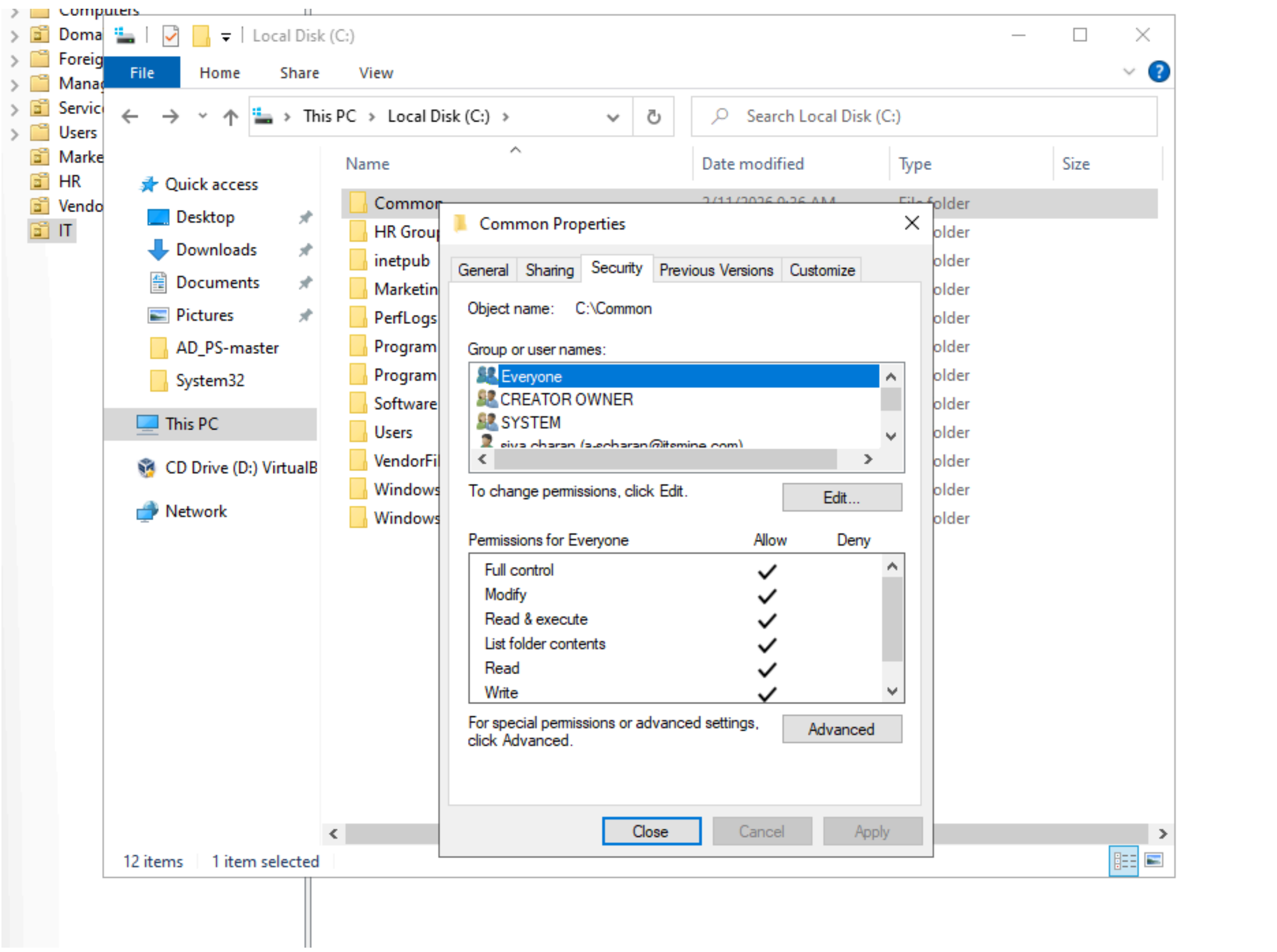
EFFECTIVE FILE PERMISSSION AND INHERITANCE :



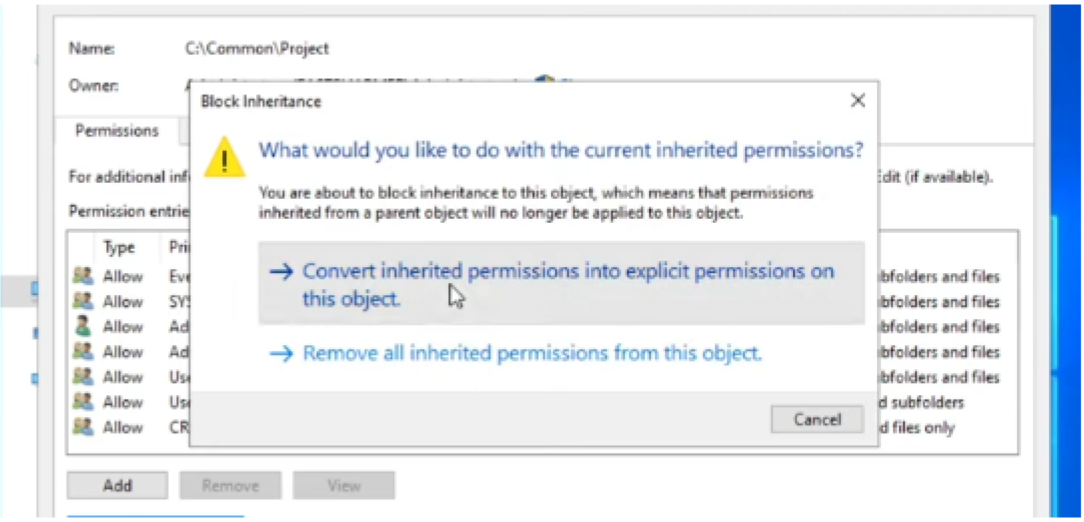
Scenario:



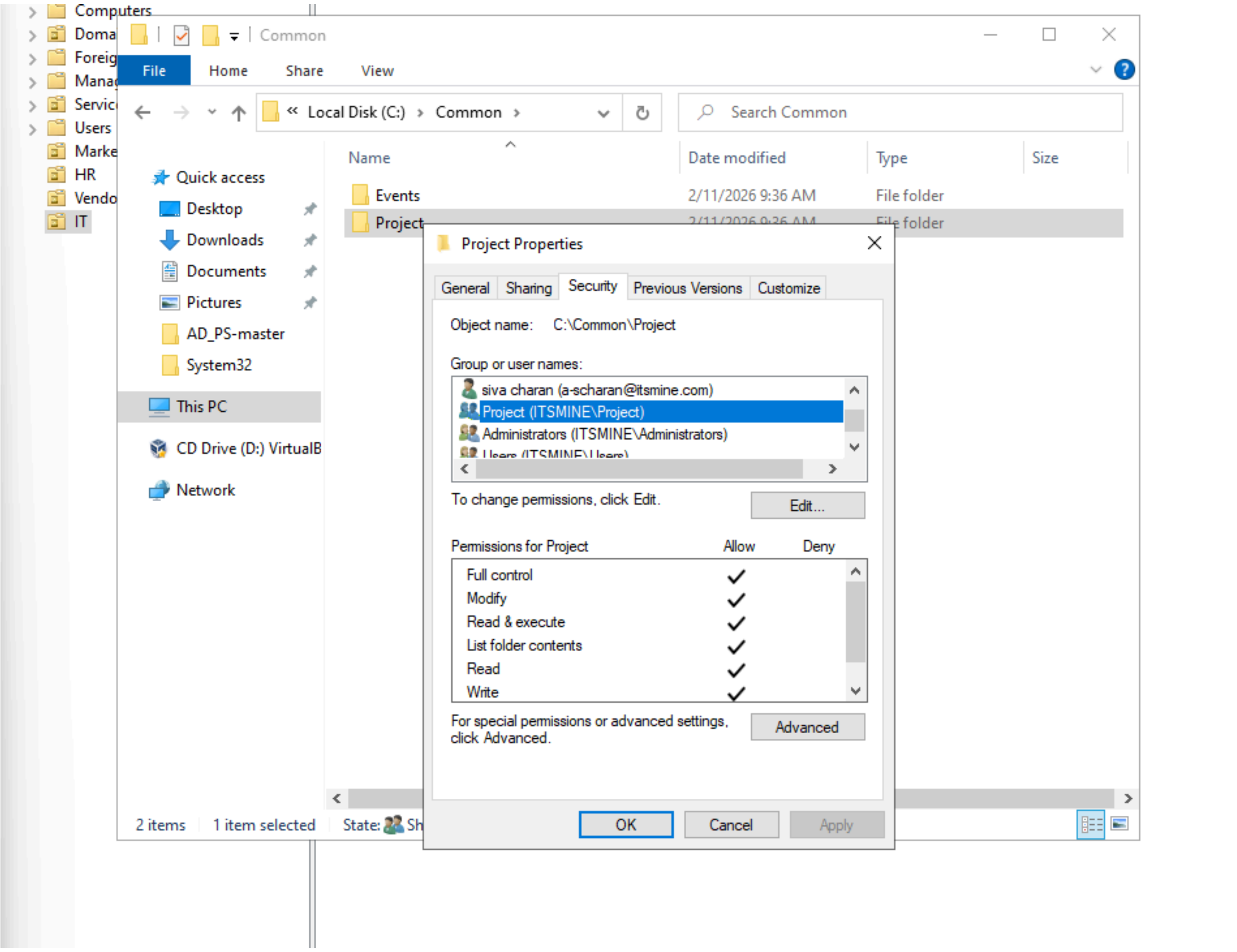
Permissions for the Common folder were reviewed to analyze inherited access entries.

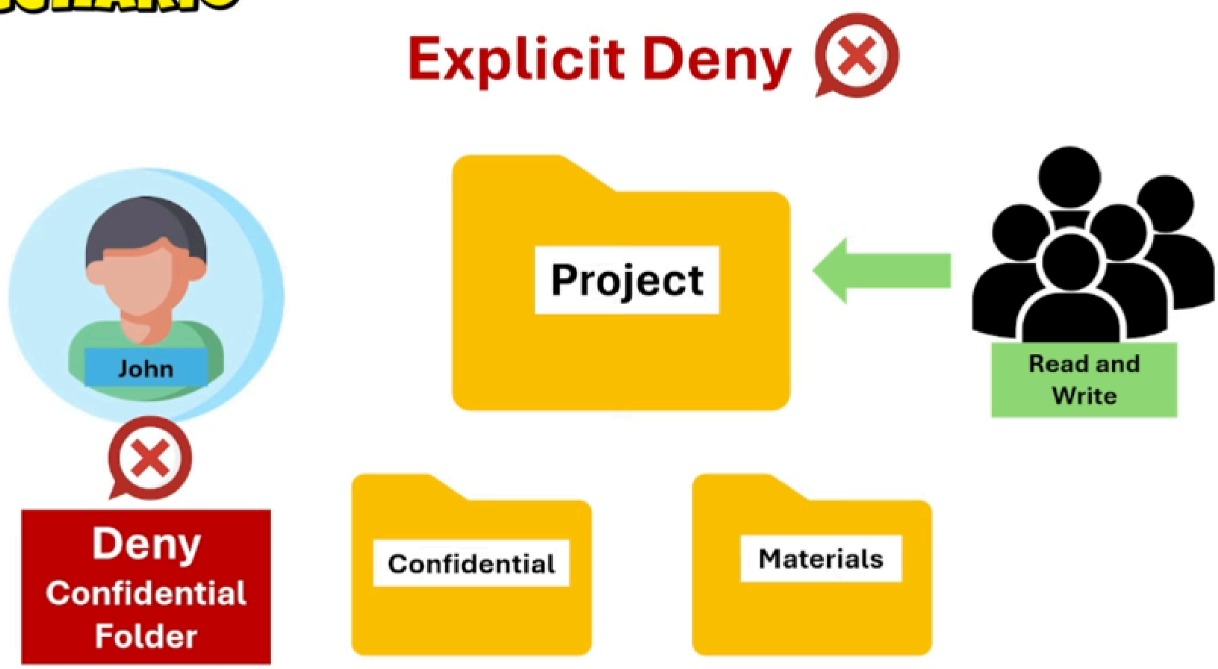


Inheritance was blocked on a subfolder to convert inherited permissions into explicit permissions. This allows fine-grained control over folder access.

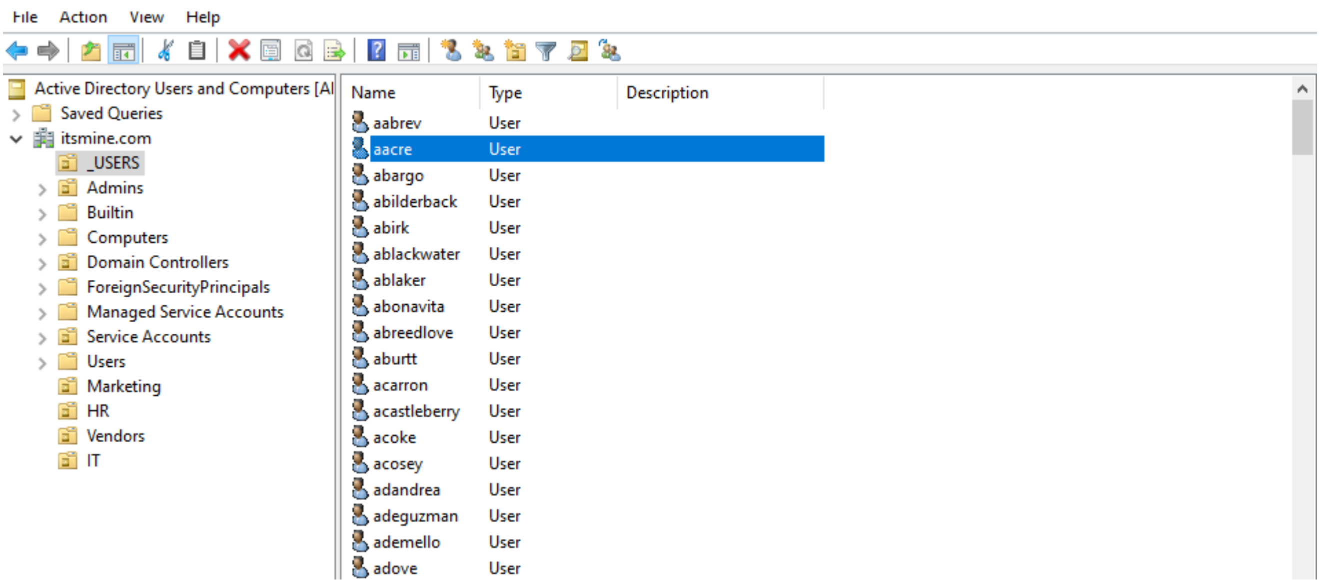


Permissions for the Project folder were configured to control access at a granular level. Specific users and groups were assigned appropriate rights to manage folder security.

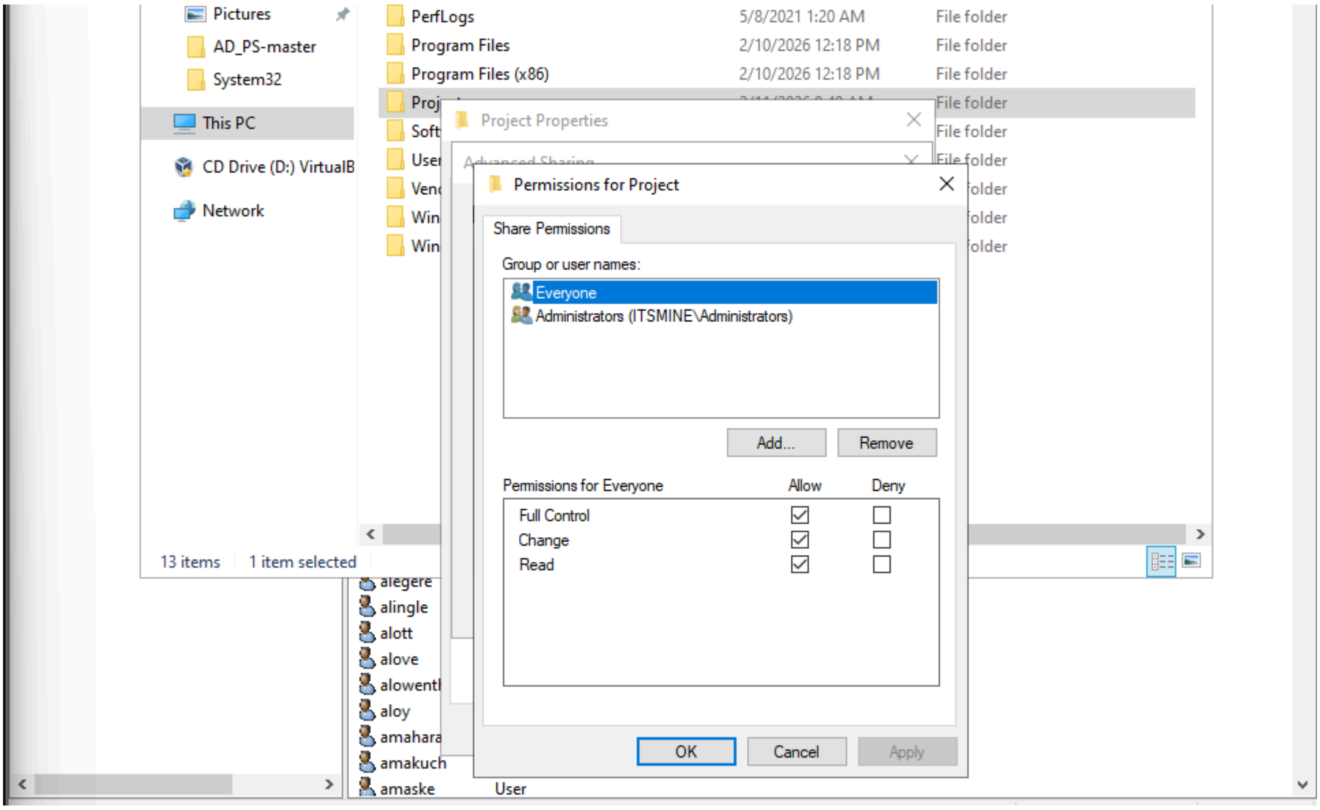




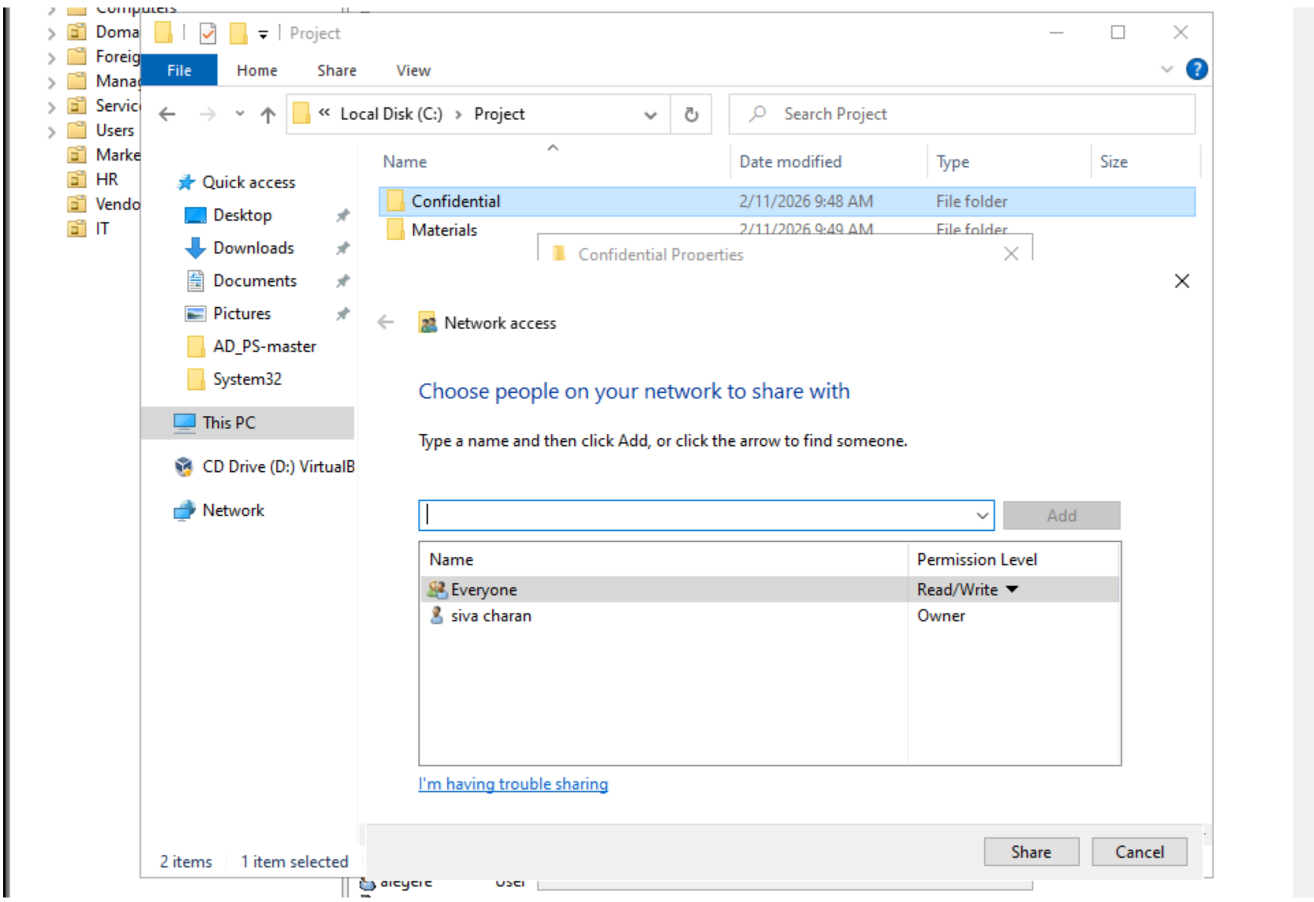
User accounts were reviewed in Active Directory to identify members involved in the permission configuration.



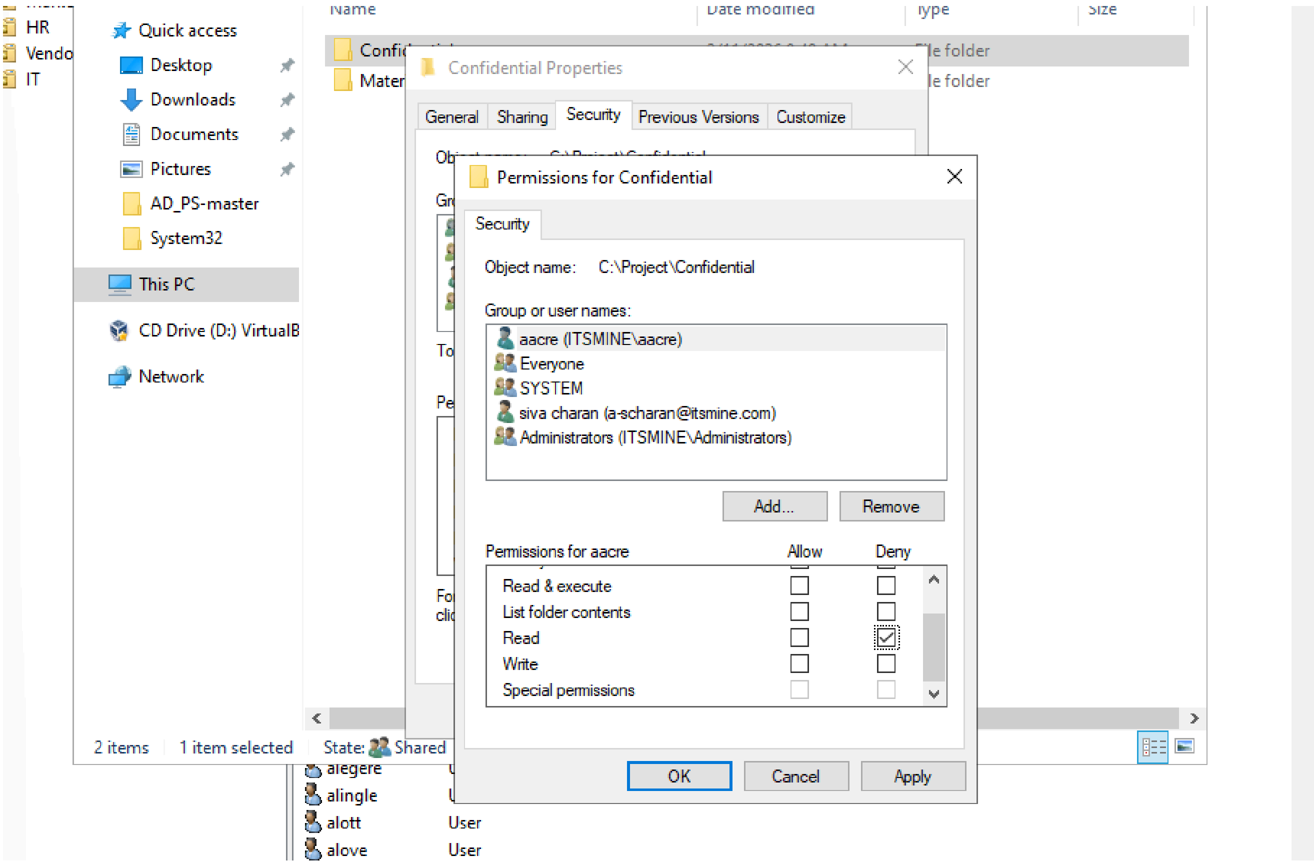
Share permissions were configured to define network-level access to the Project folder. Access was restricted based on defined user groups.



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

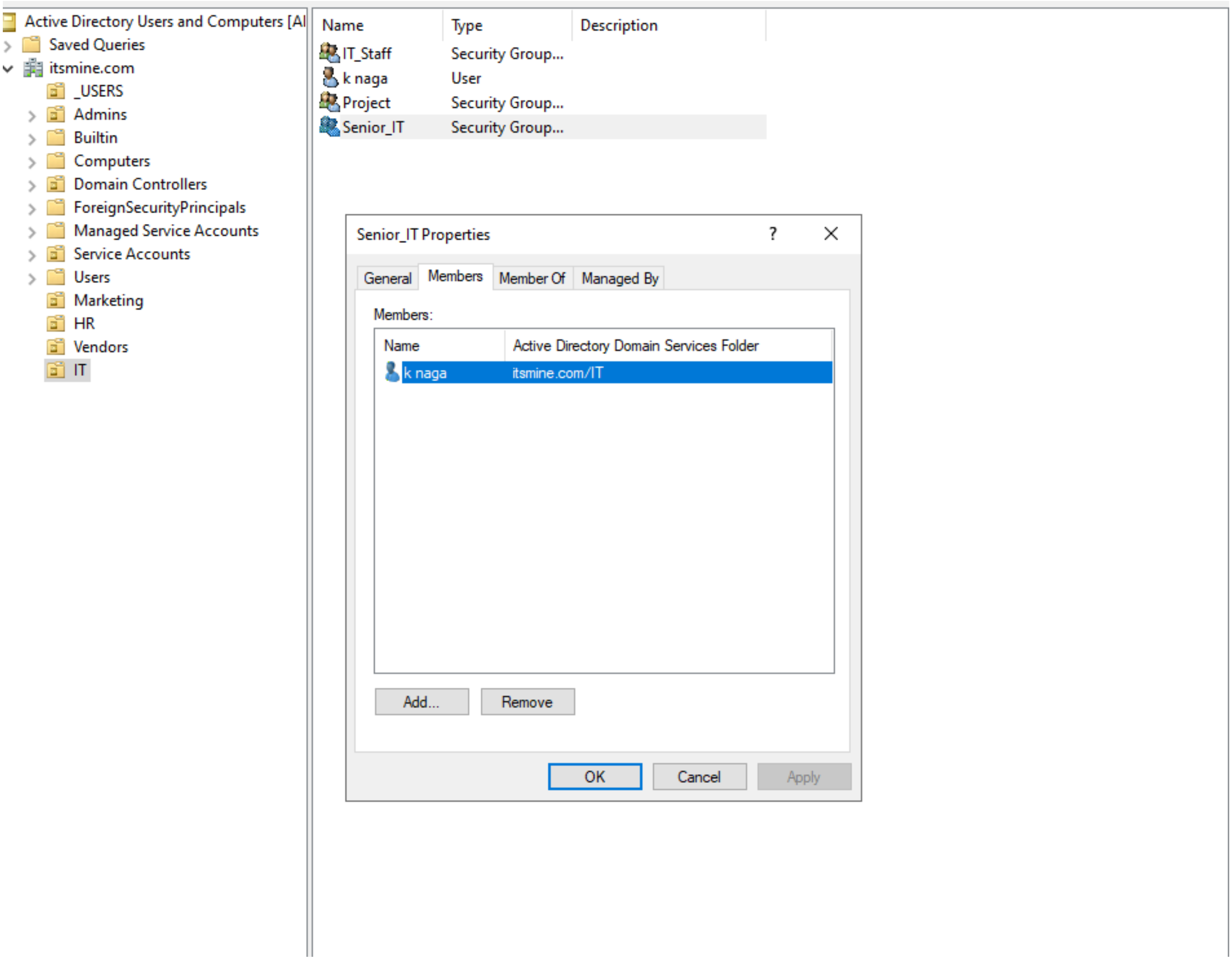


NTFS permissions were adjusted to remove unnecessary access and ensure only specific users could read or modify content.

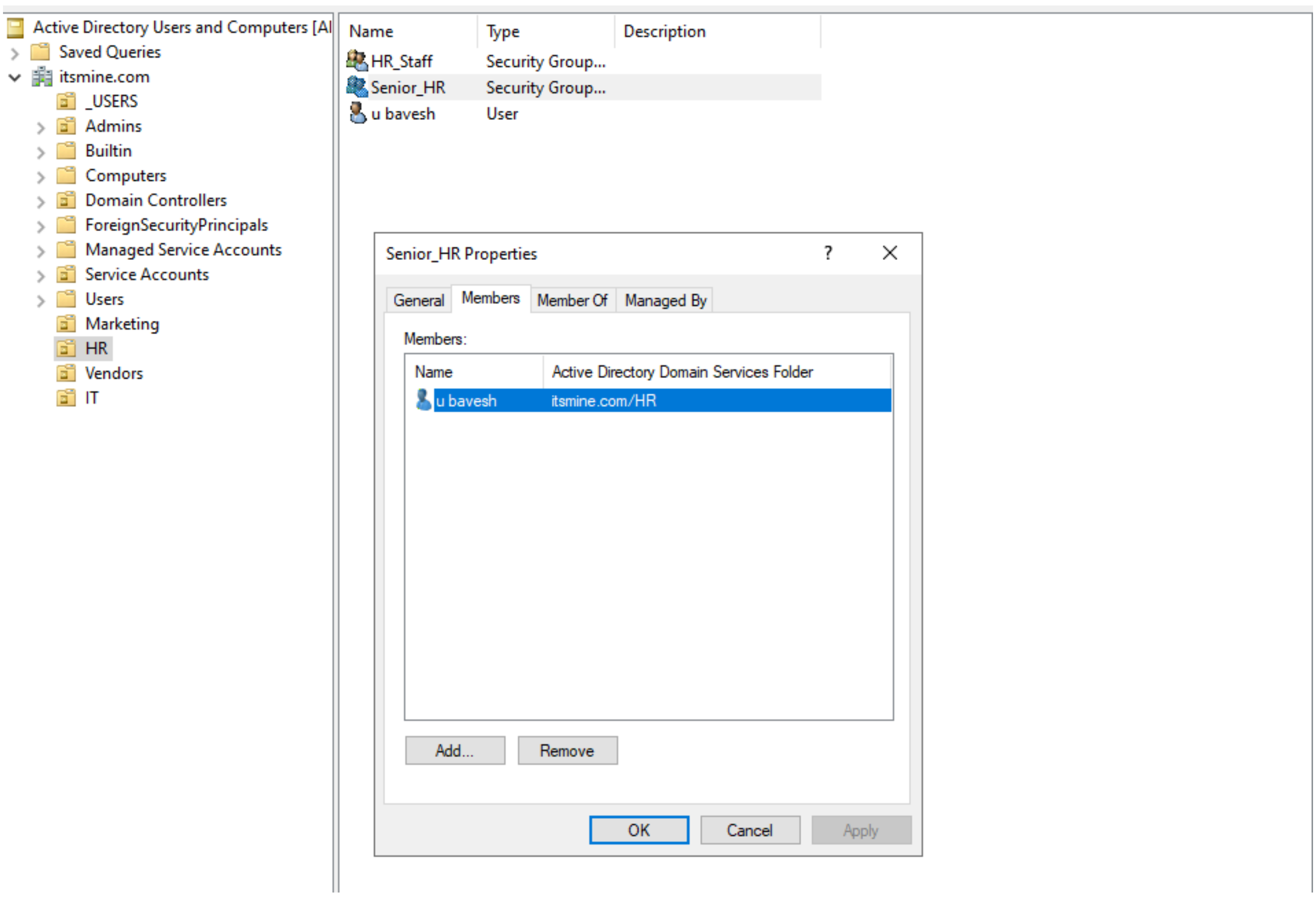


ACCESS BASED ENUMERATION :

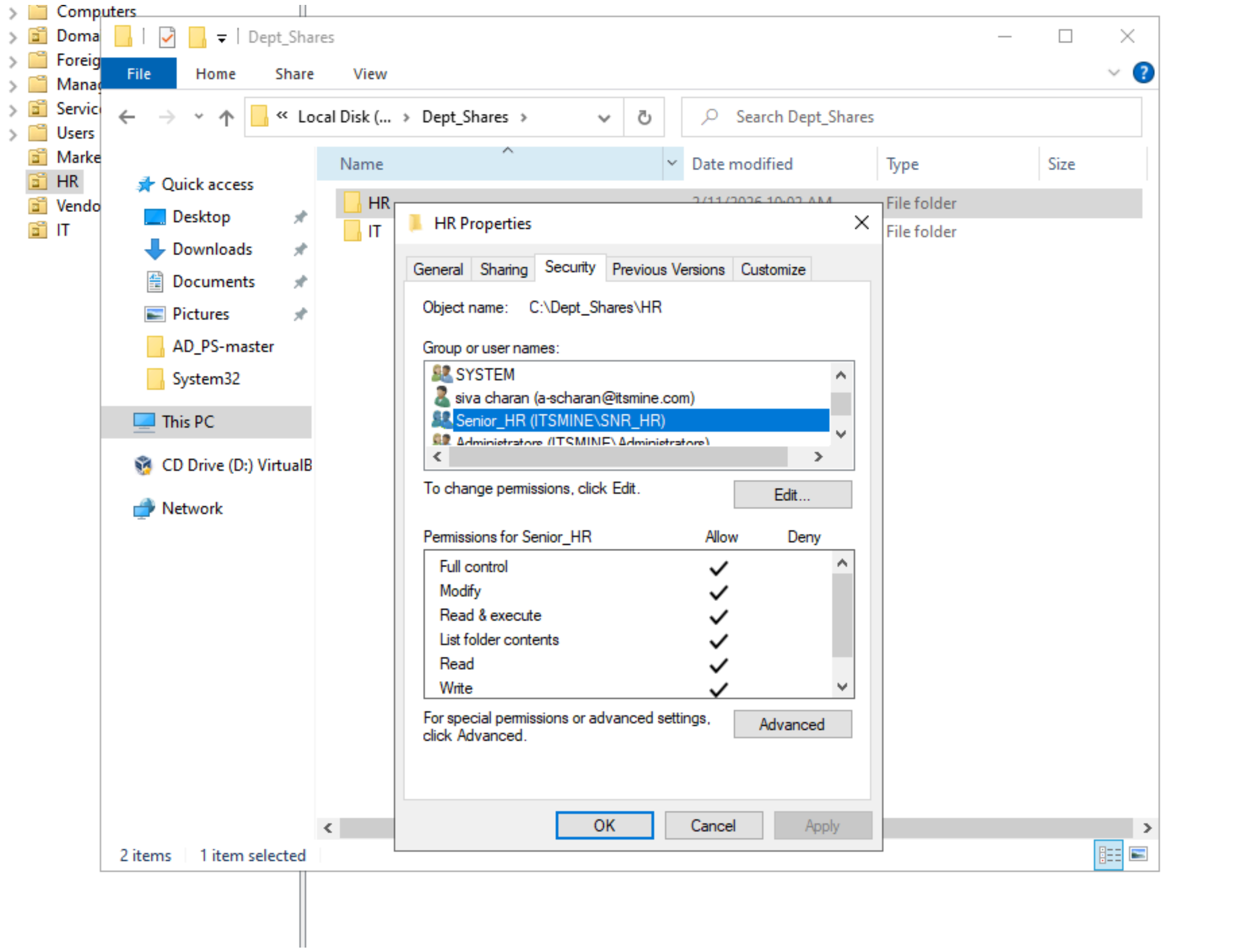
User membership in the Senior_IT group was verified to ensure correct access assignment



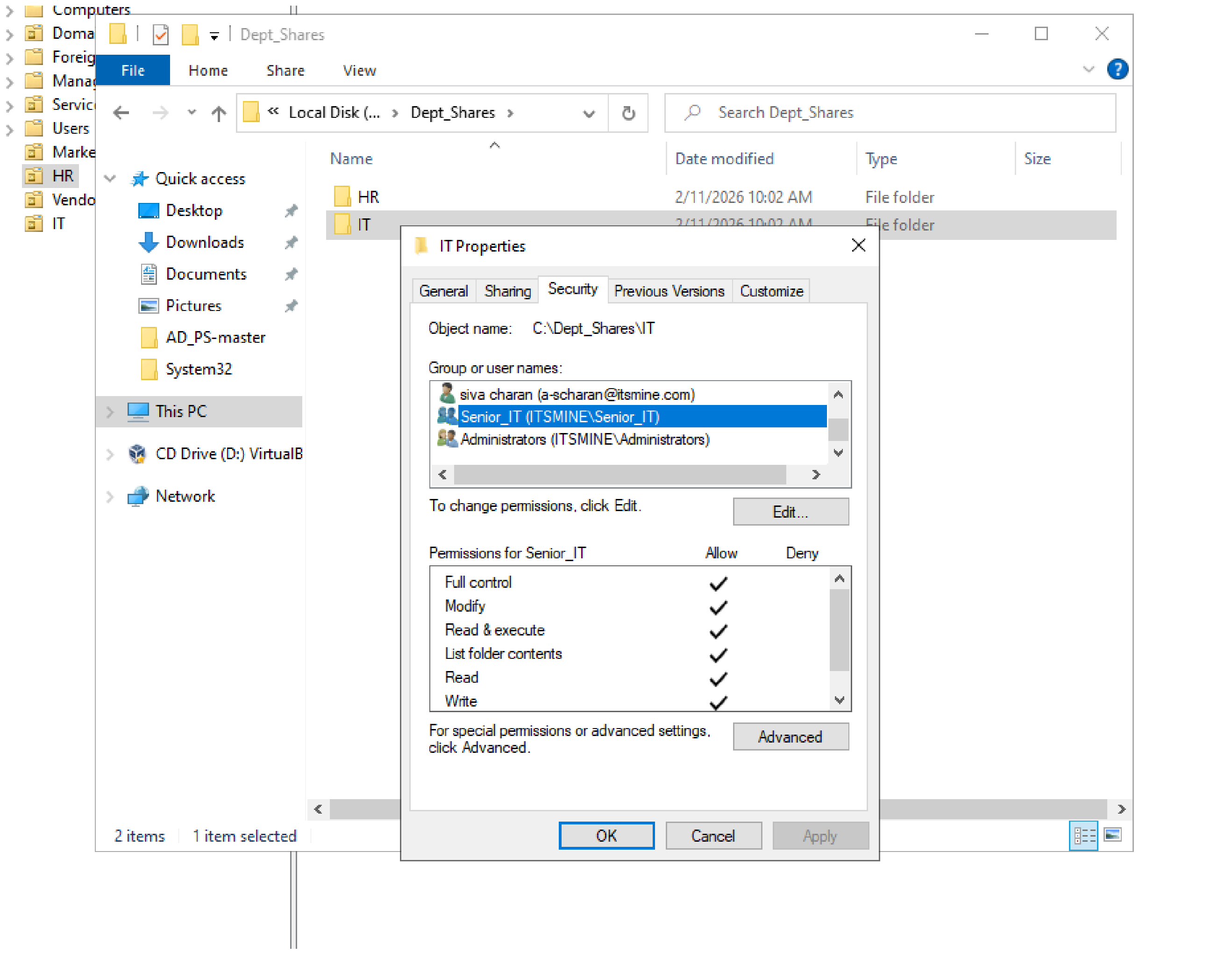
The Senior_HR security group was reviewed and validated for correct user membership.



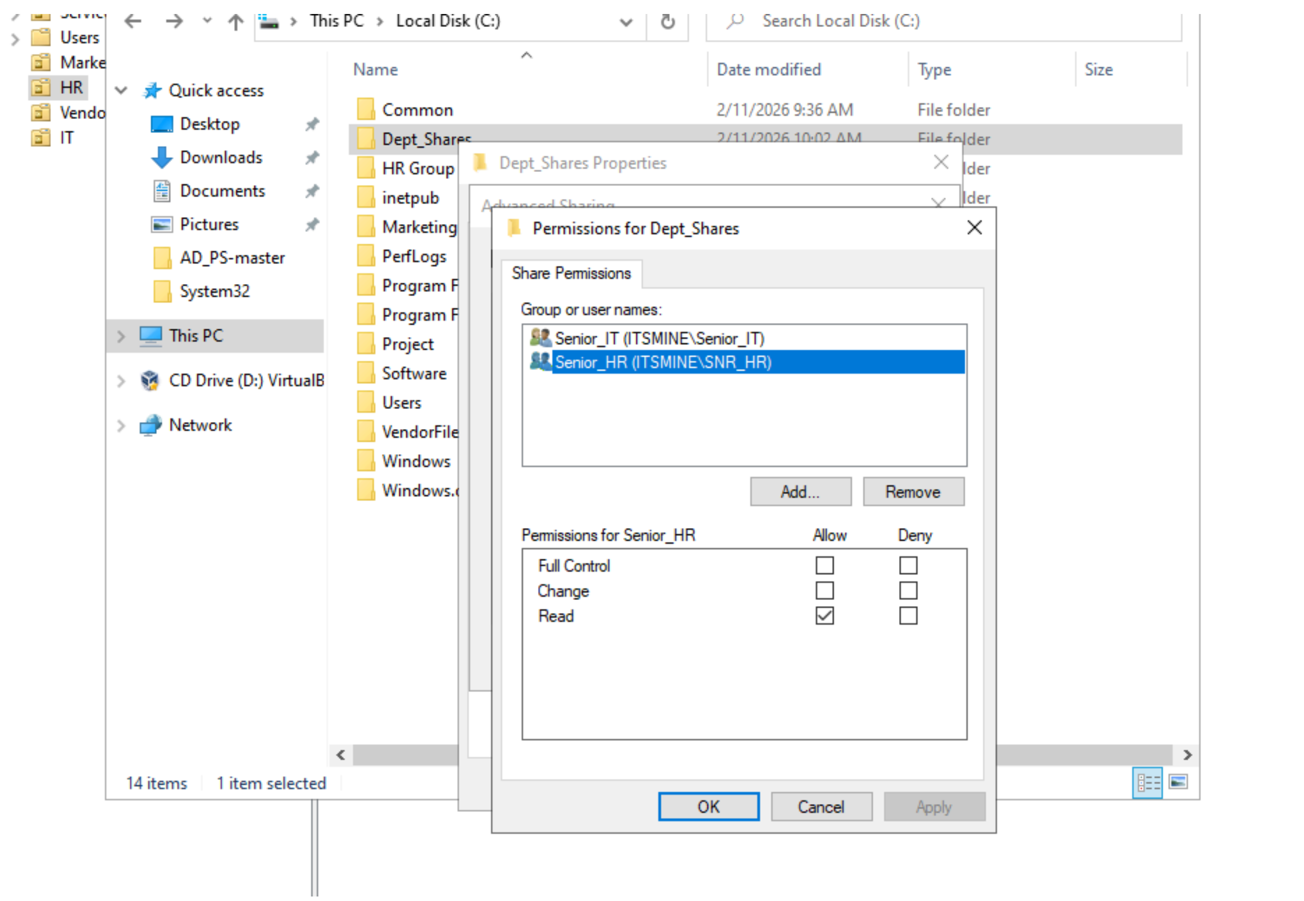
Permissions for the HR folder were configured to allow access only to authorized HR staff members.



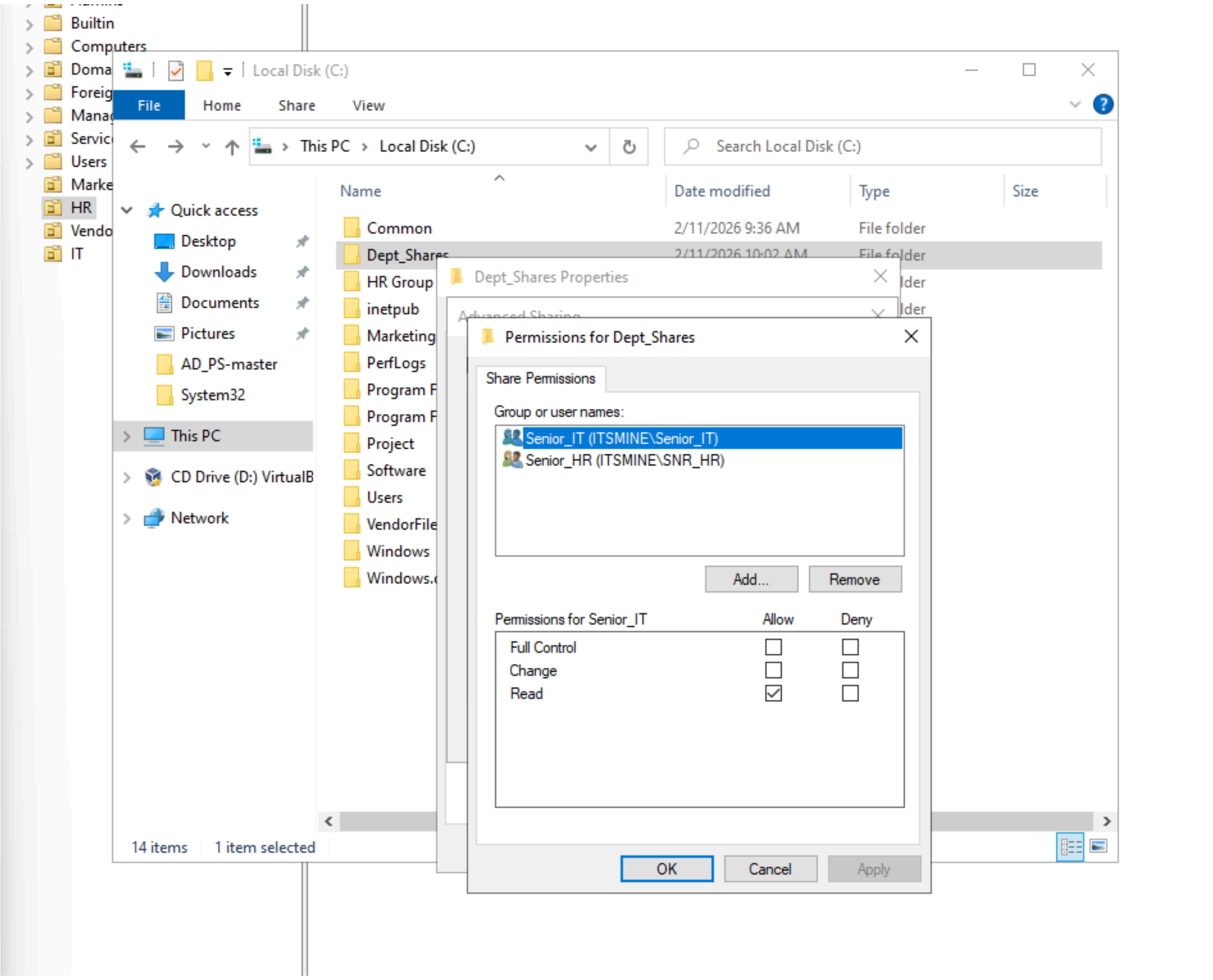
NTFS permissions were configured for the IT folder to grant access only to designated IT users.



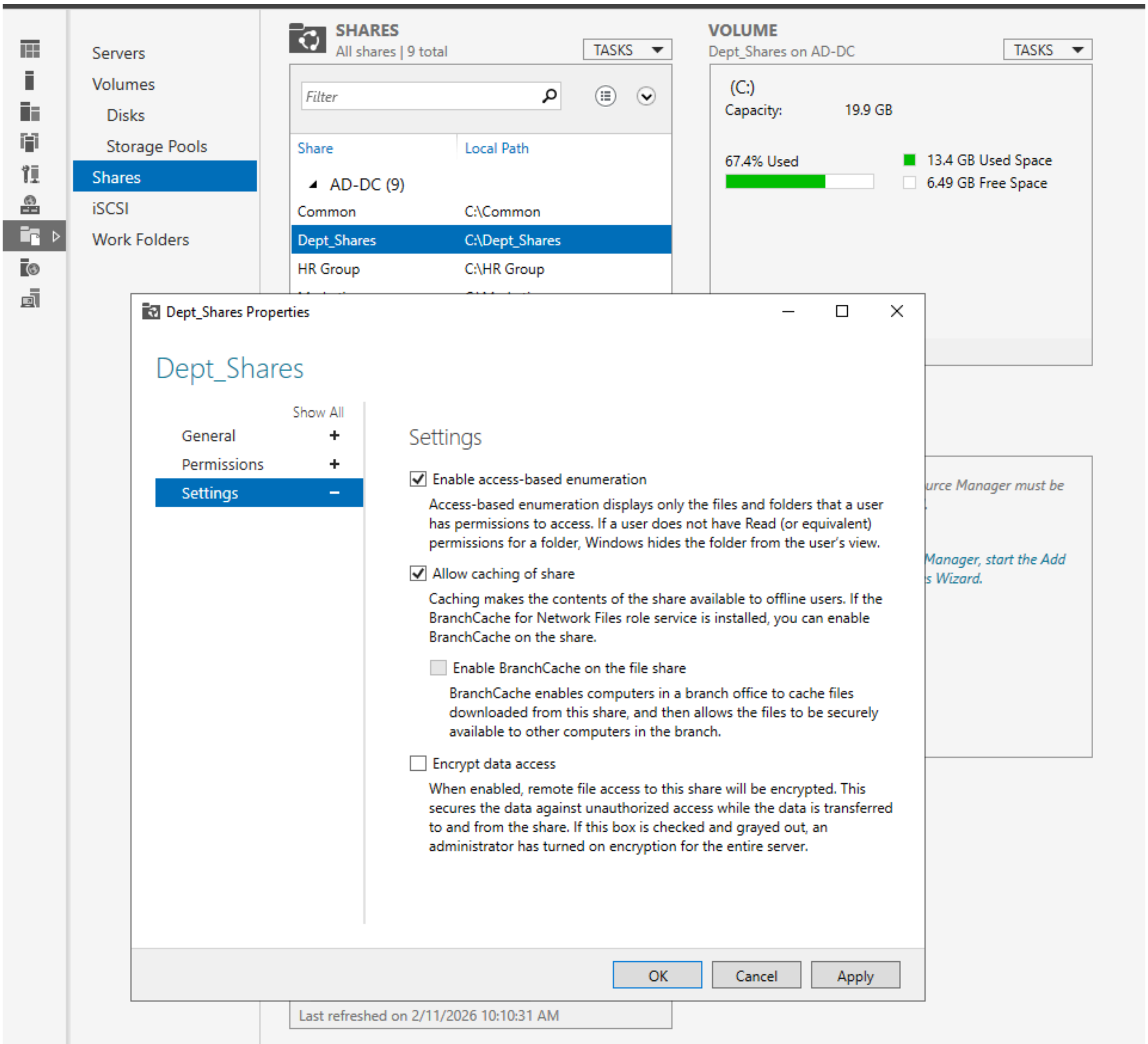
Share permissions for Dept_Shares were defined to restrict access based on group roles.



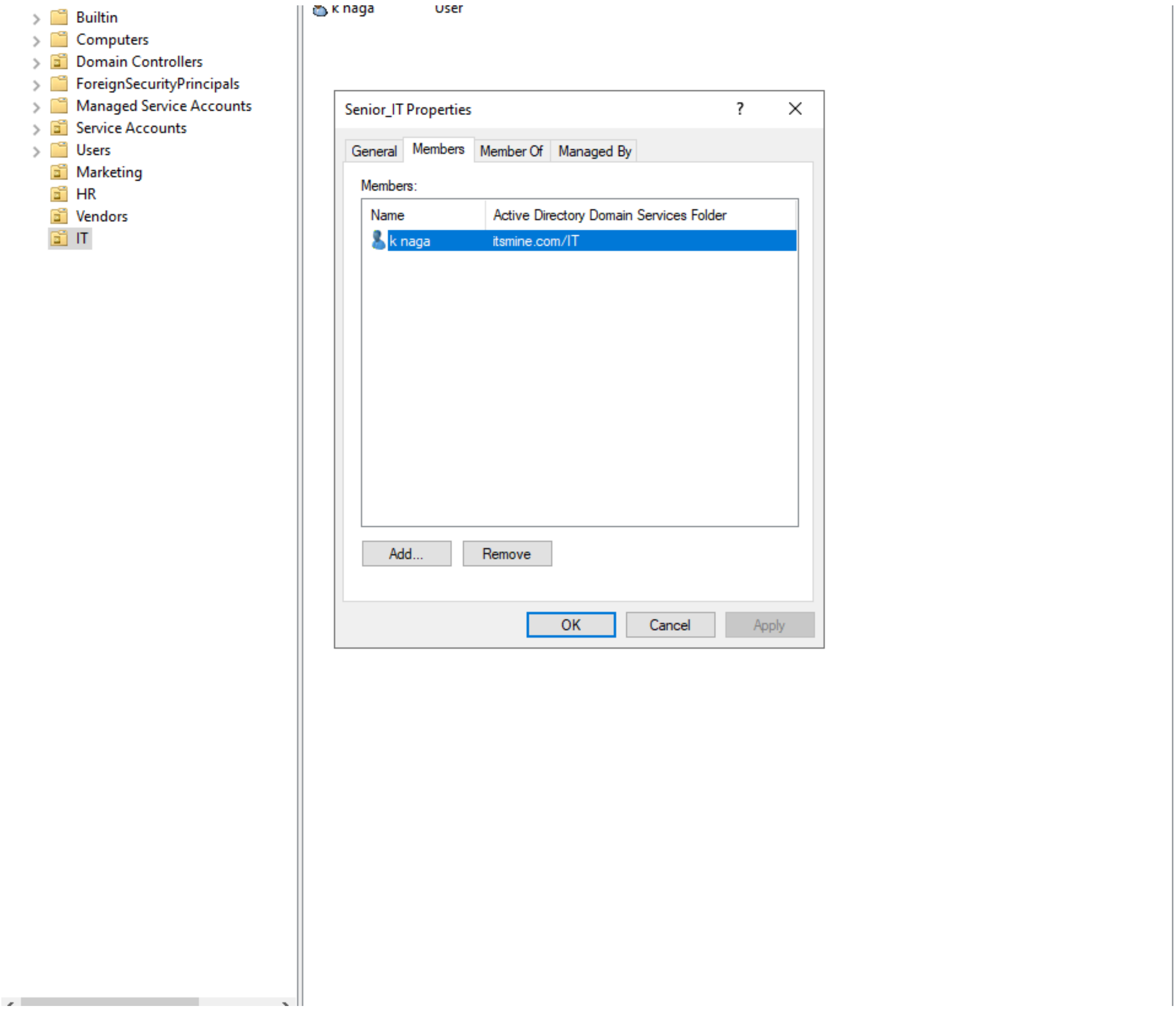
Specific security groups such as Senior_IT and Senior_HR were granted controlled access to the shared folder.



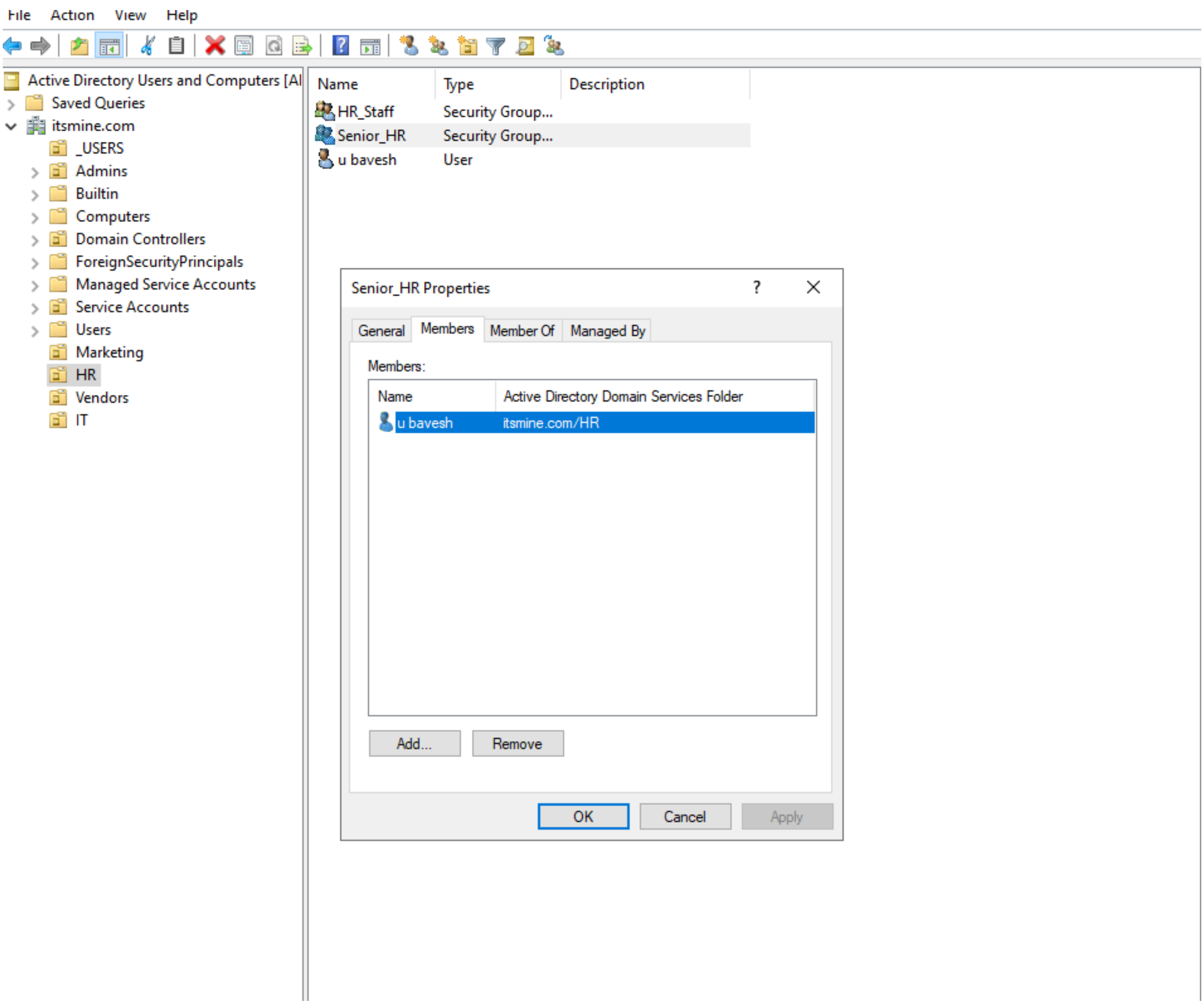
Access-Based Enumeration was enabled in the share settings. This ensures users can only see folders for which they have permissions.



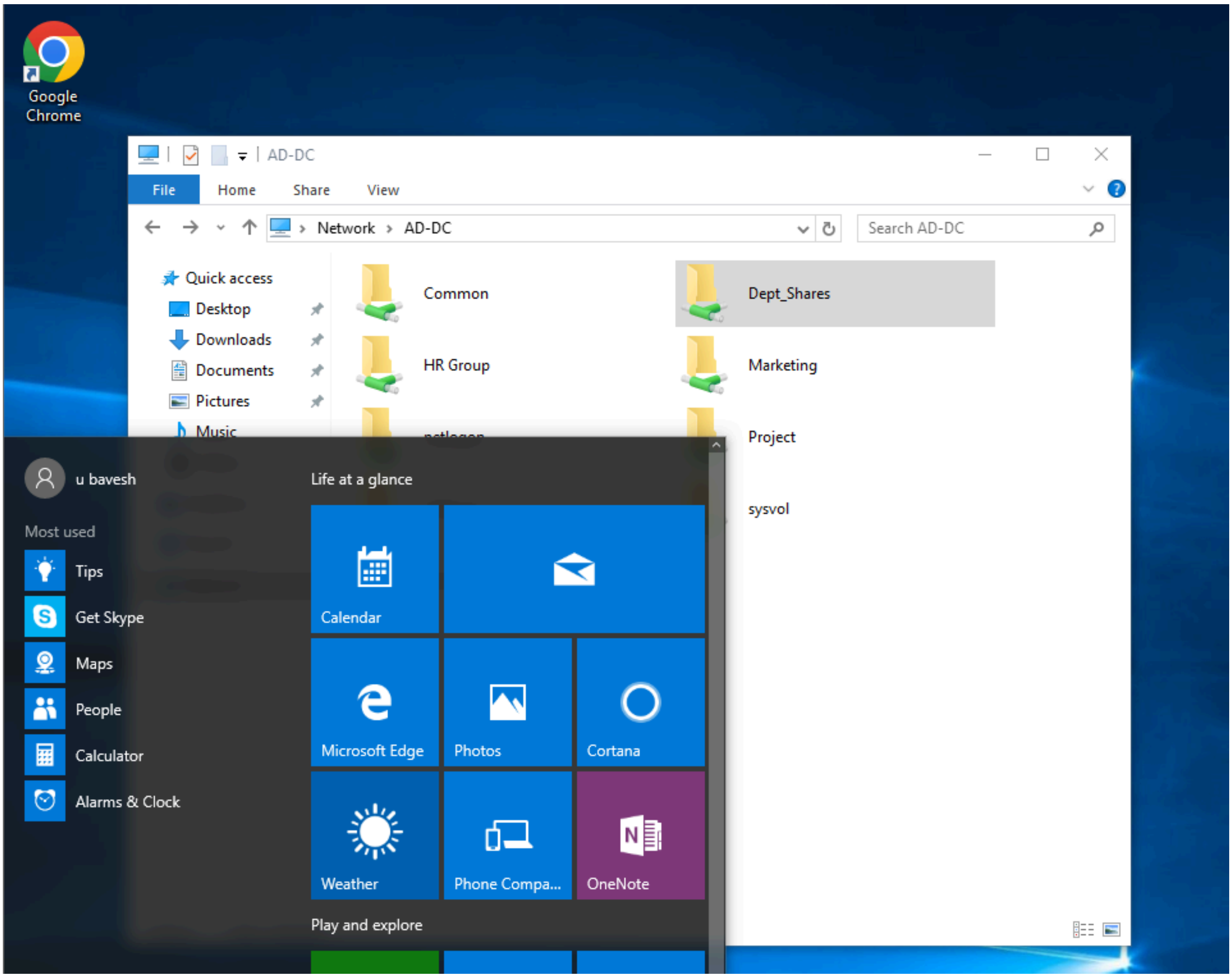
Group membership for Senior_IT was reviewed again to confirm access-based filtering will apply correctly.



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

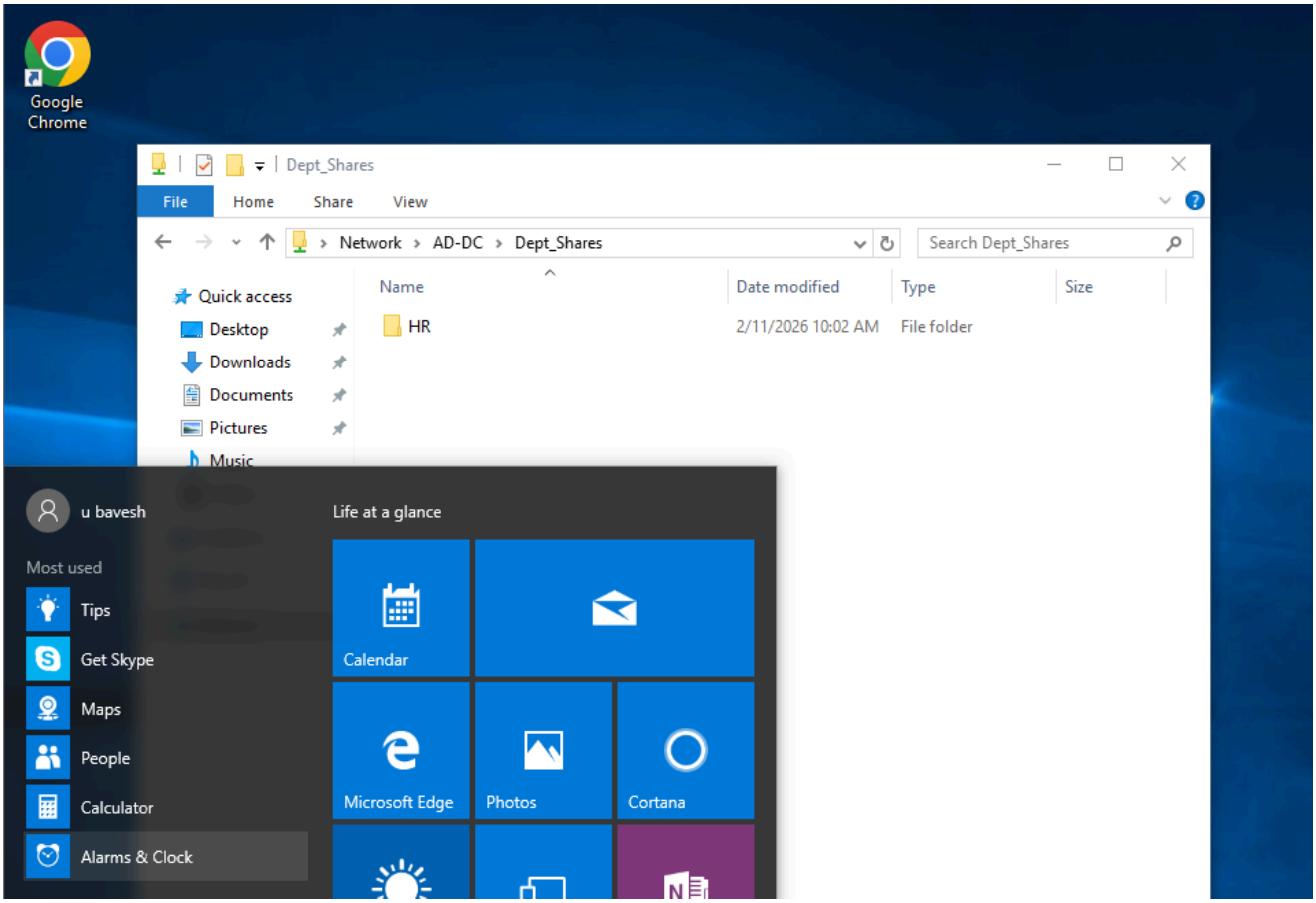


When logged in as an HR user, only permitted folders such as HR-related shares are visible.

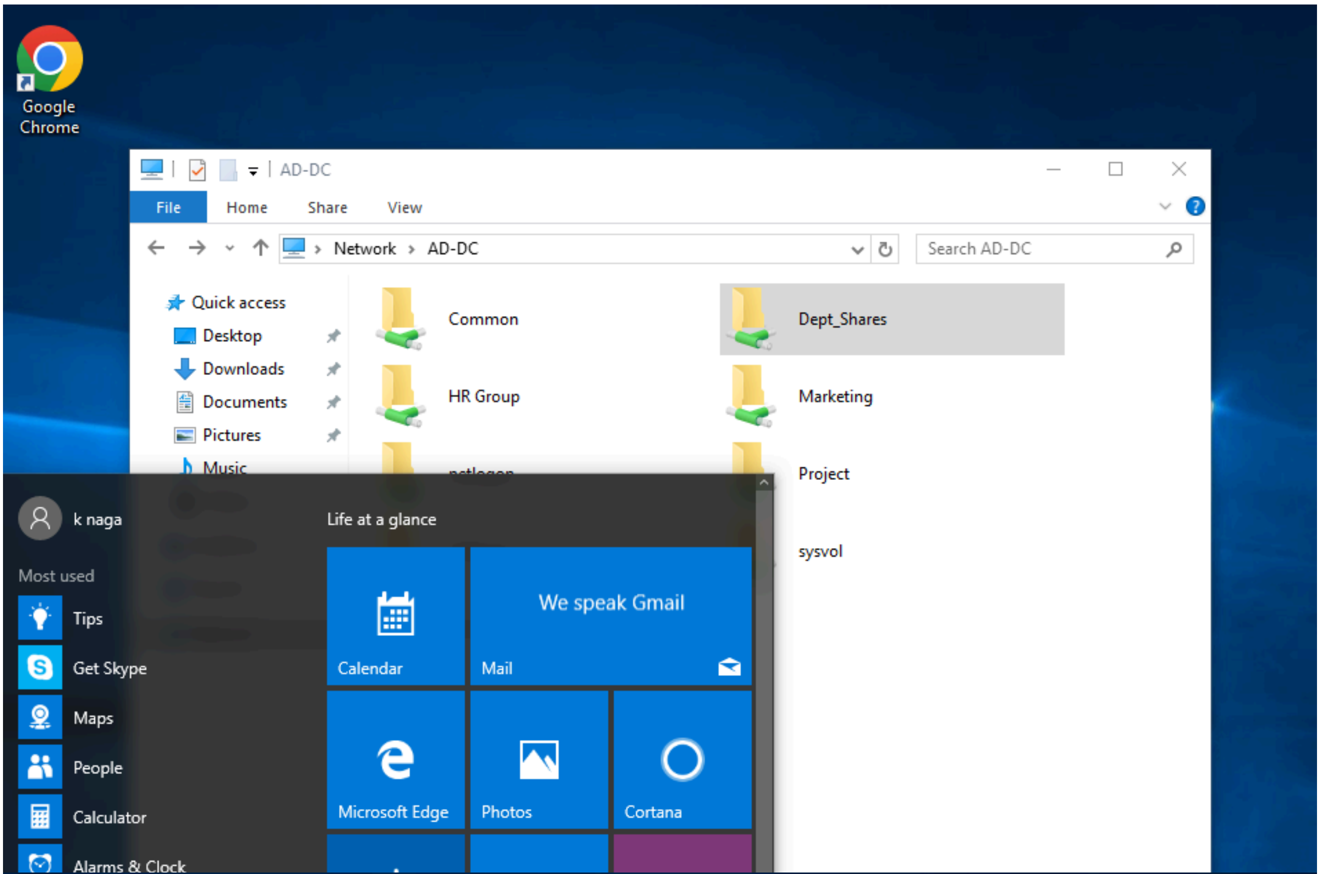


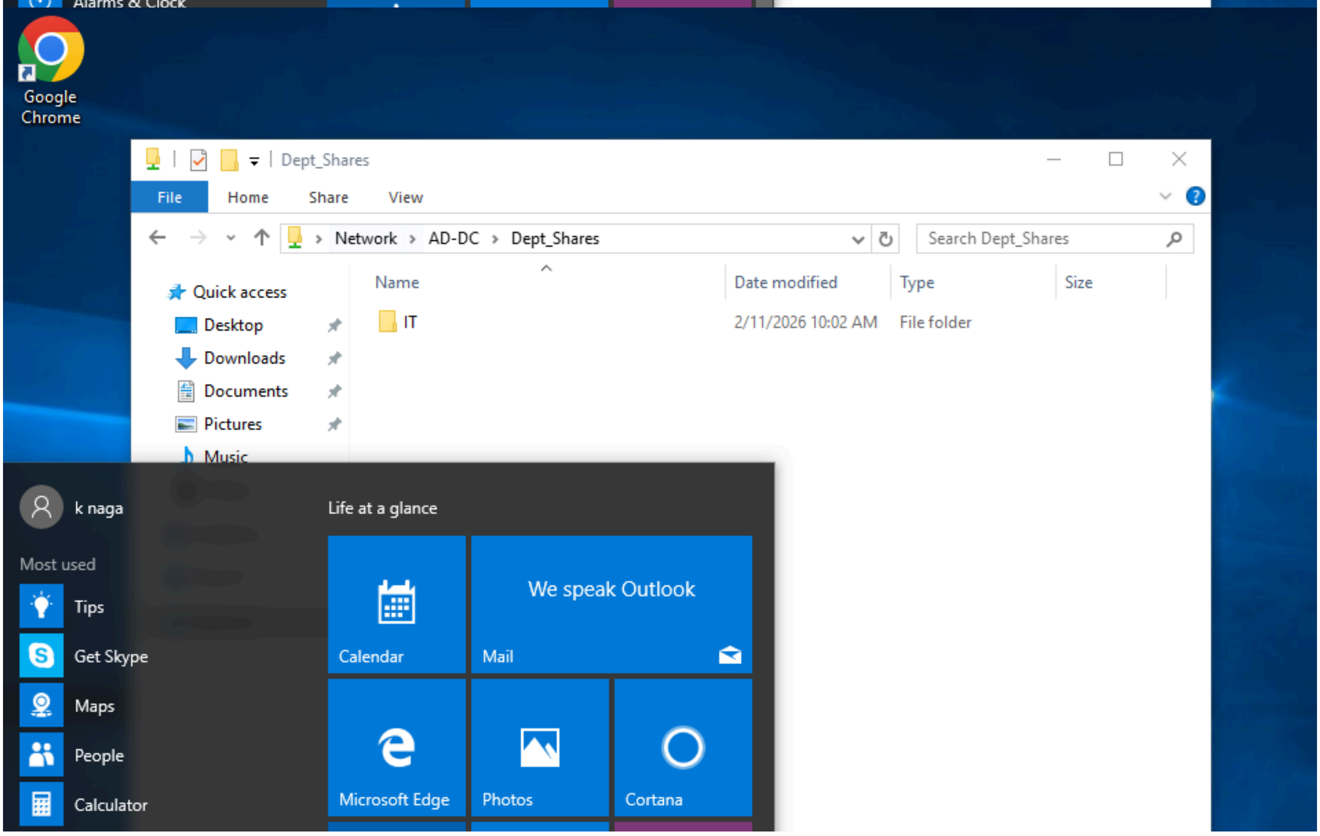
The Dept_Shares folder shows only the subfolders allowed for the logged-in user, confirming ABE functionality.

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.

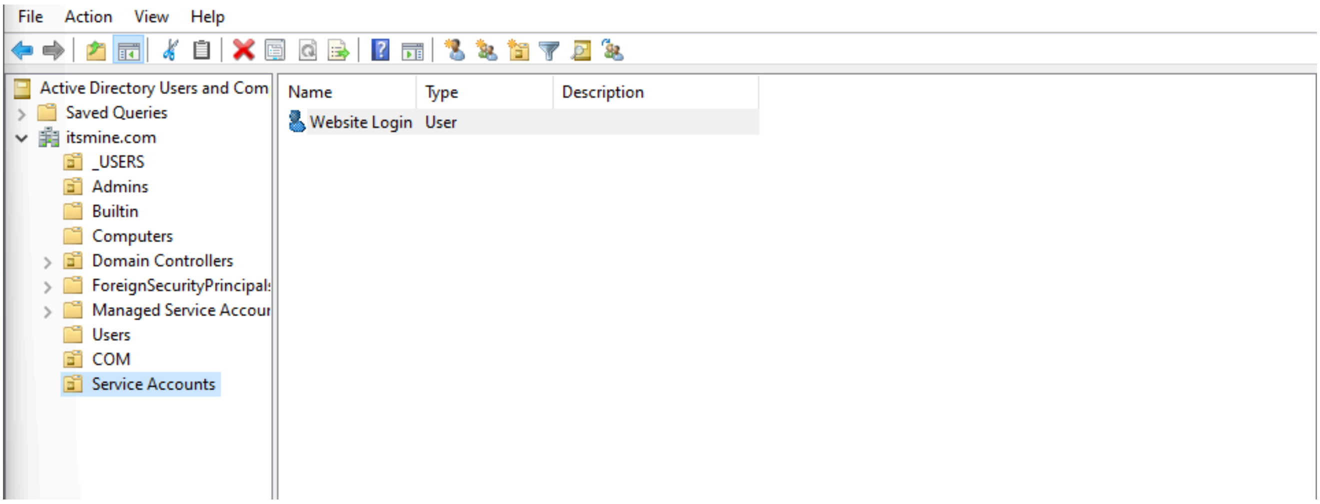




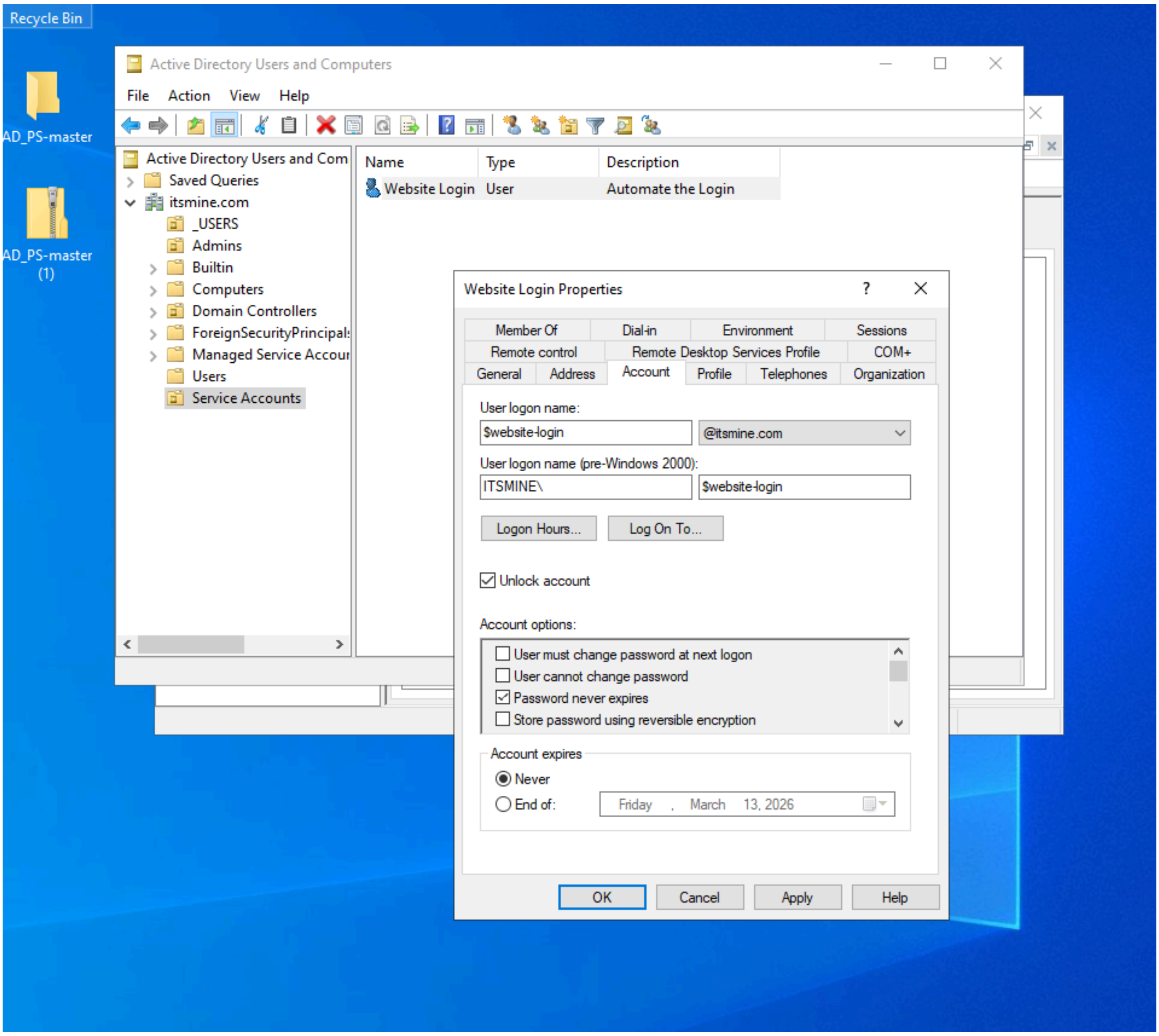
SERVICE ACCOUNT :

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.

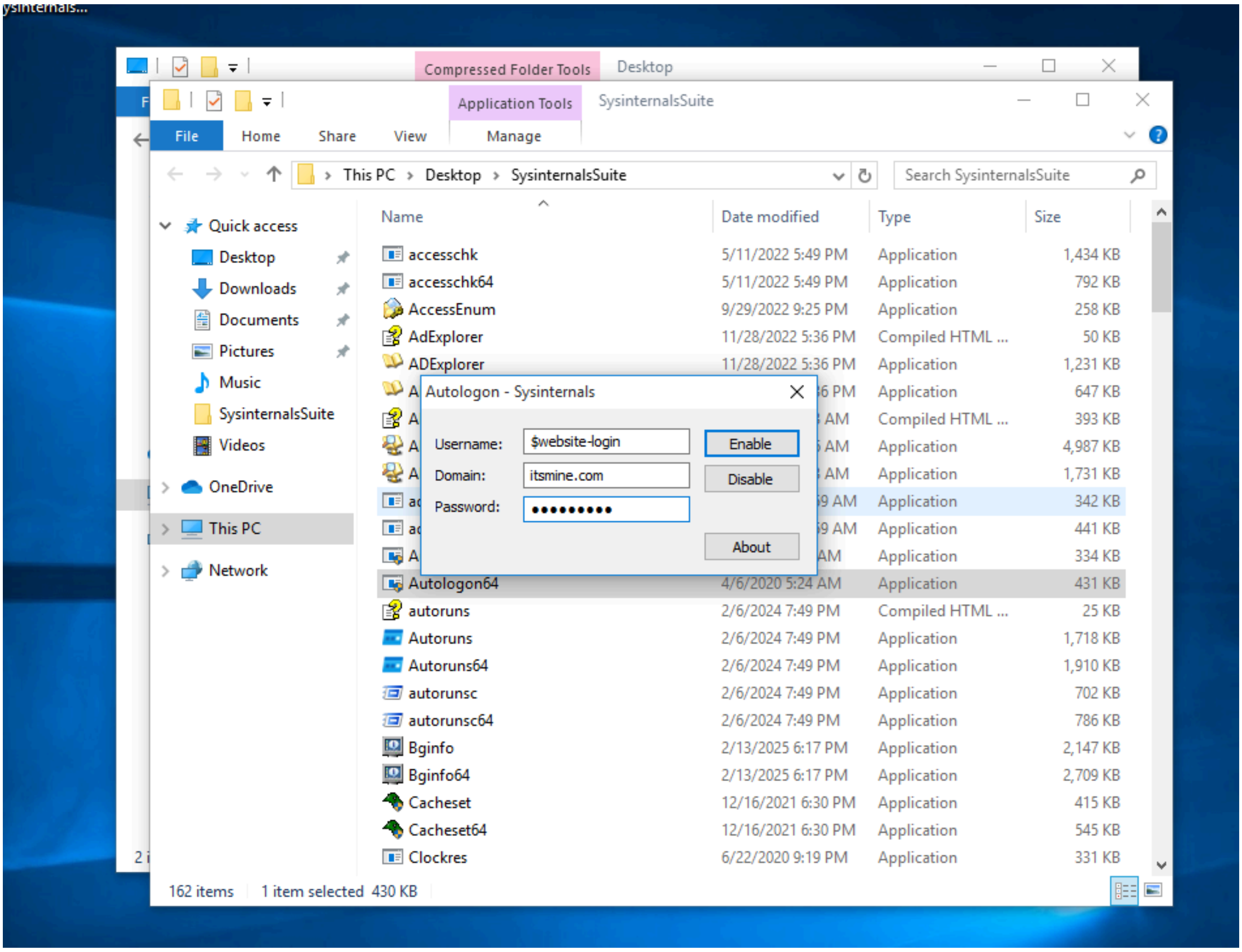
A dedicated service account (Website Login) was created in Active Directory for automated login usage.



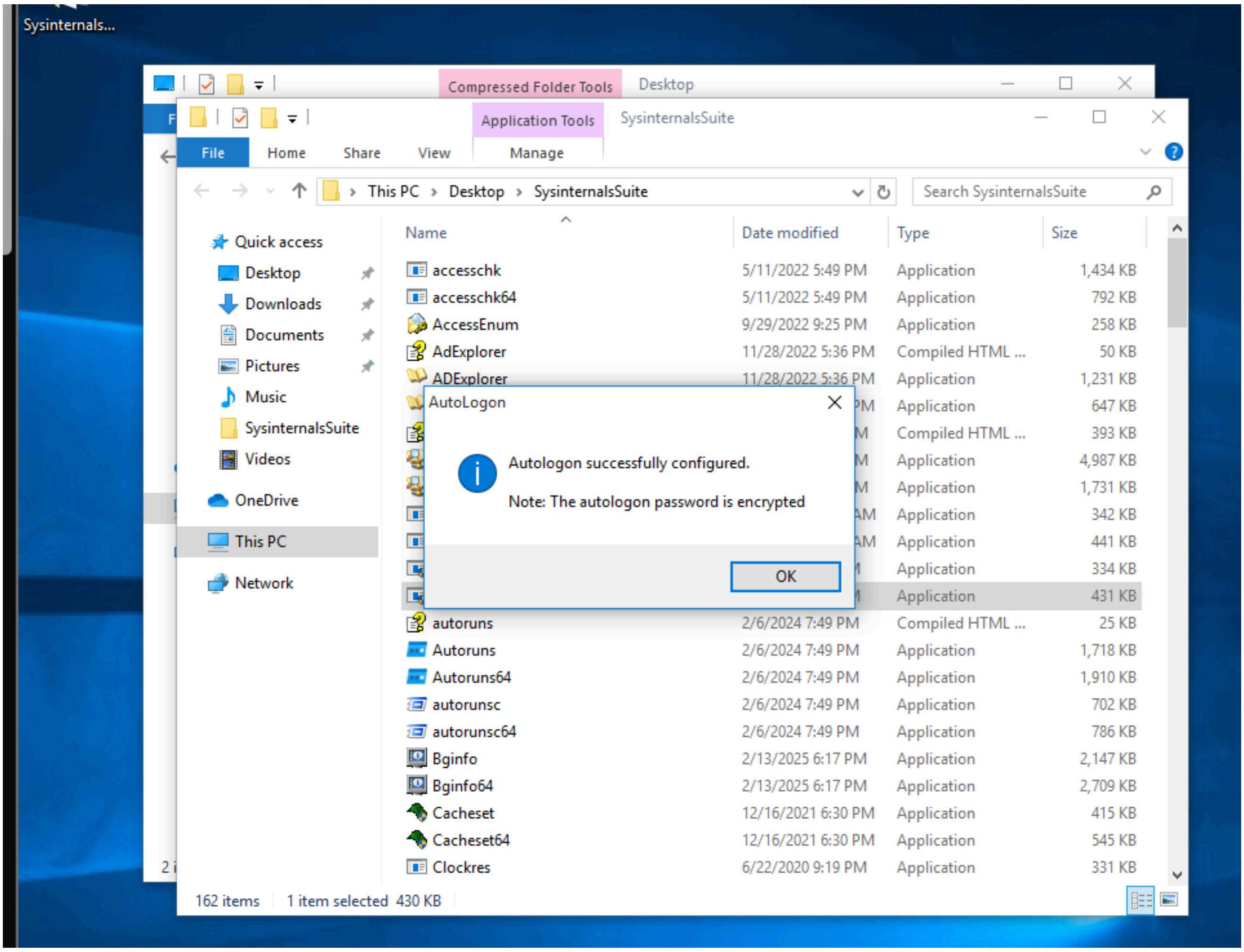
The service account properties were configured to prevent password expiration and allow automated login functionality.



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

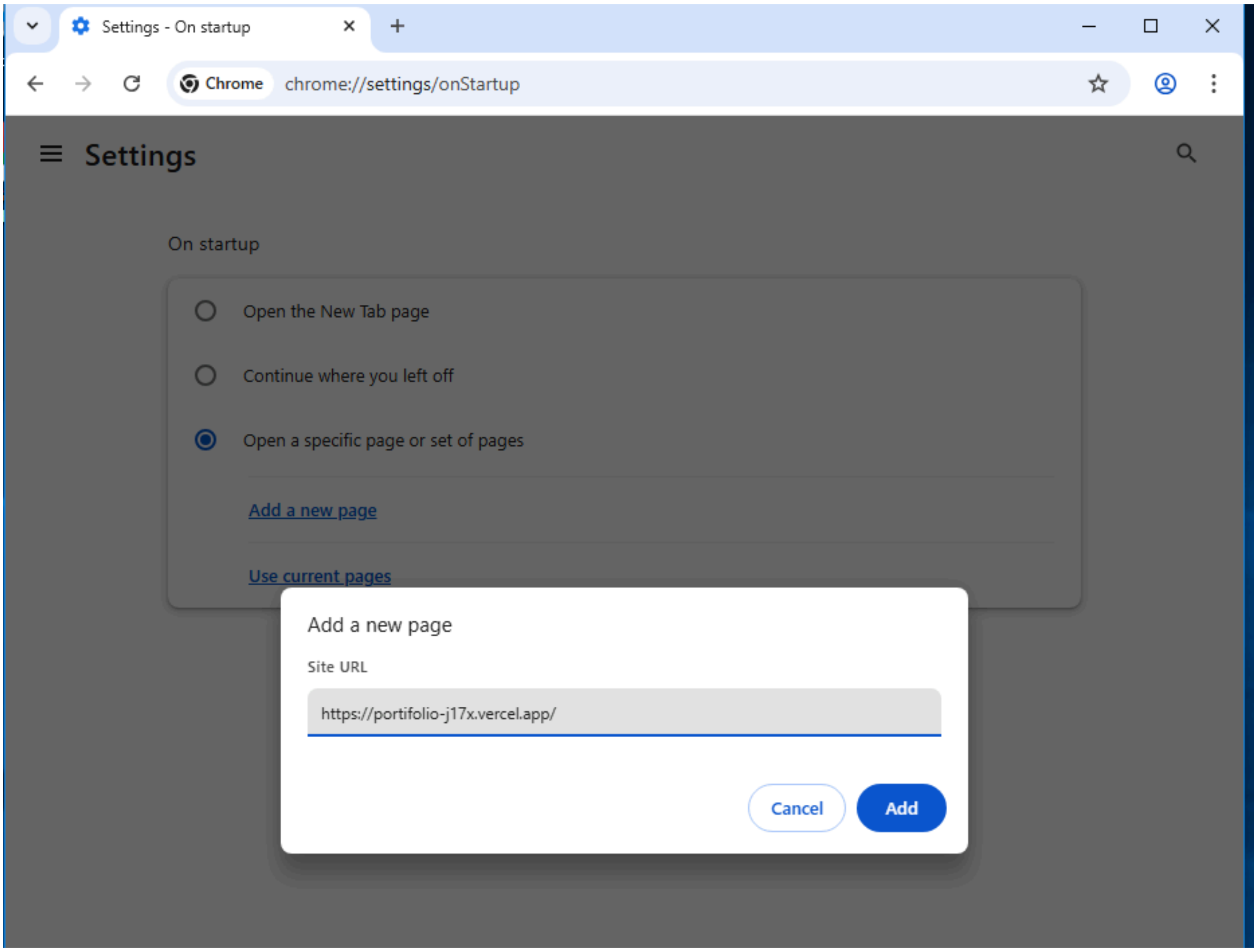


Successful autologon configuration was confirmed, ensuring the system logs in automatically after reboot.

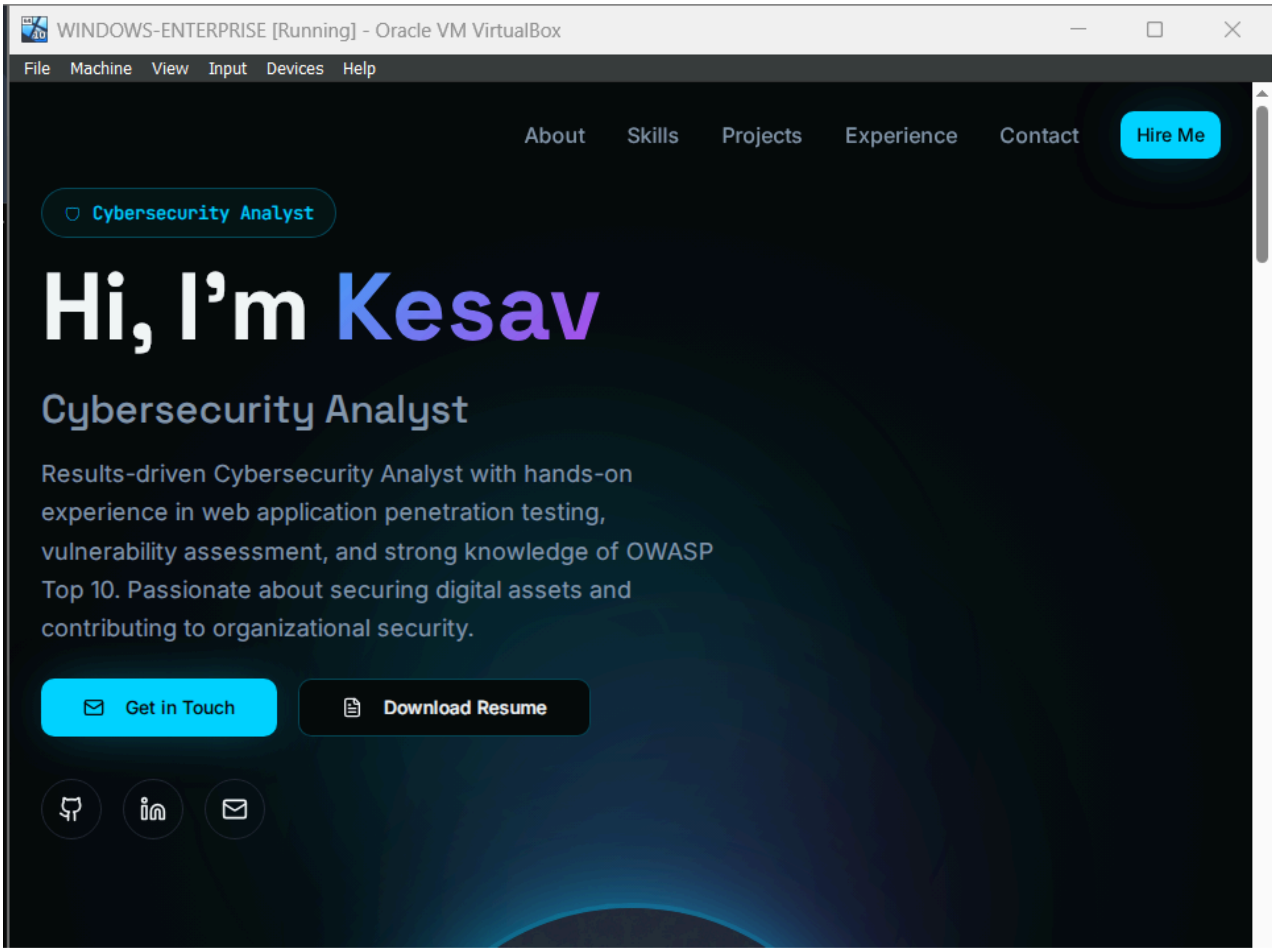


The system successfully logs in using the Website Login service account without manual input.

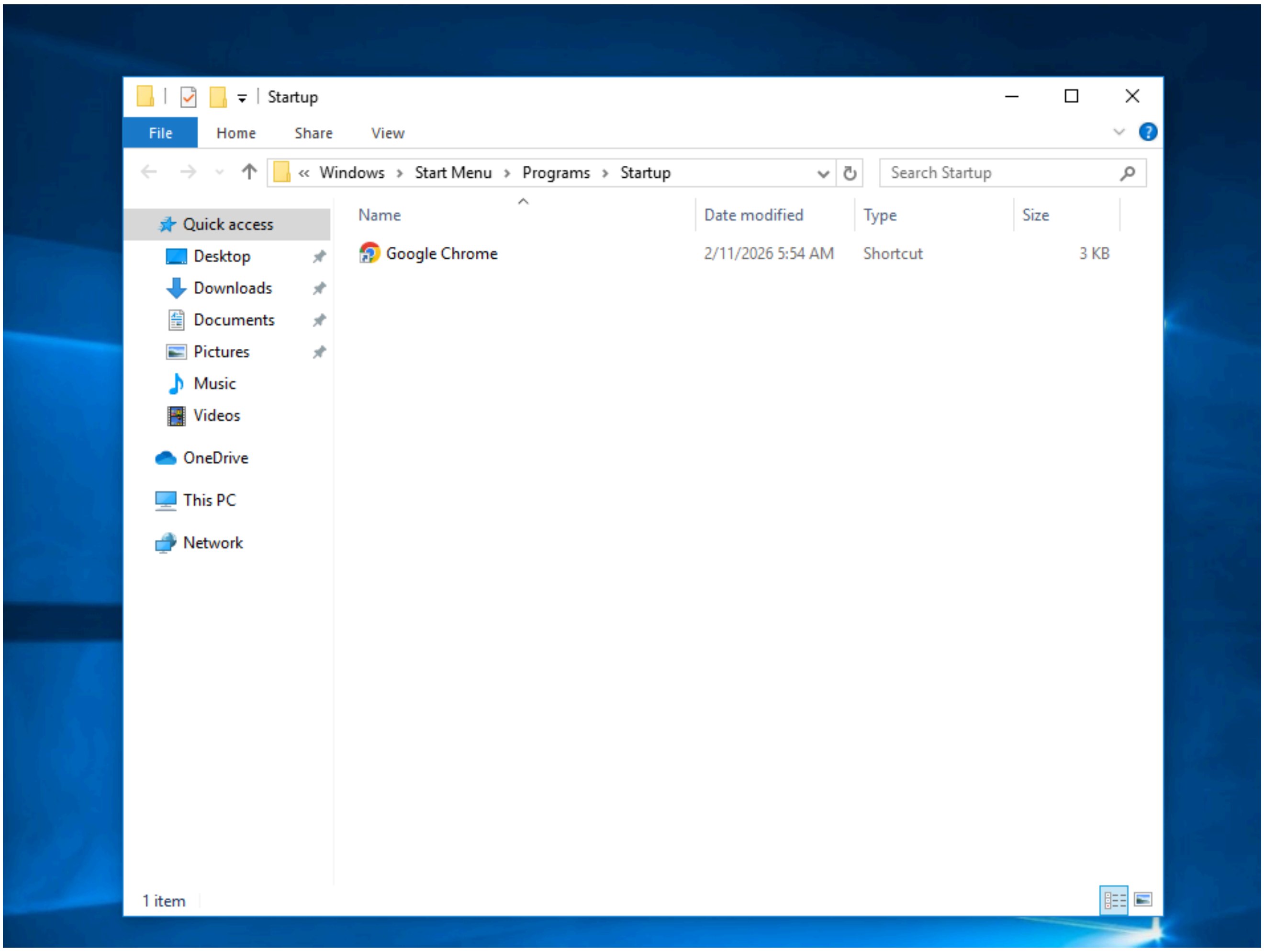
Browser startup configuration step was introduced to automatically launch a specific webpage.



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.


Startup
File
Home
Share
View
« Windows › Start Menu › Programs › Startup
Search Startup
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
Google Chrome
2/11/2026 5:54 AM
Shortcut
3 KB
1 item