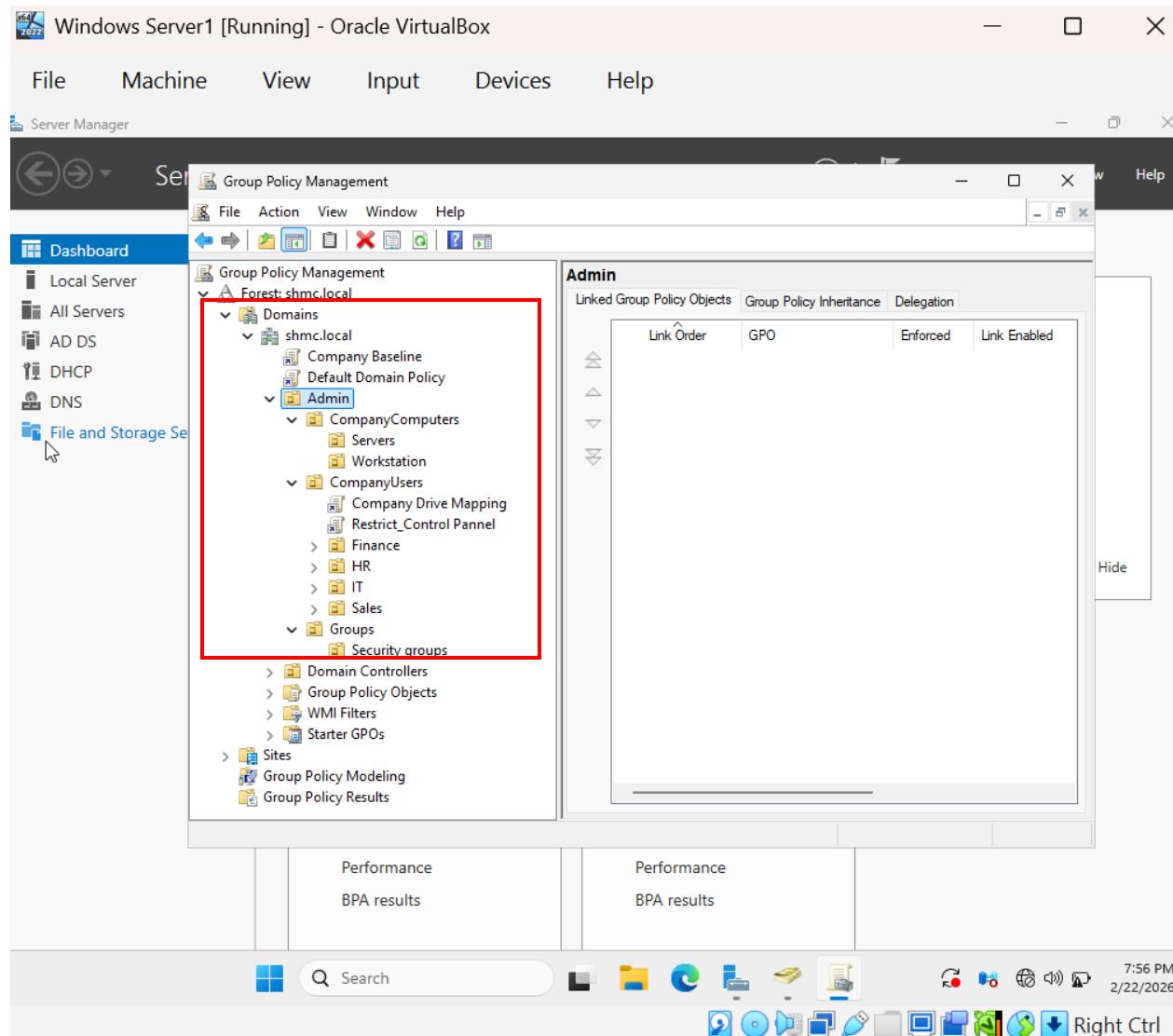


Windows Environment Design & Core Services

Built a functional enterprise-style Active Directory lab environment including organizational units (OUs), users, security groups, and Group Policy Objects (GPOs). Configured foundational network services such as DHCP and DNS to simulate real-world domain operations and centralized management.

Designed and managed Group Policy Objects (GPOs) within a structured OU framework to support role-based administration and departmental policy control. Demonstrated policy scoping, inheritance planning, and security segmentation for users and computers in a domain environment.



Configured Account Lockout Policy to protect against brute-force authentication attempts.

The screenshot shows the Active Directory Administrative Center (ADAC) interface. On the left, the Group Policy Management tree is displayed, showing the forest 'shmc.local' and its domains. A red box highlights the 'Company Baseline' GPO under the 'shmc.local' domain. The main pane displays the 'Company Baseline' details, specifically the 'Security Settings' tab. This tab contains two sections: 'Account Policies/Password Policy' and 'Account Policies/Account Lockout Policy'. Both sections are also highlighted with red boxes. The 'Account Policies/Password Policy' section lists the following settings:

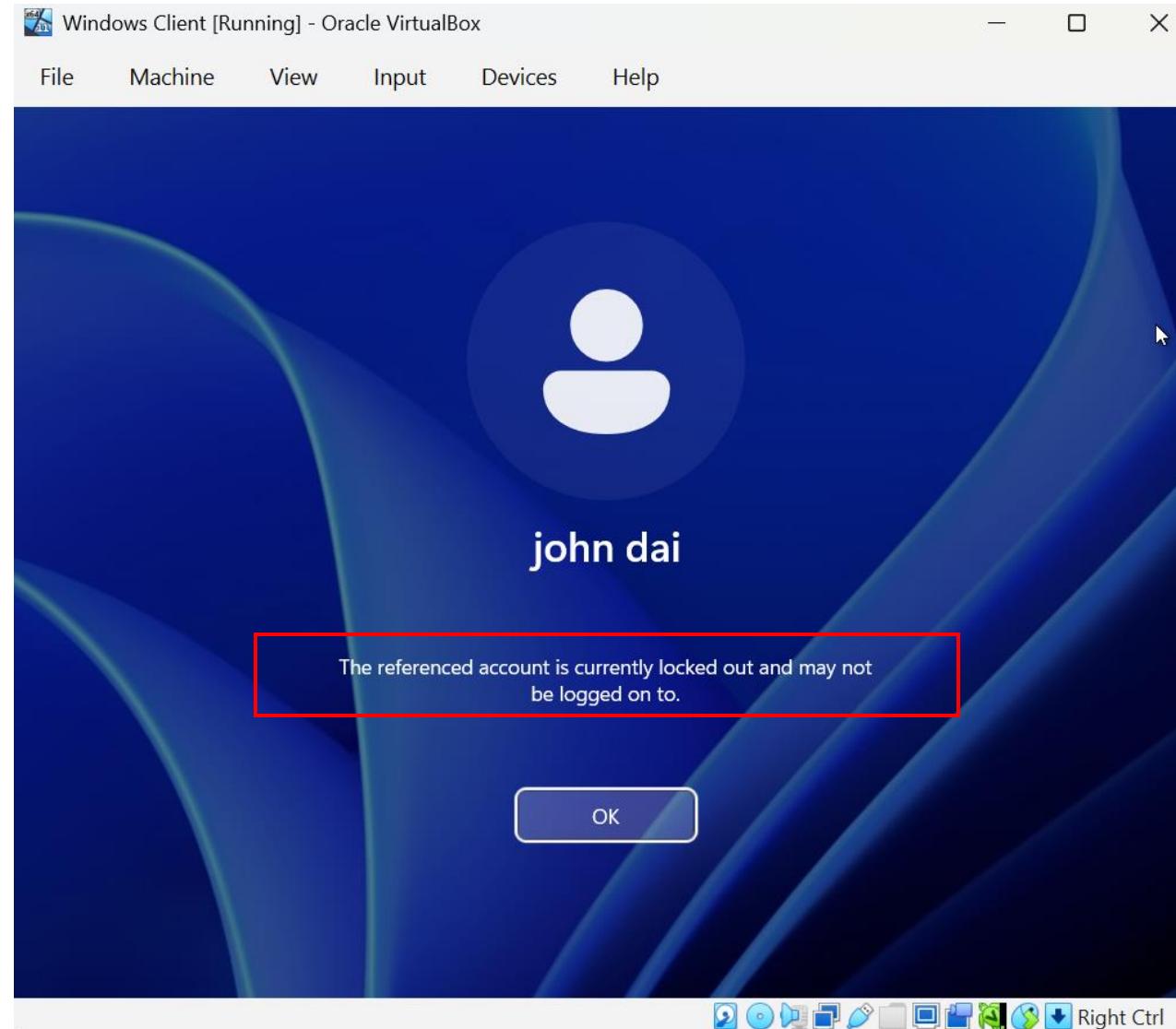
Policy	Setting
Enforce password history	3 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	12 characters
Password must meet complexity requirements	Enabled

The 'Account Policies/Account Lockout Policy' section lists the following settings:

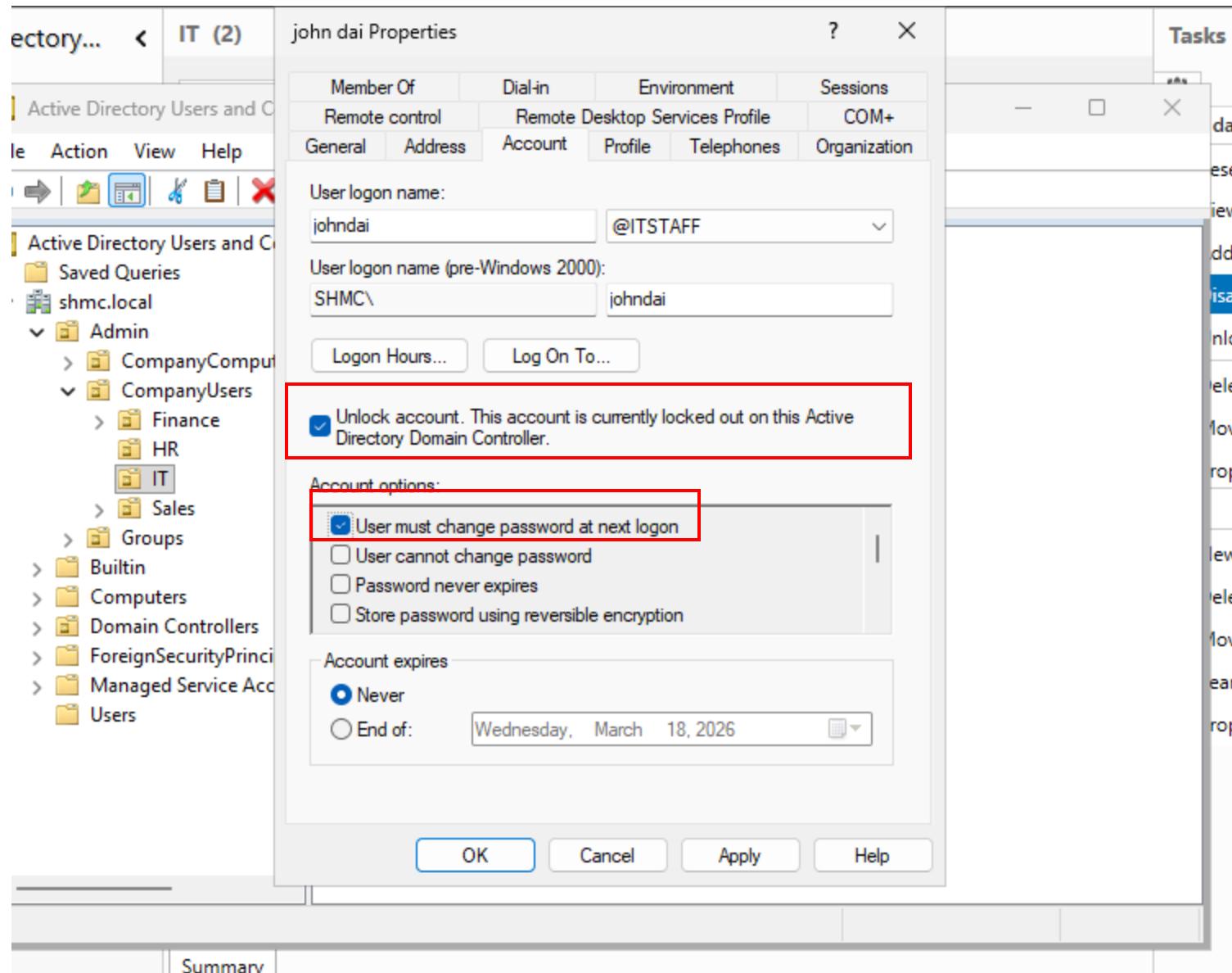
Policy	Setting
Account lockout duration	10 minutes
Account lockout threshold	3 invalid logon attempts
Allow administrator account lockout	Enabled
Reset account lockout counter after	10 minutes

Below these sections, there is a yellow-highlighted area labeled 'User Configuration (Enabled)' containing a 'Policies' section. At the bottom, it says 'Administrative Templates' and 'Policy definitions (ADMX files) retrieved from the local computer.'

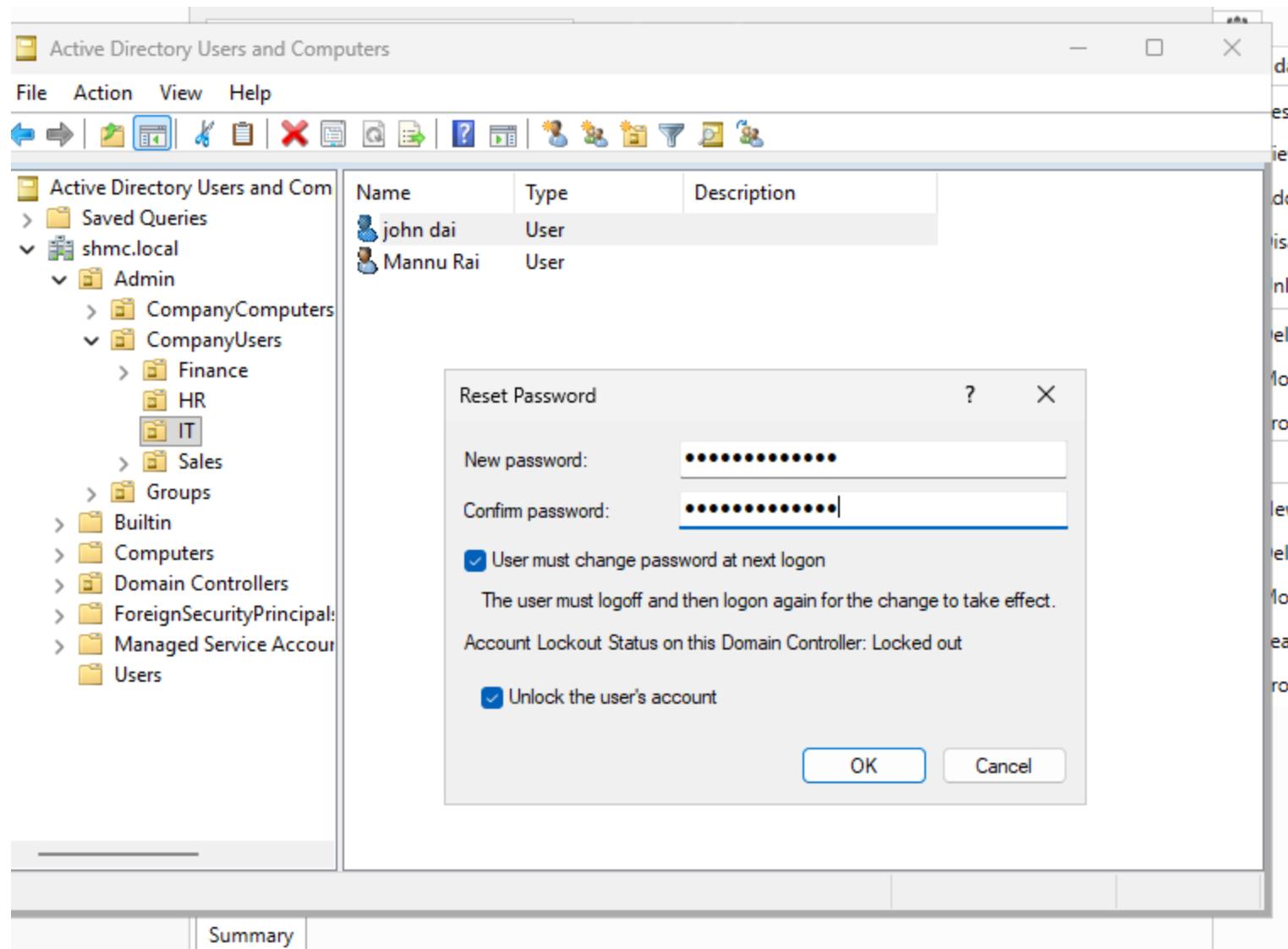
Demonstrated workings of the Account lockout GPO where a User Account has been disabled as a result of invalid password attempts.



User reports to IT about the issue, IT unlocks the account and enforces password change at next logon.

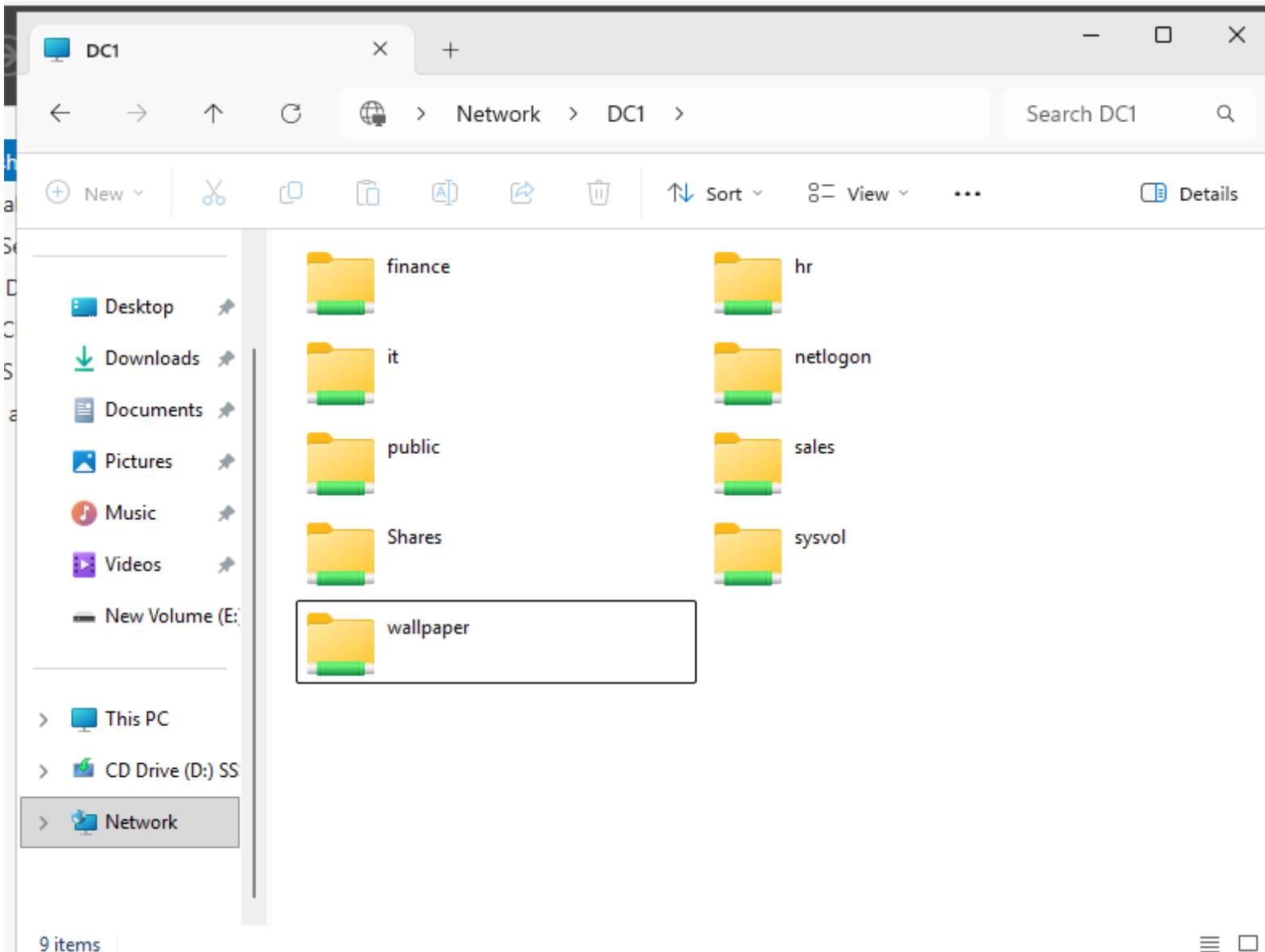


Demonstrating a password reset situation.



Network Shares and Drive mappings

- Created a Centralized File Server (DC1 In this Lab) and shared Folders over the network.
- Created a GPO that maps Drive letter for each department to the appropriate Network shares.



Drive Mapping GPO linked to Company Users OU

The screenshot shows the Group Policy Management console. On the left, the navigation pane displays the forest 'shmc.local' and various GPO objects under 'Domains'. A red box highlights the 'CompanyUsers' folder, which contains a 'Company Drive Mapping' GPO object, also highlighted with a red box. The main pane shows the 'Company Drive Mapping' properties for 'Drive Map (Drive: B)'. The 'General' tab is selected, showing settings like Action (Update), Letter (B), Location (\dc1\shares\it), and Reconnect (Disabled). The 'Common' tab shows options for processing items and security context. The 'Item-level targeting: Security Group' section at the bottom is also highlighted with a red box, showing targeting rules for the 'IT' security group.

Company Drive Mapping

Scope Details Settings Delegation

Drive Map (Drive: B)

B: (Order: 1)

General

Action	Update
Properties	
Letter	B
Location	\dc1\shares\it
Reconnect	Disabled
Label as	IT
Use first available	Disabled
Hide/Show this drive	Show
Hide/Show all drives	No change

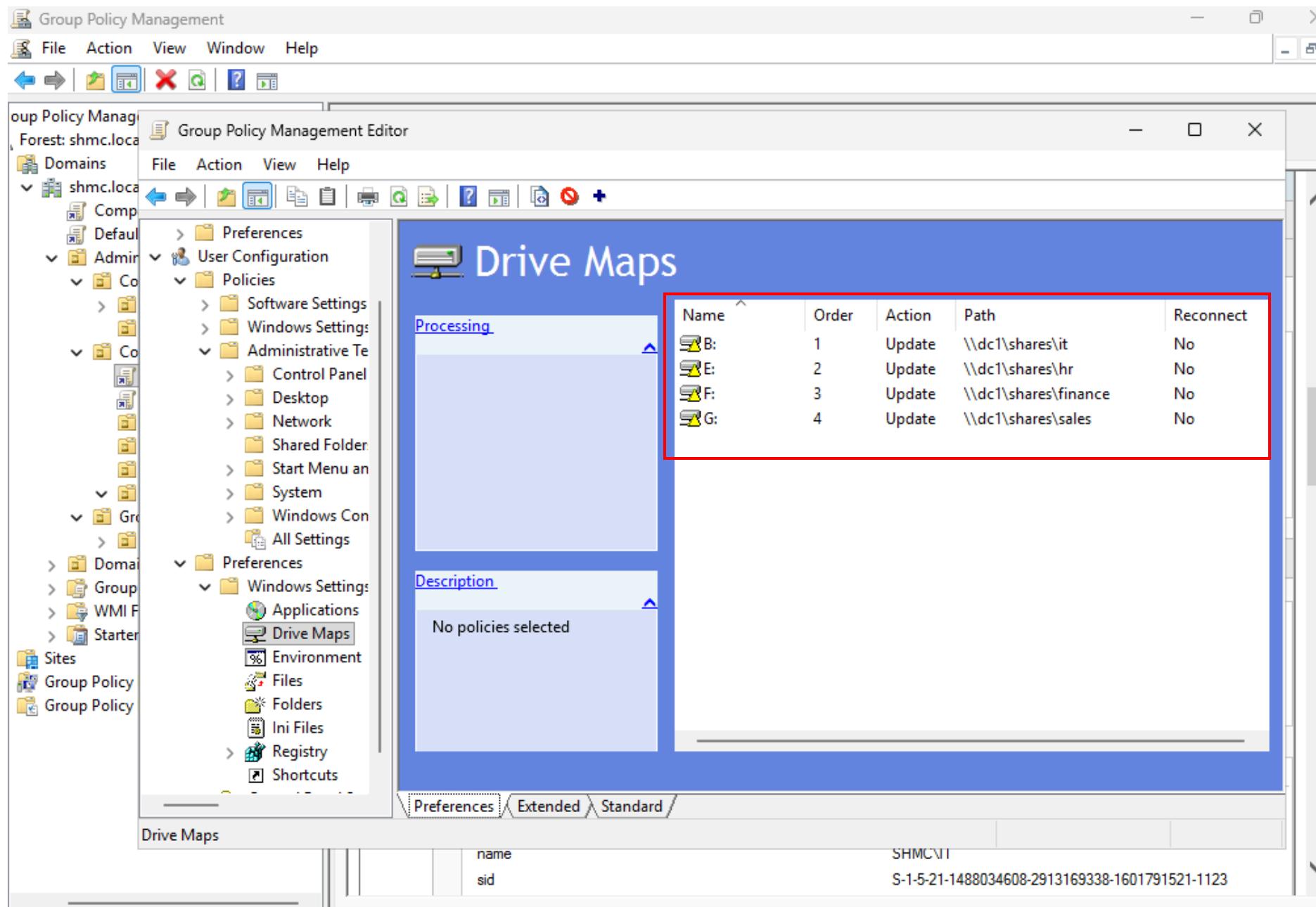
Common

Options	
Stop processing items on this extension if an error occurs on this item	No
Run in logged-on user's security context (user policy option)	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

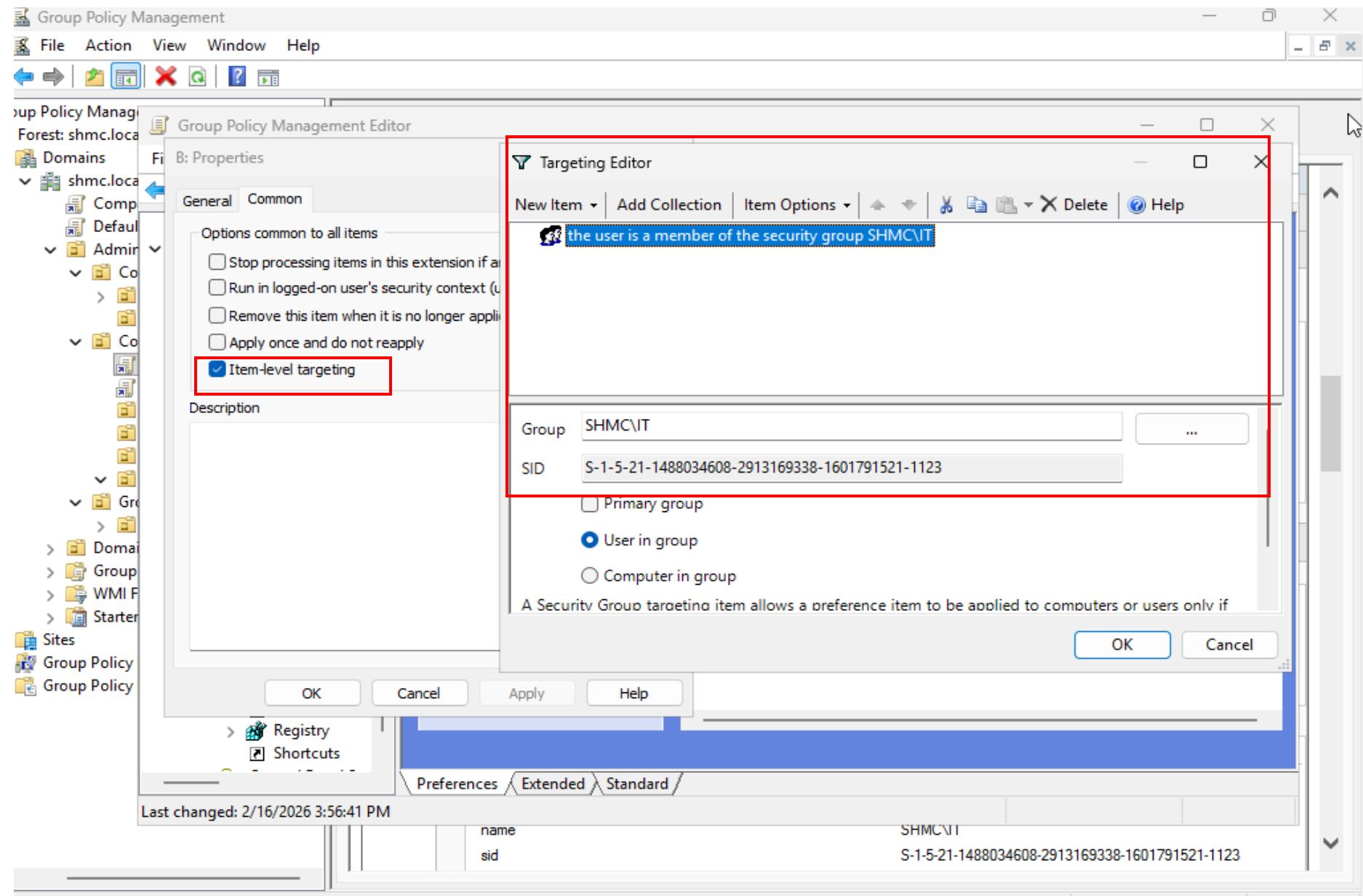
Item-level targeting: Security Group

Attribute	Value
bool	AND
not	0
name	SHMC\IT
sid	S-1-5-21-1488034608-2913169338-1601791521-1123

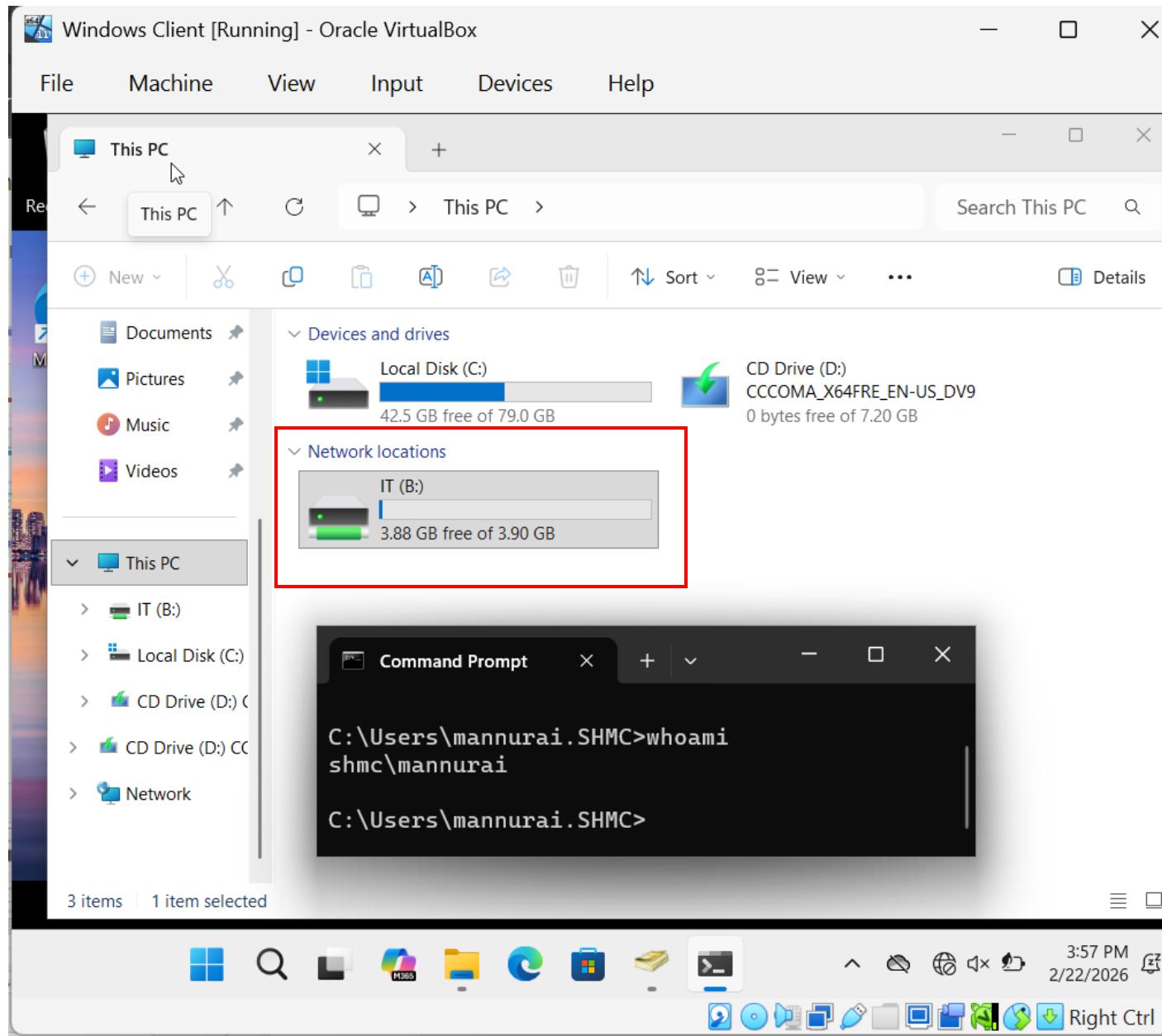
Created a GPO with Drive mappings, Assigned appropriate drive letter for each Department.



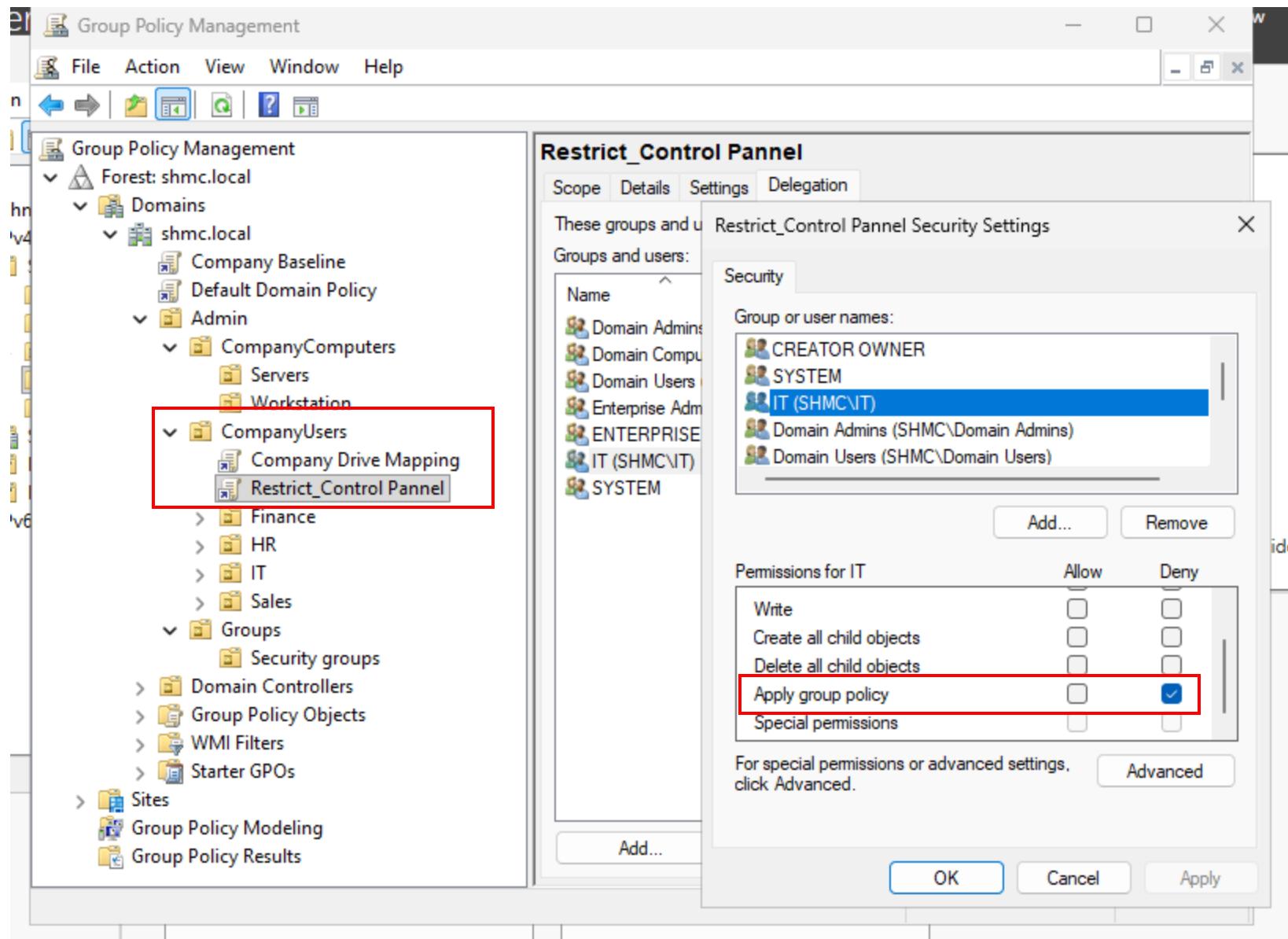
Item level Targetting for each drive maps, ensuring users from different departments are directed towards their appropriate share.



IT user logs in and finds the share using a friendly drive letter.



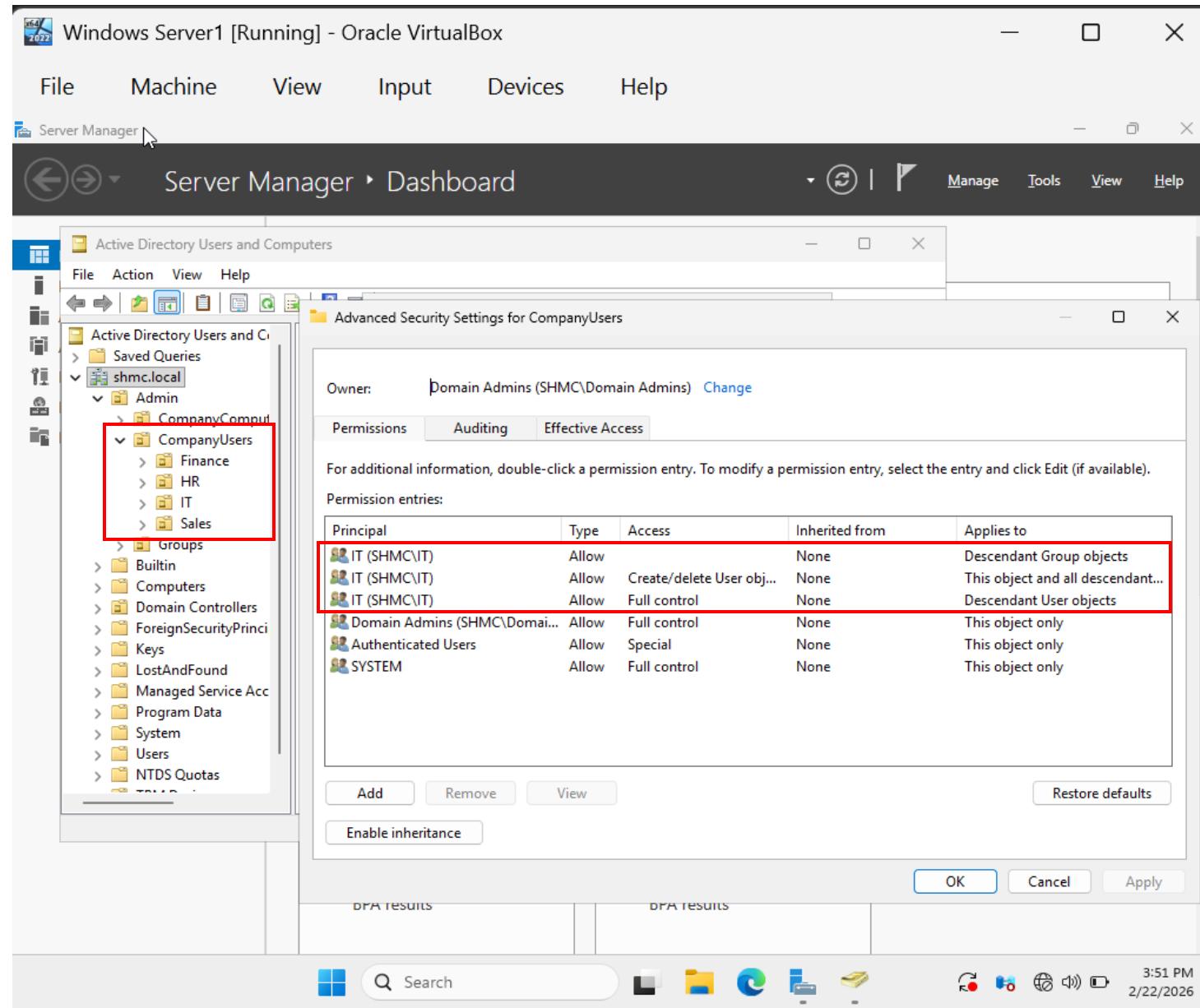
Created a GPO that restrict company users from accessing Control pannel and Sensitive computer setting, Excluded IT security group for controll and basic troubleshooting.



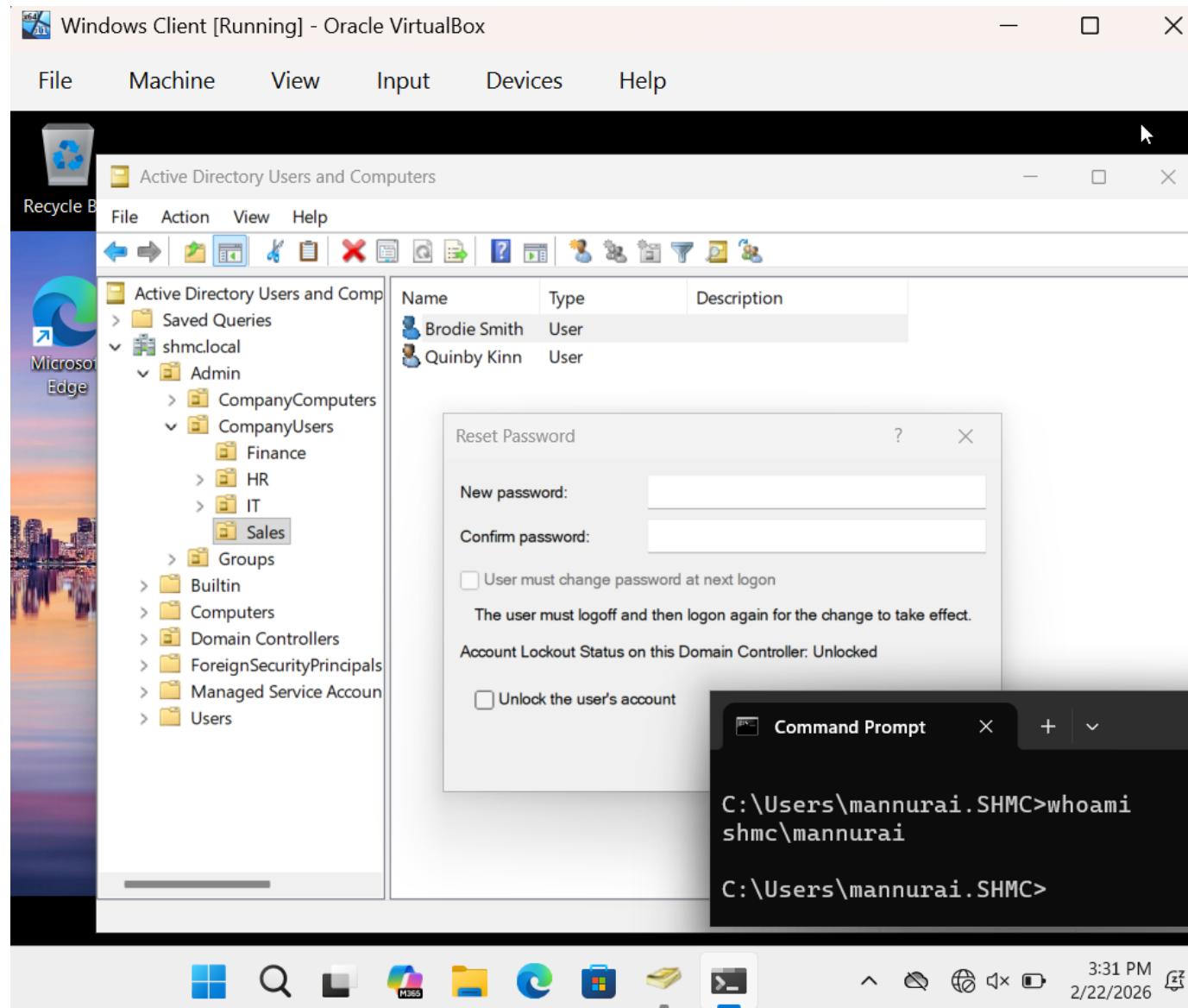
Delegation of Control

- Delegated appropriate permissions to the IT Security group over the *Company Users* OU to support routine help desk operations. Allowed tasks include user account creation/deletion, password resets, account unlock/disable actions, and group membership management. This delegation model follows least-privilege principles and reflects typical Tier 1 / help desk responsibilities in an enterprise domain environment.
- Configured least-privilege delegation for the IT Security group to perform standard help desk functions, including managing user accounts, resetting passwords, unlocking/ disabling accounts, and modifying group memberships.

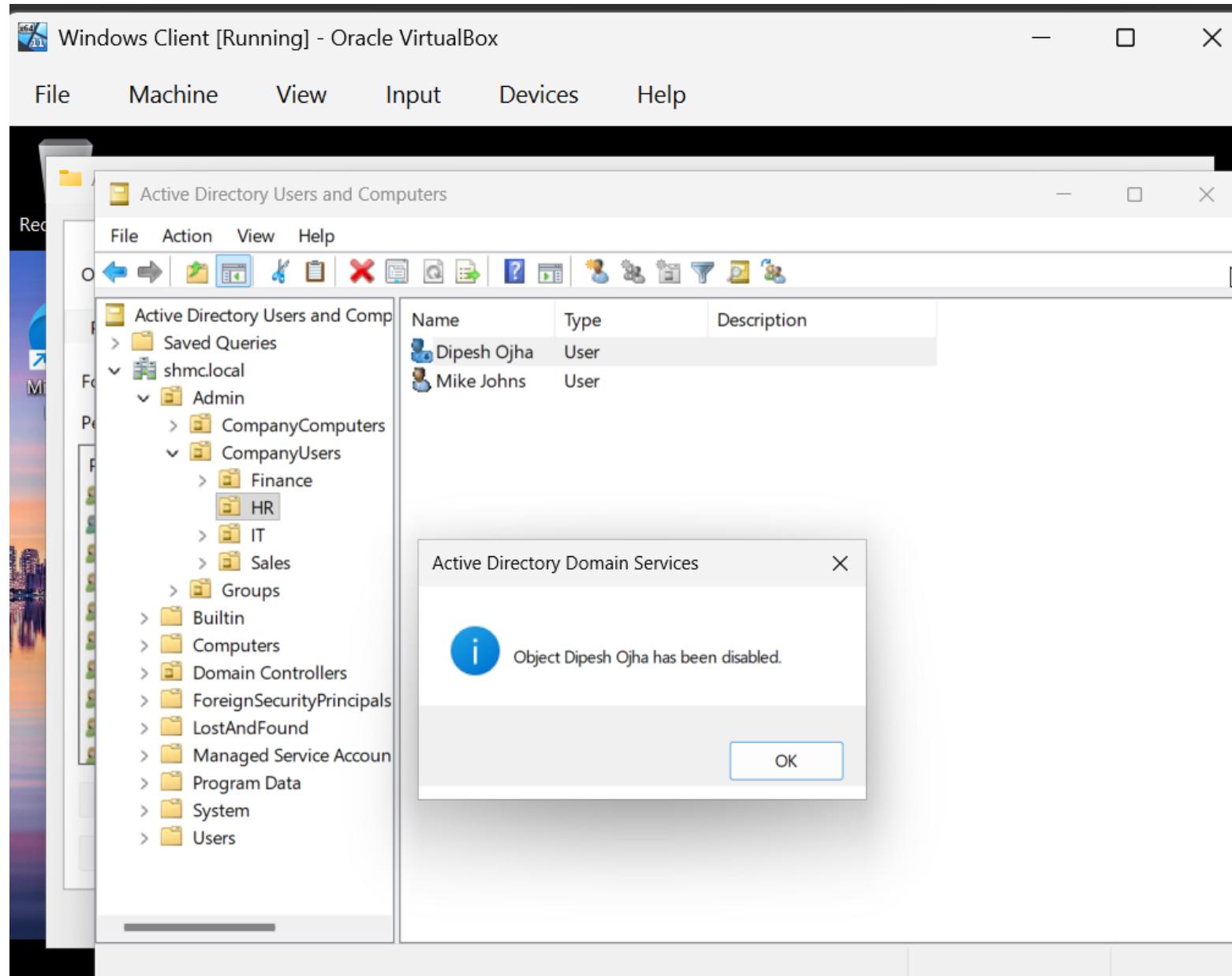
Delegating IT Security group basic management controller over Company Users OU, Any users that have issues with password, account, group membership can report to IT team member for a resolution.



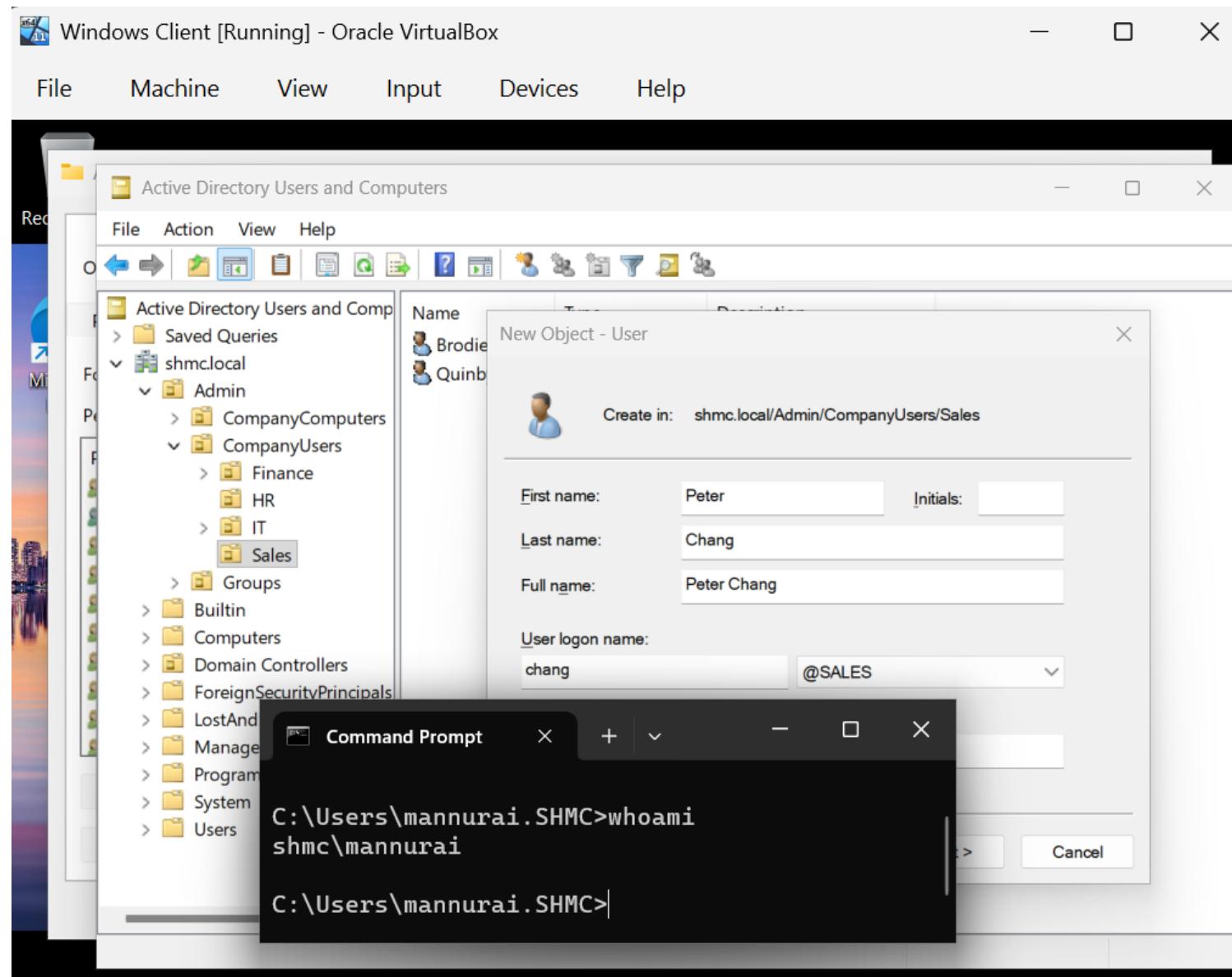
Administrating Active directory Users and Computers from member of IT security group, Mannurai a member of IT Security Group can solve issues related to users and groups using RSAT on the Client machine.



Demonstrating basic functions from IT Security group users using RSAT.



Creating a User from mannurai which belongs to IT security group.



Basic DHCP Configuration with different options such as Default gateway, DNS server and domain name.

