NANYANG POLYTECHNIC

WINDOWS PRACTICAL TEST REVISION

Name:	**Admin No.**	**Group:**	**Seat/PC No.**

INSTRUCTION:

- If you need to create any files or folders, create them in the server's (VM) C:\ drive unless the question states otherwise. Do not create them anywhere else.
- You must copy the screen output and paste it into the text box for marking. You can use the snipping or other tool to do this.
- All tasks are performed on the Windows Server. If the Windows Client need to be accessed, it shall be stated.

Tasks:

1. (a) Create a new OU (Organizational Unit) named **AppleOU** under frontier.net**.**

(b) Create a **Group** named **Sales <u>INSIDE</u> AppleOU**. Configure the group as **Global** and **Security** type.

(c) Create the User Accounts listed in Table 1 below **<u>INSIDE</u> AppleOU**. Add the user as member of the Sales group.

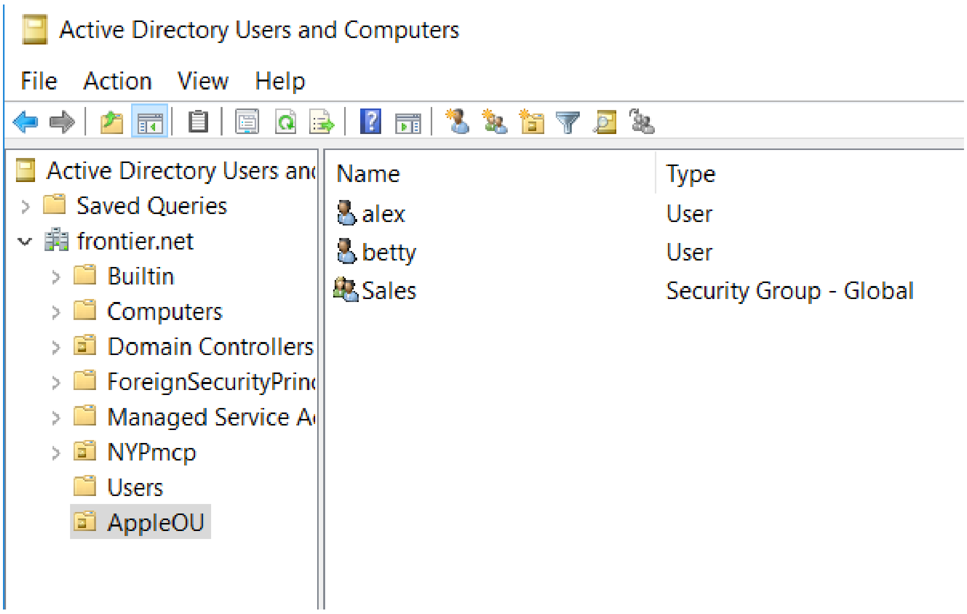
When you create the user account, the names in the **User Account** column are the login name. Set the password as ***Pa$$w0rd*** for all accounts. Disable "User must change password at next logon".

Member of	**User Account** (login name)
Sales Group	Alex
Sales Group	Betty

Table 1

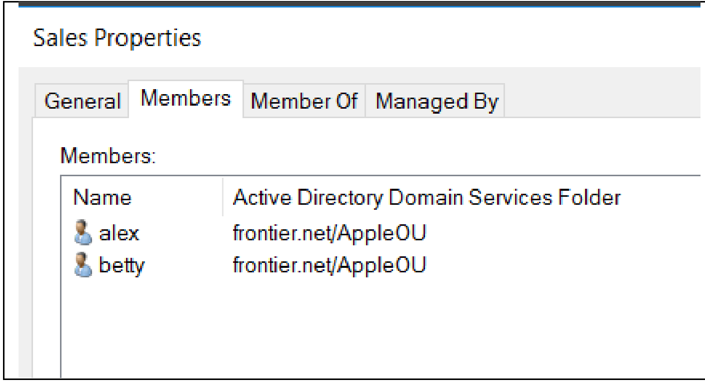
[Practical 1(d), 2A]

Use Active Directory Users and Computes to display the OU, group and members below:



Name	Type
alex	User
betty	User
Sales	Security Group - Global

Show that Alex and Betty are members of Sales group.



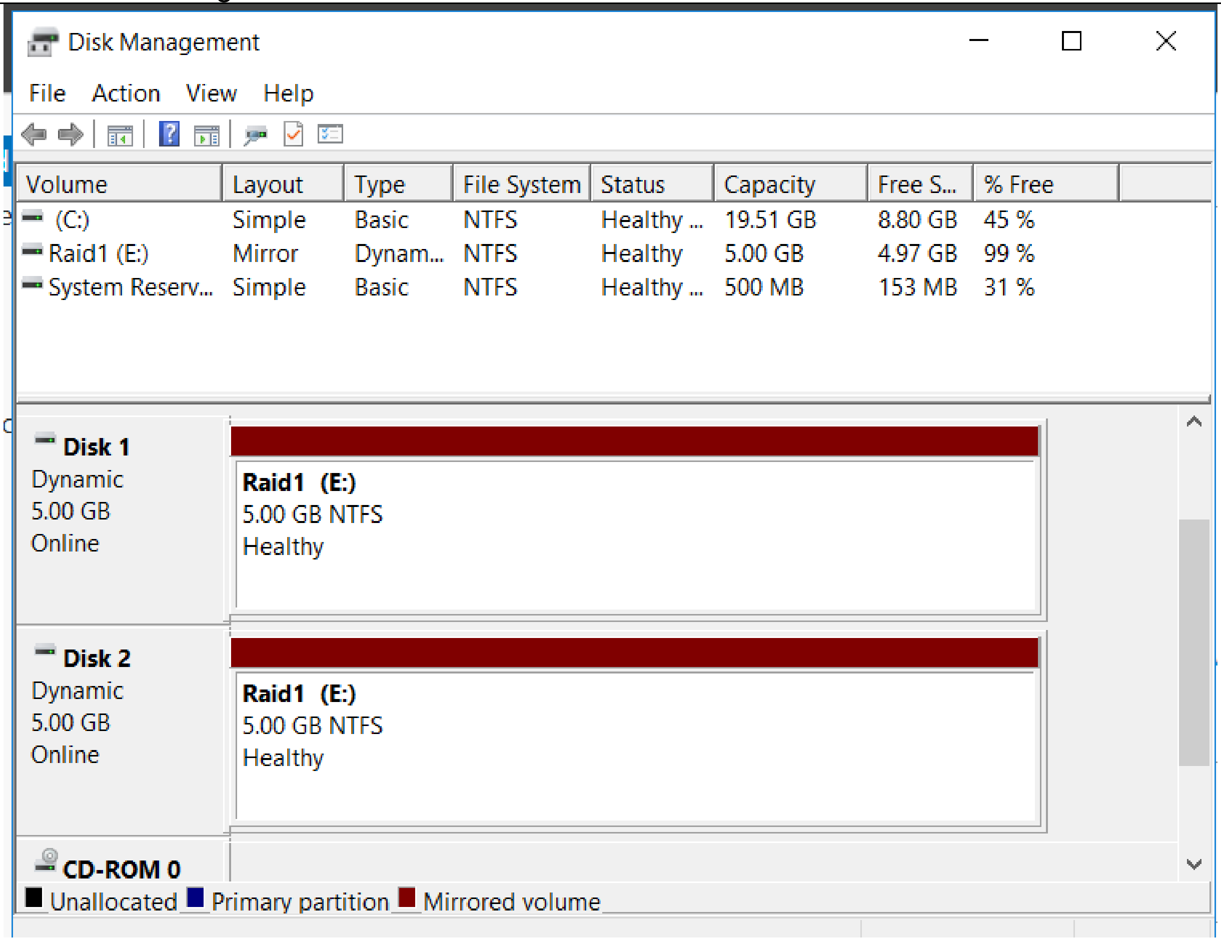
Members:

Name	Active Directory Domain Services Folder
alex	frontier.net/AppleOU
betty	frontier.net/AppleOU

2. (a) Create a **RAID 1 of 5GB**. Add hard disks if necessary. Do **NOT** use Disk 0 which contains the C: drive. Format the Raid 1 as NTFS and set the volume name as **Raid1** and the Drive as **E**: *(Note: Revise Raid 0 and 5 too)*

[Practical 3]

Use disk management to show that the Raid 1 is created.



Volume	Layout	Type	File System	Status	Capacity	Free S...	% Free
(C:)	Simple	Basic	NTFS	Healthy ...	19.51 GB	8.80 GB	45 %
Raid1 (E:)	Mirror	Dynam...	NTFS	Healthy	5.00 GB	4.97 GB	99 %
System Reserv...	Simple	Basic	NTFS	Healthy ...	500 MB	153 MB	31 %

Disk 1
Dynamic
5.00 GB
Online

Raid1 (E:)
5.00 GB NTFS
Healthy

Disk 2
Dynamic
5.00 GB
Online

Raid1 (E:)
5.00 GB NTFS
Healthy

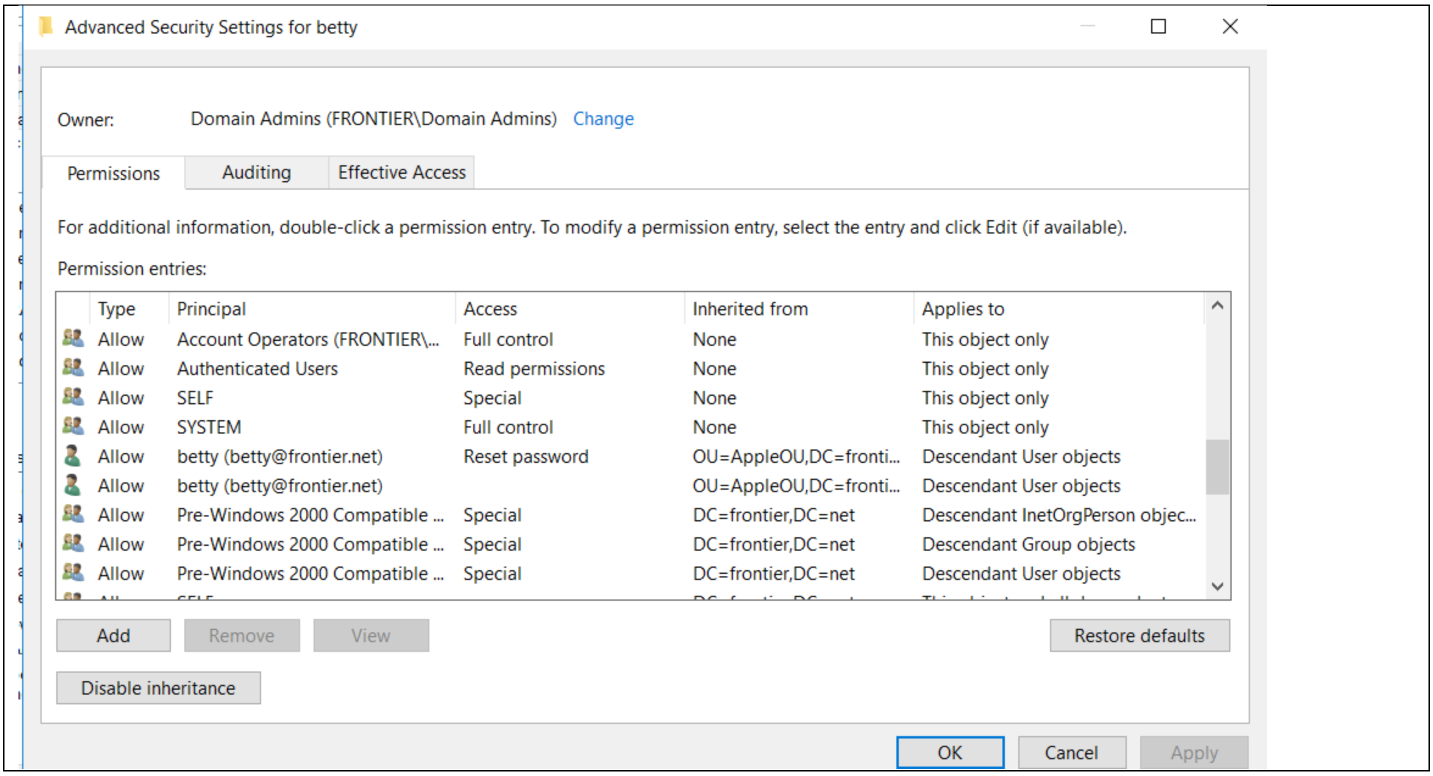
CD-ROM 0

⬛ Unallocated 🟦 Primary partition 🟥 Mirrored volume

3. Delegate the control ***Reset user passwords and force password change at next logon*** to **Betty** account**.**

[Practical 5A]

Display the screen to show that Betty has been assigned the delegation.



Owner: Domain Admins (FRONTIER\Domain Admins) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

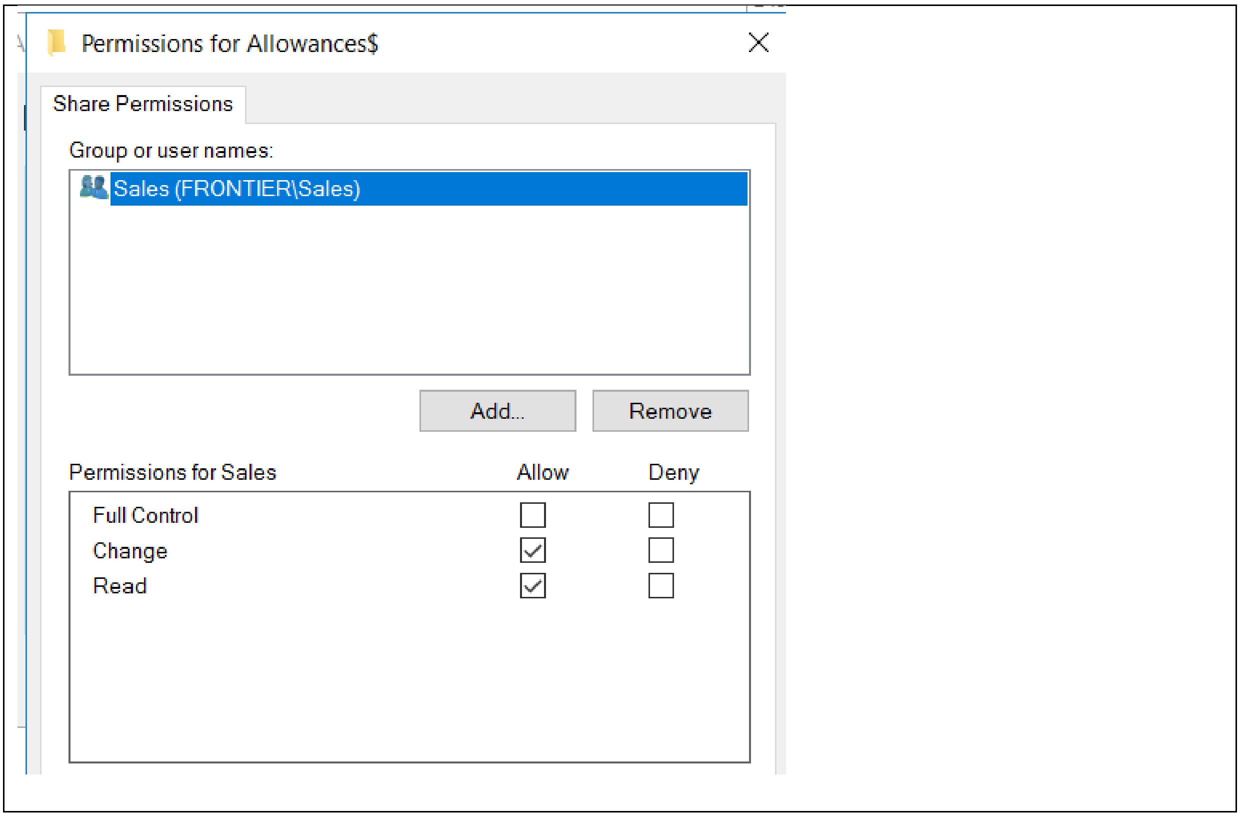
Type	Principal	Access	Inherited from	Applies to
Allow	Account Operators (FRONTIER\...	Full control	None	This object only
Allow	Authenticated Users	Read permissions	None	This object only
Allow	SELF	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	betty (betty@frontier.net)	Reset password	OU=AppleOU,DC=fronti...	Descendant User objects
Allow	betty (betty@frontier.net)		OU=AppleOU,DC=fronti...	Descendant User objects
Allow	Pre-Windows 2000 Compatible ...	Special	DC=frontier,DC=net	Descendant InetOrgPerson objec...
Allow	Pre-Windows 2000 Compatible ...	Special	DC=frontier,DC=net	Descendant Group objects
Allow	Pre-Windows 2000 Compatible ...	Special	DC=frontier,DC=net	Descendant User objects

4. (a) Configure a **shared** folder for the **Sales** group on the server **NYP-DC1** with the following settings:

- create a folder in (VM) C:\ drive called **Allowances**
- set the shared permissions as: remove **Everyone** group; set **Sales** group to allow **Change** and **Read**
- Hide the shared folder from the network discovery.

[Practical 4A]

Display the output to show the permission of the shared folder and that it is hidden from the network.



Permissions for Allowances$

Share Permissions

Group or user names:

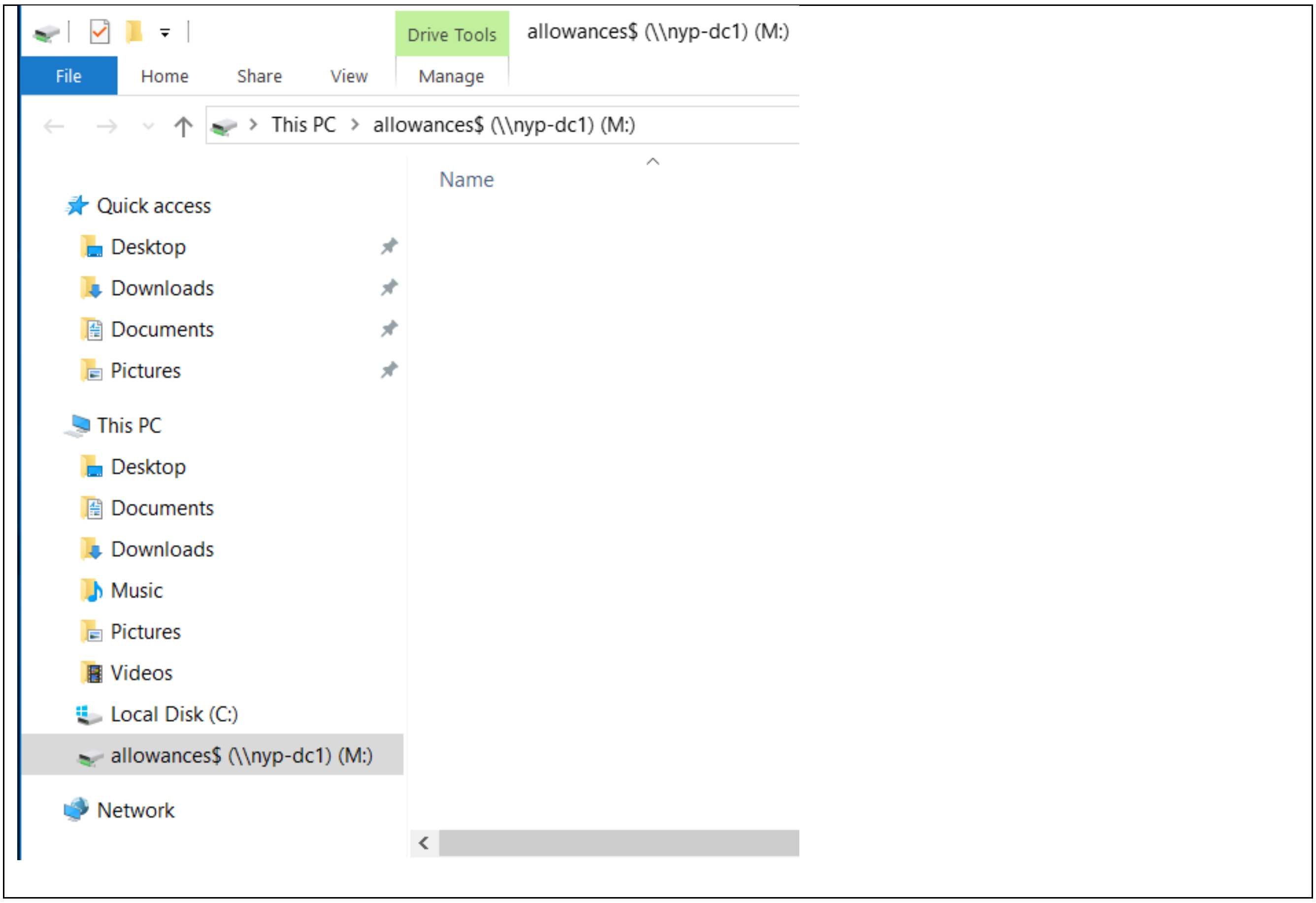
Sales (FRONTIER\Sales)

Permissions for Sales	Allow	Deny
Full Control	□	□
Change	☑	□
Read	☑	□

(b) Login to **NYP-CL1** as **Alex** and map to the **Allowances** shared folder in the Windows/File Explorer as M drive. Note the client NYP-CL1 may not be joined to the domain yet.

Note: There is a video on how to join the domain in week 1 practical folder.

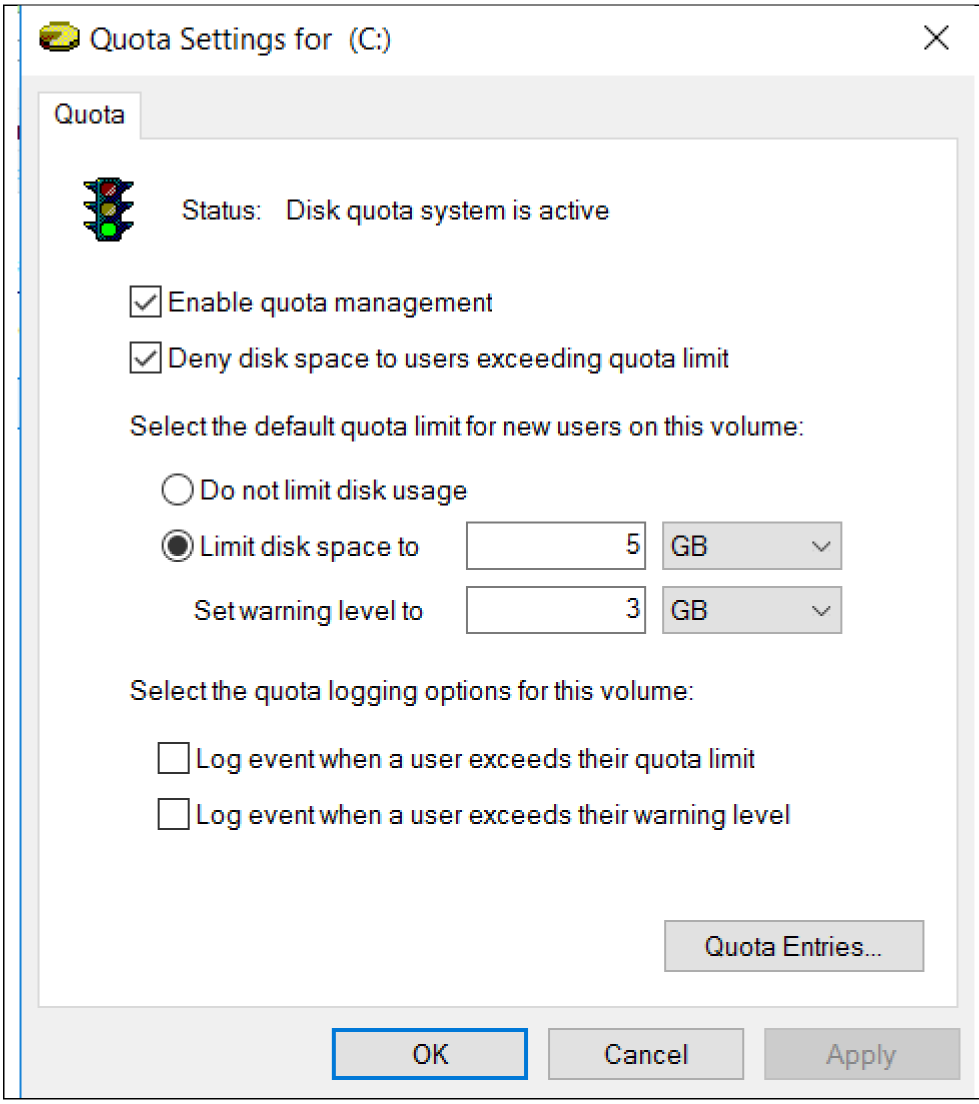
Display the file explorer to show that Alex has mapped to the shared folder as M drive.



5. (a) Use Disk Quota to limit each user to **5 GB** of data on the NYP-DC1 **C:** drive. Users will get a warning message when files storage reaches **3 GB**. Prevent users from writing to the disk once the limit is exceeded.

[Practical 4B]

Display the disk quota configuration.



Quota Settings for (C:)

Status: Disk quota system is active

☑ Enable quota management

☑ Deny disk space to users exceeding quota limit

Select the default quota limit for new users on this volume:

○ Do not limit disk usage

● Limit disk space to 5 GB

Set warning level to 3 GB

Select the quota logging options for this volume:

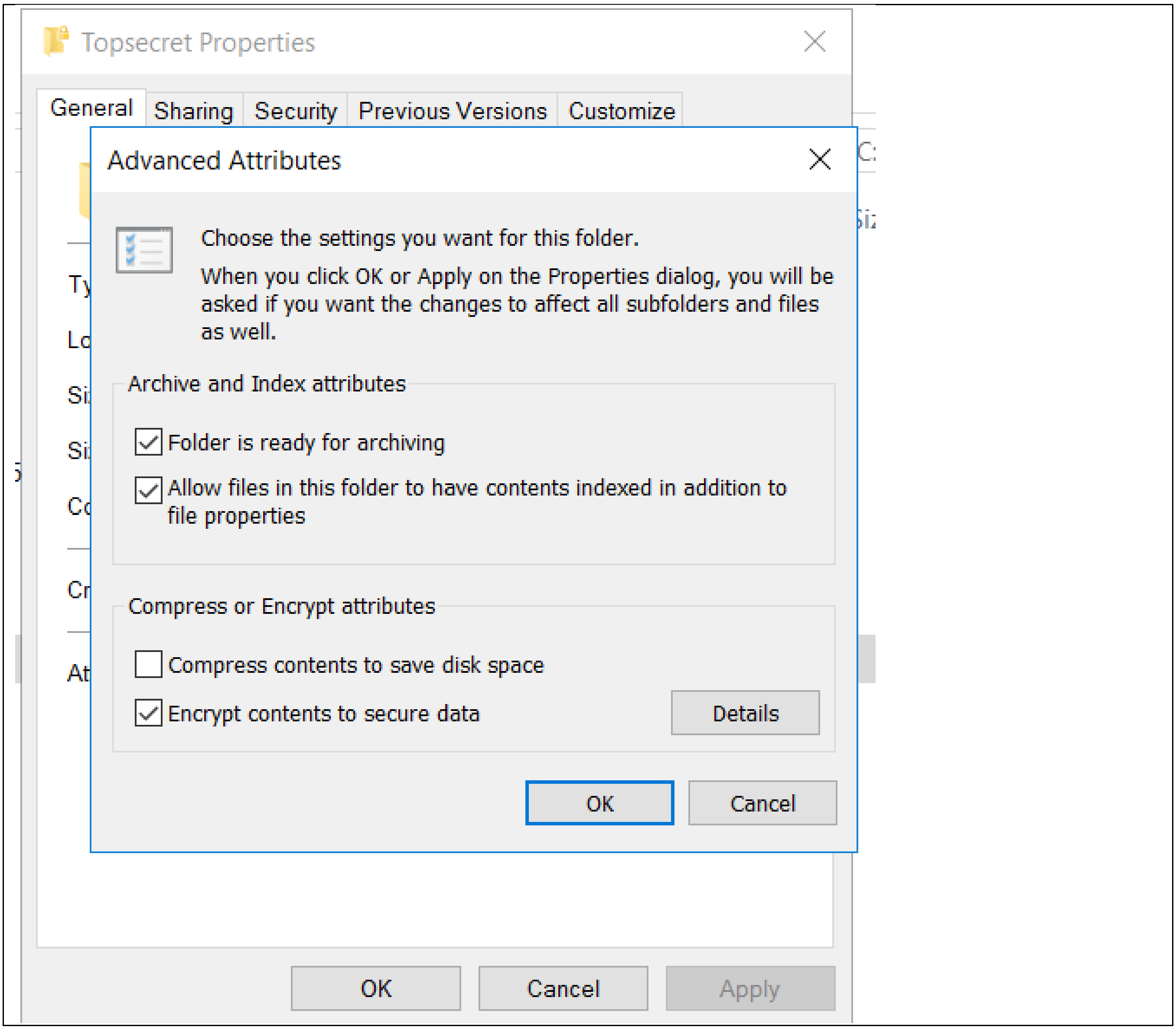
□ Log event when a user exceeds their quota limit

□ Log event when a user exceeds their warning level

(b) Create a folder in C:\ named Topsecret and encrypt it.

[Practical 4B]

Show proof that Topsecret is encrypted.



Advanced Attributes

Choose the settings you want for this folder.

When you click OK or Apply on the Properties dialog, you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

☑ Folder is ready for archiving

☑ Allow files in this folder to have contents indexed in addition to file properties

Compress or Encrypt attributes

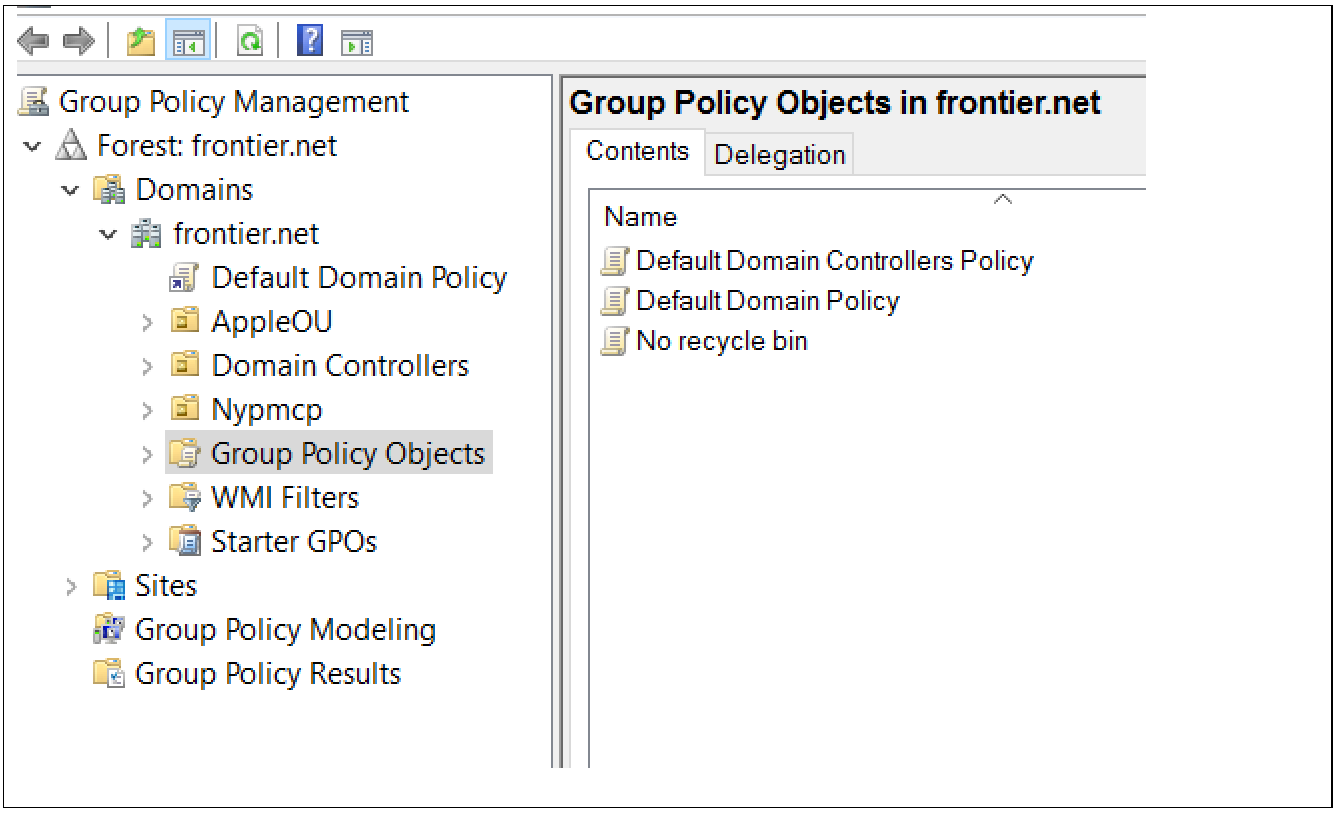
□ Compress contents to save disk space

☑ Encrypt contents to secure data

6. (b) Create a group policy called “**No Recycle bin**” in the **Group Policy Objects** folder. This policy removes the recycle bin from users’ desktop. Link the policy to AppleOU.

[Practical 2B]

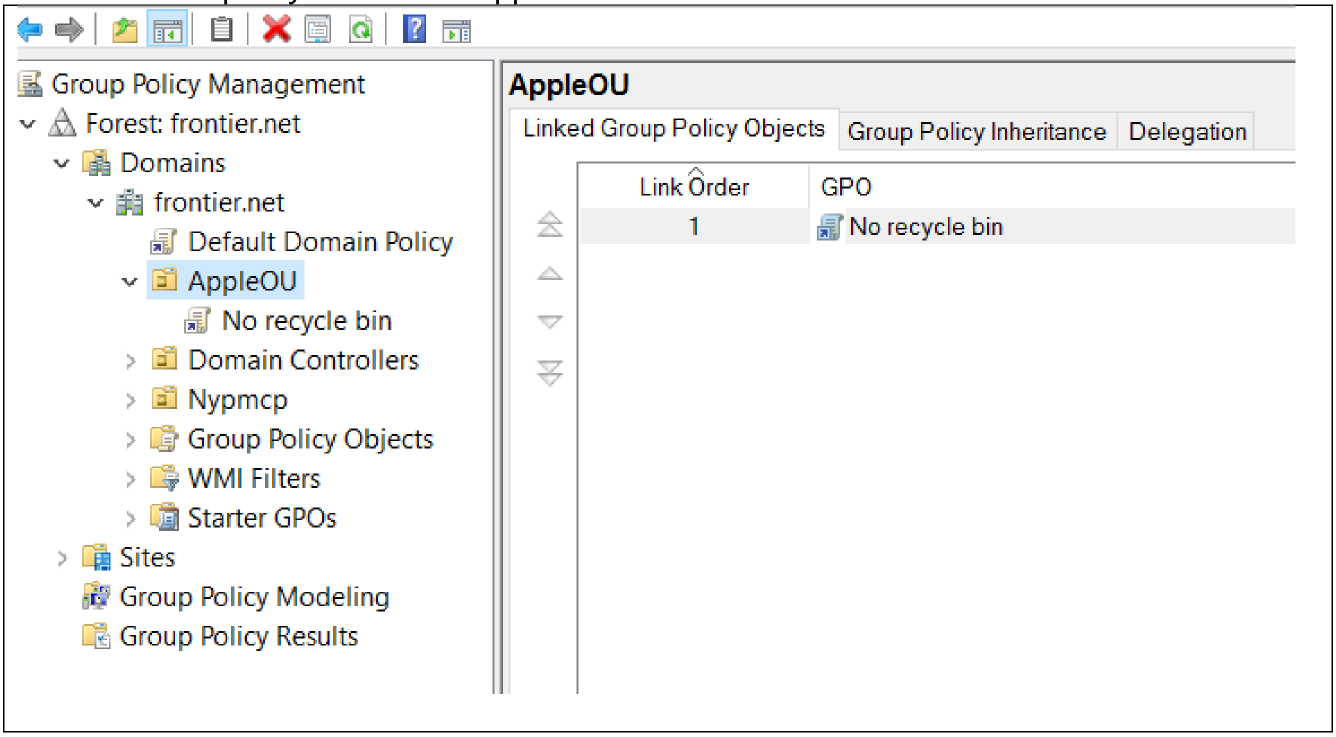
Show that the policy is in the Group Policy Objects folder.



Group Policy Objects in frontier.net

Name
Default Domain Controllers Policy
Default Domain Policy
No recycle bin

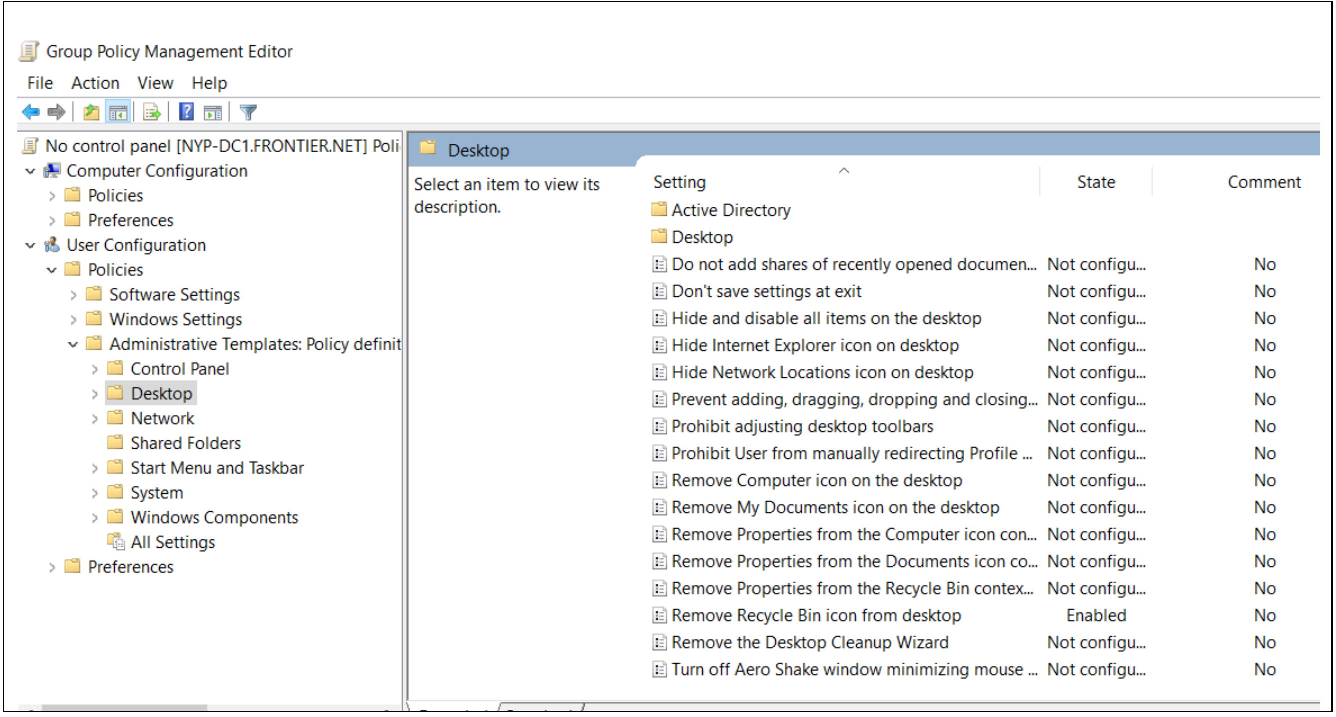
Show that the policy is linked to AppleOU OU.



AppleOU

Link Order	GPO
1	No recycle bin

Show the “No recycle bin” policy configuration.



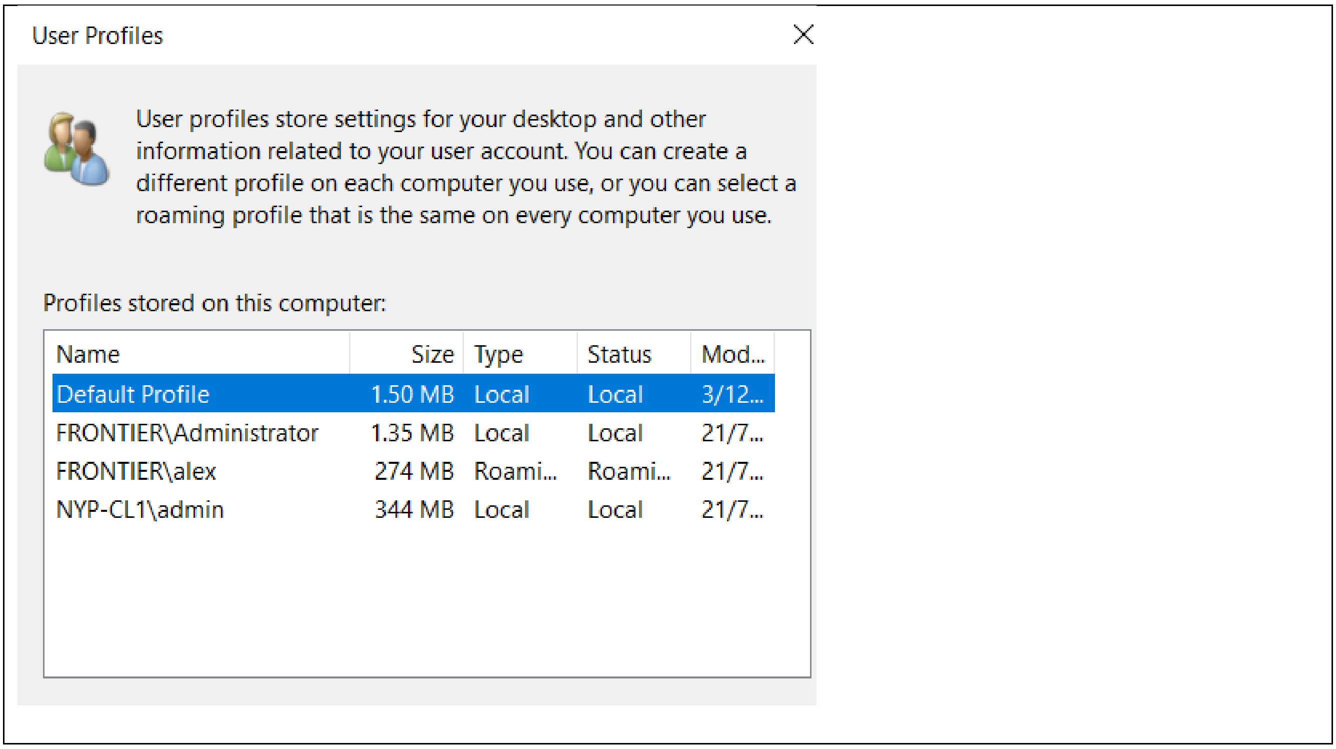
Setting	State	Comment
Active Directory		
Desktop		
Do not add shares of recently opened documen...	Not configu...	No
Don't save settings at exit	Not configu...	No
Hide and disable all items on the desktop	Not configu...	No
Hide Internet Explorer icon on desktop	Not configu...	No
Hide Network Locations icon on desktop	Not configu...	No
Prevent adding, dragging, dropping and closing...	Not configu...	No
Prohibit adjusting desktop toolbars	Not configu...	No
Prohibit User from manually redirecting Profile ...	Not configu...	No
Remove Computer icon on the desktop	Not configu...	No
Remove My Documents icon on the desktop	Not configu...	No
Remove Properties from the Computer icon con...	Not configu...	No
Remove Properties from the Documents icon co...	Not configu...	No
Remove Properties from the Recycle Bin contex...	Not configu...	No
Remove Recycle Bin icon from desktop	Enabled	No
Remove the Desktop Cleanup Wizard	Not configu...	No
Turn off Aero Shake window minimizing mouse ...	Not configu...	No

7. Configure a **Roaming** profile for **Alex**. Create any additional files or folders for this question in (VM) C:\ drive. Test the roaming profile either by using the Windows Client or using the Windows Server.

Note: in order to show the roaming profile status, you must first log into the account. You should log in from the client but if your client is unable to join the domain, then you can log into the account at the server. However, ordinary account cannot log into the server unless you make the account a member of the backup operator group.

[Practical 1(d)]

Display the screen to show Alex’s roaming profile status.



User Profiles

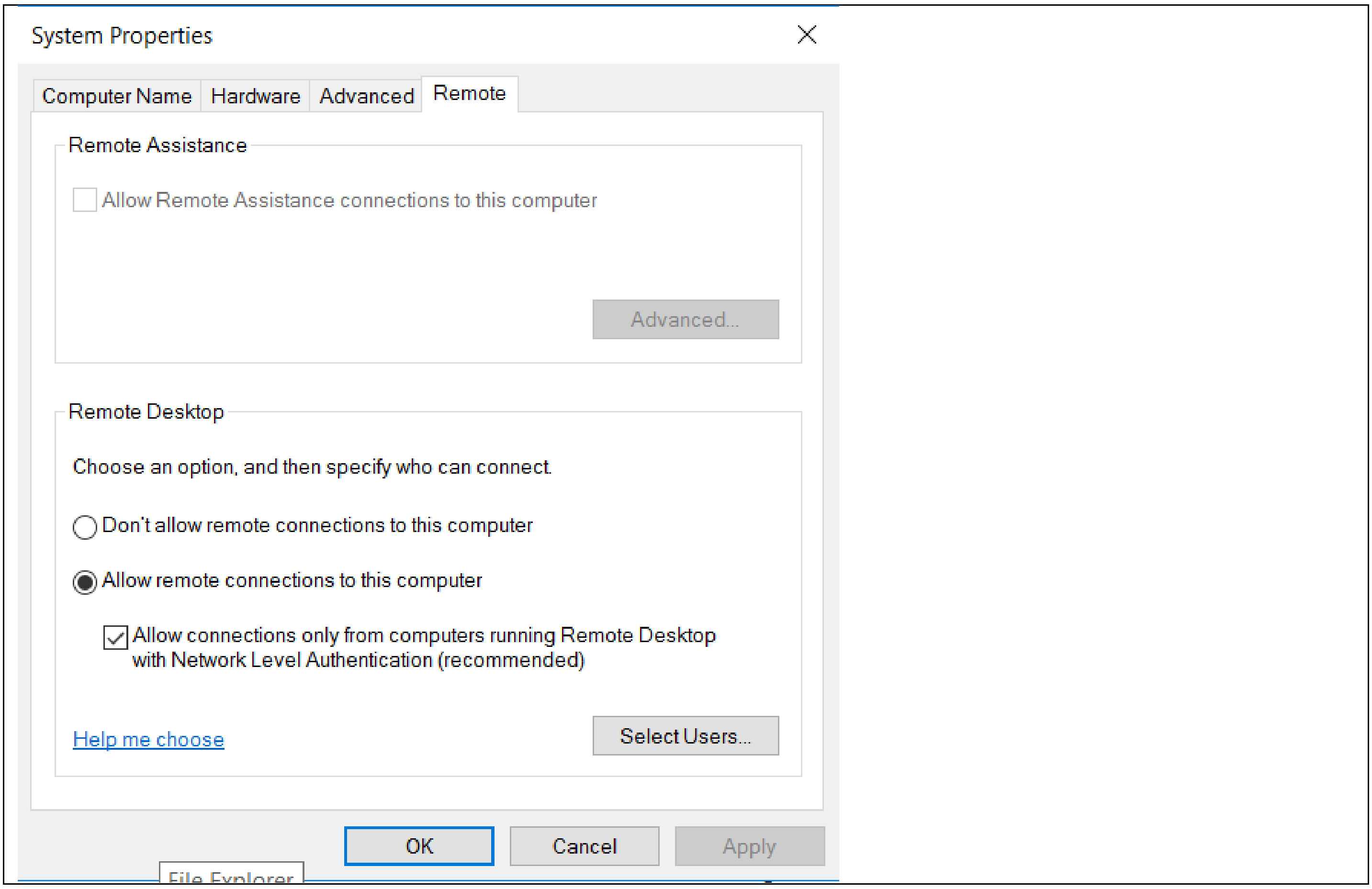
User profiles store settings for your desktop and other information related to your user account. You can create a different profile on each computer you use, or you can select a roaming profile that is the same on every computer you use.

Profiles stored on this computer:

Name	Size	Type	Status	Mod...
Default Profile	1.50 MB	Local	Local	3/12...
FRONTIER\Administrator	1.35 MB	Local	Local	21/7...
FRONTIER\alex	274 MB	Roami...	Roami...	21/7...
NYP-CL1\admin	344 MB	Local	Local	21/7...

8. Configure the Windows Server to have remote access. Display the screen to show that remote access has been activated.

[Practical 5A]



System Properties

Remote Assistance

□ Allow Remote Assistance connections to this computer

Remote Desktop

Choose an option, and then specify who can connect.

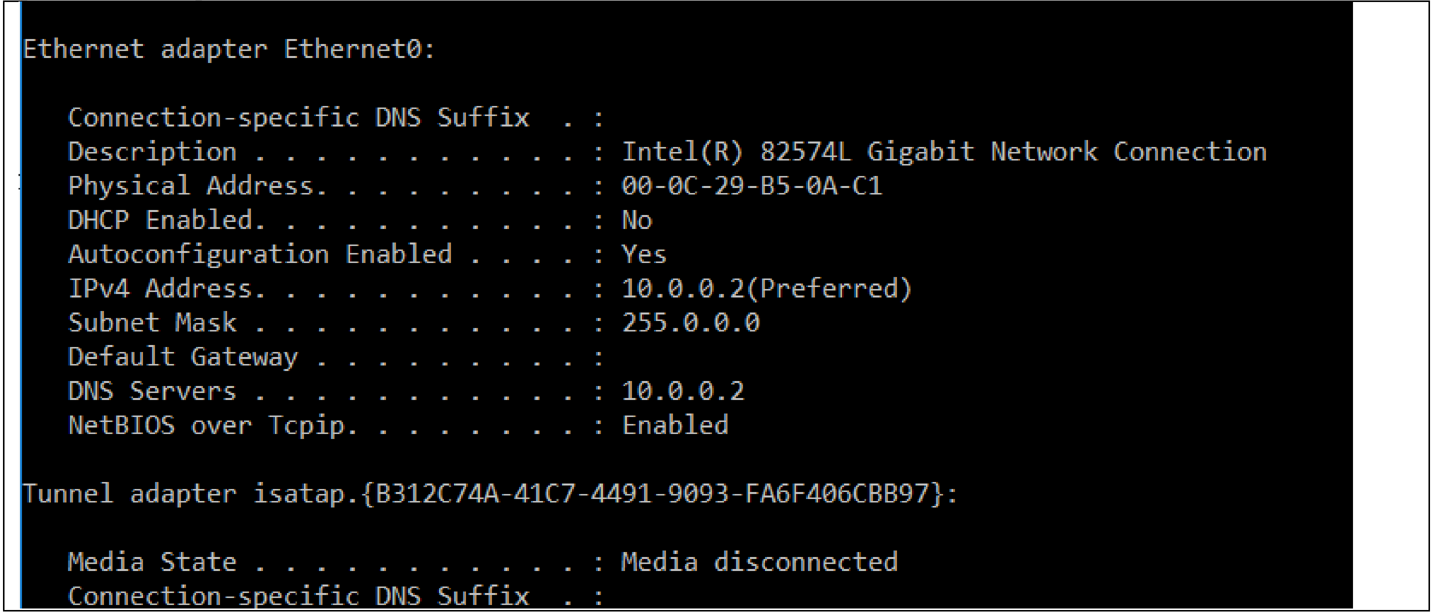
○ Don't allow remote connections to this computer

● Allow remote connections to this computer

☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

9. Show that the server network configuration is set to the following:
IP address = 10.0.0.2
Network mask = 255.0.0.0
DNS = 10.0.0.2
You can use any method to do this.

[Practical 1b]

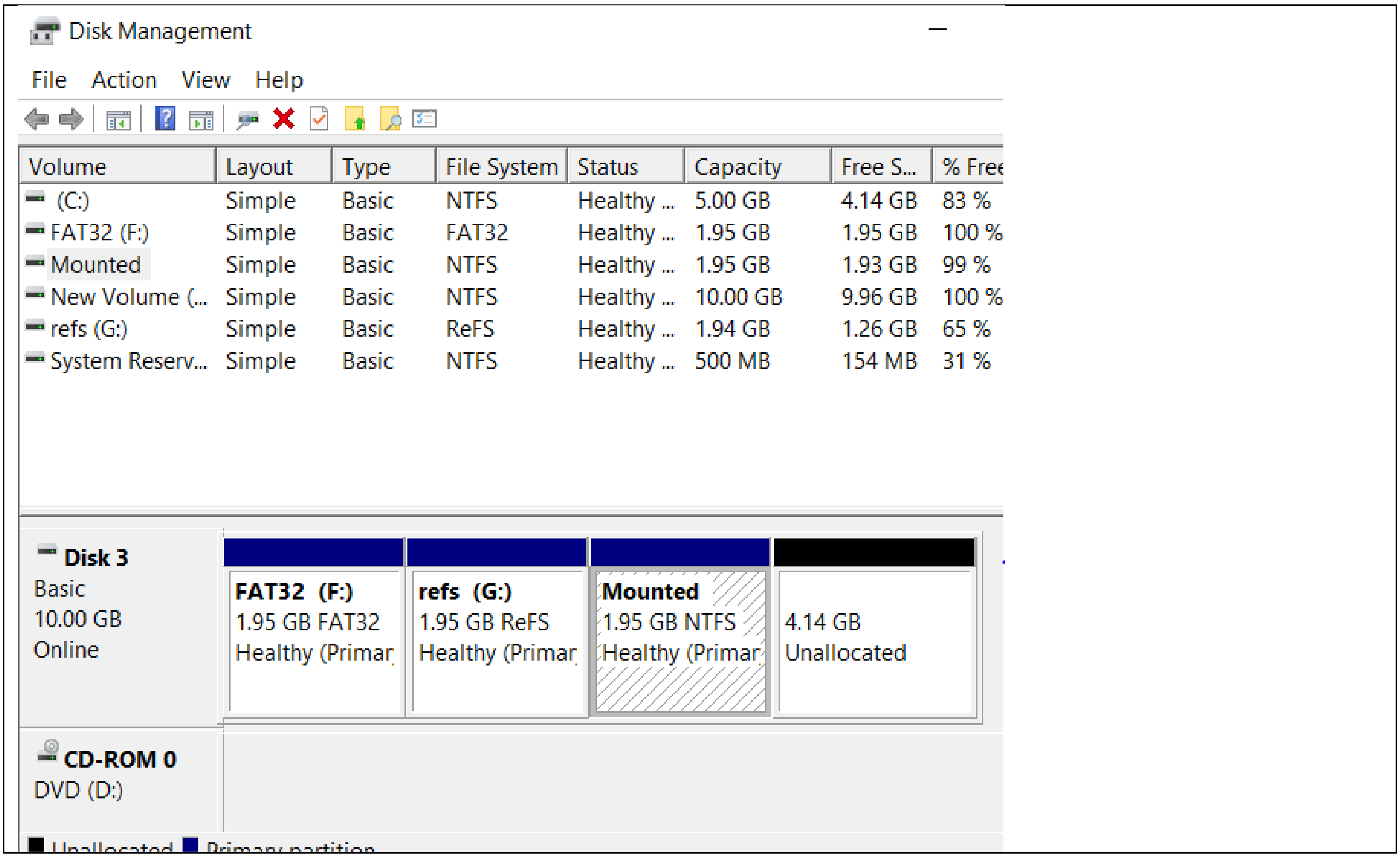


```
Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-B5-0A-C1
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.0.0.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.0.0.0
   Default Gateway . . . . . . . . . :
   DNS Servers . . . . . . . . . . . : 10.0.0.2
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{B312C74A-41C7-4491-9093-FA6F406CBB97}:

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

10. Add a new hard disk of 10 GB. Create the following volumes on it:
(a) A simple volume of 2GB formatted as FAT32. Volume name is fat32. Any drive letter.
(b) A simple volume of 2GB formatted as ReFS. Volume name is refs. Any drive letter.
(c) A simple volume of 2GB formatted as NTFS. Mount it to a folder named MountEverest in C:\ drive. The volume name is Mounted.

[Practical 3]

Use disk management to display the above results.



Volume	Layout	Type	File System	Status	Capacity	Free S...	% Free
(C:)	Simple	Basic	NTFS	Healthy ...	5.00 GB	4.14 GB	83 %
FAT32 (F:)	Simple	Basic	FAT32	Healthy ...	1.95 GB	1.95 GB	100 %
Mounted	Simple	Basic	NTFS	Healthy ...	1.95 GB	1.93 GB	99 %
New Volume (...	Simple	Basic	NTFS	Healthy ...	10.00 GB	9.96 GB	100 %
refs (G:)	Simple	Basic	ReFS	Healthy ...	1.94 GB	1.26 GB	65 %
System Reserv...	Simple	Basic	NTFS	Healthy ...	500 MB	154 MB	31 %

Disk 3
Basic
10.00 GB
Online

FAT32 (F:)
1.95 GB FAT32
Healthy (Primar

refs (G:)
1.95 GB ReFS
Healthy (Primar

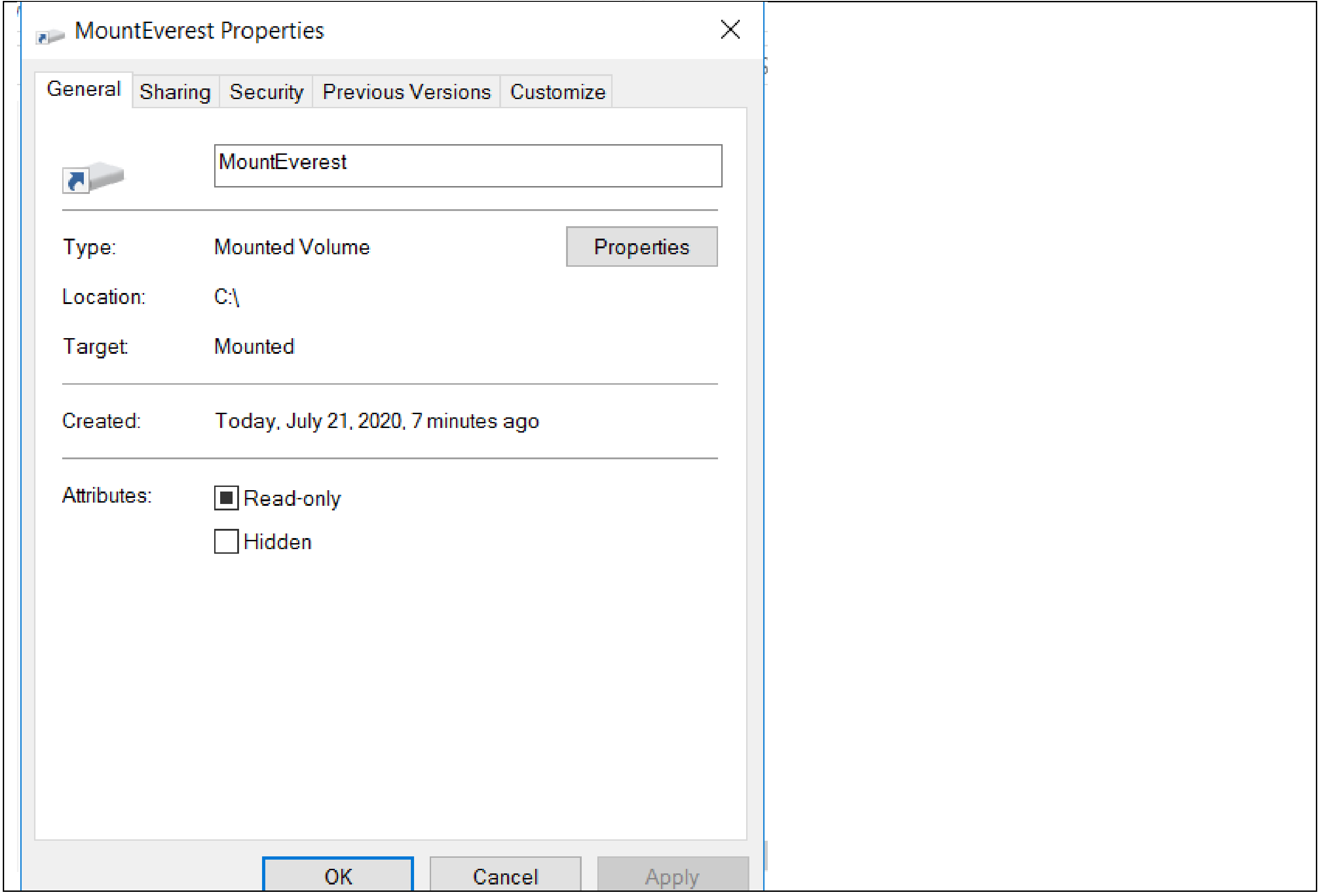
Mounted
1.95 GB NTFS
Healthy (Primar

4.14 GB
Unallocated

CD-ROM 0
DVD (D:)

■ Unallocated ■ Primary partition

Show the mounted drive details using the file explorer:



MountEverest

Type: Mounted Volume

Location: C:\

Target: Mounted

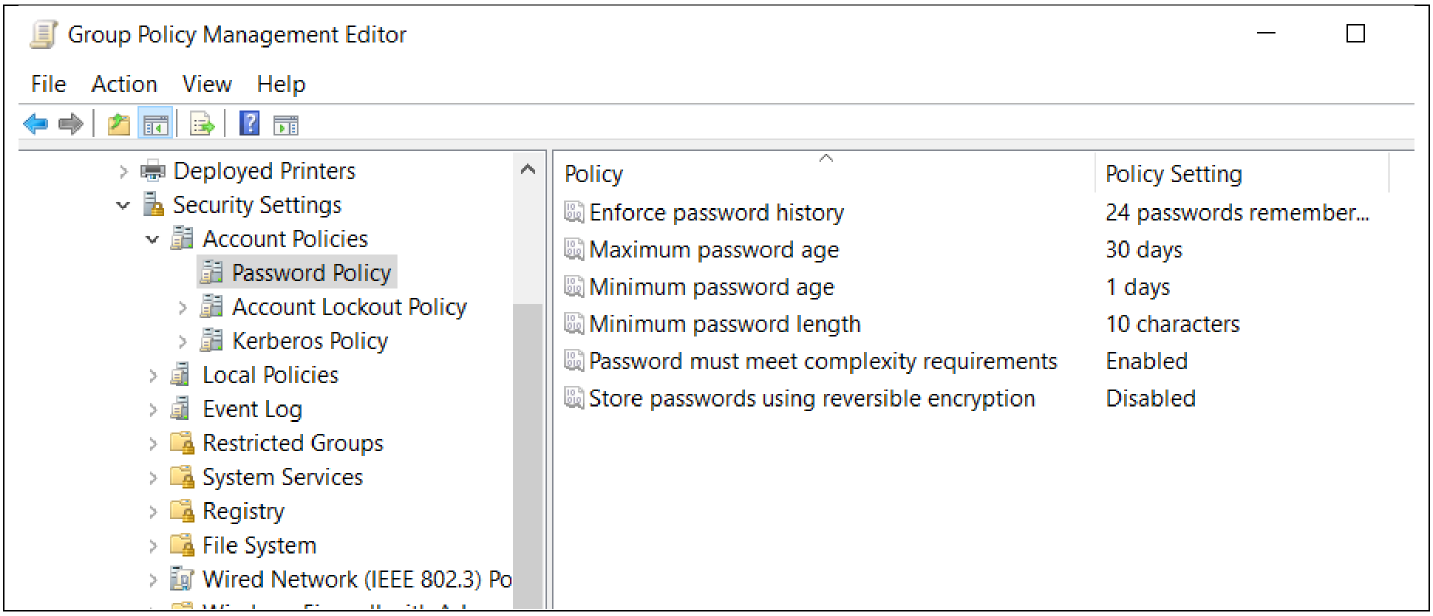
Created: Today, July 21, 2020, 7 minutes ago

Attributes: ■ Read-only
□ Hidden

11. Set the password policy for EVERYONE in the domain as follows:
(a) Password must change every 30 days (Maximum password age)
(b) Minimum password length = 10 characters
The other password settings can keep the default settings.

[Practical 6A]

Use Group Policy Management to display the password policy settings.

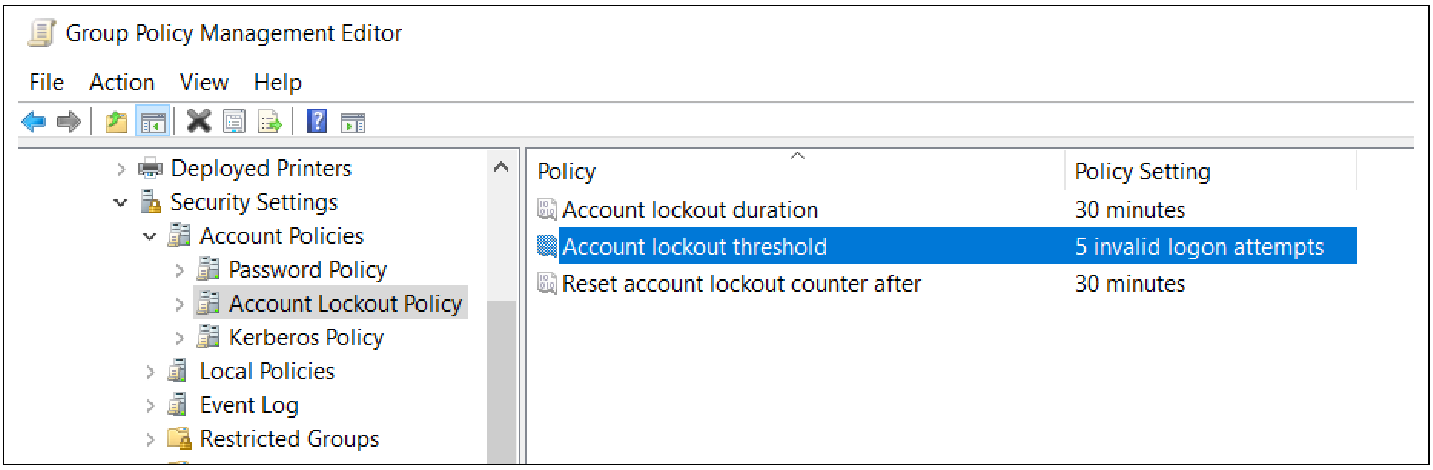


Policy	Policy Setting
Enforce password history	24 passwords remember...
Maximum password age	30 days
Minimum password age	1 days
Minimum password length	10 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

12. Configure the setting for EVERYONE in the domain such that the account is locked out after 5 failed login attempts. The lockout duration and reset duration is 30 minutes (default).

[Practical 6A - minus the template; direct configuration]

Use Group Policy Management tool to show the settings.



Policy	Policy Setting
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

- End of Paper -