

Manage and maintain network resources, and its services applying suitable policies and drafting security and redundancy practices.

1st Given Edward Patch
Software Engineer Student (of HND Year 2)
Network Operating Systems and Services
University of Wales Trinity St. Davids (of Nitheesh Murugan Kaliyamurthy)
 Swansea, Wales
 Student ID: 1801492

CONTENTS

I	Introduction	1
II	Worksheet Three - Practical	1
II-A	Windows Client I - File Permissions . .	1
II-B	Windows Server I - Folder Sharing . . .	2
II-C	Windows Client I - Network Drive . . .	4
II-D	Windows Server I - Organisational Unit	4
II-E	Windows Server I - Control Panel Restriction	5
II-F	Windows Server I - Command Prompt Restriction	5
II-G	Windows Server I - Removable Media Drives	6
II-H	Windows Server I - Organisation Unit .	6
II-I	Windows Server I - Software Install Restrictions	7
II-J	Windows Server88 I - Password Policy	7
III	Worksheet Three - Observational	8
III-A	Differences of Local Permissions and File Shares	8
III-B	Group Policy Management	8
III-C	Password Principles	8
IV	List of Abbreviations	8
V	Conclusion	8
VI	References	8

Abstract—Managing and maintaining network resources using network policy and security practices is demonstrated with Windows Servers and Windows Clients. Demonstration of permissions and techniques of file sharing are within the report.

Index Terms—Group Policies, Restrictive Access, GPM

I. INTRODUCTION

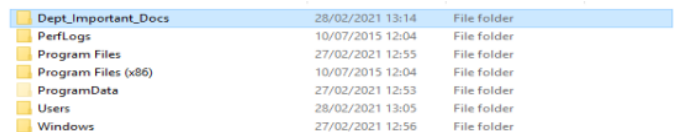
This report separates into two sections:-

- Worksheet Three - Practical.
- Worksheet Three - Observational.

II. WORKSHEET THREE - PRACTICAL

A. Windows Client I - File Permissions

Image displays the creation of the 'Debt_Important_Docs' folder.



Dept_Important_Docs	28/02/2021 13:14	File folder
PerfLogs	10/07/2015 12:04	File folder
Program Files	27/02/2021 12:55	File folder
Program Files (x86)	10/07/2015 12:04	File folder
ProgramData	27/02/2021 12:53	File folder
Users	28/02/2021 13:05	File folder
Windows	27/02/2021 12:56	File folder

Fig. 1. Figure of Windows Client I Creation of Folder.

Figure 2 shows the creation of a text file inside 'Debt_Important_Docs' folder named 'importantFile'.

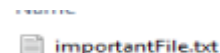


Fig. 2. Figure of Windows Client I Creation of File.

This dialog pops up after attempting to remove default groups from the File Permissions — Security tab.

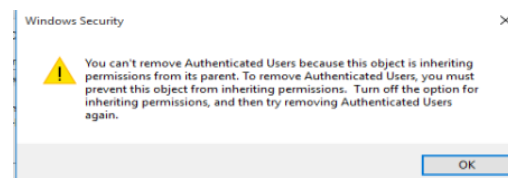


Fig. 3. Figure of Windows Client I Folder Security.

Process shows the method to remove the inheritance connected to the default groups. This enables the removal of the default groups, for example Authenticated Users and SYSTEM.

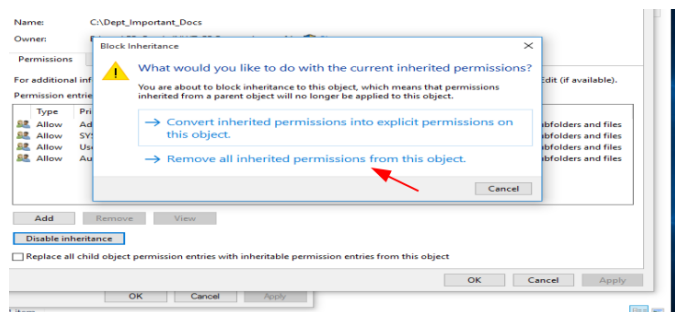


Fig. 4. Figure of Windows Client I Folder Security.

The figure 5 displays the confirmation dialog to remove all access to all user groups. This provides a clean slate to create new permissions.

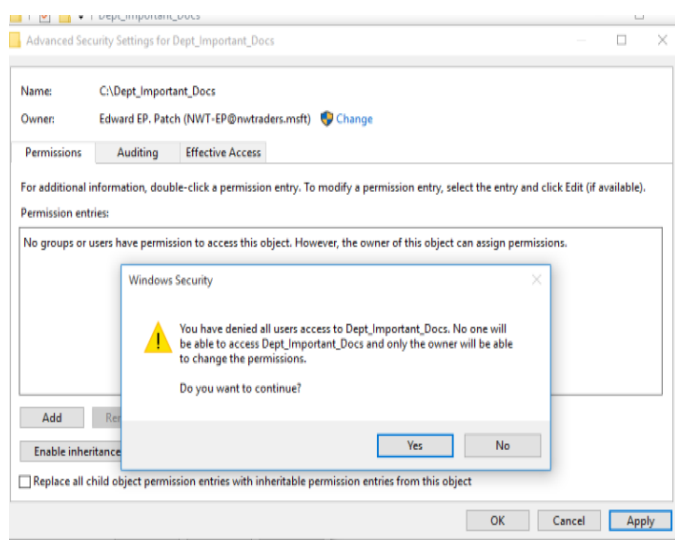


Fig. 5. Figure of Windows Client I Folder Security.

Evidence of *Edward EP. Patch (NWT-EP@nwtraders.msft)* being added to the permissions. **Note:** *Gareth GS. Smith (NTW-GS@nwtraders.msft)* was added to the permissions.

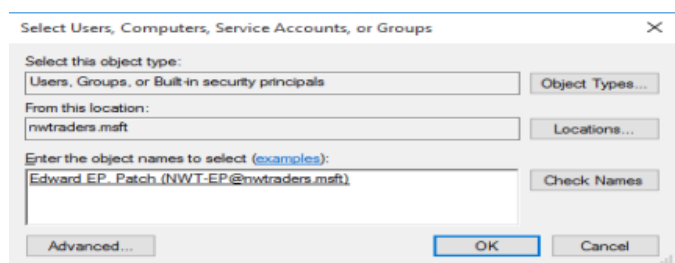


Fig. 6. Figure of Windows Client I Folder Security.

Figure 8 indicates that the Modify permission was not given to the user.

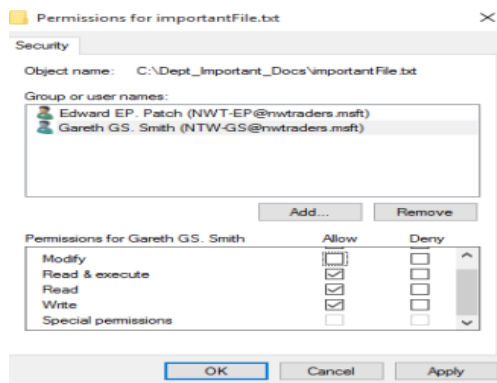


Fig. 7. Figure of Windows Client I Folder Security.

Text is added to the text file, which is evidence in the figure below.

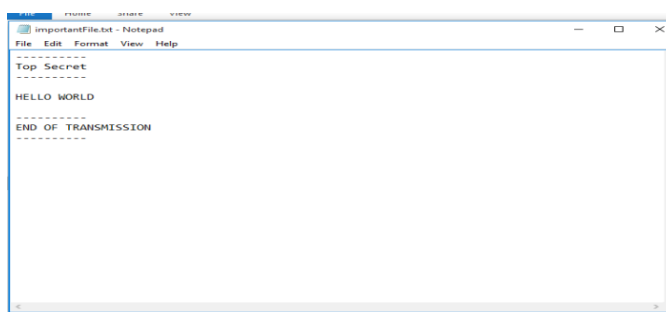


Fig. 8. Figure of Windows Client I Folder Security.

B. Windows Server I - Folder Sharing

Server Message Block (SMB) Share Feature was setup on *Windows Server I* to share files towards other workstations within the network.

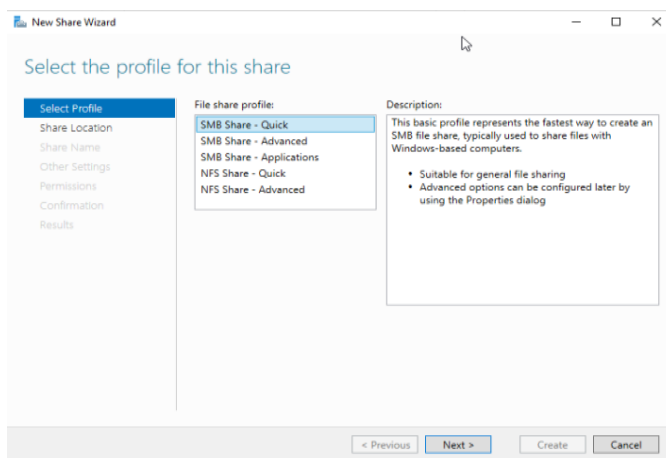


Fig. 9. Figure of Windows Server I Folder Sharing.

Windows Server I (DC1-NWT) C drive was selected for the file sharing to be enabled on the network.

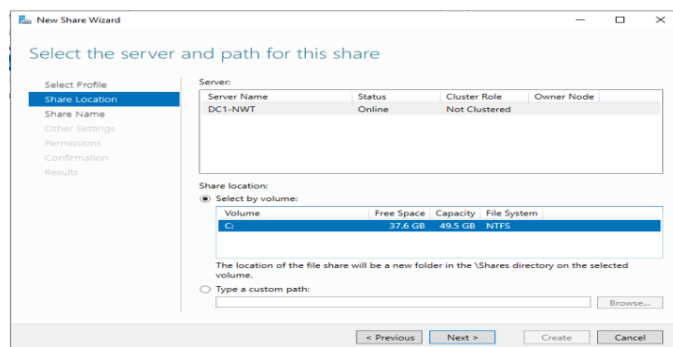


Fig. 10. Figure of Windows Server I Folder Sharing.

Set Share Name to 'DebtNetShare\$' and selected the location for file sharing.

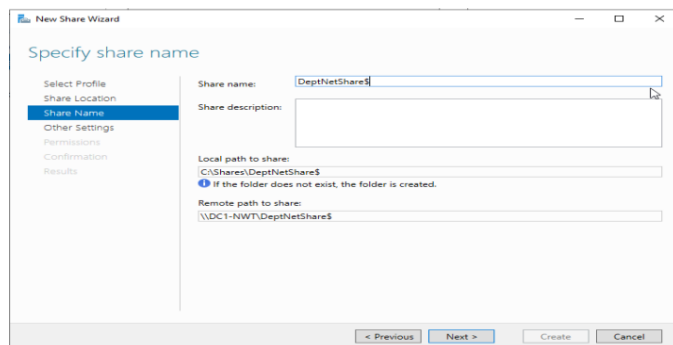


Fig. 11. Figure of Windows Server I Folder Sharing.

Configured the share settings of *DebtNetShare\$* to **Enable access-based enumeration** and **Allow caching of share**.

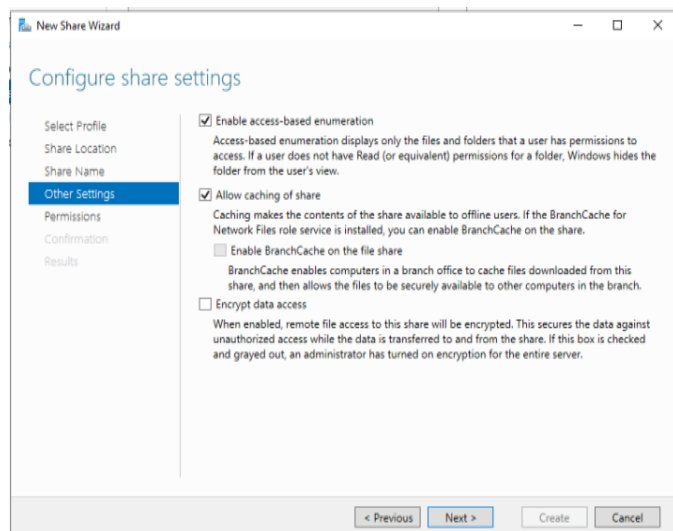


Fig. 12. Figure of Windows Server I Folder Sharing.

Set permissions under *DebtNetShare\$* for *Edward EP. Patch* user to have *Modify, Read & Execute, List folder contents, Read and Write*.

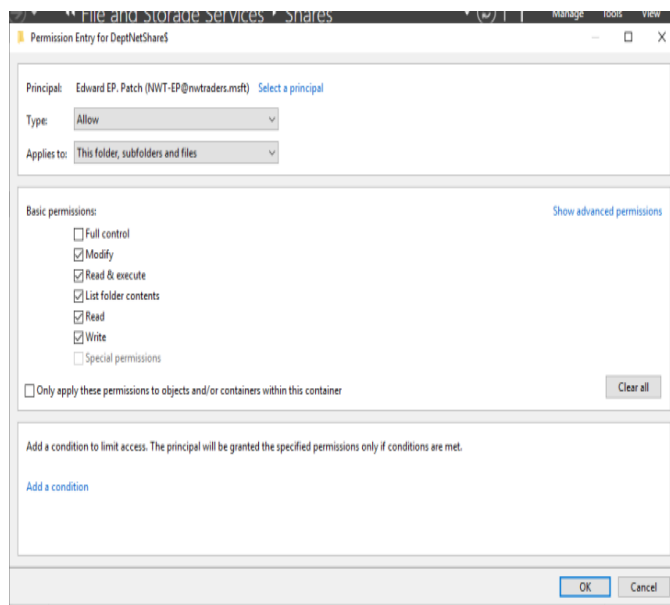


Fig. 13. Figure of Windows Server I Folder Sharing.

Set permissions under *DebtNetShare\$* for *Gareth GS. Smith* user to have *Modify, Read & Execute, List folder contents, Read and Write*.

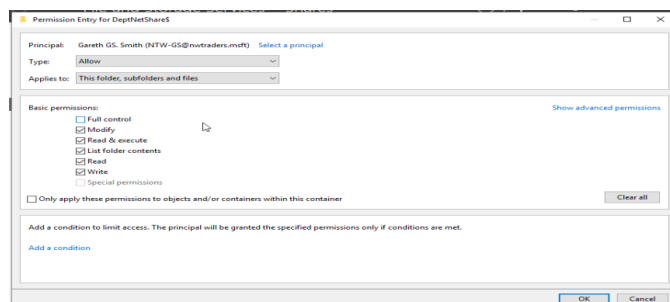


Fig. 14. Figure of Windows Server I Folder Sharing.

An overview of the Folder Permissions.

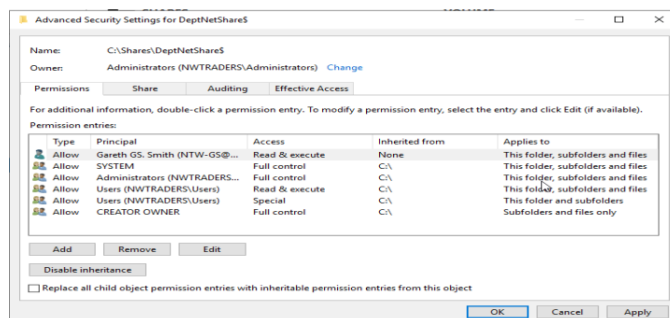


Fig. 15. Figure of Windows Server I Folder Sharing.

C. Windows Client I - Network Drive

The figure 16 shows the *DebtNetShare\$* File Share. The address of the File Share is `\\DC1-NWT\DebtNetShare$`.

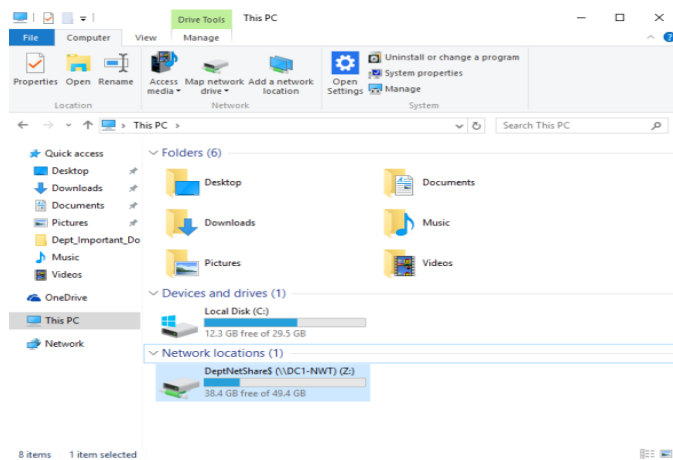


Fig. 16. Figure of Windows Client I Network Drive.

The folder and text file was created in the File Share.

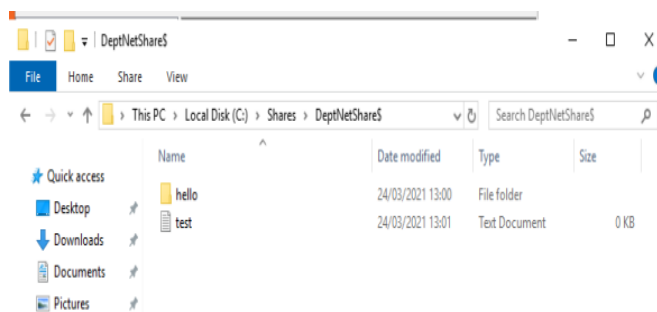


Fig. 17. Figure of Windows Client I Network Drive.

Evidence:

Evidence of folders and files created from *Windows Client I* displayed on *Windows Server I*.

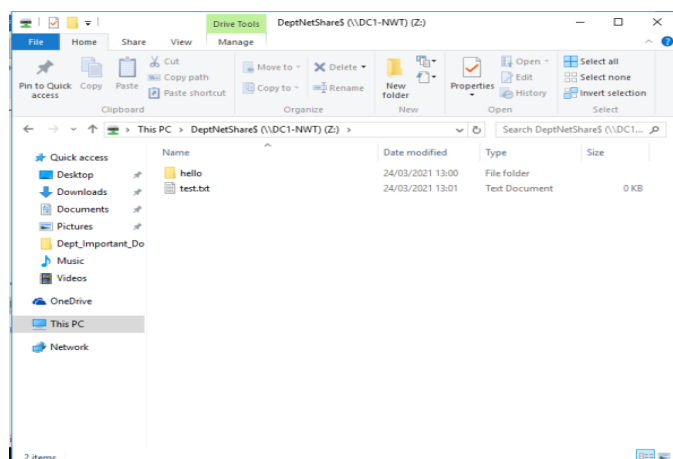


Fig. 18. Figure of Windows Server I Network Drive.

Creation of a Organisational Unit set with the name '*Non Admin Users*'.

D. Windows Server I - Organisational Unit

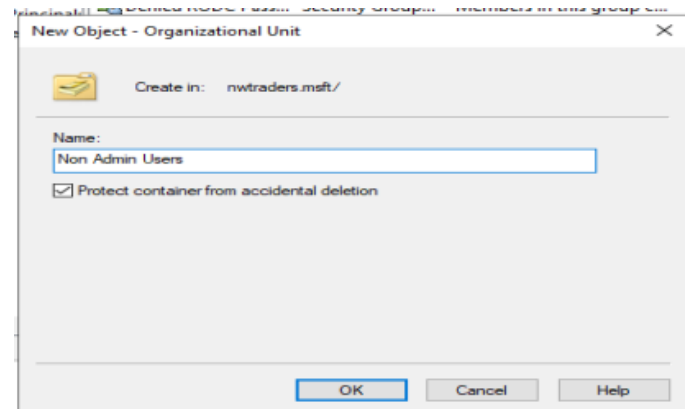


Fig. 19. Figure of Windows Server I Organisational Unit.

A new user is created named *John JM. Maryland (NWT-JM)*.

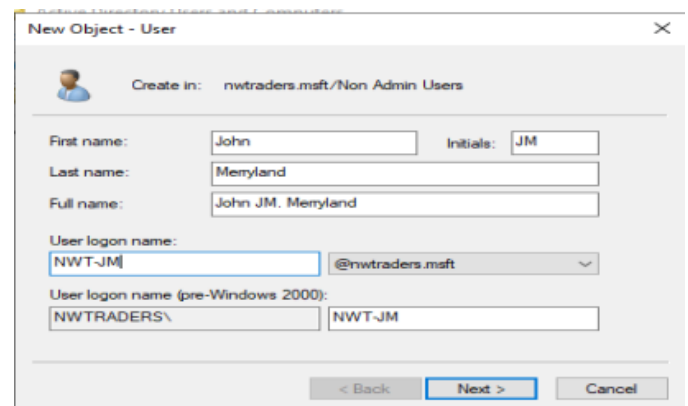


Fig. 20. Figure of Windows Server I Organisational Unit.

All users created including the previously created user is moved to the *Non Admin Users* Organisational Unit Group.

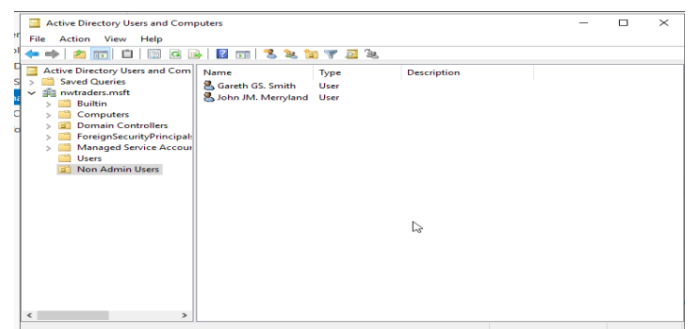


Fig. 21. Figure of Windows Server I Organisational Unit.

E. Windows Server I - Control Panel Restriction

In Group Policy Management Console under Non Admin Users created a group policy named 'NoCtrlPanlAccess'.

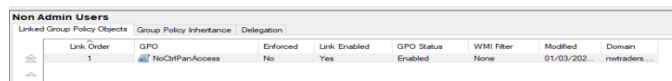


Fig. 22. Figure of Windows Server I Group Policy Management Console.

The figure 23 enabled the **Prohibit access to Control Panel and PC settings** under the 'NoCtrlPanlAccess'.

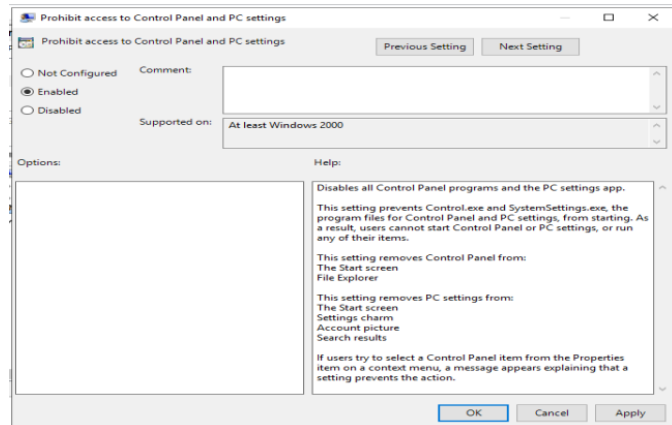


Fig. 23. Figure of Windows Server I Group Policy Management Console.

Updated Policies: The GPUupdate script updates the policies set within the server.

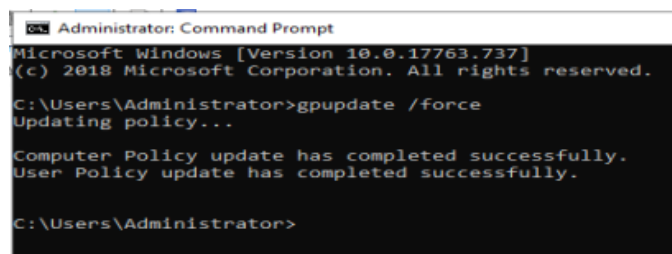


Fig. 24. Figure of Windows Server I GPUupdate Script.

Evidence: Evidence of Control Panel being unauthorised for **Non Admin Users**.

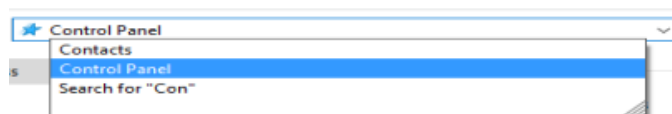


Fig. 25. Figure of Windows Client I Control Panel Error.

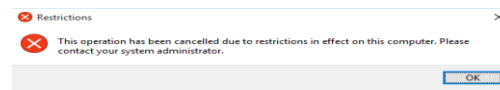


Fig. 26. Figure of Windows Client I Control Panel Error.

F. Windows Server I - Command Prompt Restriction

The figure 27 enabled the **Prohibit access to command prompt** under the 'NoCtrlPanlAccess'.

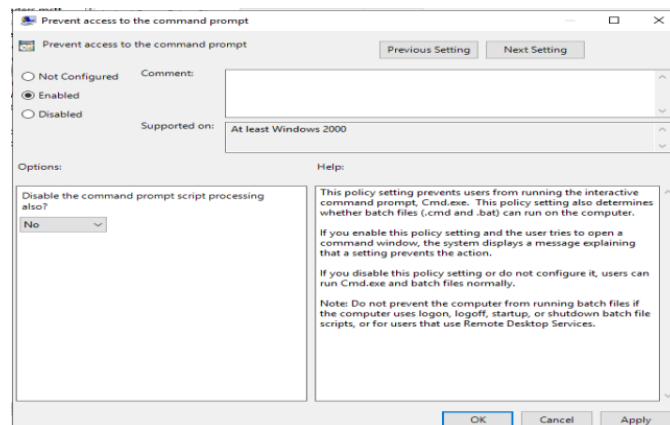


Fig. 27. Figure of Windows Server I Group Policy Management Console.

Evidence: Evidence of the Command Prompt blocked on the *Windows Client I*. However, the PowerShell is not disabled in this setup, which offers more power, to running scripts and administrative commands.

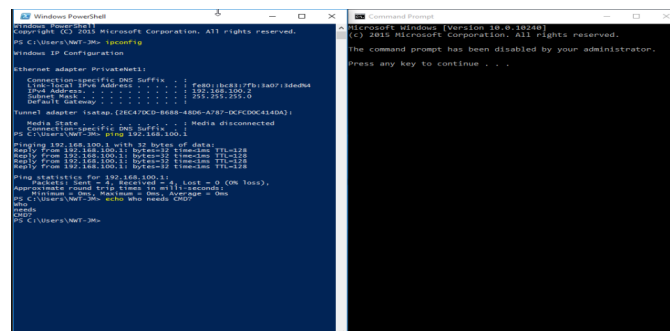


Fig. 28. Figure of Windows Client I Command Prompt and Powershell Access.

G. Windows Server I - Removable Media Drives

Created a Group Policy Organisation named 'NoauthSoftInstallS'.

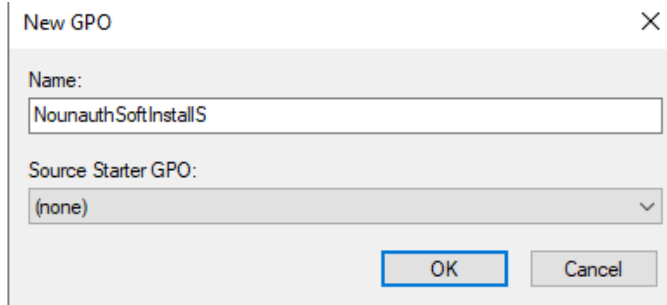


Fig. 29. Figure of Windows Server I Group Policy Management Console.

Inserted Universal Serial Bus (USB) via Virtual Box.

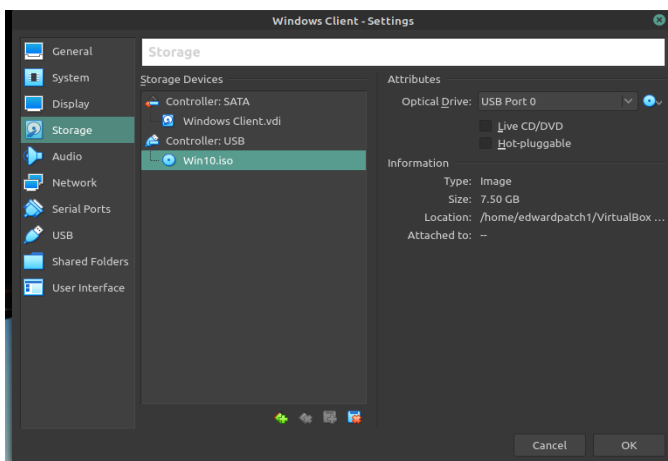


Fig. 30. Figure of Windows Server I Group Policy Management Console.

Evidence:

USB never displays, which could suggest that the policy works.

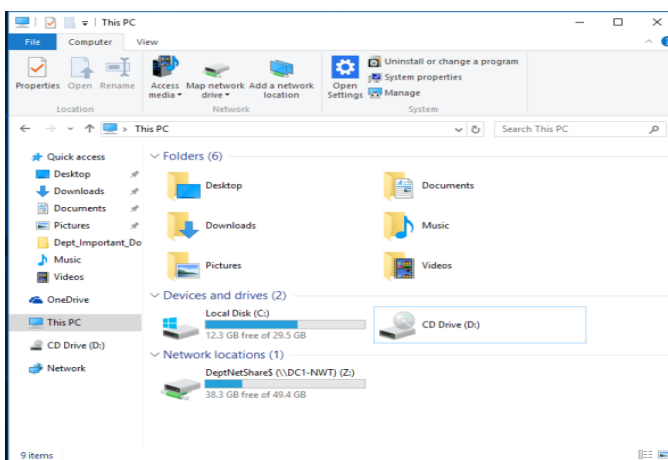


Fig. 31. Figure of Windows Server I Group Policy Management Console.

H. Windows Server I - Organisation Unit

Within the Server Manager, a new Organisation Unit named 'NWClient Computers' is created. Moved DC1-NWT to NWClient Computers.

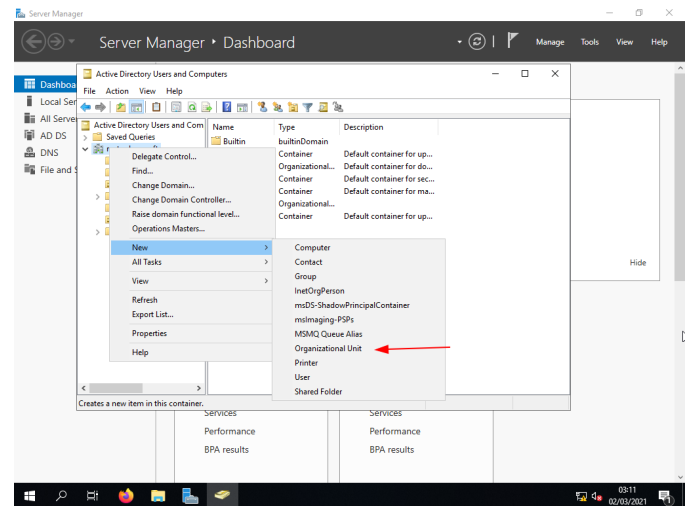


Fig. 32. Figure of Windows Server I Organisational Unit.

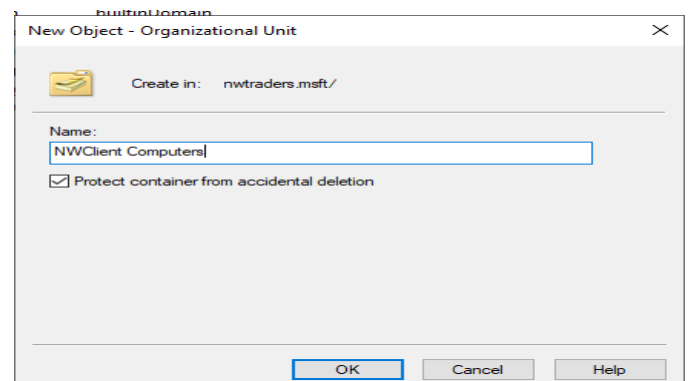


Fig. 33. Figure of Windows Server I Organisational Unit.

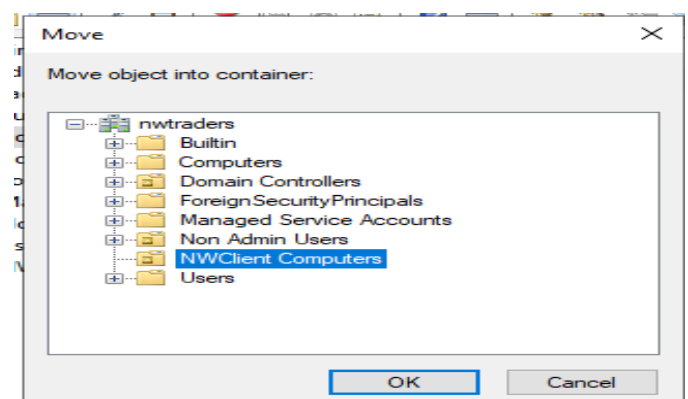


Fig. 34. Figure of Windows Server I Organisational Unit.

I. Windows Server I - Software Install Restrictions

Created a Group Policy Organisation named 'NounauthSoftInstallS'.

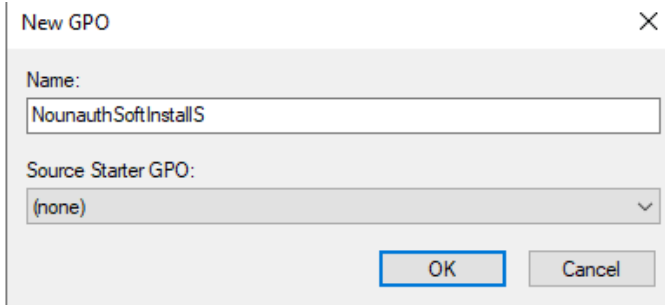


Fig. 35. Figure of Windows Server I Group Policy Management Console.

The figure 36 enabled the **Prohibit User Installs** under the 'NounauthSoftInstallS'.

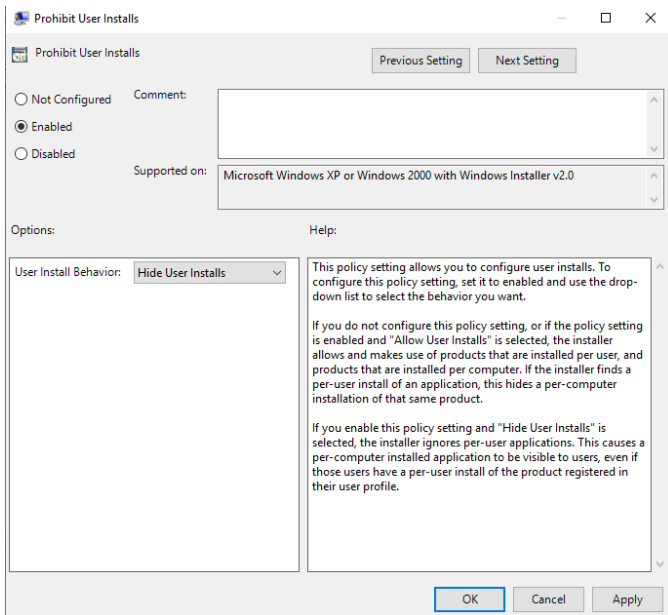


Fig. 36. Figure of Windows Server I Group Policy Management Console.

Updated Group Policies with GPOUpdate script.

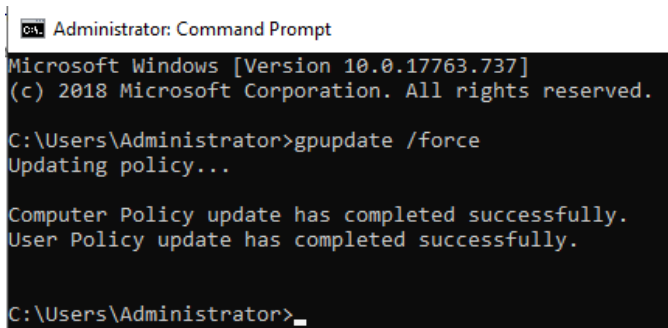


Fig. 37. Figure of Windows Server I GPOUpdate Script.

Evidence:

The evidence shows that a non-administrator can not install software.

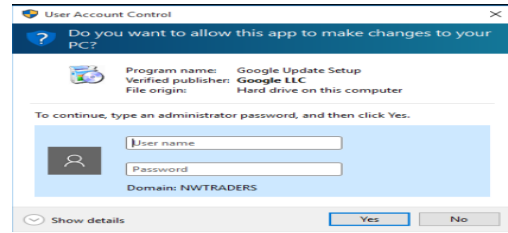


Fig. 38. Figure of Windows Client I Installation of Google Chrome.

J. Windows Server88 I - Password Policy

A password policy was put in place to prevent passwords that are less than ten characters, any weak and common passwords from being used within the network.

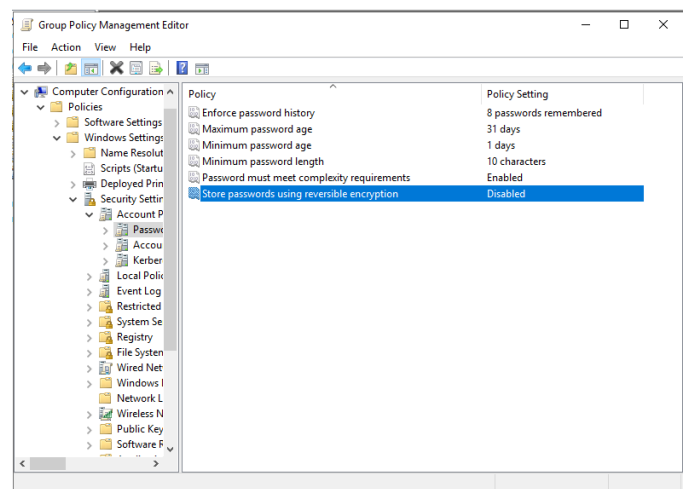


Fig. 39. Figure of Windows Server I Group Policy Management Console.

Updated the policies within the network via the GPOUpdate script.

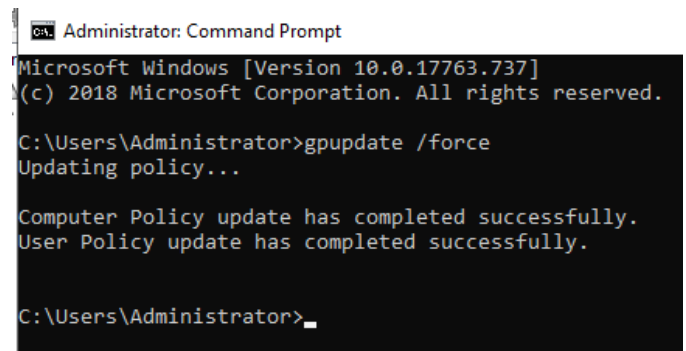


Fig. 40. Figure of Windows Server I GPOUpdate Script.

Evidence: Evidence shows that the password policy in place works. The password was eight characters long, mixed with case-sensitive and case-insensitive, numerical and special characters. **Note:** After testing the password policy, the user account was created successfully with twelve characters.

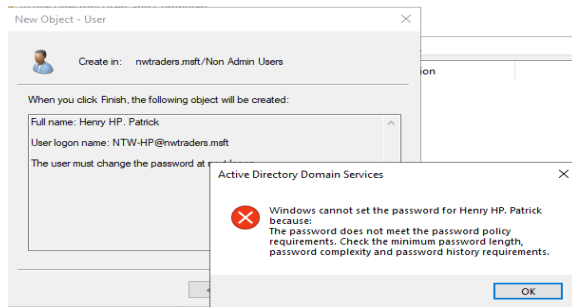


Fig. 41. Figure of Windows Server I Testing of Password Policy.

III. WORKSHEET THREE - OBSERVATIONAL

A. Differences of Local Permissions and File Shares

The difference between local permissions and file shares is that local permissions is enabled for those who connect via a workstation within the network. Whereas, remote users that access outside require permissions for the file share area.

File Transfer Protocol (FTP) Permissions cited from Dan Gookin [1], How to Set File Permissions on a Remote FTP Site:

- Read.
- Write.
- Execute.

File-Sharing cited from Cindy NG [2], New Technology File System (NTFS) Permissions vs Share: Everything You Need to Know:

- Full Control.
- Modify.
- Read and Execute.
- List Folder Contents.
- Read.
- Write.

B. Group Policy Management

Group Policy Management controls the policies put in place for different Organisation Unit's. An example from Leopide, Danny Murphy [3] Top 10 Most Important Group Policy Settings for Preventing Security Breaches, Disable Guest Account policy, "Through a Guest Account, users can get access to sensitive data. Such accounts grant access to a Windows computer and do not require a password. Enabling this account means anyone can misuse and abuse access to your systems.

Thankfully, these accounts are disabled by default. It's best to check that this is the case in your IT environment as, if this account is enabled in your domain, disabling it will prevent people from abusing access:

In Group Policy Management Editor (opened for a custom GPO), go to 'Computer Configuration' 'Windows Settings'

'Security Settings' 'Local Policies' 'Security Options'. In the right pane, double-click 'Accounts: Guest Account Status' policy. Select 'Define this policy setting' checkbox and click 'Disabled'. Click 'Apply' and 'OK'."

C. Password Principles

Having Password house styles in practice helps reminds users to set strong and unique passwords. Controlling when a password expires and altering password requirements can make it hard to penetrate even if encrypted passwords are leaked from the company.

Peters & Associates [4] Five Core Principles of Password Security article, suggests that passwords should be too complex to memorise in the following statement:-

"There is a direct correlation between the difficulty to crack a password and its length, complexity and uniqueness. Thus, good passwords should be longer than 8 characters and contain a good mixture of upper- and lower-case letters, numbers and special characters such as '@ % \$ ~ #.'"

The length and composition of such passwords make them difficult to memorize, which is great for security, but hard for a human to control. The control is exponentially more challenging as the number of digital accounts increases. Again, great for security, but difficult to manage without help."

IV. LIST OF ABBREVIATIONS

- *SMB* - Server Message Block.
- *GPM* - Group Policy Management.
- *USB* - Universal Serial Bus.
- *GPUUpdate* - Group Policy Update (Command Script).
- *FTP* - File Transfer Protocol.
- *NTFS* - New Technology File System.

V. CONCLUSION

The report covers the methods in place to restrict user activity. These things cover:-

- Control Panel Access.
- Command Prompt Access.
- Removeable Drive Access.
- Installation Restriction.

VI. REFERENCES

- [1] D. Gookin, "How to Set File Permissions on a Remote FTP Site - dummies." [Online]. Available: <https://www.dummies.com/computers/operating-systems/windows-xp-vista/how-to-set-file-permissions-on-a-remote-ftp-site/>
- [2] N. Cindy, "NTFS Permissions vs Share: Everything You Need to Know," Oct. 2016, section: Data Security. [Online]. Available: <https://www.varonis.com/blog/ntfs-permissions-vs-share/>
- [3] D. Murphy, "Top 10 Most Important Group Policy Settings for Preventing Security Breaches," Dec. 2019. [Online]. Available: <https://www.lepide.com/blog/top-10-most-important-group-policy-settings-for-preventing-security-breaches>
- [4] PetersAssociates, "Five Core Principles of Password Security," Aug. 2019. [Online]. Available: <https://www.peters.com/blog/password-security/>