

Worksheet 3

Author: Tomos Leggett · **Student Code:** 1901852 · **Module Code:** ACCA5023

Worksheet 3

Task 1: Understanding NTFS & Share Permissions

NTFS

Share

Task 2: Utilising Group Policy Management Console to better facilitate network object management

Restricting access to the Control Panel

Restricting access to the command prompt

Restricting access to removable media drives

Restricting software installs

Enforcing Password Policy in the 'nwtraders.msft' domain

Task 3: Observational Tasks

The main differences between local permissions and file shares

NTFS (Local Permissions)

Share

What's the difference?

The role of Group Policy Management in the network environment

What is Group Policy

Sound password principles in a modern network environment

Create a strong, long password (or 'passphrase')

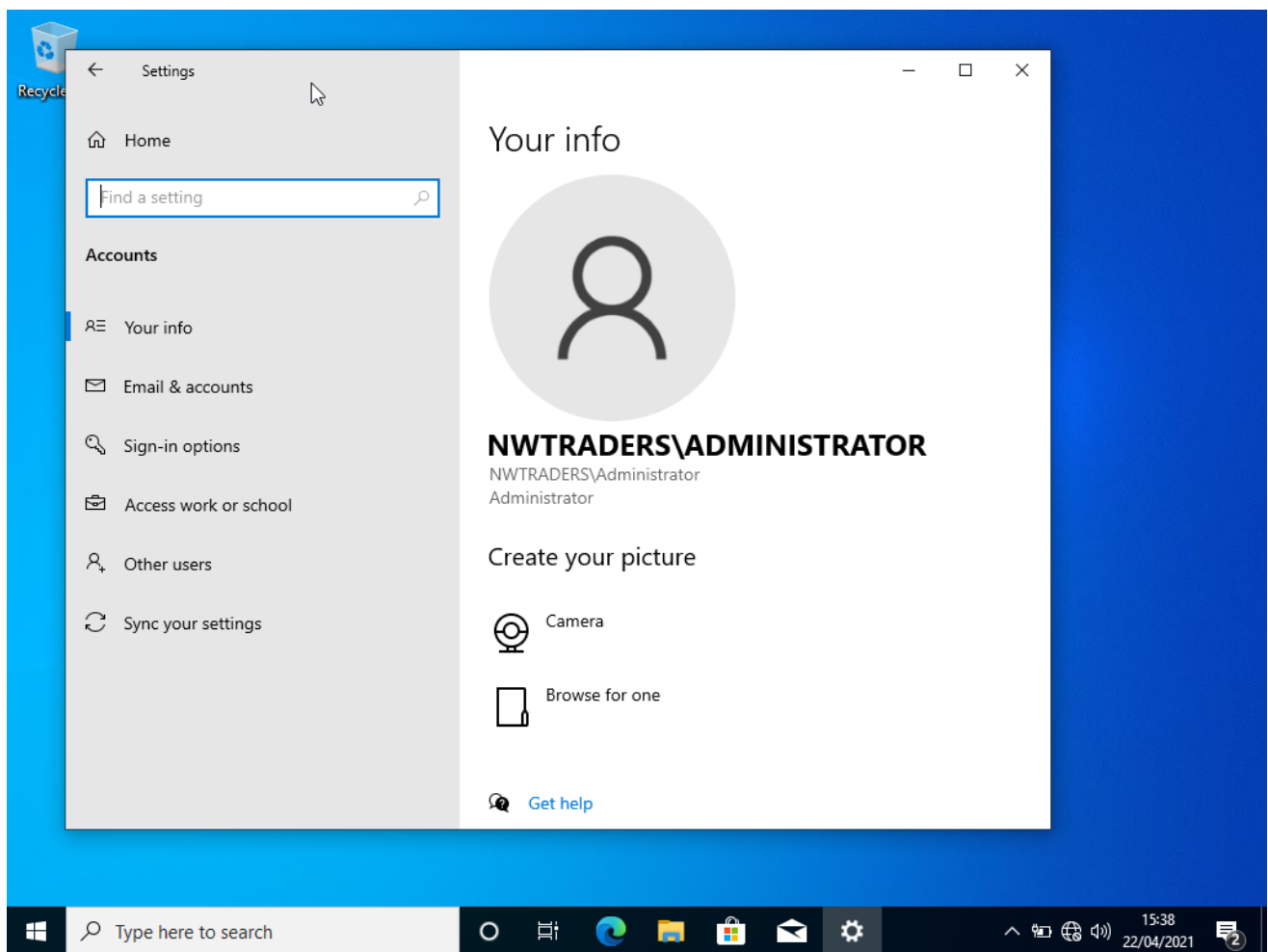
Implement a second factor of authentication

Enforcing a password history policy

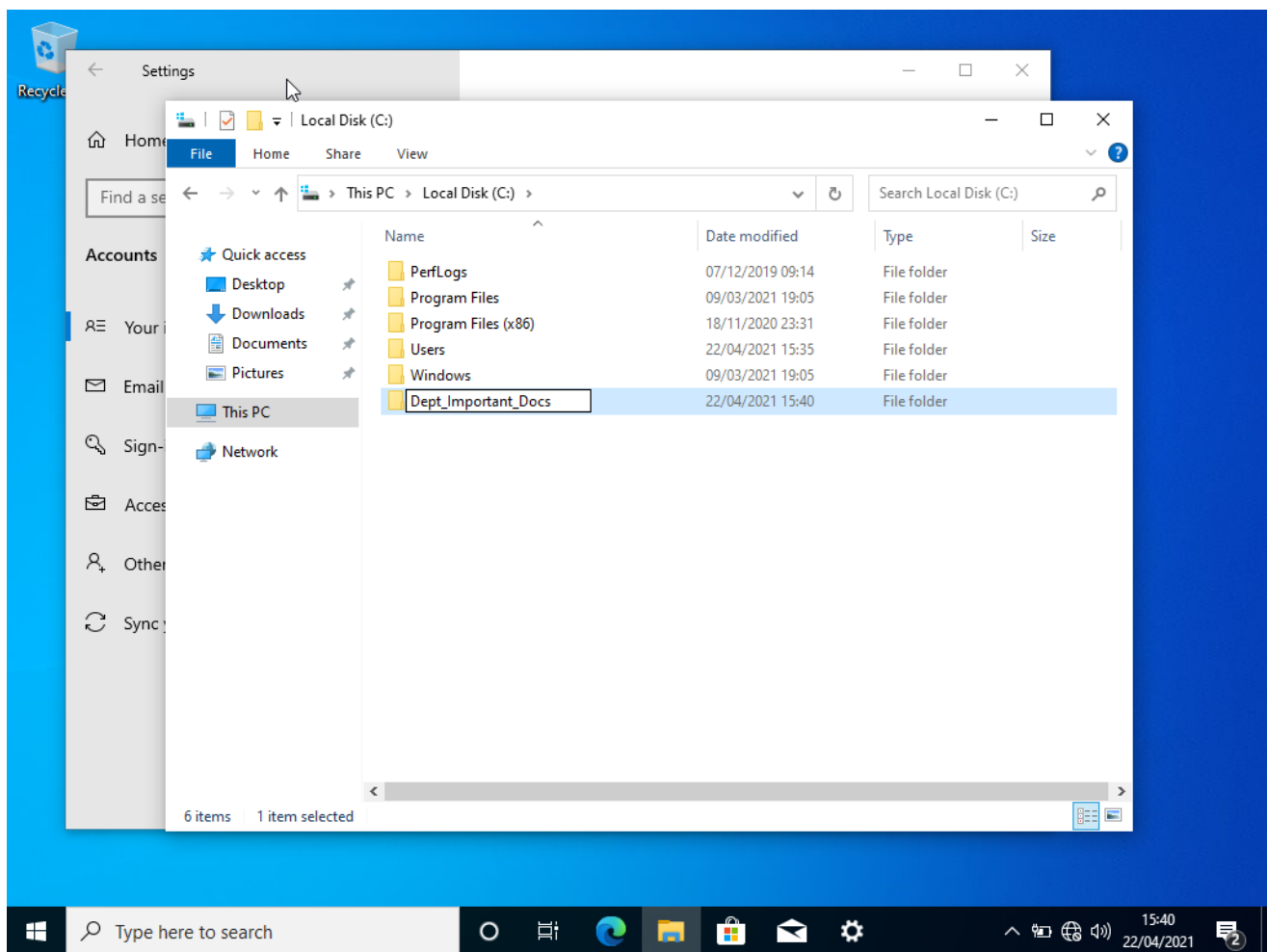
References

Task 1: Understanding NTFS & Share Permissions

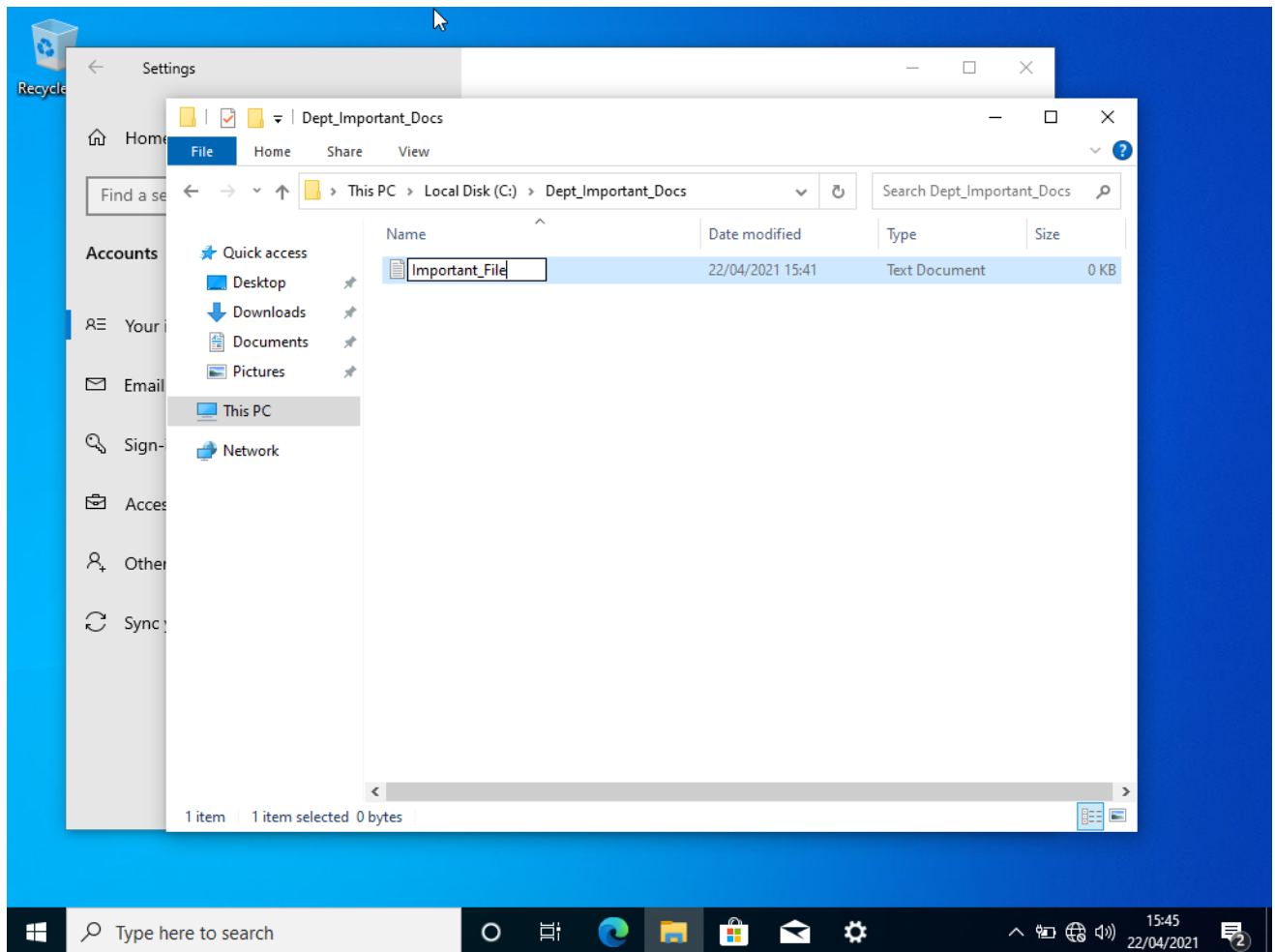
NTFS



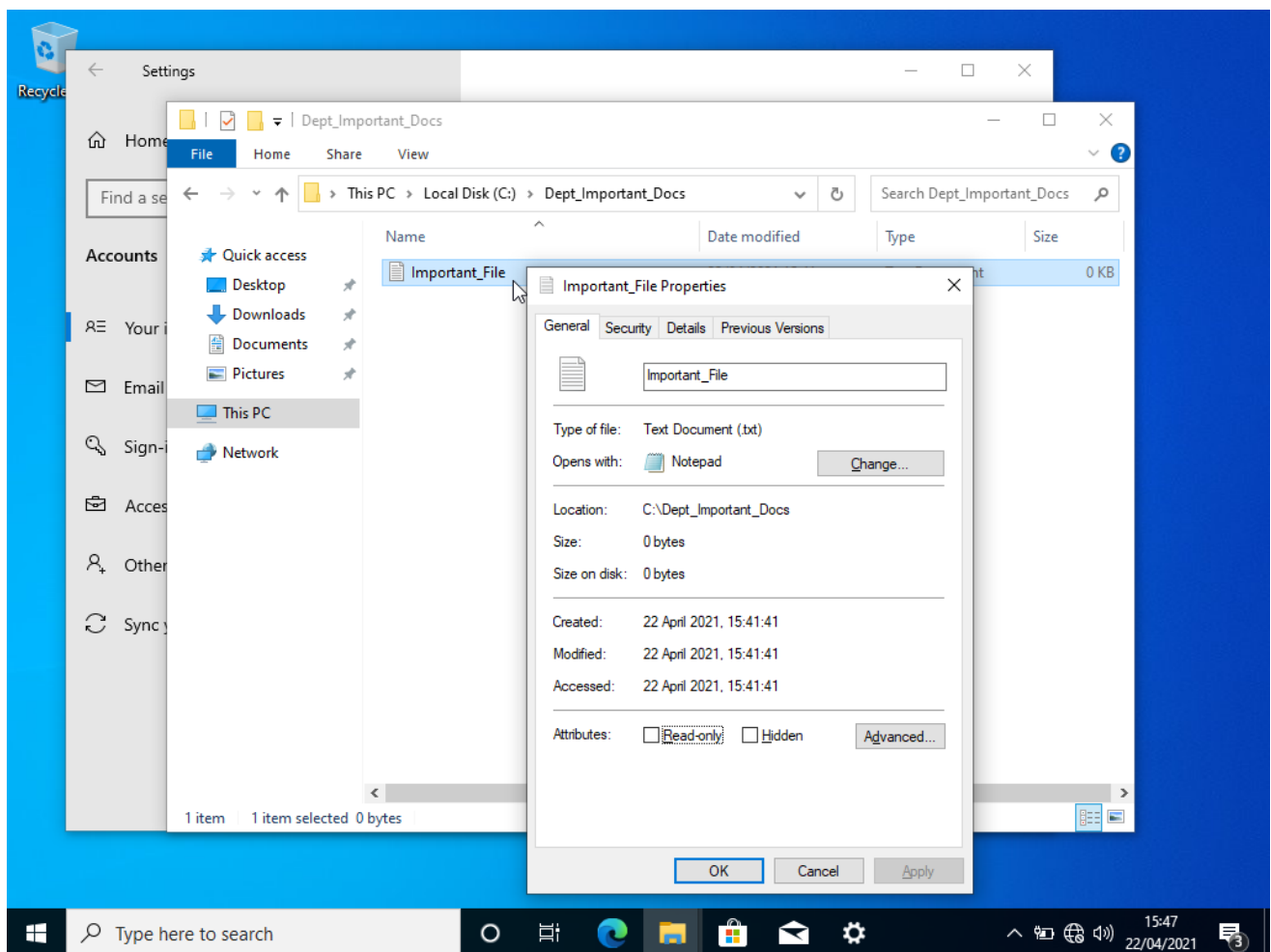
The author began by logging into the administrator account on the NWTRADERS domain via Client 1 with Server 1 running in the background.



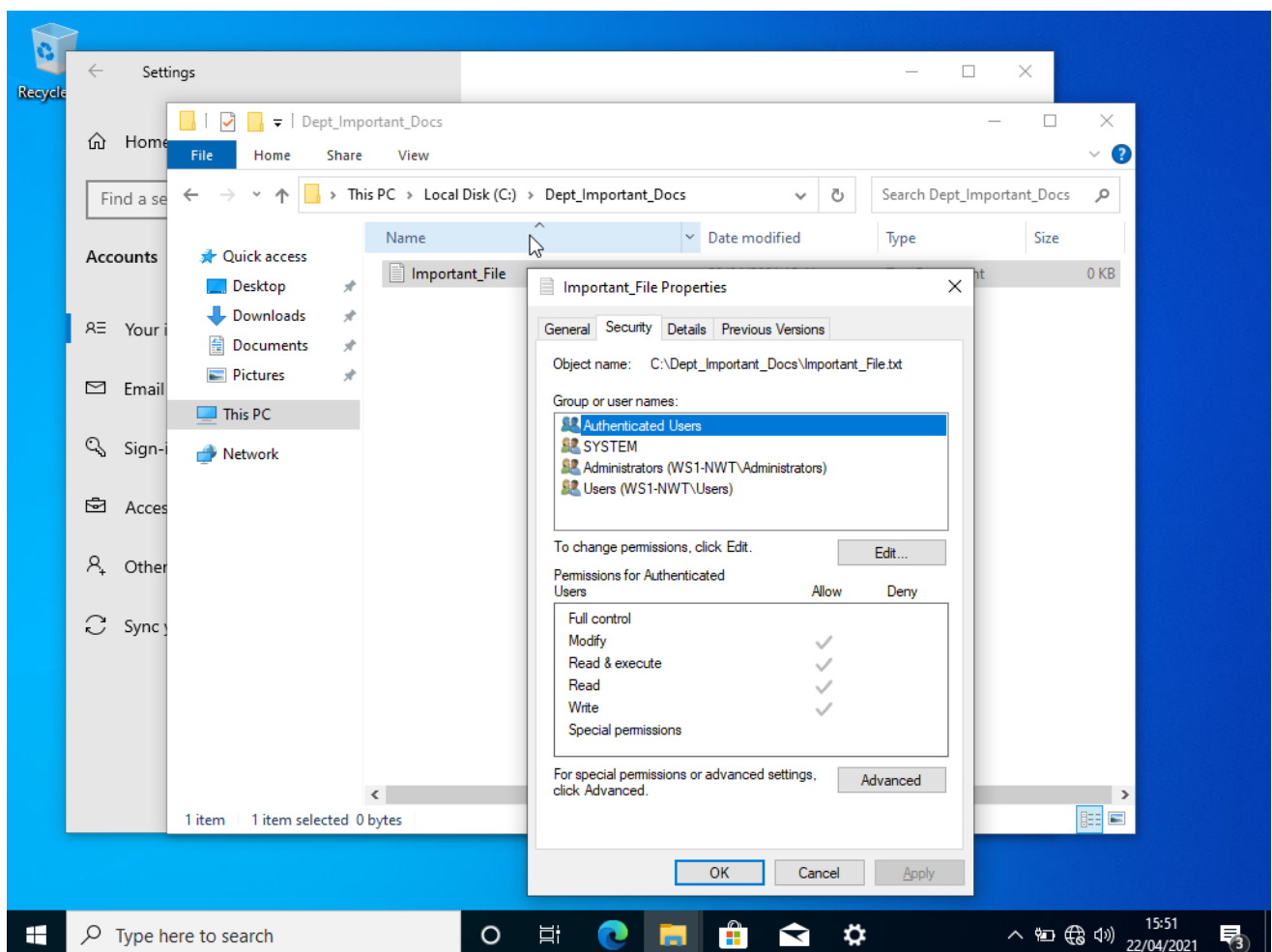
A new folder was created in the C: directory named 'Dept_Important_Docs' respectfully.



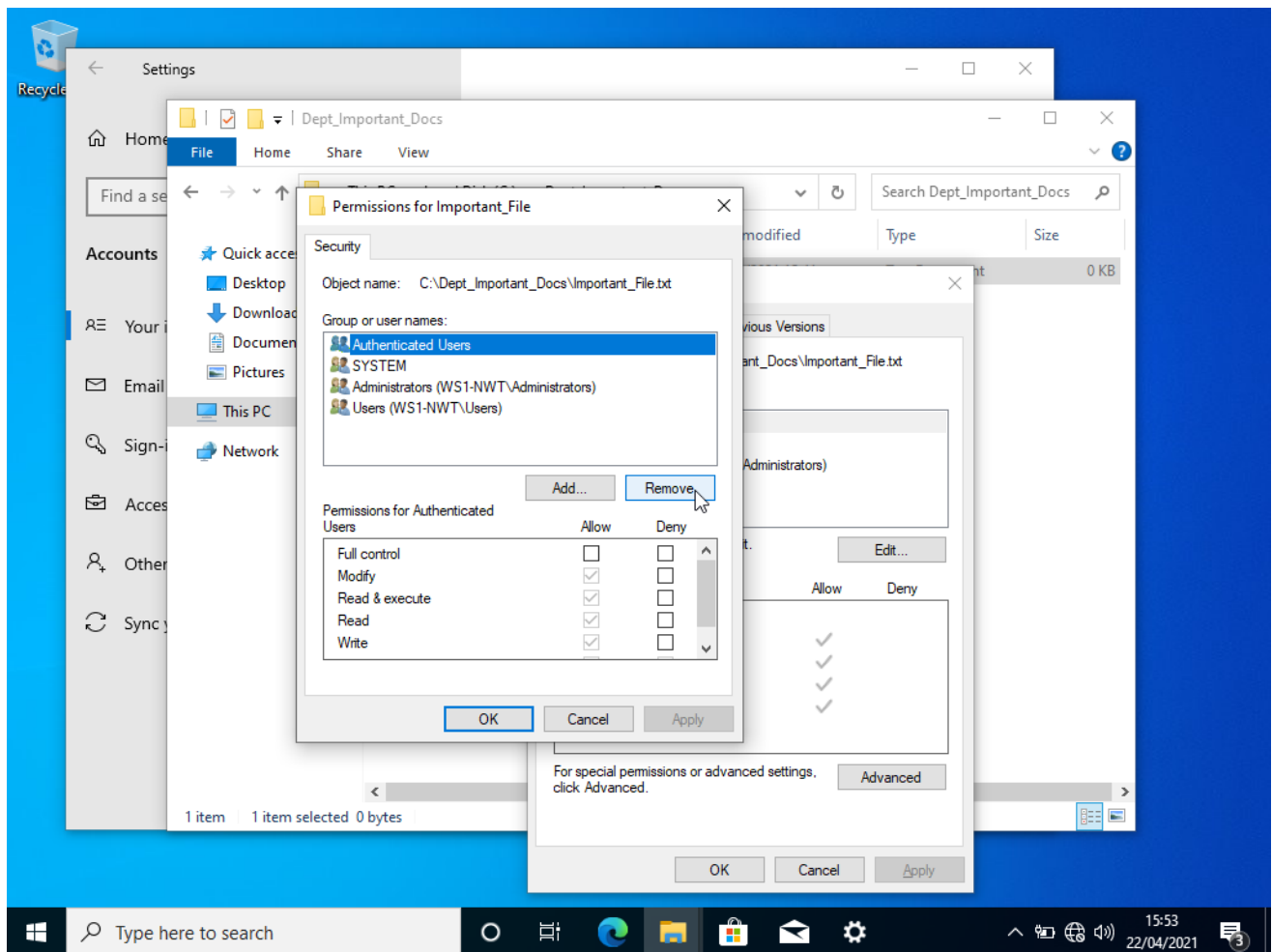
A new text document named 'Important_File' was created in the directory.



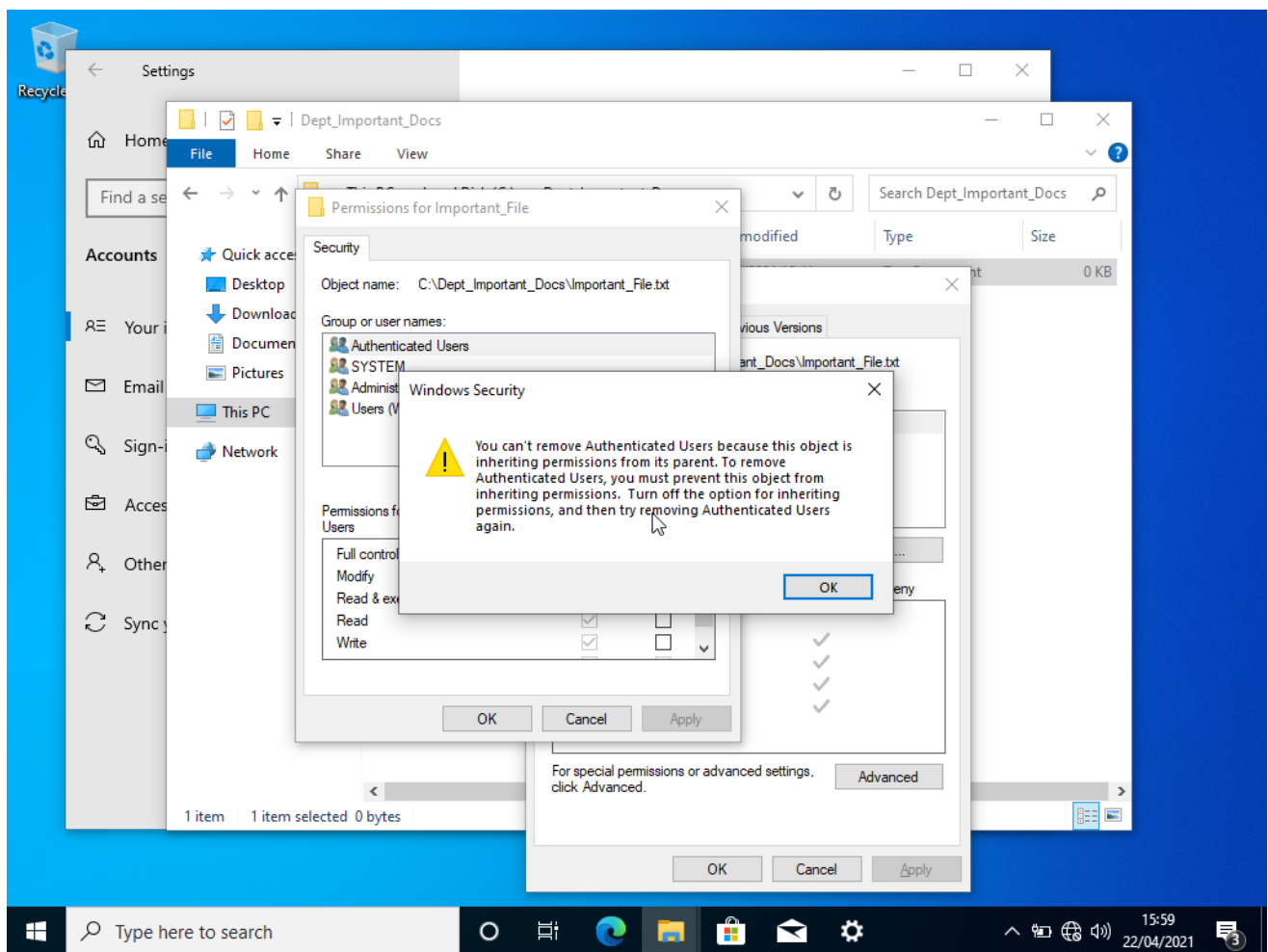
The properties window was opened for the new file accordingly.



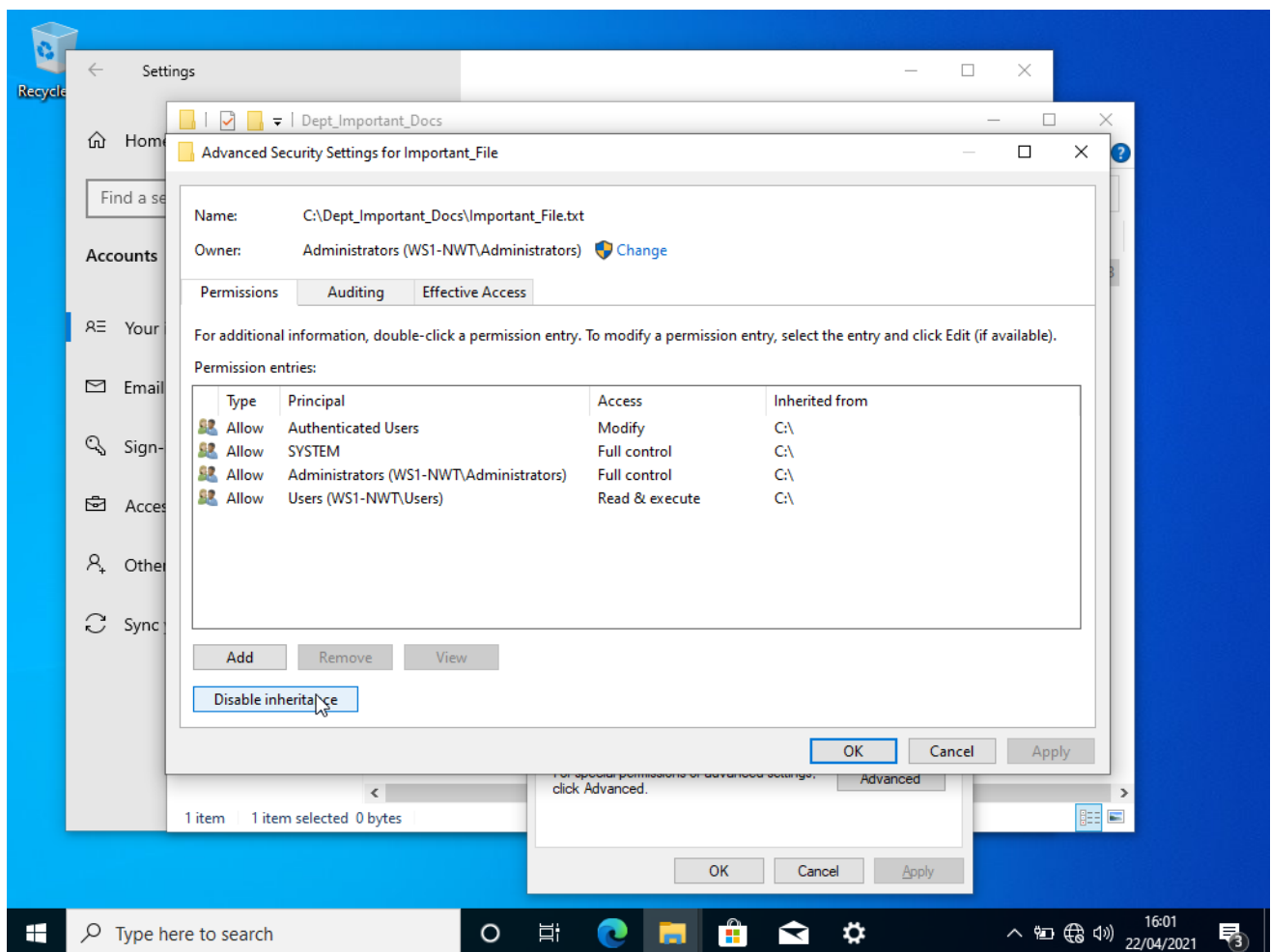
The author navigated to the security tab for the Important_File.



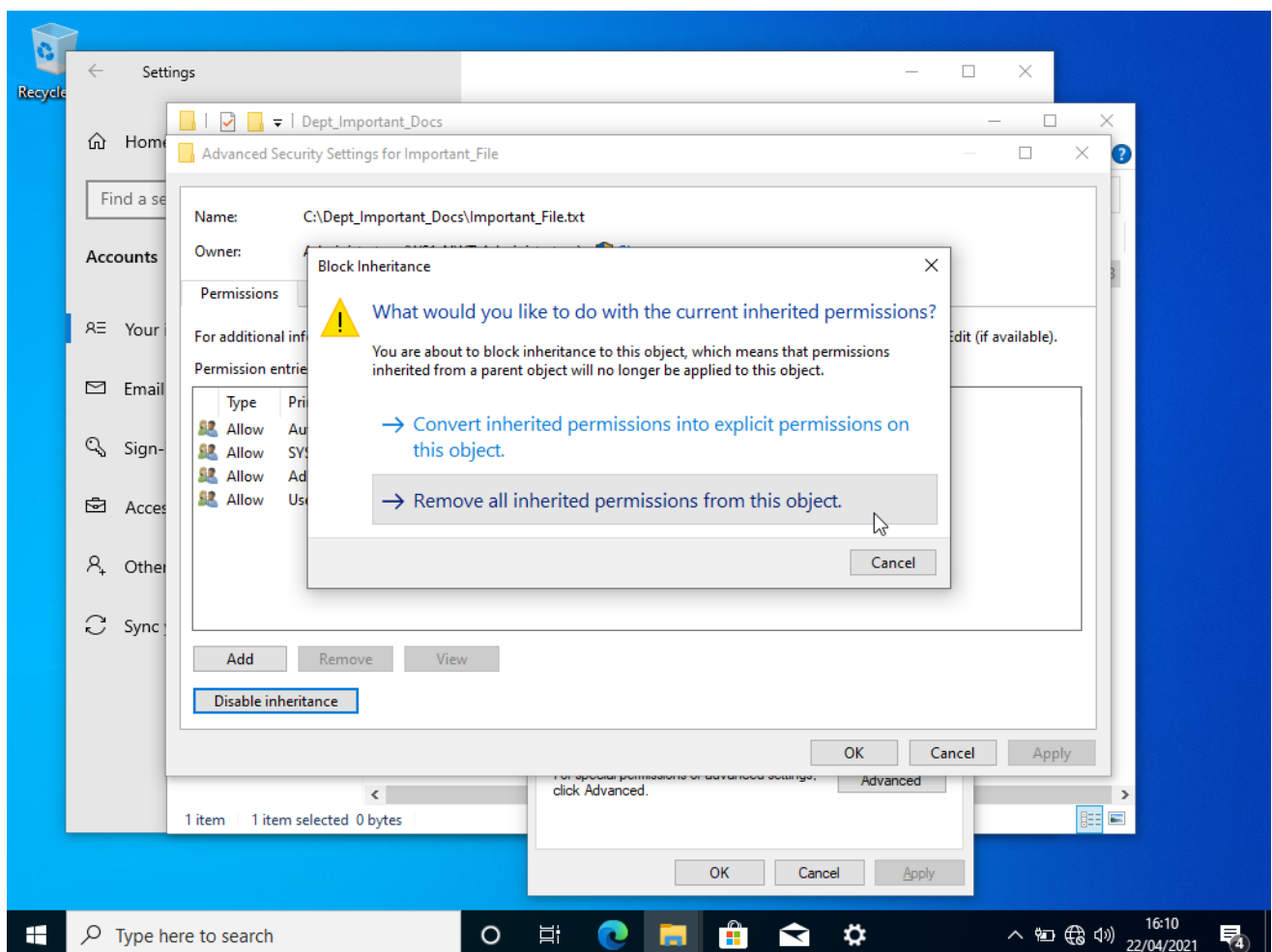
The author removed the 'Authenticated Users' group from the permissions tab.



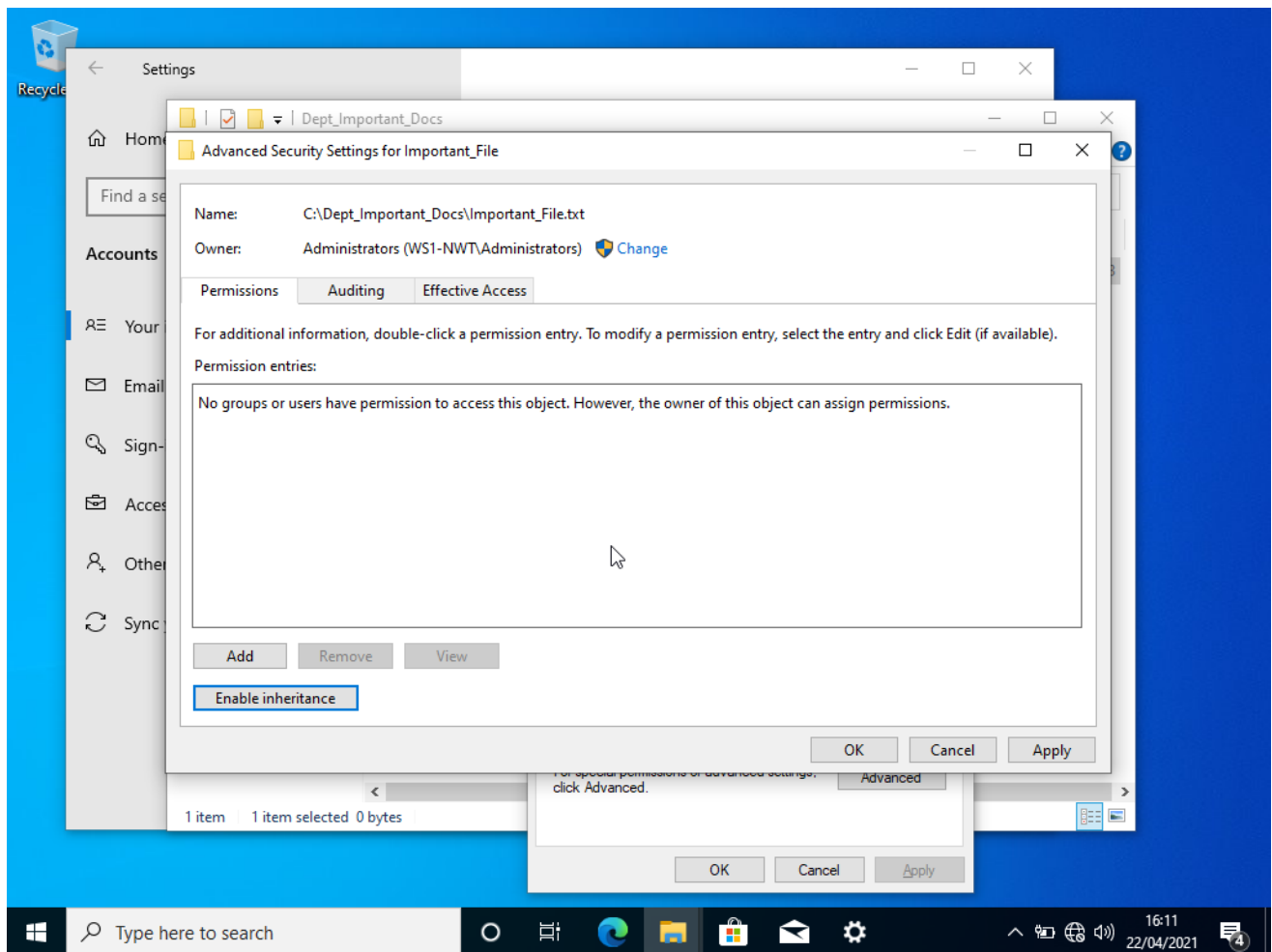
An error dialogue appears, informing the author that the permissions of this folder is currently being inherited.



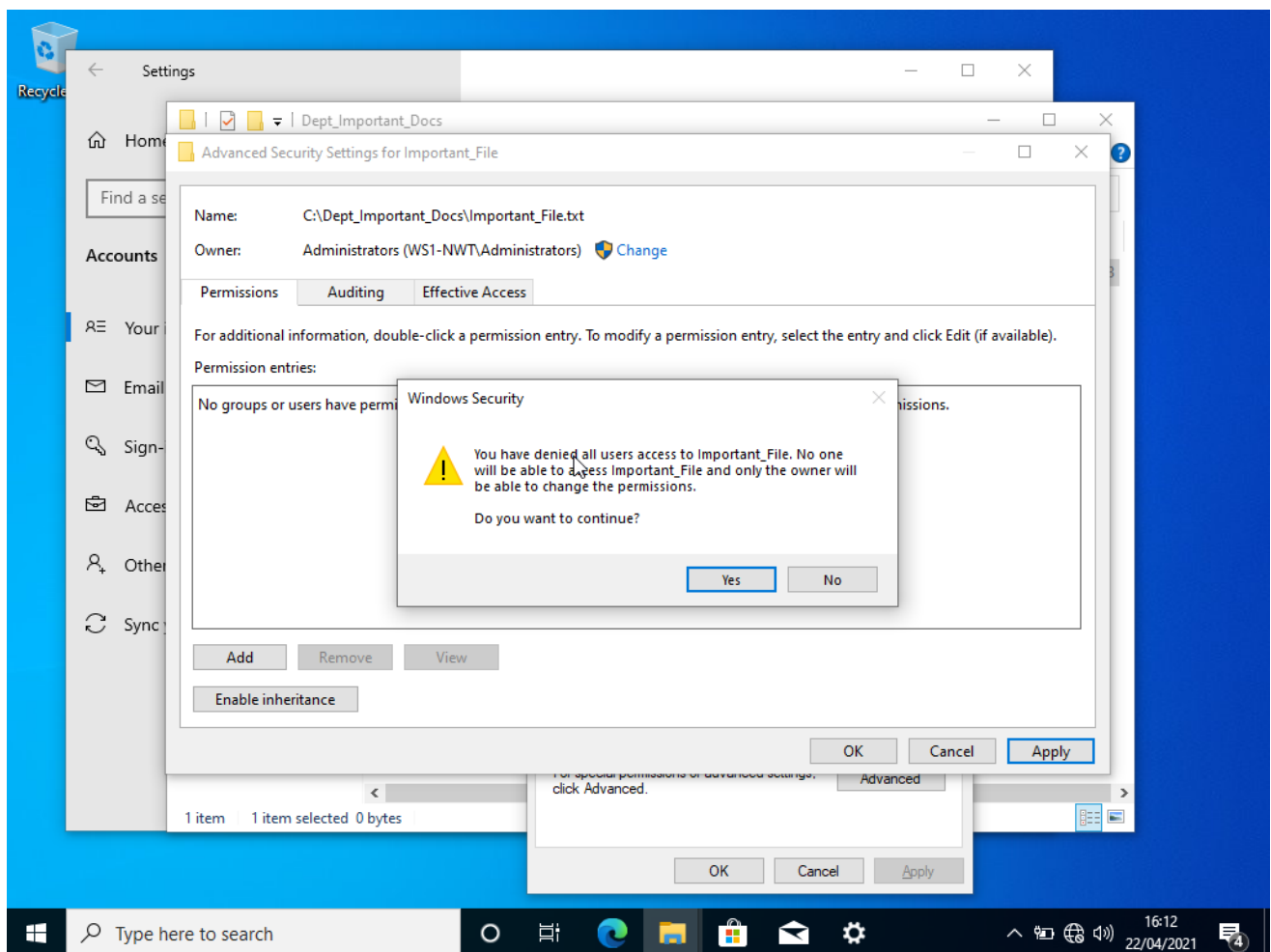
The author disabled the inheritance for this file.



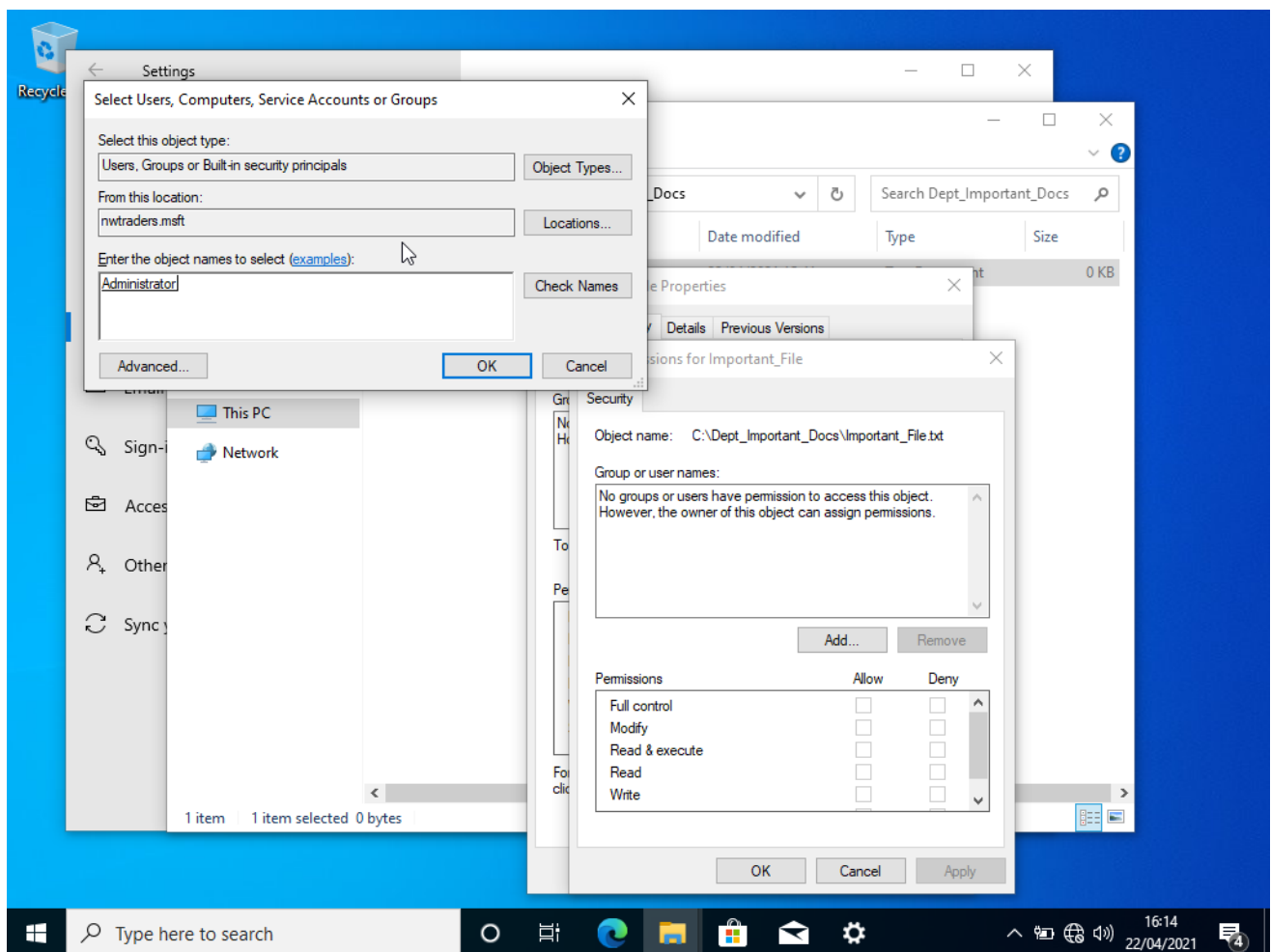
The author selected 'Remove all inherited permissions from this object.'



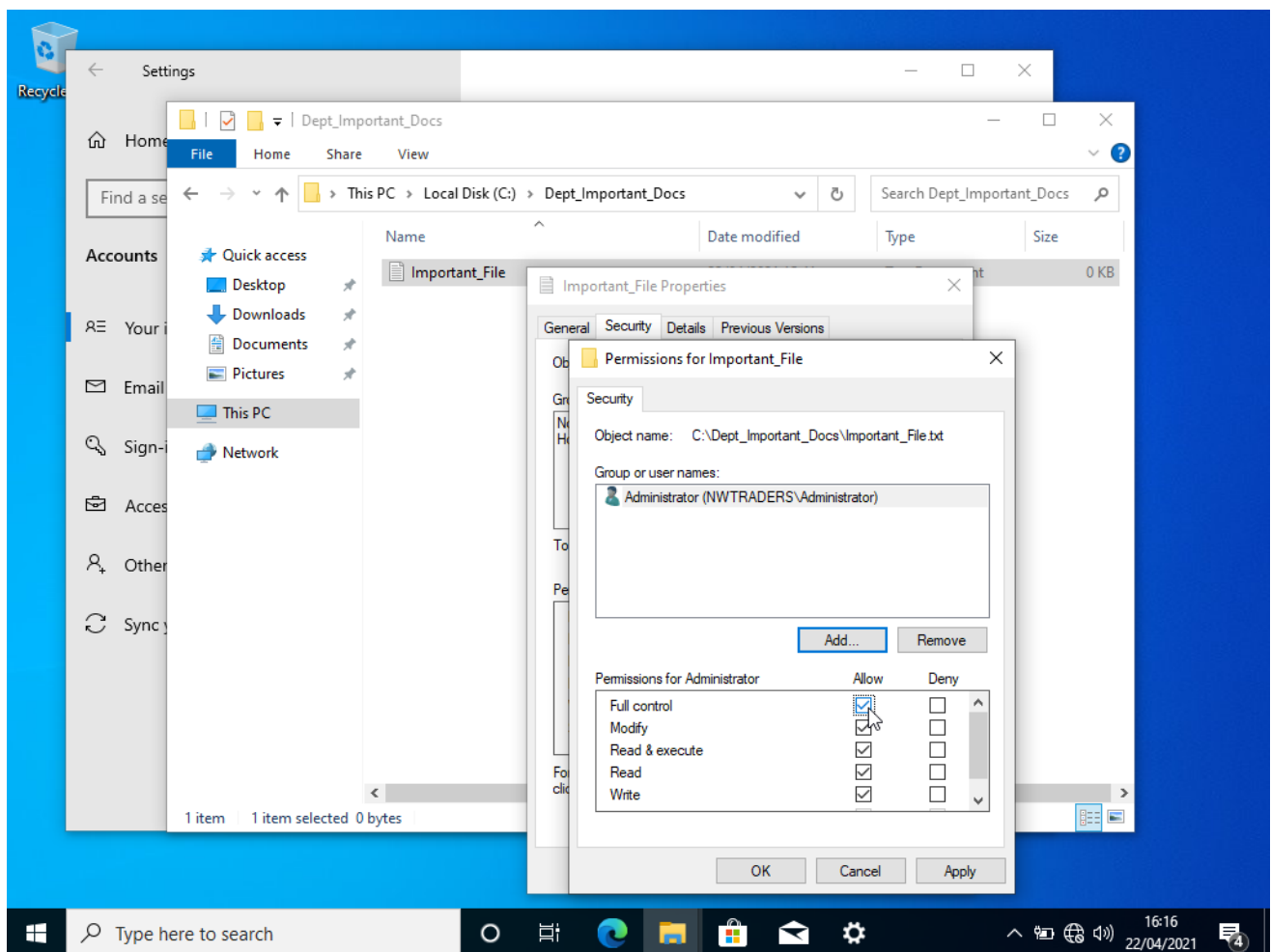
The inheritance was successfully removed.



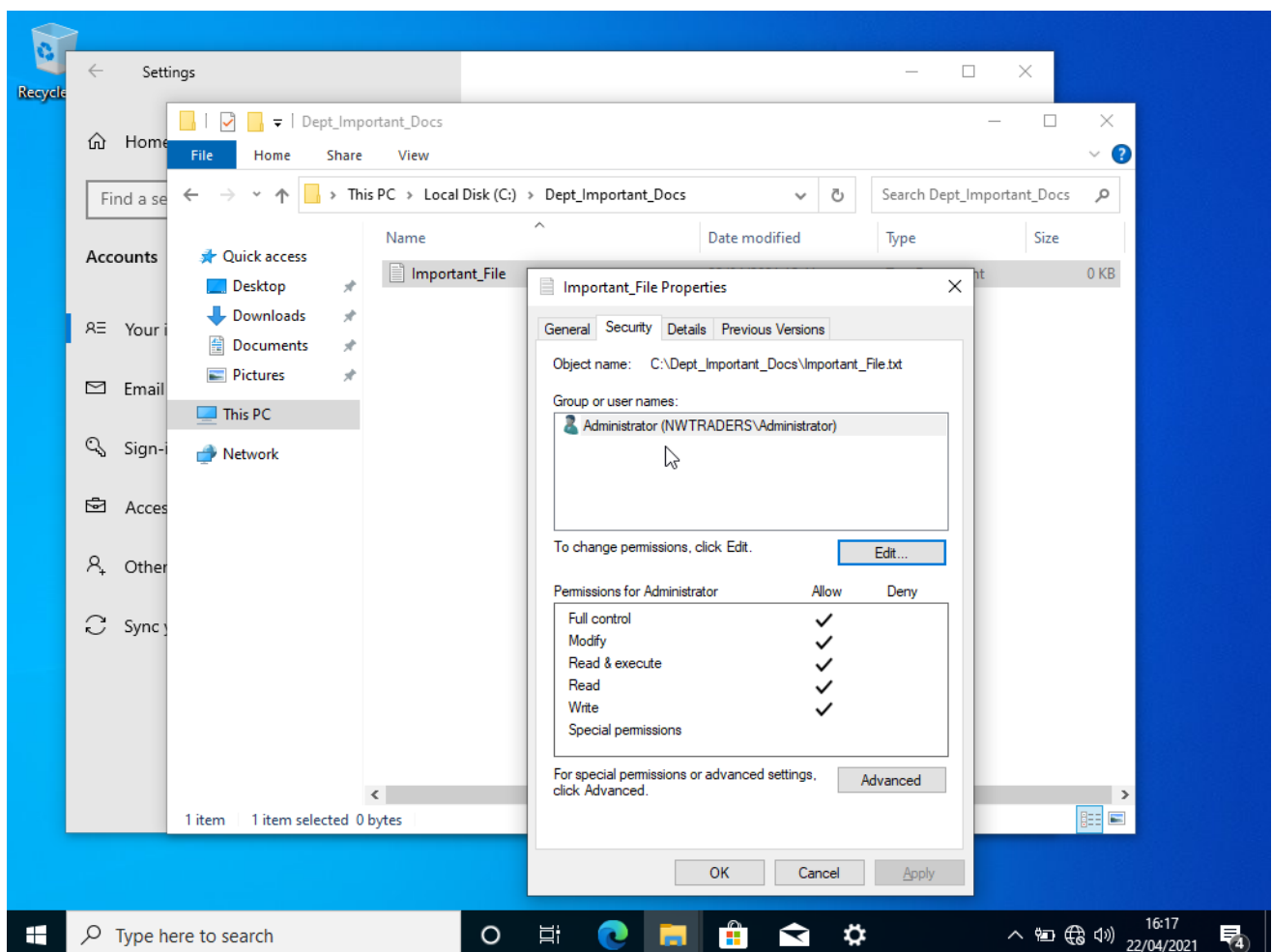
A security warning appears warning the author that the access to this file will be denied for all users except the owner. The author clicks “Yes” to confirm this dialogue.



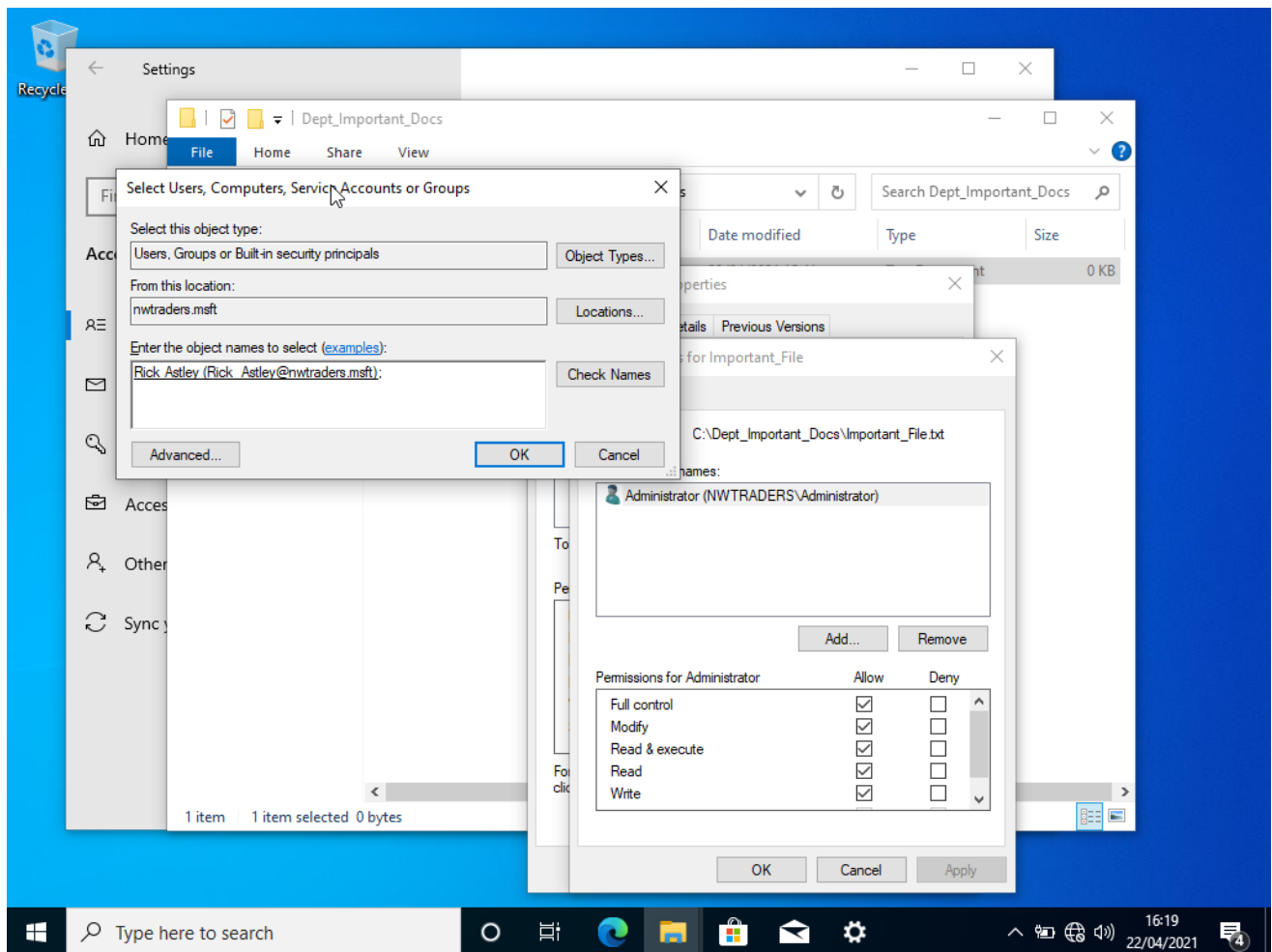
The author adds Administrator to the list of users under the permissions property for the Important_File.txt file. The author enters Administrator and presses the 'Check Names' button which underlines the administrator's account, verifying the account exists in the namespace.



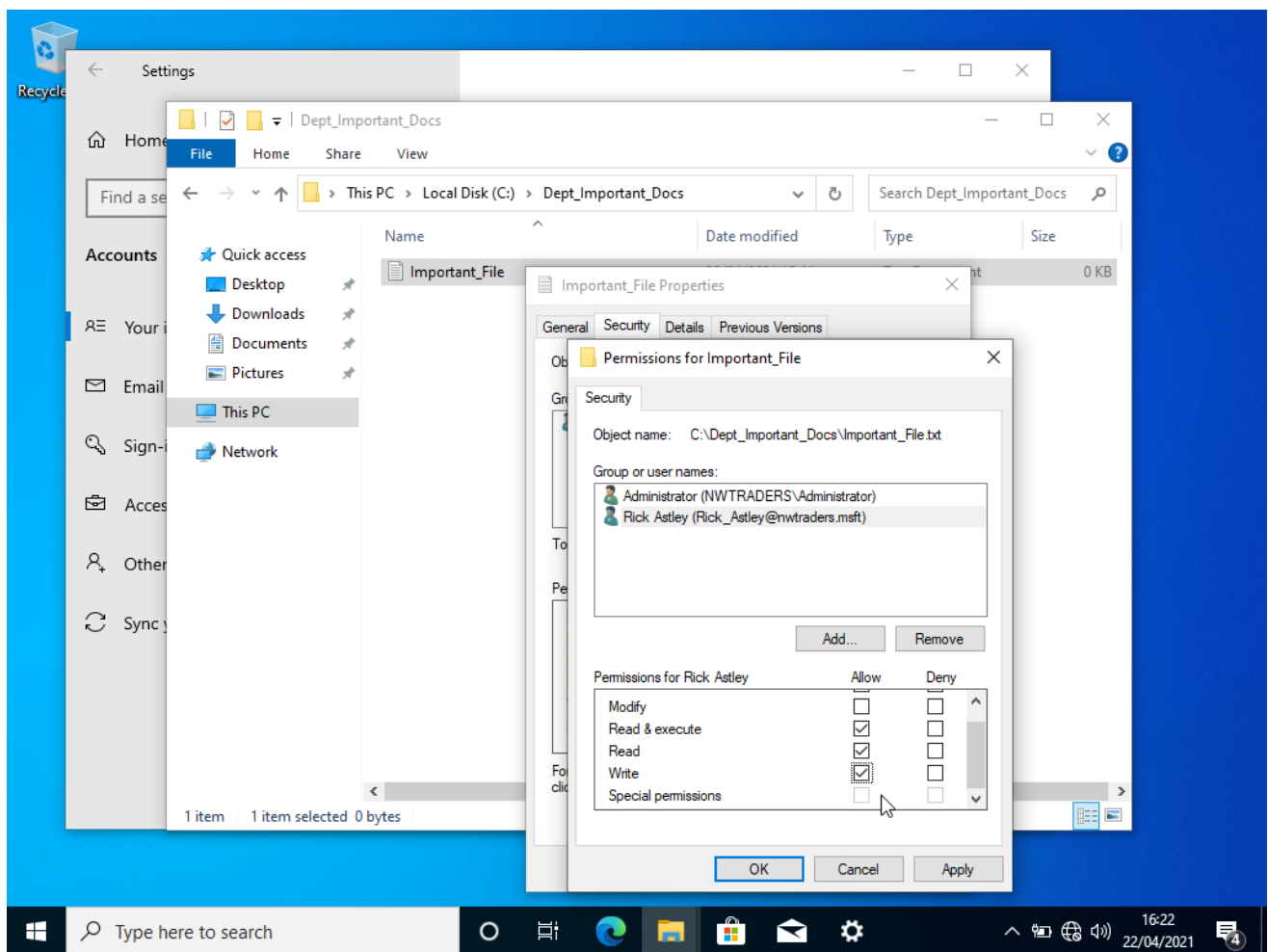
The author gives the Administrator full control over the file itself.



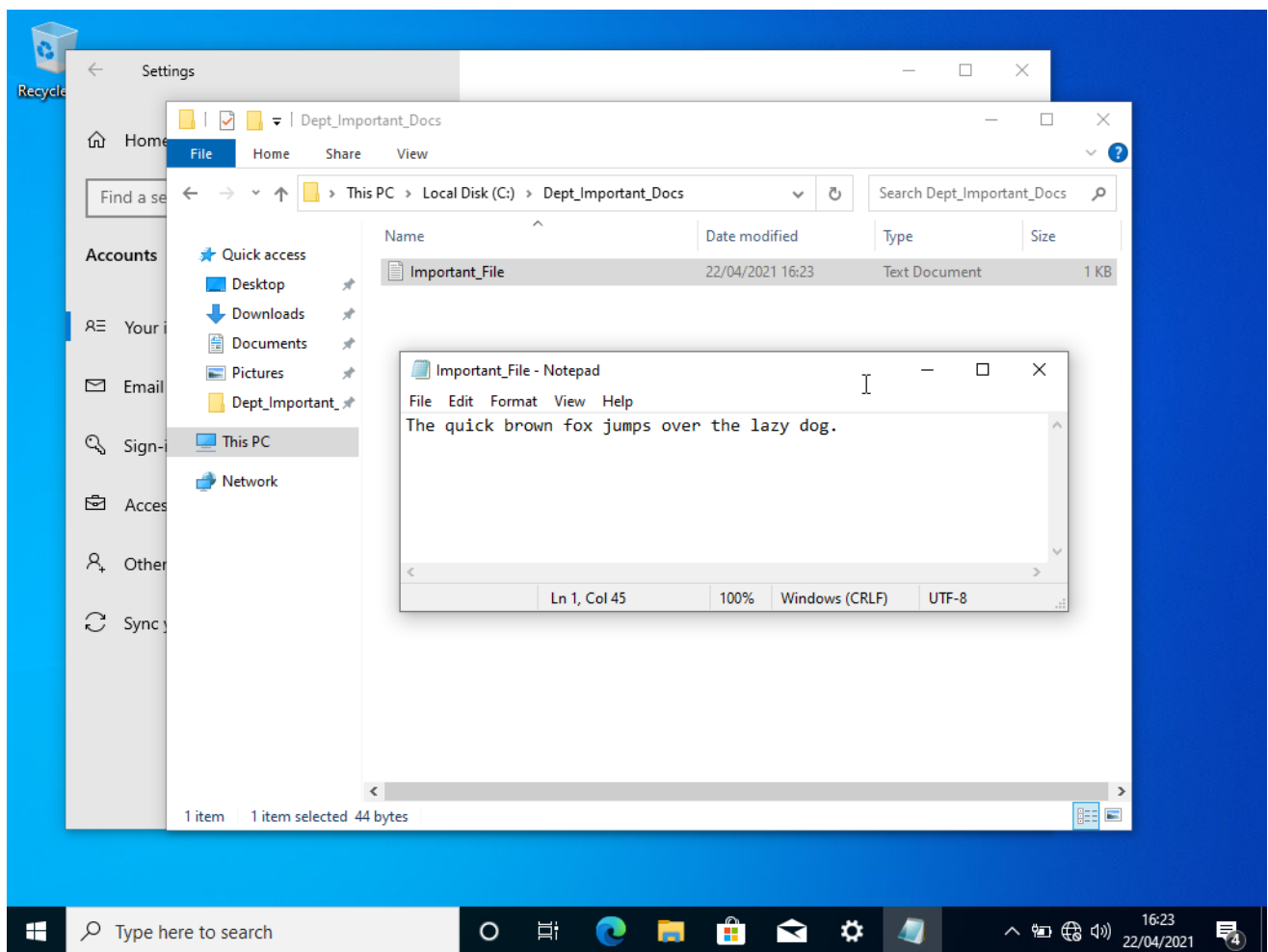
The permission is given successfully.



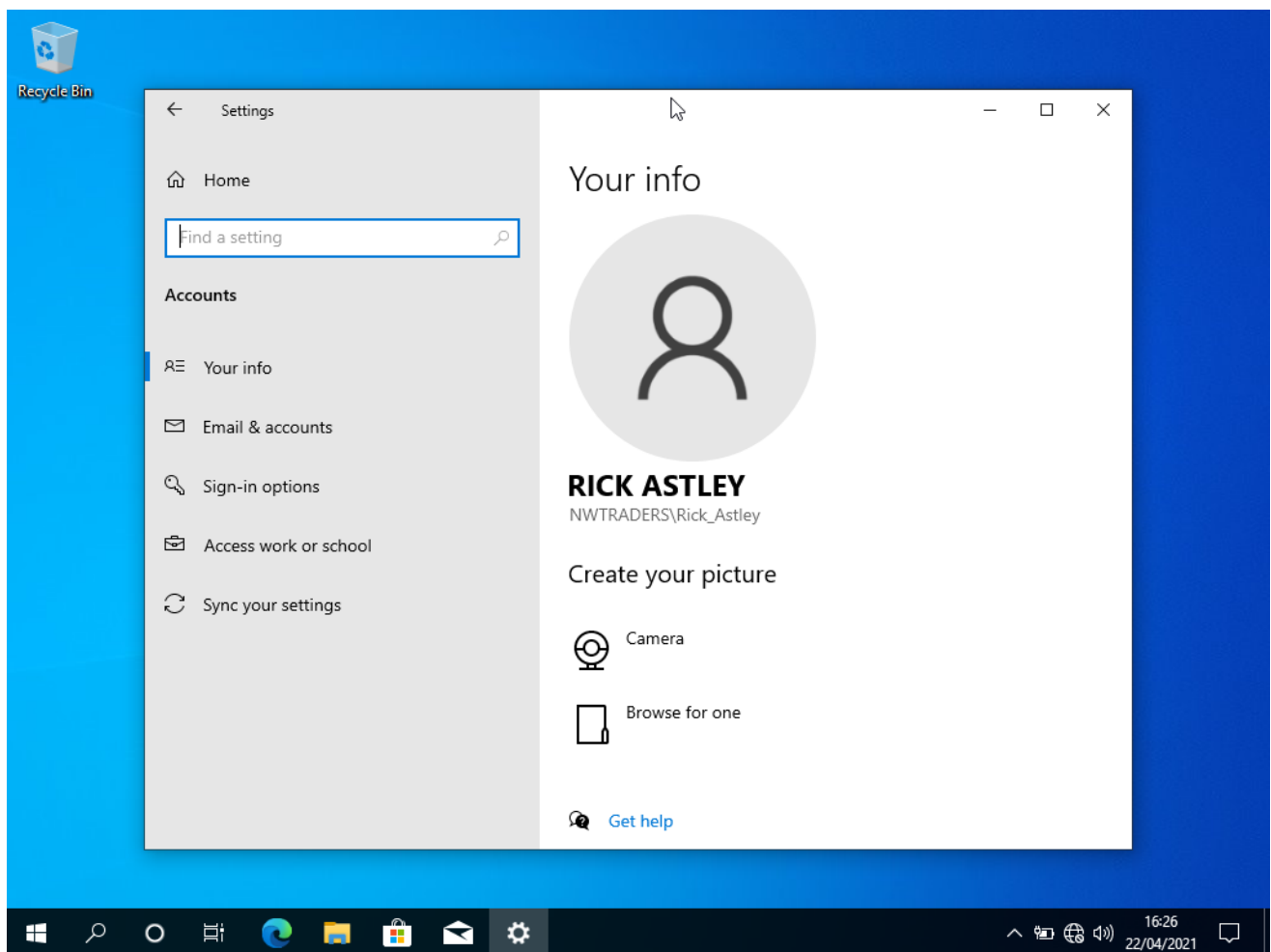
Rick Astley (The secondary example account) is added to the permissions list.



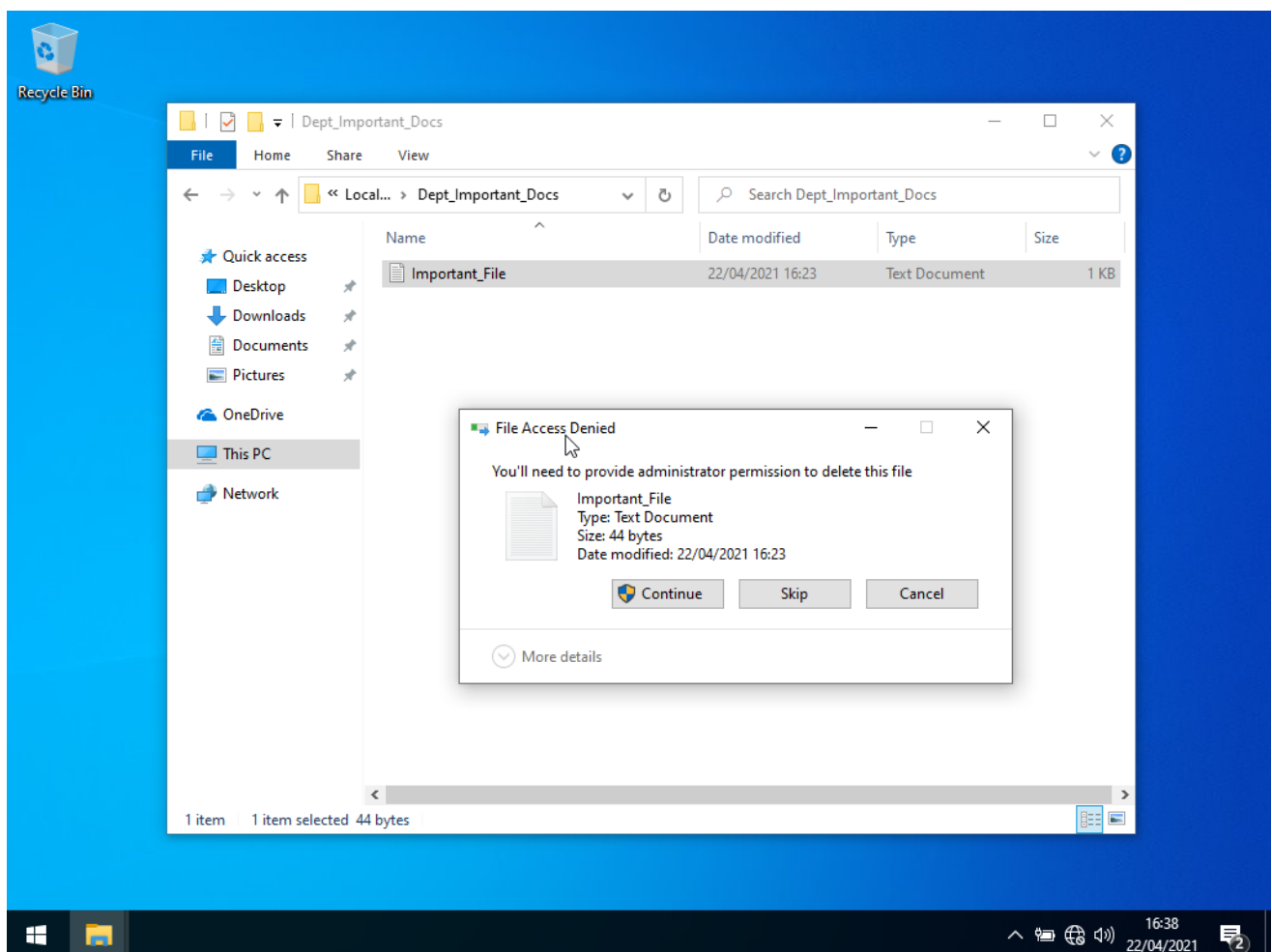
Rick Astley is given permission to Read & Execute, Read and Write but not permission to modify or full control.



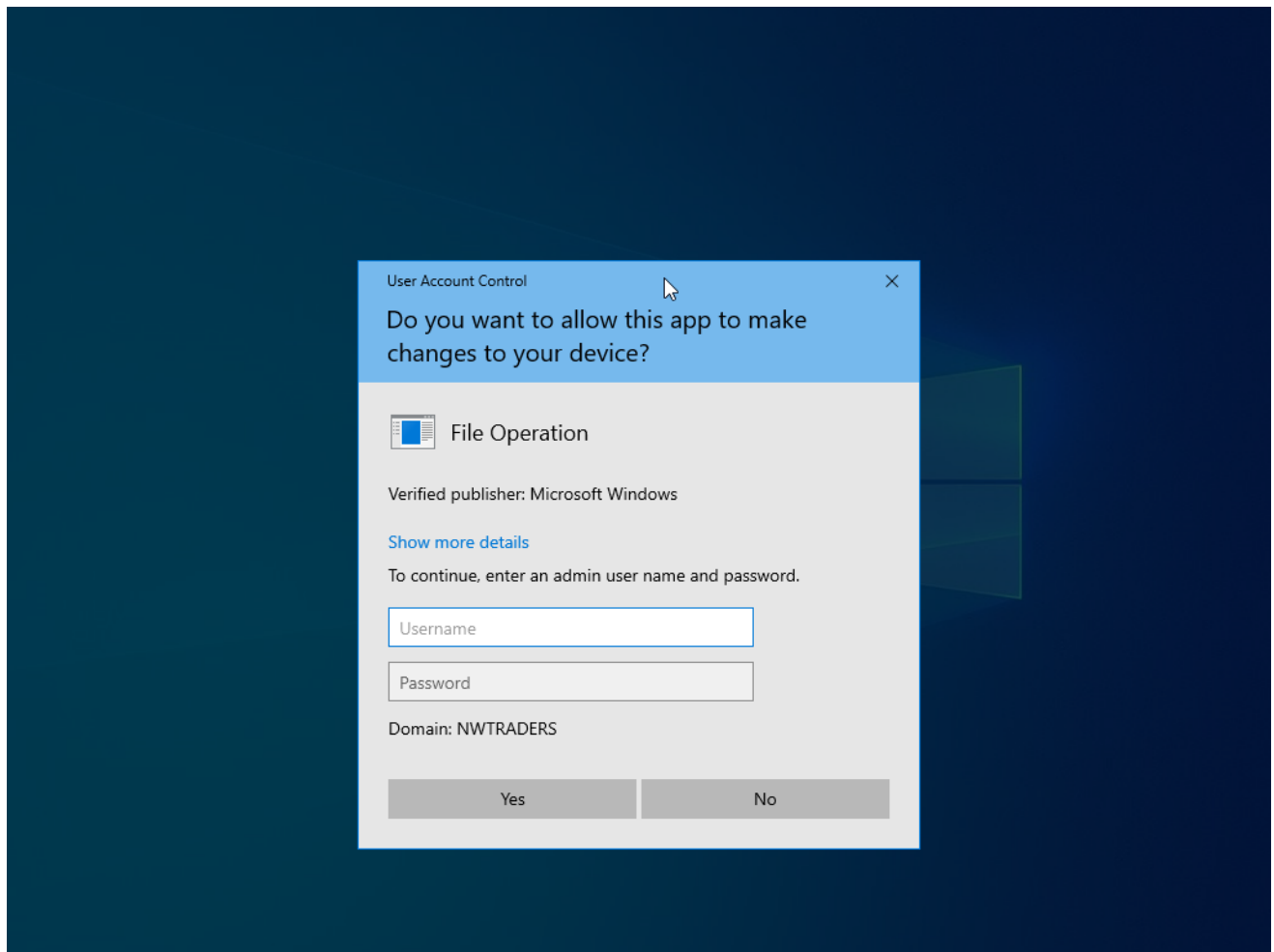
The administrator is allowed to edit the text of the document itself and insert the phrase “The quick brown fox jumps over the lazy dog.”



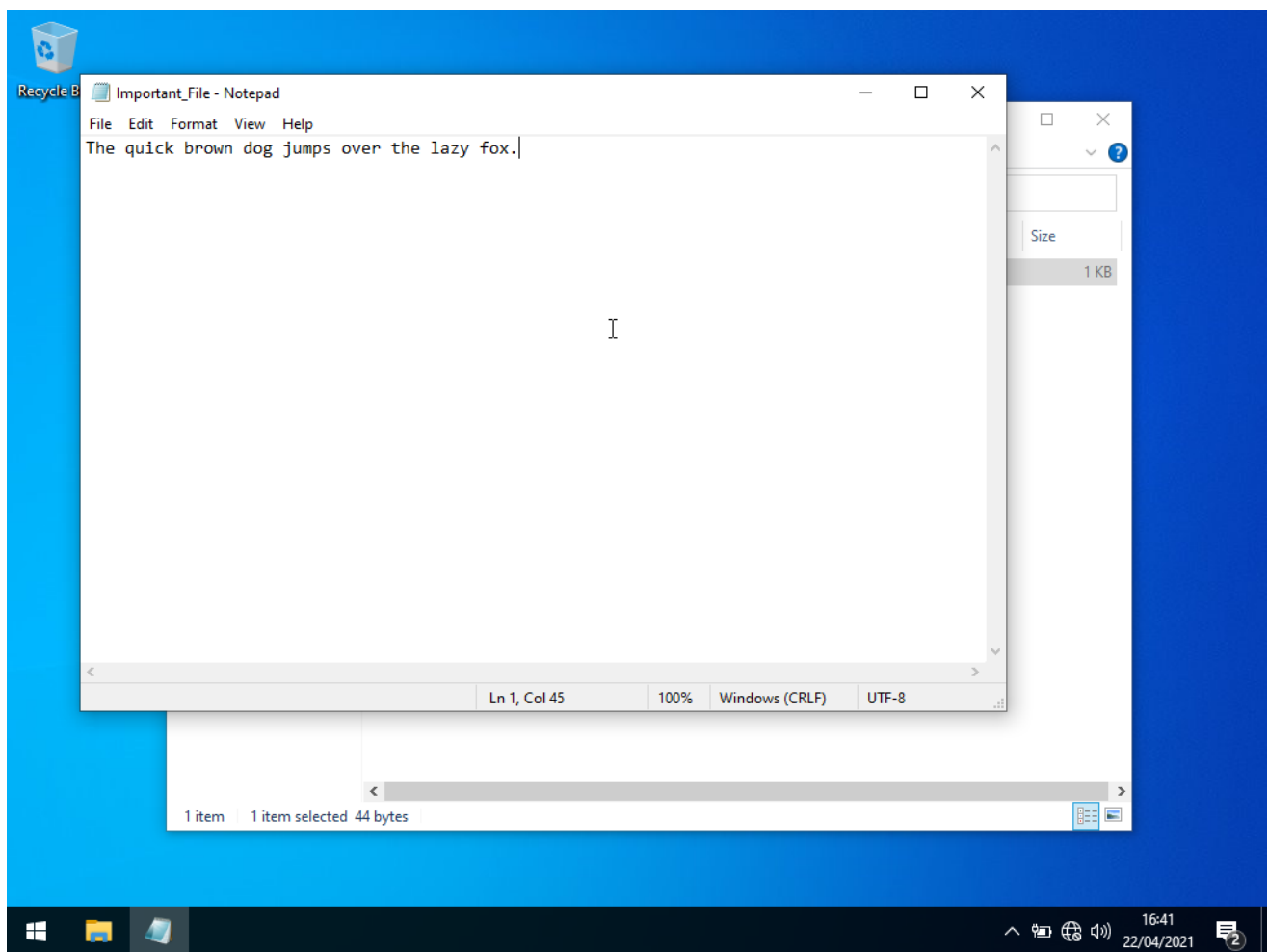
The author switched users to Rick Astley.



In an attempt to delete the file as Rick Astley, A 'File Access Denied' dialogue appeared.

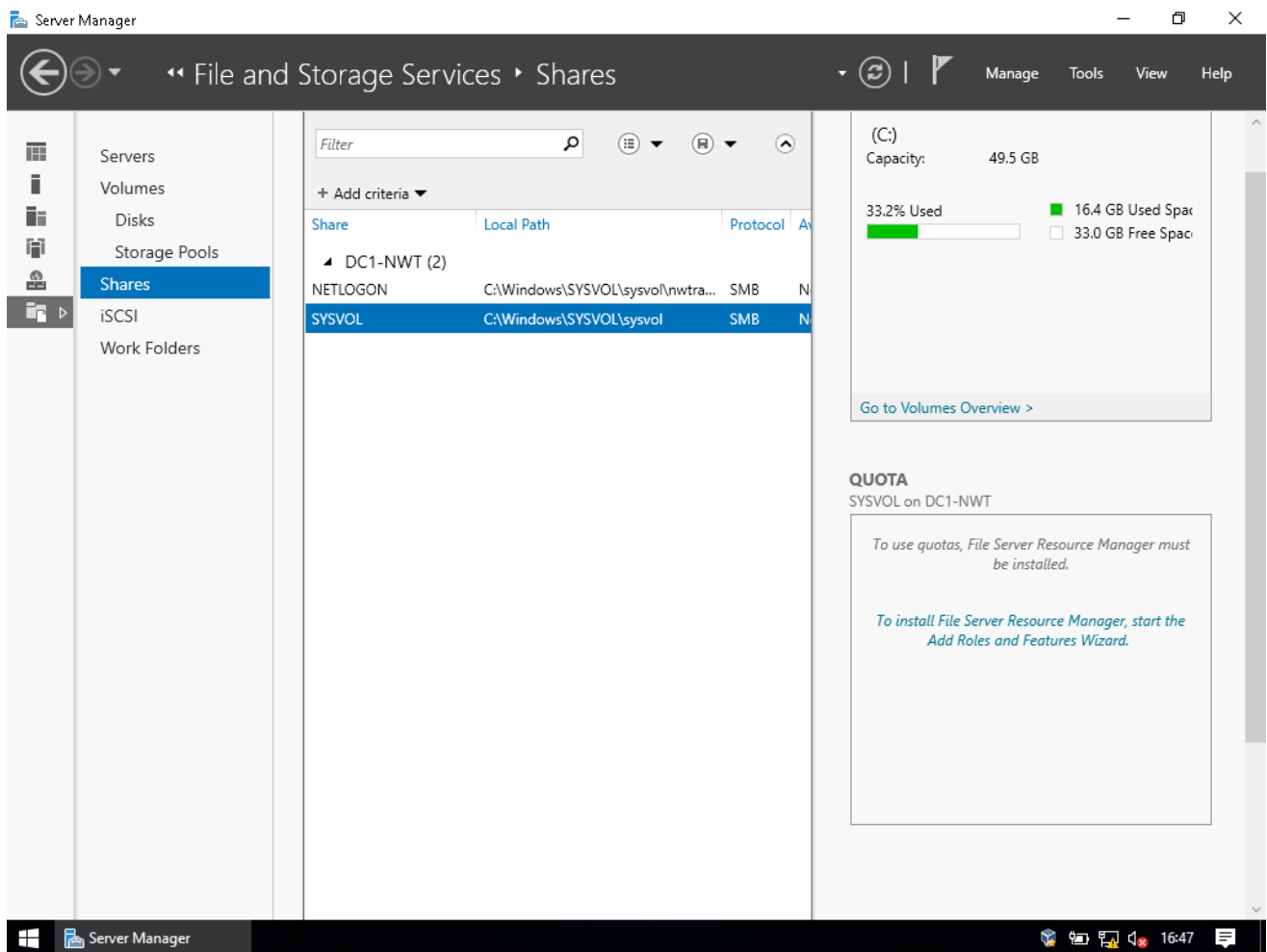


In order to delete the file, the user would need to provide administrative details first.

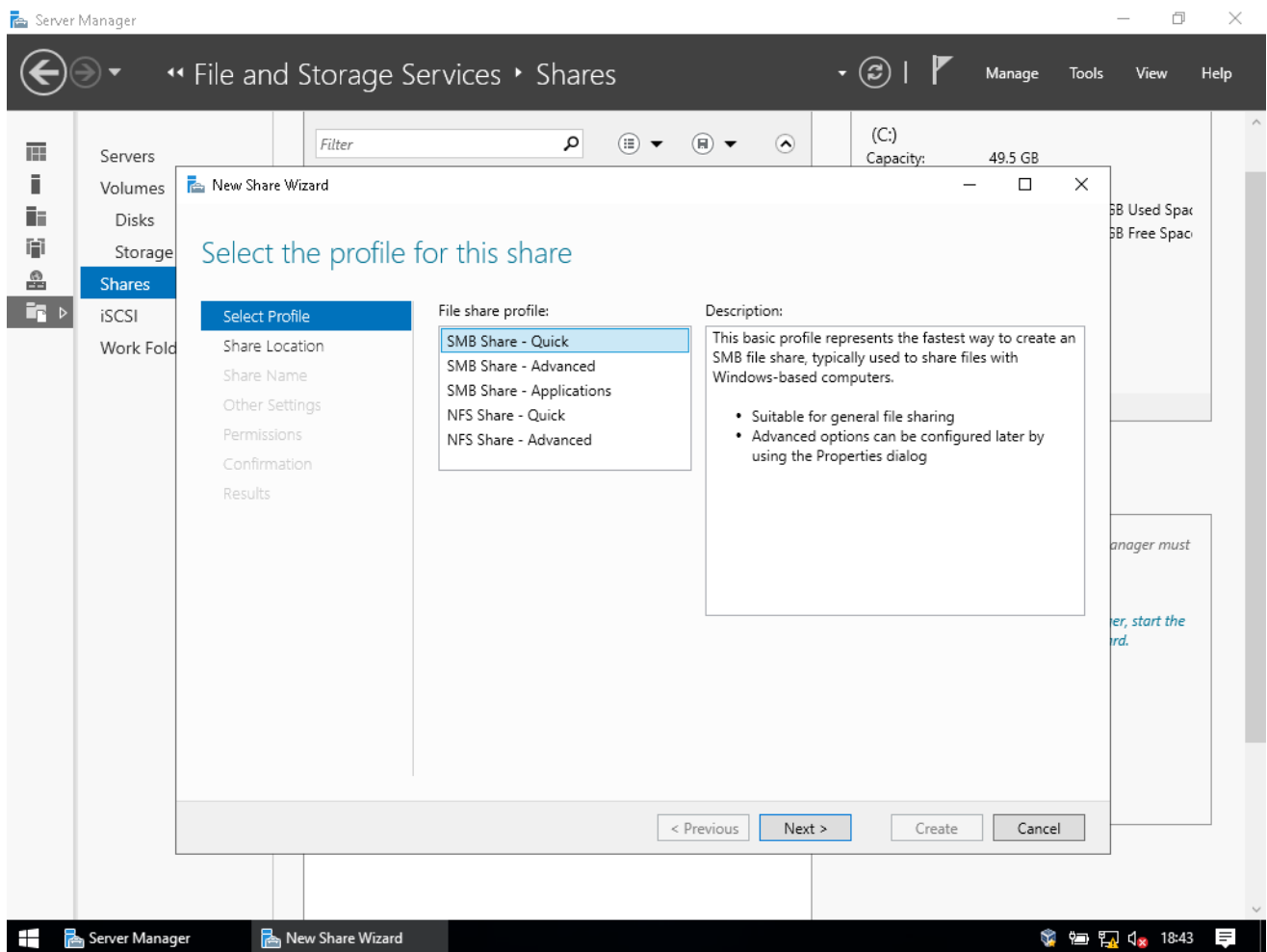


The file itself however can still be edited and saved.

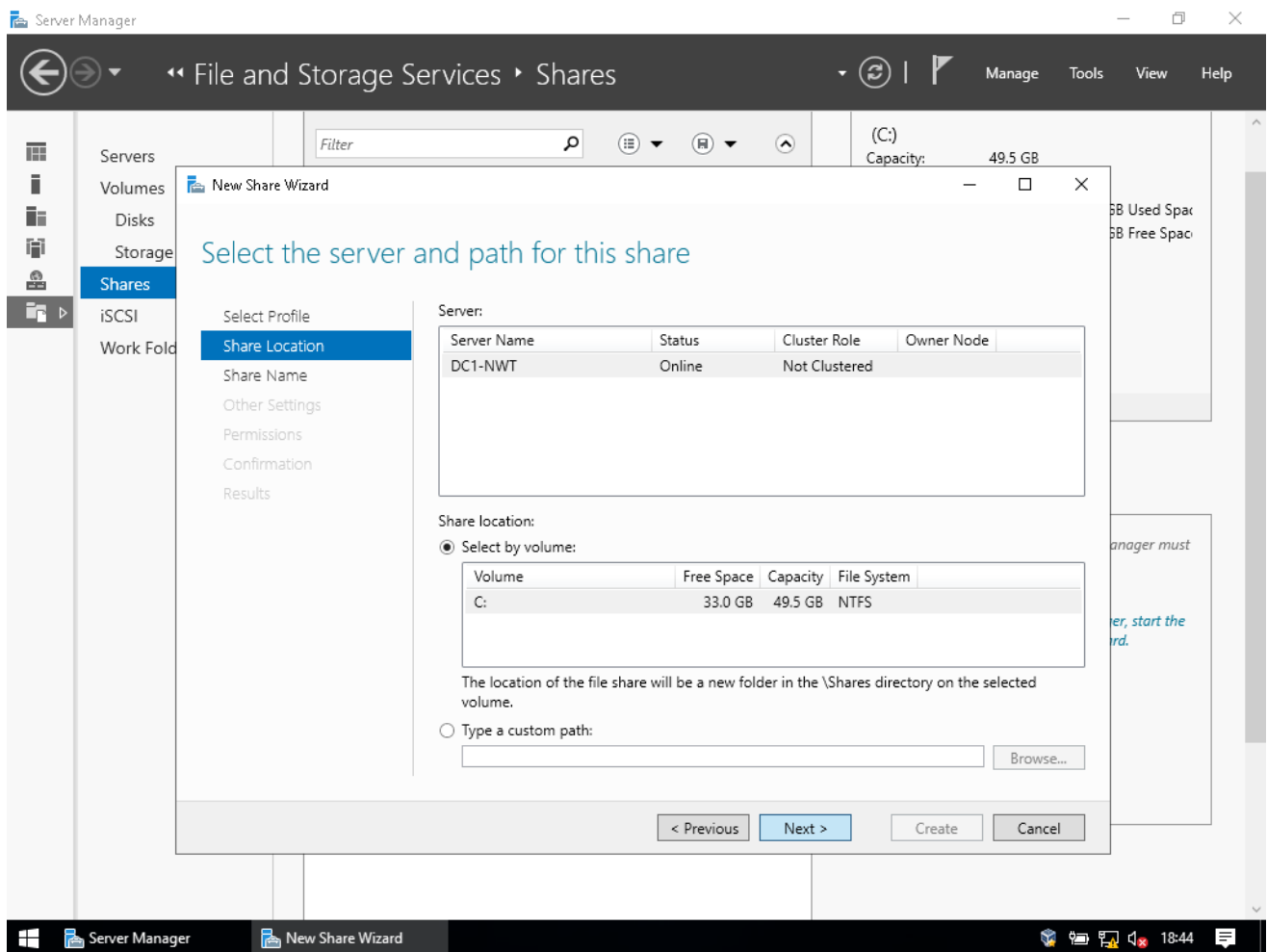
Share



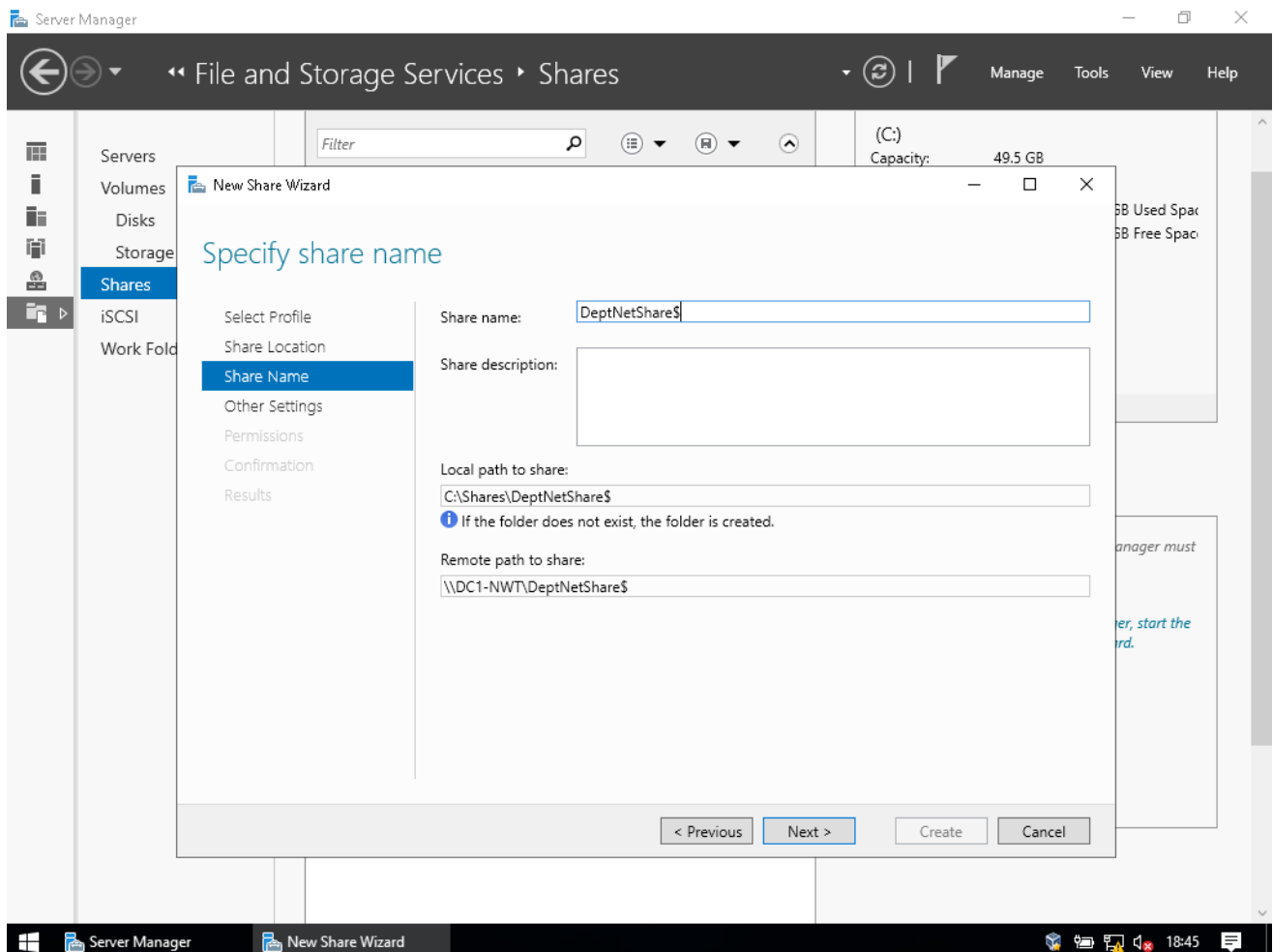
On Server 1, the author opens the Server Manager and navigates to the 'Shares' section.



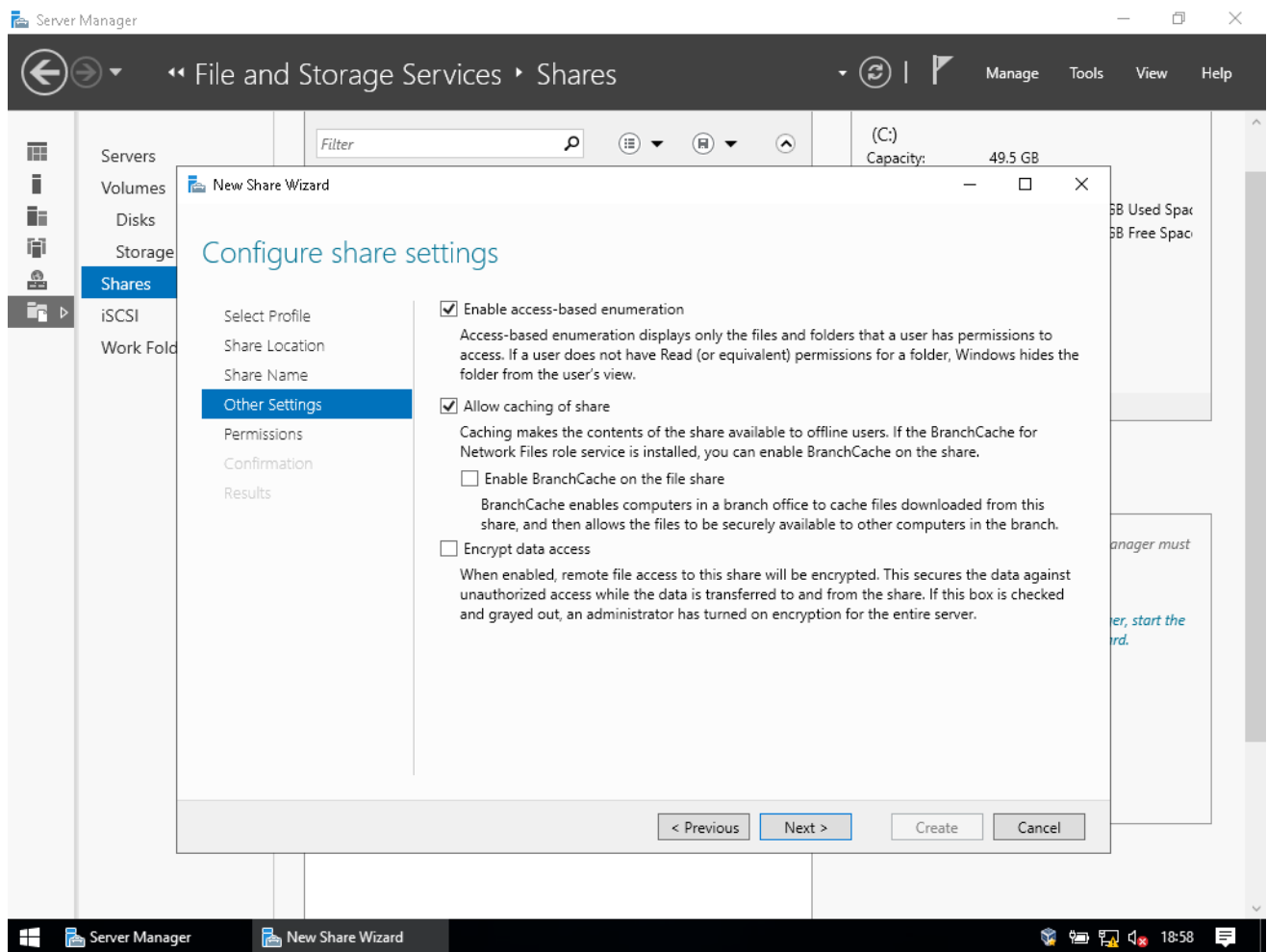
The author begins to create a new share and is greeted with the new share wizard. The 'SMB Share - Quick' option is selected by the author.



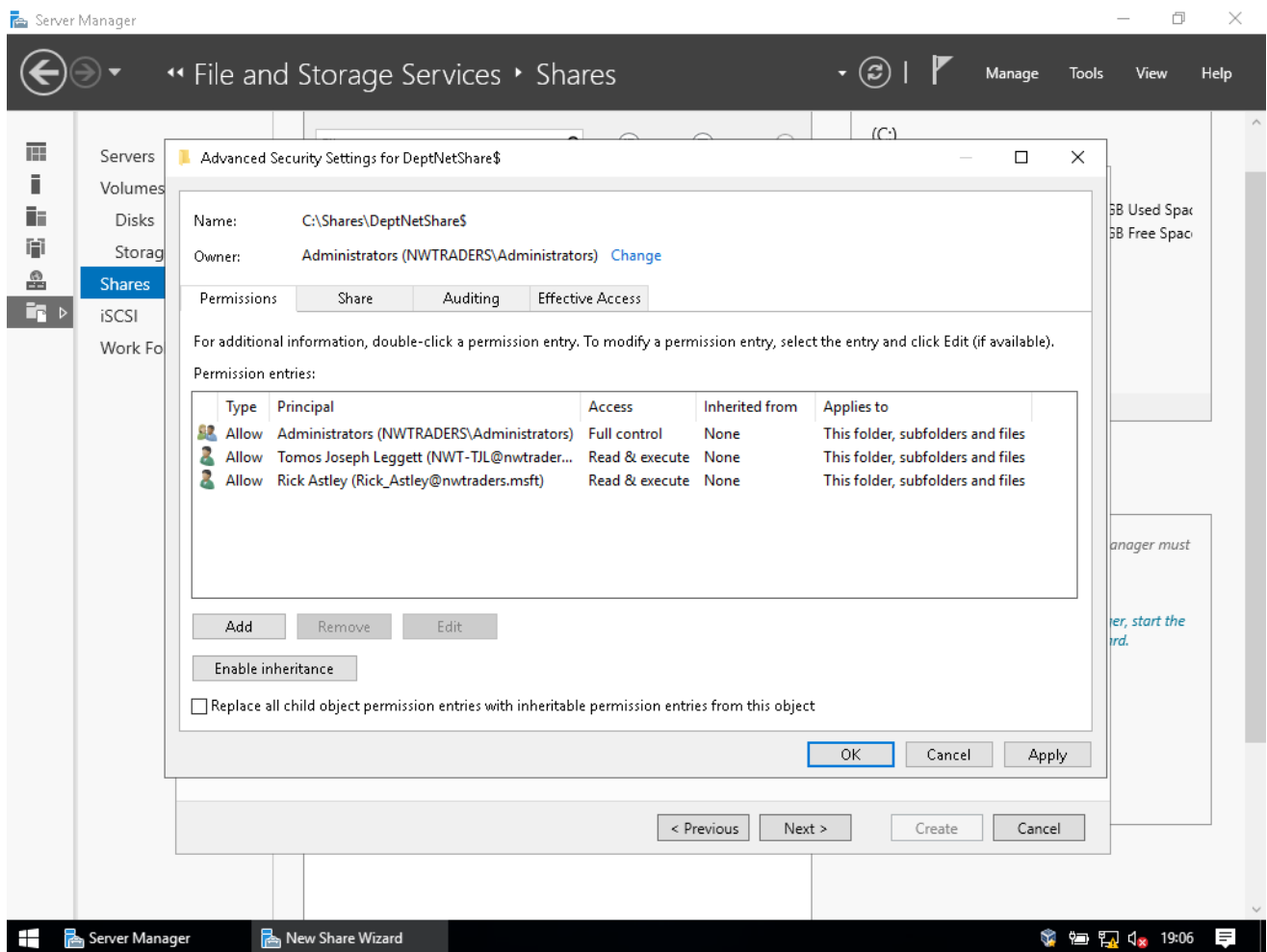
The author selects 'Select by volume' and then clicks 'Next'.



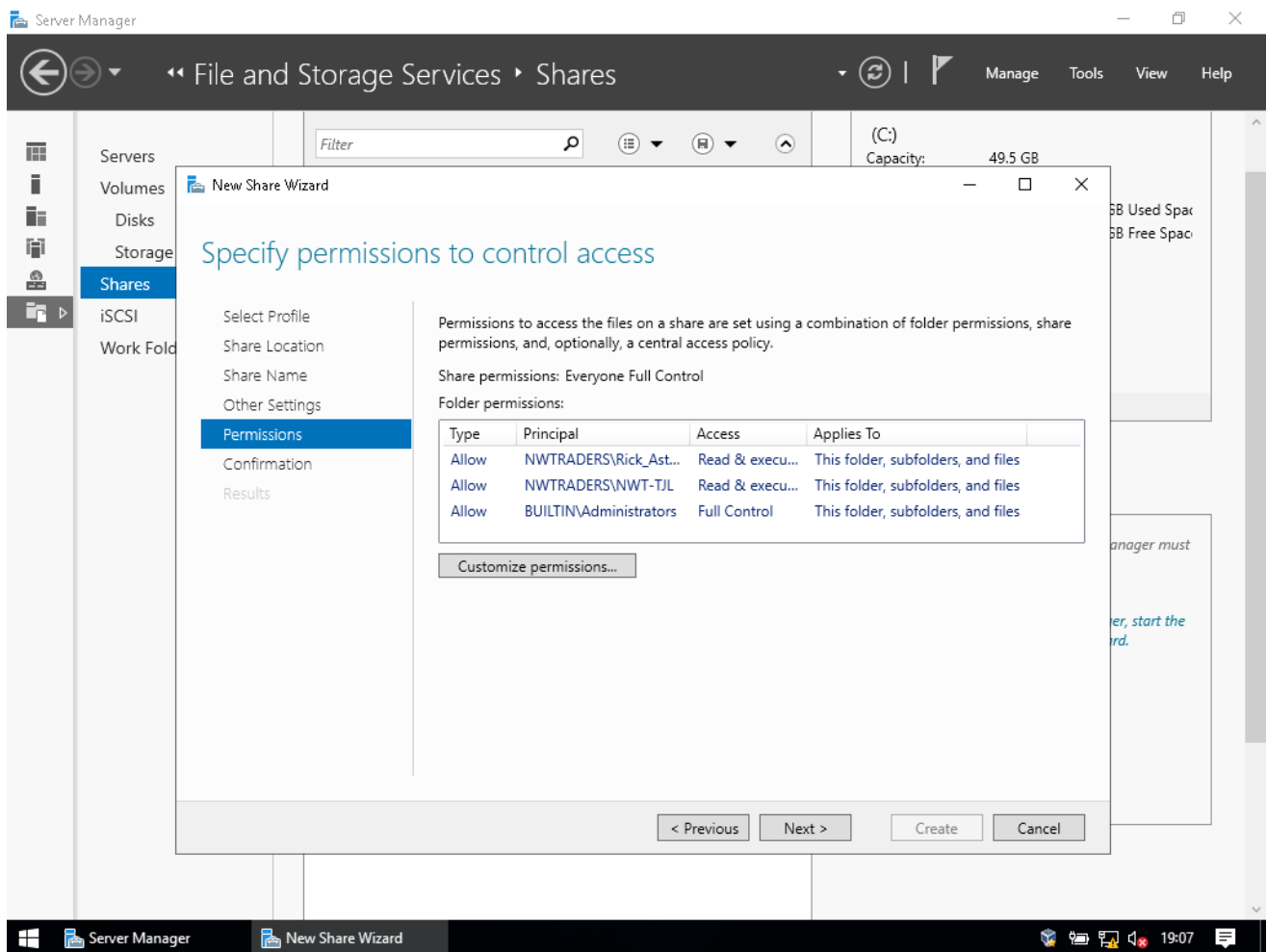
The name of the share is set to 'DeptNetShare\$'. The local path is set automatically to 'C:\Shares\DeptNetShare...' as this directory doesn't exist, it'll be created. The remote path is also set automatically to '\\DC1-NWT\DeptNetShare...'



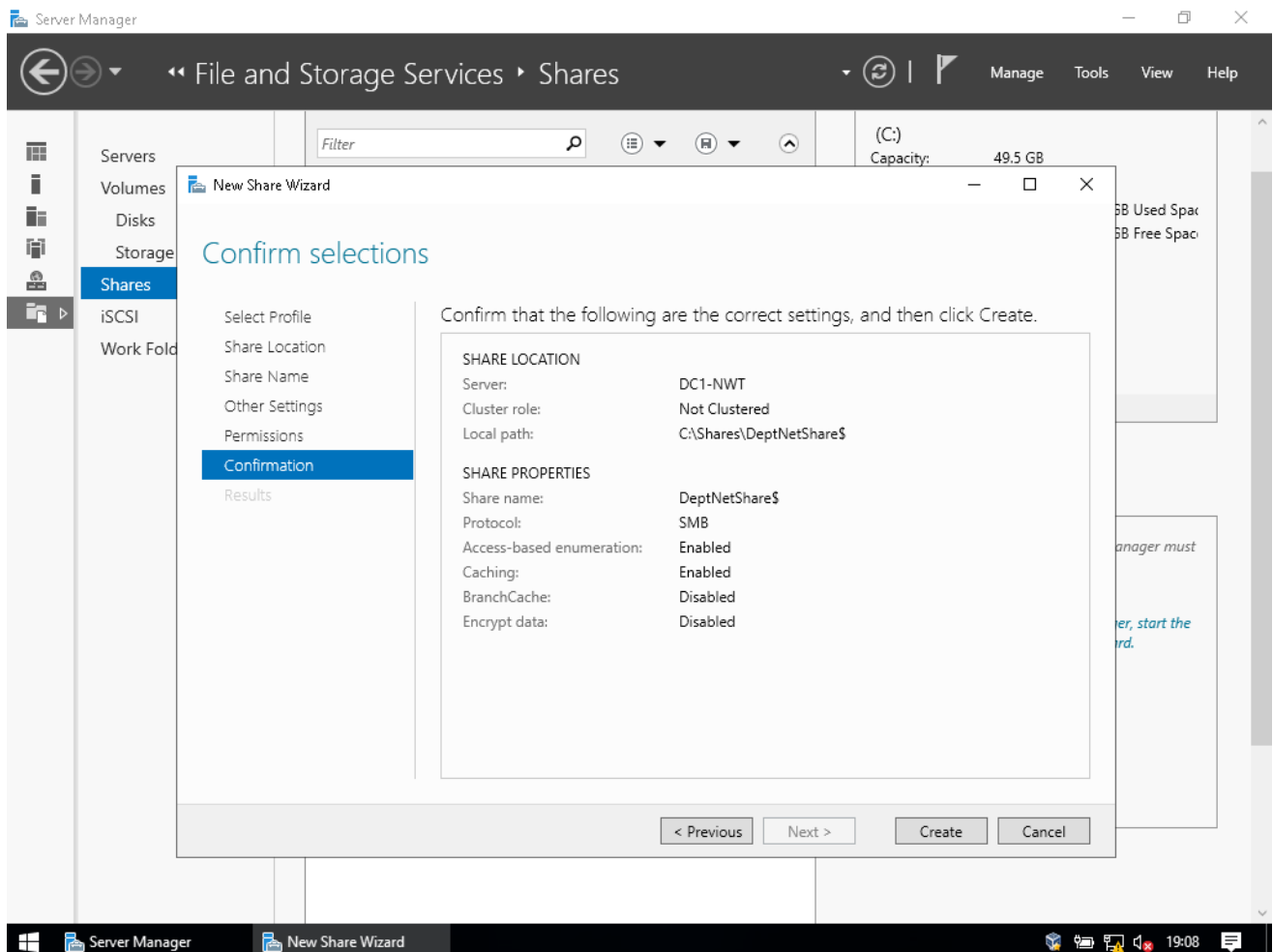
As detailed in the brief, the 'Enable access-based enumeration' and 'Allow caching of share' is required to be checked. Access-based enumeration is toggled as it will only display files and directories that the particular users accessing this share have the rights to access. Caching of share is enabled so that users can see their files and directories even when they go offline by caching said files to a local disk on their machine.



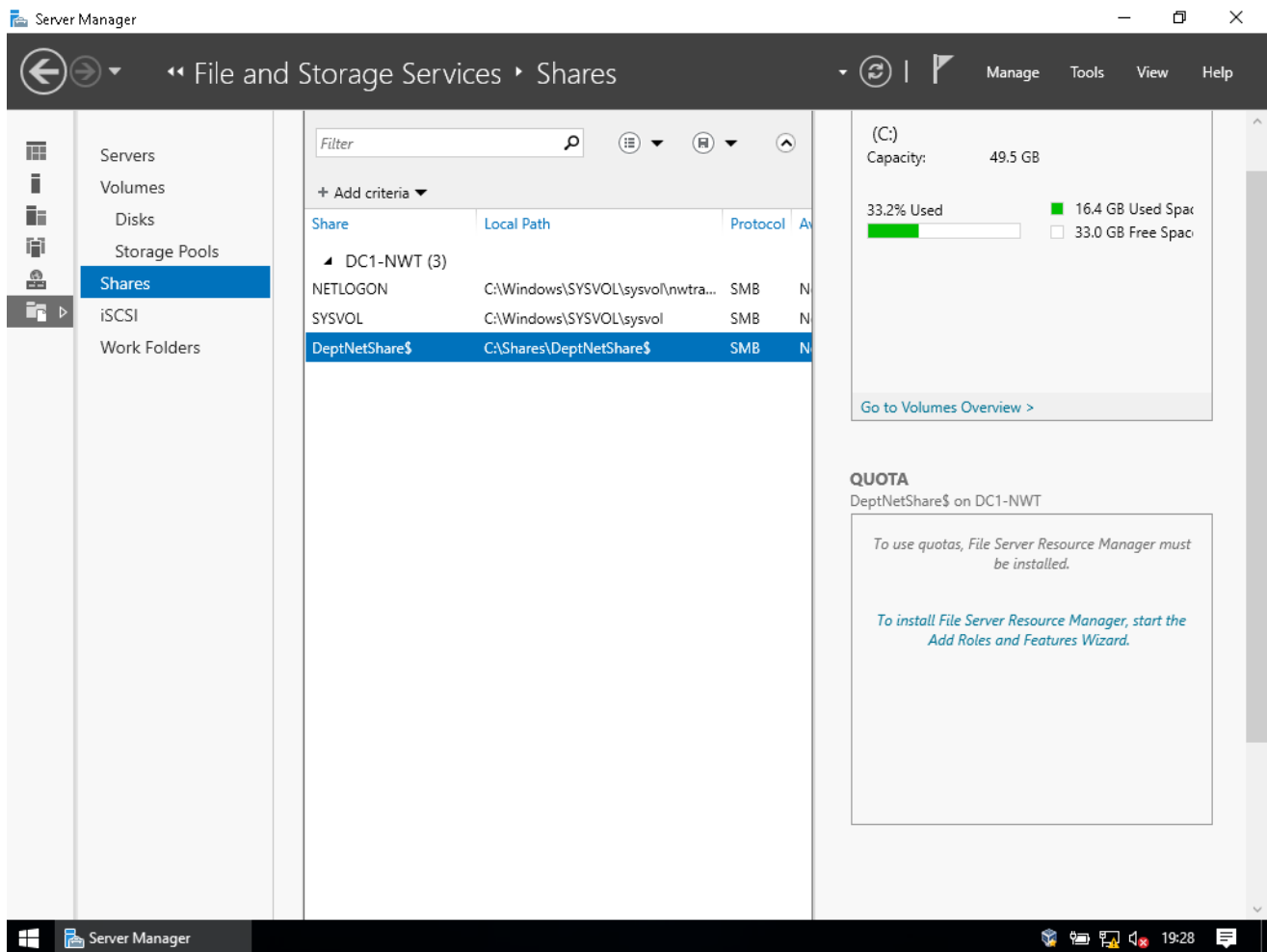
As requested, the author has specified the permissions according to the brief. The administrators group has Full control over the share, whilst Tomos Joseph Leggett and Rick Astley have only Read & execute control.



This is confirmed in the next screen of the wizard.

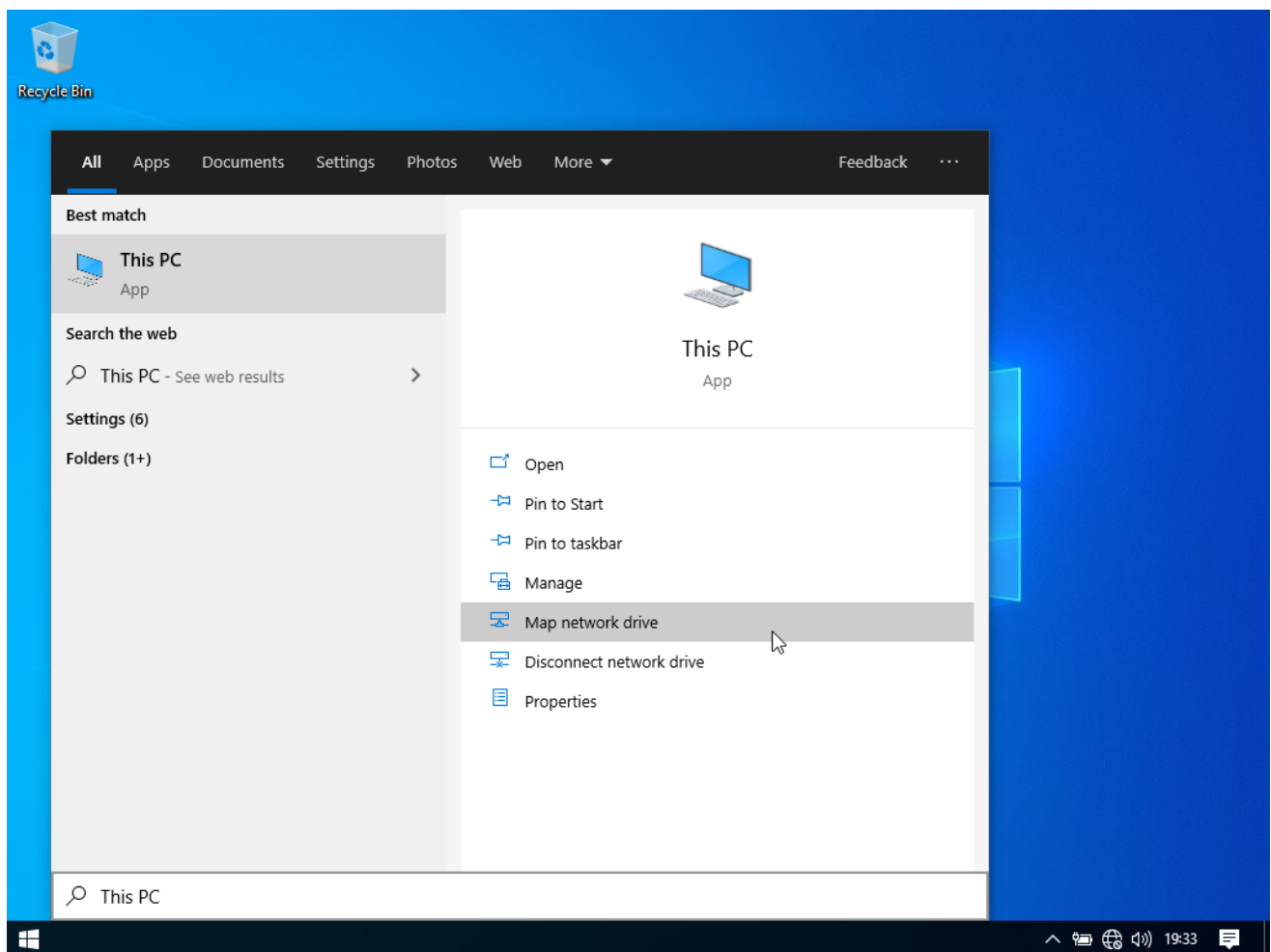


The final confirmation page of the wizard showcases a confirmation screen where the author can verify that everything is okay.

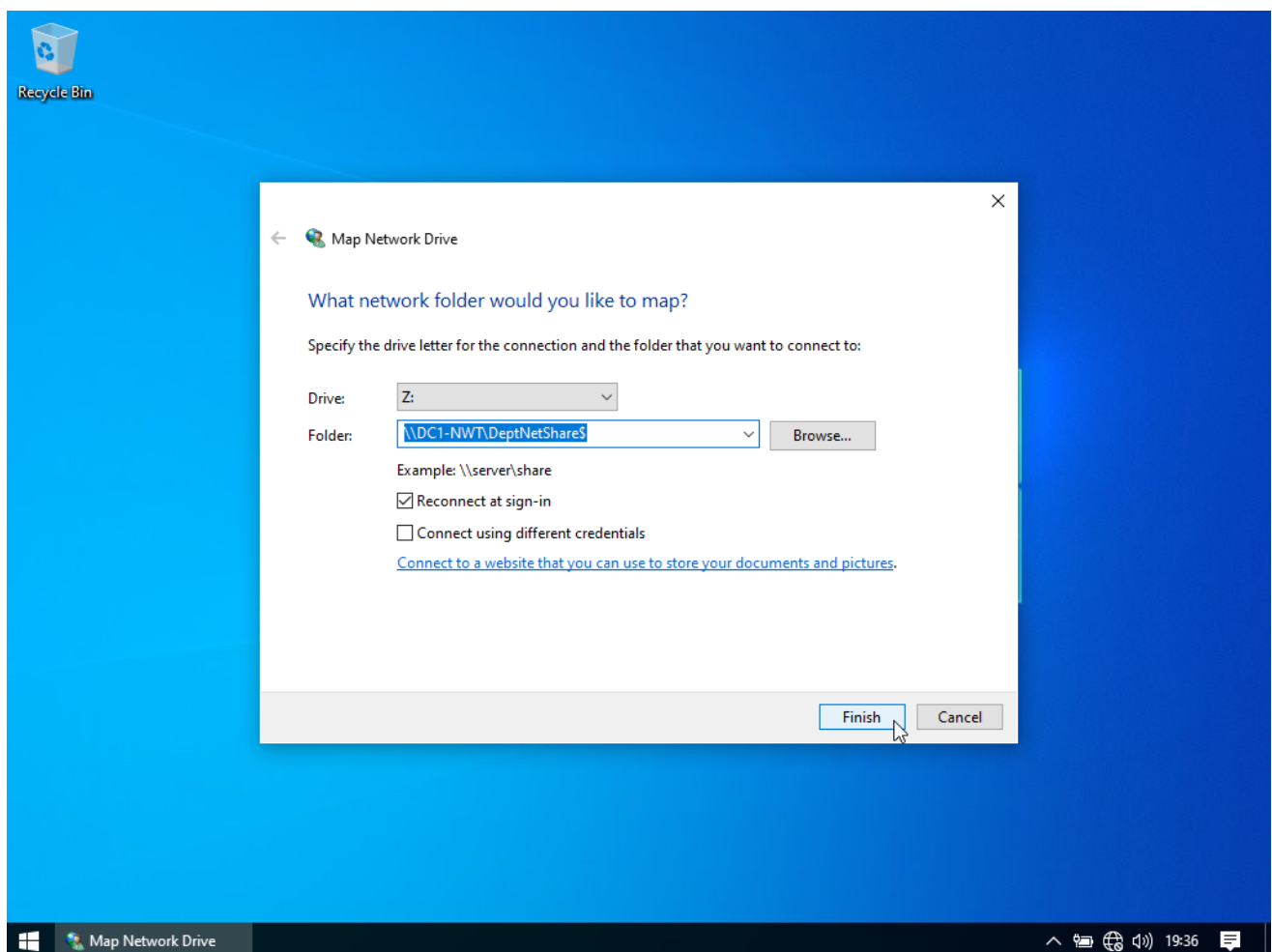


The share was successfully created.

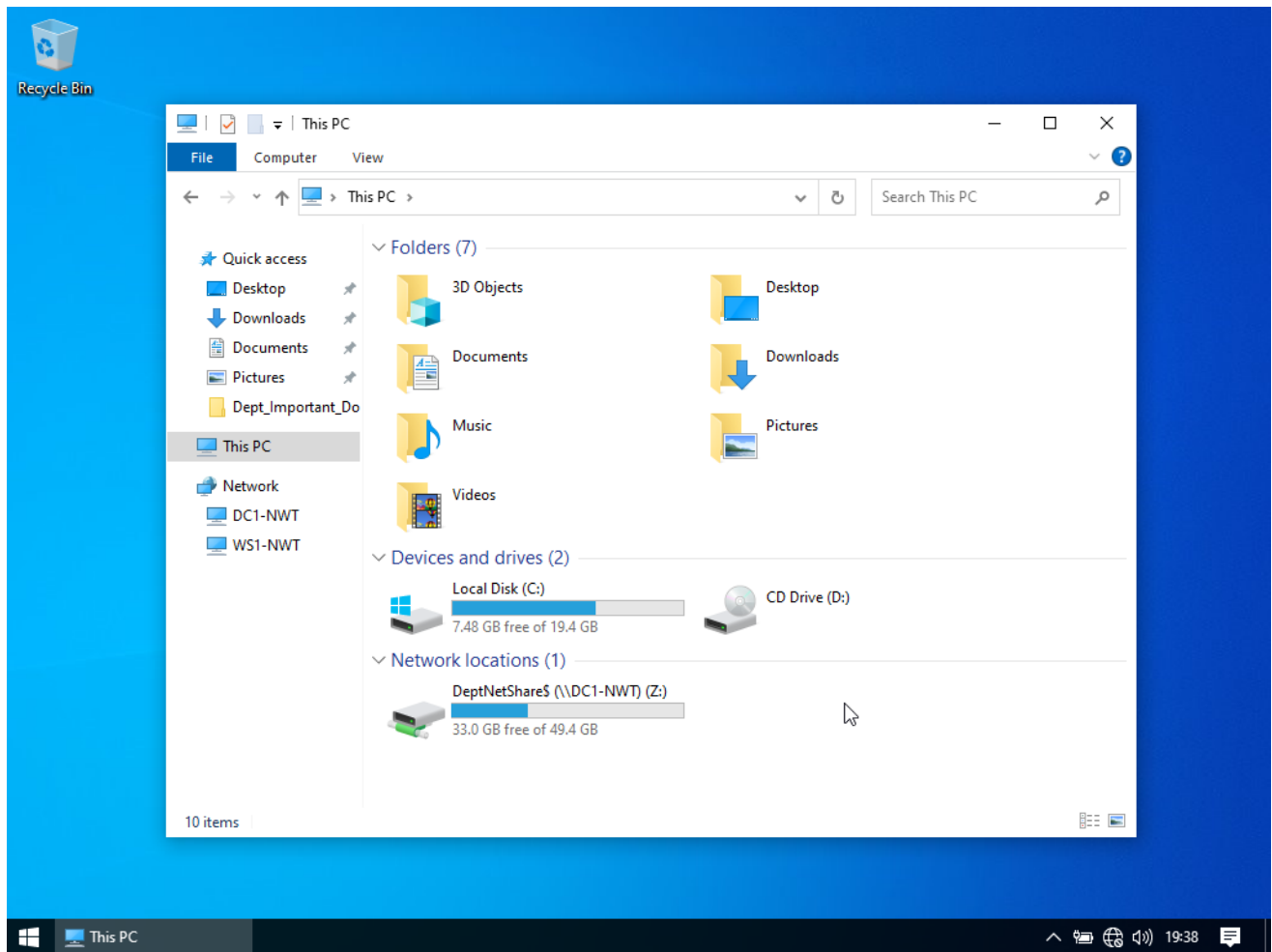
// Switching back to Client 1 //



The author will now map the share as a network drive.

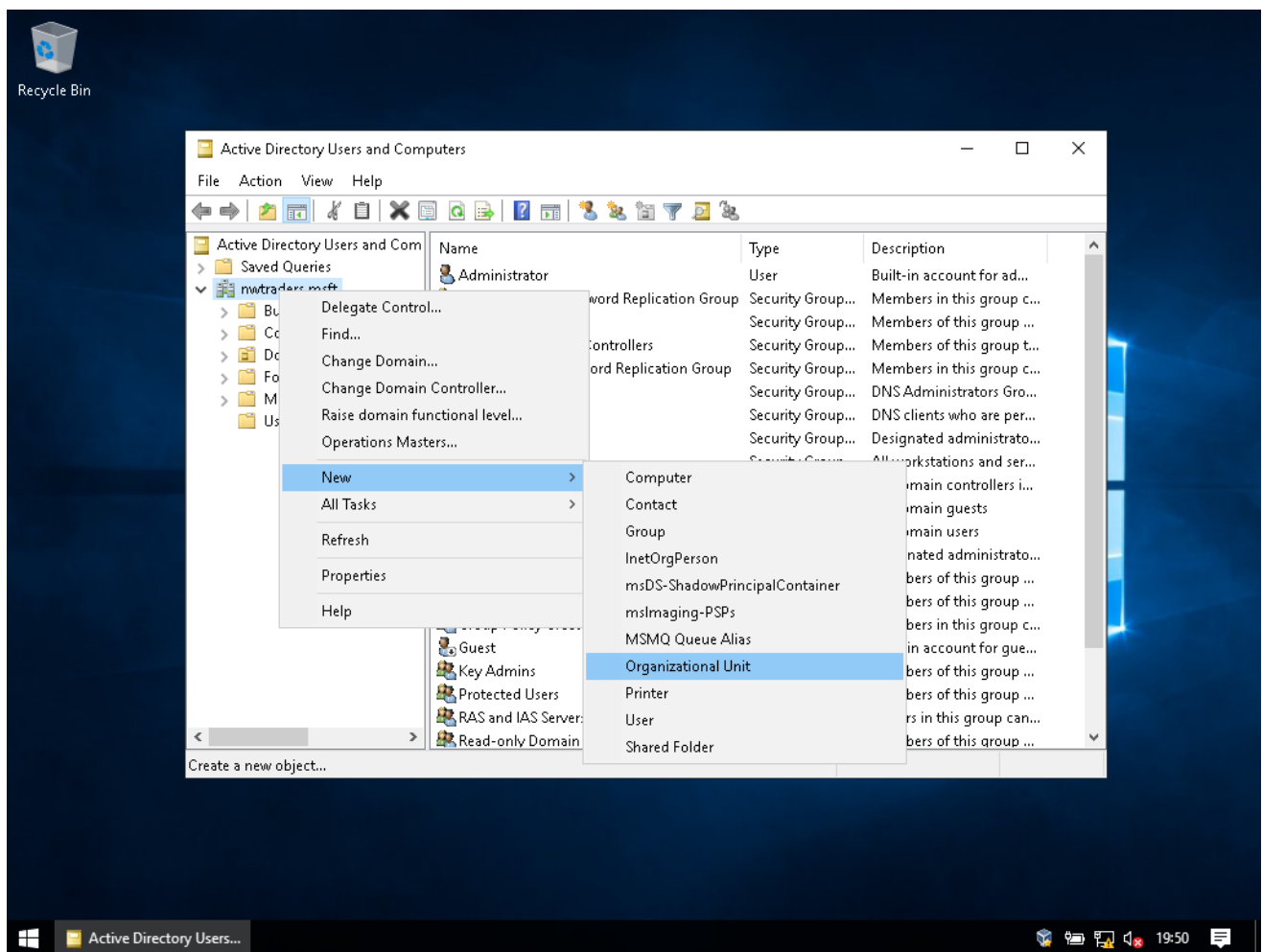


The folder was set to the full file share name including the \$ symbol. The drive symbol was set to Z by default and was left unchanged.

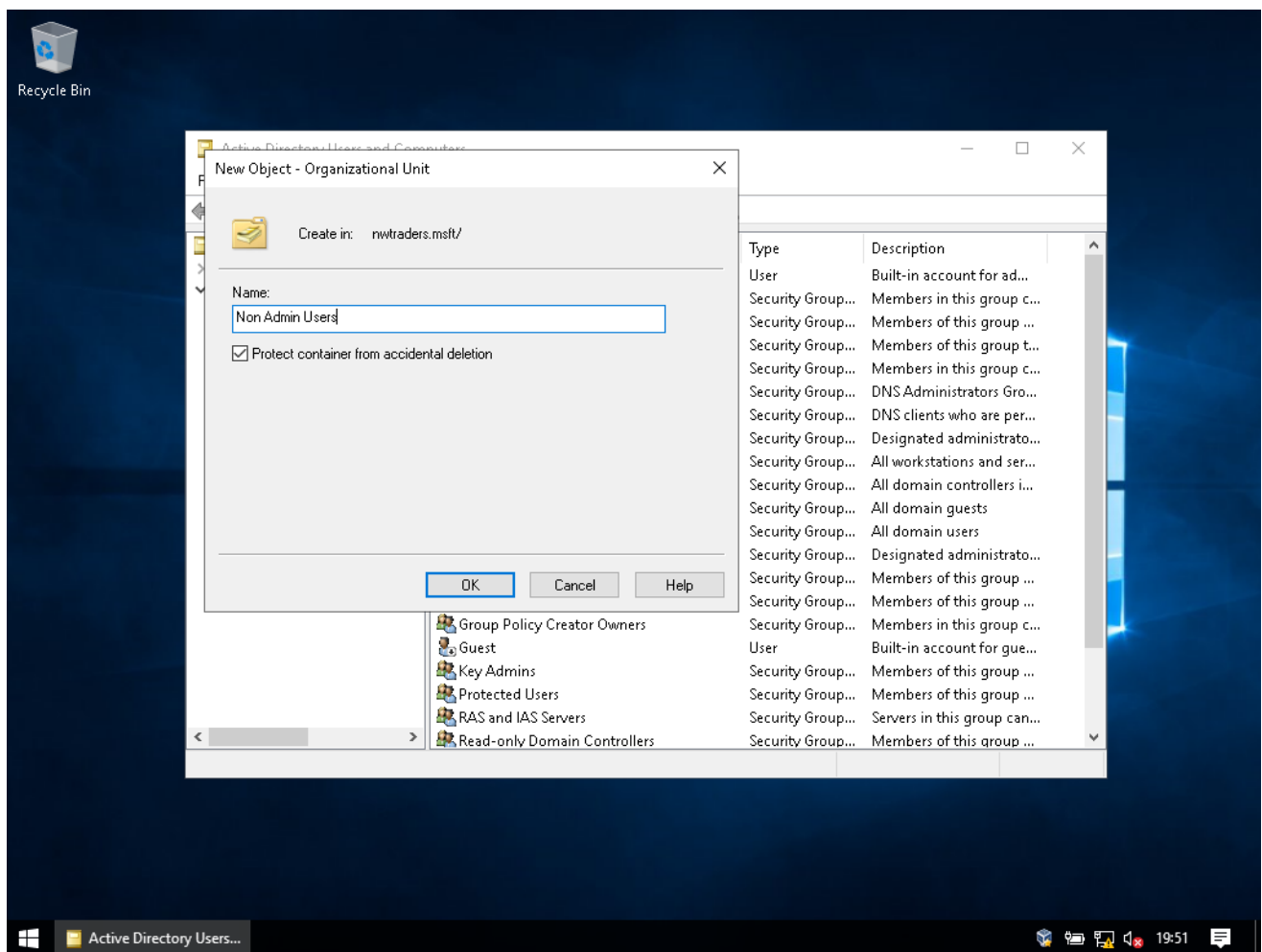


The author can confirm that located in the 'This PC' folder, a network location named DeptNetShare\$ can be seen as the Z drive.

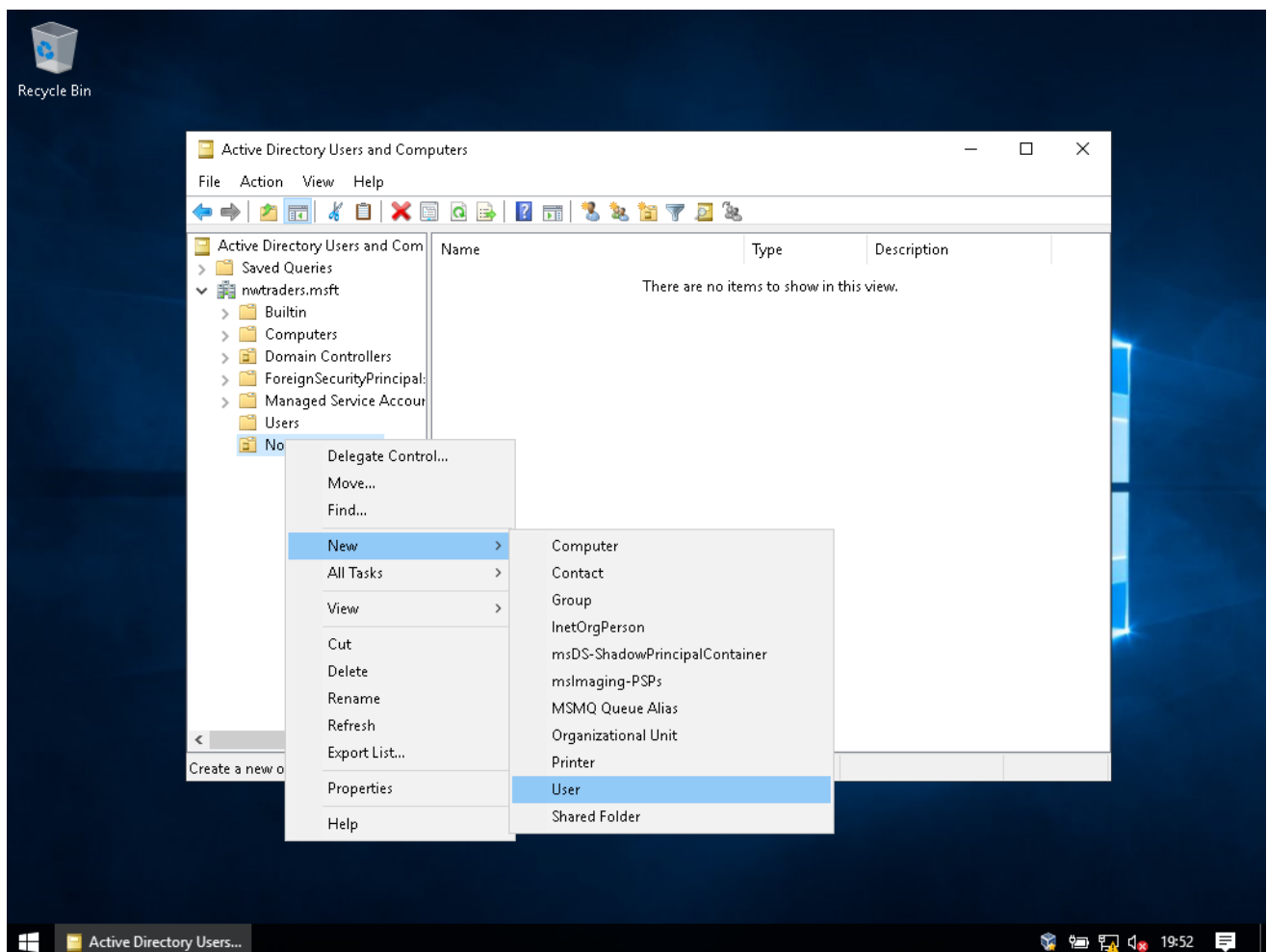
Task 2: Utilising Group Policy Management Console to better facilitate network object management



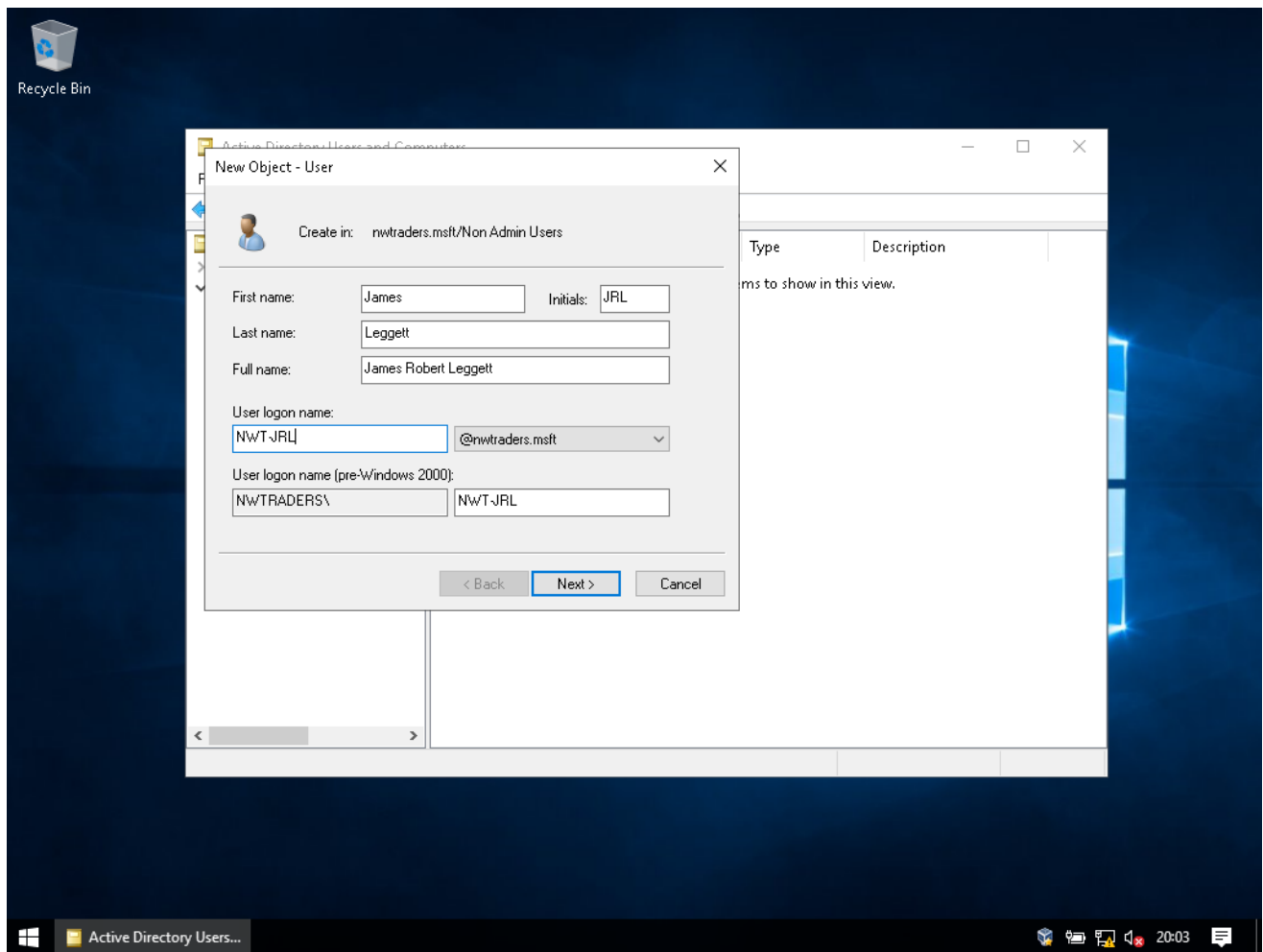
The author will now create a new Organisational Unit to restrict access to the control panel.



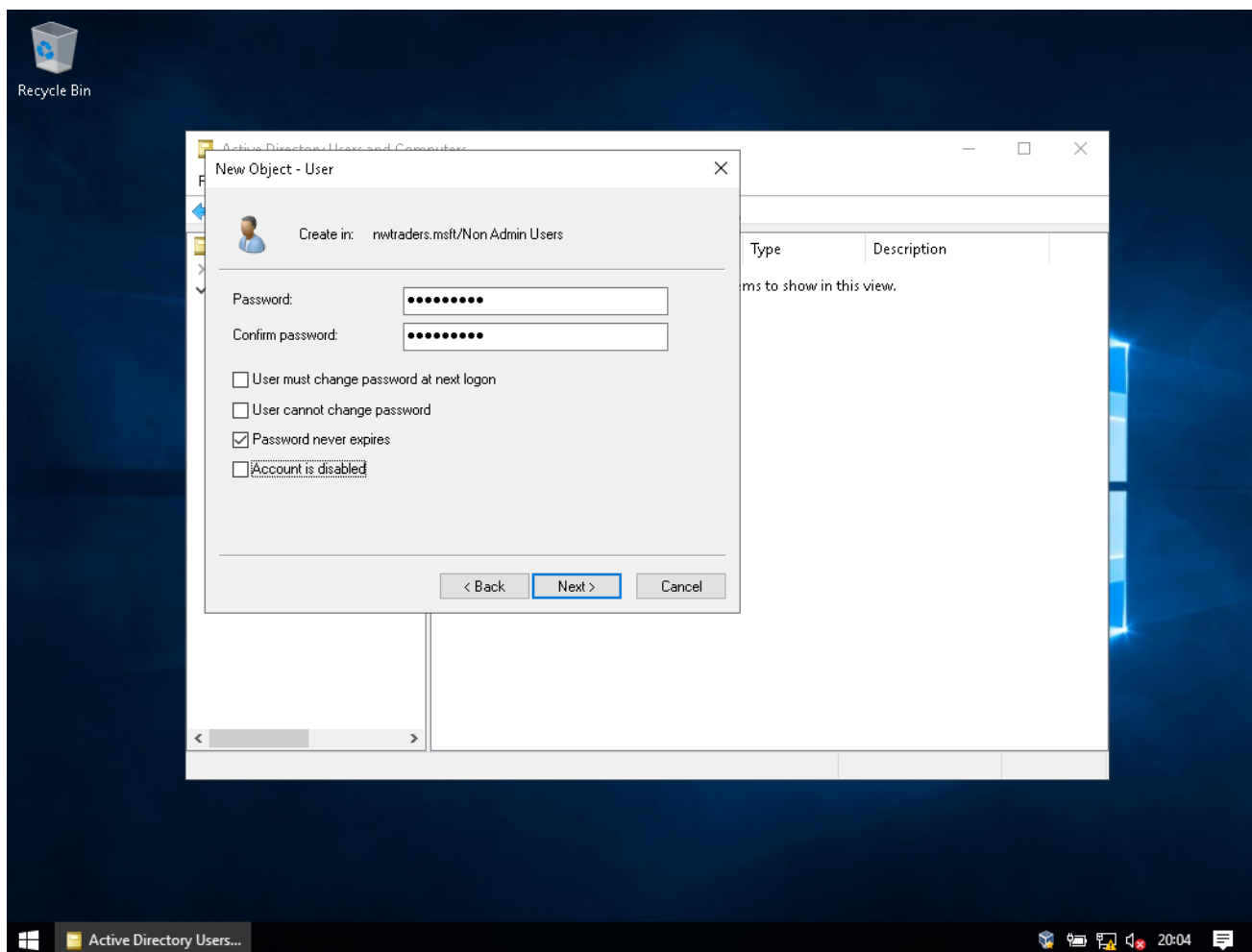
The Organisational Unit will be named 'Non Admin Users' accordingly.



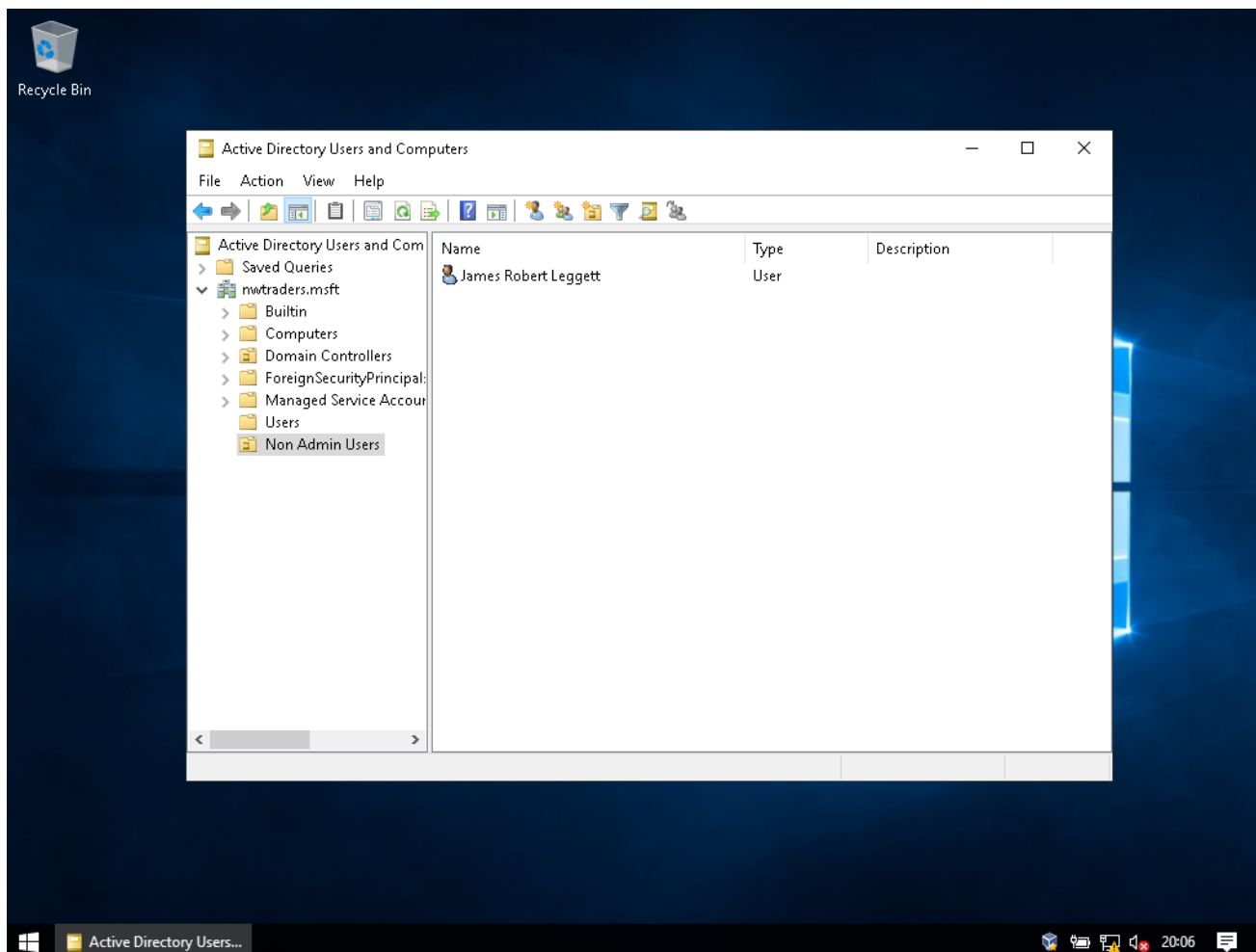
A new user will be created inside the Non Admin Users unit.



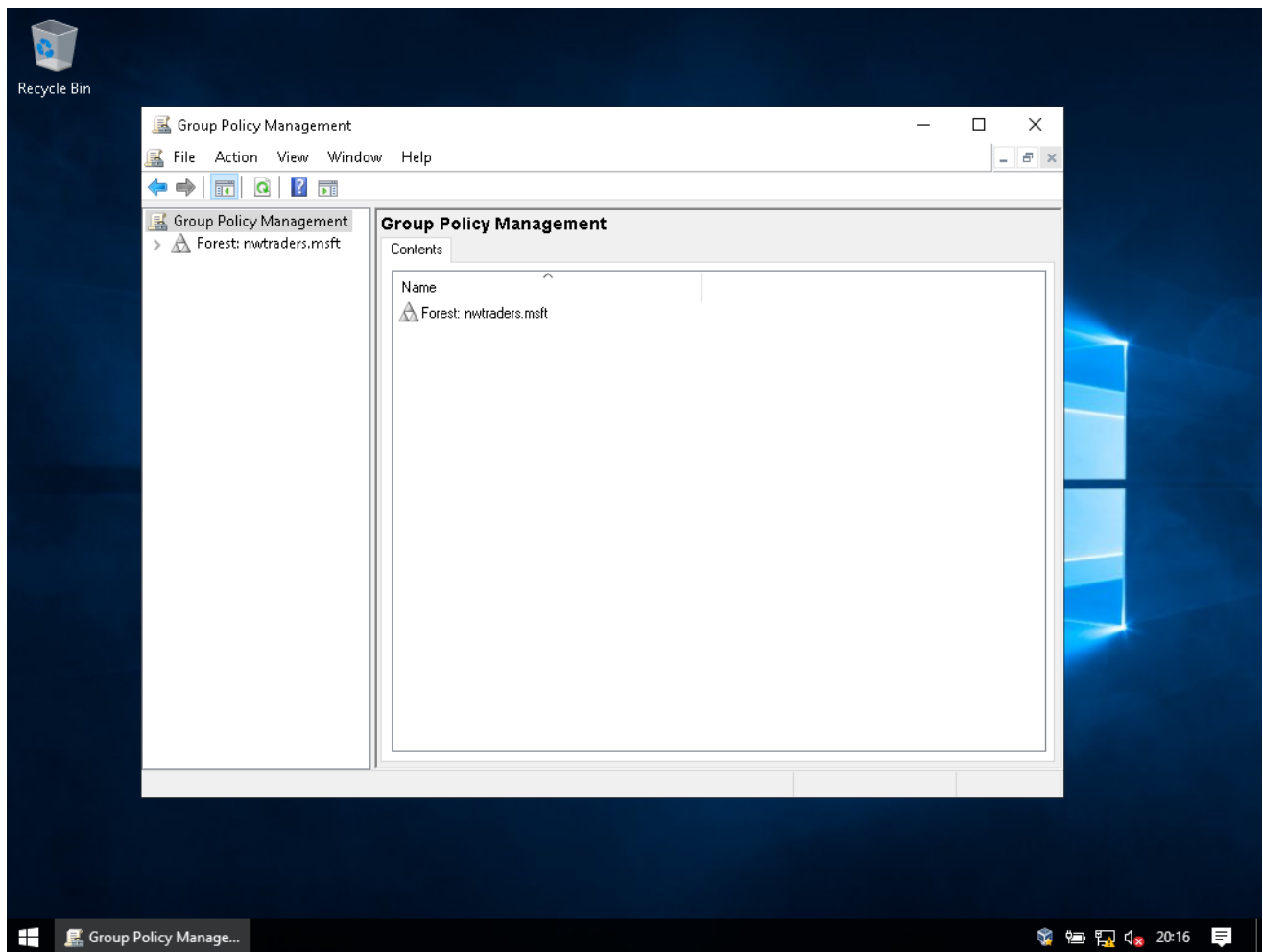
A new account will be created with the name 'NwT-JRL'



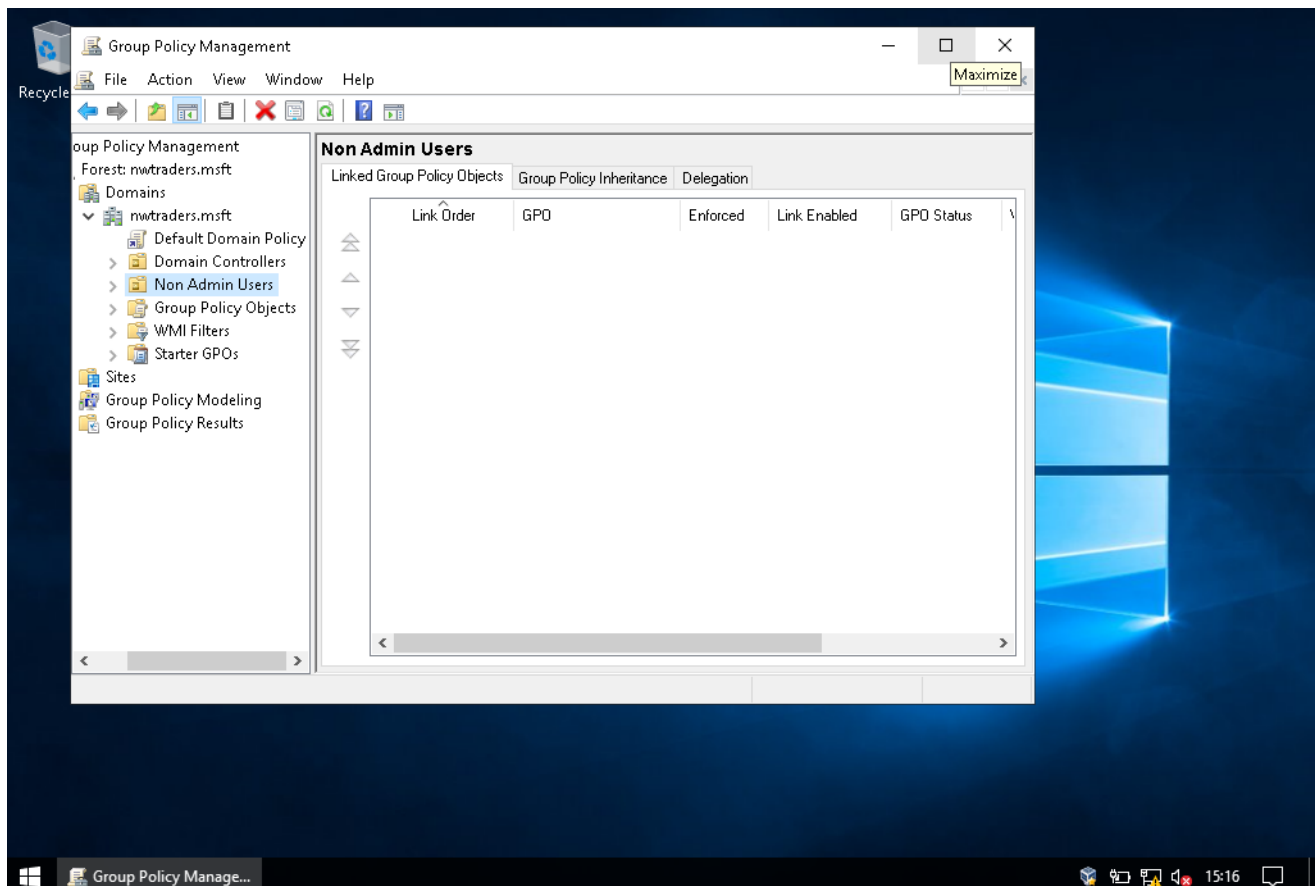
The password was set to P@ssw0rd1.



Confirmation of the lone account in the Non Admin Users unit.

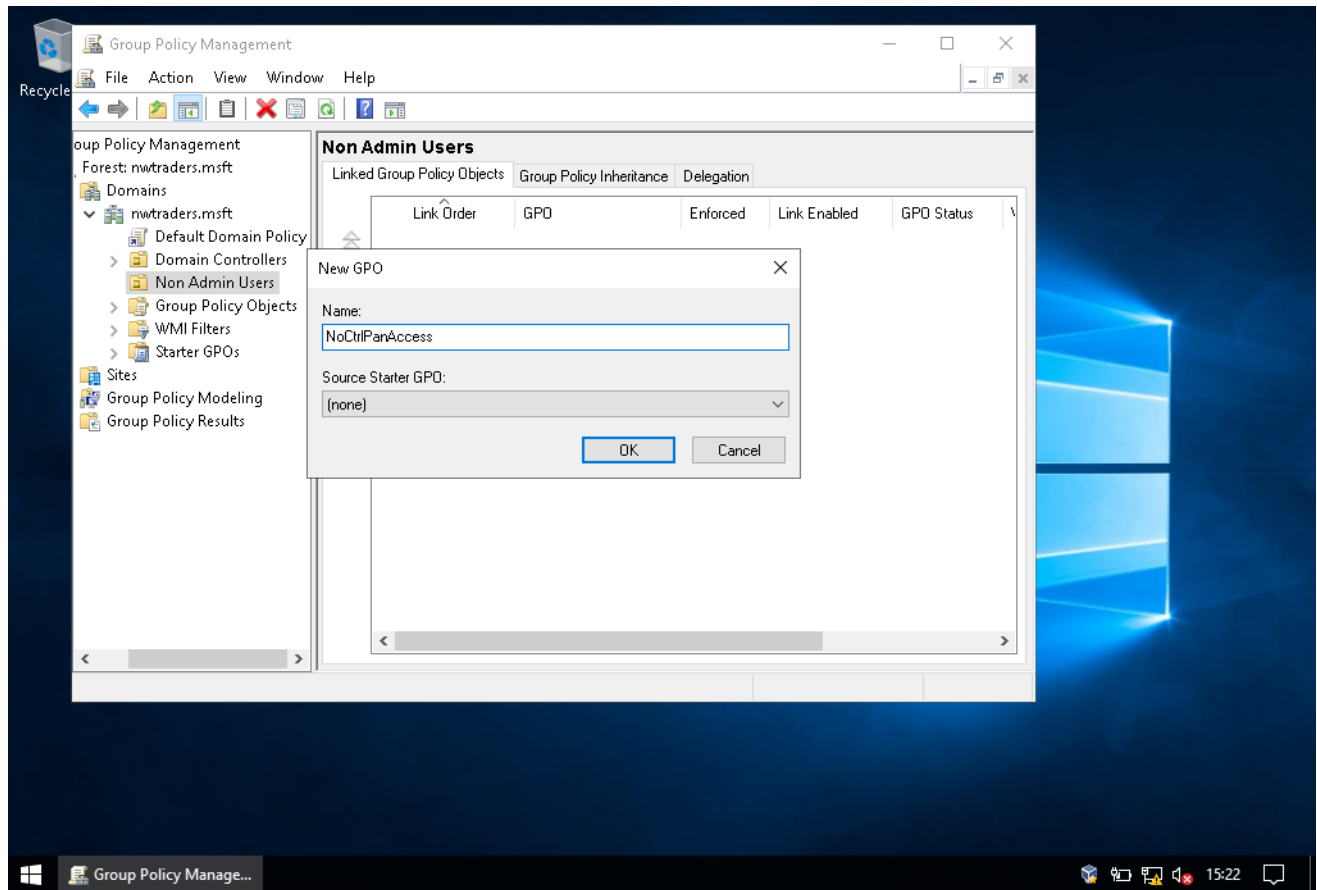


The Group Policy Management application is launched.

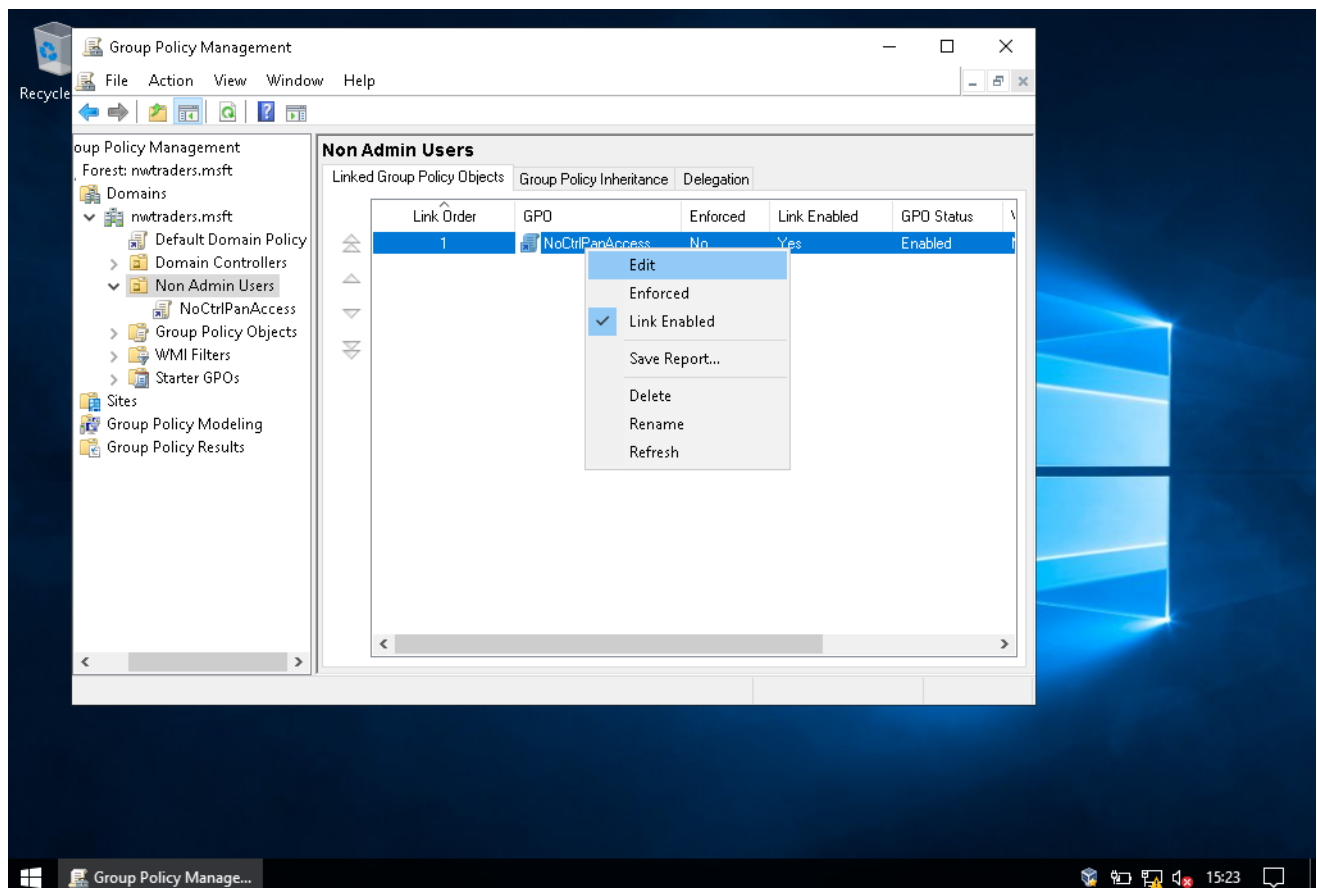


Restricting access to the Control Panel

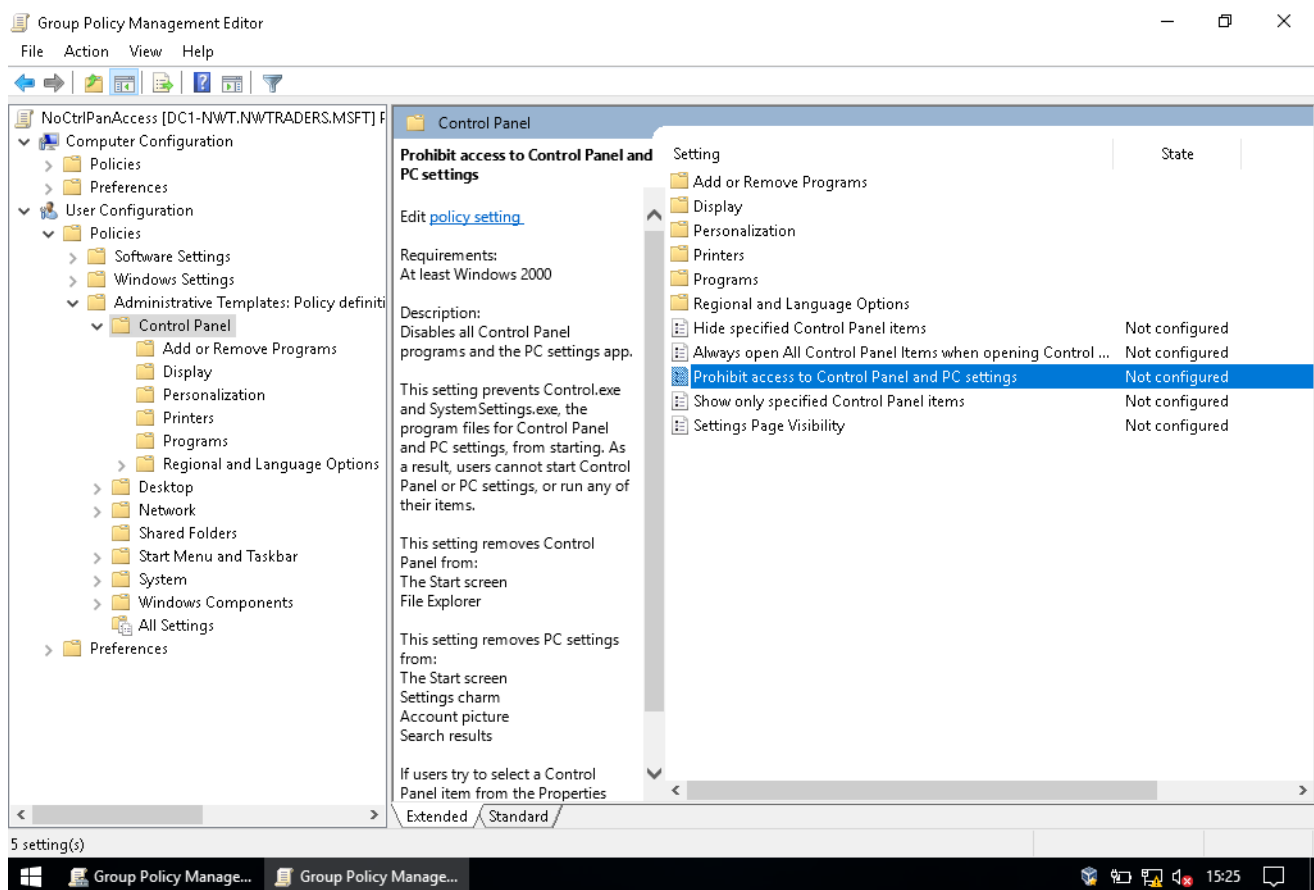
The 'Non Admin Users' object is loaded.



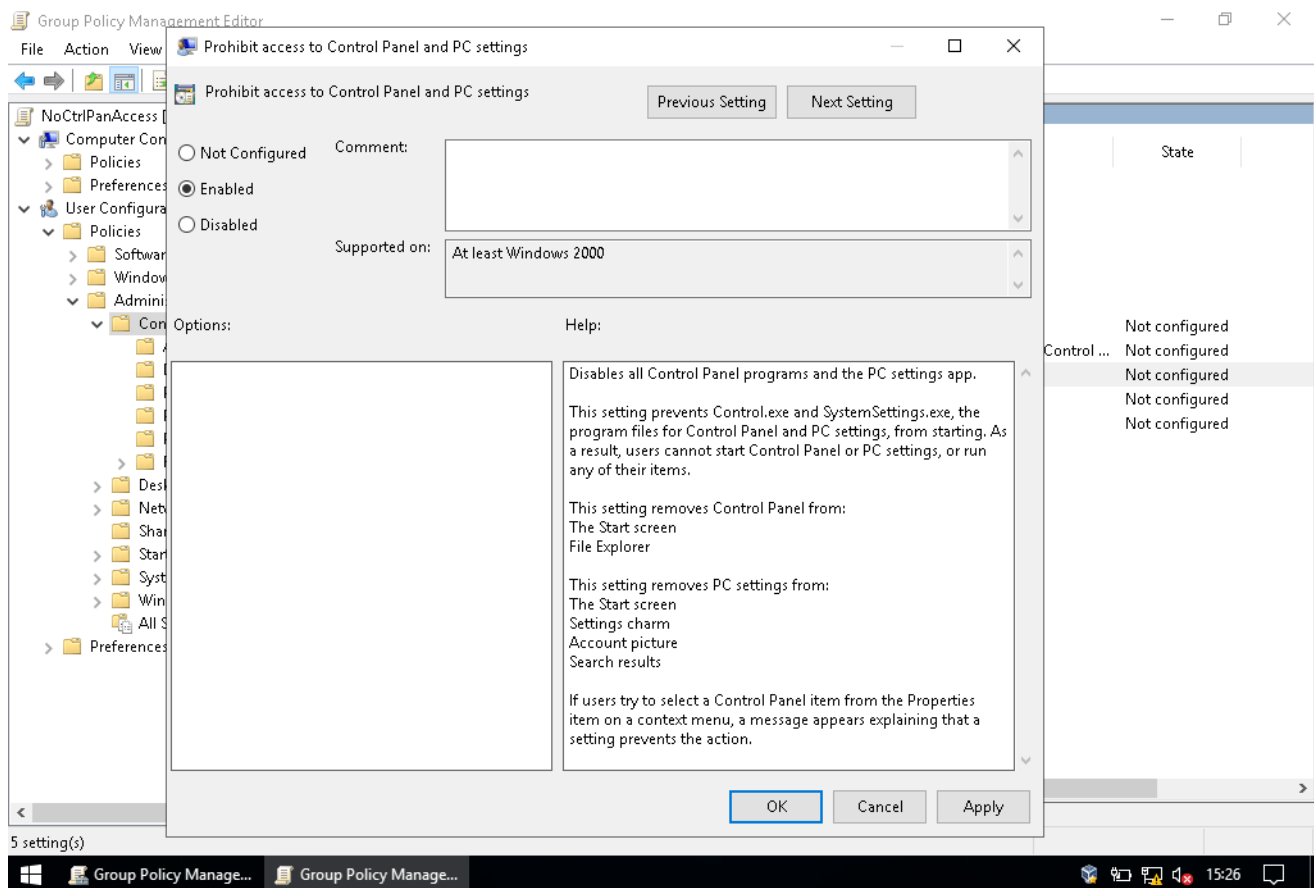
A new GPO is created and named 'NoCtrlPanAccess' for the Non Admin Users object.



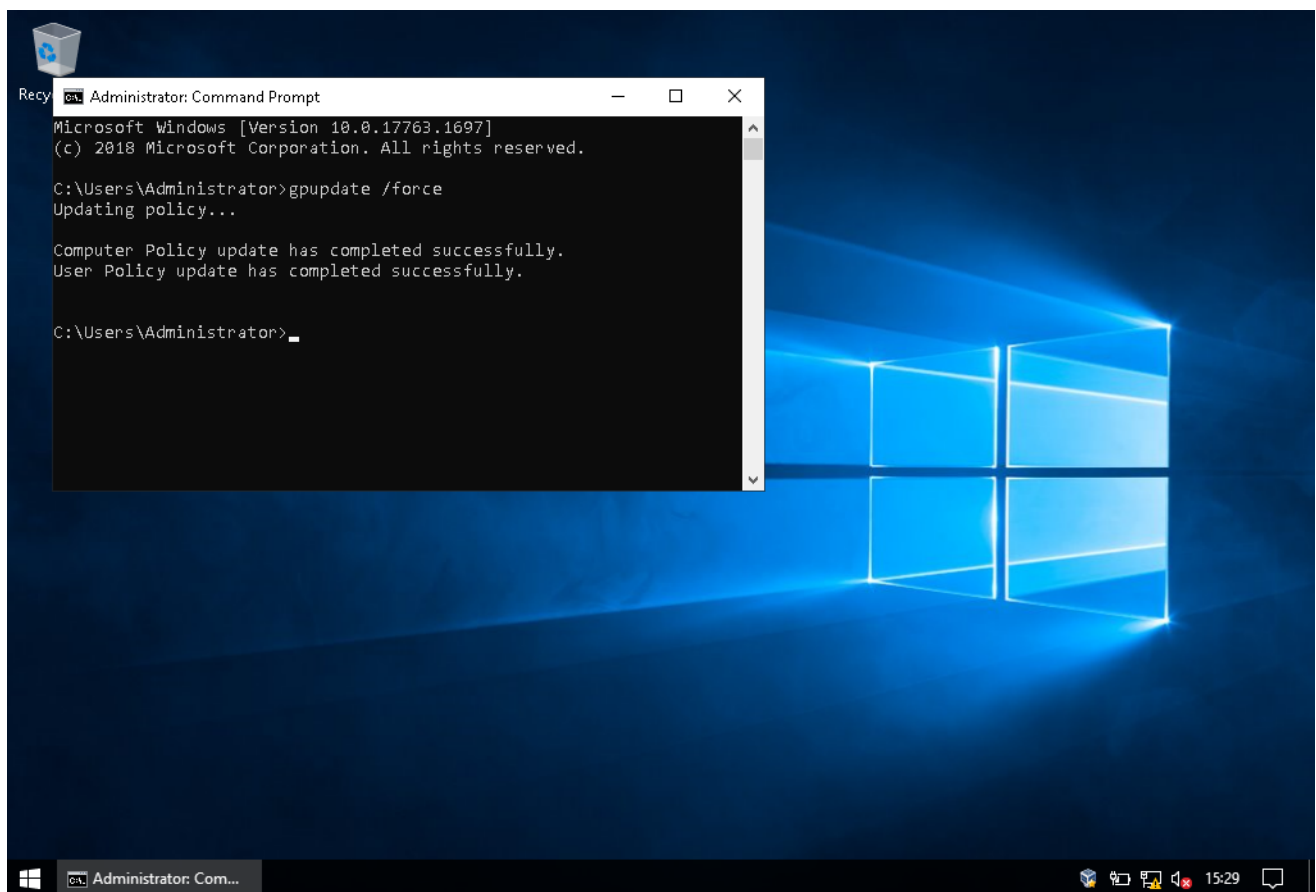
The author will now proceed to edit the NoCtrlPanAccess GPO.



The 'Prohibit access to Control Panel and PC settings' setting is located.



The setting is set to 'Enabled' and applied.

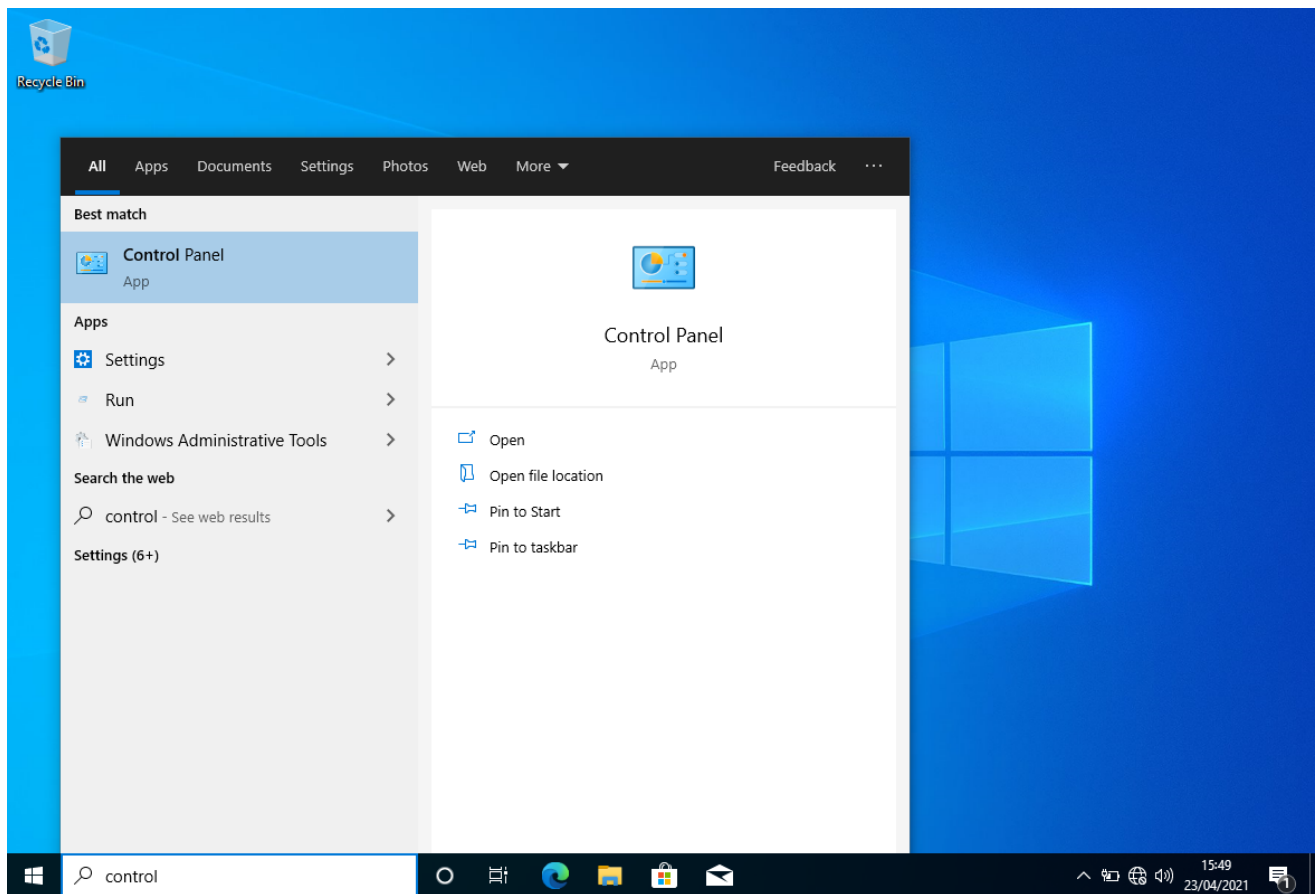


The **gpupdate /force** was run from an admin command prompt to ensure that Active Directory searches for new settings and policies automatically. The update completed successfully.

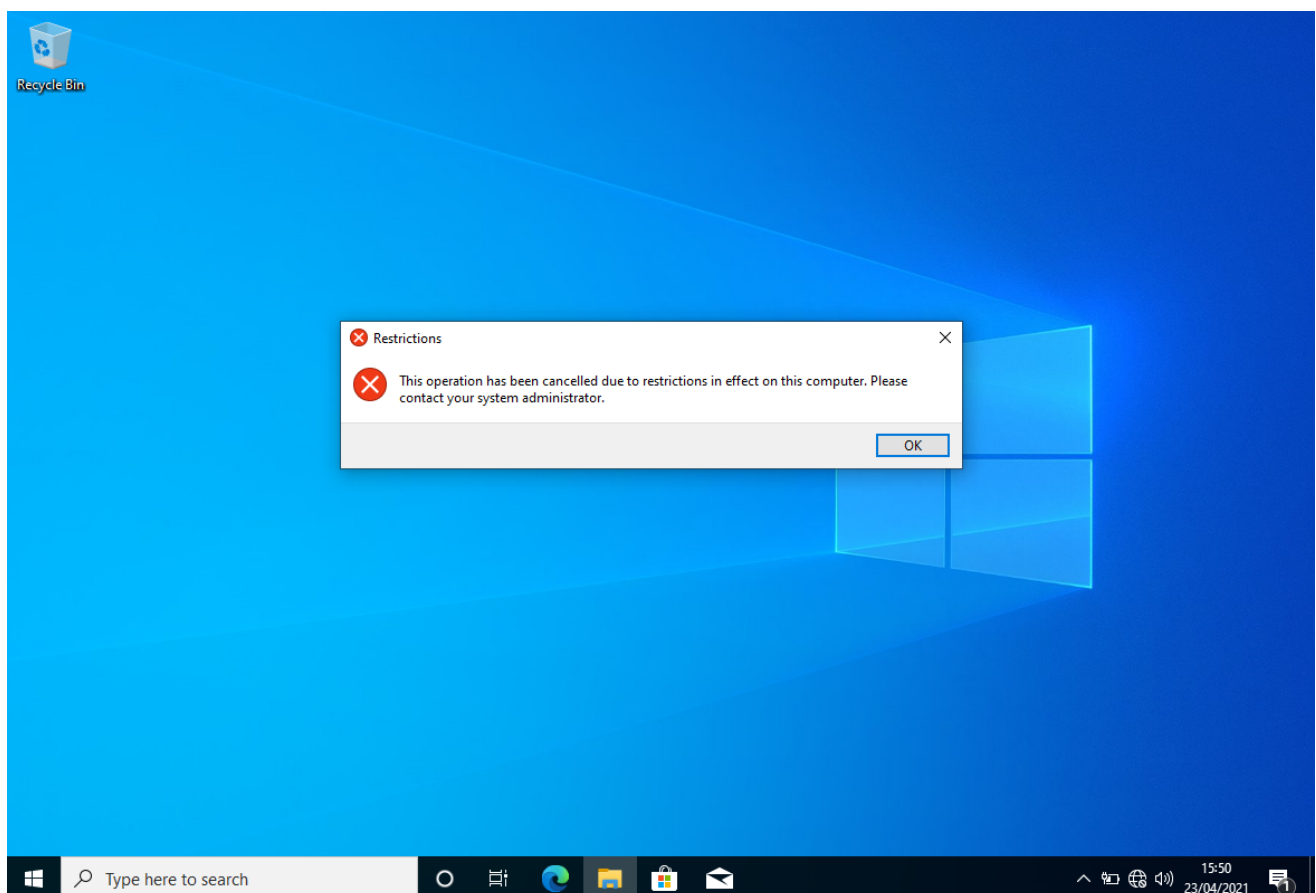
This might take several minutes

Don't turn off your PC

The author logs in as the non-admin.



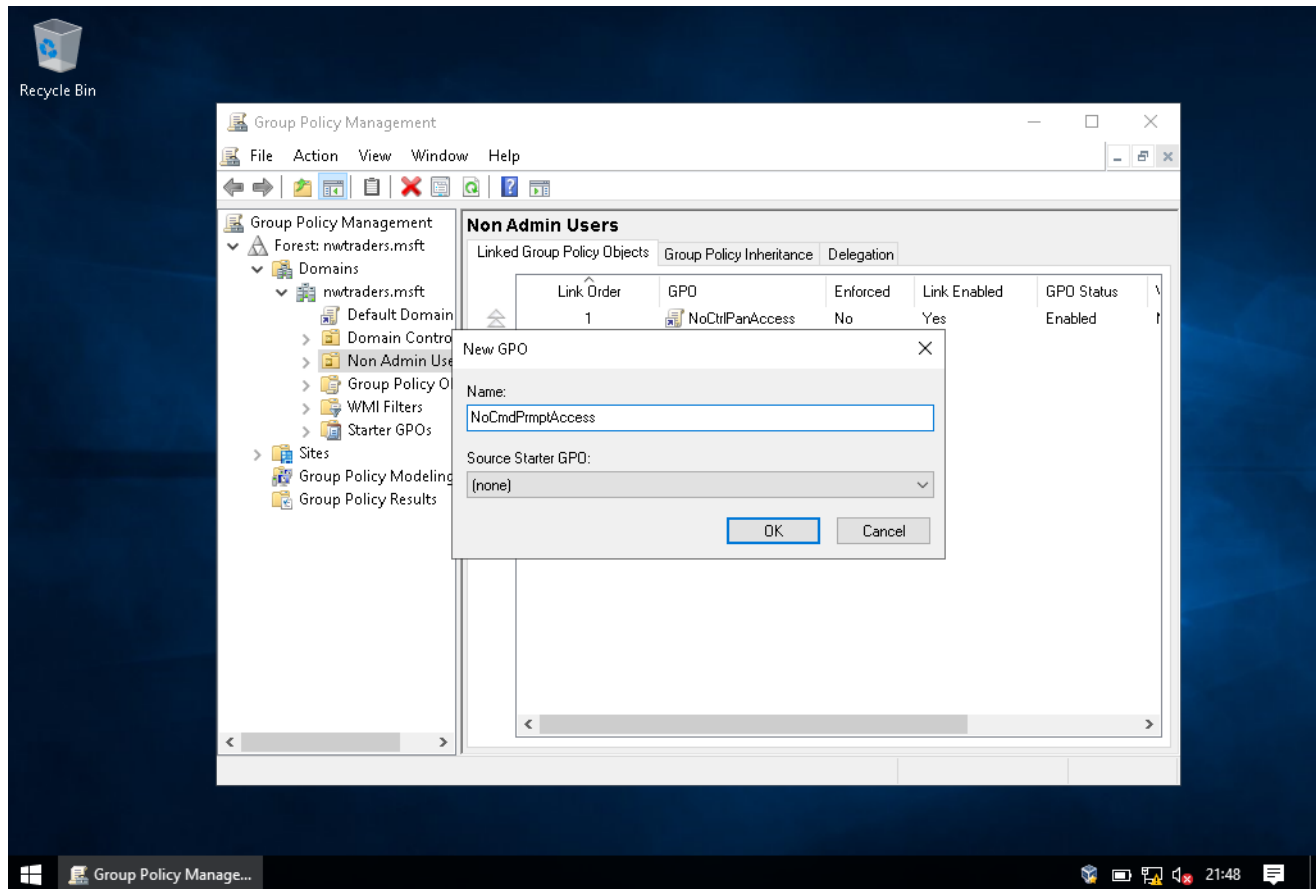
The author will attempt to run the control panel as the non admin account



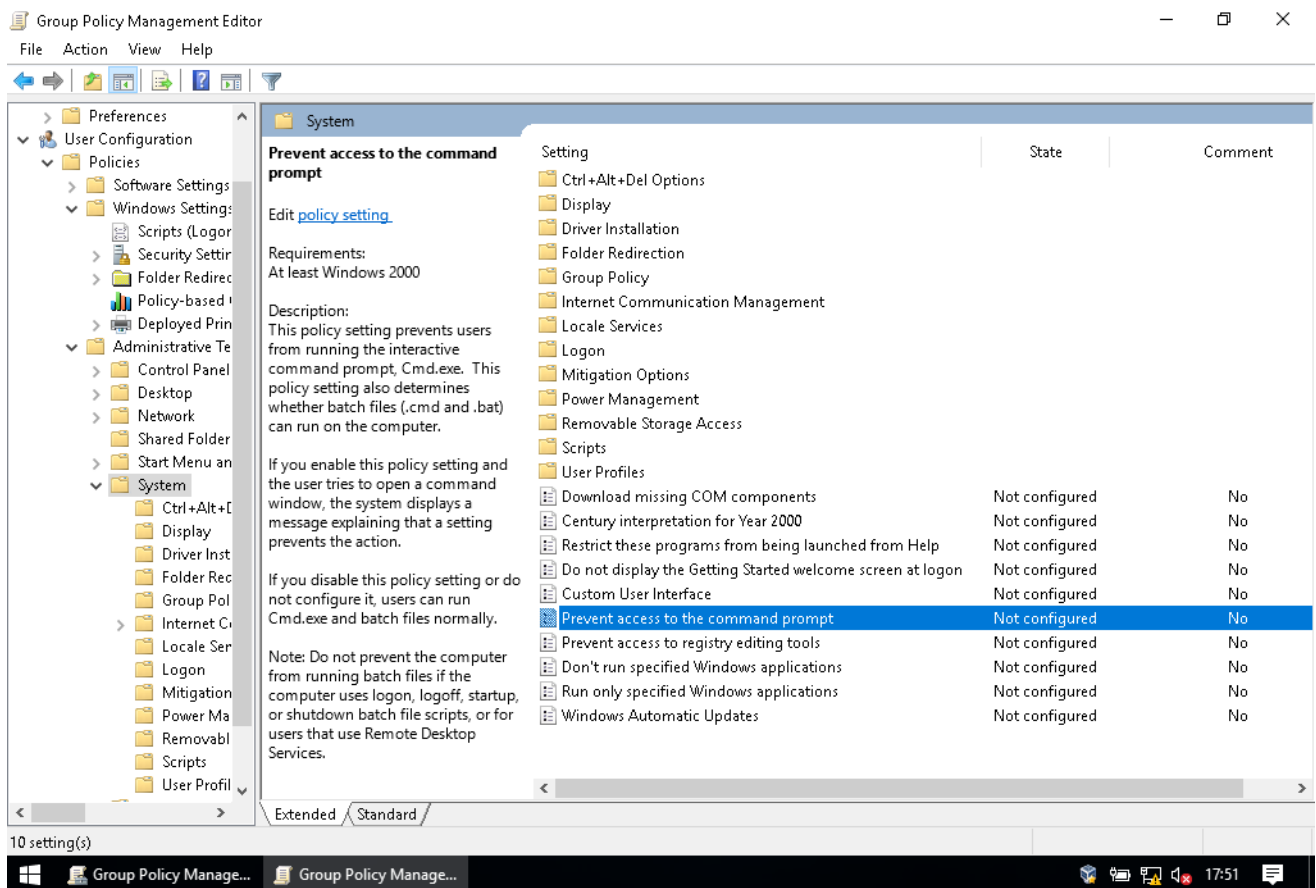
The task was successful. A restriction dialogue appears disallowing the user from accessing the control panel.

Restricting access to the command prompt

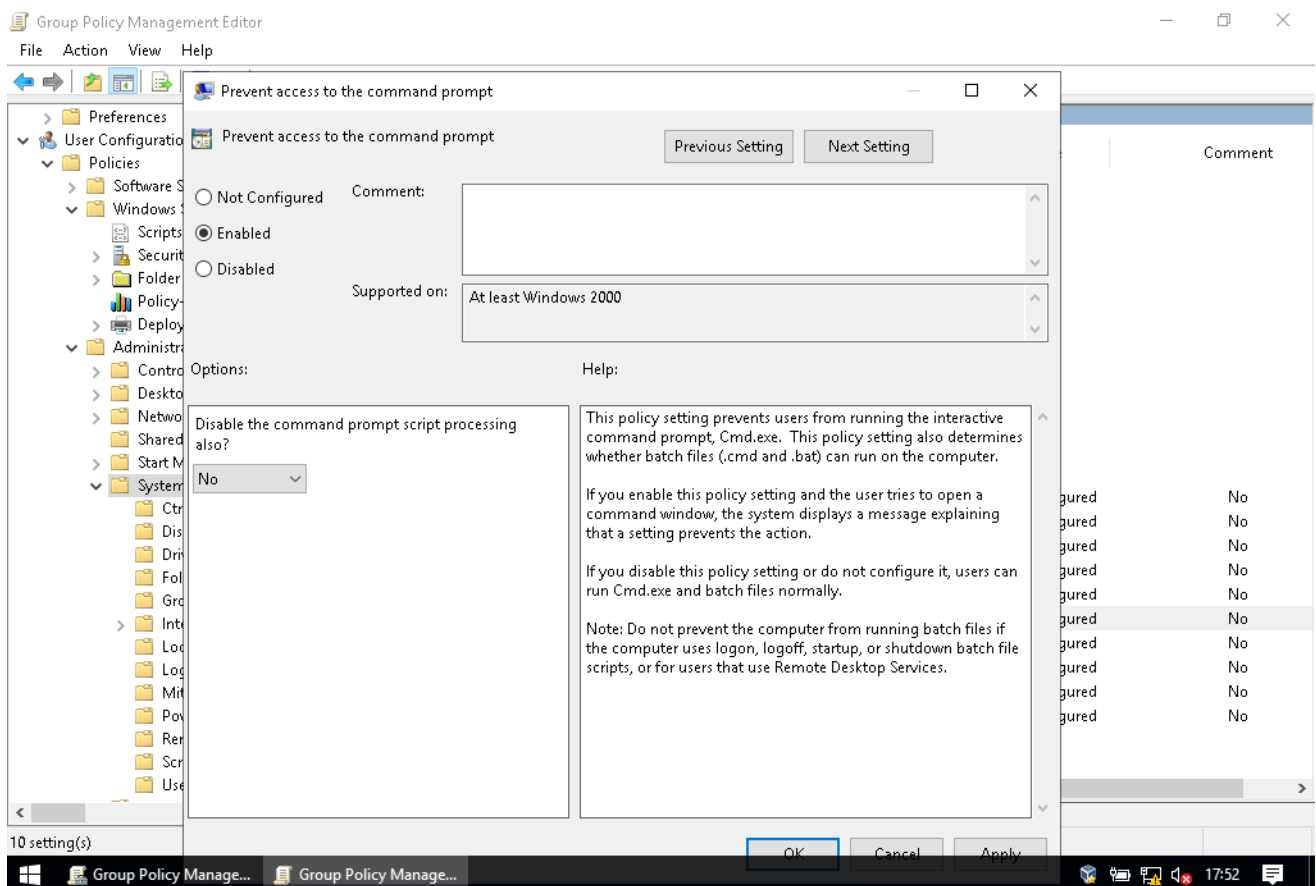
Access to the command prompt will need to be restricted as well, as access to the command prompt grants the user the ability to change system settings and access system features that would otherwise not be available on the desktop environment.



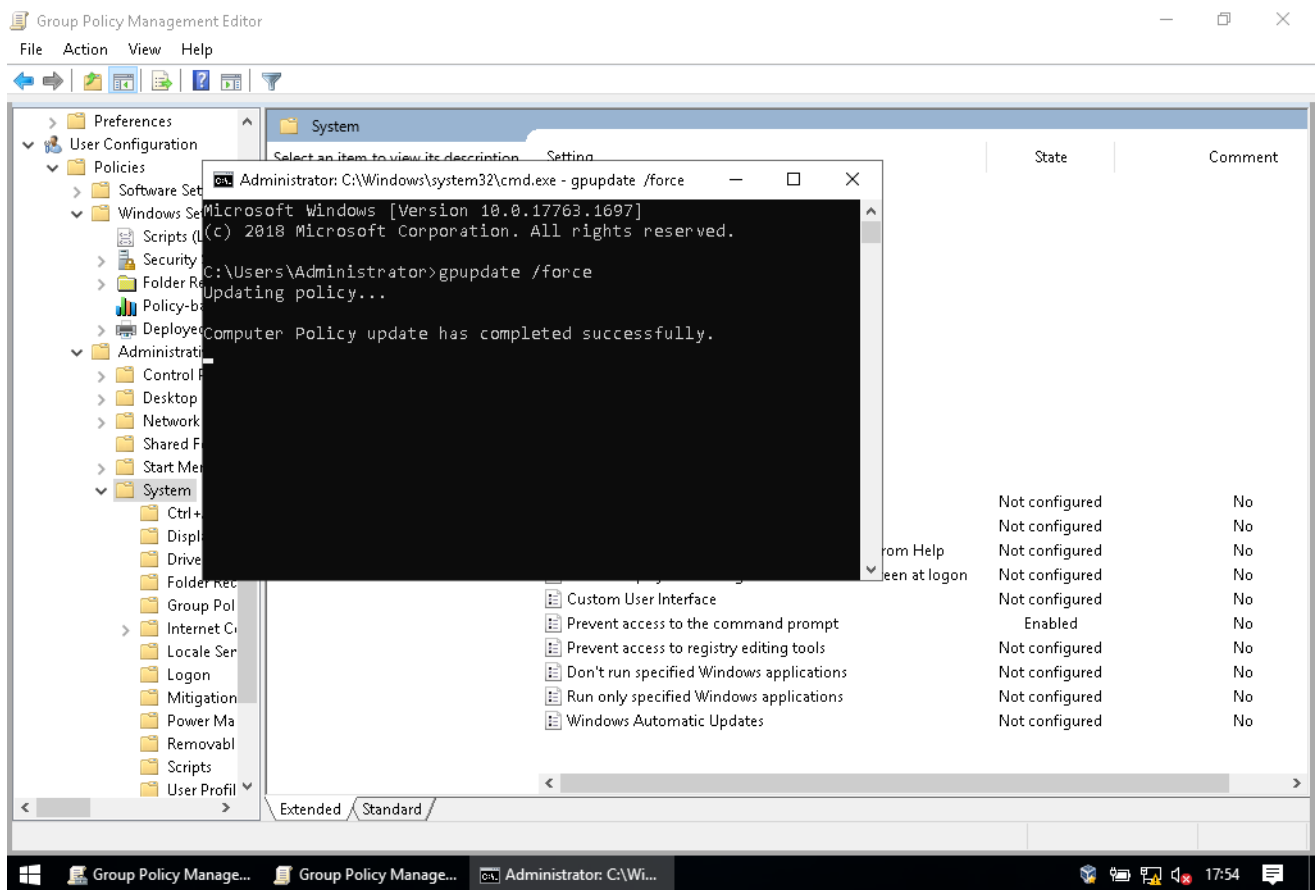
A new group policy object was created by the name of 'NoCmdPromptAccess' as directed by the brief:



The 'Prevent access to the command prompt' setting is located.

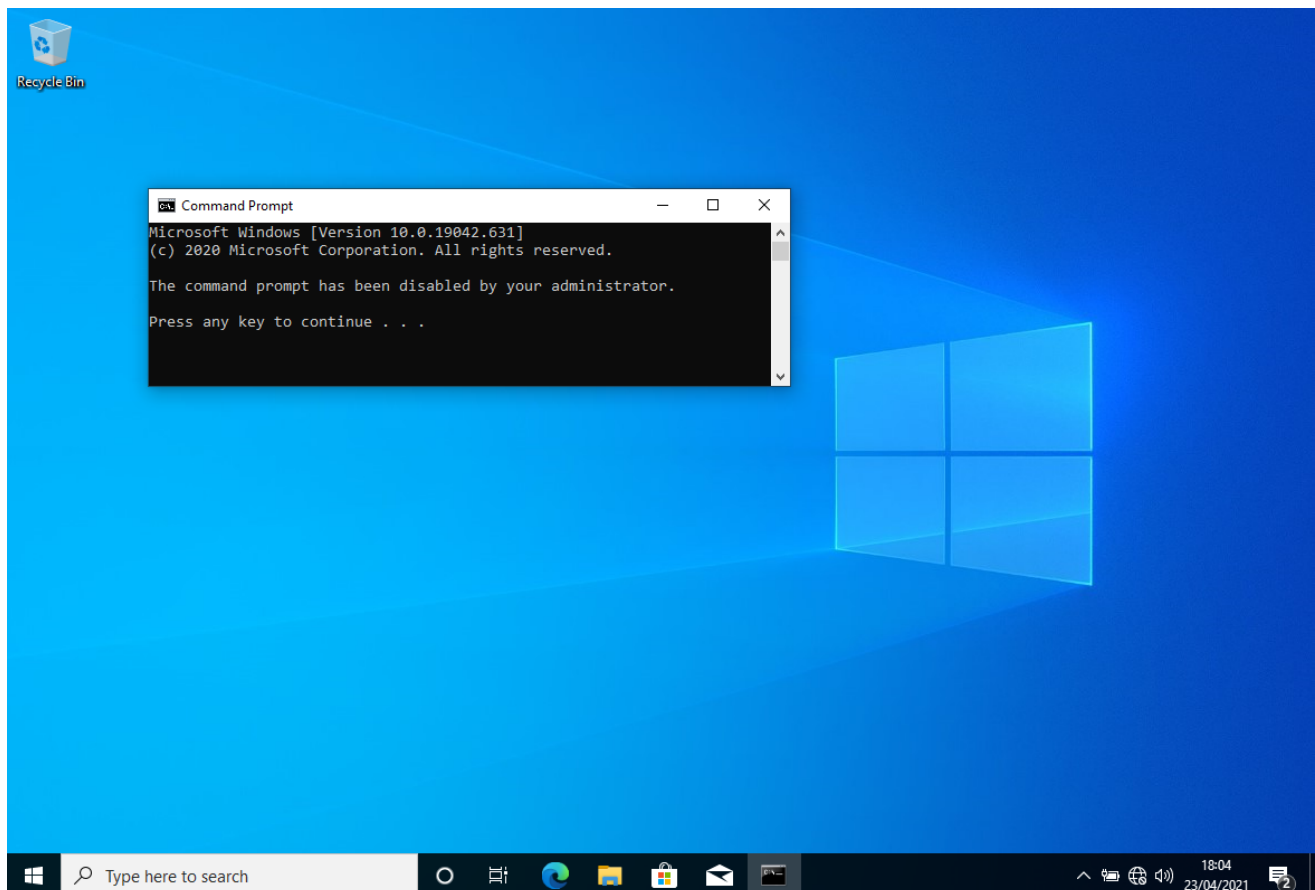


And the setting itself is enabled and applied.



And the `gpupdate /force` command is run to force a group policy update again.

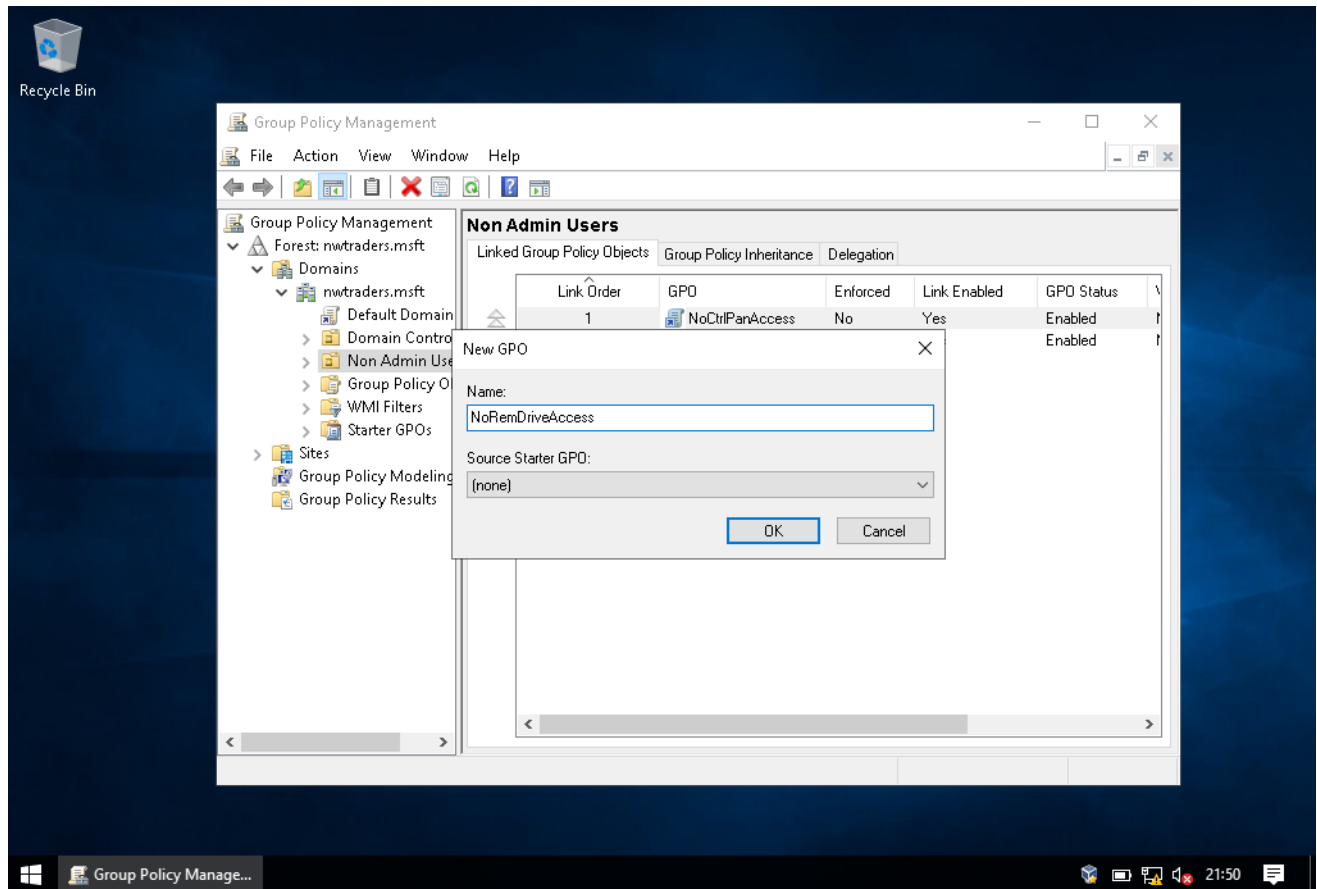
When attempting to run the command line on Client 1:



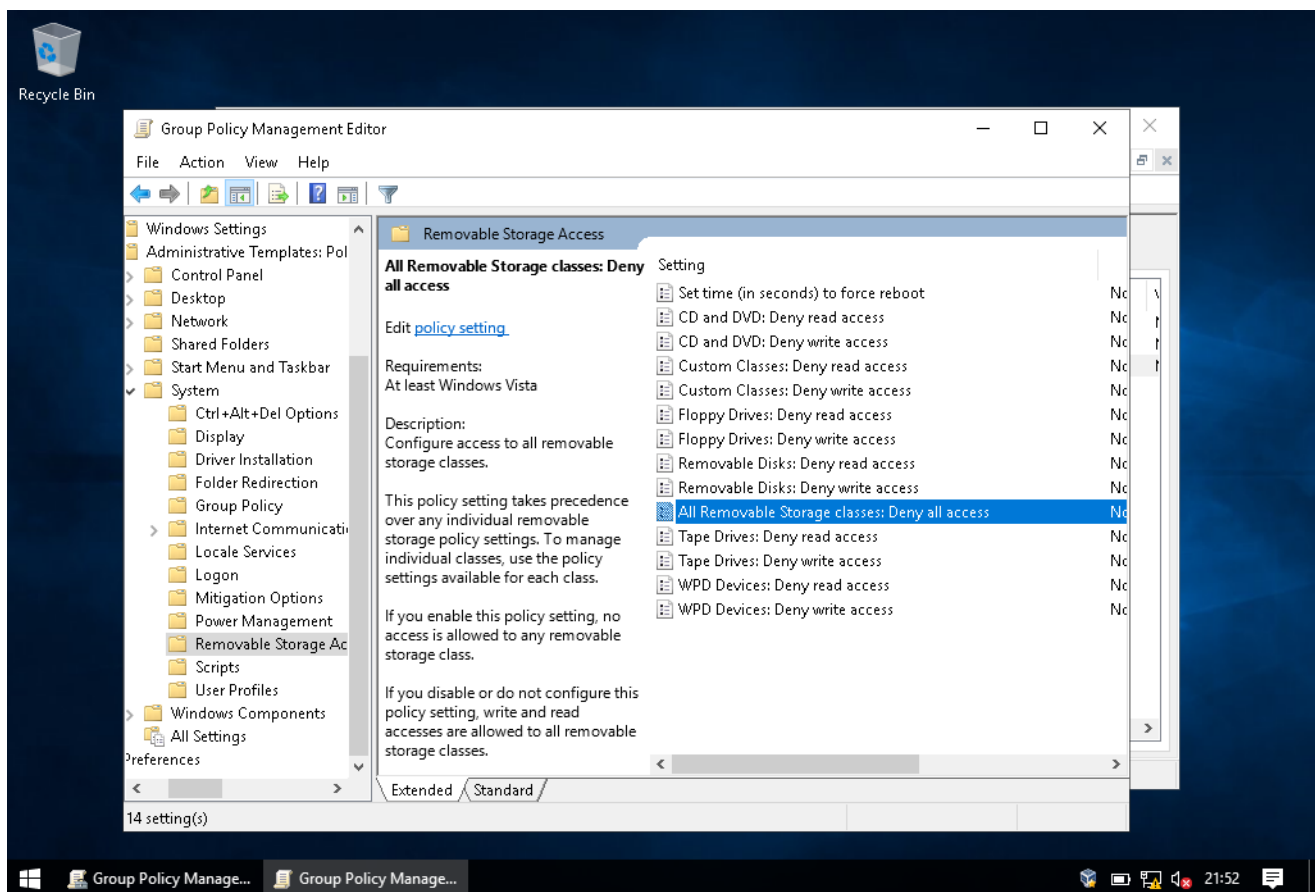
The command prompt is disabled, and cannot be used.

Restricting access to removable media drives

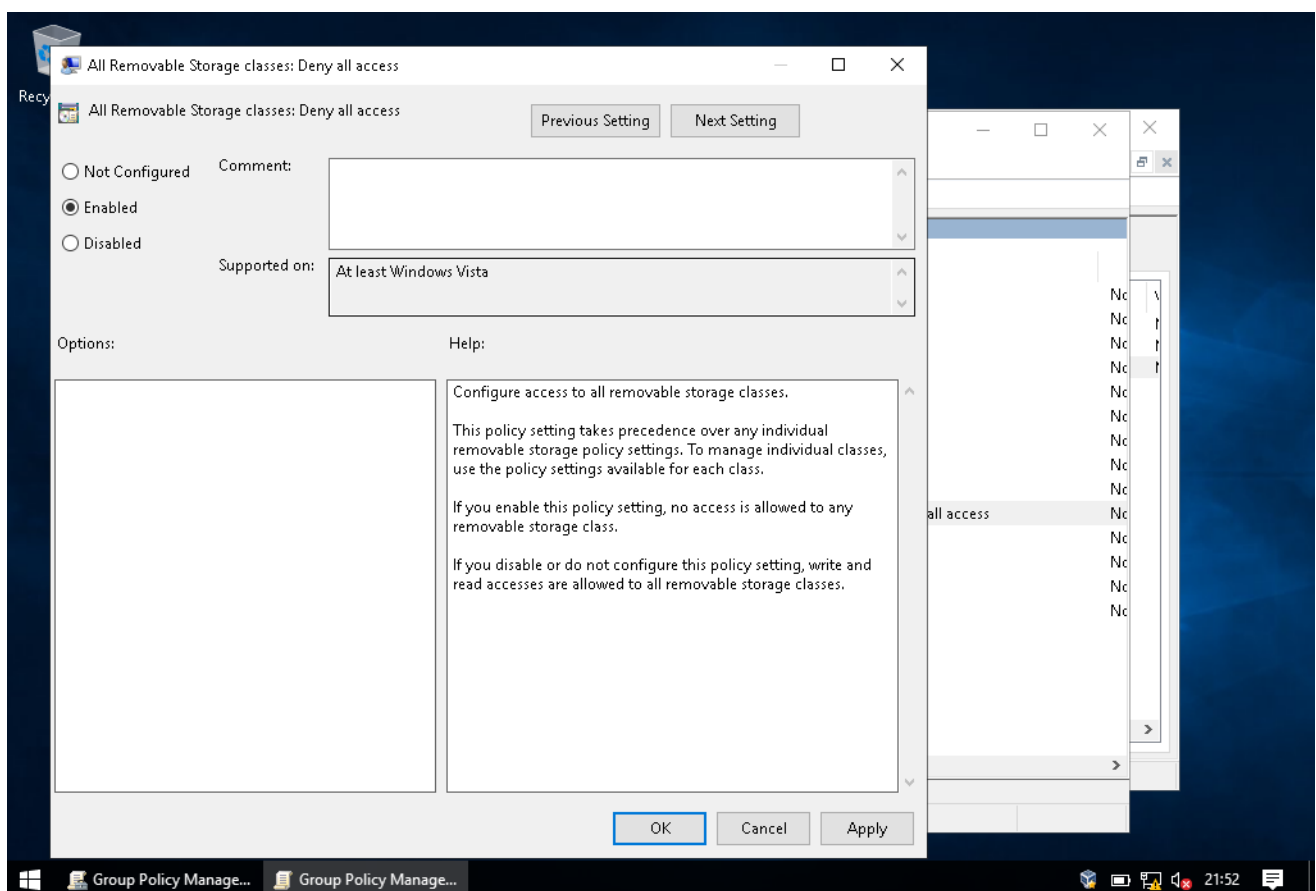
Restricting access to removable media drives will tighten system security, removable drives may contain malware or backdoor trojans. Restricting access to removable drives also protects against data theft.



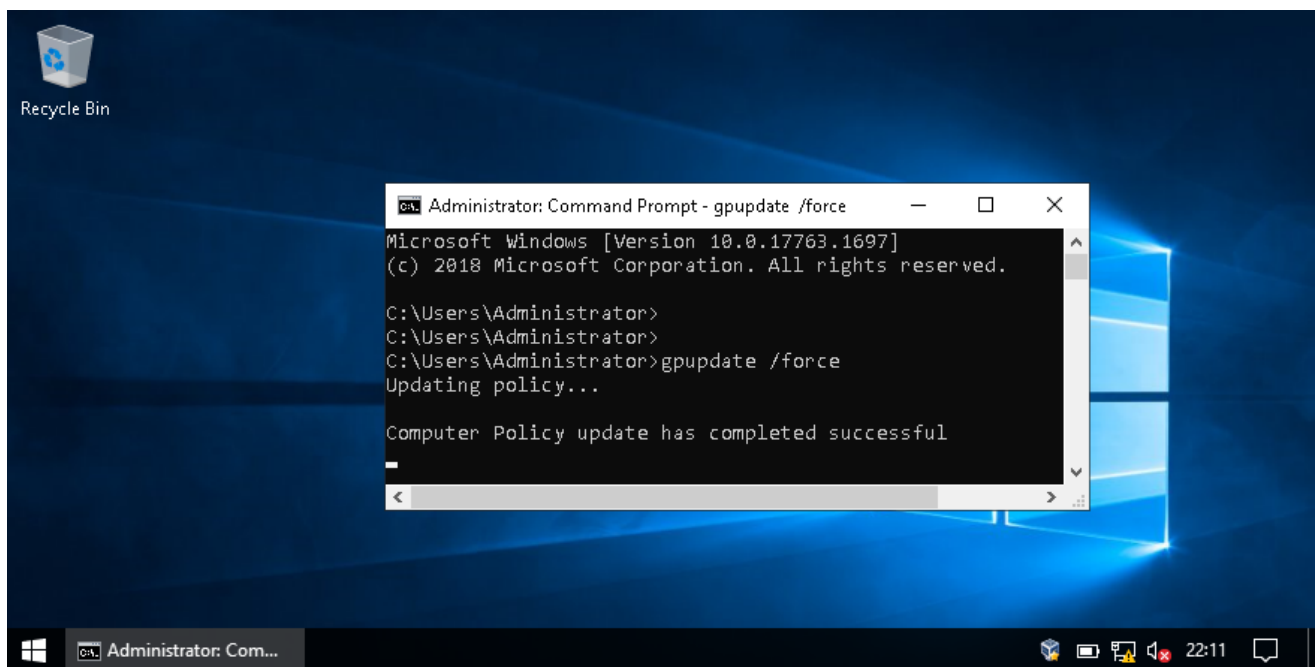
A new GPO named 'NoRemDriveAccess' is created.



The 'All Removable Storage classes: Deny all access' setting was located.



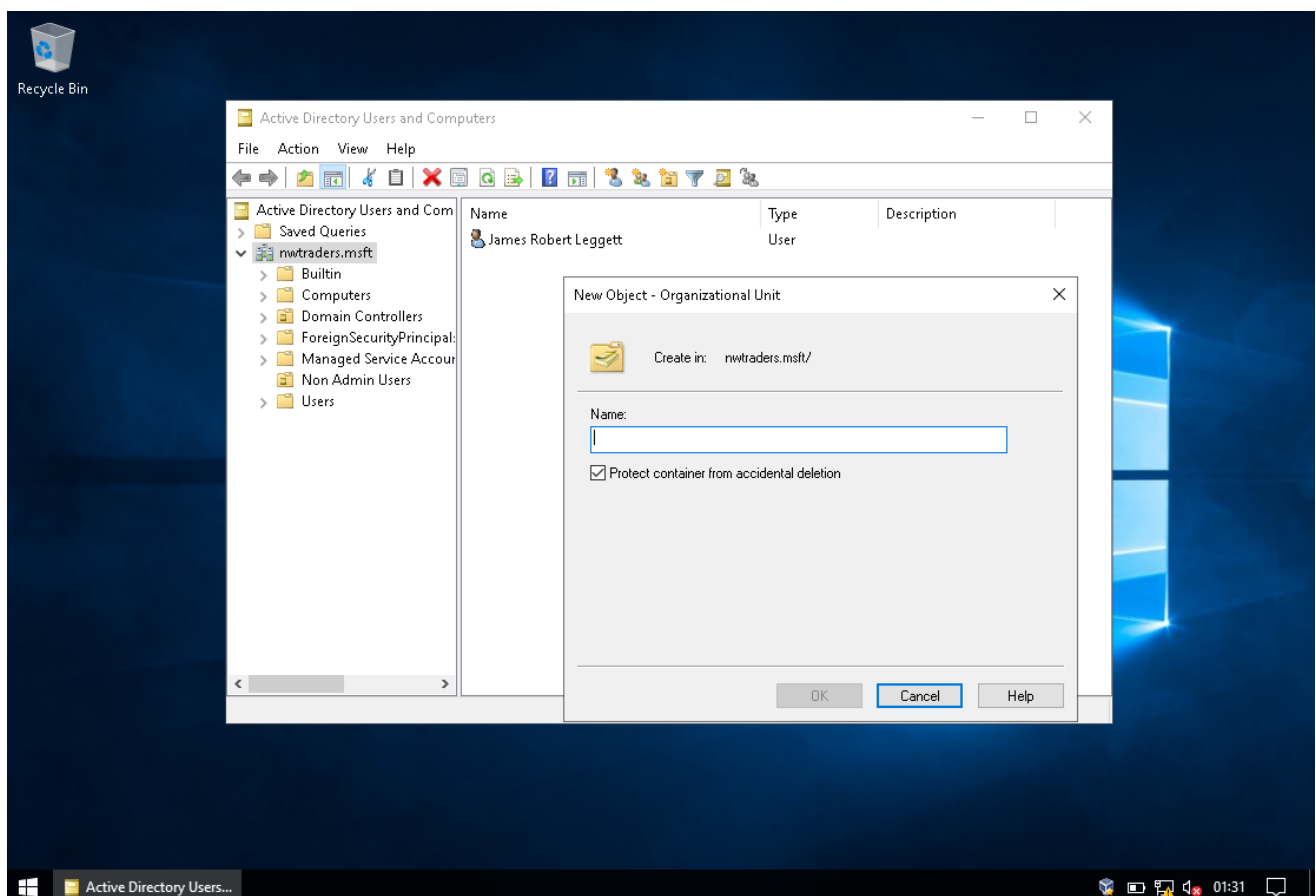
The setting was enabled.



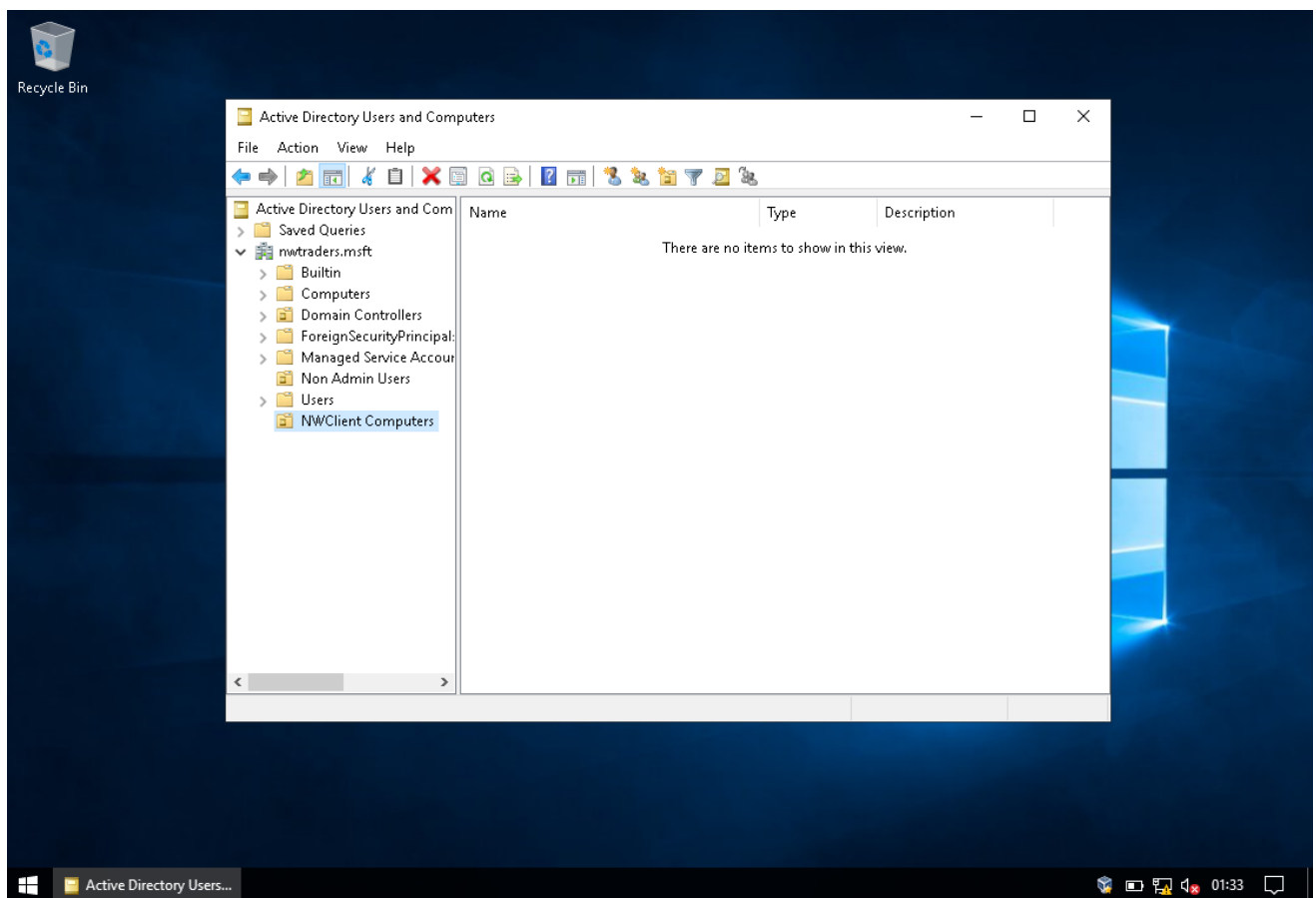
The `gpupdate /force` command was launched and completed successfully.

The author was unable to get this to work, even after disabling several removable storage policies, restarting the client PC and using the update command, the non admin user was able to open the VirtualBox Guest addons disk, and all other removable hardware. As for external USB storage devices, they simply didn't appear. Neither did floppy disks or external drives.

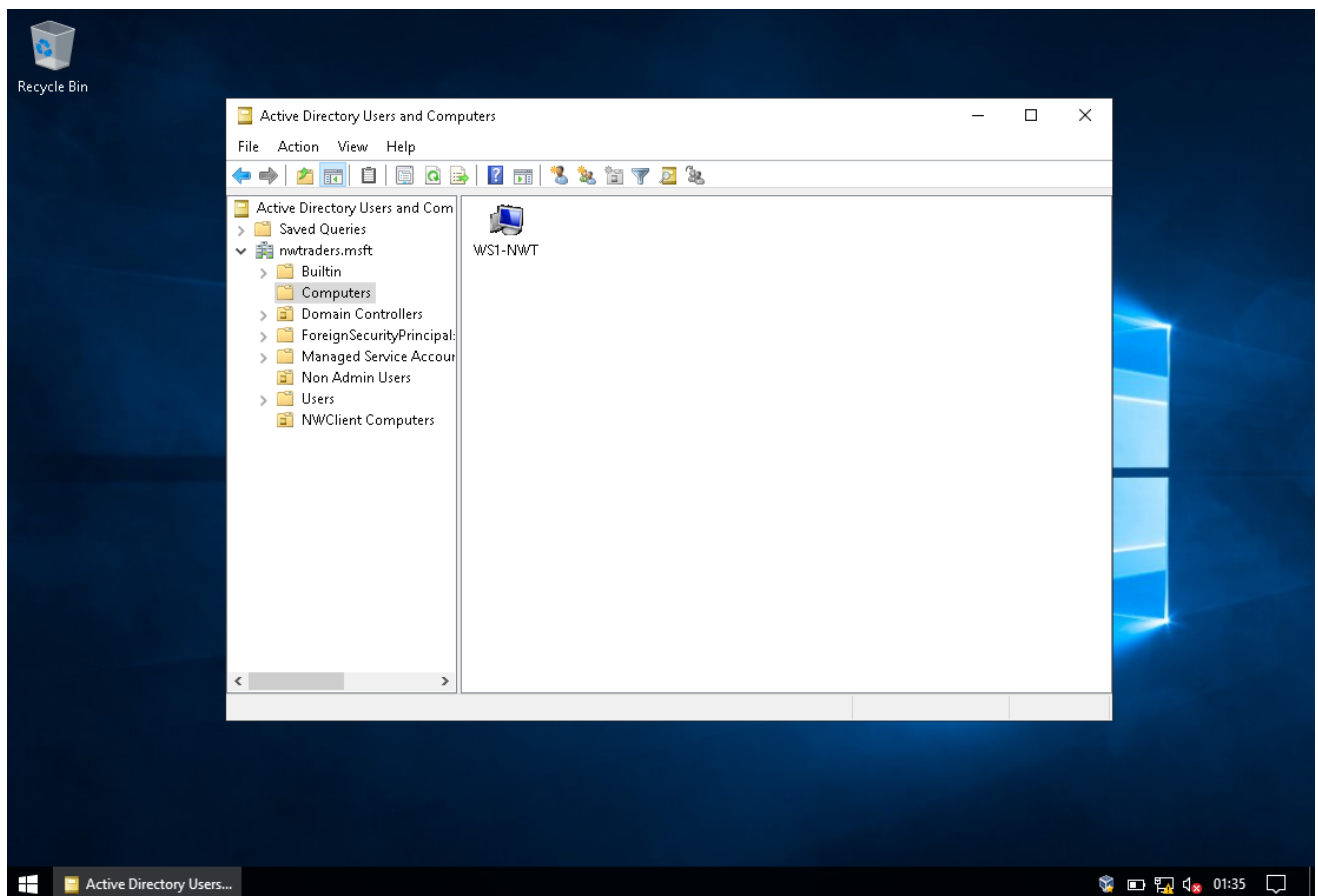
Restricting software installs



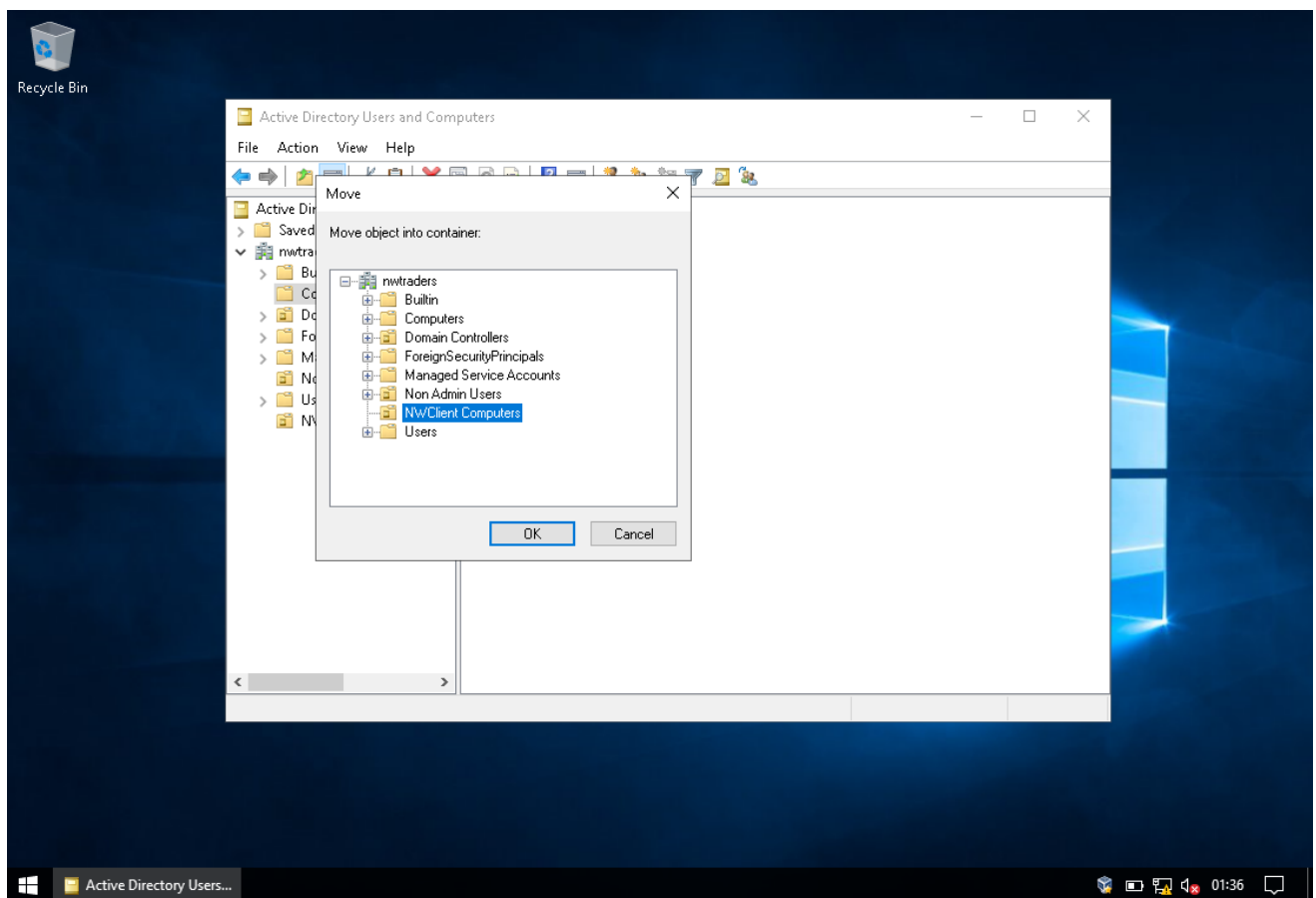
A new Organisational Unit will be created as instructed by the brief.



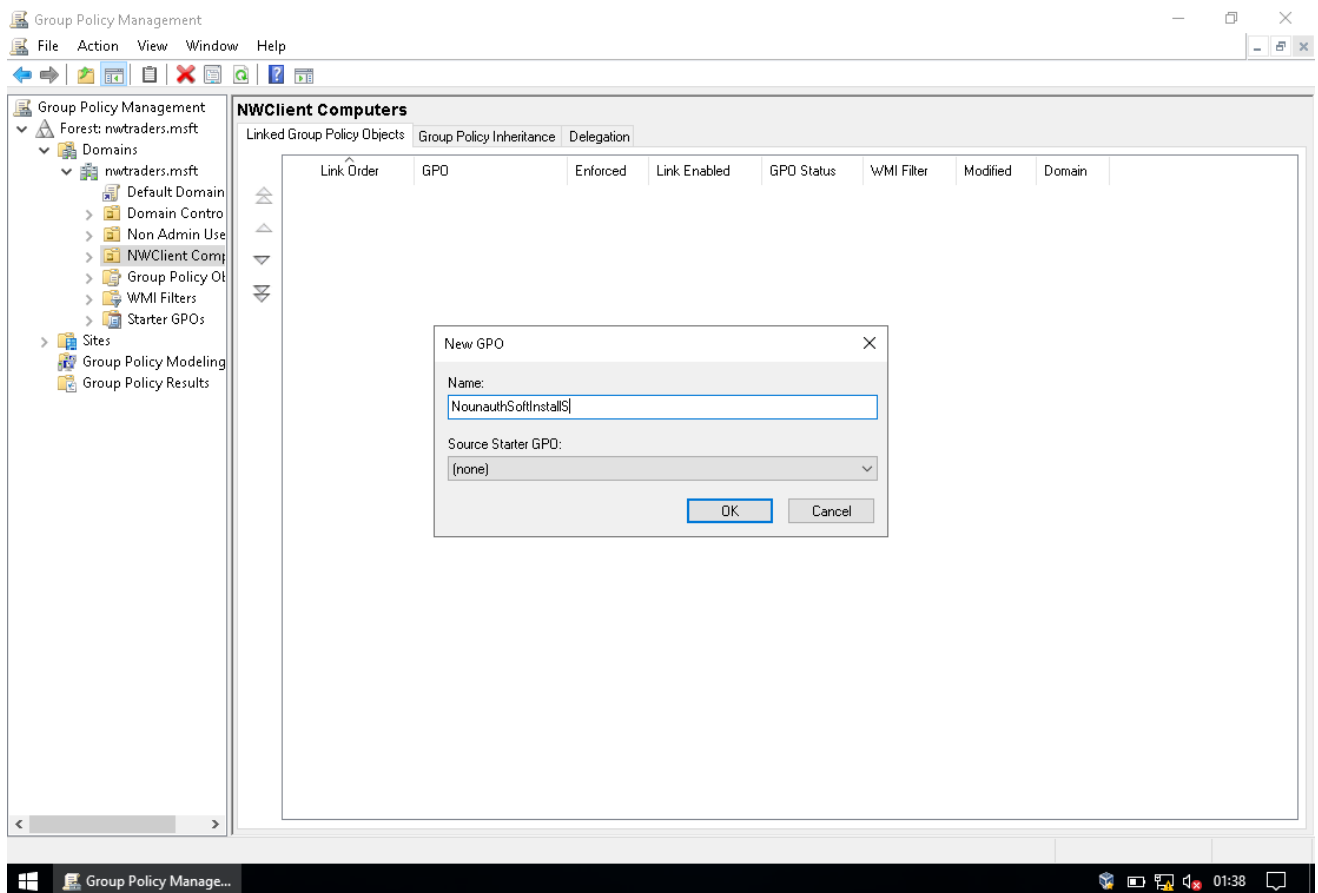
The “NWClient Computers” organisational unit has been created successfully.



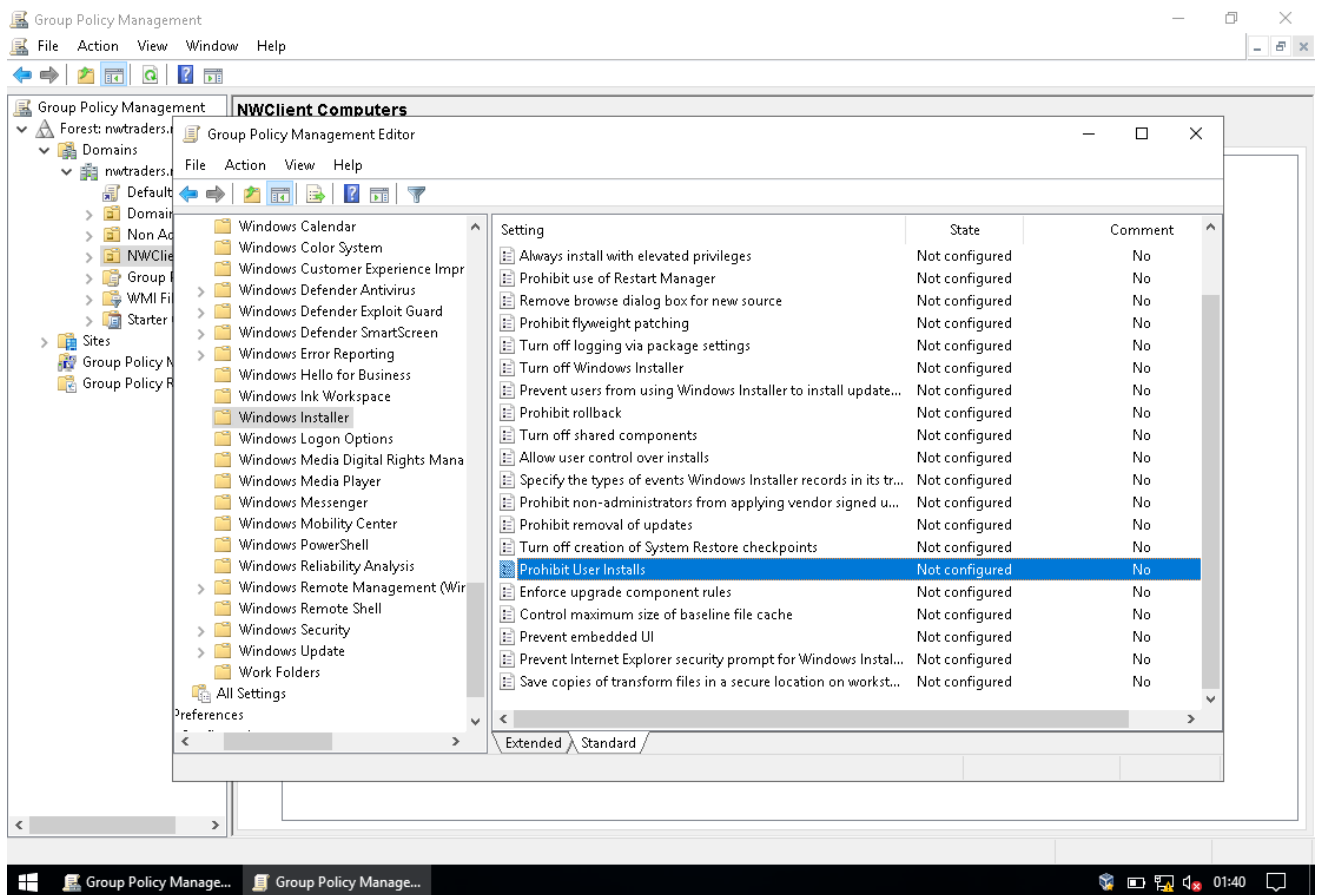
A computer is located in the “Computers” folder, which is the Client computer.



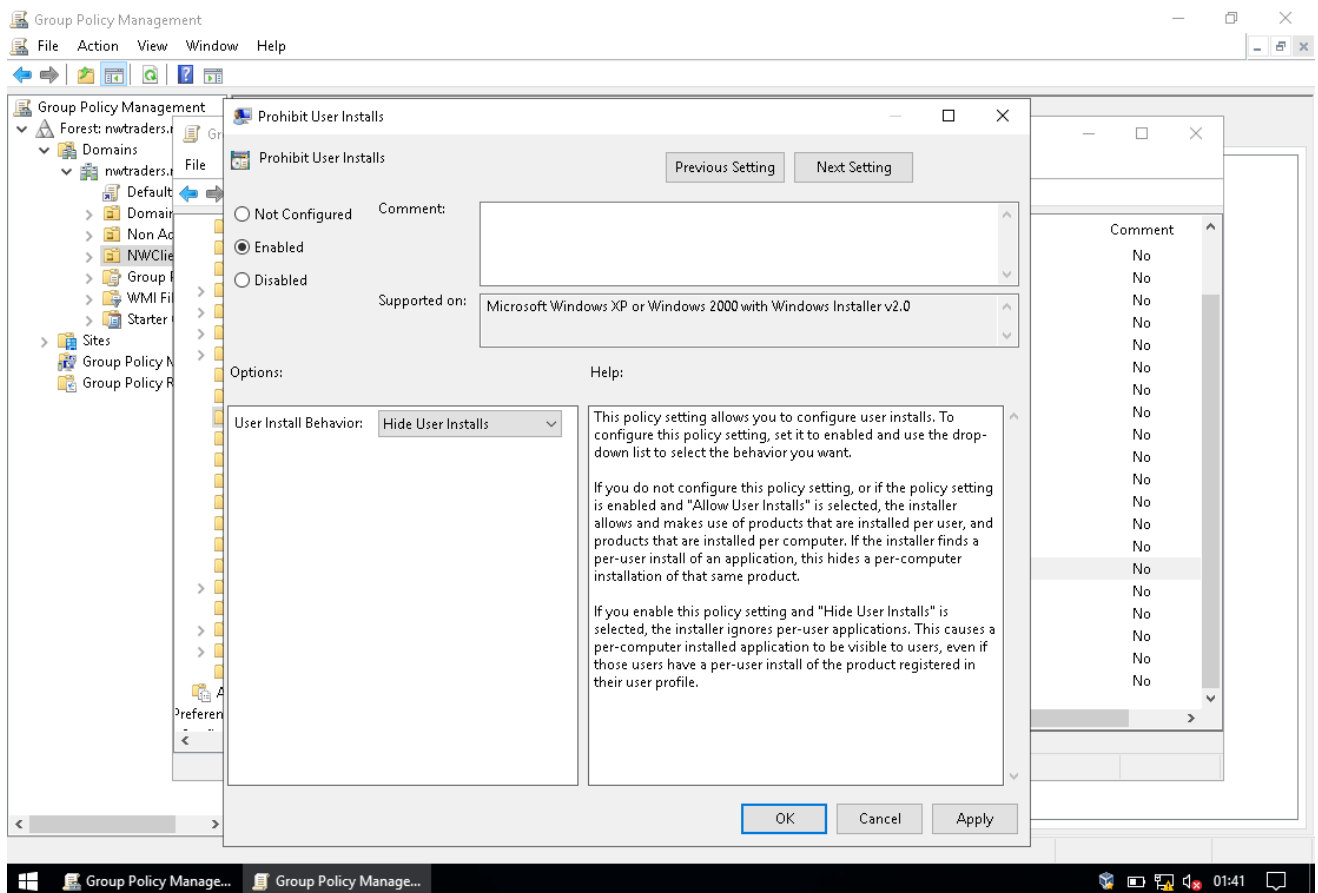
The author will now move said client to the NWClient Computers organisational unit.



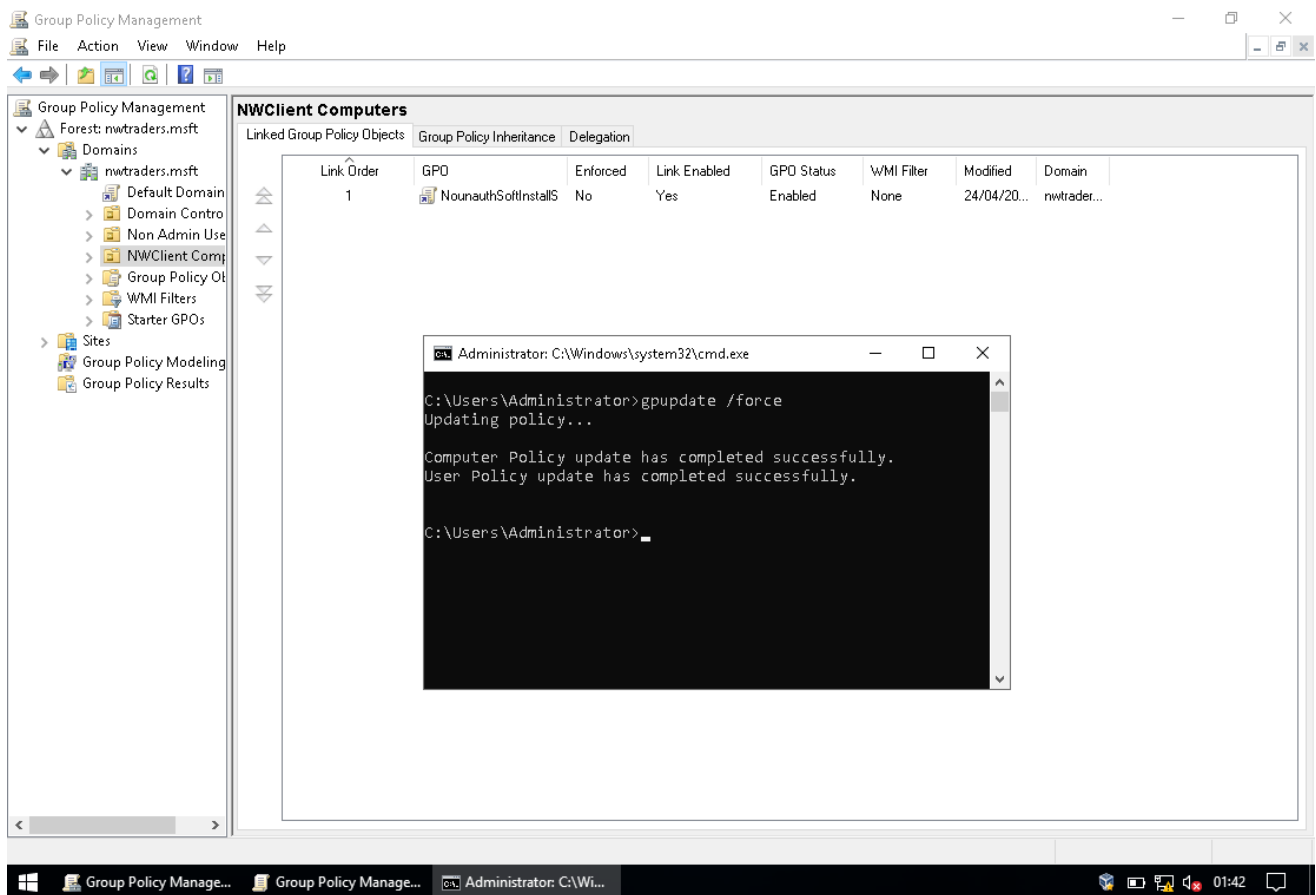
A new group policy object will be created, named 'NounauthSoftInstallS' respectfully.



The 'Prohibit User Installs' setting is located successfully.

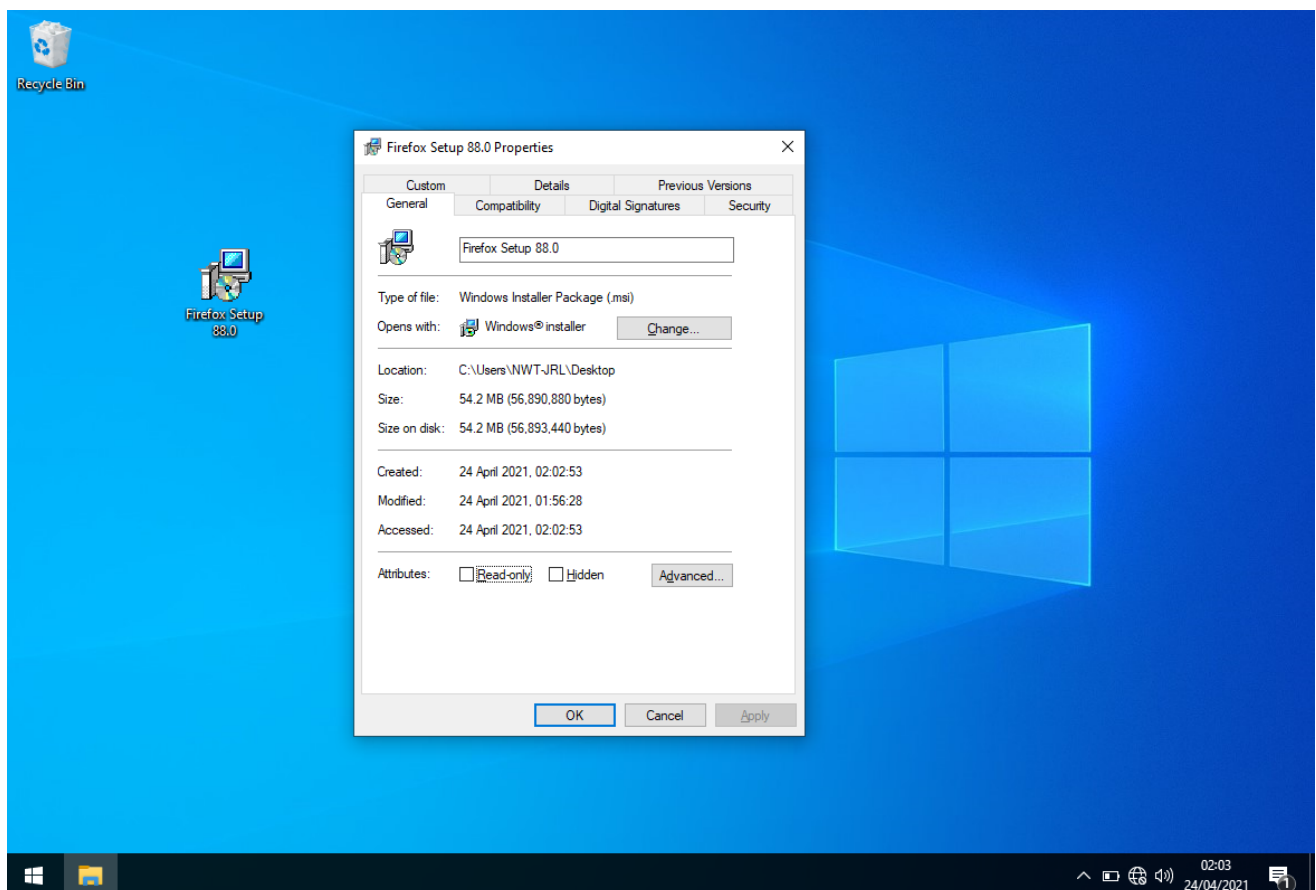


The 'Prohibit User Installs' setting is now enabled.

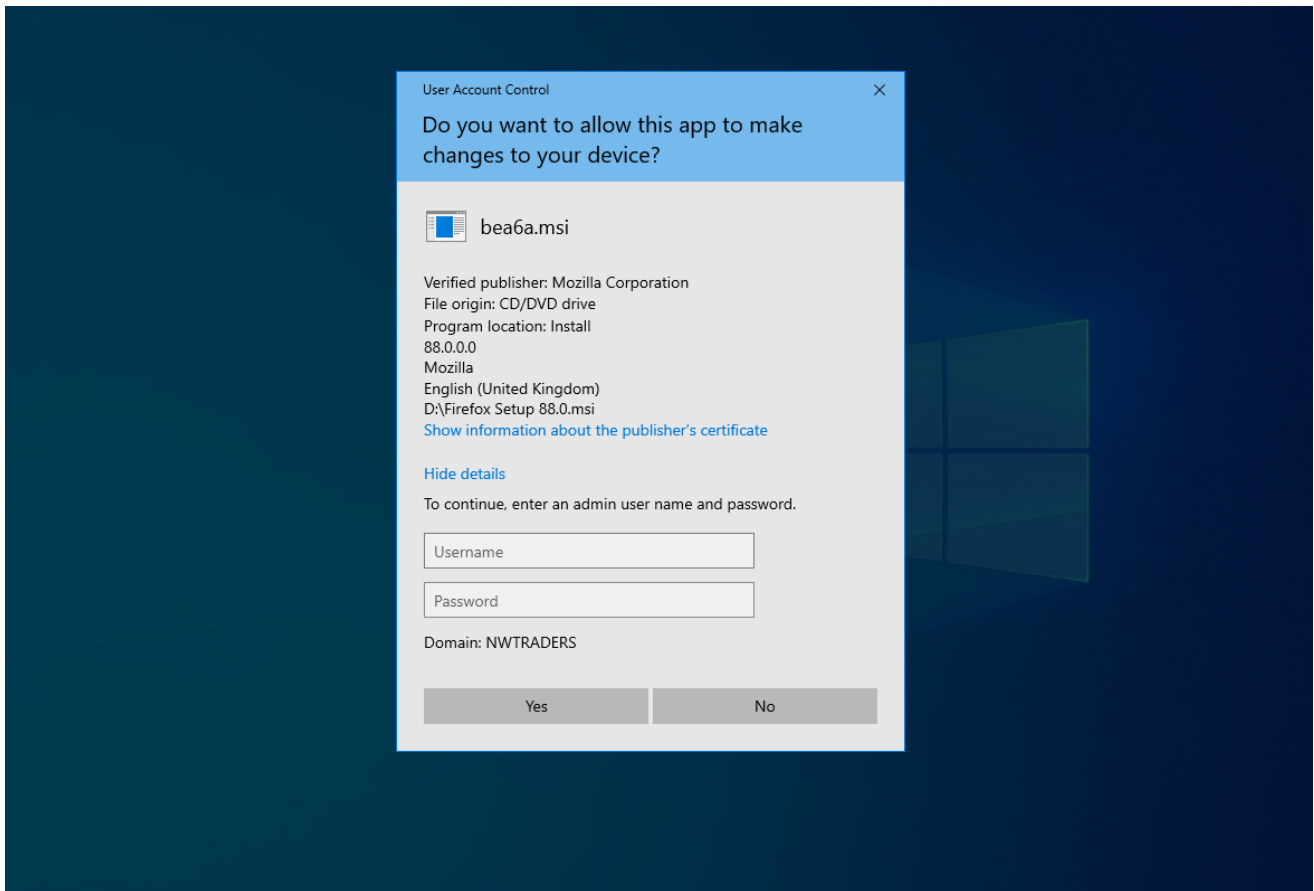


The `gpupdate /force` command is successfully run and the update is completed.

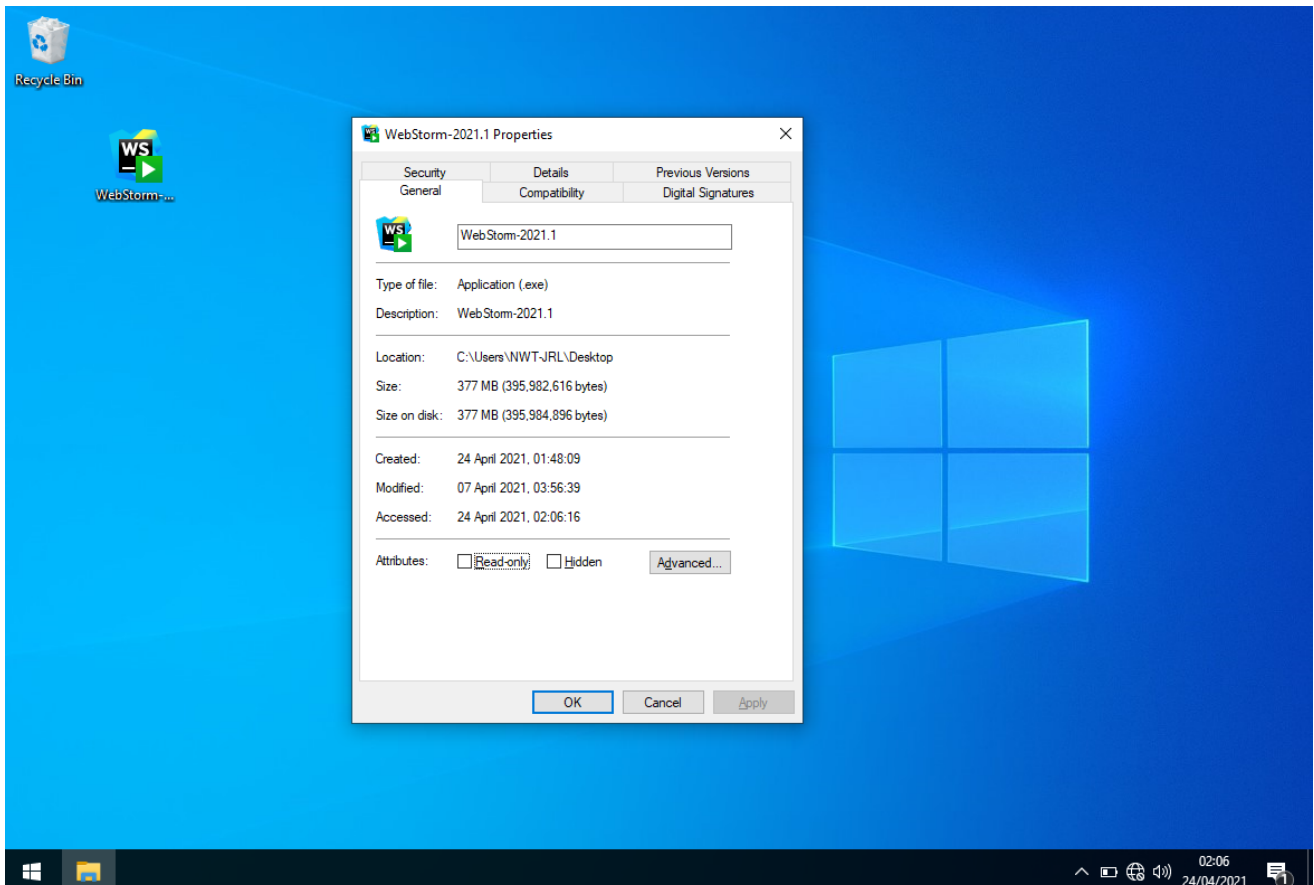
// Switching to the Client //



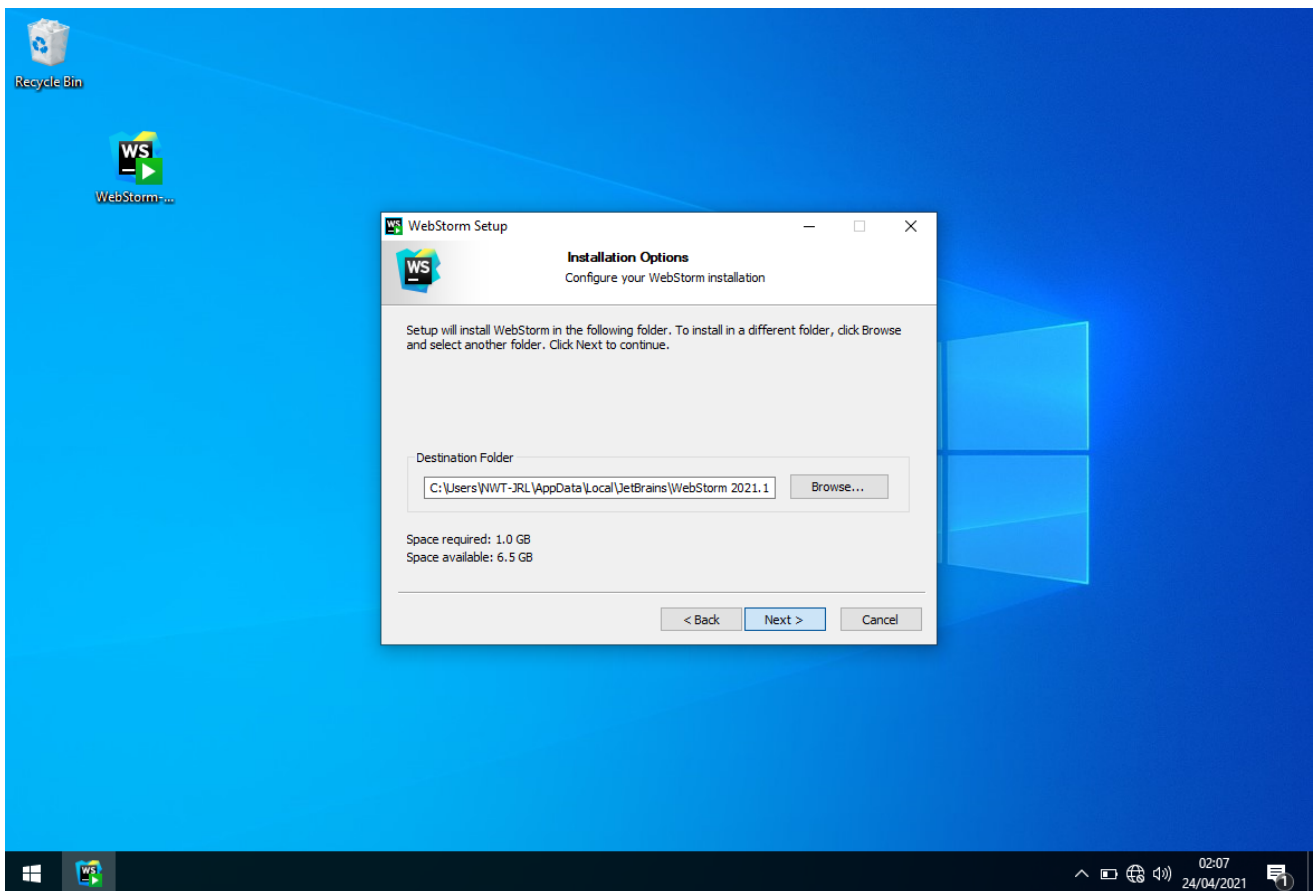
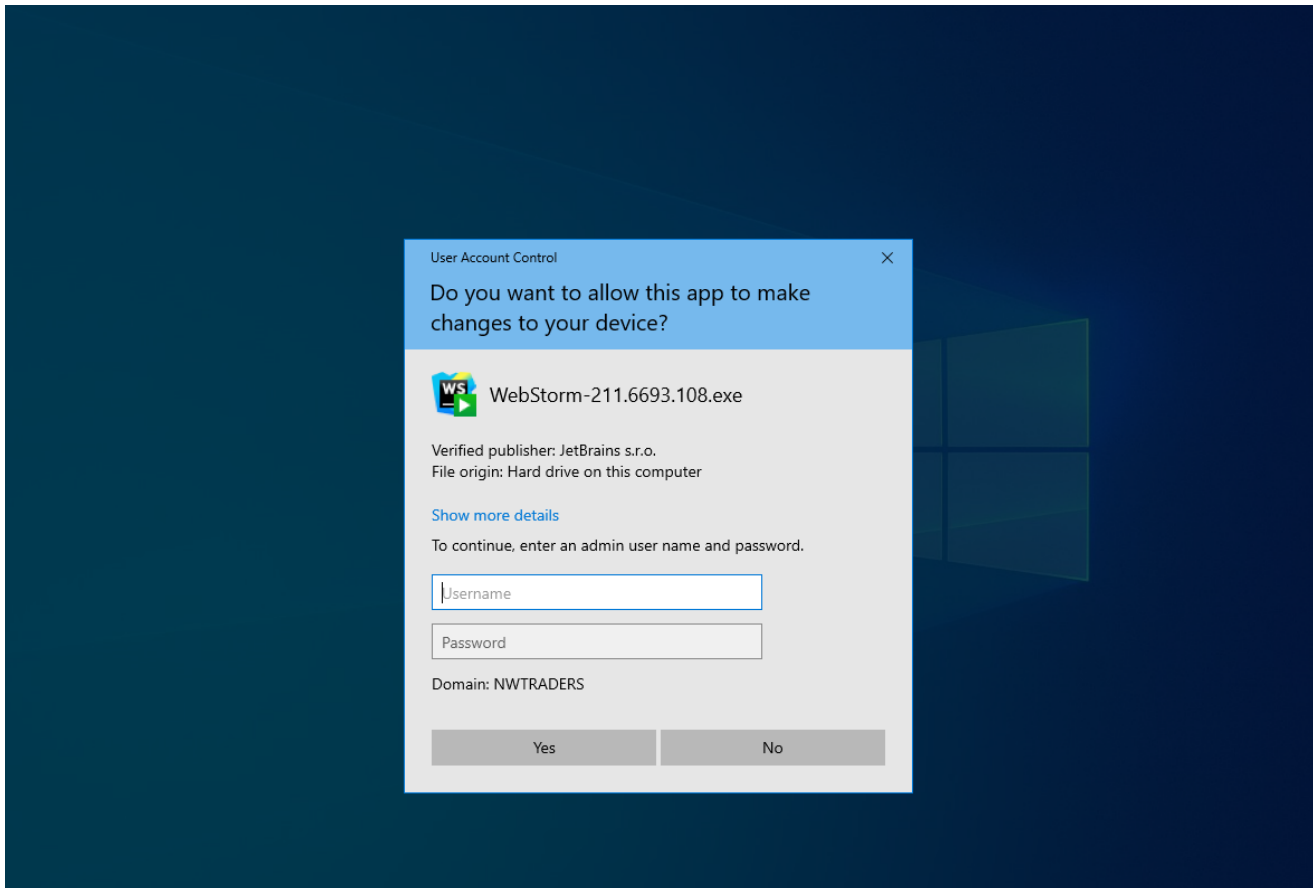
On the desktop, imported from the host, is an MSI file using the Windows Installer for the Firefox Browser. When opening the installer, the installer immediately asks for admin rights:



When the user clicks 'no' the installer exits and nothing happens.

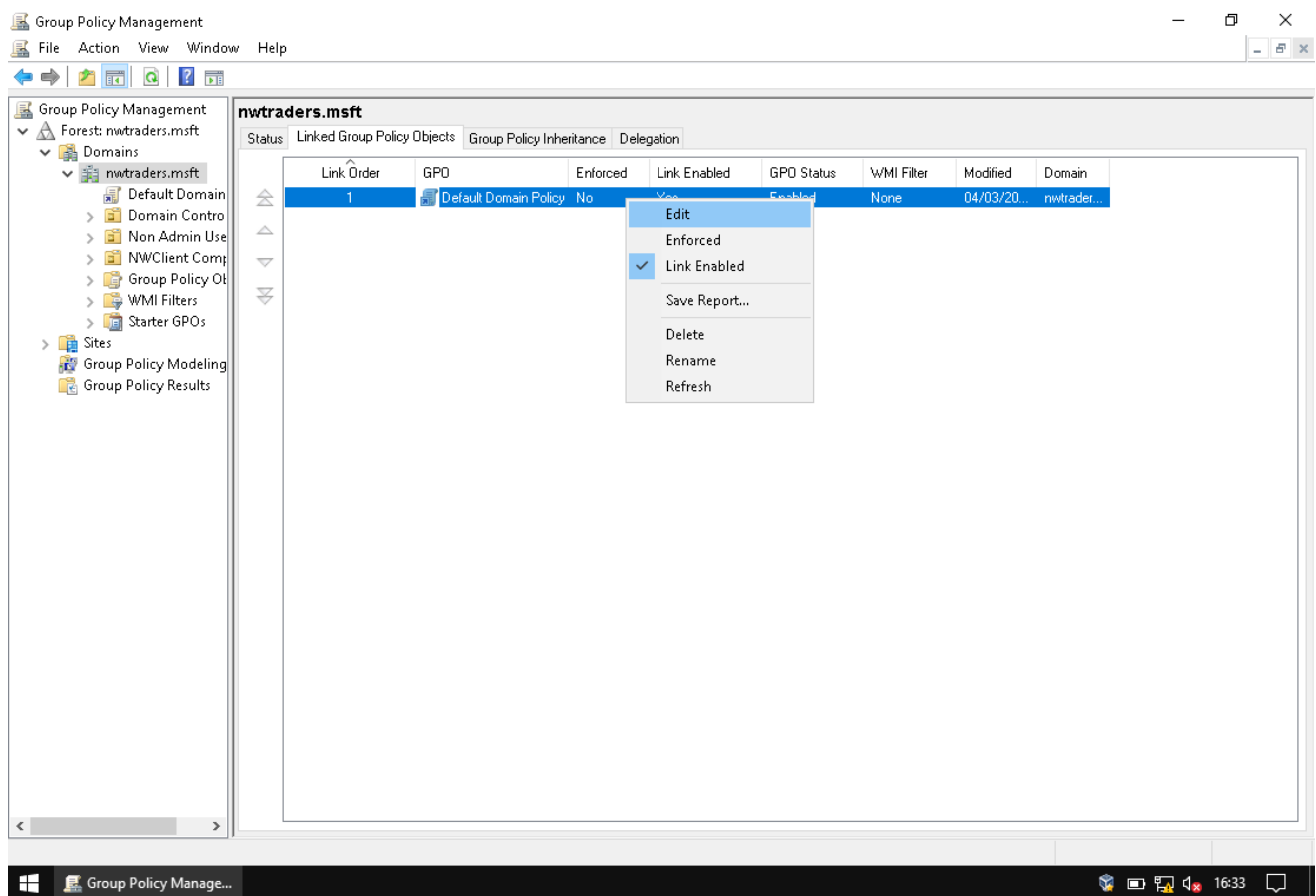


On the desktop there is also an executable that installs Web Storm. When running this installer, it also immediately asks for admin rights:

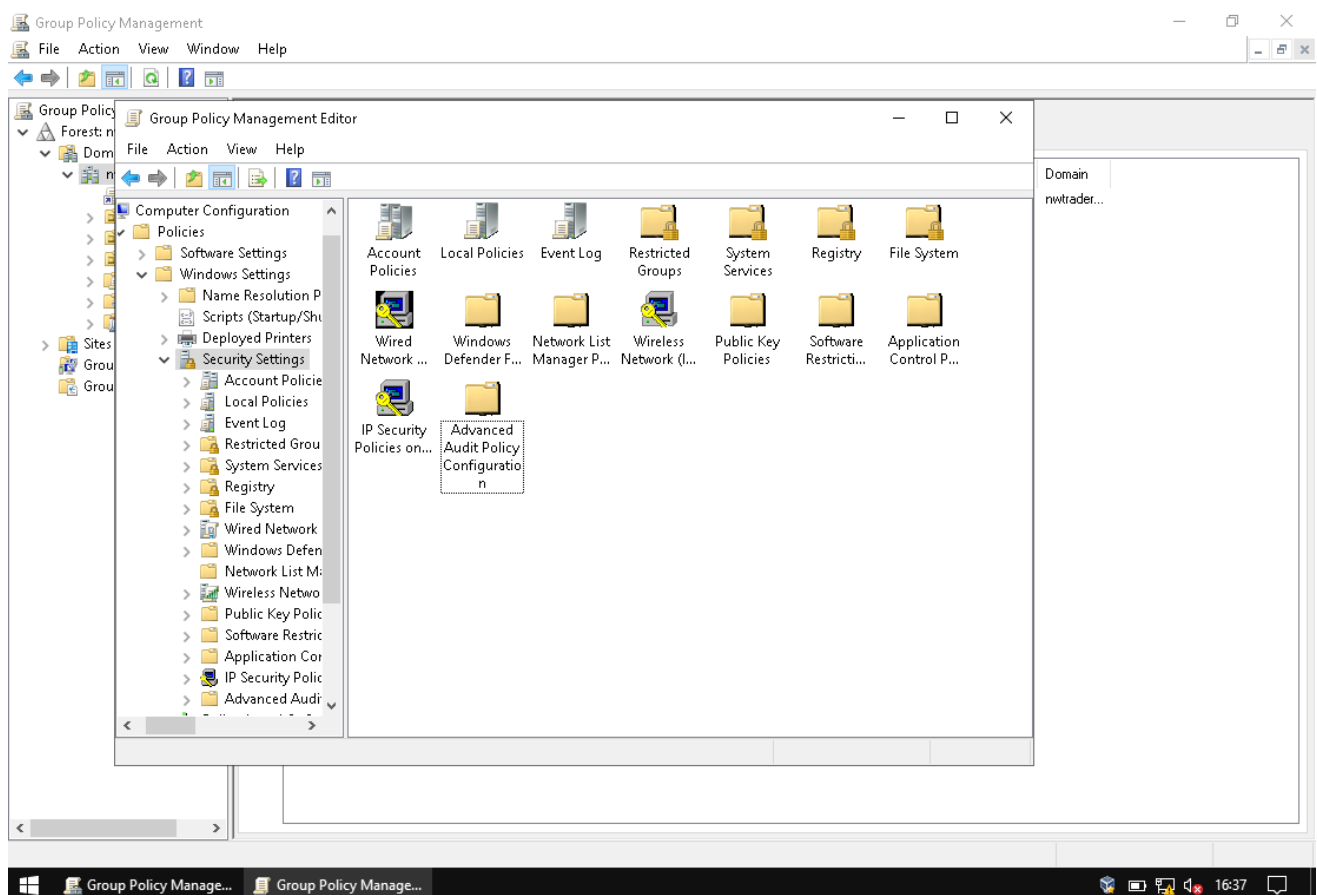


When the user clicks no, the installer runs anyway, but the Next button doesn't do anything at all and the user cannot proceed.

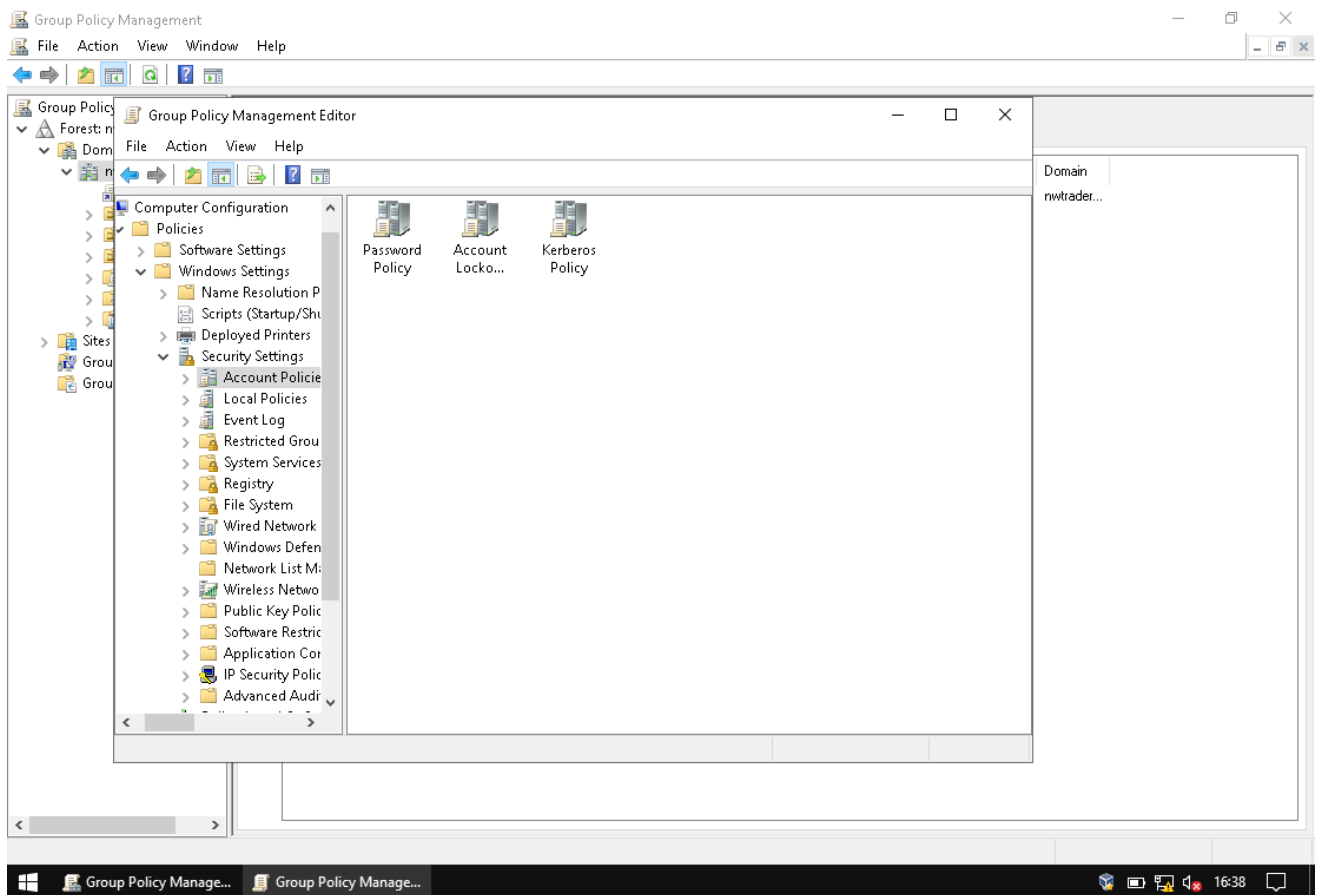
Enforcing Password Policy in the 'nwtraders.msft' domain



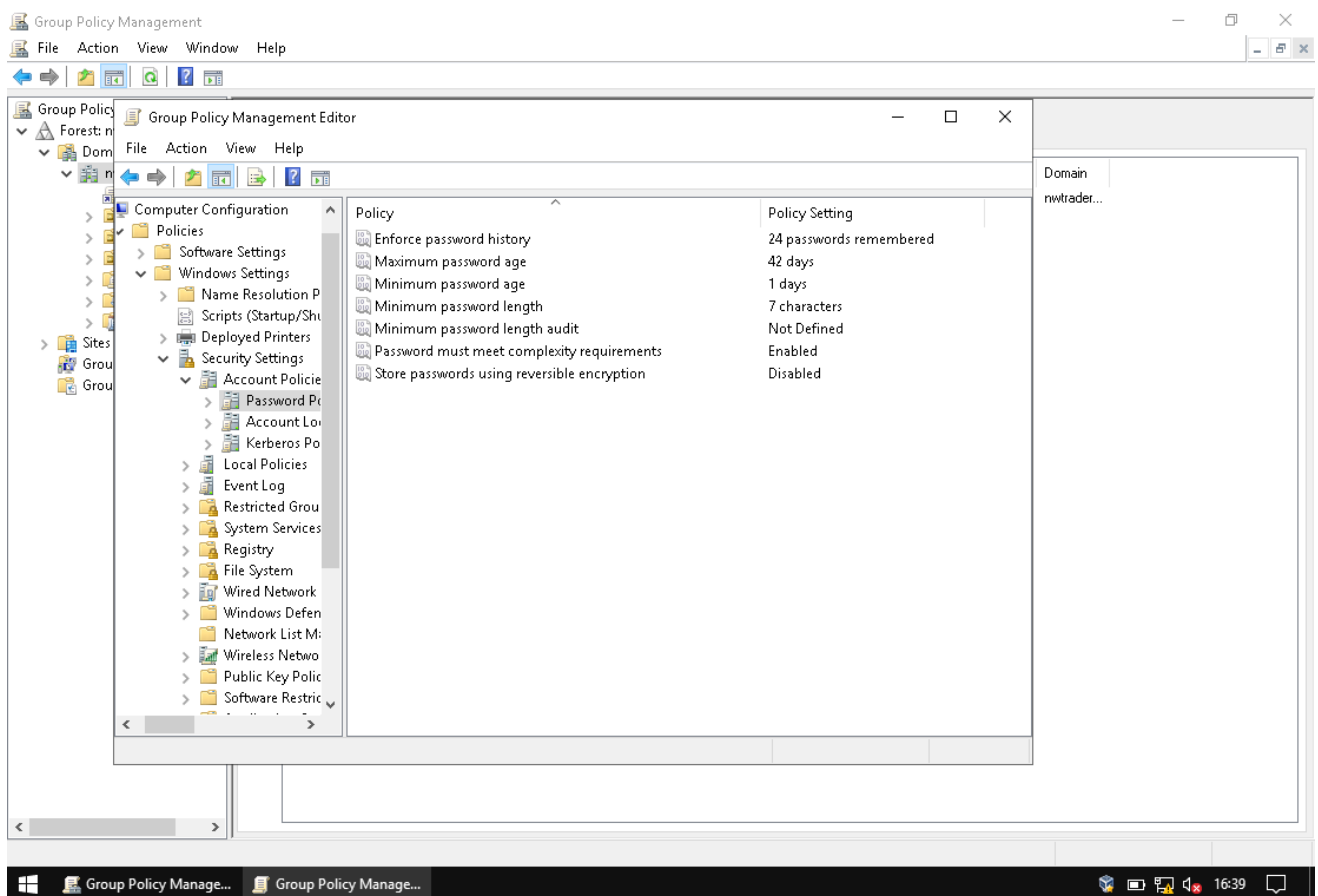
For enforcing a password policy, the author will edit the Default Domain Policy using Group Policy Management.

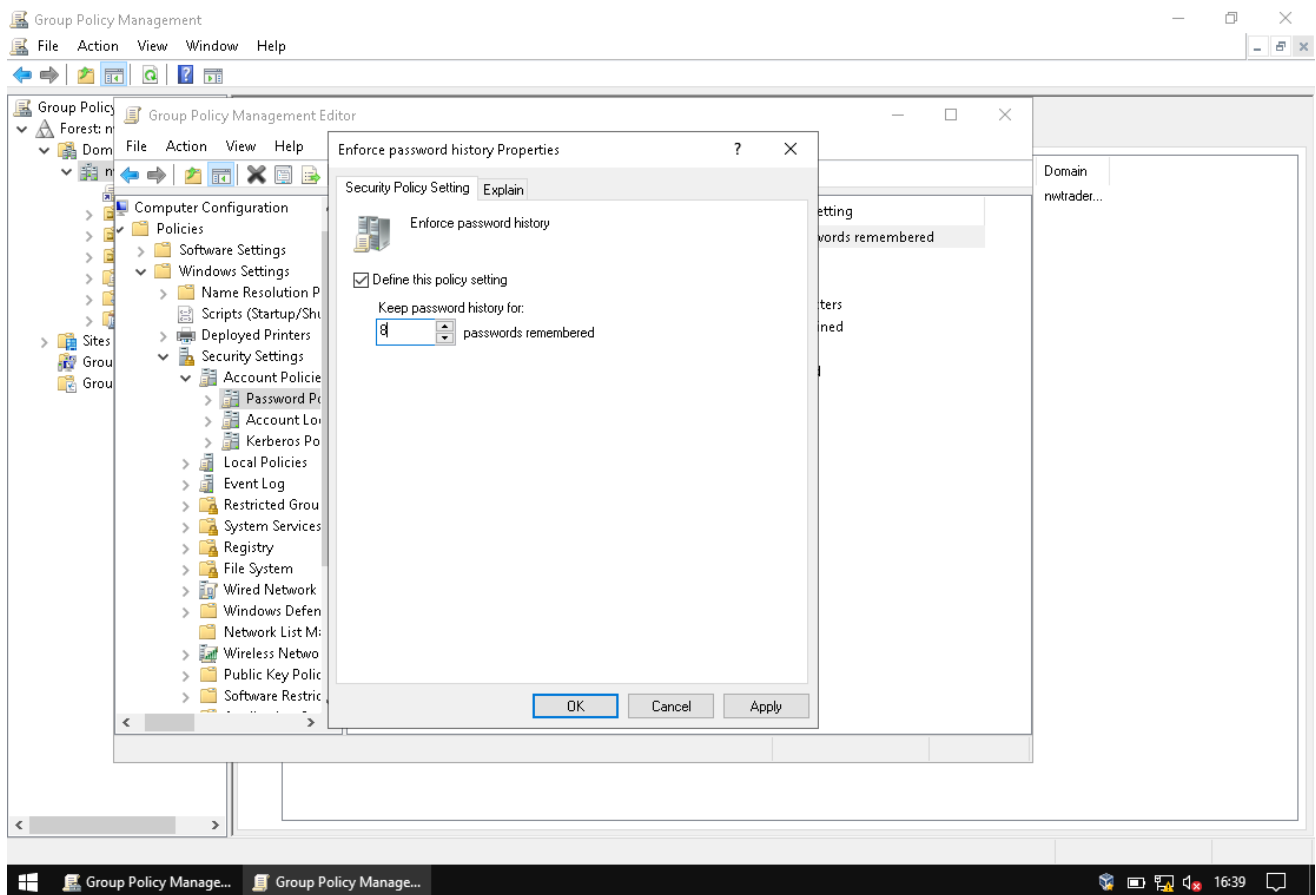


The author navigated to 'Security Settings'.

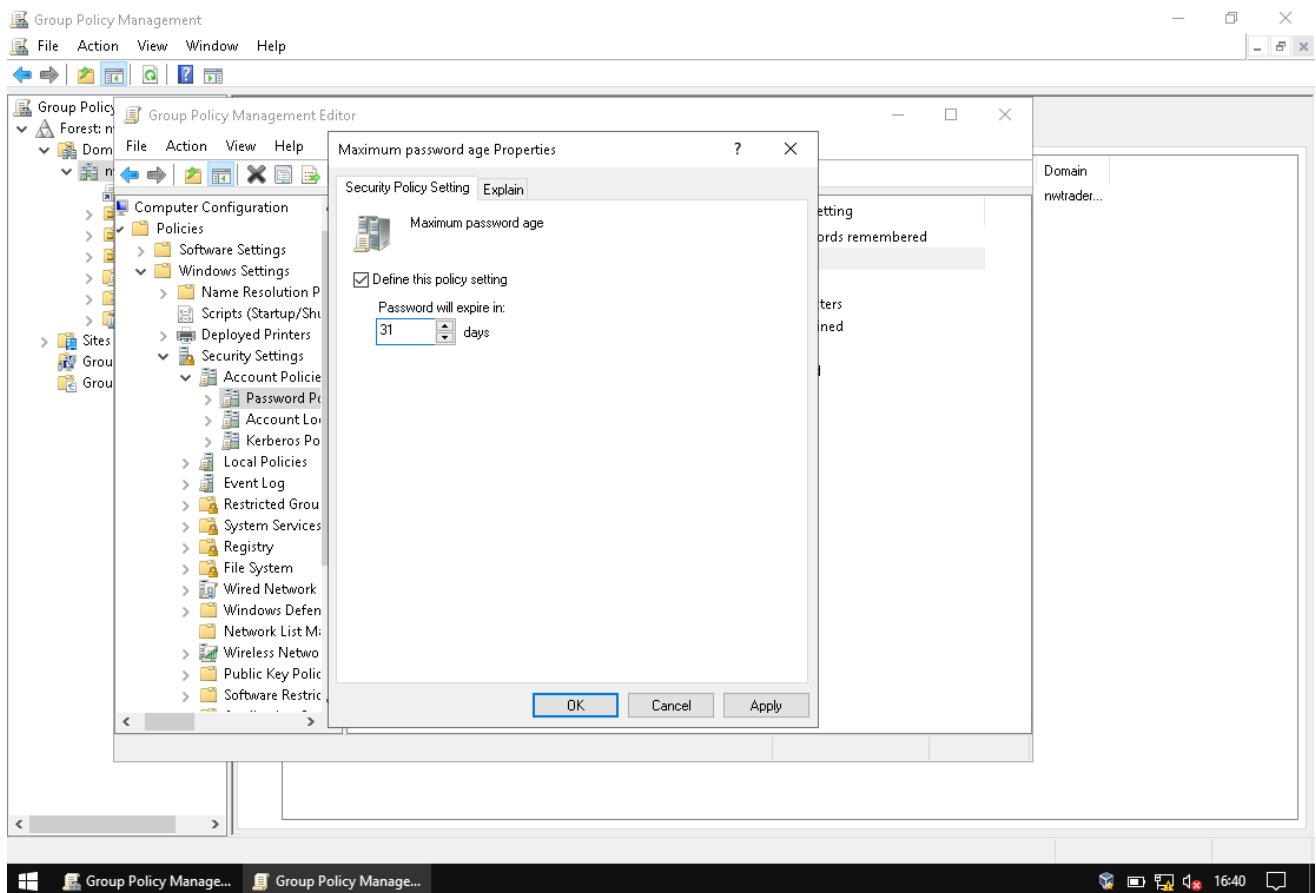


The author navigated to 'Account Policies'. Inside the folder were 3 objects, the author navigates to 'Password Policy'.

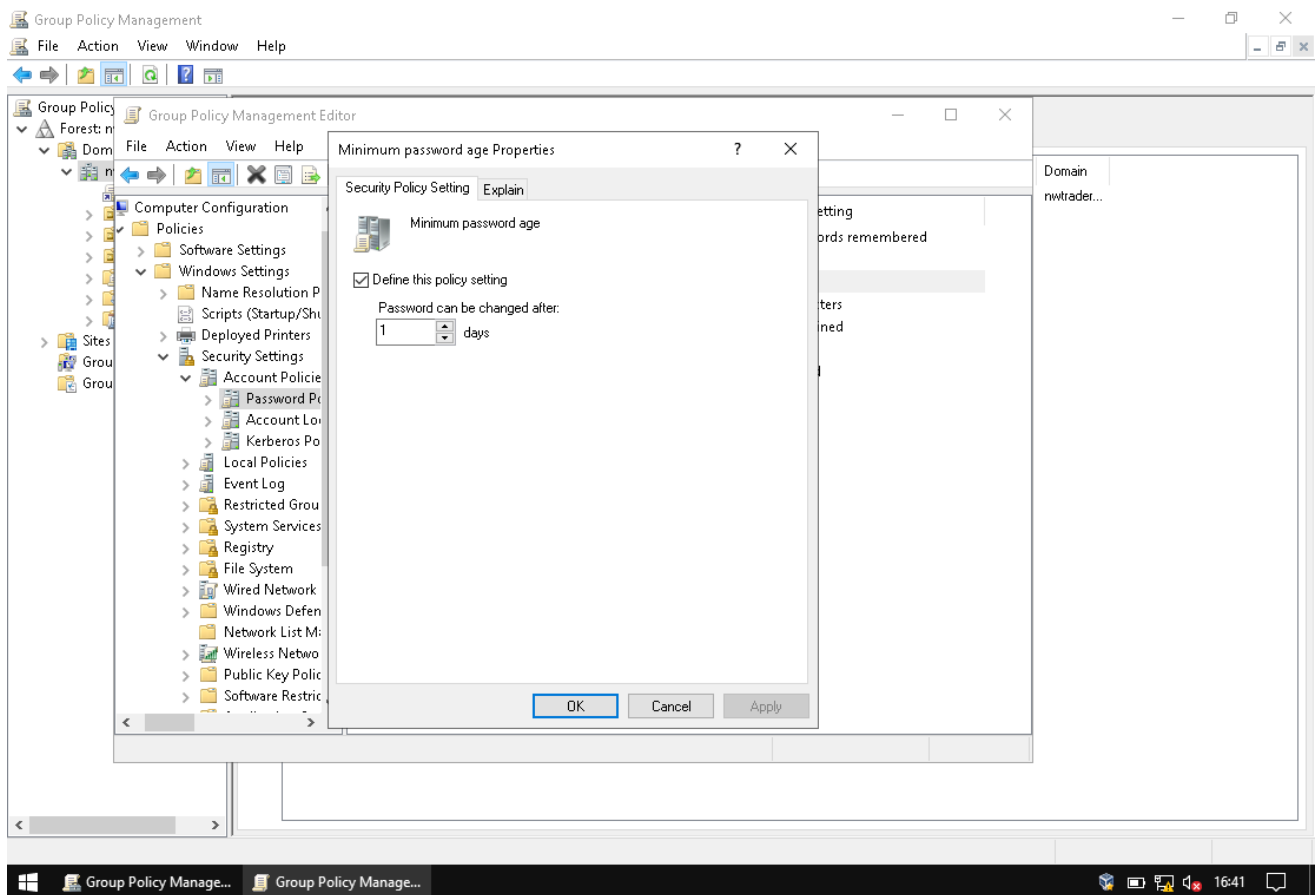




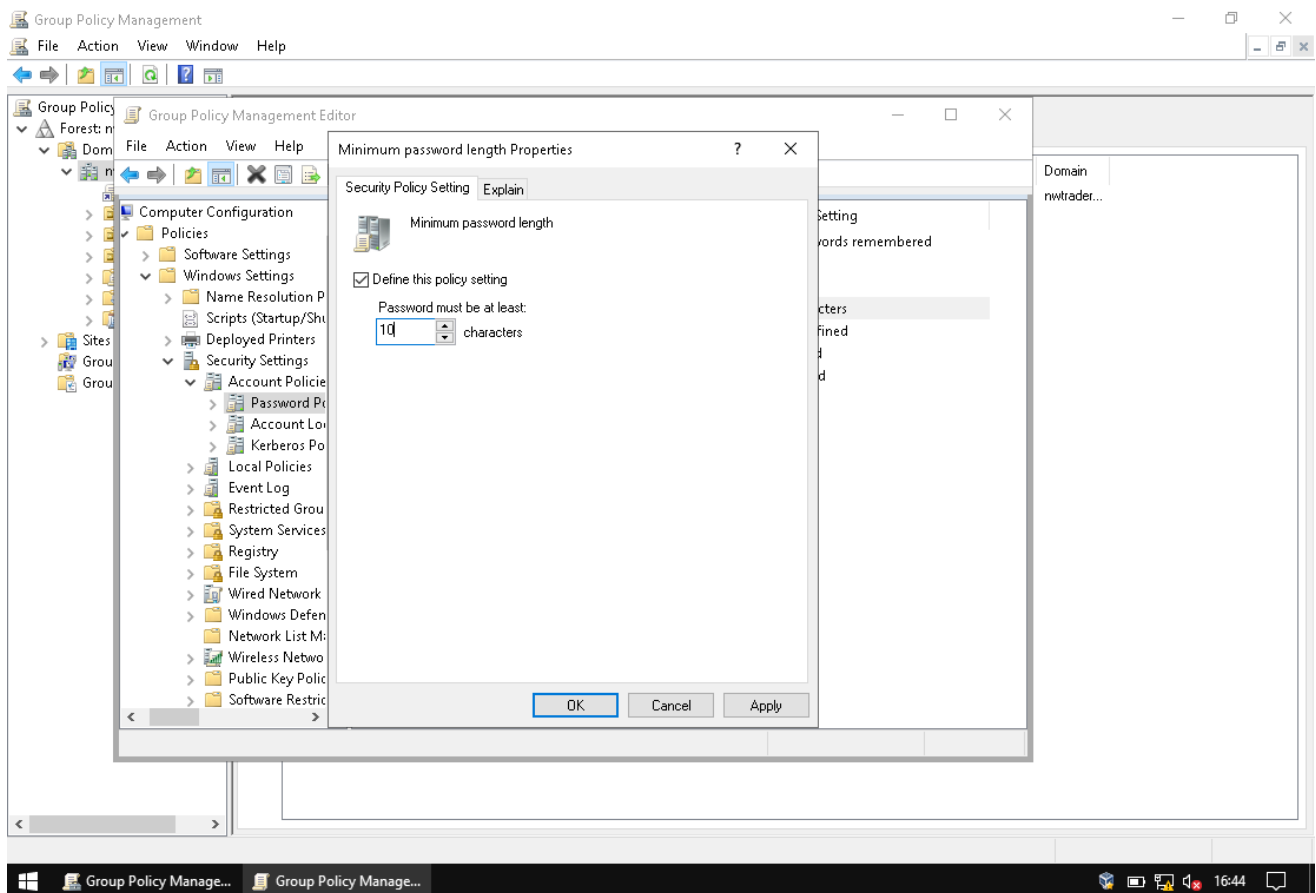
‘Enforce password history’ was set to ‘8’.



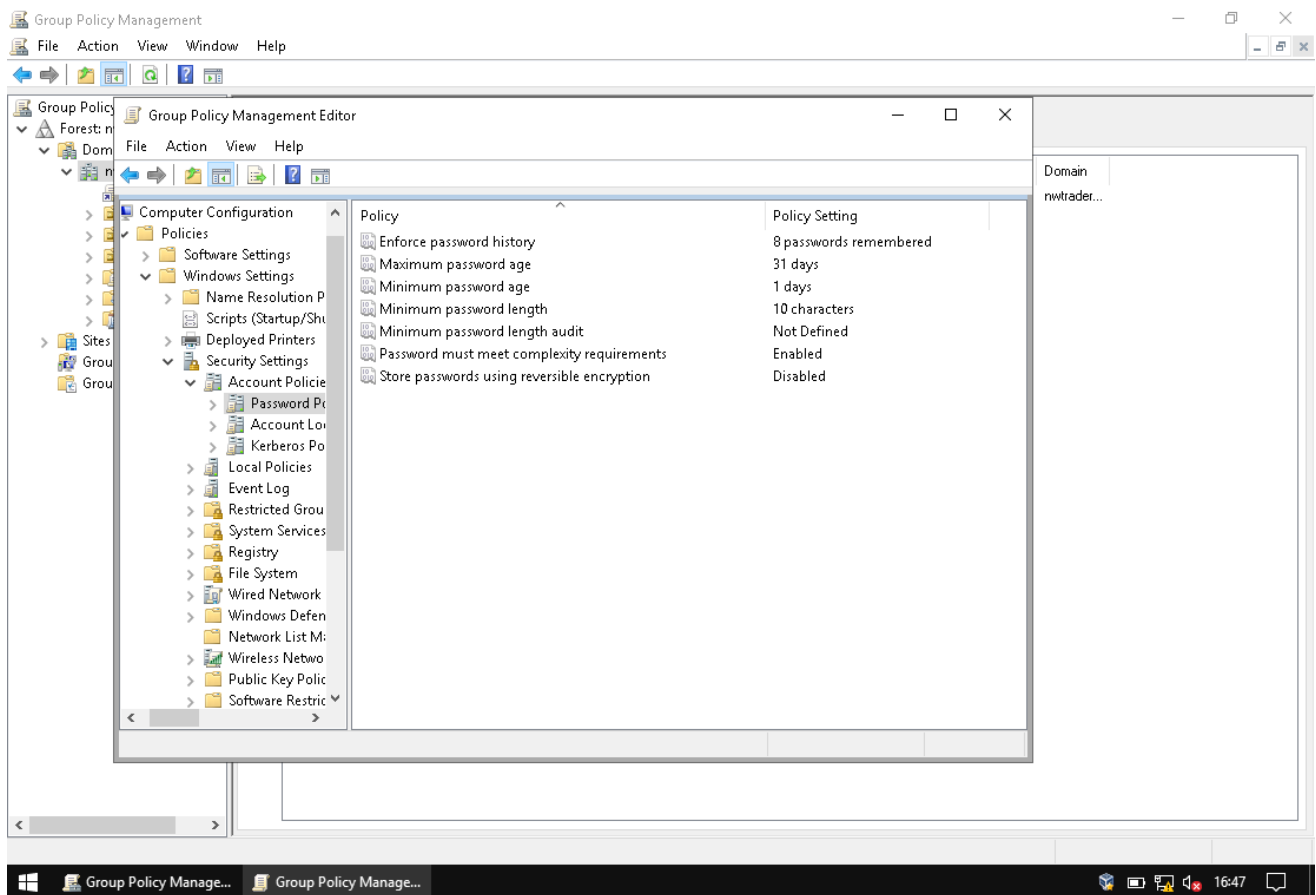
‘Maximum Password age’ was set to ‘31’



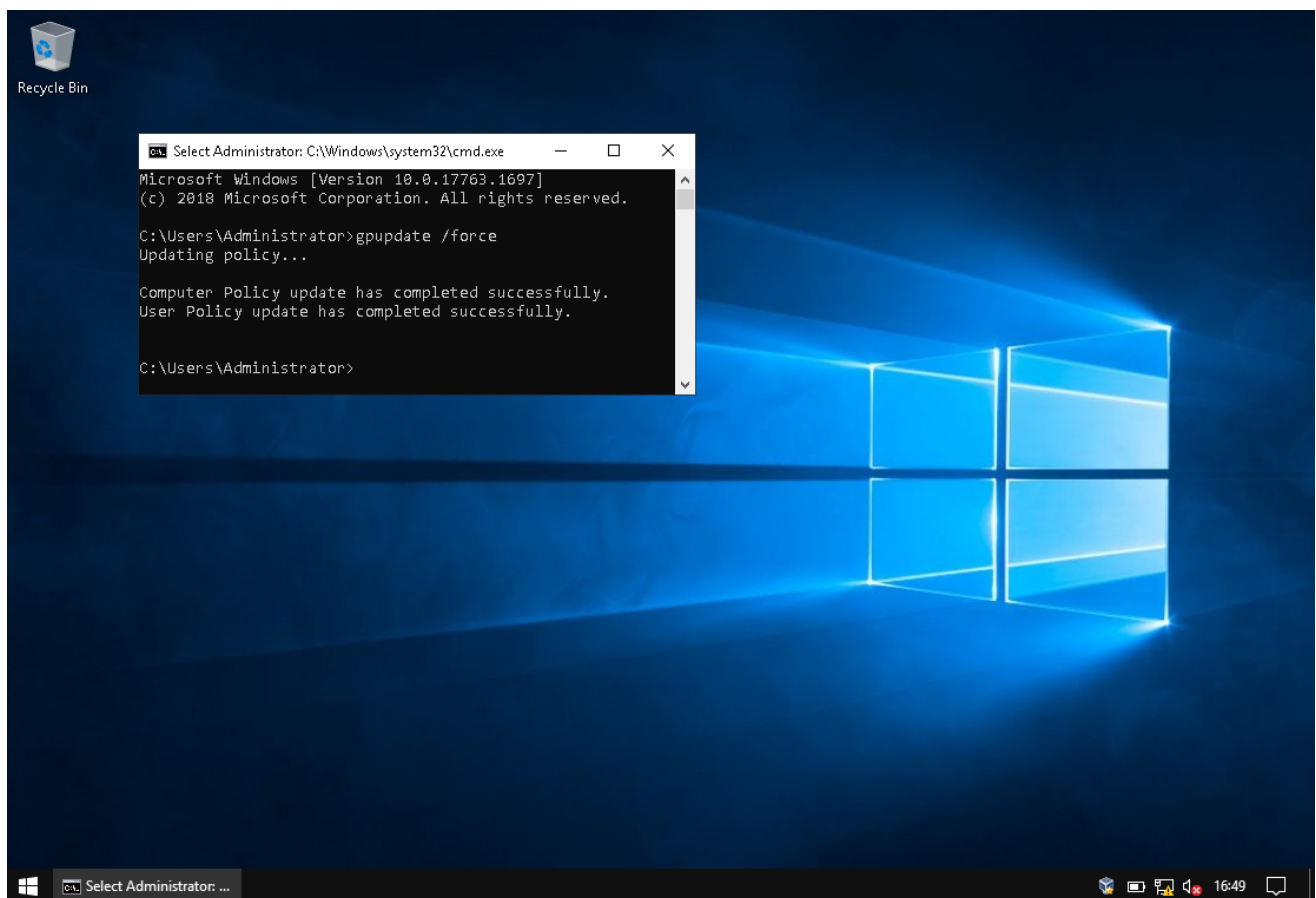
'Minimum Password Age' was set to '1' by default.



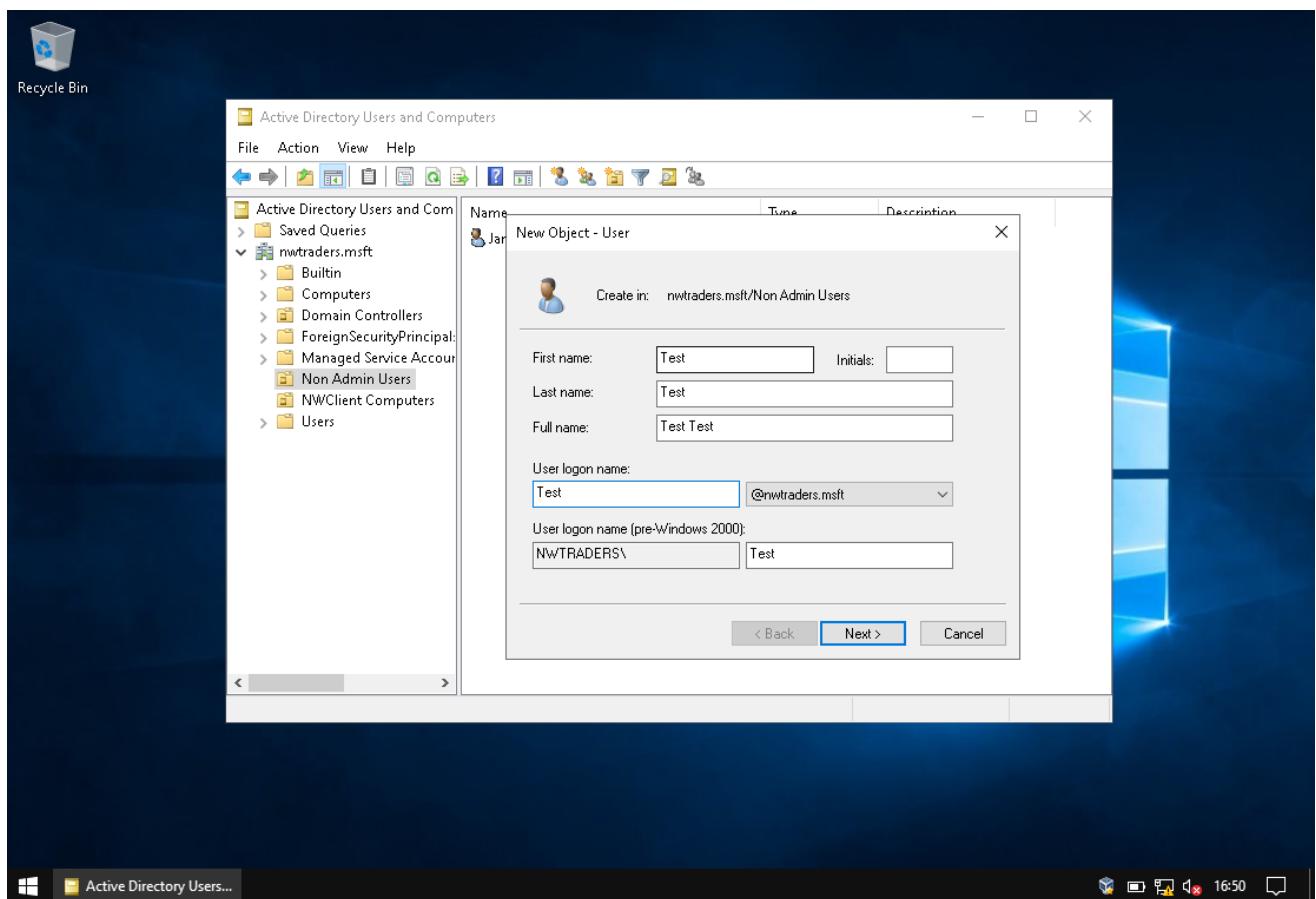
'Minimum Password Length' is set to '10'.



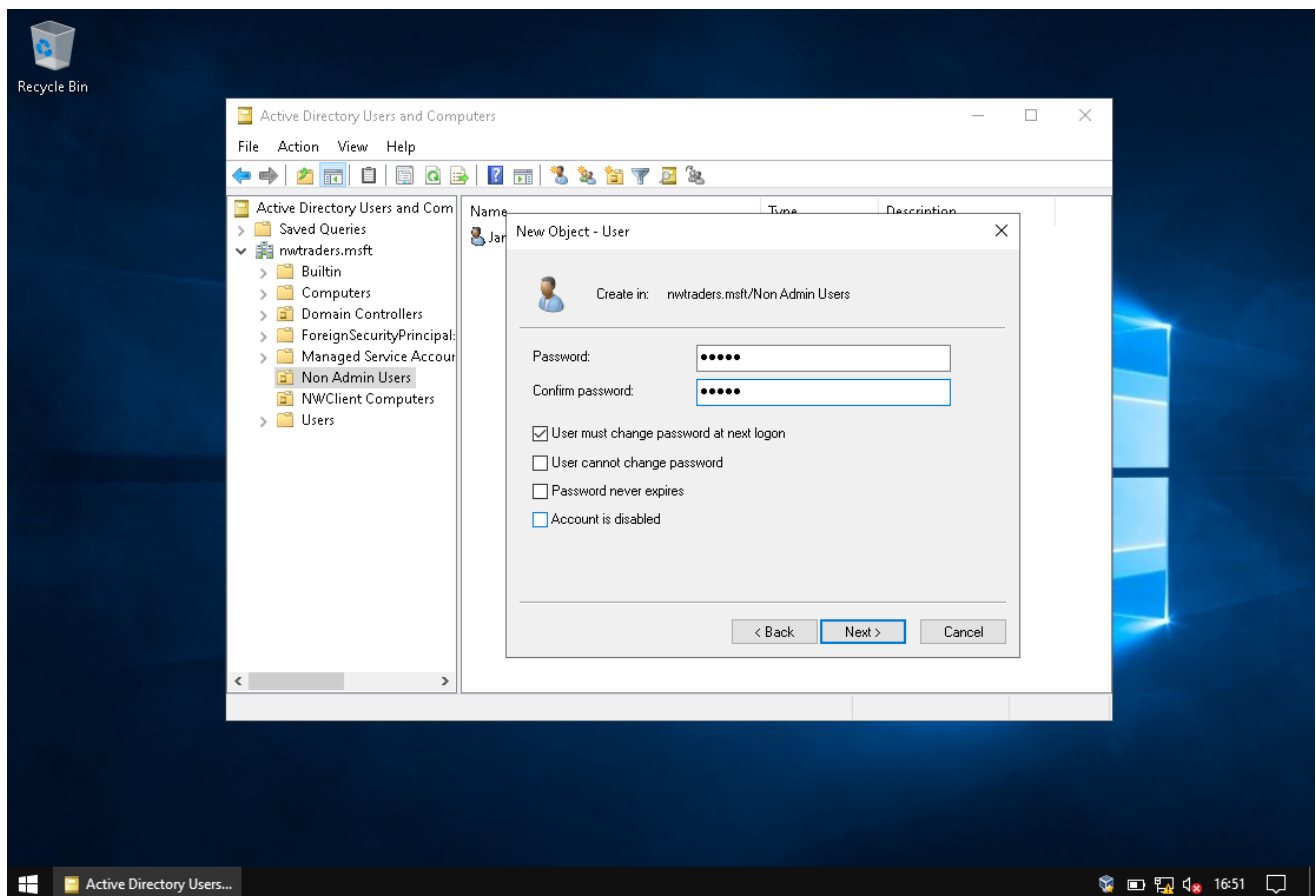
The settings are revised according to the brief's requests. Everything is set accordingly.



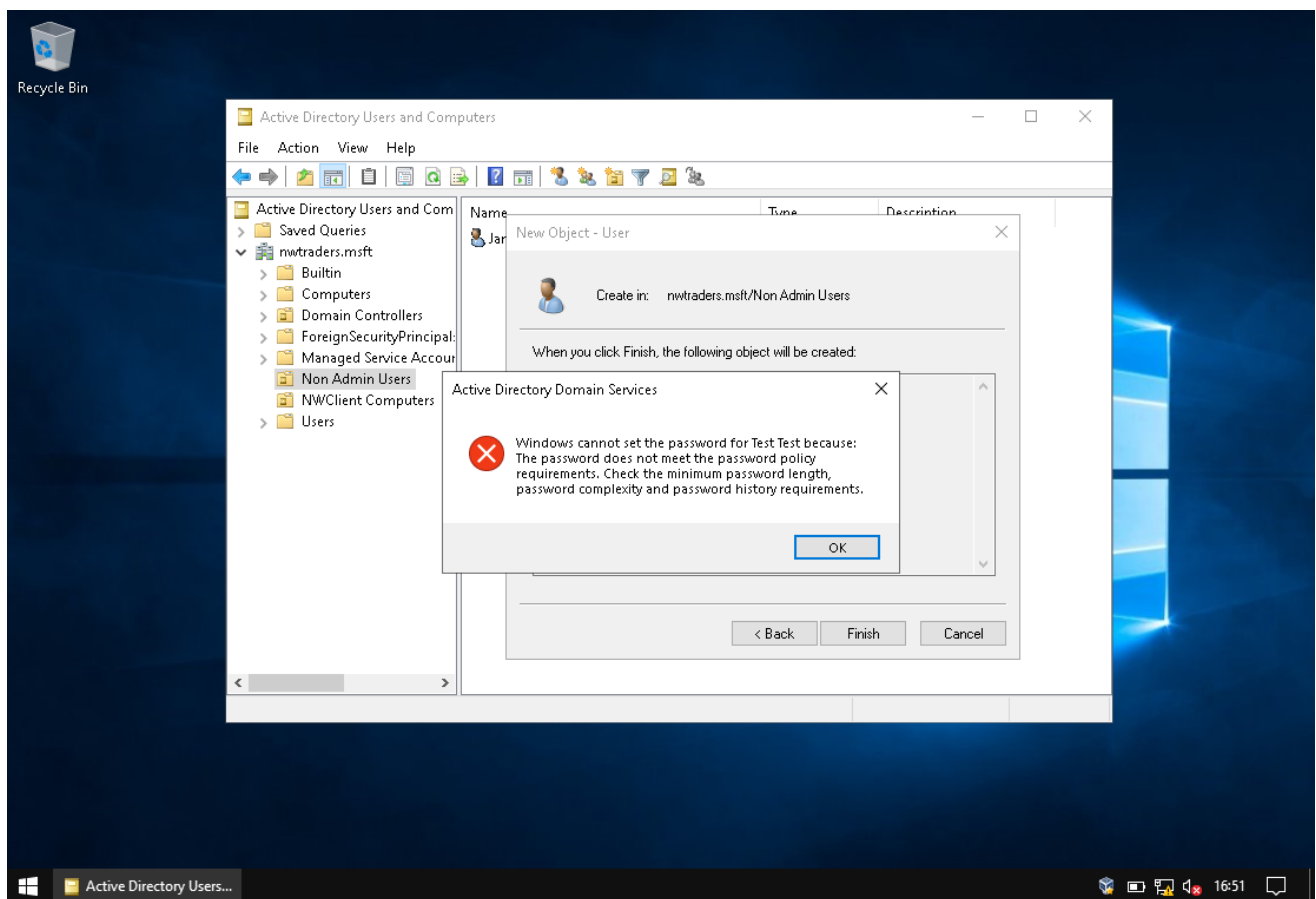
As usual, the Group Policy update is run.



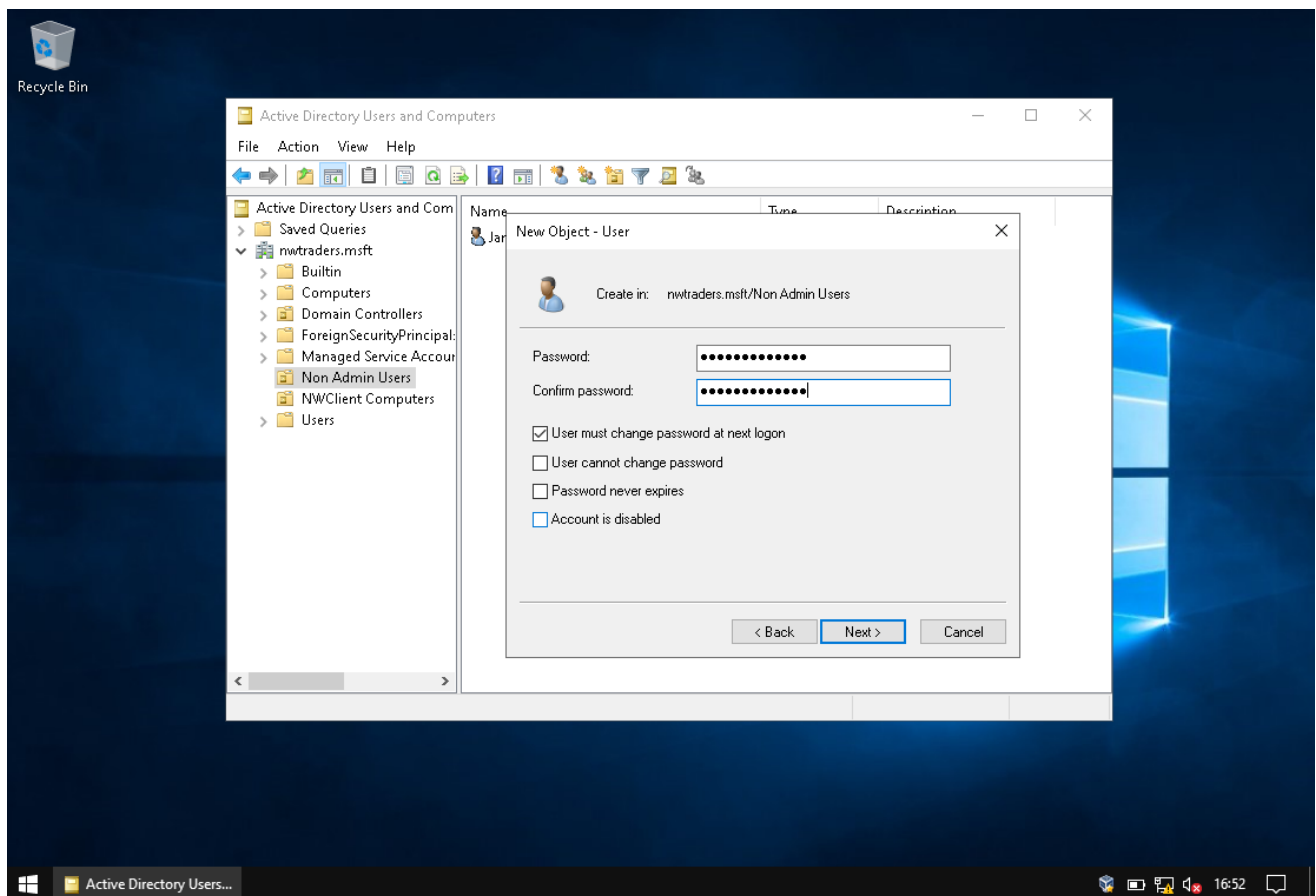
A new test account is being created to test the new group policy.



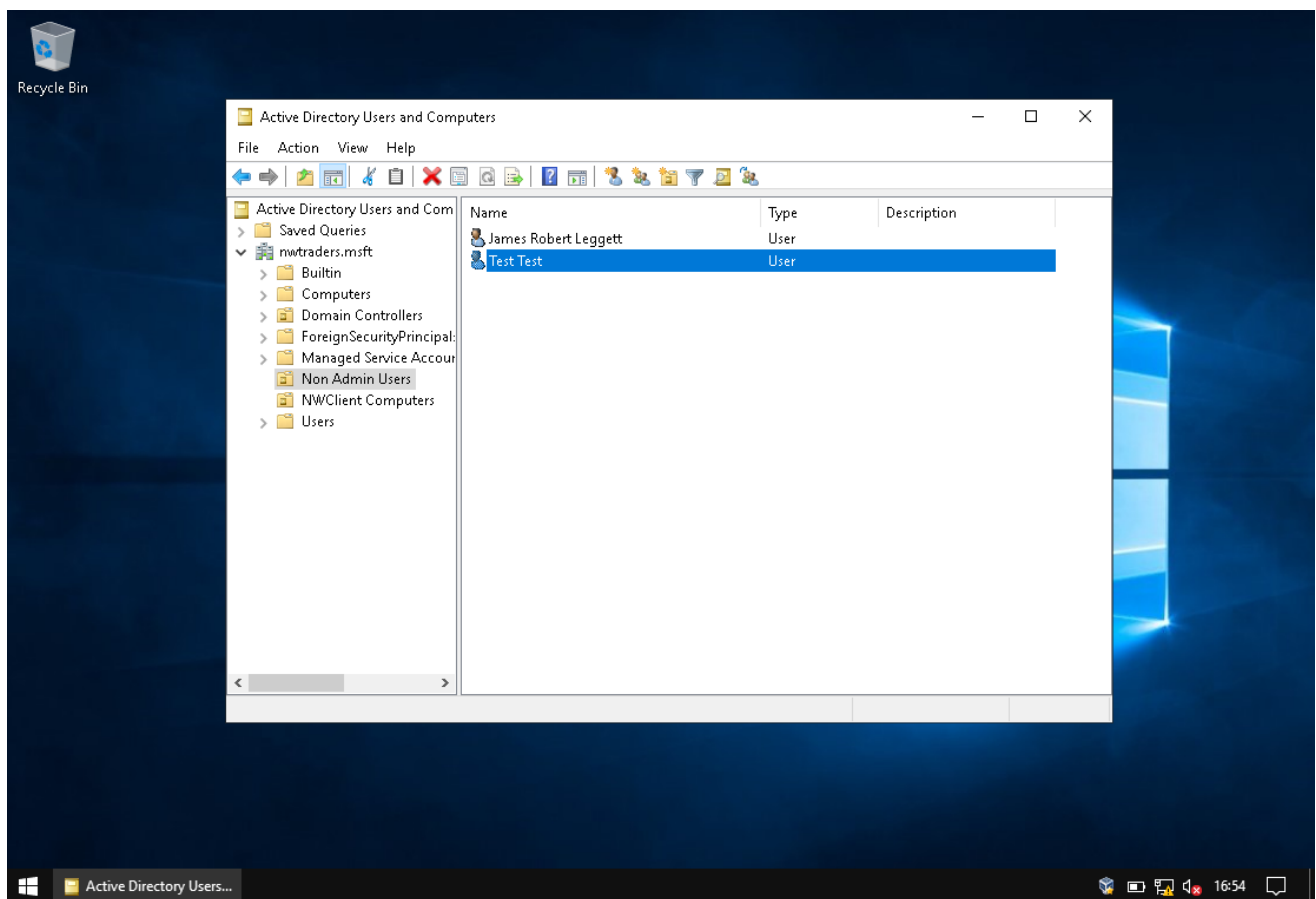
The password is set to **Hello**.



An error shows. The minimum password length check works!



The password is set to P@ssphrase!!!.



The test account is created successfully.

Task 3: Observational Tasks

The main differences between local permissions and file shares

NTFS (Local Permissions)

The **New Technology File System** is a new process used in Windows NT based operating systems for storing, filtering and organising files efficiently and effectively. It was introduced in 1993 along with the introduction of the Windows NT kernel, named after the NTFS system. It is a much more efficient alternative to FAT (File Allocation Table). It includes a major security access control service that allows admins to place permission properties onto physical files which enables the ability to restrict access to certain files and directories to certain users. [1]

NTFS has a range of different file permissions that can be changed for both individual users and specific groups. These include '**Full Control**' which enables users to obtain full control over the file. They can open the file, edit the file, delete the file and even change permissions of the file. '**Modify**' allows users to open and edit the files and directories, and allows deletion of the folder. The '**Read & Execute**' permission allows users to open the file and sub-directories and even execute scripts and programs, but they cannot edit or delete. '**List folder contents**' is the same as Read & Execute, but is inherited by folders only. '**Read**' only allows users to read the files, and won't allow them to execute or edit them and finally '**Write**' allows users to create files and folders, and edit existing files. [2]

Share

Share permissions are permissions designed for directories that are accessed via a network. These permissions don't apply to local users accessing said directories via a local account. They're a lot more general than the NTFS permissions and only have 3 permissions: '**Read**' which allows users to read and run files but not edit or delete them. '**Change**' which allows users to edit the files along with read them, but cannot change permissions themselves, and '**Full Control**' which is like change, but allows users to edit the permissions (usually used by admins by default). [3]

What's the difference?

NTFS permissions are more intricate, and allow a greater level of control over directories or folders than share permissions, however, share permissions can be more restrictive than NTFS permissions; they can be applied across networks and can restrict the number of connections to a folder. They can both be applied over each other, however, the strictest restriction will apply, meaning that if a file was set to 'Write' by NTFS, but 'Read' by share, then the folder itself can only be read, and not edited (written) as share restricts this functionality based on policy. [4]

The role of Group Policy Management in the network environment

What is Group Policy

Group Policy is a major function within the Windows desktop environment that allows network admins to add policies and restrictions to certain functions or settings for certain groups of users (i.e. students) that ensure data is protected and secure from back door access. With group policy, users will only have access to certain files and settings, and depending on the group policy, may not be able to execute their own programs or browse directories outside their own user directory.

Group policy is a part of active directory, and is defined through the domain controller. [5]

Sound password principles in a modern network environment

Create a strong, long password (or 'passphrase')

According to NIST (National Institute of Standards and Technology) section 5.1.1.1, passwords must be at least 8 characters in length and may be entirely numeric. [6]

One of the easiest ways a hacker could gain access to an account, is by simply guessing the password associated for it. By setting a weak or easy to guess password, a hacker could simply guess the password, especially if it's a weak password, or a commonly used password. [7]

Another reason for a strong and complex password is that it restricts the likelihood of a successful brute-force attack on your personal account. A brute force attack is a simple process, where a hacker executes a script on a computer that simply attempts to log into multiple accounts with various simple and common passwords. [8] A strong and long password (or 'passphrase') requirement will greatly reduce the likelihood of a user setting their password as a common password.

Implement a second factor of authentication

Two factor authentication (2FA) is a security method that requires the user provide another form of authentication after their password. The second form of authentication could be a biometric factor, such as a face or fingerprint, or in the instance of a networking environment, a physical key, security token or smart card is also a valid method of providing a second factor of authentication. 2FA works by requesting a second method of authentication that only the user themselves could provide, such as an item on their person or a characteristic such as their iris or fingerprint. [9]

For a modern network environment, the best solution would be using a **physical security key** (or a smart card).

Enforcing a password history policy

A password history policy is a policy set to restrict the amount of times an old password can be re-used when a password is reset. This restricts users from simply recycling the same old password over and over again to further enhance the security benefits of passwords that automatically reset. [10]

References

- [1] T. Mesevage, "What Is NTFS and How Does It Work?", *Datto.com*, 2019. [Online]. Available: <https://www.datto.com/blog/what-is-ntfs-and-how-does-it-work>.
- [2] C. NG, "NTFS Permissions vs Share: Everything You Need to Know", *Inside Out Security*, 2021. [Online]. Available: <https://www.varonis.com/blog/ntfs-permissions-vs-share/>
- [3, 4] "NTFS vs. Share Permissions: What's the Difference? - DNSstuff", *Software Reviews, Opinions, and Tips - DNSstuff*, 2020. [Online]. Available: <https://www.dnsstuff.com/ntfs-vs-share-permissions>.
- [5] C. Hoffman, "What Is "Group Policy" in Windows?", *How-To Geek*, 2016. [Online]. Available: <https://www.howtogeek.com/125171/htg-explains-what-group-policy-is-and-how-you-can-use-it/>.
- [6] P. Grassi, J. Fenton, E. Newton, R. Perlner, A. Regenscheid and W. Burr, "NIST Special Publication 800-63B", *Pages.nist.gov*, 2017. [Online]. Available: <https://pages.nist.gov/800-63-3/sp800-63b.html>.

[7] “The Importance of Strong, Secure Passwords”, *Secure Data Recovery Services*, 2021. [Online]. Available: <https://www.securedatarecovery.com/resources/the-importance-of-strong-secure-passwords>.

[8] J. Petters, “What is a Brute Force Attack? Definition | Varonis”, *Inside Out Security*, 2020. [Online]. Available: <https://www.varonis.com/blog/brute-force-attack/>.

[9] L. Rosencrance, P. Loshin and M. Cobb, “What is Two-Factor Authentication (2FA) and How Does It Work?”, *SearchSecurity*. [Online]. Available: <https://searchsecurity.techtarget.com/definition/two-factor-authentication>.

[10] J. Knafo, “Top 10 Password Policies and Best Practices for System Administrators”, *The Devolutions Blog*, 2018. [Online]. Available: <https://blog.devolutions.net/2018/02/top-10-password-policies-and-best-practices-for-system-administrators>.