

# Worksheet 3

Network Operating Systems and Services (NOSS)  
ACCA5023

Adam Vimpany: 1810613

# Task 1: Understanding NTFS and Share Permissions

Figure 1 Dept Important Docs folder created.

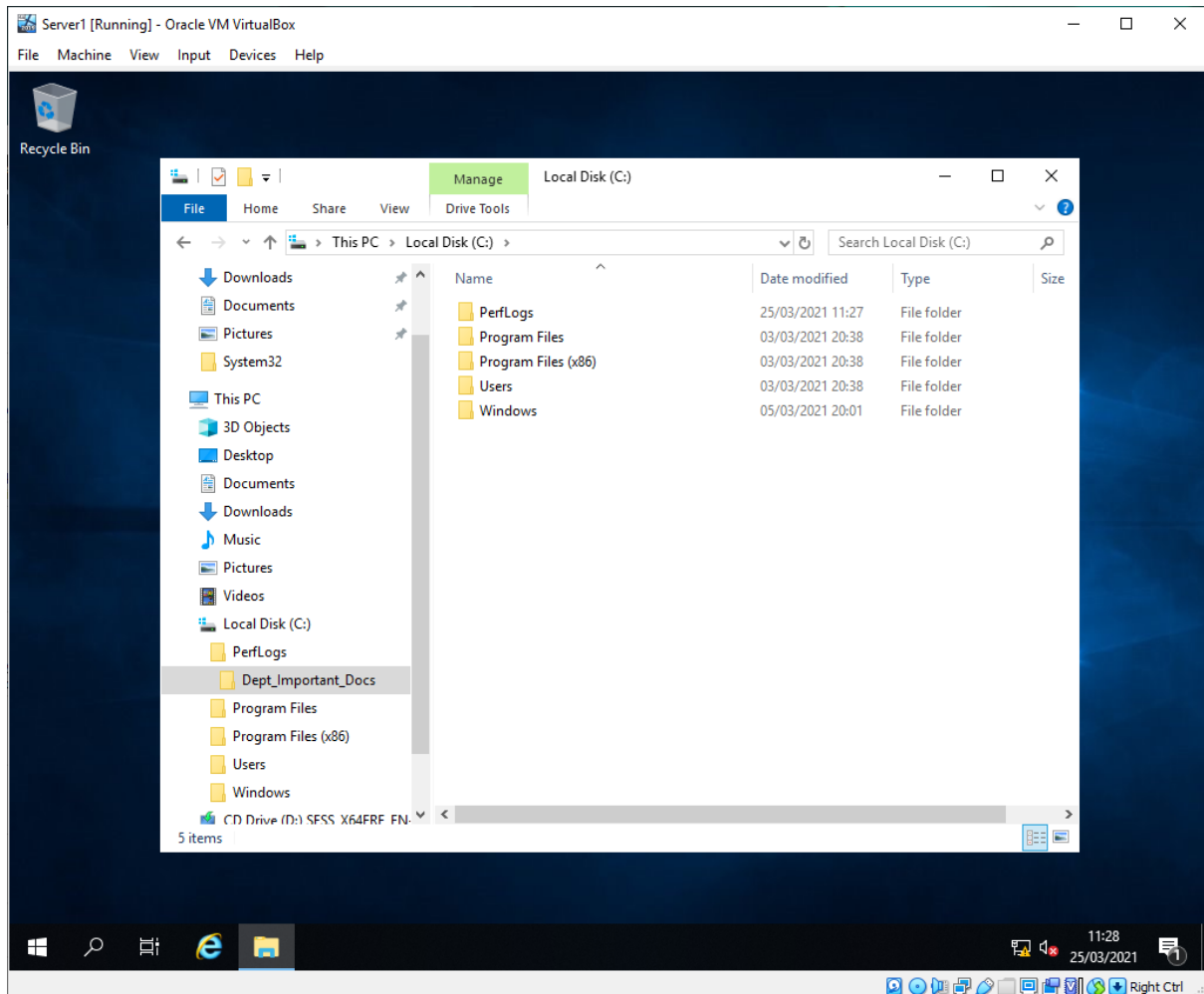


*Figure 2 New Text Document file created*

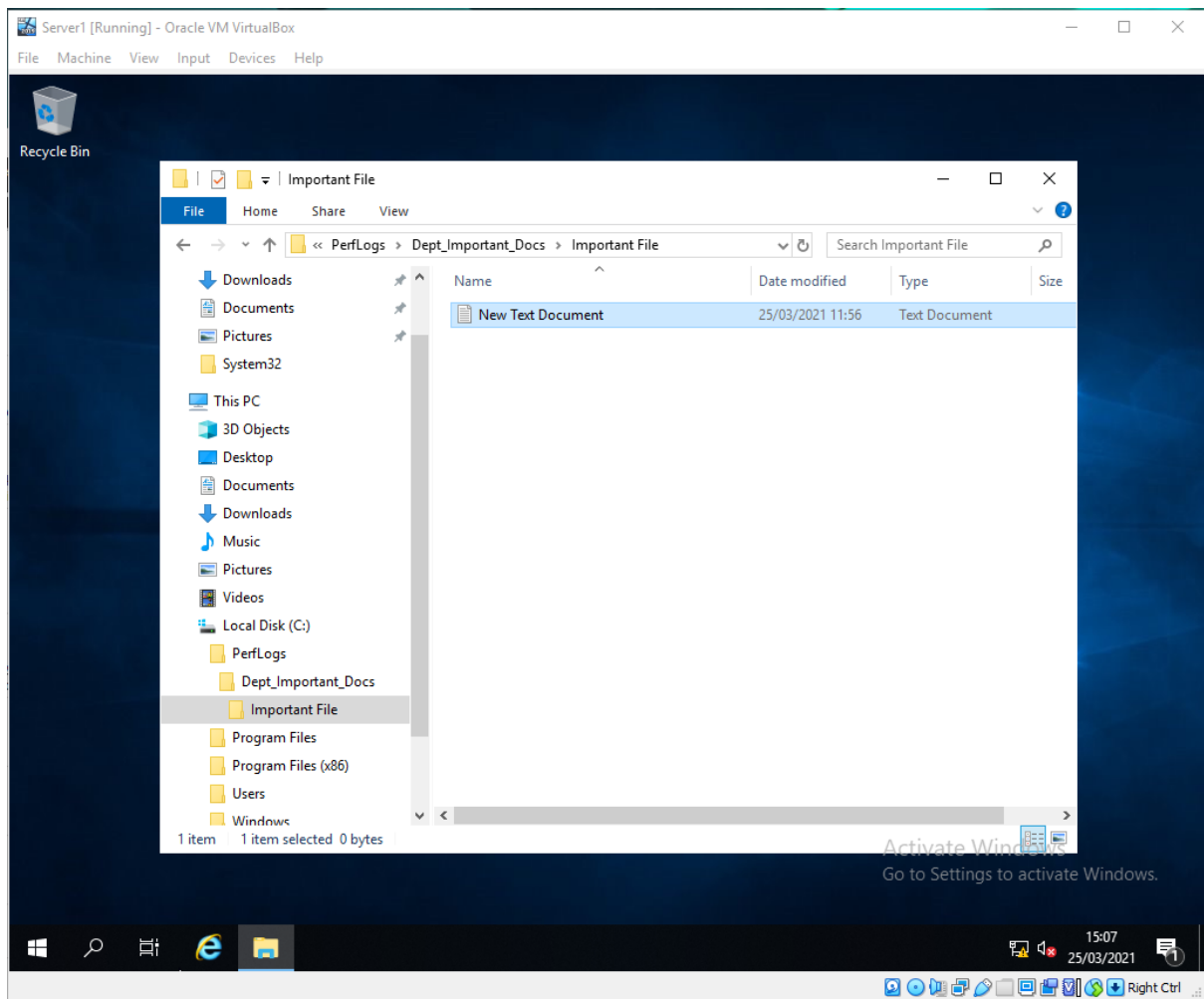


Figure 2 Disabled block inheritance > Removed all inherited permissions.

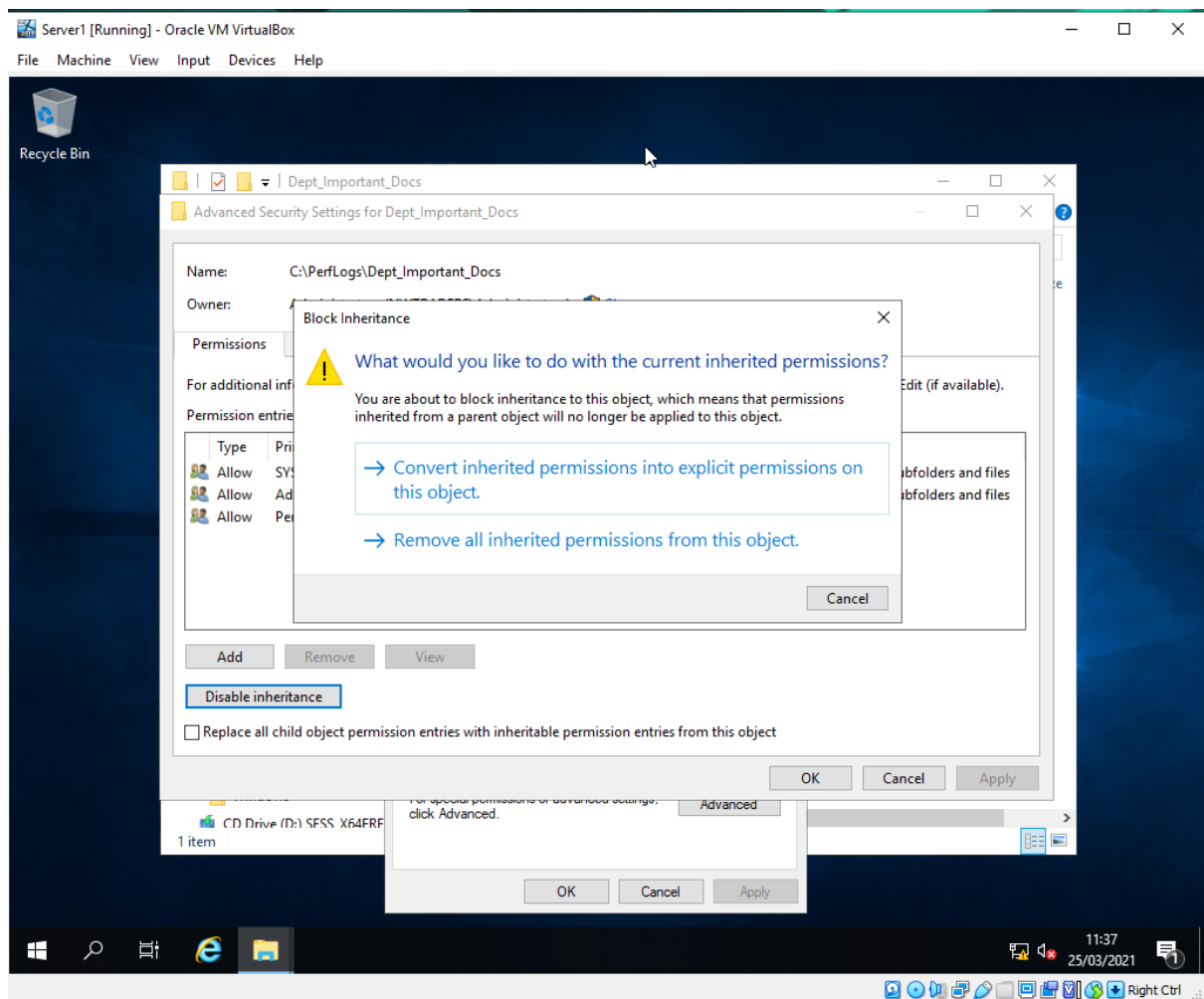


Figure 3 Check name verification for current user

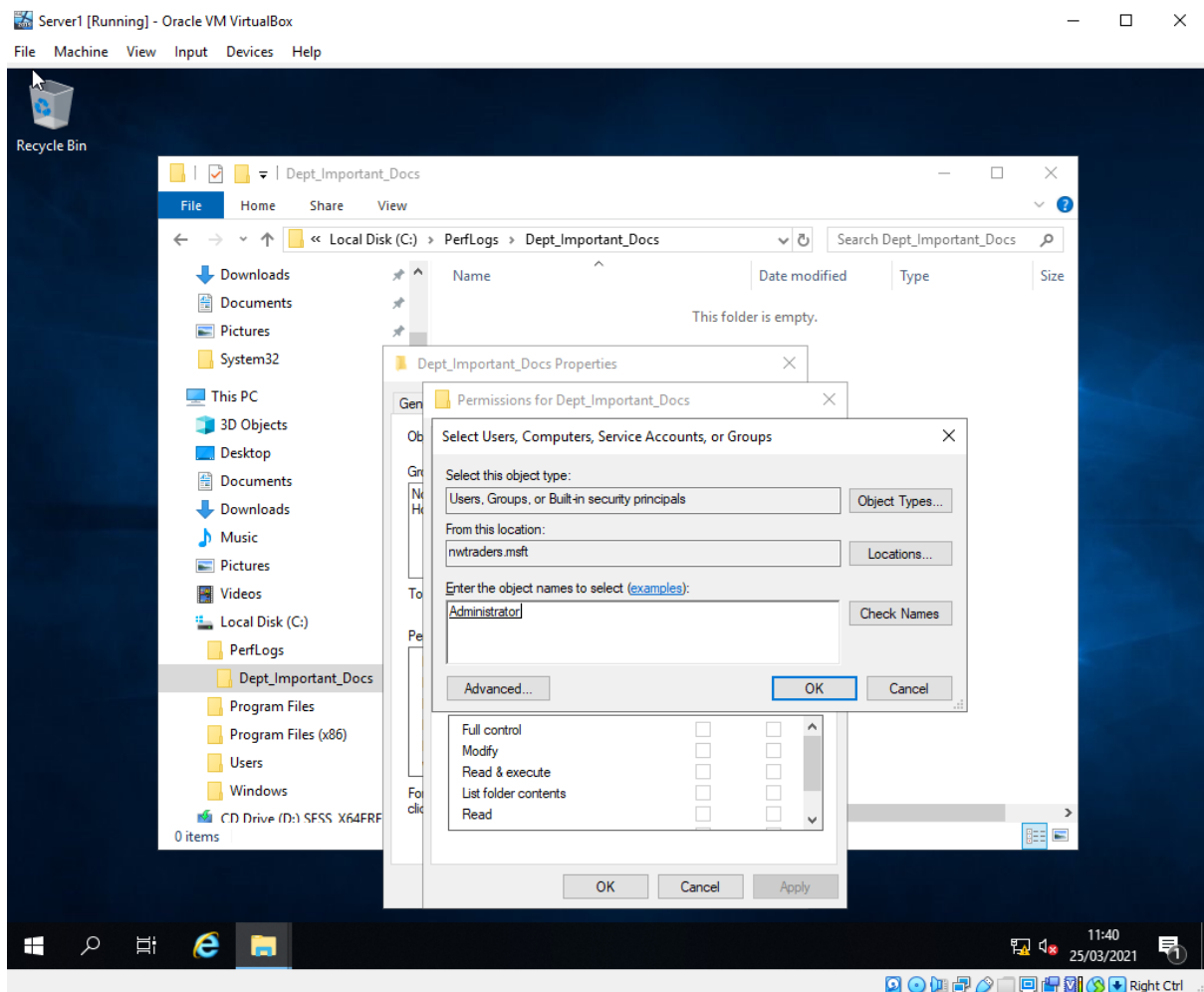


Figure 4 Full control given to Administrator user from NWTRADERS domain

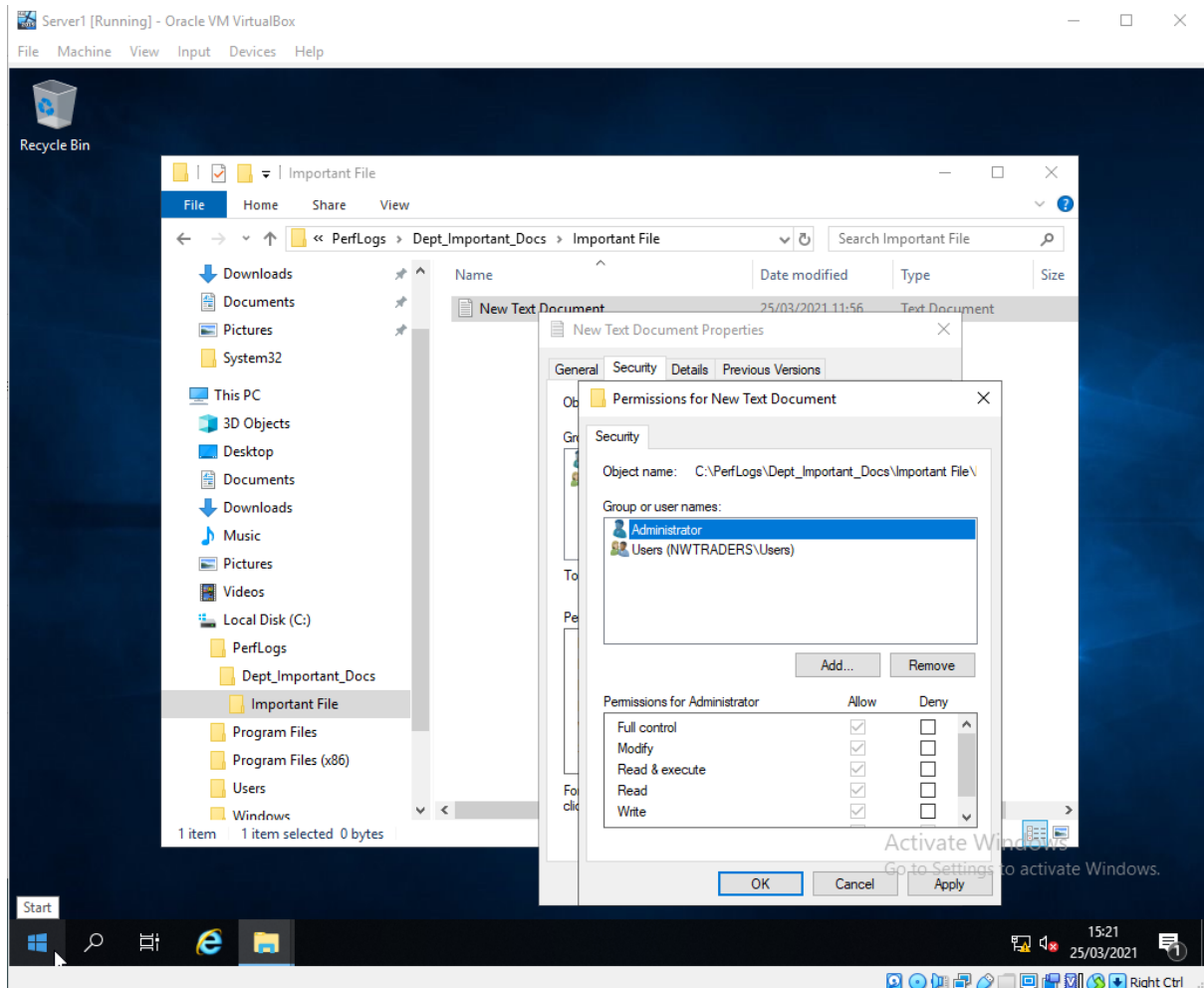


Figure 5 Access control level Inherited from folder "Dept\_Important\_Docs" for file "Important File".

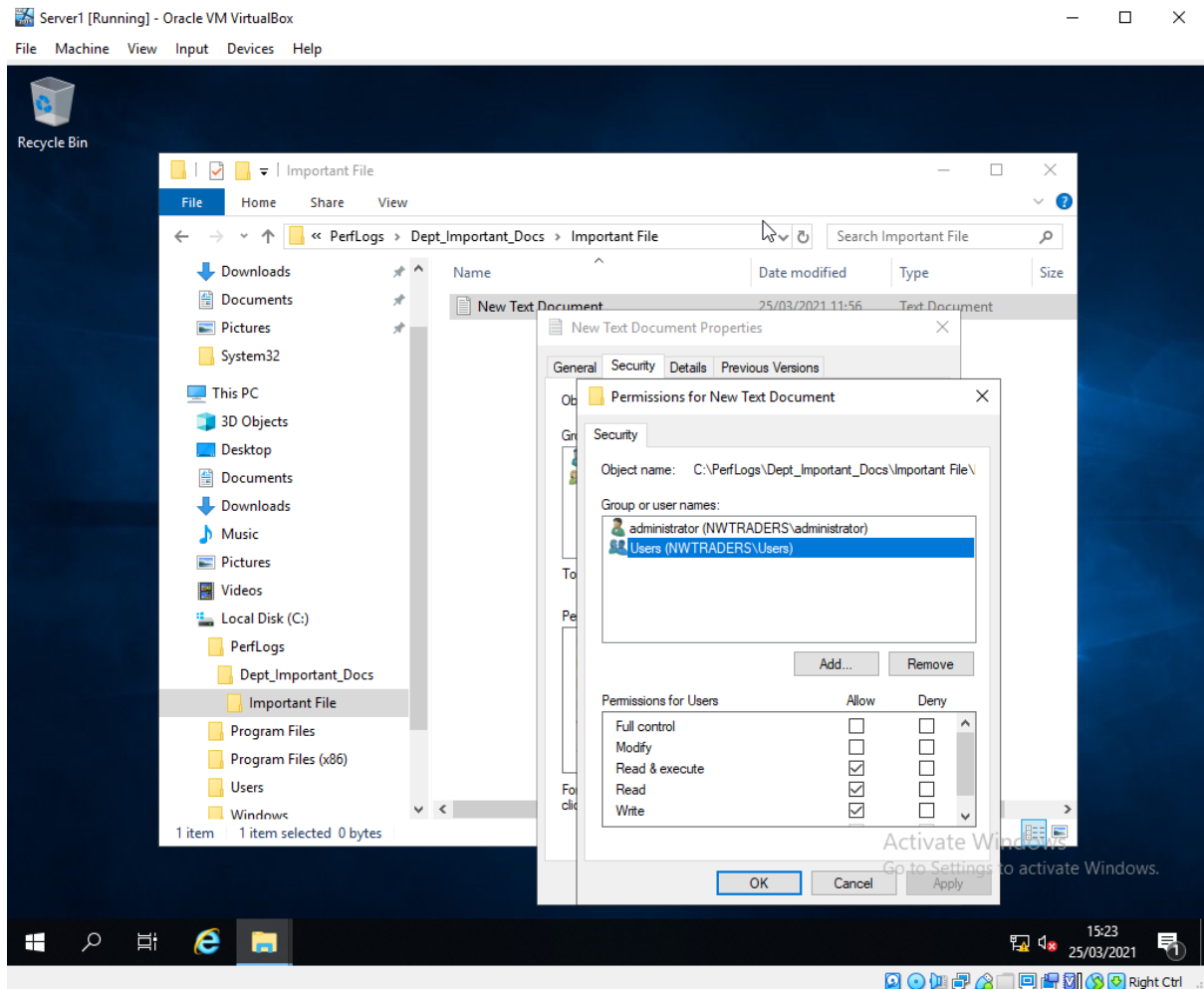


Figure 6 Granted specific access rights to user Adam Vimpany

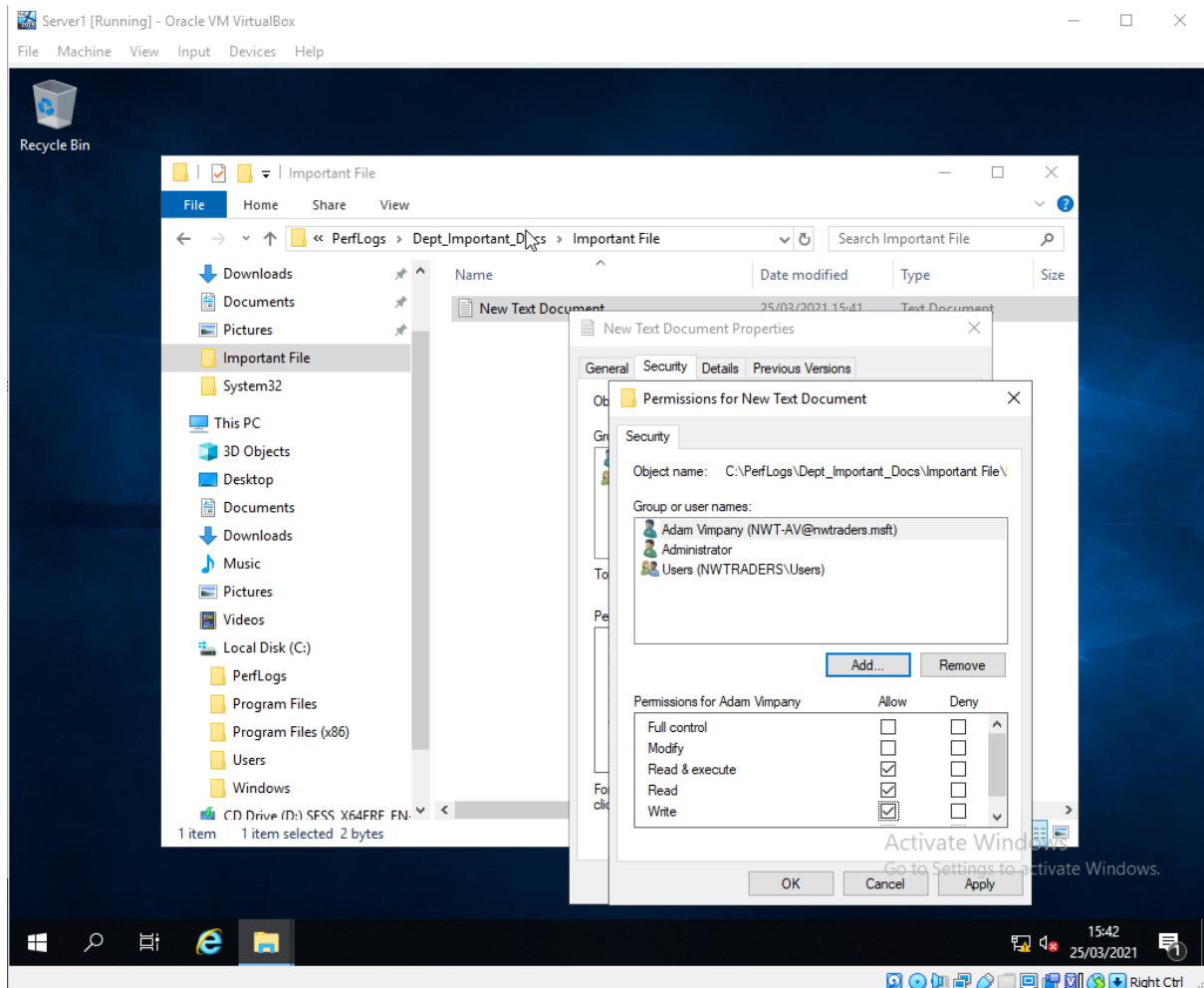


Figure 7 Edit and save text file from administrator account

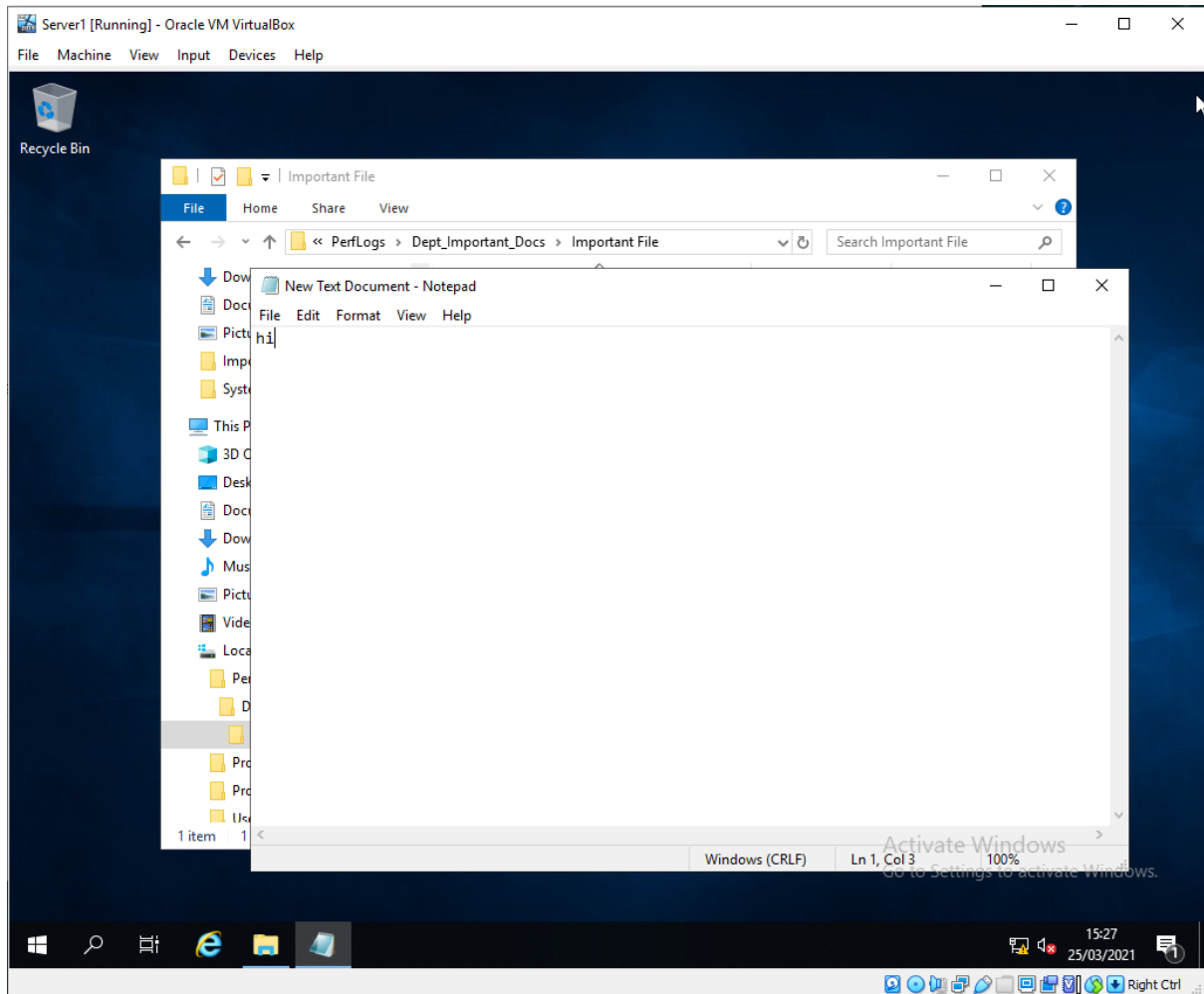


*Figure 8 File can be eddited with "other" non admin user account*

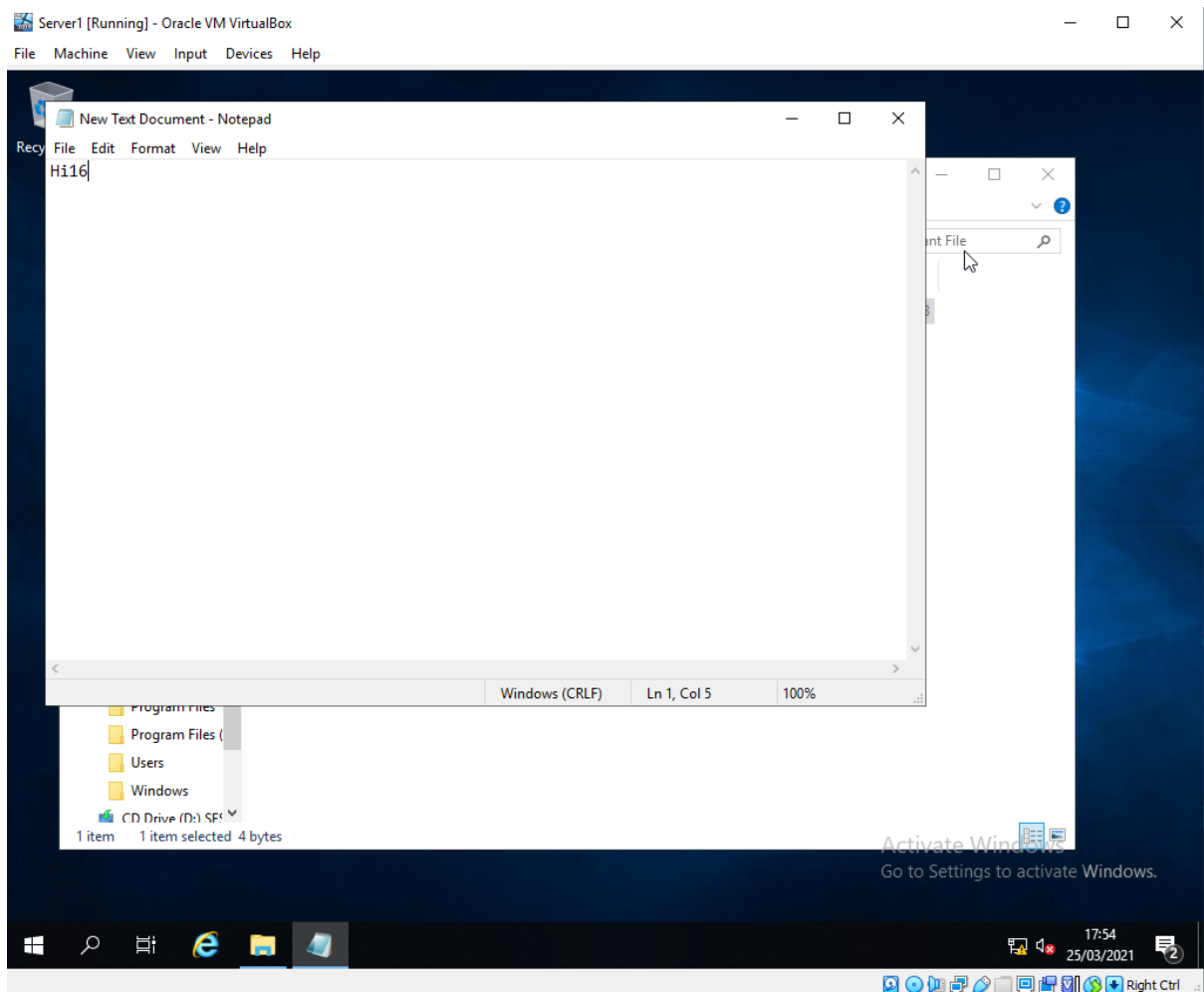
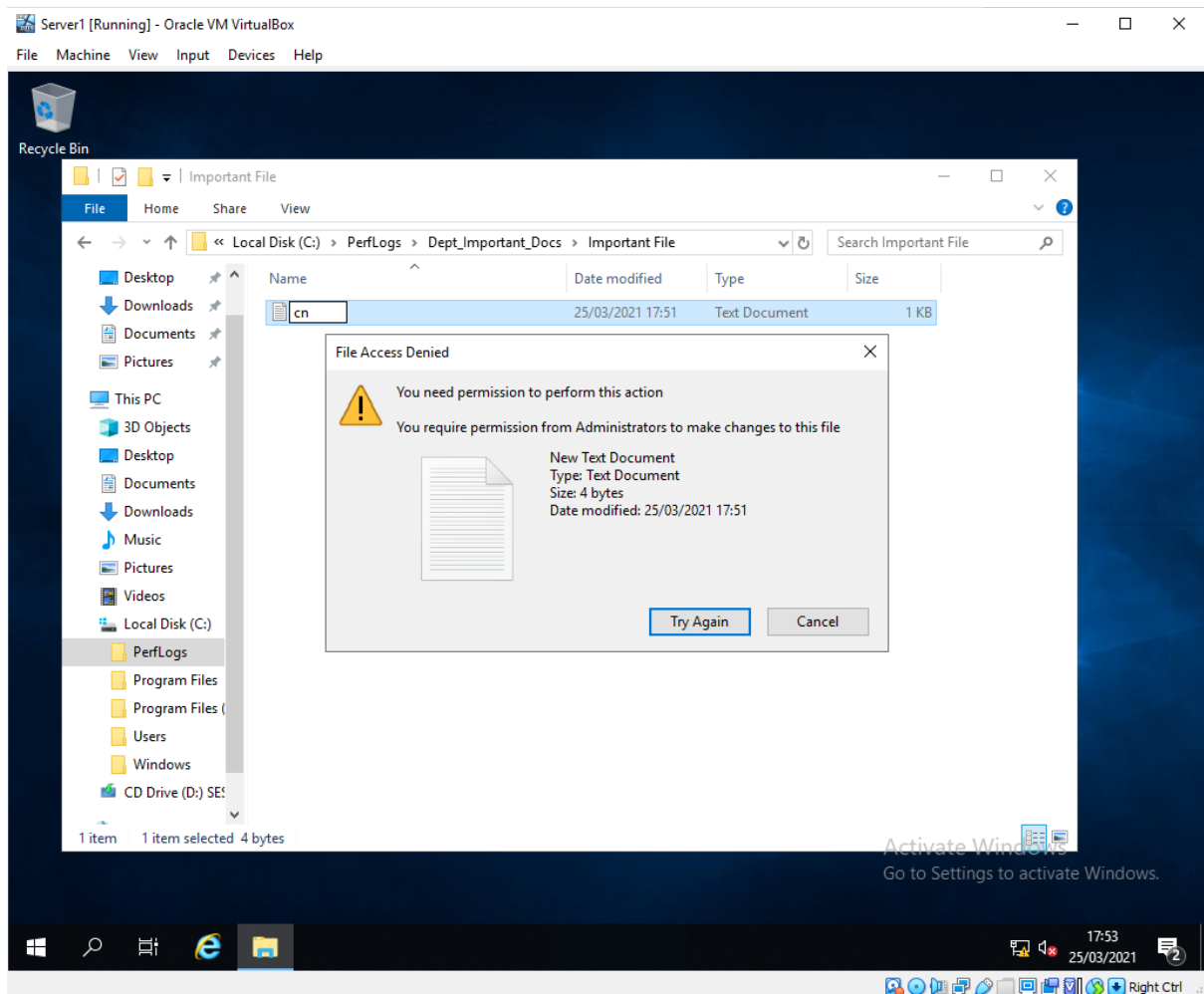


*Figure 9 File cannot be modified by non administrator user account*



## Task 2 – Share Permissions

Figure 10 SMB Share - Quick Selected

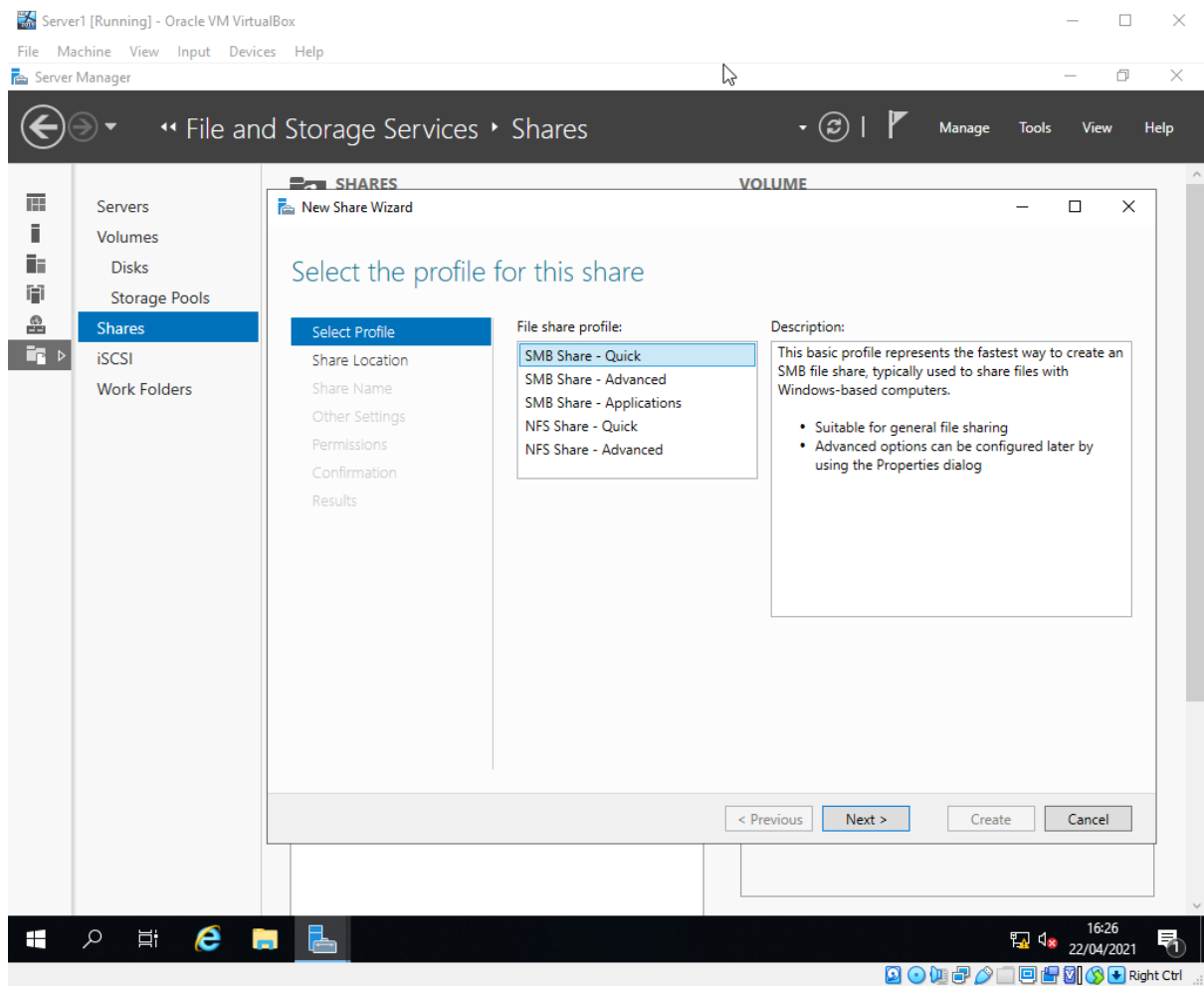


Figure 11 Set up file paths

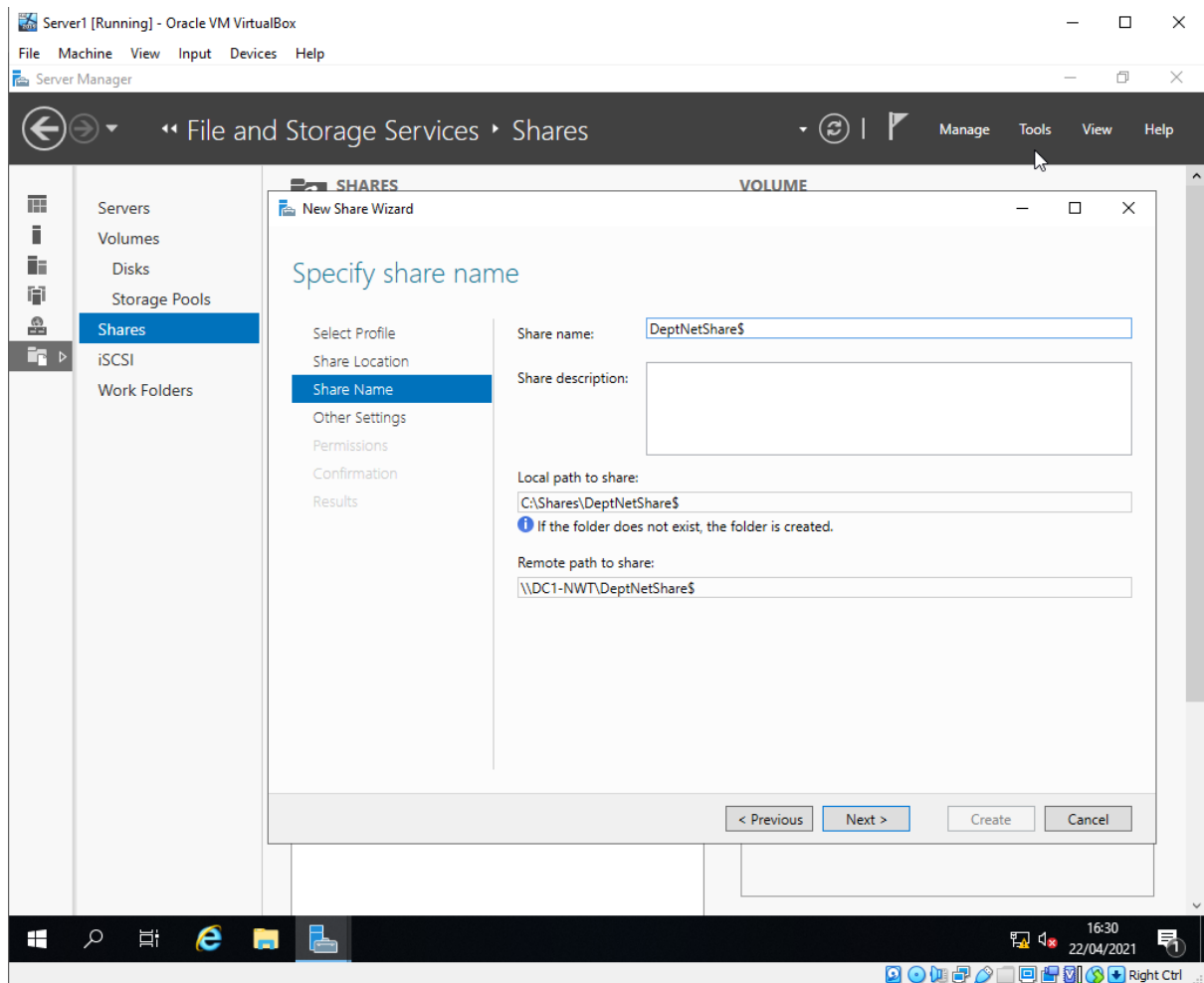


Figure 12 additional settings configured

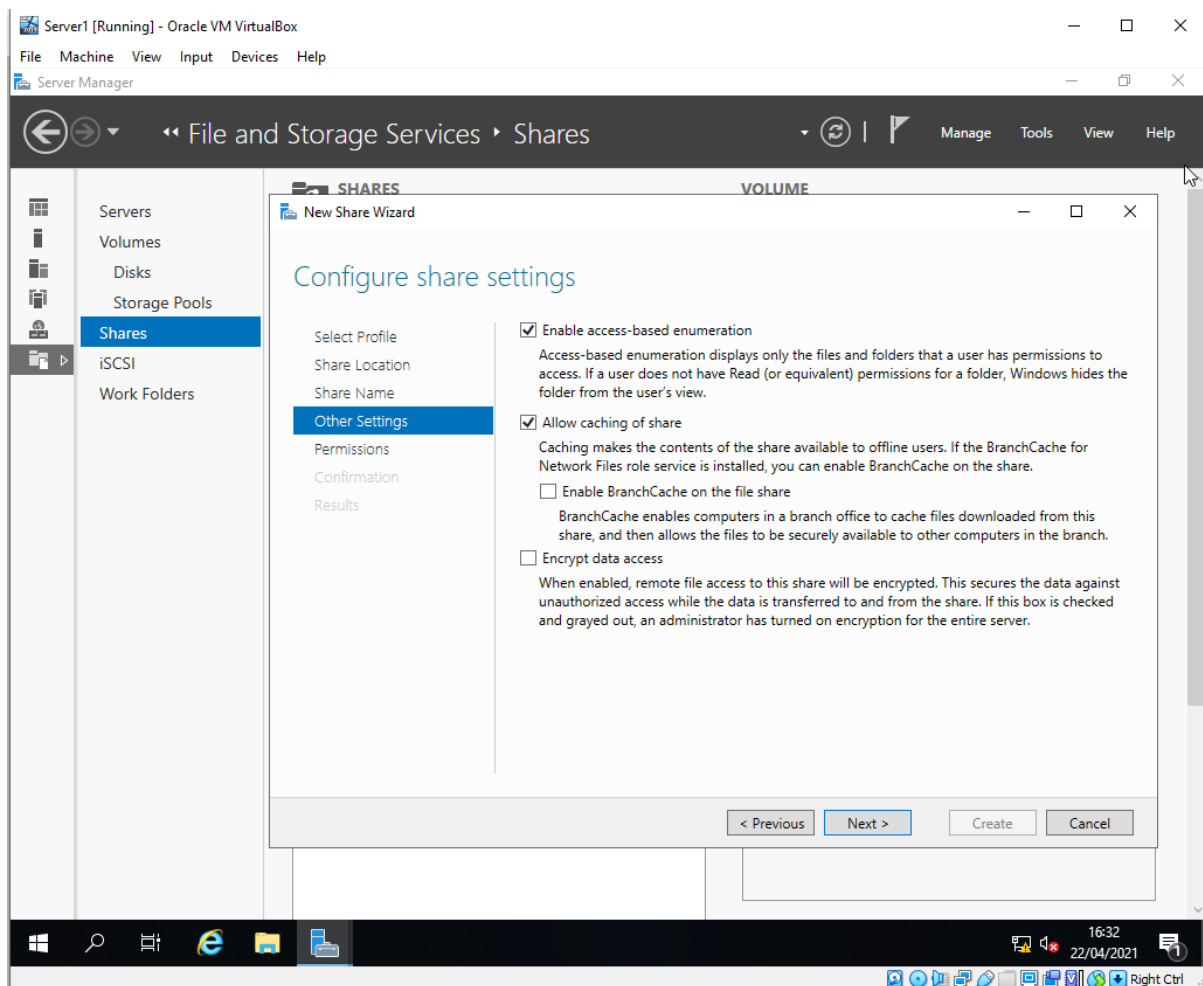


Figure 13 specified permission to access control screen

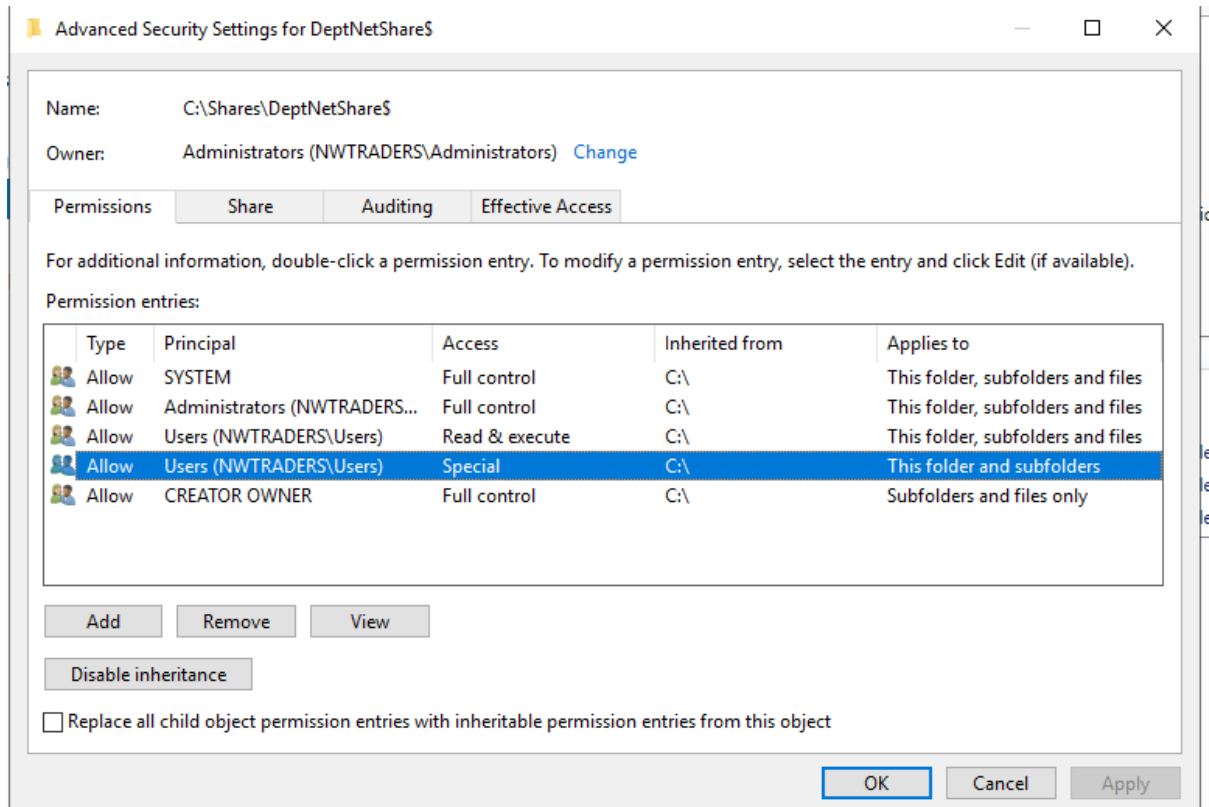
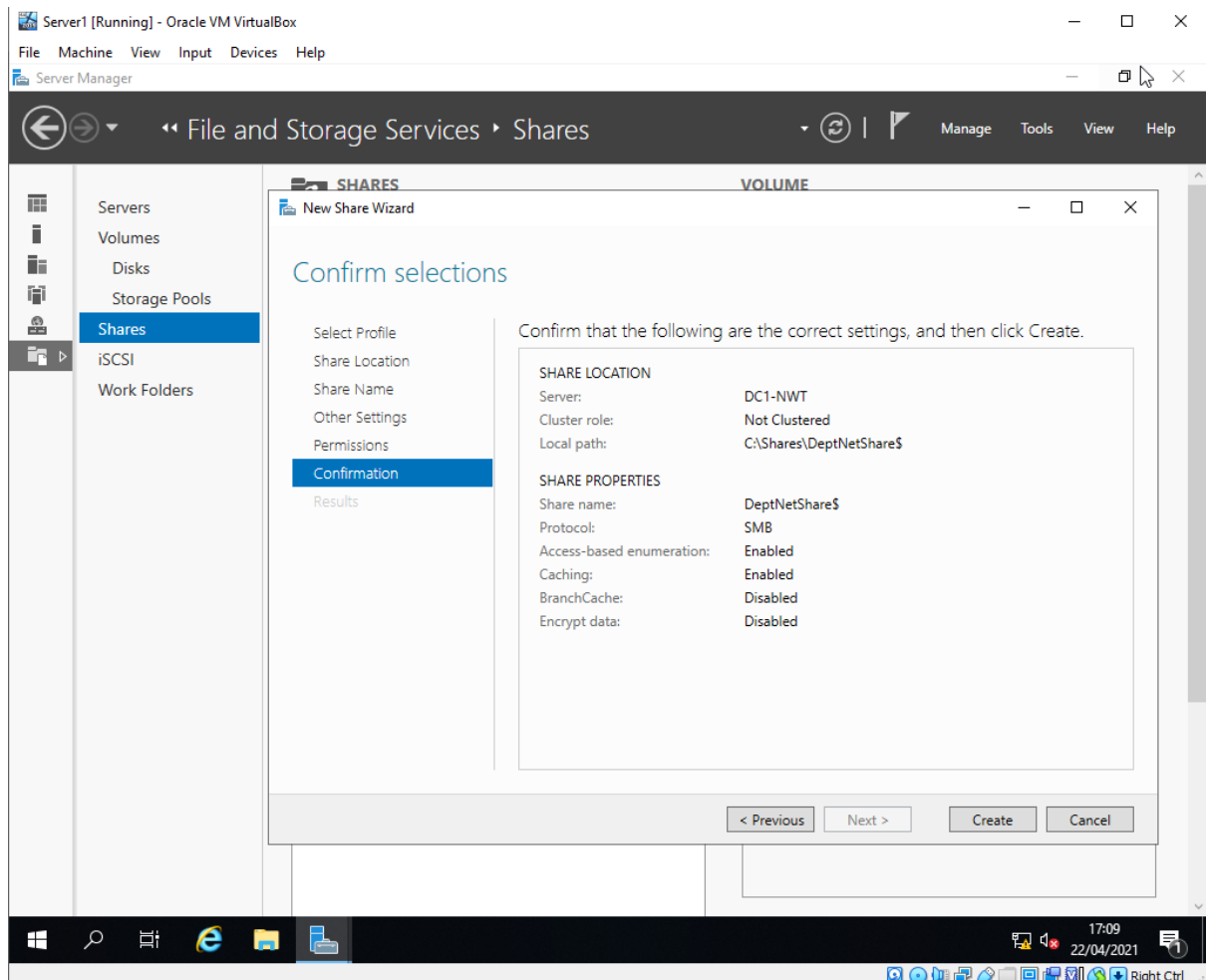
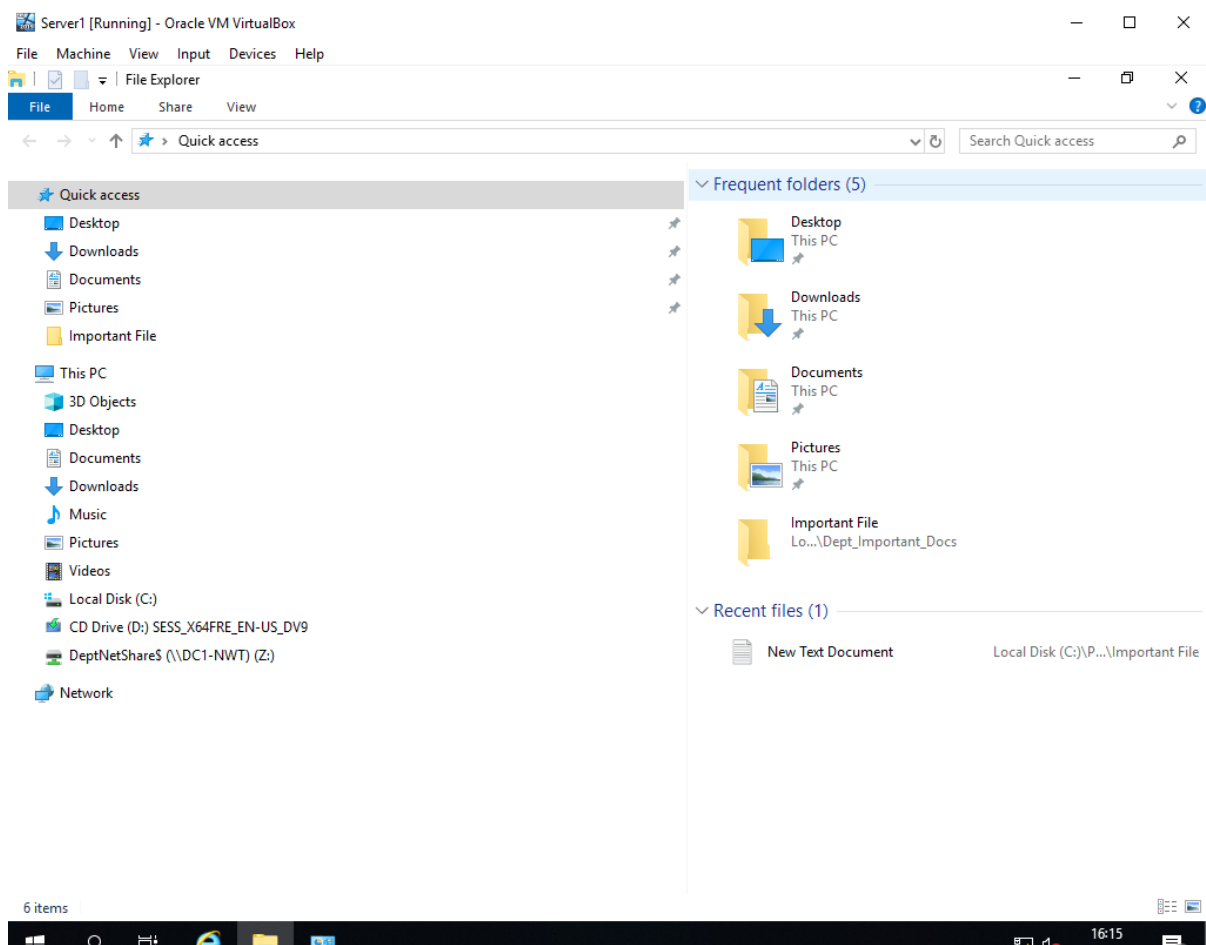


Figure 14 Verified settings are correct



## Accessing the file share/server over the network

*Figure 15 Network drive mapped*



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

*Figure 16 User created within Non Admin Users Organisational Unit*

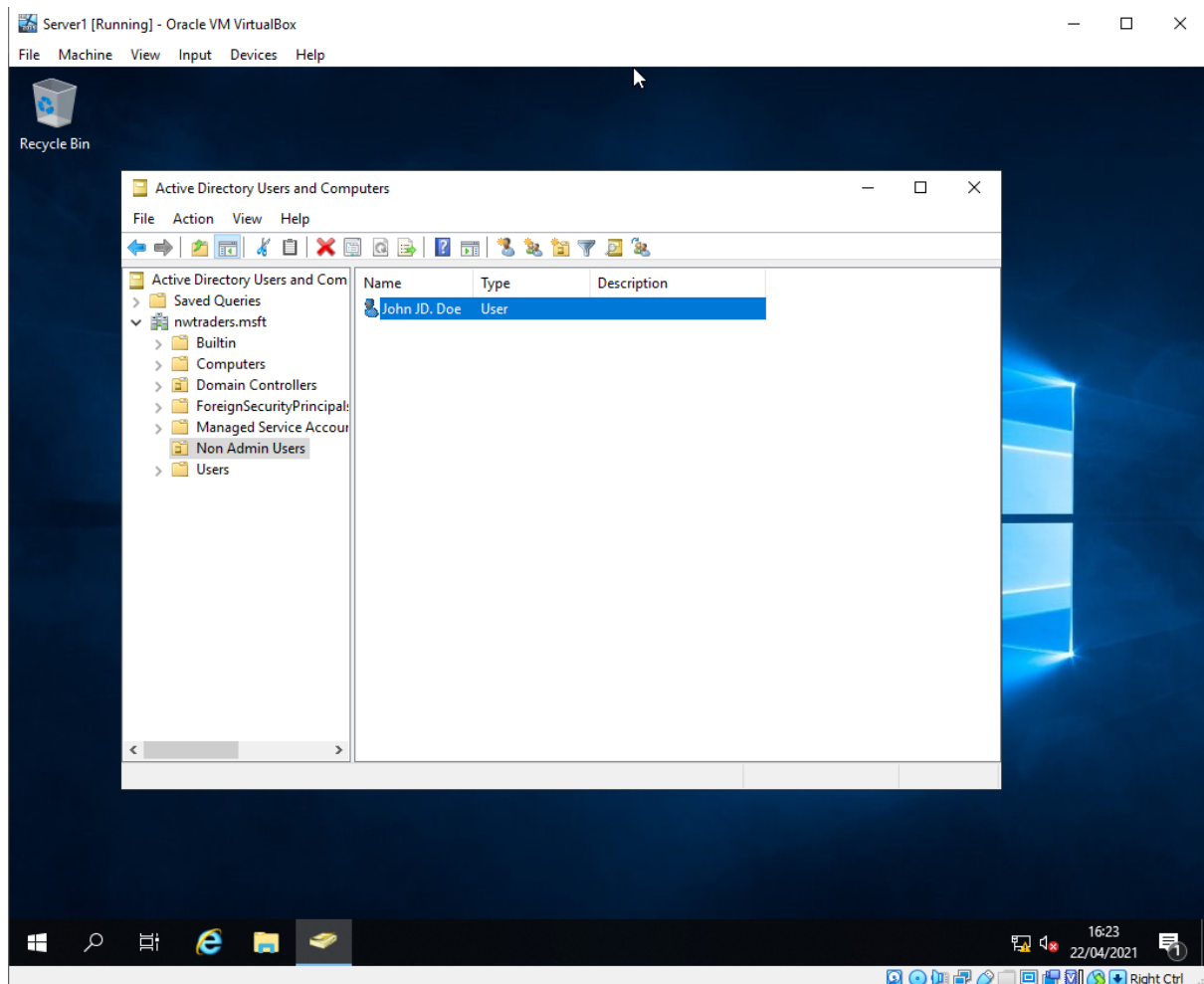


Figure 17 GPO created

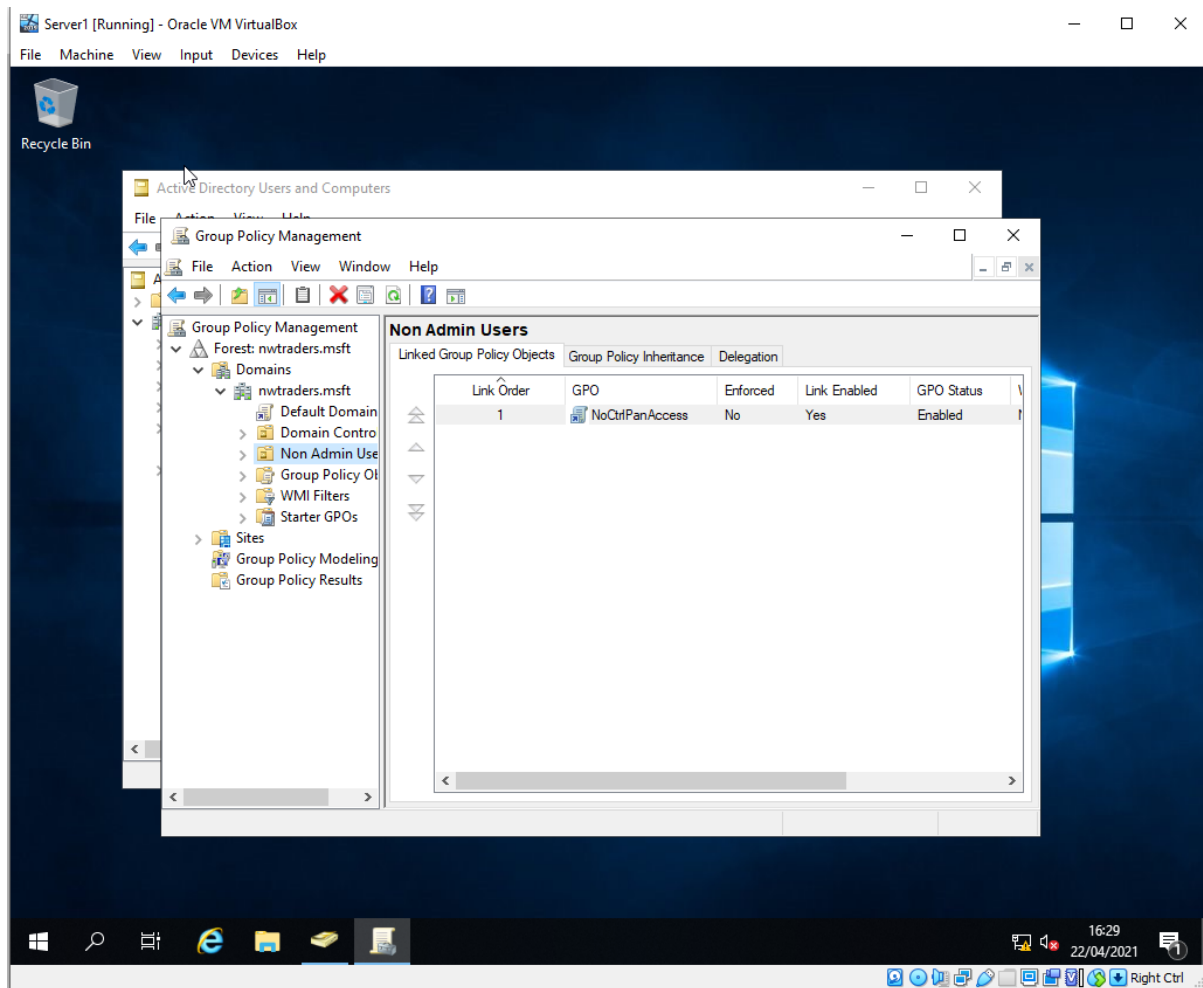


Figure 18 Control Panel Access set to prohibited.

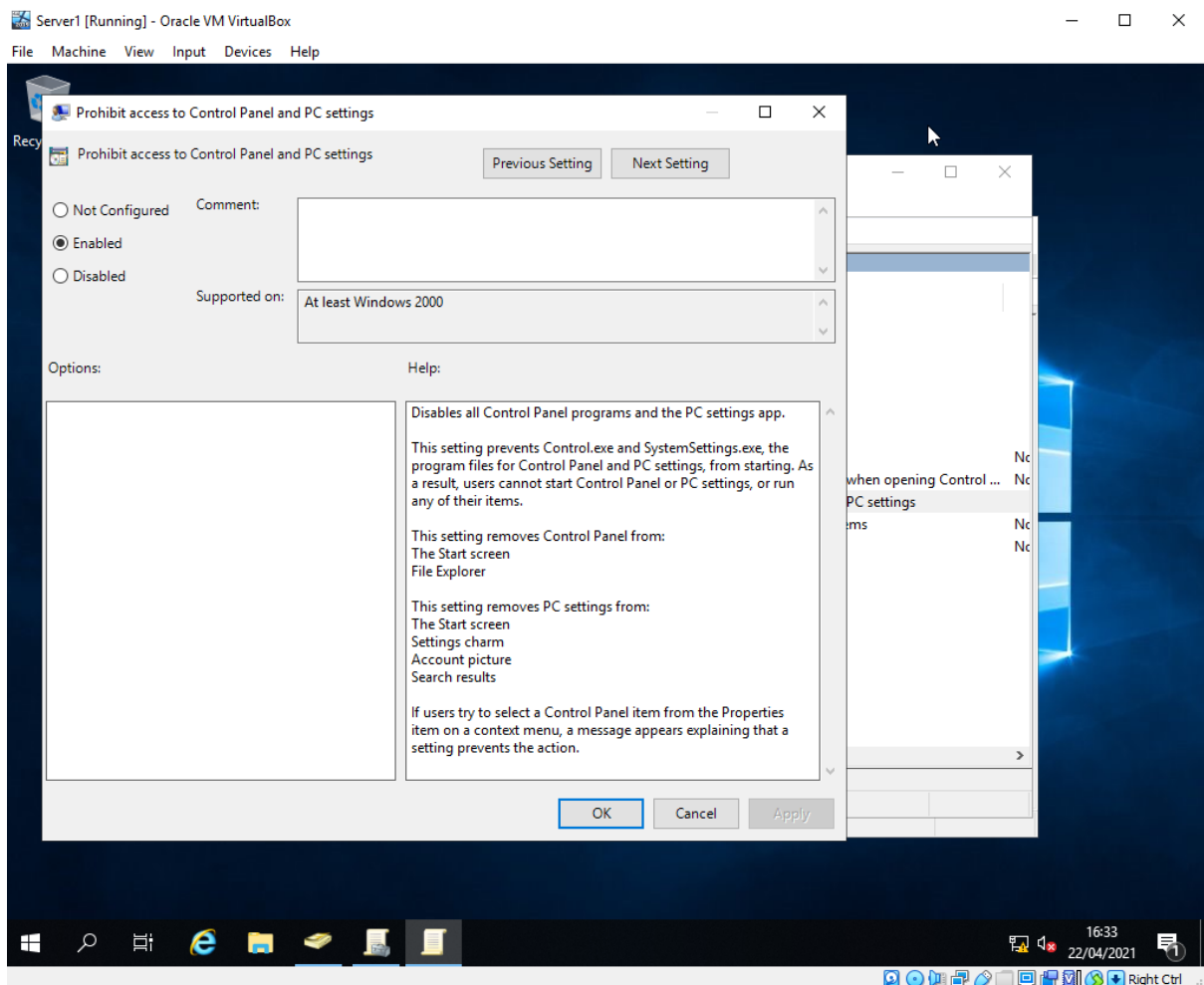


*Figure 19 Gpupdate command ran*

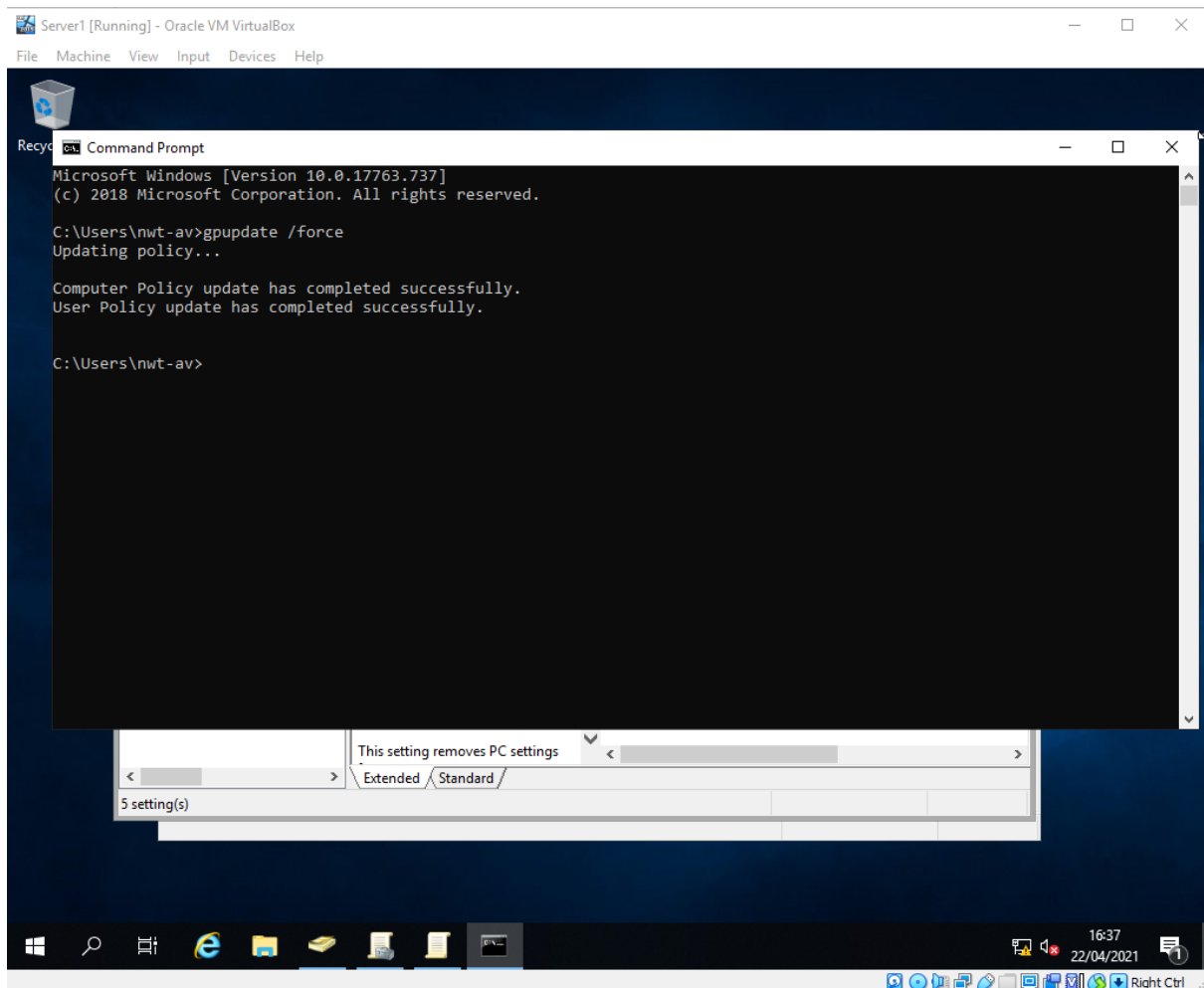
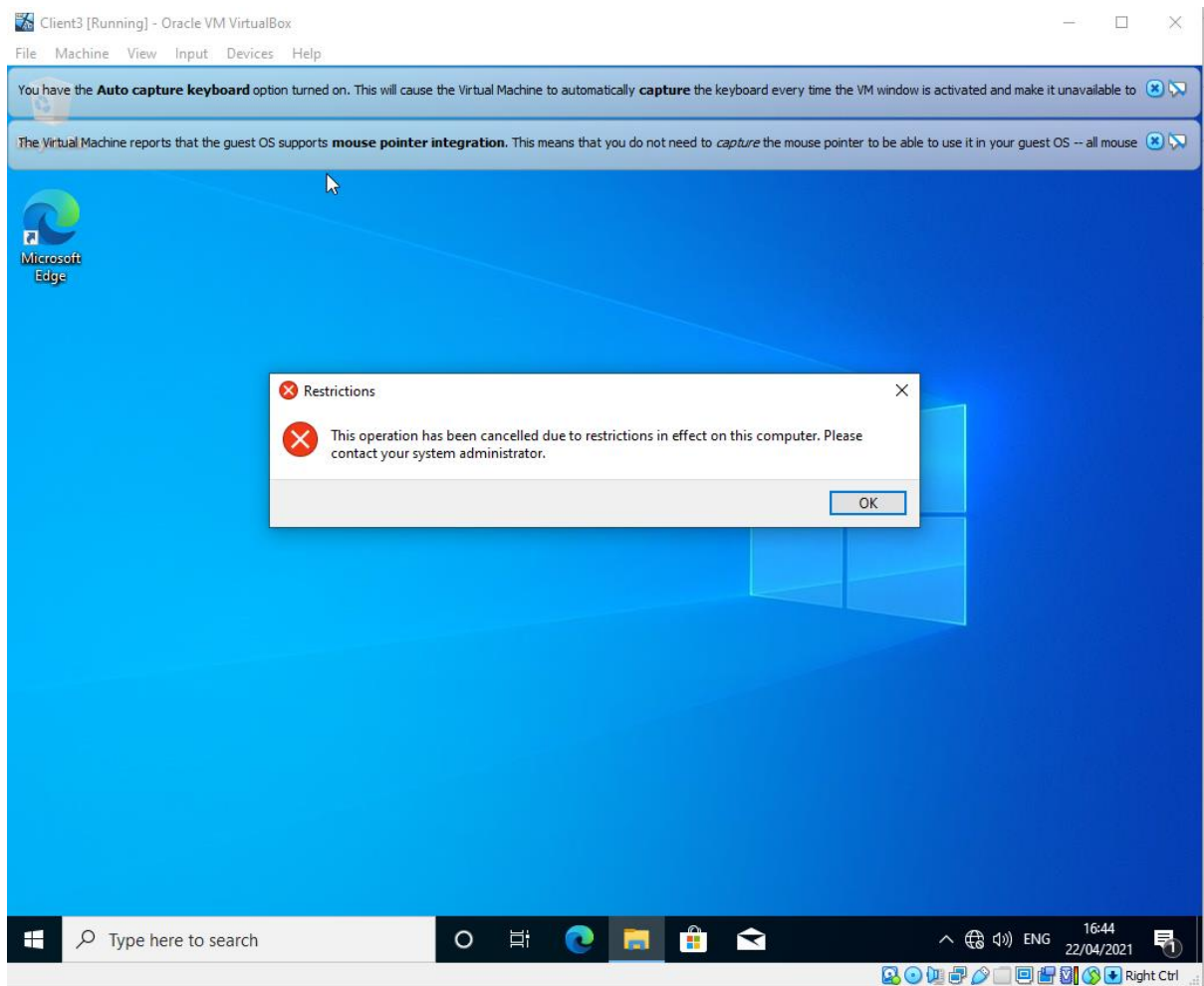


*Figure 20 The new user is unable to access the control Panel*



The screenshot displays a Windows 7 desktop environment. The desktop background is the standard Windows 7 blue logo wallpaper. In the top-left corner, there is a Recycle Bin icon. The taskbar at the bottom contains the Start button, a search icon, and several application icons including Internet Explorer, File Explorer, and a folder named '10 setting(s)'. The system tray in the bottom-right corner shows the time as 16:53 and the date as 22/04/2021, along with a notification icon.

The main window is the 'Group Policy Management Editor', which is open to the 'User Rights Assignments' section. The left-hand navigation pane shows a tree structure with 'User Rights Assignments' expanded. The right-hand pane displays the details for the 'Prevent access to the command prompt' policy. The policy is currently set to 'Enabled'. The description pane on the right provides a detailed explanation of the policy's function and a note about not preventing batch file execution if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Remote Desktop Services.

Figure 22 gpupdate command ran following policy update

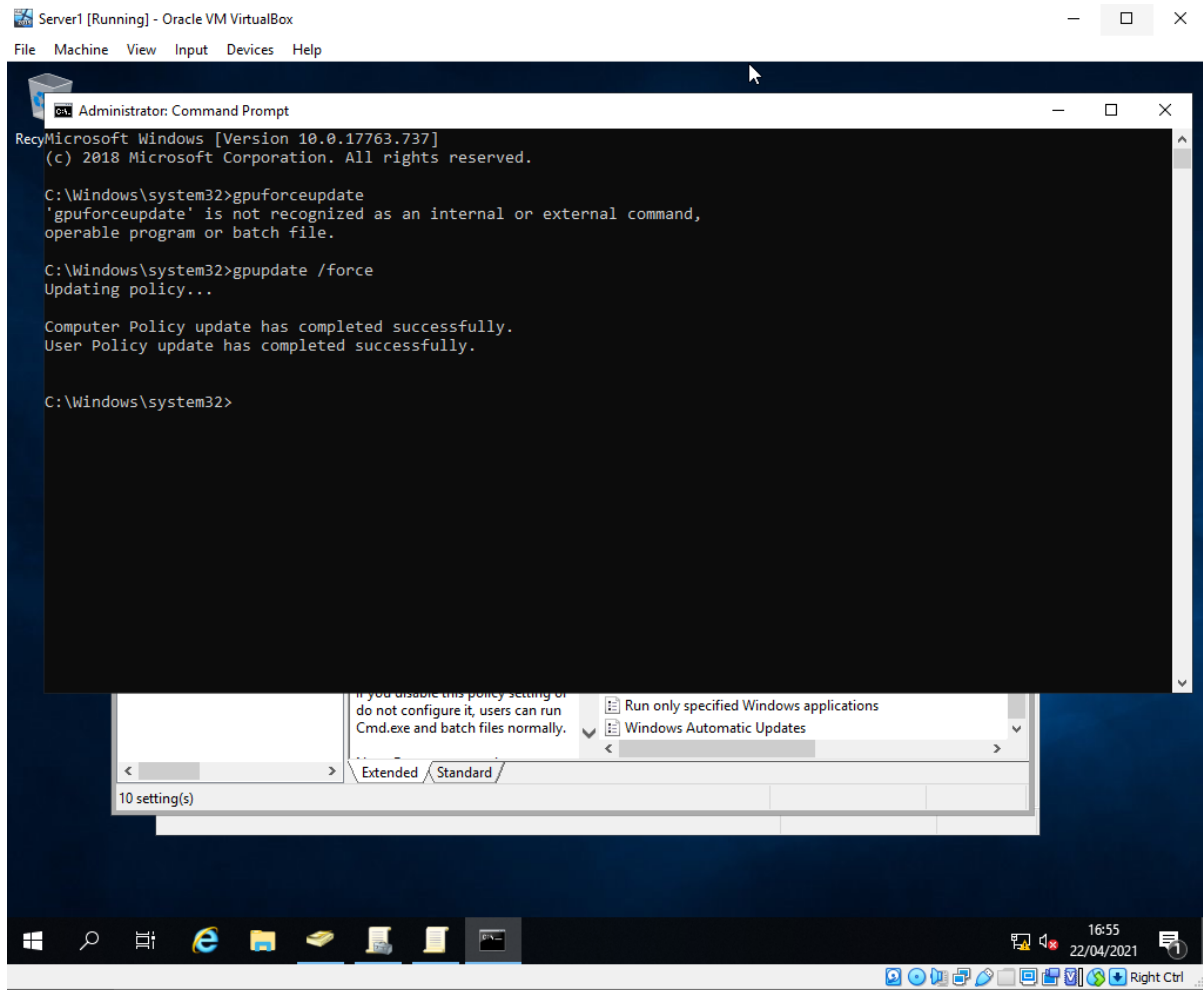


Figure 23 Evidence of command prompt disabled for new user

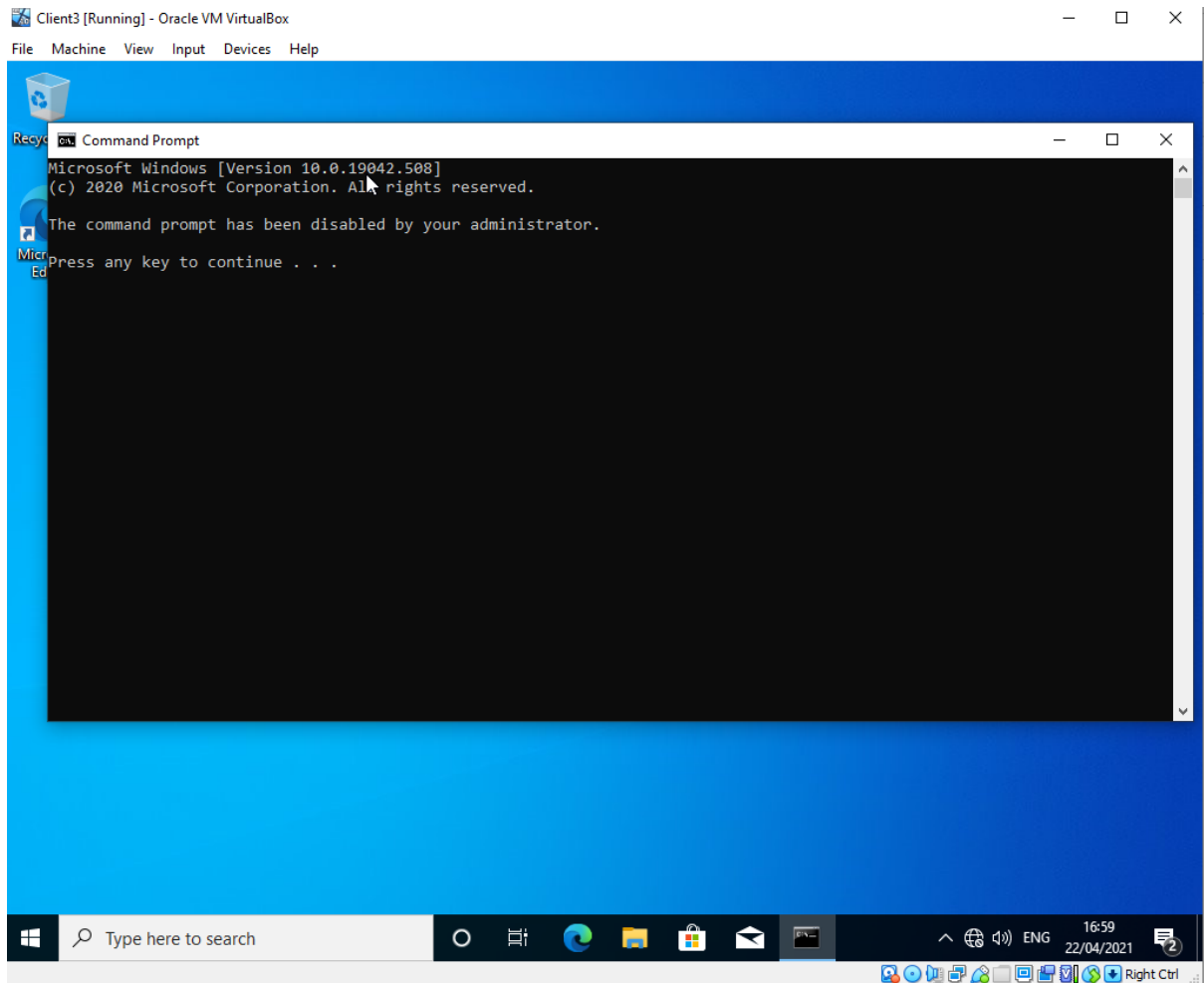


Figure 24 GPUUPDATE /FORCE MUST FIRST BE RUN IN ORDER TO APPLY THE UPDATE ACROSS THE DOMAIN.

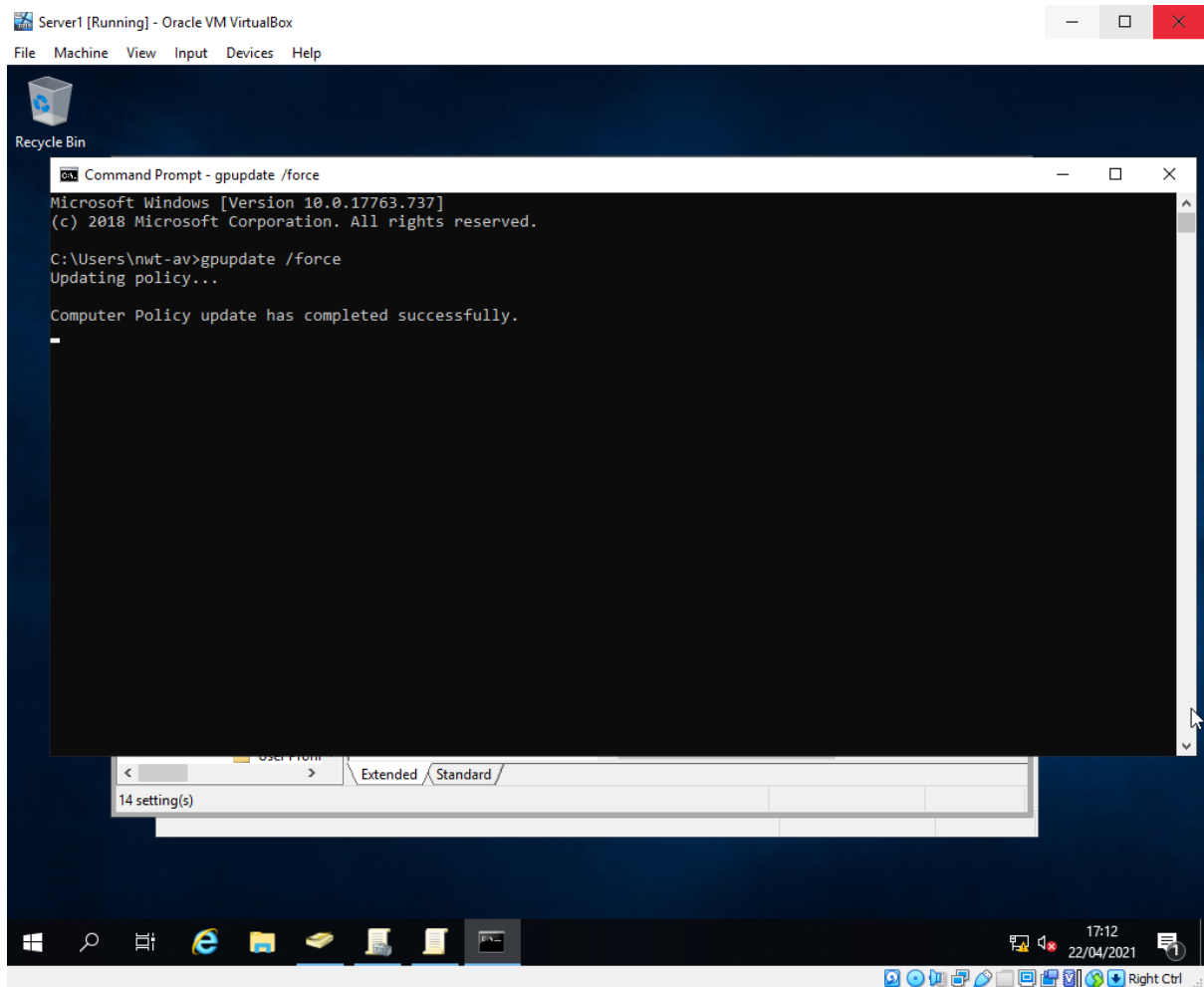


Figure 25 Error message when trying to use removable media for new user.  
Only after applying gpupdate on server1

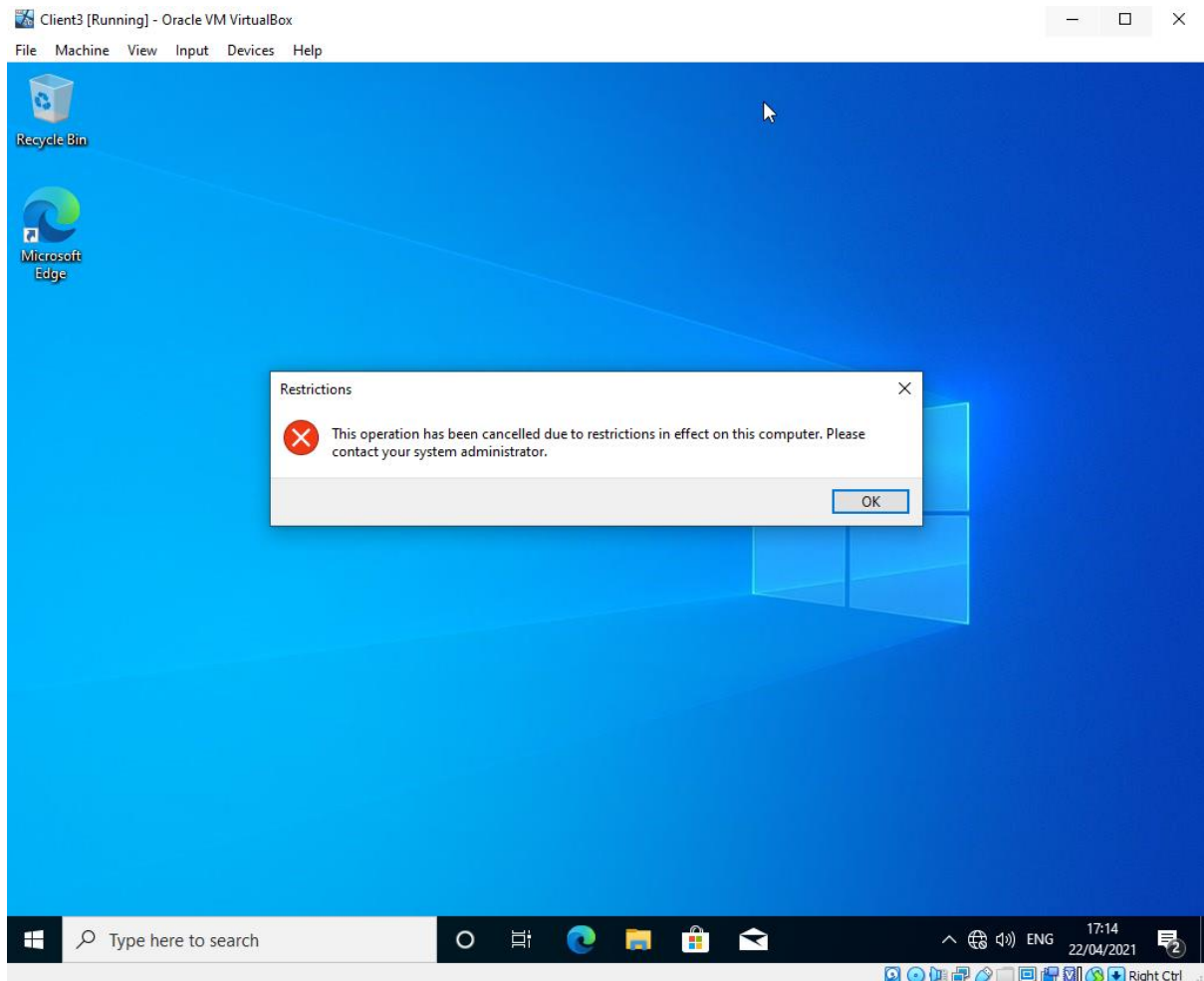


Figure 26 Computer Object moved into newly created OU

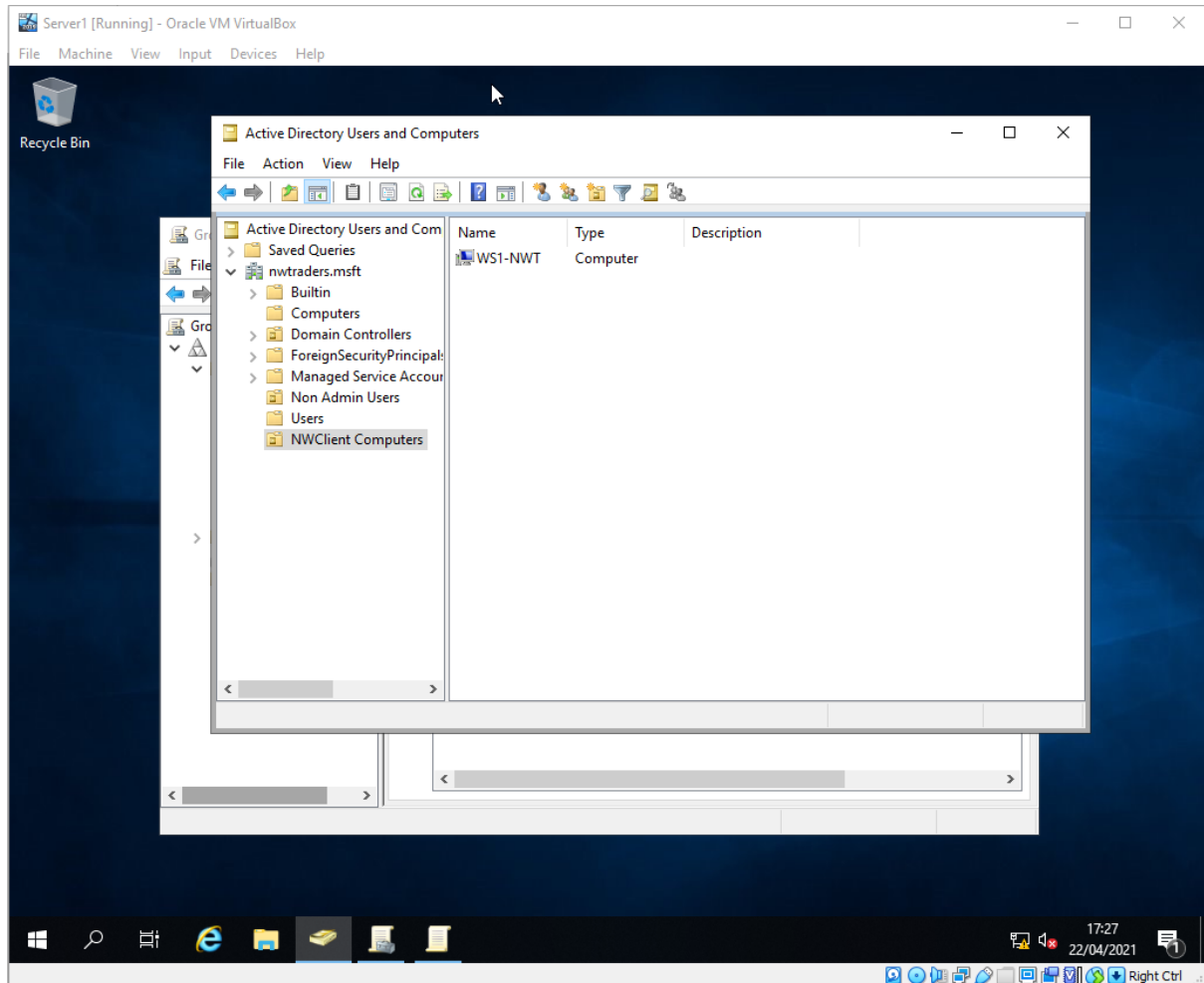


Figure 27 New group policy NounauthSoftInstallS created

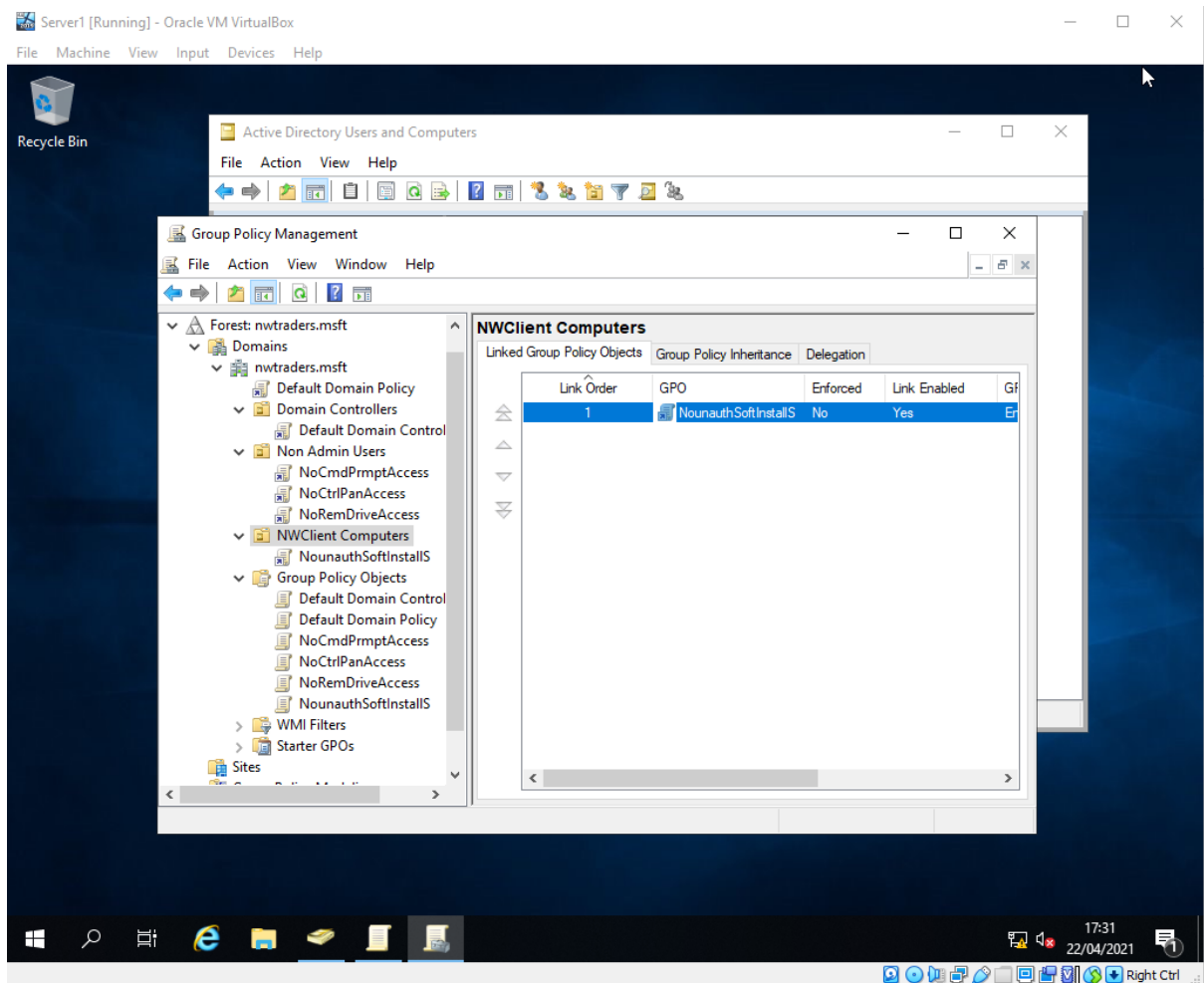


Figure 28 gpupdate ran after prohibiting user install.

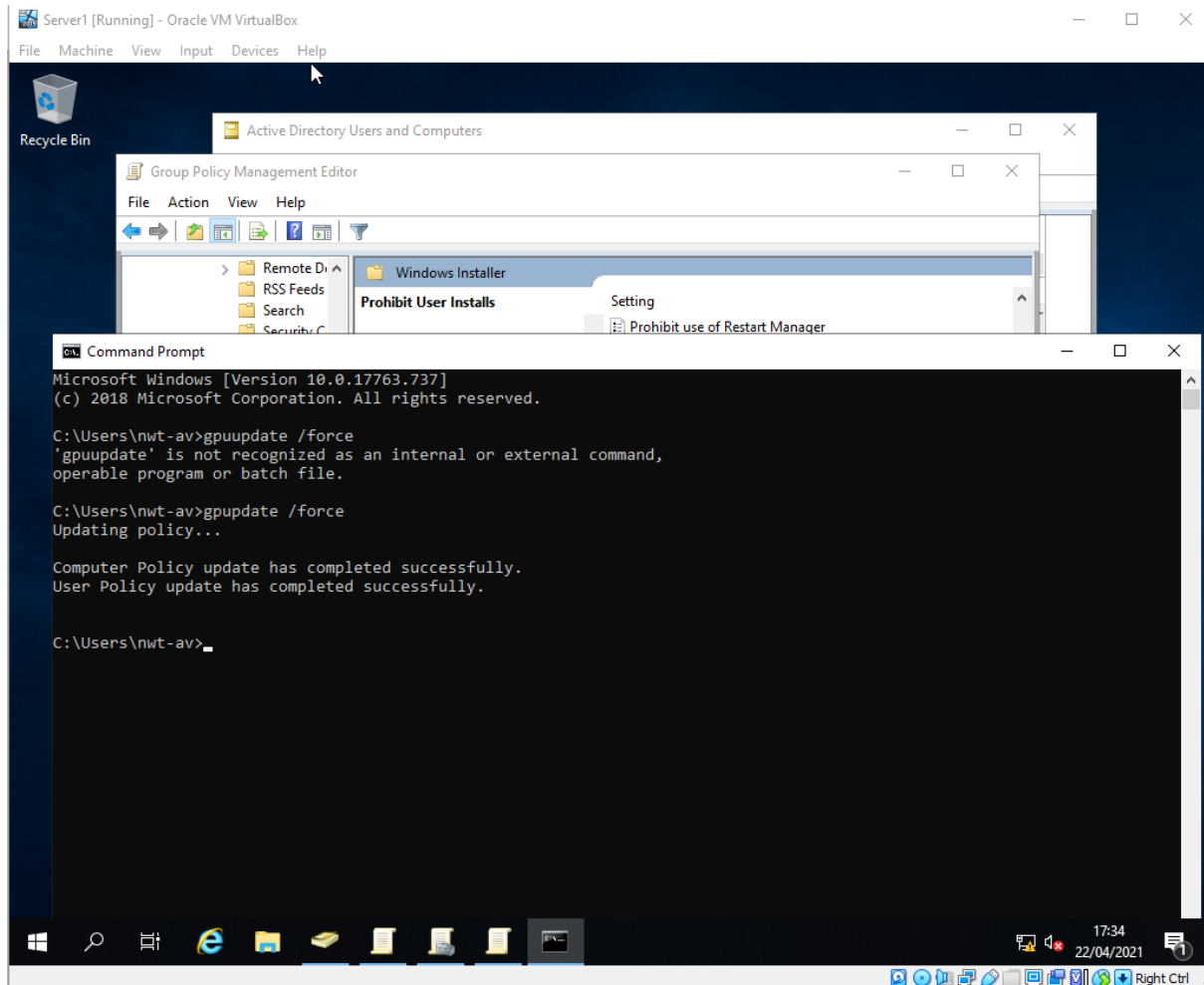


Figure 29 New user cannot install software on client. Admin prompt is displayed.

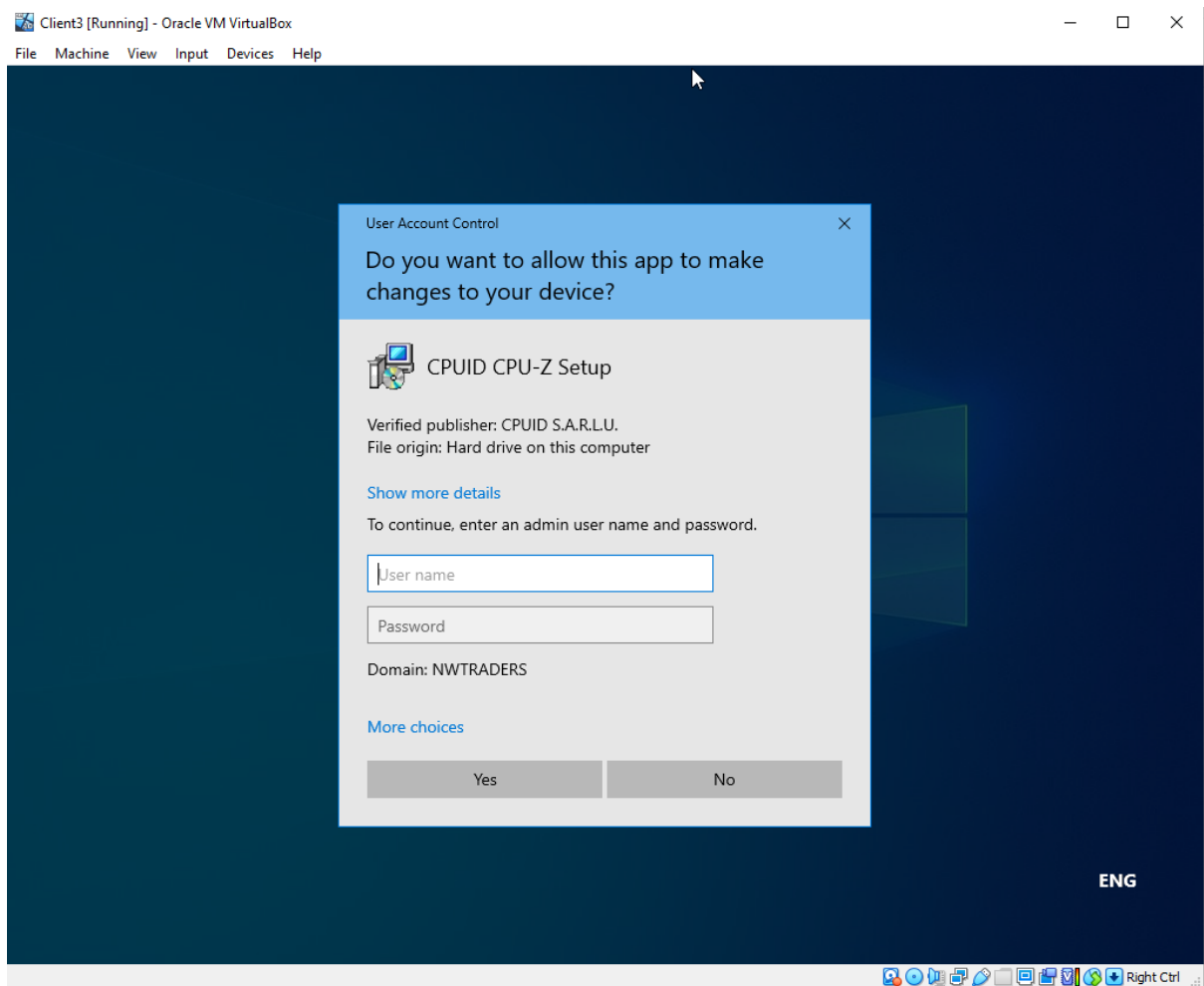


Figure 30 Password settings configured in Group Policy Password Editor

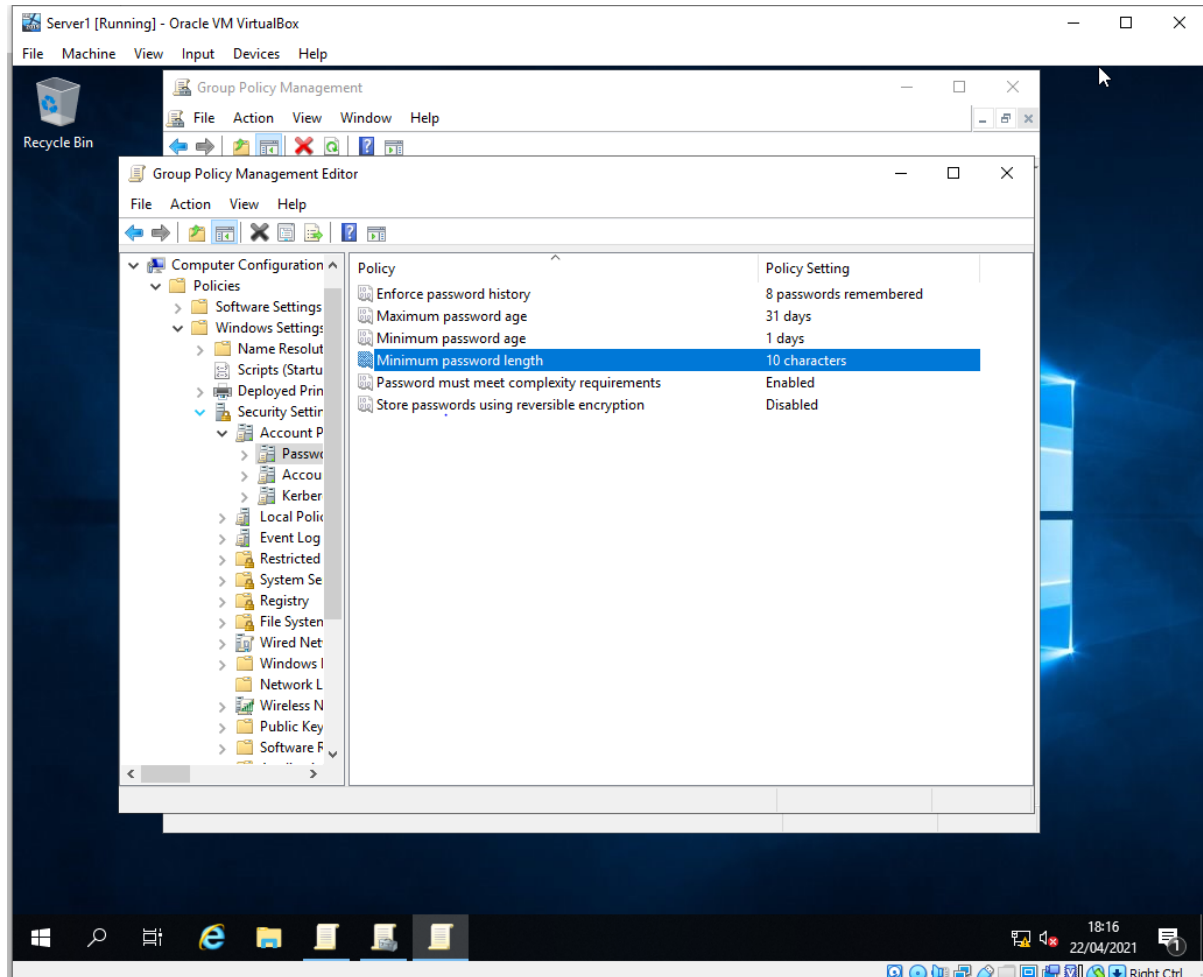


Figure 31 gpupdate to enforce new password rules across the domain

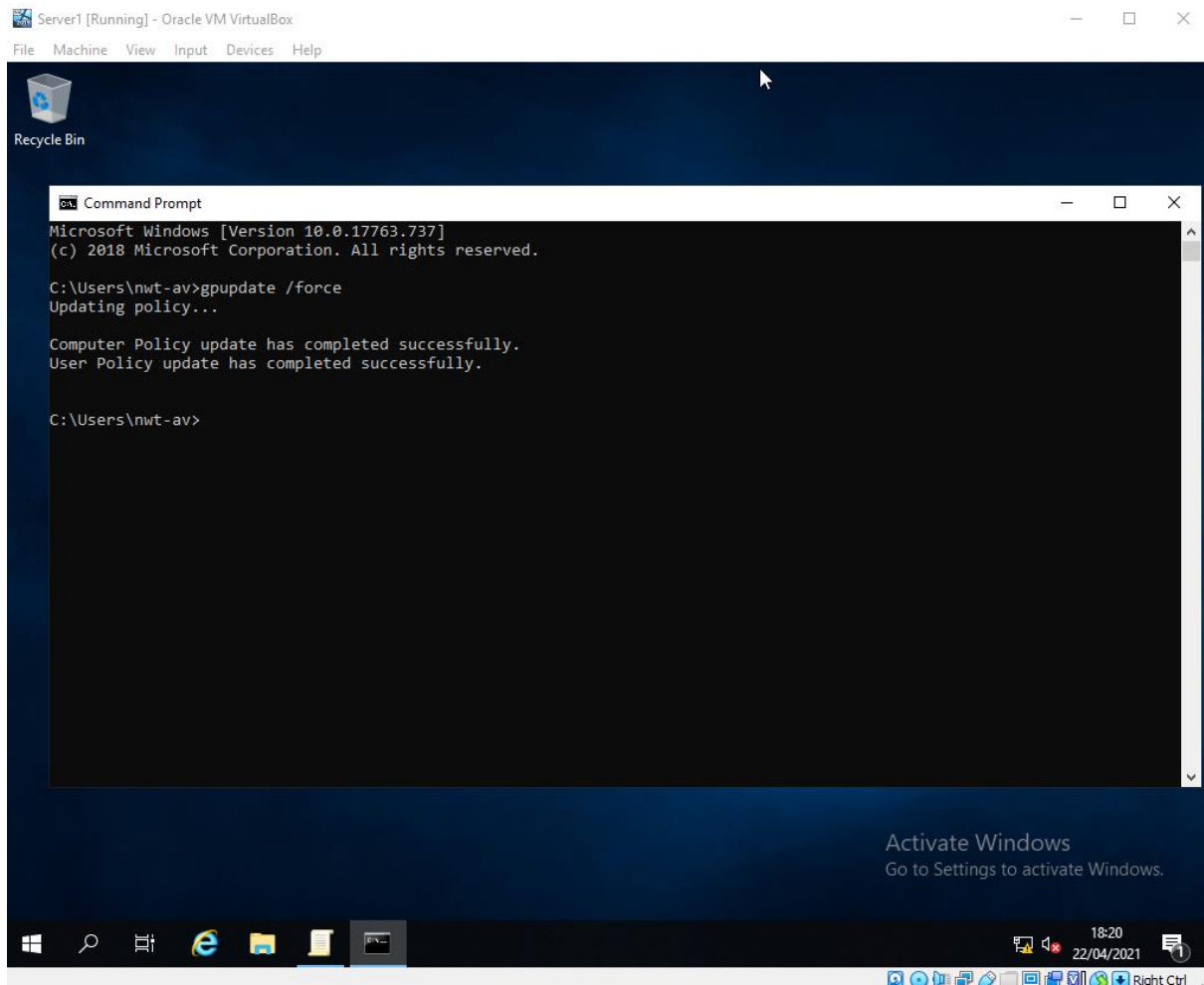
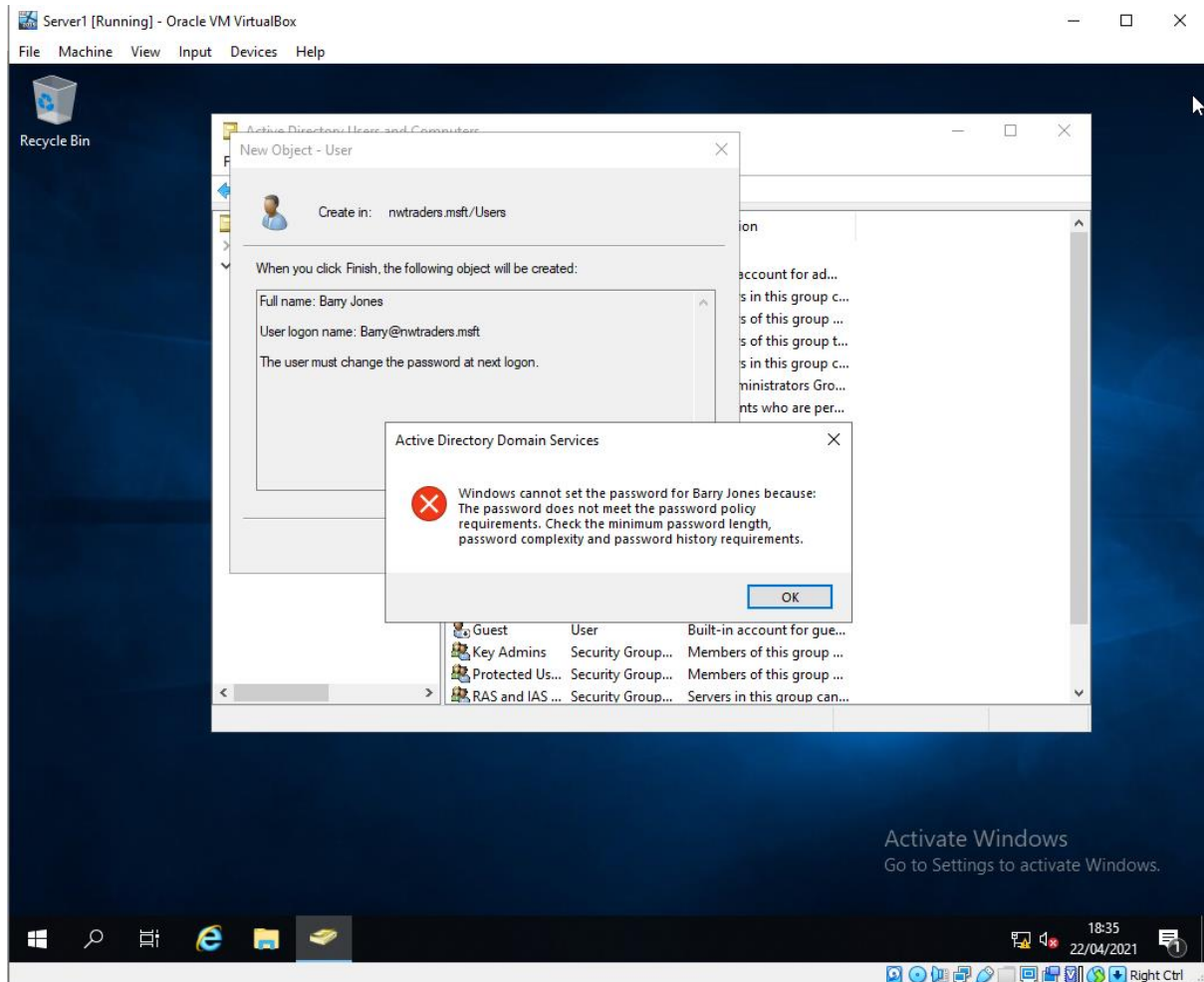


Figure 32 Evidence that it's not possible to create an account with less than the 10 characters as defined in the password policy. The same error is given if you try to create a password without special chracaters.



## Task 3: Observational Tasks

### 3 a) Explain the main differences between local permissions and file shares.

Local permissions, or New Technology File System (NTFS) permissions, and Share permissions, are both ways of allowing or preventing access by users to data on a network.

NTFS permissions are applied to data stored in NTFS file systems and applies to users both locally and on the network: the policy restrictions are applied to the user at logon, regardless of where they are accessing the network from. NTFS file systems are used for their portability and are commonly found on workstations and servers. However, share permissions are applied to the files and folders themselves within a share: the files and folders are set to "Allow" or "Deny" access or modifications to them. Share permissions can be applied to FAT and FAT32 file systems, as well as NTFS.

NTFS permissions can allow a user different levels of access to files: "Full Control" where a user can add, modify or delete files and change permissions settings for all files; "Modify", which allows the user to view and modify files, as well as add and delete files in a directory; "Read and Execute", which allows the user to read files and run scripts, but cannot make changes to or delete files; "Read", where the files can only be viewed and not changed; and "Write", where users are only able to add to files or add new files in a directory. They can be applied to all users on the network who access shared resources and can be applied to local files and folders too.

File shares work differently but perform a similar purpose to NTFS permissions. They are applied only to shared files on the network, and do not apply to local files, unlike NTFS permissions. They can however be applied to FAT and FAT32 file systems, unlike NTFS permissions. File shares have fewer, but simpler, levels of control for files than NTFS: permissions can be set to "Full Control," "Change" or "Read," which allows ease of management, but less-specific control of permissions.

### 3 b) Describe the role of Group Policy Management in the network environment, you can use example policies in your answer.

Group Policy Management, using the Group Policy Management Console (GPMC) allows a Network Administrator to configure Group Policy settings for a whole Active Directory (AD) forest. Operating systems (OS), applications and security control settings can be configured on Active Directory Organisational Units (OU) centrally from a template, without needing to apply settings locally. Group Policy Objects (GPOs), found under the "Forest > Domain" tabs of the GPMC, allow the management of these OS, applications and settings through determining the standard for behaviour of the system for specific users or computers (1). They are used to save time for the administrator, whilst maximising security when there is a need for configuration for large numbers of users and machines (1).

Policies are used to control what a user or computer is authorised to do on a system: for example, they may be used to restrict access to sensitive data or enforce password policies. It can also be used

to deploy software or files to users or computers (2) or to set scripts to run at predetermined times (3). Policies are changed using the Group Policy Management Editor, for either “Users” or “Computers”: the key difference between the two types is that the “Computer” configuration is applied on PC start-up, and the “User” policies are applied on user login (4). Policy settings take priority over other application settings, and any changes to the configuration will either be prevented entirely (greyed-out) or will revert to its original value on refresh (4). Policy settings will Background Refresh every 90 minutes ( $\pm 30$  minutes, randomised) by default, or every five minutes for Domain Controllers (5), but this can be changed if required. Preferences can also be set for computers or users, and are set when the system starts for the first time, but these are able to be changed by users as they are not enforced by a background refresh like policies are: they are instead usually applied for the convenience of the user (4).

As briefly outlined previously, there are different types of Group policies that can be applied to a GPO. Applications can be either assigned or published to either a user or computer using the GPMC (2). When an application is *assigned* to a user or computer, it is automatically installed when either the user logs in or the computer starts, respectively. Typically, software assignments are given to computers rather than users to prevent programs from being installed and uninstalled when a user logs in and out (6). This is useful for critical programs that users are likely to require in the course of their work, for example, email clients, internet browsers, word processors and other essential applications. It streamlines the deployment of new hardware, by applying a baseline functionality that is appropriate for the Group to which the user or computer belongs. A user is not able to uninstall or modify software that has been assigned to their computer or account, which prevents issues for users (and administrators) caused by unauthorised changes. They are also unable to download unauthorised software which may introduce vulnerabilities to the network. The ability to redeploy software using the GPMC ensures that updates can be rolled out to all instances where the software has been installed (2). This is an important feature of Group Policy Management, as software updates (for example, to fix security vulnerabilities) can be first tested for compatibility and then rolled out system-wide. Software updates can also be rolled-back rapidly if bugs, vulnerabilities or other issues are discovered after release to users. It ensures that all users or computers belonging to a GPO will have the same software versions, without the need for an administrator to update individual computers, or relying on users to accept software update requests. Applications can also be *published*, which adds the program to the “Add or Remove Programs” feature in Windows, to allow users to install it if they choose.

The GPMC can also be used to deploy files or folders across domain computers. Common uses for this functionality are to ensure scripts, system tools and configuration or INI files are automatically copied or updated on all user computers (7). This ensures that computers across the system can be initialised, maintained and updated efficiently, preventing conflicts and security vulnerabilities that may be caused by incompatible or out of date settings or scripts.

Scripts can be scheduled using the GPMC, for example, computer startup and shutdown scripts, or user logon and logoff scripts (8). These can be used to automate essential tasks, for example to map network drives and install a default printer when a user logs in, to remove temporary files that were created during a session when a user logs off, or backup files and folders before a computer is shutdown.

The GPMC is also used to restrict access to servers, computers or share drives for a GPO. For example, a computer that is connected to — or reserved for use with — a piece of equipment can be set to only allow users who are authorised to use that equipment (i.e., members of that GPO) to

logon to it. Removable storage drives can also be restricted or allowed as required. It may be necessary for removable storage drives to be disabled for most normal users on the network for security purposes. This will prevent unauthorised copies of sensitive data being made and lost, and prevent removable storage devices that are infected from affecting the network. There may be exceptions that need to be added, for example if equipment uses removable storage for data logging, it can be added to a GPO that will allow this.

The GPMC is used to apply password policies to users, ensuring that all users have an appropriate password according to local policy. This is discussed in more detail in the next section,

### 3 c) Give some examples of sound 'password' principles in modern network environments.

Passwords are an essential method of authentication for users to access a network. The breaching of passwords on a network is a common cause of security concerns for an administrator. Insufficient password requirements can allow unauthorised access to a network and compromise data security, while overzealous requirements can dissuade users from engaging with password security requirements and, for example, write their password down, thereby negating the entire purpose of the requirements.

Any organisation must have a clear, comprehensive password policy for users (and administrators) to adhere to, in order to ensure both security and practicality. The Digital Identity Guidelines published by the National Institute of Standards and Technology (NIST) are commonly used as a basis for a secure password policy for enterprise networks (9).

The NIST Digital Identity Guidelines state that passwords that are chosen by a user should be a minimum of eight characters in length with a maximum character limit of up to 64 characters (9). As such, the administrator should impose an eight-character minimum limit for password acceptance when the user creates their password. Where the administrator creates a random password for a user, for example, when a password is reset or when the account is first created, the password should be a minimum of six characters in length, entirely numeric, and created using a random bit generator (9).

The password should be of sufficient complexity that it is not easily guessed or otherwise discovered. It is important that this point be emphasised in the network password policy. The administrator of a network environment should allow all print ASCII characters and the space character to be included in a password, plus Unicode characters to allow the user to create any complex password of their own choosing. However, NIST no longer advises verifiers to impose any complexity requirements on user passwords at creation: people have a limited capacity to remember complex, arbitrary passwords, and enforcing complexity requirements has a minimal benefit for security, but serious detriment to usability (9). In one study, using simulated password-cracking algorithms, it was found that a basic, sixteen-character password was superior to a complex eight-character password against large numbers of guesses (10). As such, it is better from a security perspective to encourage longer passwords that are easily memorable to the user, than to impose complex passwords that are less likely to be remembered, causing the user to record their password somewhere, thereby causing a security vulnerability. For this reason, it is also important not to

require periodic password changes, and only require a password change in the evidence of security vulnerabilities or breaches (9).

Password creation requests should be compared against a blacklist of forbidden passwords, and then any unsuitable or unsafe requests rejected (9). These may be passwords that consist of repeating characters (e.g. "12341234", or "zzzzzzzz"), dictionary words, passwords that consist of the name of the service or username, and passwords that have been used in previous breaches. It has been shown that using a robust password blacklist increases password security against being guessed (11). Ideally, the service should offer guidance to the user when selecting a password, for example by using a password-strength meter, as this has been shown to support the user in selecting a strong password (11).

It is important to implement a rate-limiting mechanism, such as a Captcha or time-out, in order to prevent brute-force guessing attacks or Distributed Denial-of-Service (DDoS) attacks caused by rapid, repeated failed login attempts (9).

One-way key derivation functions (KDF) should be used to hash passwords, this prevents an attacker from (or makes it prohibitively expensive to-) learning user passwords should they manage to access the hashed password files (9).

## Bibliography

1. **DoD Cyber Exchange.** Group Policy Objects. *DoD Cyber Exchange Public*. [Online] [Cited: 20 April 2021.] <https://public.cyber.mil/stigs/gpo/>.
2. **Microsoft.** Use Group Policy to remotely install software. *Microsoft*. [Online] September August 2020. [Cited: 20 April 2021.] <https://docs.microsoft.com/en-us/troubleshoot/windows-server/group-policy/use-group-policy-to-install-software>.
3. **Knowledge Base, Indiana University.** Group Policies in Microsoft Active Directory. *Knowledge Base*. [Online] Indiana University, 30 August 2018. [Cited: 20 April 2021.] <https://kb.iu.edu/d/aigk>.
4. **Wilson, M.** Group Policy Management - Guide & Tutorial along with Defintions! *PC & Network Downloads*. [Online] 19 November 2020. [Cited: 20 April 2021.] [https://www.pcworld.com/group-policy-management#:~:text=Group%20Policy%20\(GP\)%20is%20a,within%20an%20Active%20Directory%20environment.&text=This%20feature%20helps%20network%20admins,to%20set%20a%20new%20configuration..](https://www.pcworld.com/group-policy-management#:~:text=Group%20Policy%20(GP)%20is%20a,within%20an%20Active%20Directory%20environment.&text=This%20feature%20helps%20network%20admins,to%20set%20a%20new%20configuration..)
5. **Knowledge Base, Indiana University.** Why your Windows group policy doesn't take effect immediately. *Knowledge Base*. [Online] Indiana University, 14 January 2019. [Cited: 20 April 2021.] <https://kb.iu.edu/d/ajqs>.
6. —. ARCHIVED: In the IU Active Directory, how should I deploy software? *Knowledge Base*. [Online] Indiana University, 5 August 2018. [Cited: 21 04 2021.] <https://kb.iu.edu/d/akcl>.
7. **Windows OS Hub.** Copy Files or Folders to All Computers via GPO. *Windows OS Hub*. [Online] 26 November 2020. [Cited: 20 April 2021.] <http://woshub.com/copy-files-on-all-computers-group-policy/>.
8. **Microsoft.** Using Startup, Shutdown, Logon and Logoff Scripts in Group Policy. *Microsoft*. [Online] 08 August 2016. [Cited: 20 April 2021.] [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn789196\(v=ws.11\)#:~:text=user%20logon%20scripts-,To%20assign%20user%20logon%20scripts,Scripts%20\(Logon%2FLogoff\)..](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn789196(v=ws.11)#:~:text=user%20logon%20scripts-,To%20assign%20user%20logon%20scripts,Scripts%20(Logon%2FLogoff)..)
9. **Grassi, PA et al.** *Digital Identity Guidelines: Authentication and Lifecycle Management*. Gaithersburg, MD : National Institute of Standards and Technology, 2017. SP 800-63B.
10. *Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms.* **Kelley, PA et al.** Pittsburgh, PA : 2012 IEEE Symposium on Security and Privacy, 2012.
11. *Password Creation in the Presence of Blacklists.* **Habib, H et al.** Chicago : Internet Society, 2017. ISBN 1-891562-47-9.