# CPEN 418: Security in Computer Systems
# Lab 2

**Name: ASAAH COLLINS**

**ID: 10852443**

## Exercise 1: Adding users to the system.

[3 – 7] Adding new account.

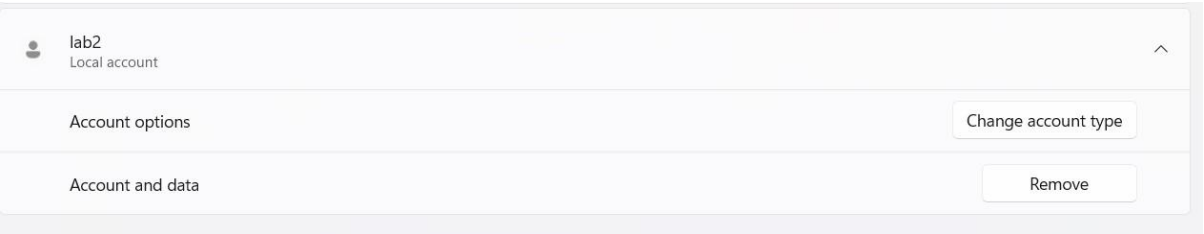


Fig 1.1 lab2 user created.

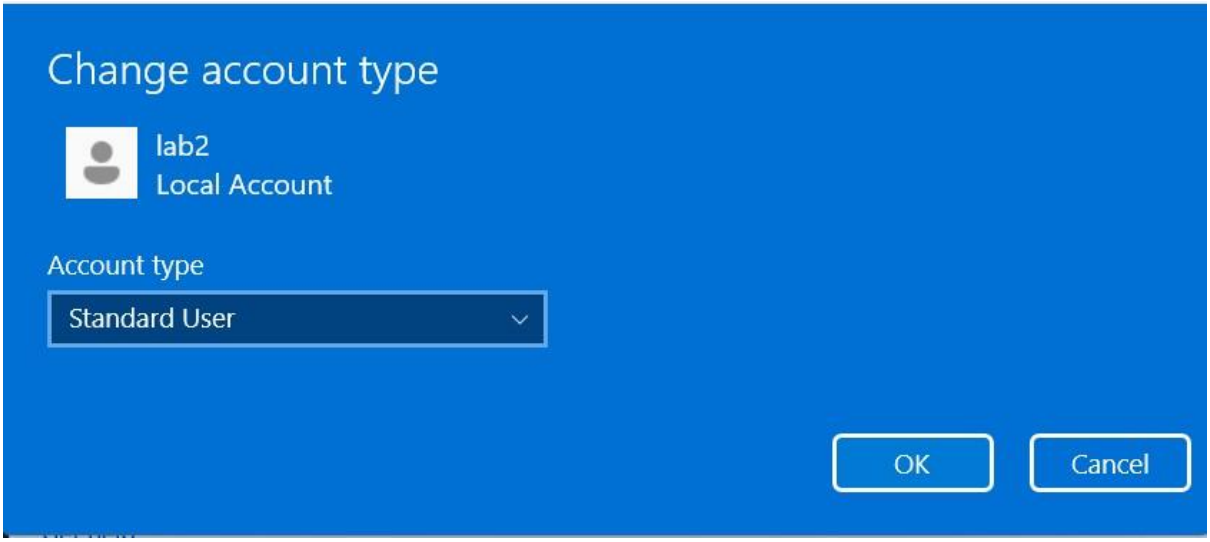


Fig 1.2 Account type set to standard user.

## Exercise 2: Studying the effects of using the Read-Only and Hidden attributes of a file

[1 – 5] Creating read-only files

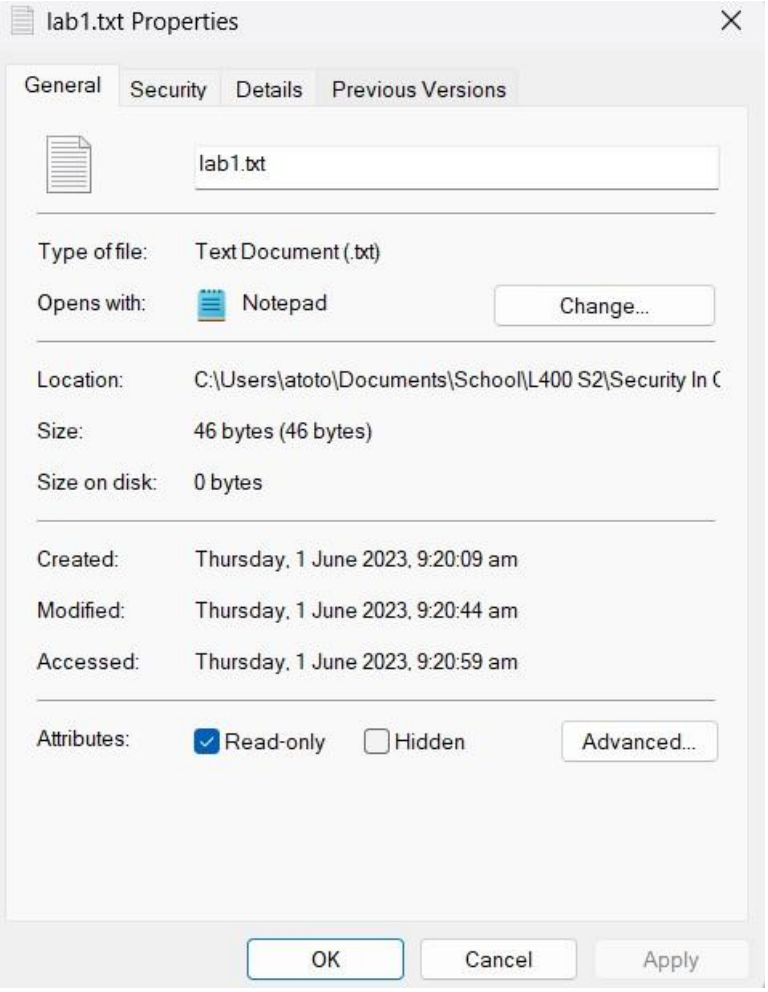


Fig 2.1 File set to read-only.

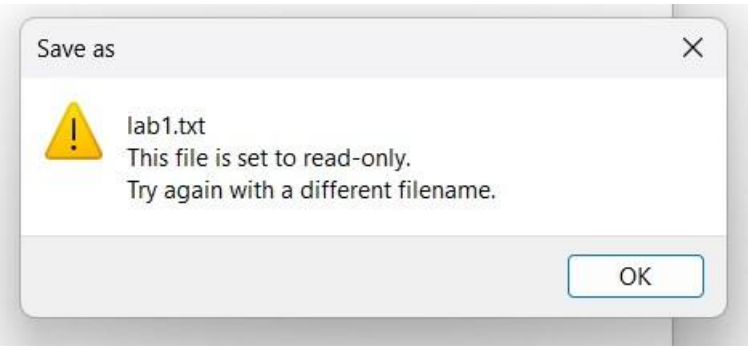


Fig 2.2 Save error for read only file

**Q5. The file has been set to read only. This results in any efforts to make changes to it causing an error. This error occurs because changing the contents of a read-only file violates its properties.**

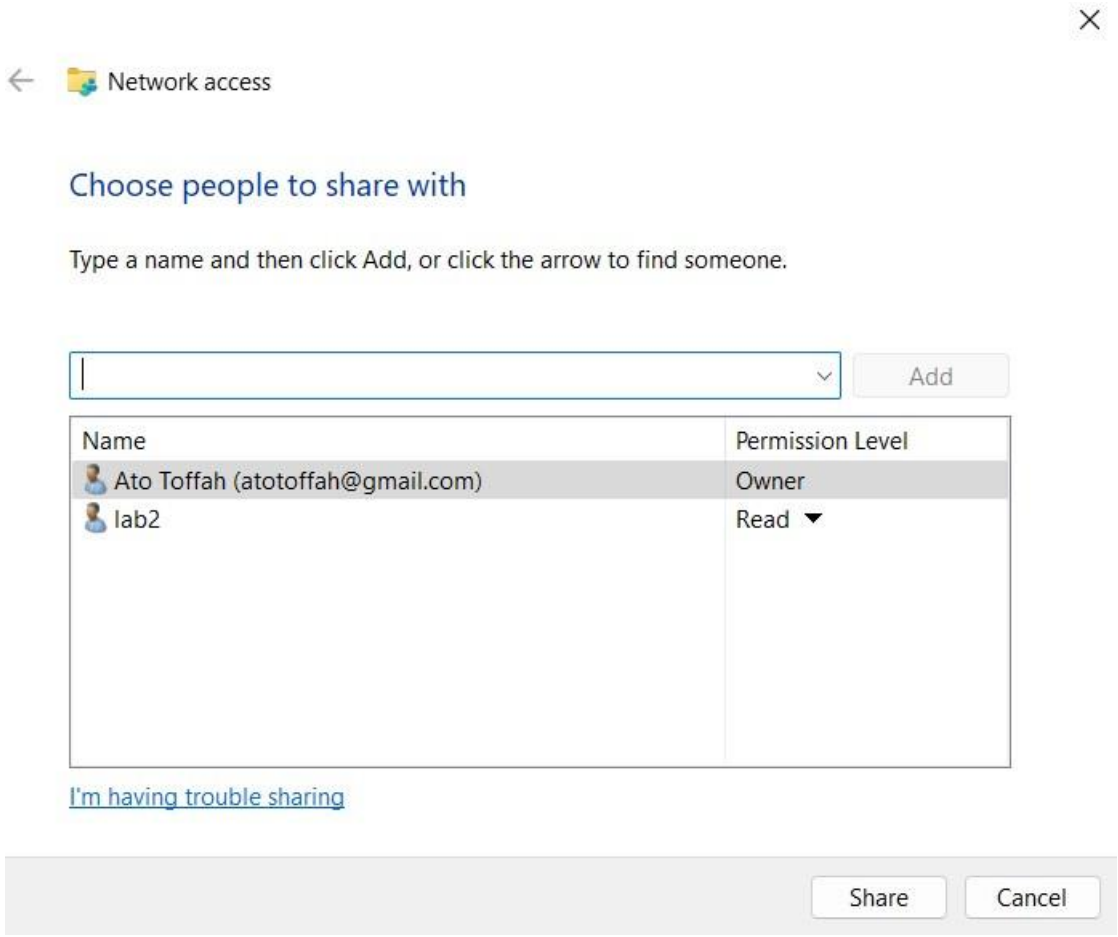


Fig 2.3 Sharing file with other user

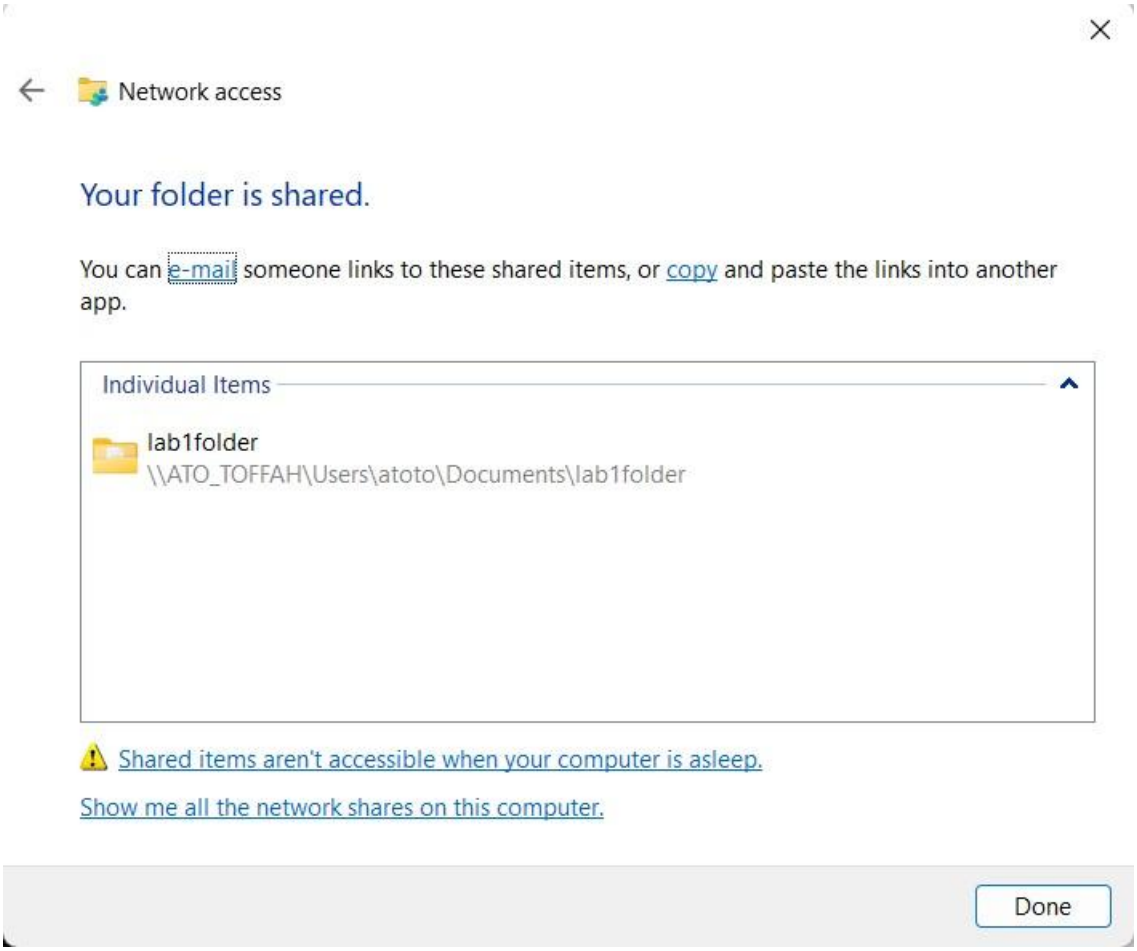


Fig 2.4 File shared successfully

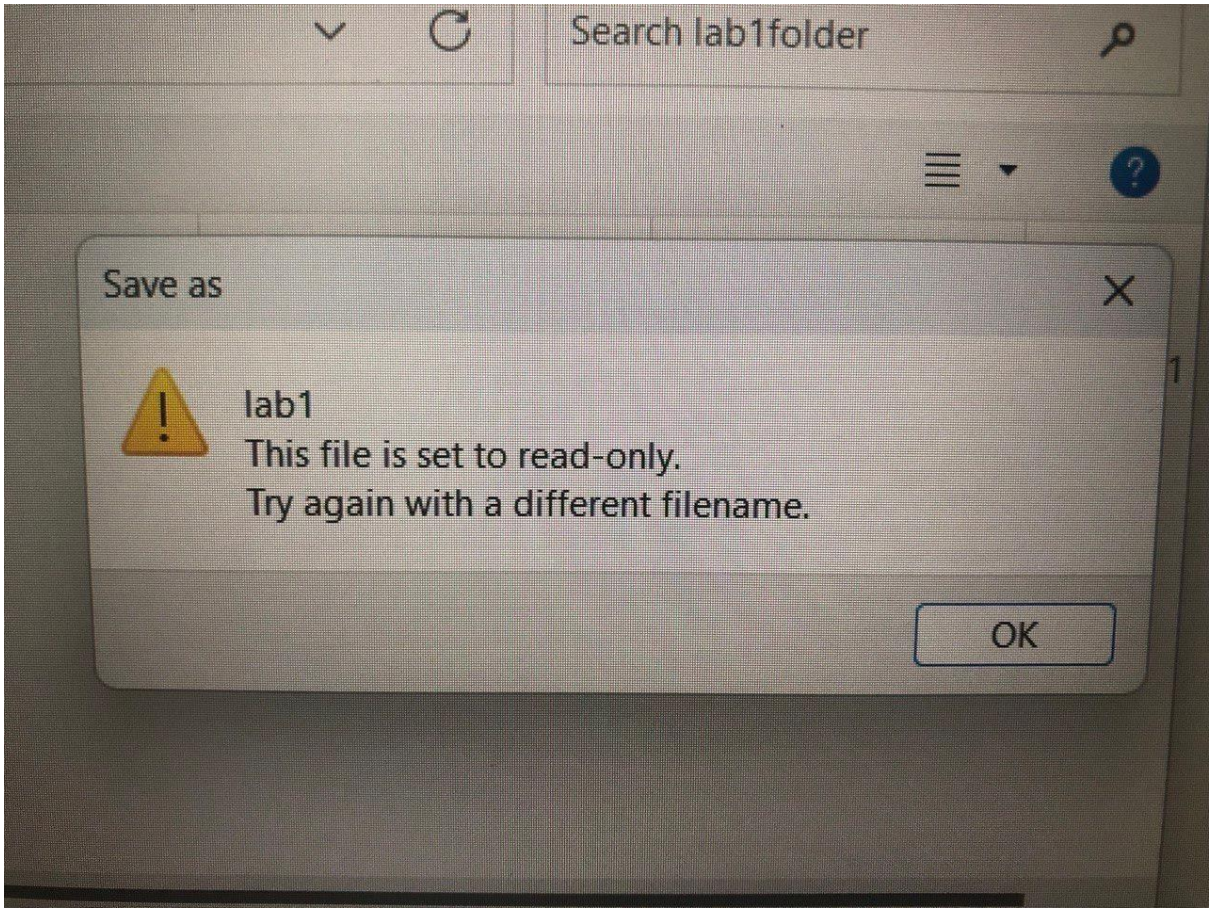


Fig 2.5 lab2 user modification attempt

**File cannot be modified by the other user as it is read only.**

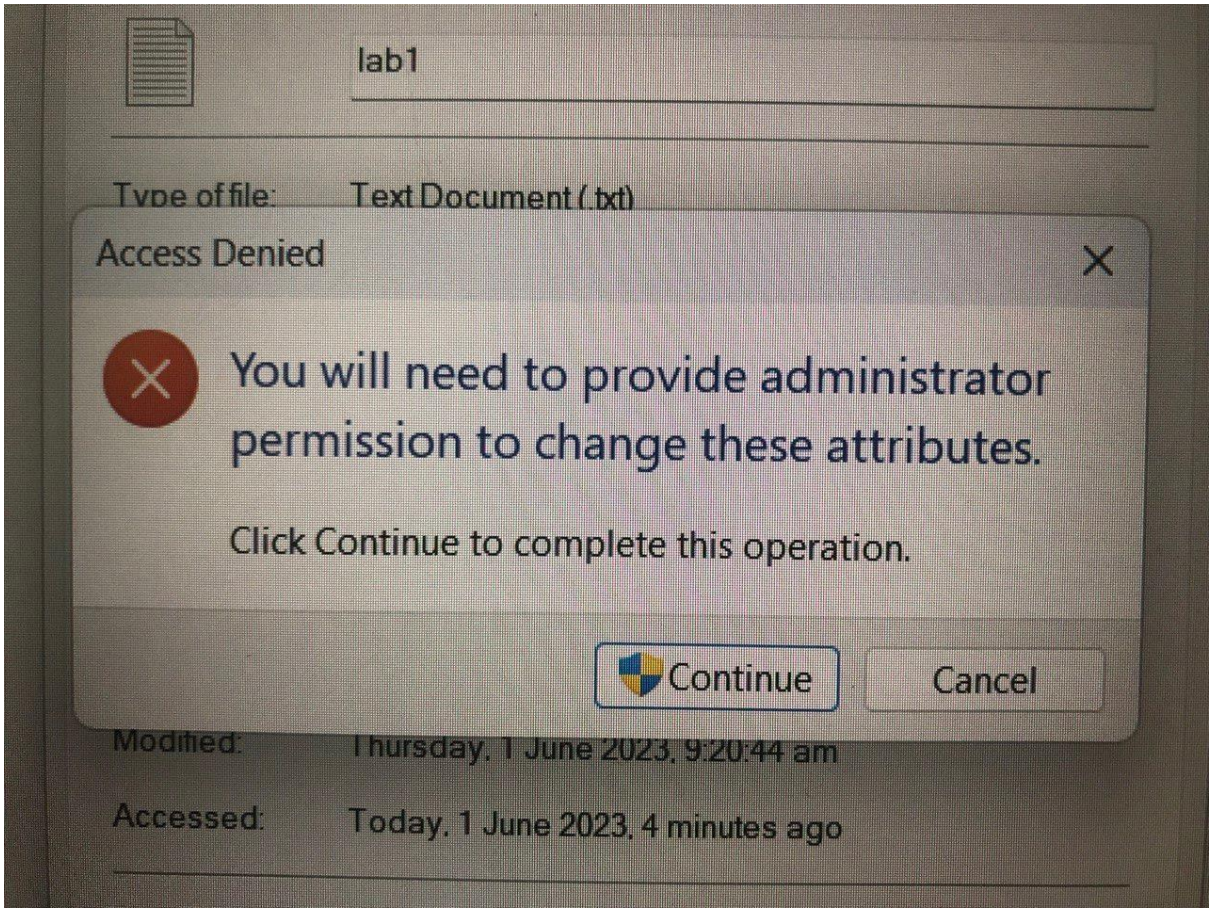


Fig 2.6 lab2 user change read-only property

**lab2 user cannot make changes to shared file properties without permission from the administrator.**

This folder is empty.

Fig 2.7 File hidden and can no longer be seen in folder.




**Q14. Go to: View > Show > Hidden Items to view hidden items in the folder.**

# Exercise 3: Demonstrate the Use of Encryption of Files

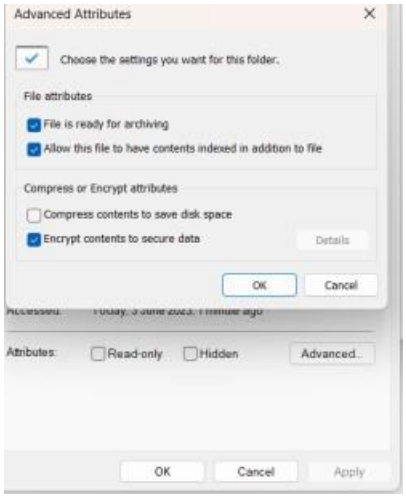


Fig 3.1 Encrypting file

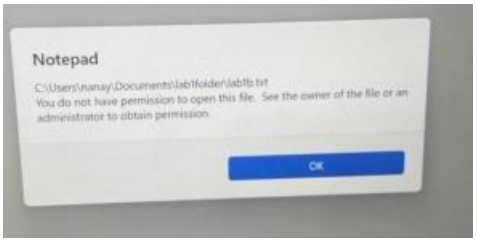


Fig 3.2 lab2 user cannot access encrypted file

## Exercise 4: To Explicitly Assign Permissions to Different Users for a Given File

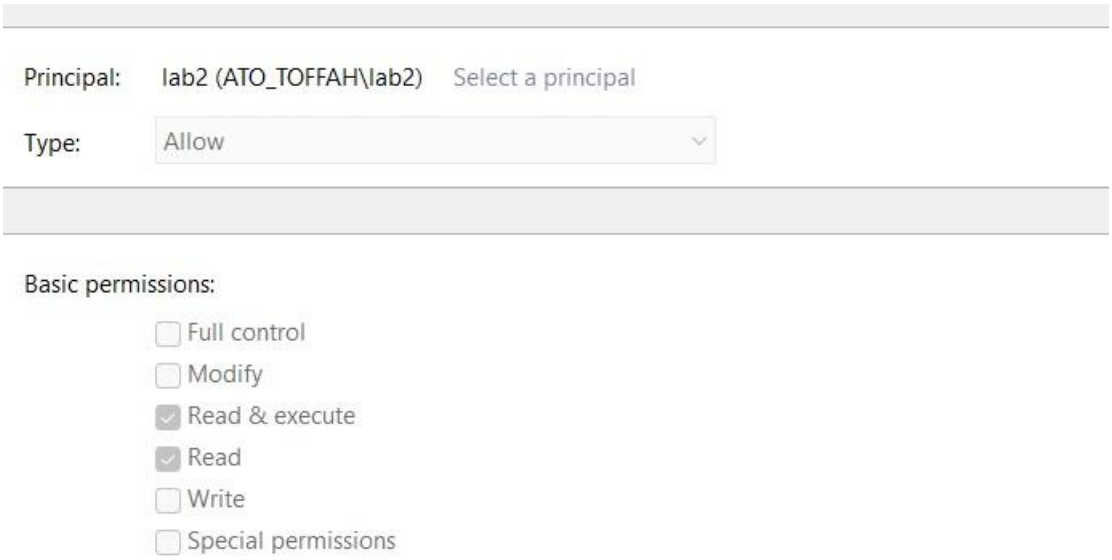


Fig 4.1 lab2 default permissions

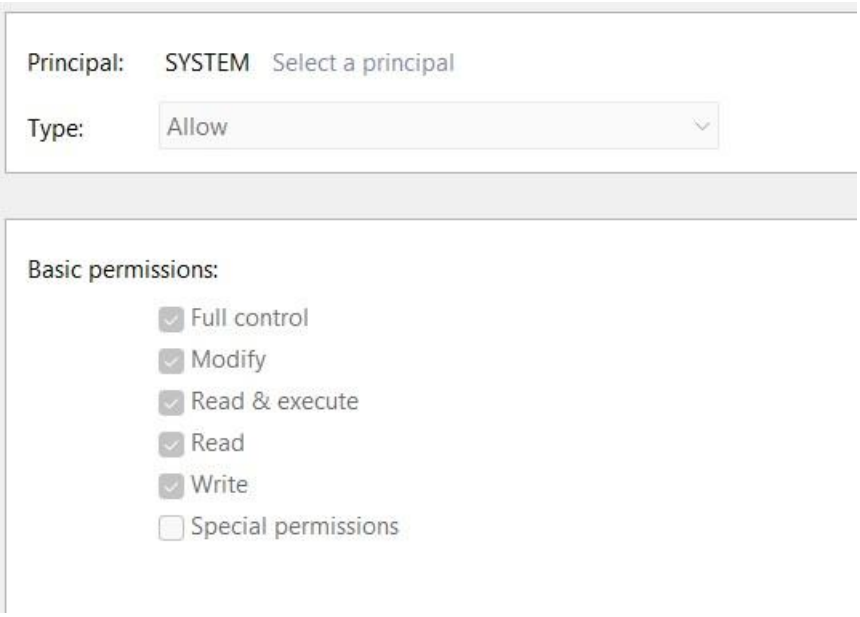


Fig 4.2 System default permissions

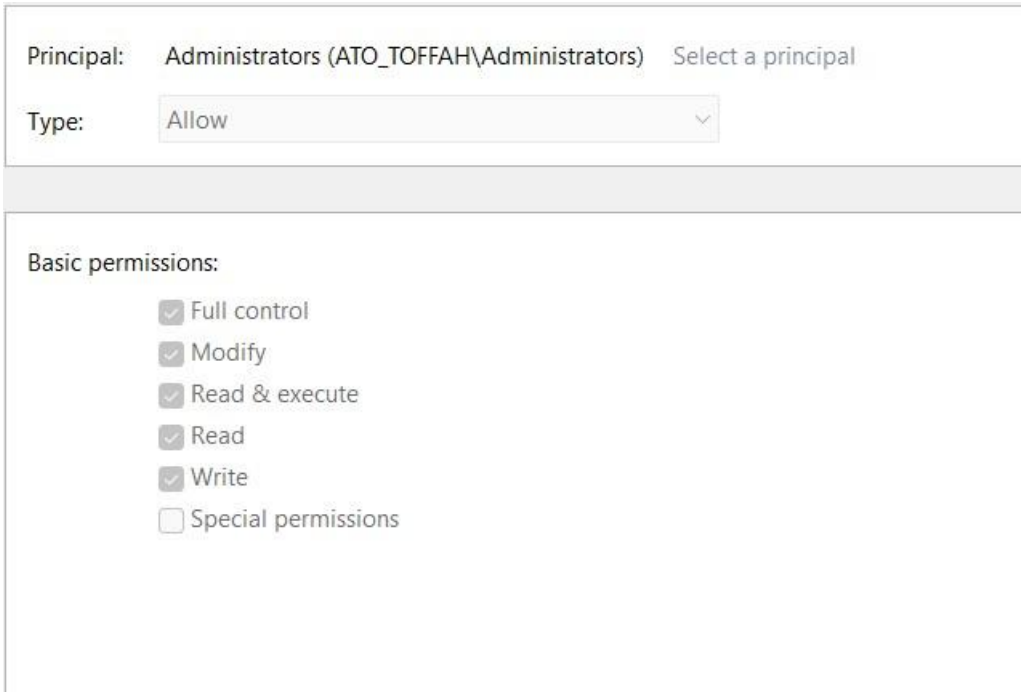


Fig 4.3 Administrators default permissions.

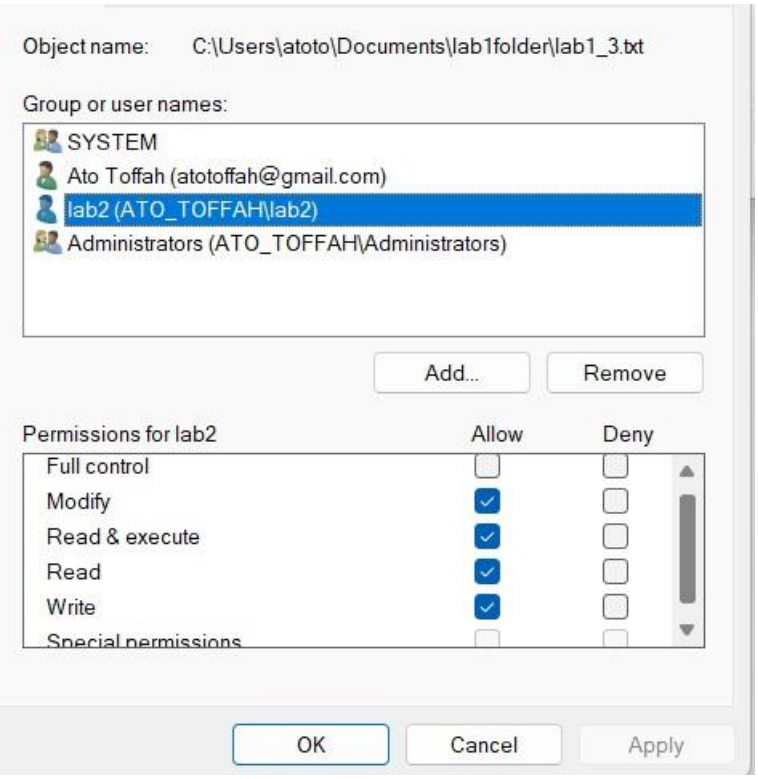


Fig 4.4 View/ Edit permissions

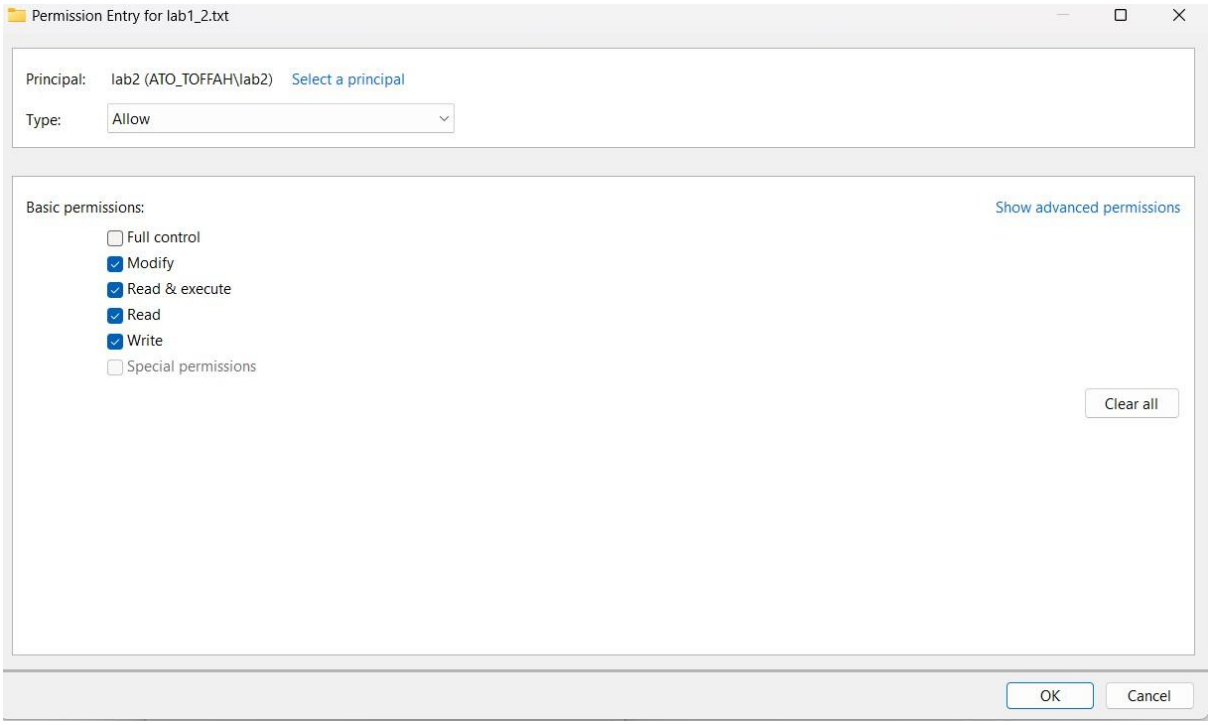


Fig 4.5 lab2 new permissions.

**After changing the permissions, it can be seen in the advanced window that lab2 user can now modify and write to the file.**

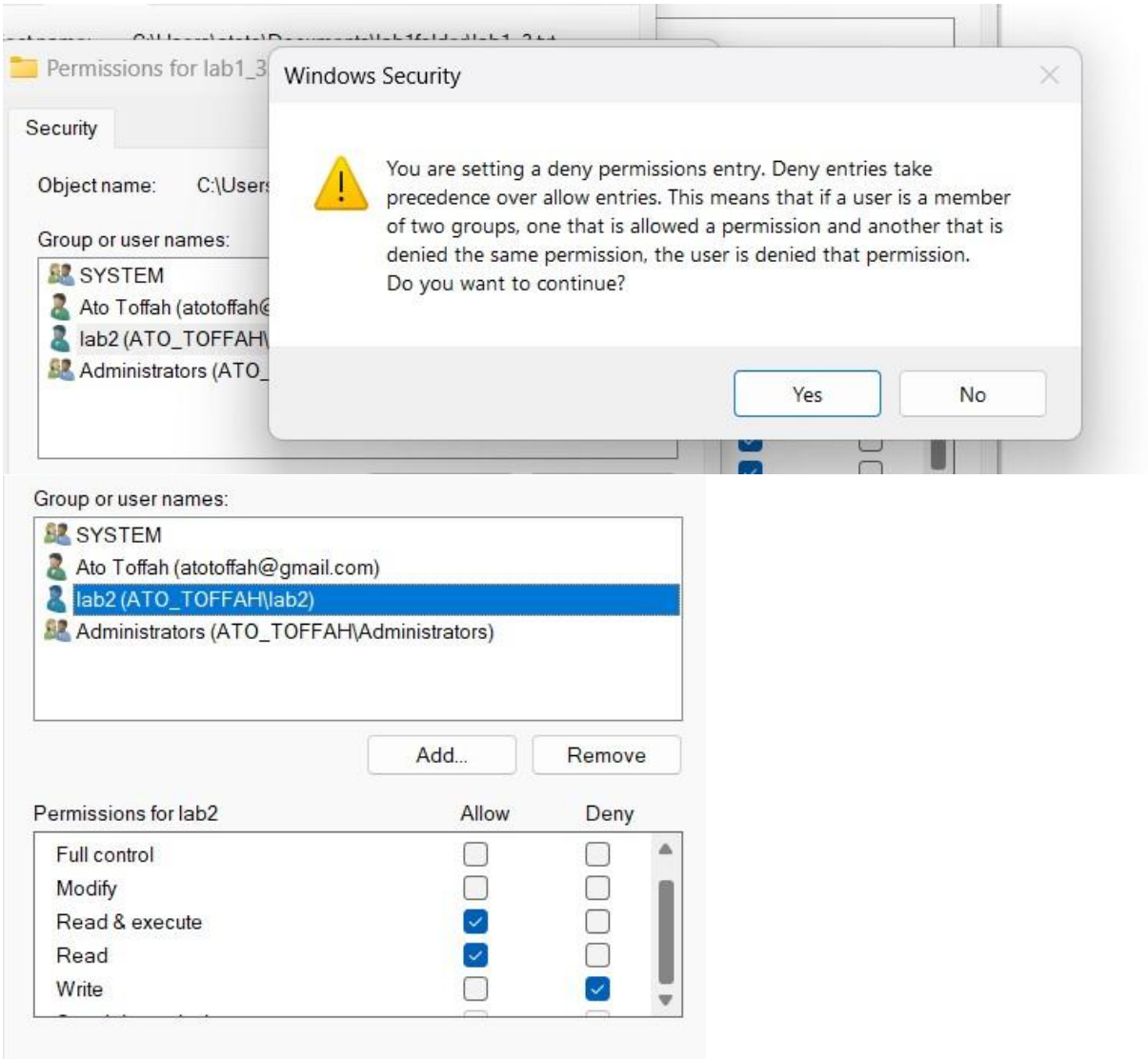


Fig 4.6 Deny Write for lab2

**The user lab2 can no longer write to or modify the file.**

# Exercise 5: Auditing in Windows

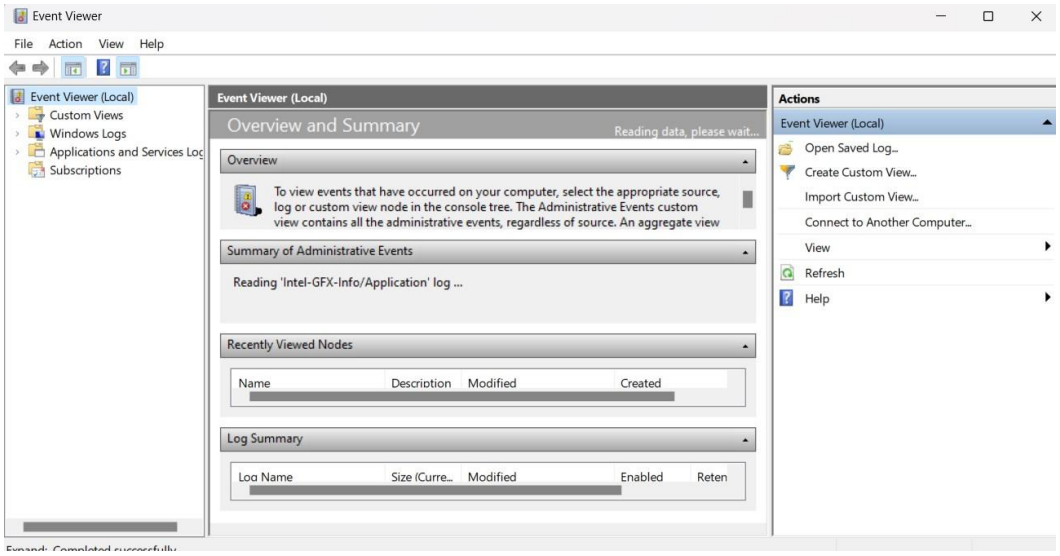


Fig 5.1 Event Viewer

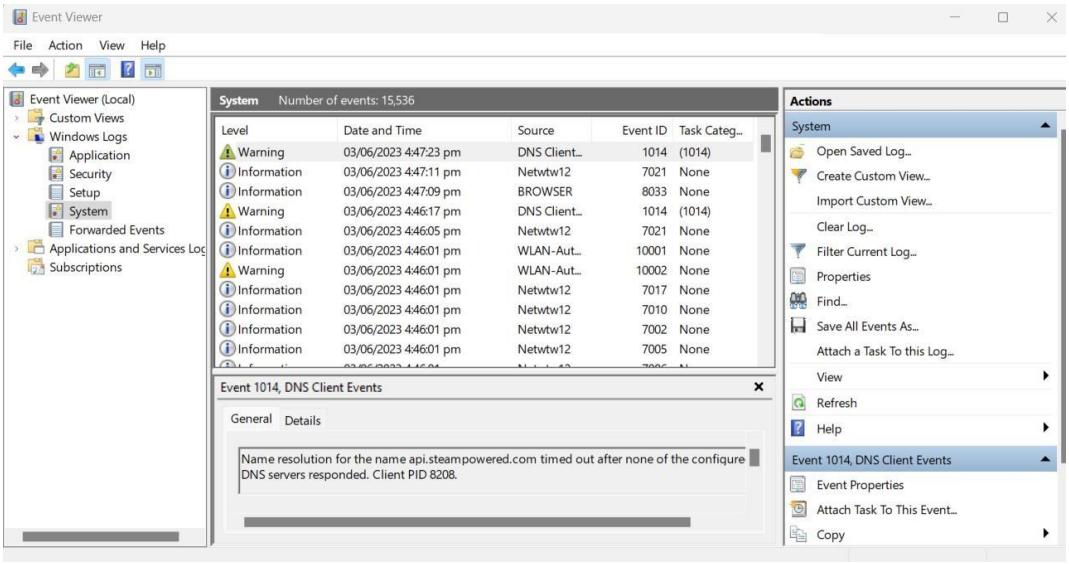


Fig 5.2 System Logs

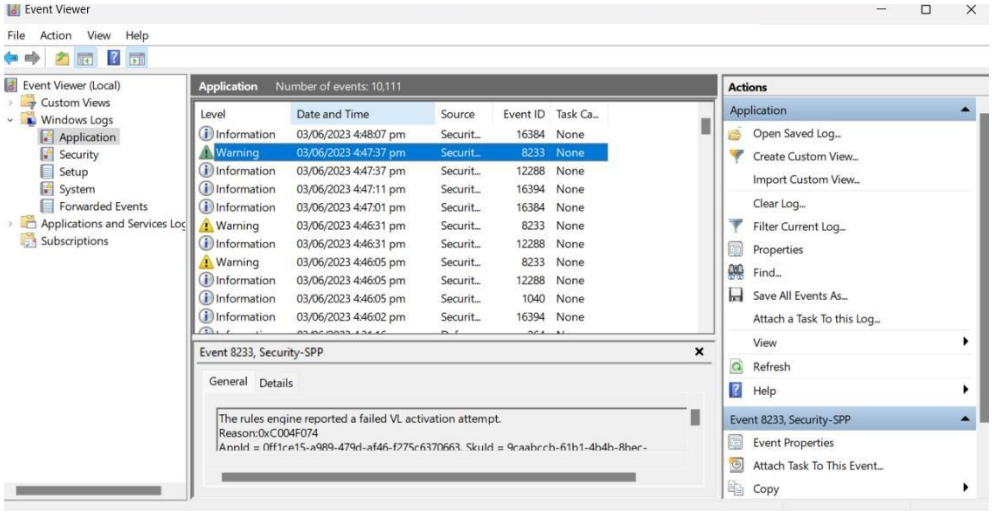


Fig. 5.3 Application Logs

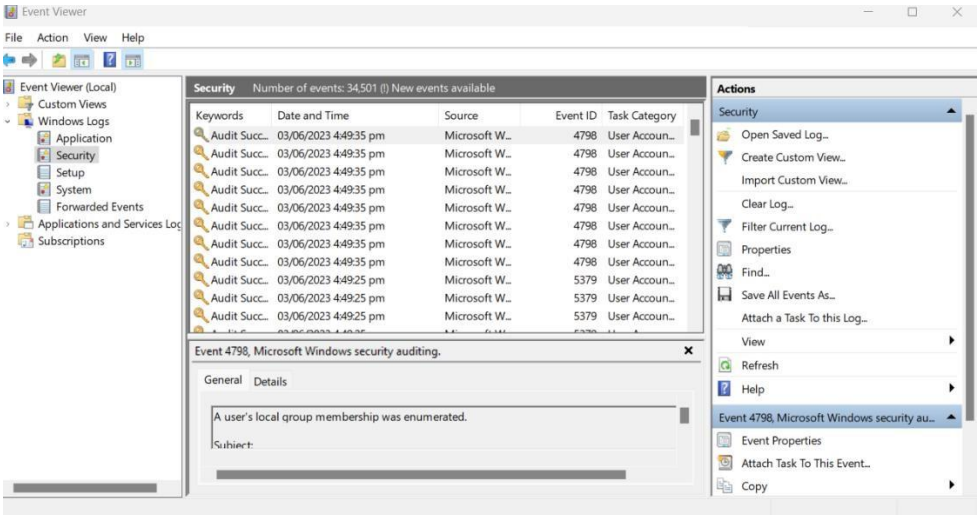


Fig 5.4 Security Logs

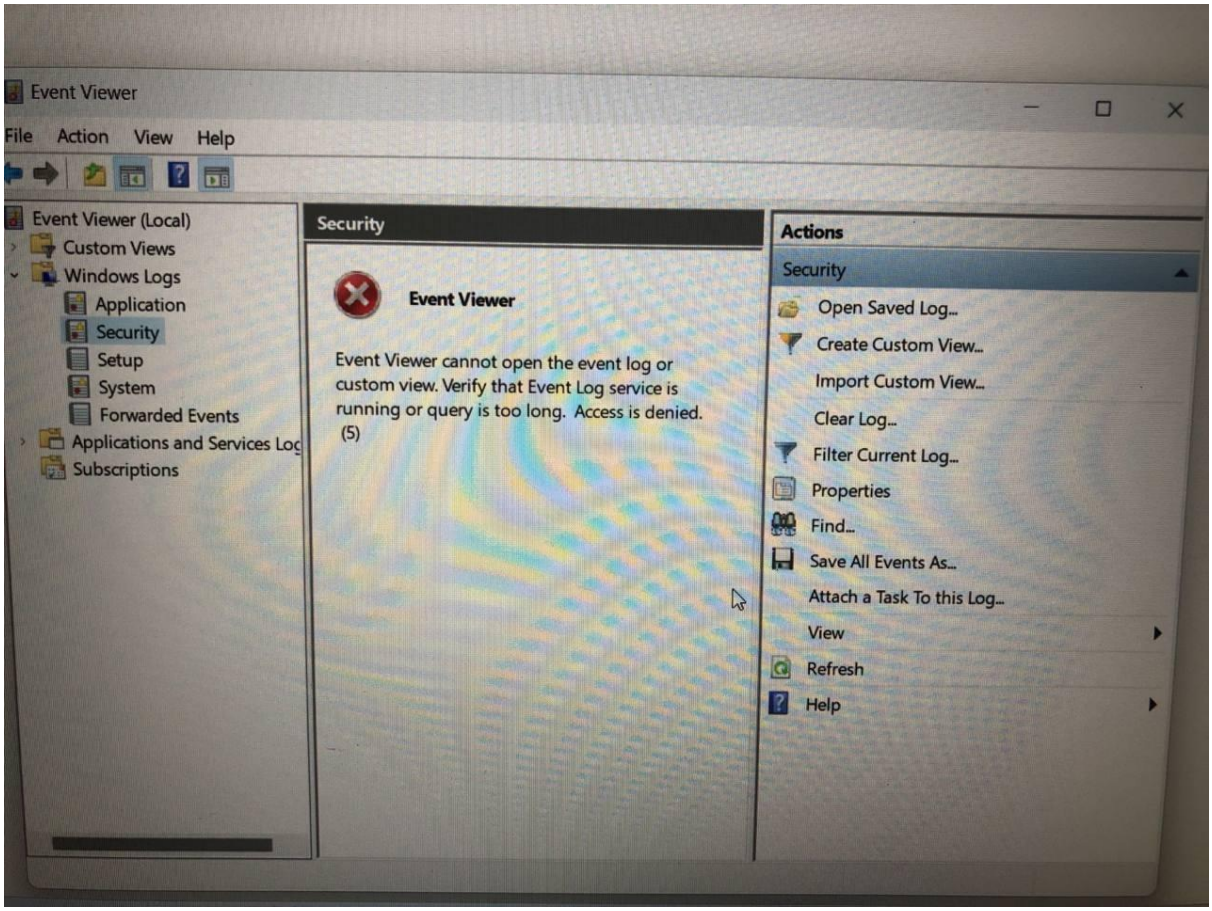


Fig 5.5 lab2 Security Logs

**Q7. Standard users cannot view security logs. This is because security logs contain sensitive information that is not suitable for standard users to view.**

**Q8. Security logs focus on recording security-related events and are restricted to privileged users, while system logs capture general system events and are accessible to normal users for troubleshooting purposes.**

# Exercise 6: Object Access Auditing

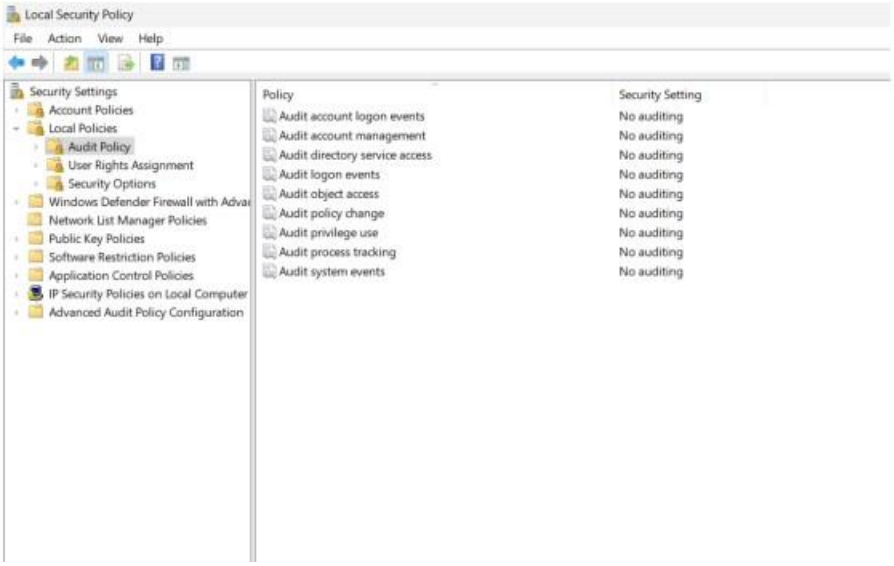


Fig 6.1 Audit Policy

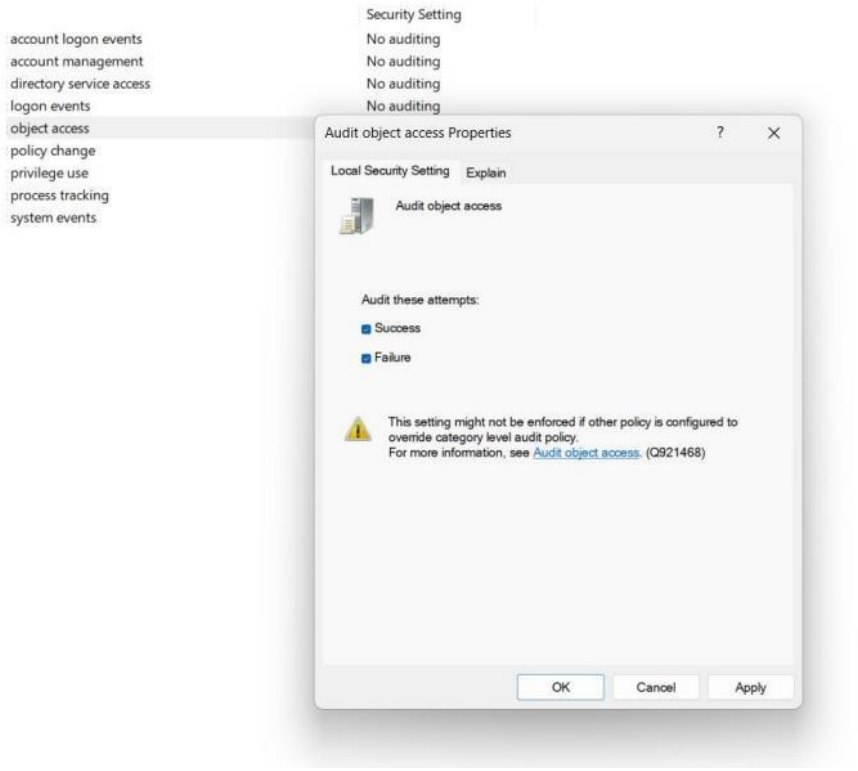


Fig 6.2 Audit object access properties.

**Q7. Audit policies are disabled by default because of user account control settings and also security software conflicts**