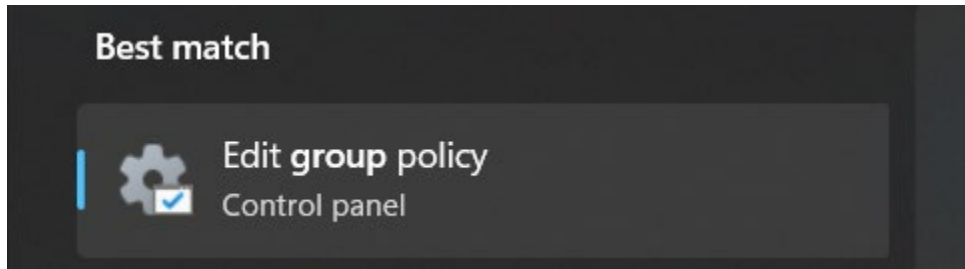


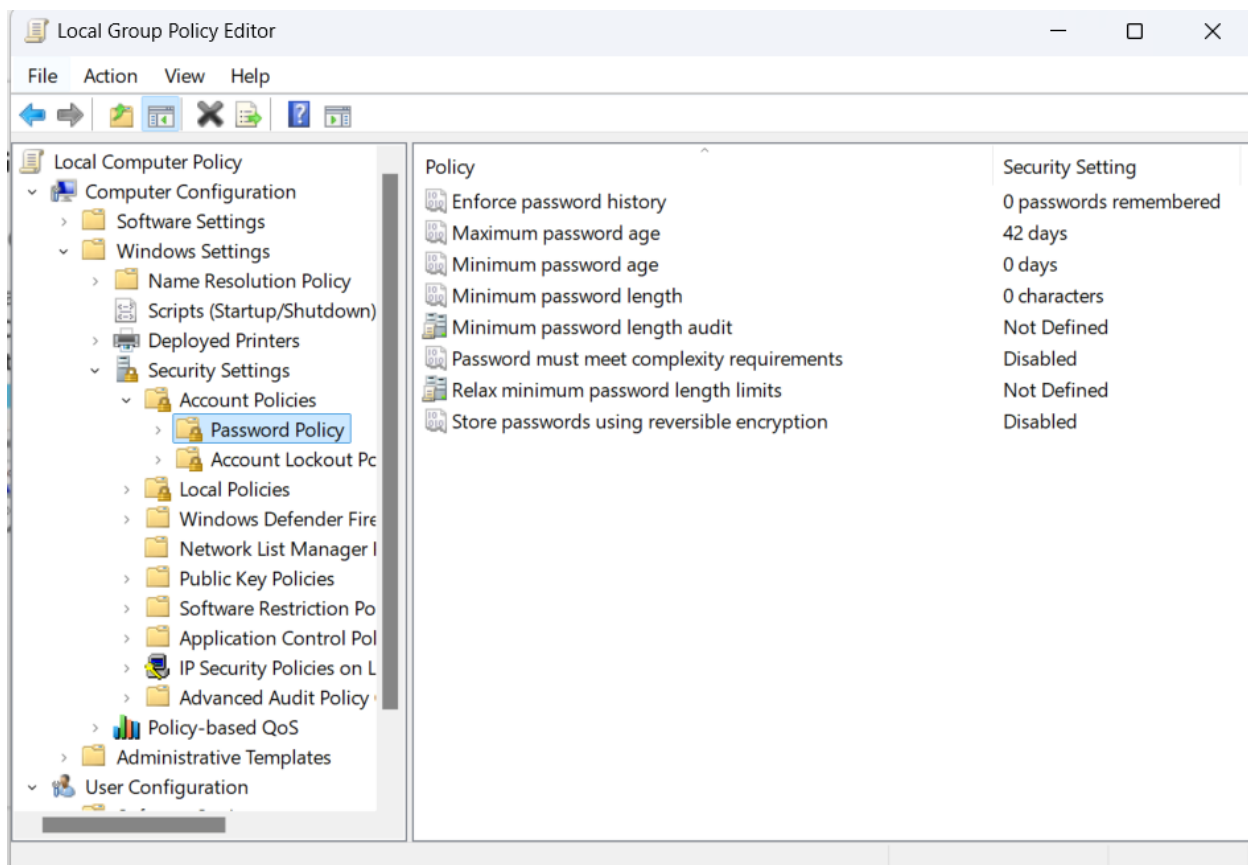
# System Hardening Fundamentals

## 1. ENABLING STRONG PASSWORDS

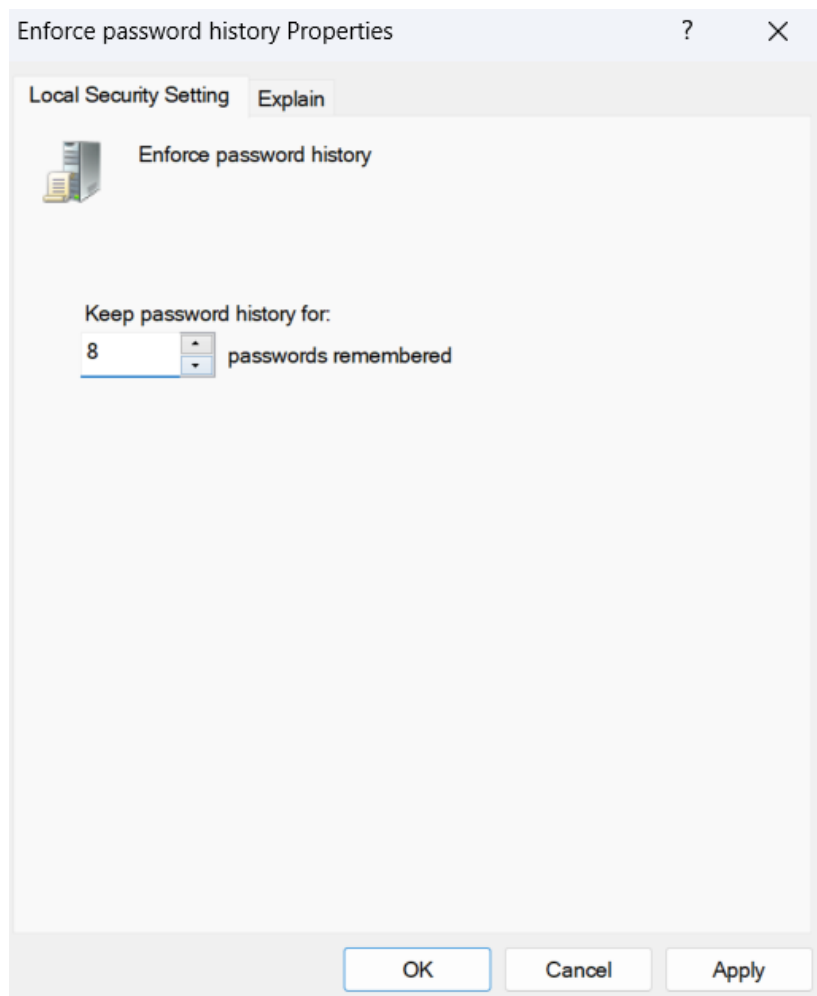
[1] Open Local Group Policy Editor



[2] navigated to Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy




[3] Click on Enforce password history and set it to enabled to require password changes after a certain number of days ( 8 days)



[2]Set the minimum password length to 12 characters & Enable Password Complexity

Minimum password length Properties ? X

Local Security Setting Explain

 Minimum password length

Password must be at least:  

12

 characters


OK

Cancel

Apply

Password must meet complexity requirements Properties ? X

Local Security Setting Explain

 Password must meet complexity requirements

☒ Enabled

☐ Disabled

OK

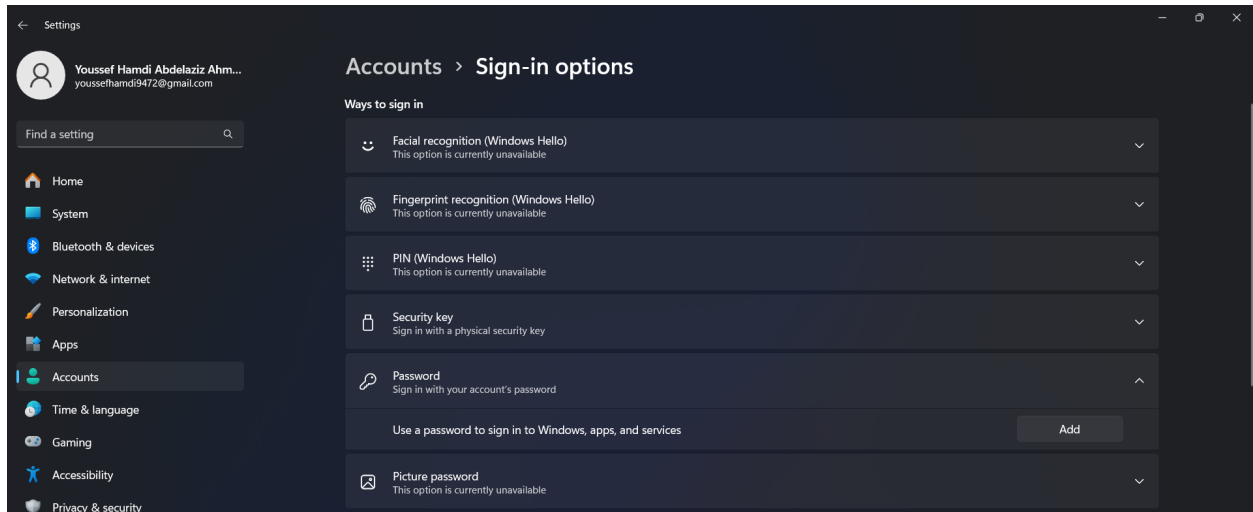
Cancel

Apply

## **2.ENABLING MULTI-FACTOR AUTHENTICATION**

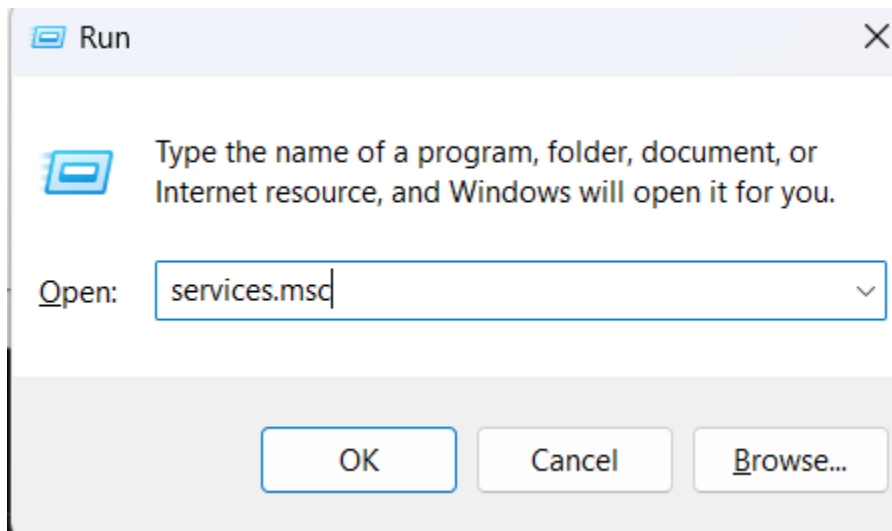
Open sign-in settings

Add a login Password to pc using my Microsoft account also enable Multi-factor authentication

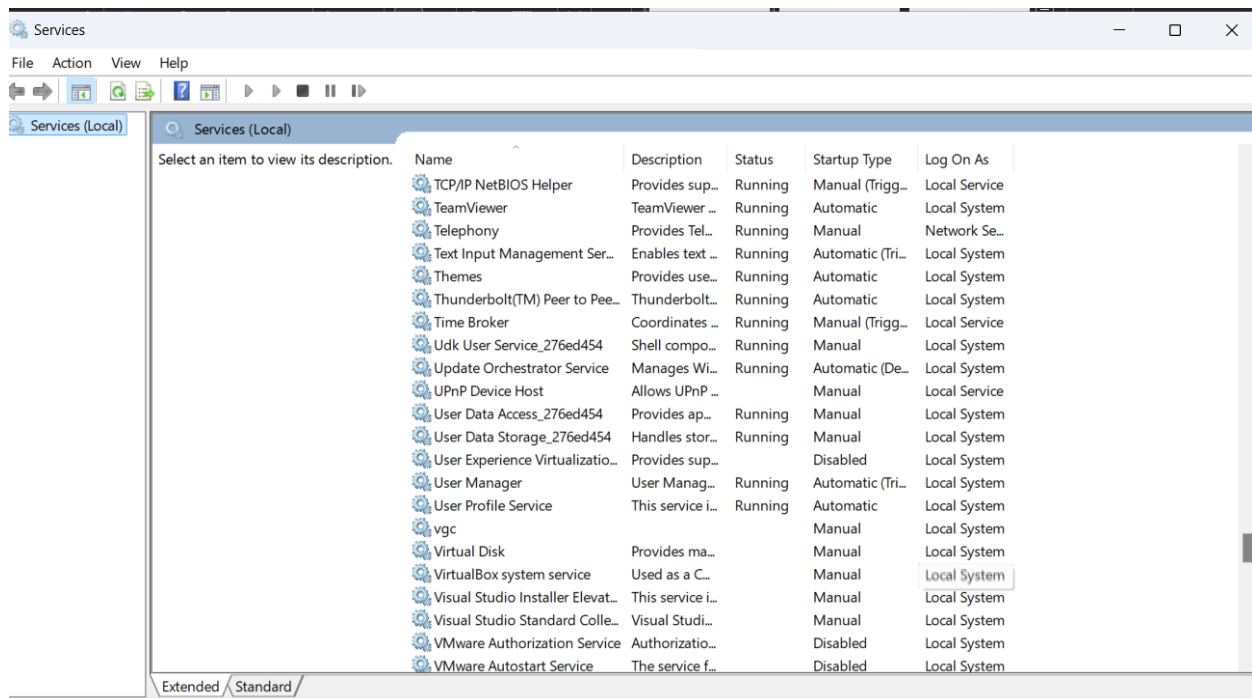


## **3. DISABLING UNNECESSARY SERVICES AND APPLICATIONS**

Open Services >( Win + R) and write services.msc



[2] check list of running services and disable those that are not necessary, such as: teamviewer



## 4.KEEPING SOFTWARE UPDATED WITH THE LATEST SECURITY PATCHES

[1] Open Settings > Update & Security > Windows Update

Enable auto checking for update



## **Overview**

- **Enforcing Strong Password Policies**

- **Implementation:** Set requirements for password length, complexity, and history.
- **Advantage:** Defends against brute-force attacks and prevents unauthorized access.

- **Using Multi-Factor Authentication (MFA)**

- **Implementation:** Activated MFA on user accounts.
- **Advantage:** Provides an additional layer of security to prevent account breaches.

- **Disabling Unnecessary Services**

- **Implementation:** Turned off non-essential services like unused apps
- **Advantage:** Minimizes the attack surface by removing potential vulnerabilities.

- **Performing Regular Updates**

- **Implementation:** Enabled automatic updates and ensured systems are up to date.
- **Advantage:** Addresses security flaws, protecting against exploits and malware.