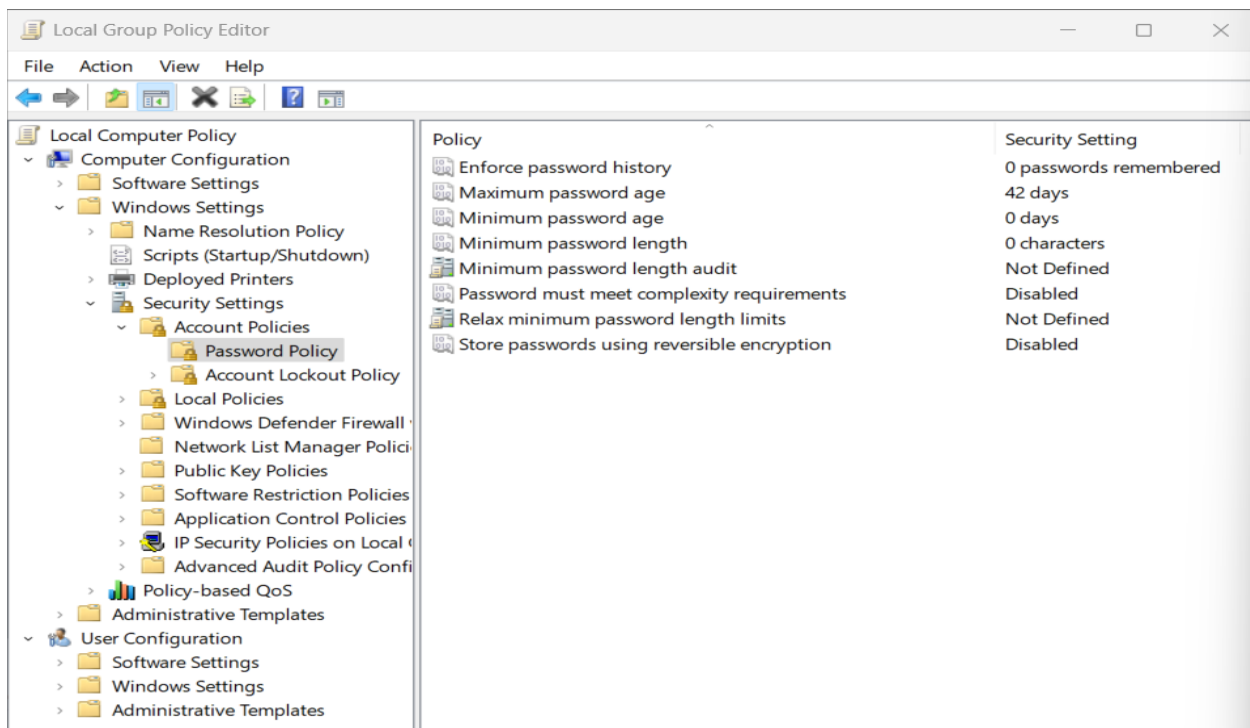# System Hardening Fundamentals

01. ENABLING STRONG PASSWORDS AND MULTI-FACTOR AUTHENTICATION
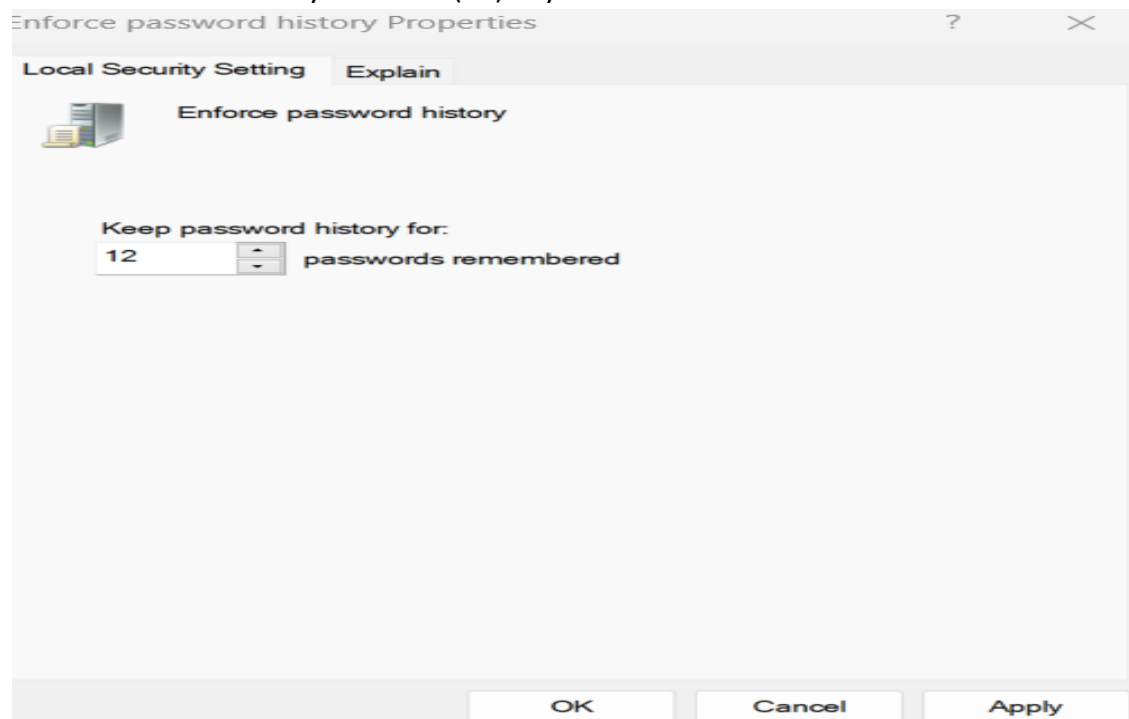
[1] Open Local Group Policy Editor

[2] After that we navigated to
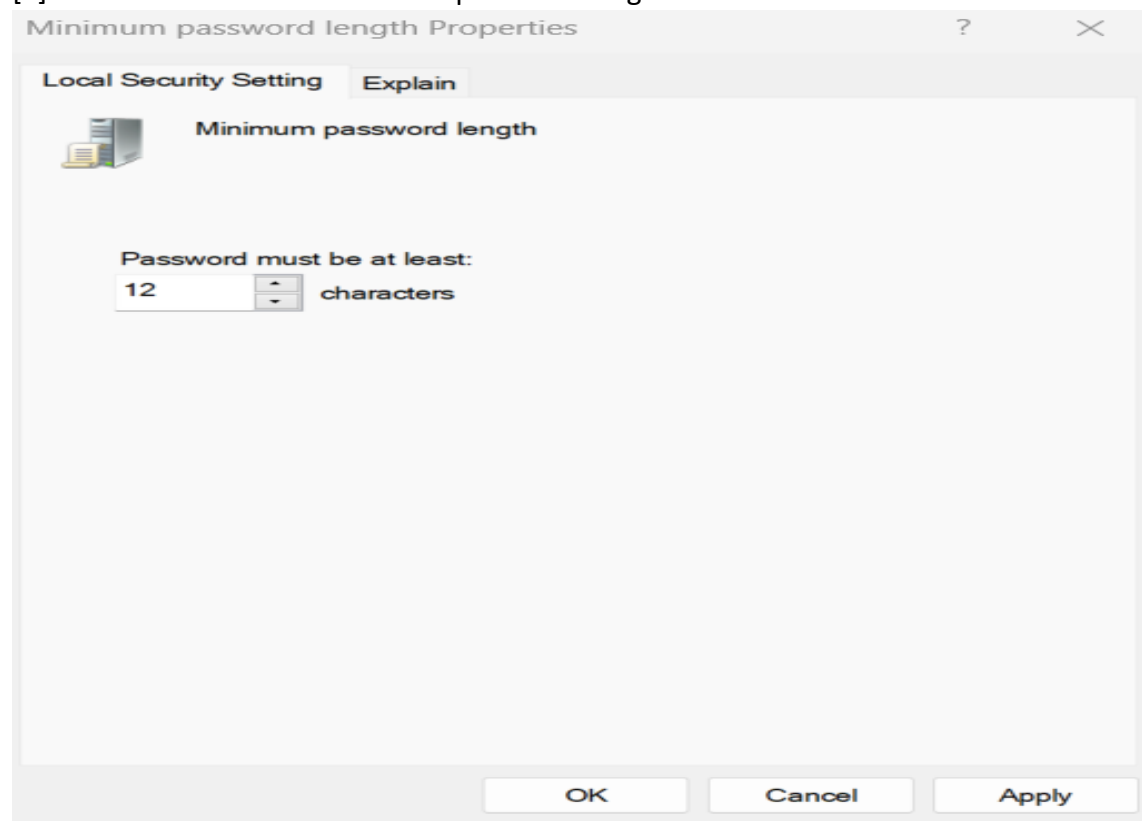
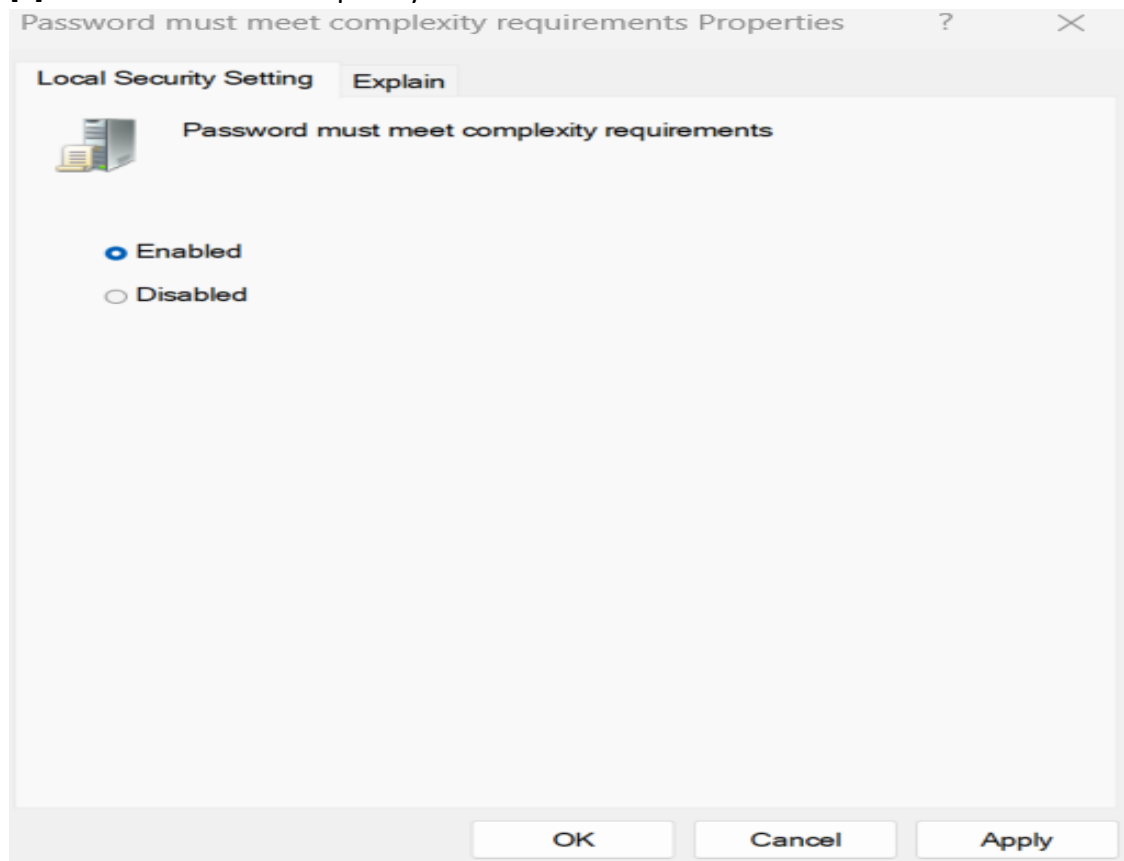Computer Configuration > Windows Settings >Security Settings > Account Policies > Password

[3] we click on Enforce password history and set it to enabled to require password changes after a certain number of days . in case (12) days

Enforce password history Properties   ?   ✕

Local Security Setting   Explain

Enforce password history

Keep password history for:
12   ⬍   passwords remembered

OK   Cancel   Apply

[4]After that we set the minimum password length to 12 characters

Minimum password length Properties   ?   ✕

Local Security Setting   Explain

Minimum password length

Password must be at least:
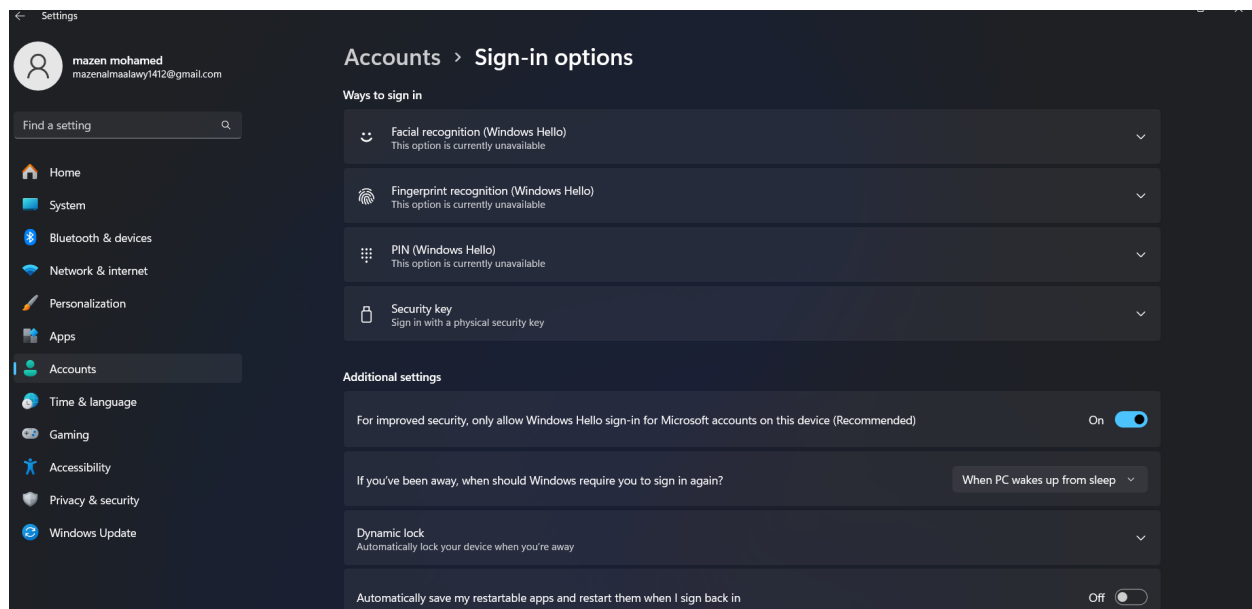12   ⬍   characters

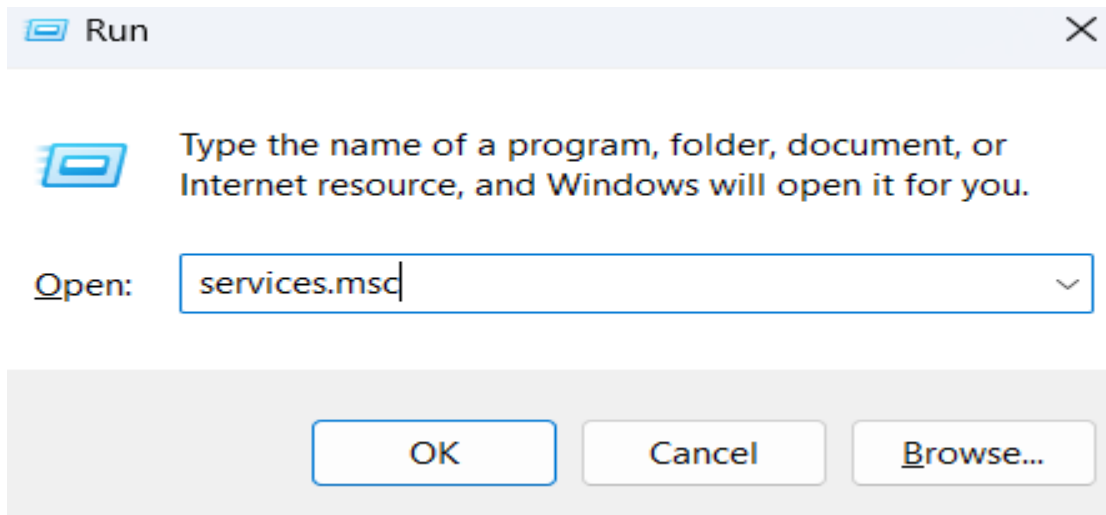OK   Cancel   Apply

[5] Enable Password Complexity

ENABLING STRONG PASSWORDS AND MULTI-FACTOR AUTHENTICATION

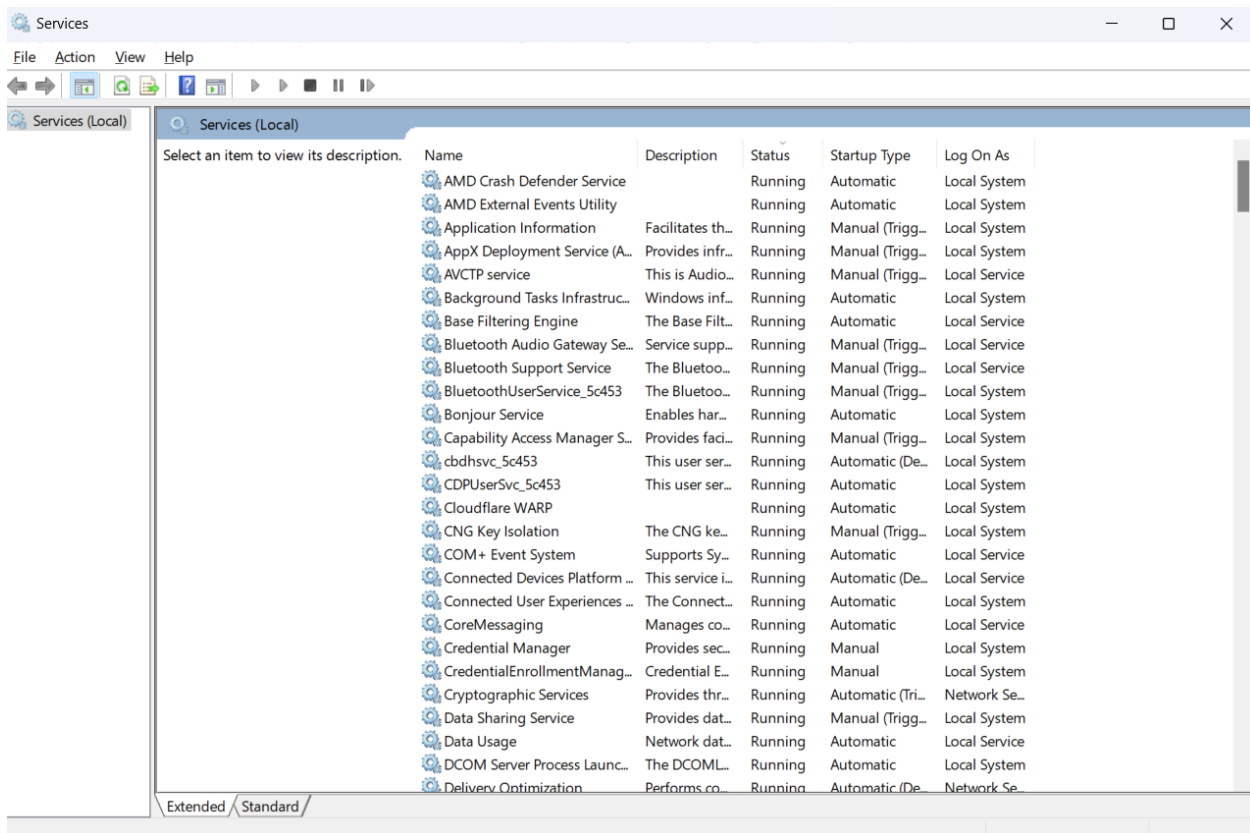[6]. sign-in settings for my windows to add a login PIN to my windows using my microsoft account

2. DISABLING UNNECESSARY SERVICES AND APPLICATIONS

[1] We go to the Service menu by searching for it in the run (Win + R) with services.msc

[2] Review the list of running services and disable those that are not necessary

KEEPING SOFTWARE UPDATED WITH THE LATEST SECURITY PATCHES

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

1. Enforcing Robust Password Policies

- **Implementation**: Establish clear guidelines for password length, complexity, and reuse limitations.
- **Benefit**: Strengthens defense against brute-force attacks and reduces the risk of unauthorized access.

2. Utilizing Multi-Factor Authentication (MFA)

- **Implementation**: Ensure MFA is activated across all user accounts.
- **Benefit**: Adds an extra layer of protection, reducing the likelihood of account compromises.

3. Disabling Redundant Services

- **Implementation**: Deactivate unnecessary services and applications.
- **Benefit**: Reduces the attack surface by eliminating exploitable vulnerabilities.

4. Conducting Regular Updates

- **Implementation**: Enable automatic updates and maintain system software at the latest version.
- **Benefit**: Fixes known security issues and shields systems against malware and other exploits.