Session8 Project2.1: System Hardening Fundamentals

1.1 Enable Strong Passwords

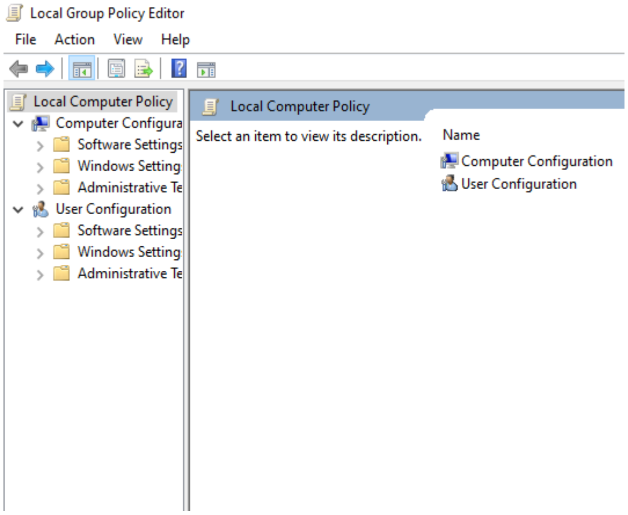
Action:

Configure Windows to require strong passwords for all user accounts by setting password policies through Group Policy or Local Security Policy.

Set a minimum password length (at least 12 characters), enforce complexity (uppercase, lowercase, numbers, and special characters), and set an expiration period for passwords.

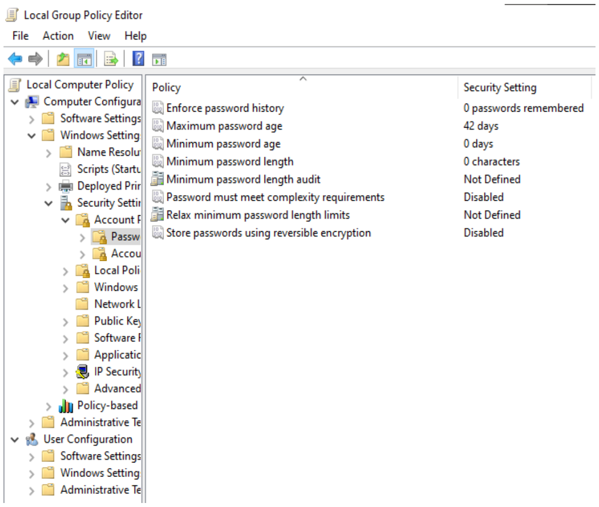
Steps:

1. Open Local Group Policy Editor



Select an item to view its description.

2. Go to Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy.

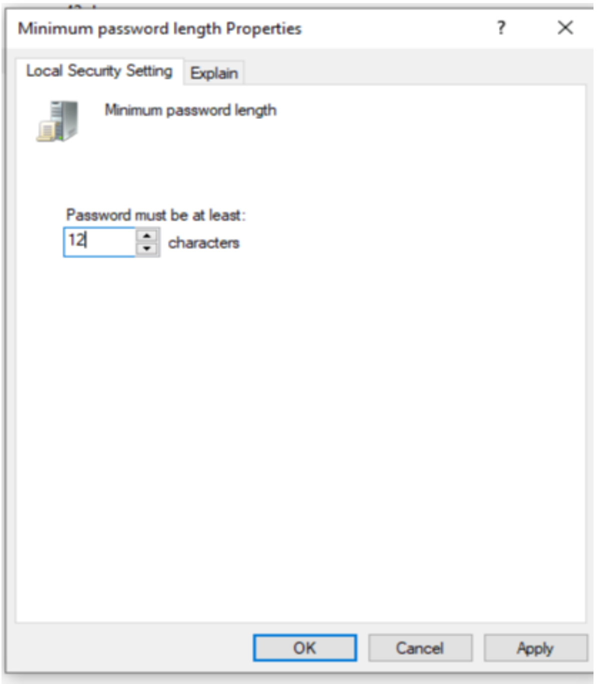


Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Disabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled

3. Set the following:

Minimum Password Length: 12 characters or more.

.



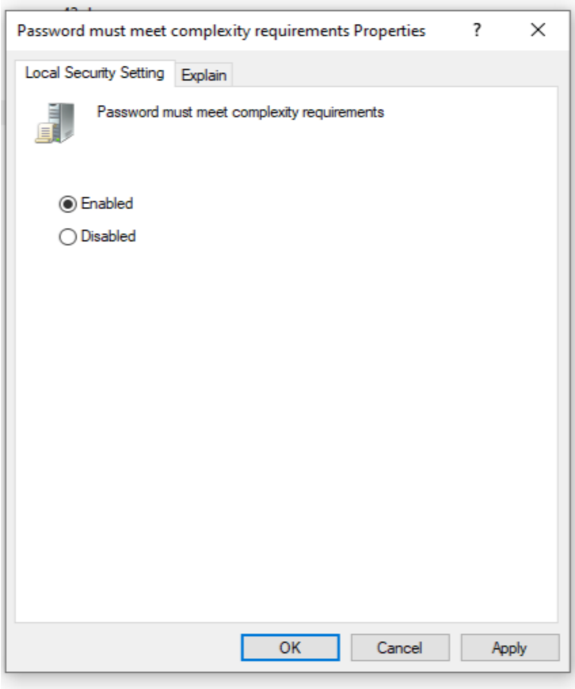
Minimum password length Properties

Minimum password length

Password must be at least:

12 characters

Password must meet complexity requirements: Enabled.



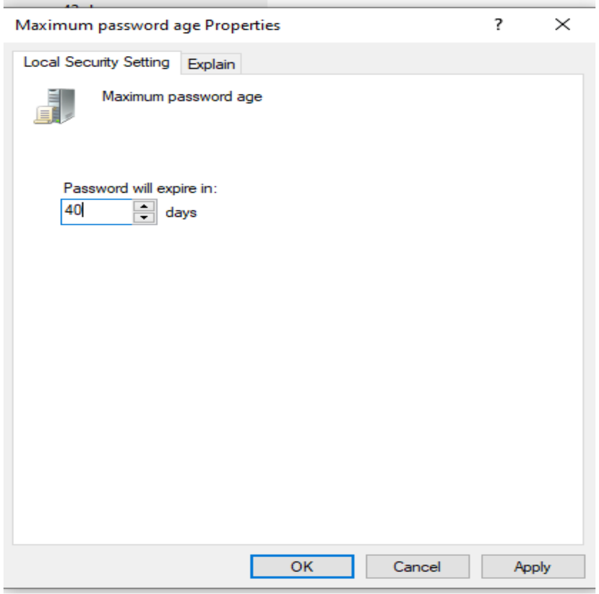
Password must meet complexity requirements Properties

Password must meet complexity requirements

● Enabled

○ Disabled

Maximum password age: 30 to 60 days



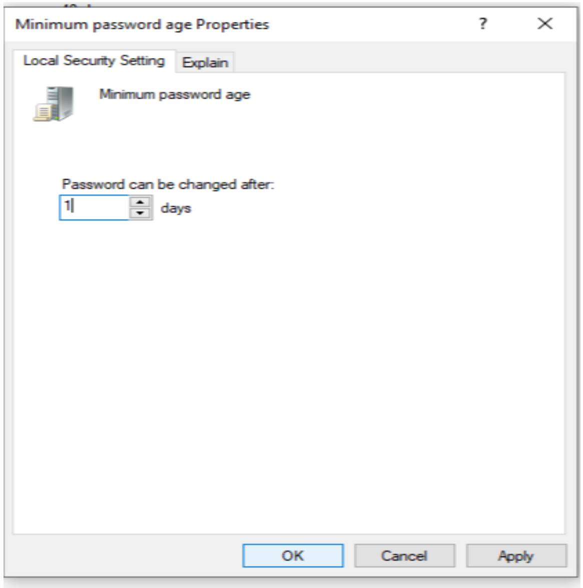
Maximum password age Properties

Maximum password age

Password will expire in:

40 days

Minimum password age: 1



Minimum password age Properties

Minimum password age

Password can be changed after:

1 days

Benefit: Strong passwords reduce the risk of unauthorized access through brute-force or dictionary attacks

1.2 Enable Multi-Factor Authentication (MFA)

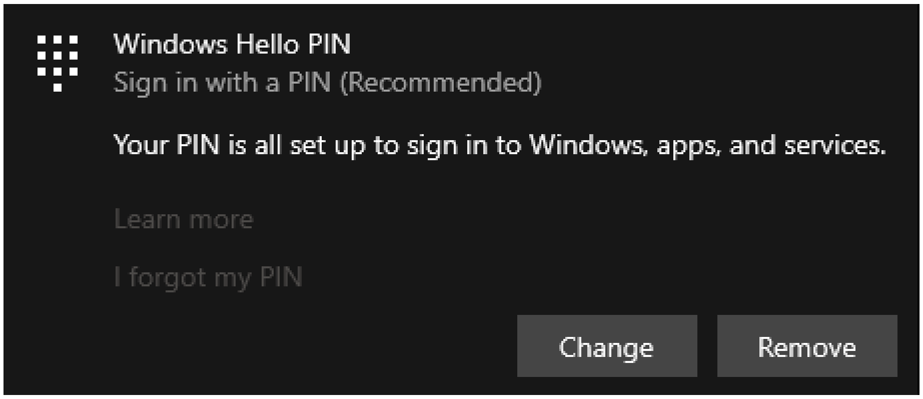
Action:

Enable MFA for all users on your system where possible. This can be done using Windows Hello, Microsoft Authenticator, or Third-Party MFA Solutions.

Steps:

1. Go to Settings > Accounts > Sign-in options.

2. Under Windows Hello, set up facial recognition, fingerprint, or PIN as an additional layer of authentication.



Windows Hello PIN

Sign in with a PIN (Recommended)

Your PIN is all set up to sign in to Windows, apps, and services.

3. For enterprise environments, use Azure Active Directory or Active Directory Federation Services (ADFS) to enable MFA.

Benefit: MFA greatly enhances security by requiring something you know (password) and something you have (phone or hardware token), preventing unauthorized access even if the password is compromised.

2. Disable Unnecessary Services and Applications

Action:

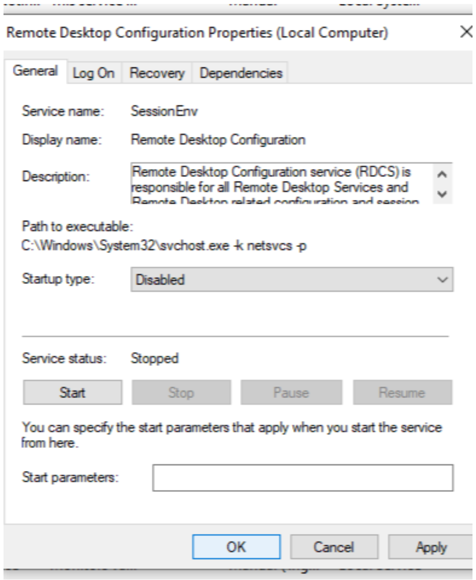
Disable services and applications that are not needed to reduce the attack surface of the system.

Steps:

1. Open Services by typing services.msc in the Start menu.

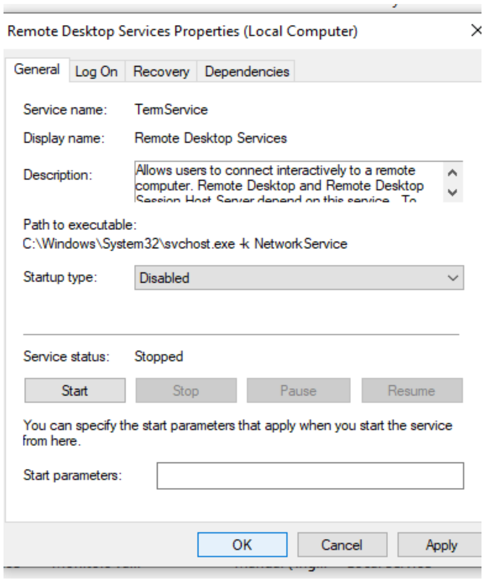
2. Review the list of running services and disable those that are not necessary, such as:

Remote Desktop (if not required): Right-click > Properties > Disabled.



Remote Desktop Configuration Properties (Local Computer)

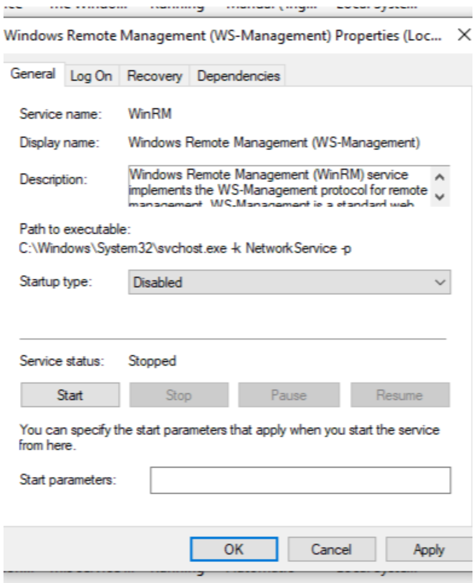
Service name: SessionEnv
Display name: Remote Desktop Configuration
Description: Remote Desktop Configuration service (RDCS) is responsible for all Remote Desktop Services and Remote Desktop related configuration and session
Path to executable:
C:\Windows\System32\svchost.exe -k netsvcs -p
Startup type: Disabled
Service status: Stopped
You can specify the start parameters that apply when you start the service from here.
Start parameters:



Remote Desktop Services Properties (Local Computer)

Service name: TermService
Display name: Remote Desktop Services
Description: Allows users to connect interactively to a remote computer. Remote Desktop and Remote Desktop Session Host Server depend on this service. To
Path to executable:
C:\Windows\System32\svchost.exe -k NetworkService
Startup type: Disabled
Service status: Stopped
You can specify the start parameters that apply when you start the service from here.
Start parameters:

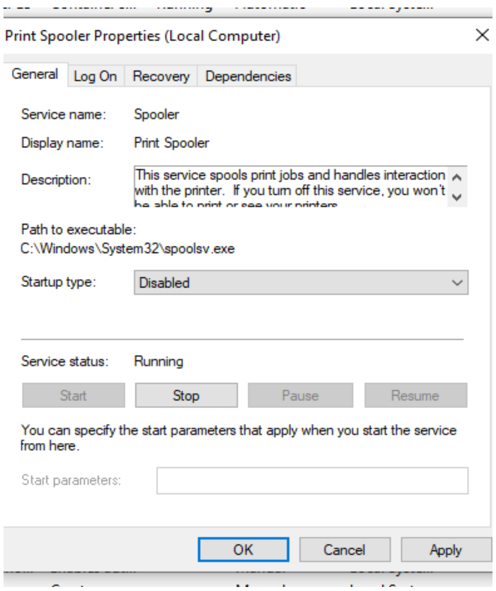
Windows Remote Management: Disabled.



Windows Remote Management (WS-Management) Properties (Loc...

Service name: WinRM
Display name: Windows Remote Management (WS-Management)
Description: Windows Remote Management (WinRM) service implements the WS-Management protocol for remote management. WS-Management is a standard web
Path to executable:
C:\Windows\System32\svchost.exe -k NetworkService -p
Startup type: Disabled
Service status: Stopped
You can specify the start parameters that apply when you start the service from here.
Start parameters:

Print Spooler (if not using printers): Disabled.



Print Spooler Properties (Local Computer)

Service name: Spooler
Display name: Print Spooler
Description: This service spools print jobs and handles interaction with the printer. If you turn off this service, you won't be able to print or see your printers.
Path to executable:
C:\Windows\System32\spoolsv.exe
Startup type: Disabled
Service status: Running
You can specify the start parameters that apply when you start the service from here.
Start parameters:

3. Uninstall unnecessary software through Control Panel > Programs > Uninstall a program.

Benefit: Disabling unnecessary services and applications reduces the attack surface and prevents attackers from exploiting vulnerabilities in unused software.

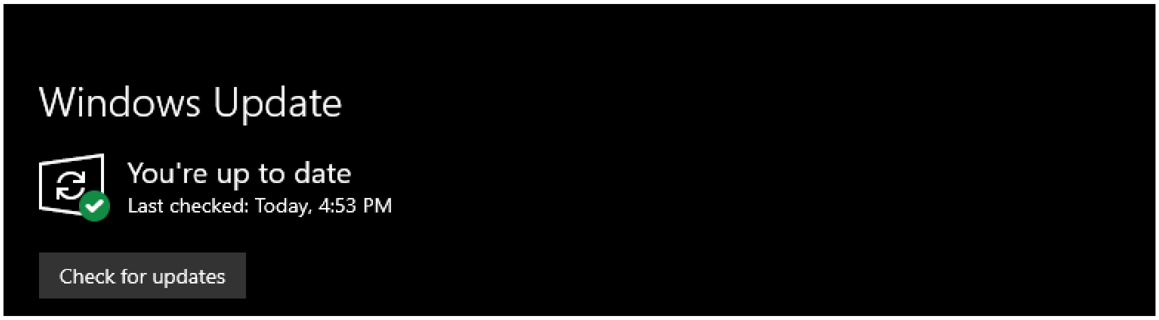
3. Keep Software Updated with Latest Security Patches

Action:

Regularly apply security patches and updates to the Windows OS and installed software to close known vulnerabilities.

Steps:

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



You're up to date

Last checked: Today, 4:53 PM

2. Ensure Automatic Updates are enabled for both security patches and driver updates.

3. Regularly check for updates by clicking Check for Updates.

4. Enable Windows Defender Antivirus or use a trusted third-party antivirus solution to regularly update virus definitions.

Benefit: Keeping software updated ensures that the system is protected against newly discovered security vulnerabilities and exploits.