Windows Security Hardening

What is Windows Security Hardening?

Windows Security Hardening refers to the process of strengthening the security of a Windows operating system by configuring its settings, disabling unnecessary features, and enabling built-in protection tools. The main goal is to reduce the system's vulnerability to cyber threats such as malware, ransomware, unauthorized access, and data breaches.

Why is Security Hardening Important?

As cyber threats become more advanced, simply installing antivirus software is no longer enough. Windows security hardening provides multiple layers of protection to ensure:

- Confidentiality (your data is private)
- Integrity (your data isn't tampered with)
- Availability (your system stays up and running)

It also ensures systems comply with security standards in organizations, government, and personal use.

Key Objectives of Windows Security Hardening:

1. Prevent Unauthorized Access – Block hackers or intruders
2. Minimize Attack Surface – Remove unused services/features
3. Enhance System Monitoring – Enable alerts and logging
4. Ensure Data Protection – Use encryption and backup tools
5. Maintain System Updates – Patch known vulnerabilities

Benefits of Windows Security Hardening:

- Stronger protection against threats
- Reduced risk of data loss or theft
- Better system stability and performance
- Compliance with security standards (e.g., ISO, CIS)
- Peace of mind for users and organizations

Password Manager

What is a Password Manager?

A Password Manager is a tool or app that saves and organizes all your passwords securely. Instead of remembering many passwords, you only need to remember one master password to access them all.

Why Use a Password Manager?

- Helps you create and store strong, unique passwords for every account
- Saves time by auto-filling login details
- Keeps your passwords safe and encrypted
- Prevents you from using weak or repeated passwords
- Reduces the risk of your accounts being hacked

Step-by-Step Procedure to Use a Password Manager:

1. Choose and Install a password manager app or use a built-in one (like Google Password Manager).
2. Create a Master Password – this is the only password you need to remember, so make it strong and unique.
3. Add Passwords:
    - Let the manager save passwords automatically when you log in to websites, or
    - Manually enter your existing passwords into the app.
4. Use Auto-Fill – When you visit a website or app, the password manager fills in your username and password automatically.
5. Generate New Passwords – When creating new accounts or changing passwords, use the manager's password generator for strong passwords.
6. Sync Across Devices – If available, enable sync so your passwords are available on your phone, tablet, and computer.
7. Regularly Update and review saved passwords for security.

Windows Hardening Checklist

This section is a guide to enable basic security features and hardening measures and to help build your confidence to move onto more advanced hardening. As you work your way through this list, it's a good security habit to research each item before you go through with it.

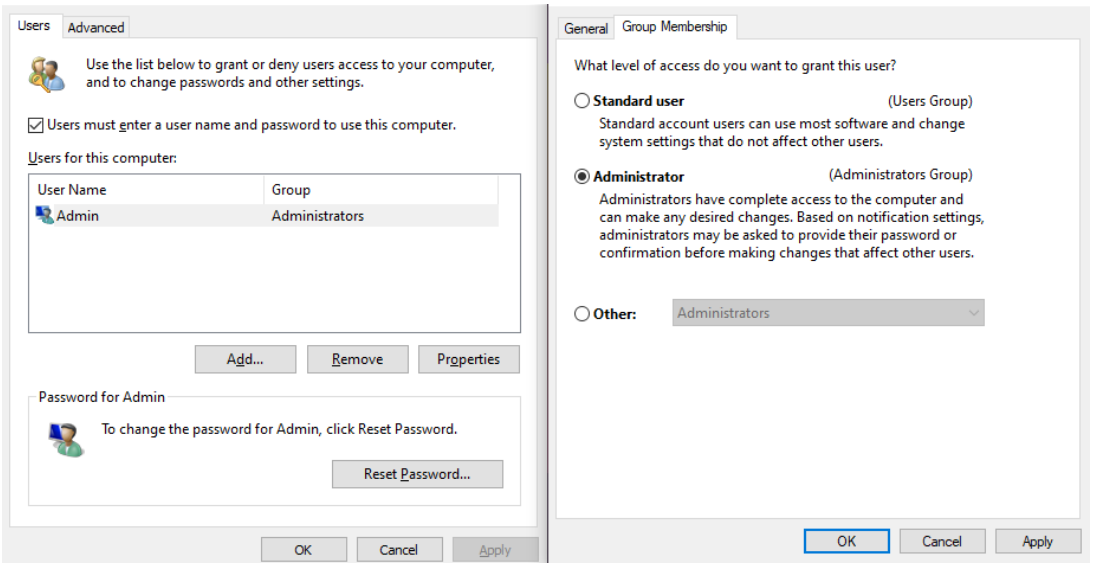
Account Setup

Force Accounts to Have Passwords

- Open the "Run" app by searching for it or using Win+ r.
- Type netplwiz into the dialog box and click "OK".
- Check the box labeled "Users must enter a user name and password to use this computer." in the "User Accounts" window.

Limit Administrator Privileges to only Necessary Accounts

- From the same "User Accounts" window, you can set whether or not accounts have administrator privileges.
- Select an account that you want to add or remove administrator privileges from, then click "Properties".
- In the new window, switch to the "Group Membership" tab, and select "Standard User" or "Administrator" as appropriate.



Require Log In on Screensaver

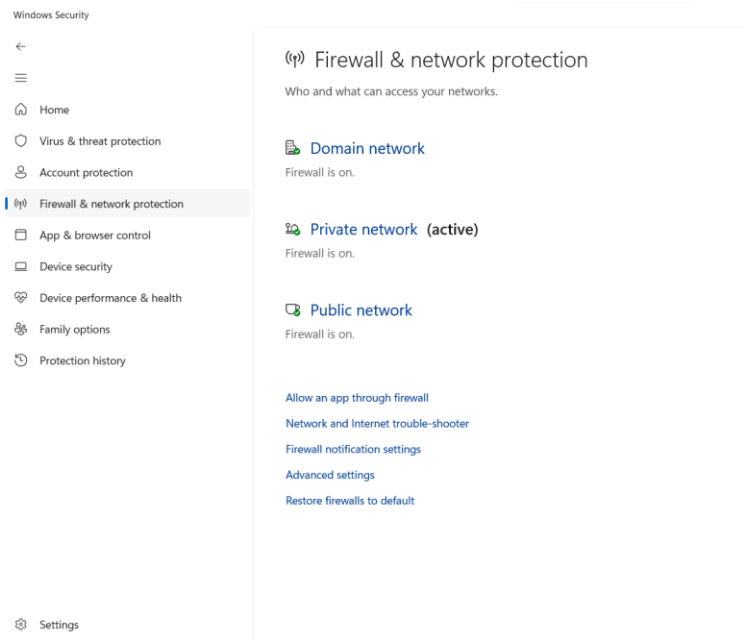
- Open the "Settings" app.
- Go to the "Accounts" section.
- Go to the "Sign-in options" section in the sidebar.
- Under the "Require sign-in" header, select "When PC wakes up from sleep"

Windows Security Features

1. Turn On Windows Firewall

Steps Performed:

1. Press Windows + R, type control, and press Enter.
2. Go to System and Security → Windows Defender Firewall.
3. Click Turn Windows Defender Firewall on or off.
4. Enable it for both Private and Public networks.
5. Click OK.



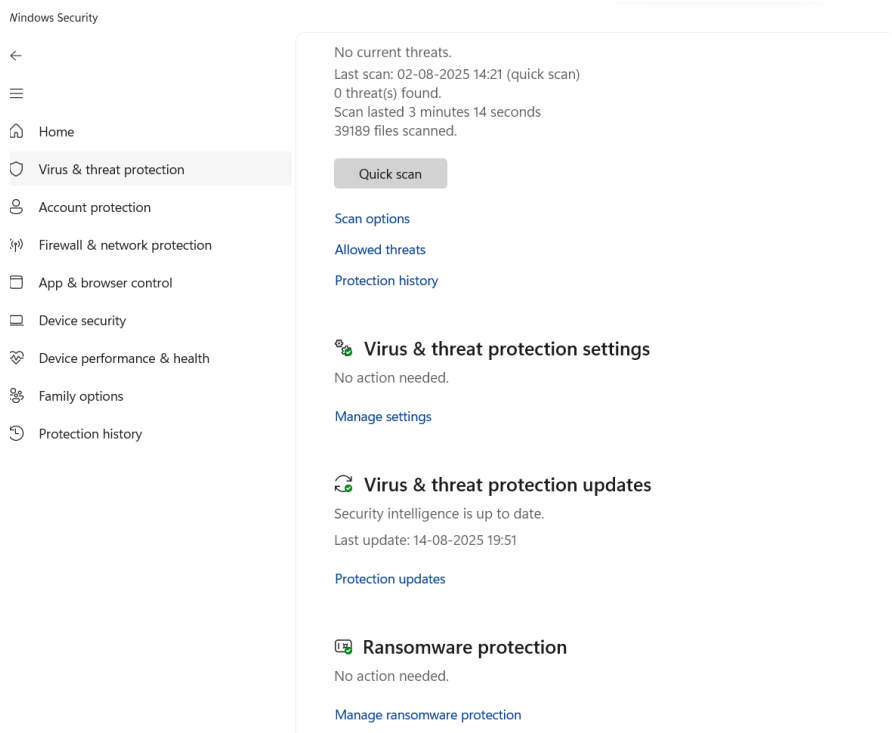
I enabled Windows Defender Firewall to monitor and block unauthorized network access, which helps in protecting the system from external attacks.

2. Turn On Windows Built-In Antivirus (Windows Security / Defender)

Steps Performed:

1. Open Settings (Windows + I).
2. Go to Privacy & Security > Windows Security > Virus & threat protection.
3. Under Virus & threat protection settings, click Manage settings.
4. Ensure the following are ON:
    - Real-time protection
    - Cloud-delivered protection
    - Automatic sample submission

- Tamper Protection

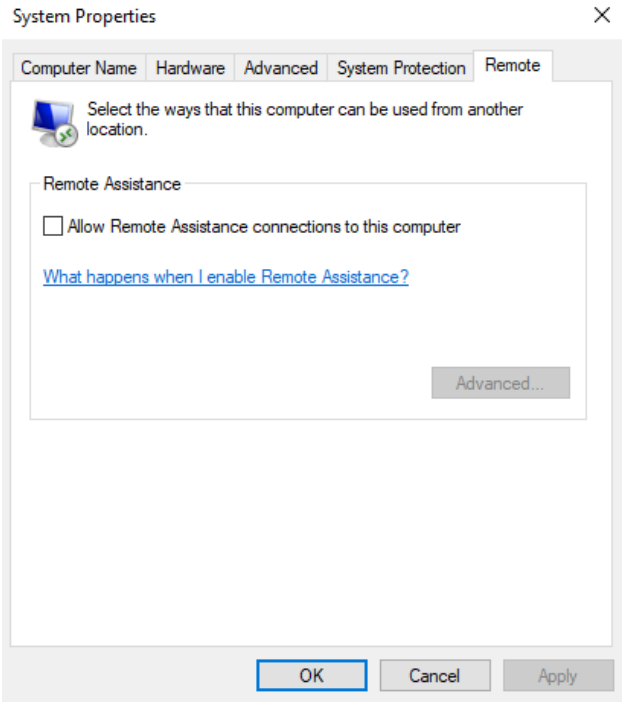


I enabled key features of Windows Defender Antivirus to ensure real-time protection against malware and threats.

3. Disable Remote Access (Remote Desktop / RDP)

Steps Performed:

1. Open Settings (Windows + I).
2. Navigate to System > Remote Desktop.
3. Turn the Remote Desktop switch OFF.

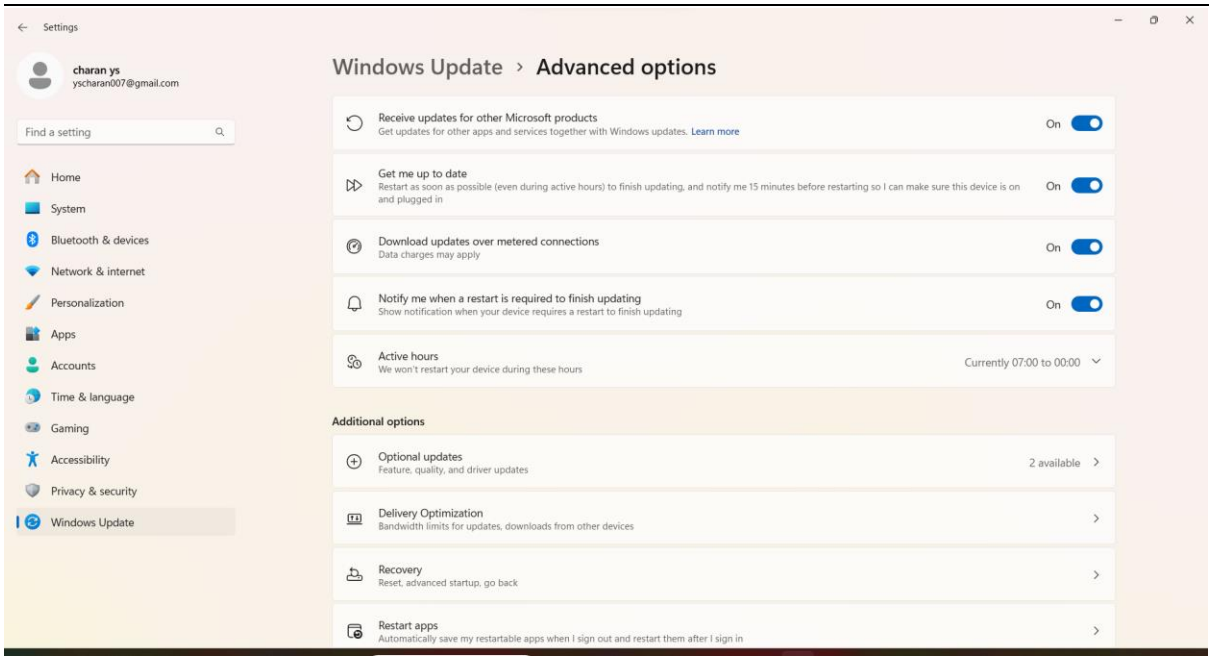


I disabled Remote Desktop access to reduce the risk of unauthorized remote access and RDP-based attacks.

4. Allow Automatic Microsoft Software Updates

Steps Performed:

1. Go to Settings → Windows Update.
2. Click Advanced options.
3. Enabled the following:
    - Receive updates for other Microsoft products
    - Get me up to date
    - Download updates over metered connections (optional)
4. Returned and clicked Check for updates.



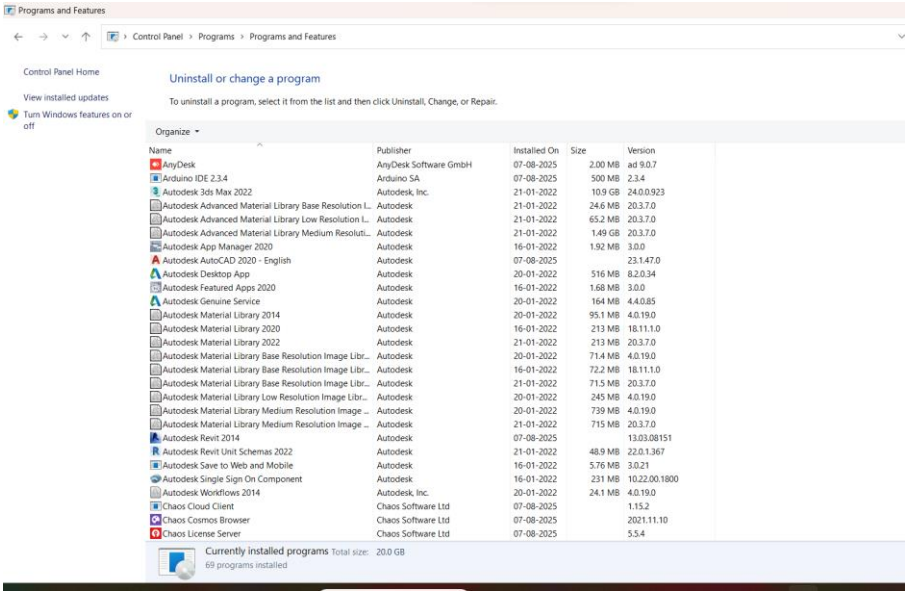
I enabled automatic updates to ensure that the system receives timely security patches and software updates.

5.Uninstall Unused Programs:

Uninstalling unused programs means removing software you don’t use anymore from your computer. This helps make your system faster, safer, and cleaner.

Step Performed:

- Click on Start Menu → Type and open Control Panel
- Click on Programs
- Then click on Programs and Features
- Look through the list of installed programs
- Right-click on an unused program → Click Uninstall
- Follow the prompts to remove it



It Reduces security risks (some old programs may have bugs or viruses) and Improves performance (less programs running in the background).

6. Miscellaneous Best Practices

a. Enabled BitLocker Encryption

Steps:

1. Searched for BitLocker.
2. Clicked Manage BitLocker.
3. Clicked Turn on BitLocker and followed setup (saved recovery key).

Enabled BitLocker encryption to protect data at rest in case of device loss or theft.

b. Set a Strong Password

Steps:

1. Pressed Ctrl + Alt + Delete → Selected Change a password.
2. Created a strong password (8+ characters, mixed symbols and letters).

Set a strong user password to reduce the risk of unauthorized physical or local access.

c. Turned Off File Sharing

Steps:

1. Opened Control Panel → Network and Sharing Center.
2. Clicked Change advanced sharing settings.
3. Turned OFF File and printer sharing for private and public profiles.

Summary

Windows Security Hardening is a set of steps used to improve the security of a Windows system. It includes enabling built-in protections like the firewall and antivirus, disabling risky features like remote access, and regularly updating the system. These actions help protect the computer from viruses, hackers, and other threats, keeping data safe and the system running smoothly.

Author:

Security Hardening Conducted by: Priyanka H S

Security audit via windows10 on Laptop.