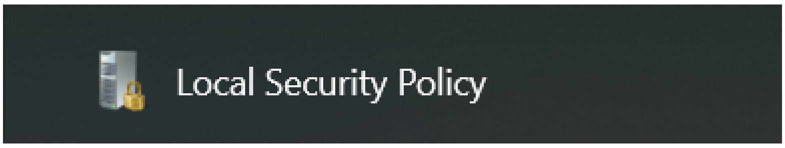
1. **Enabling Strong Passwords**

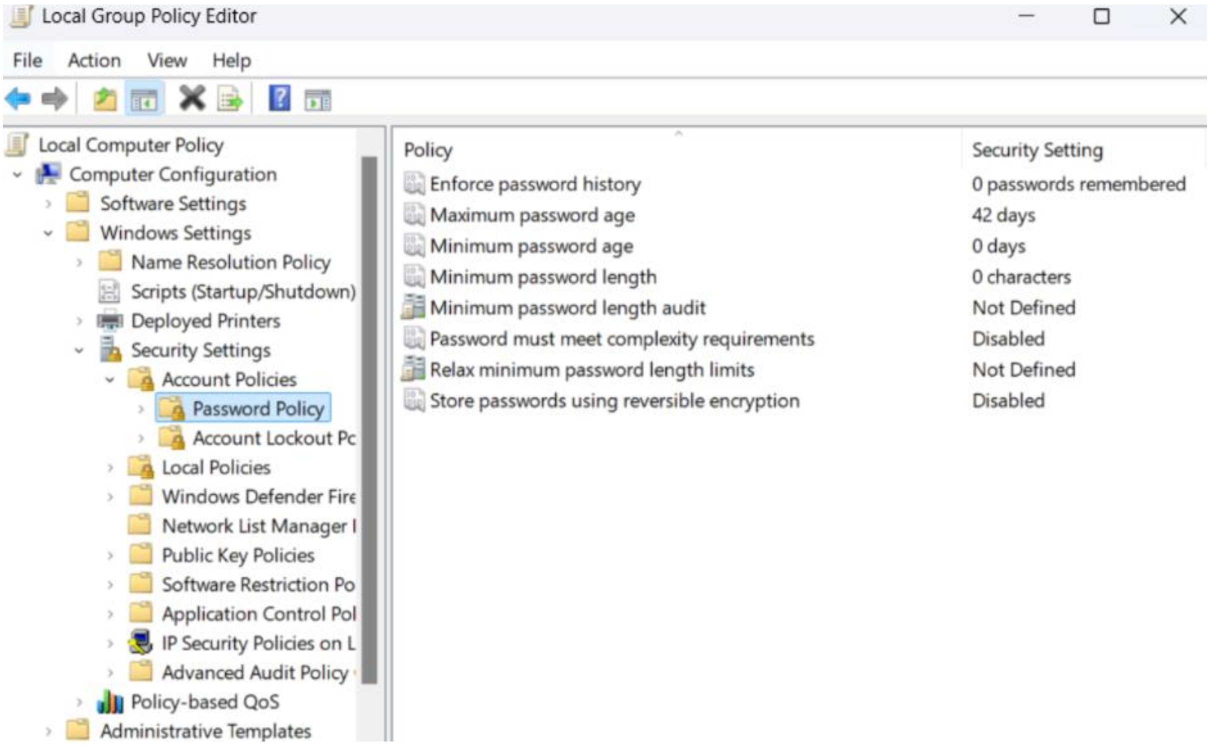
1) Open Local Group Policy Editor



Local Security Policy

2) navigated to Computer Configuration > Windows Settings >Security Settings > Account

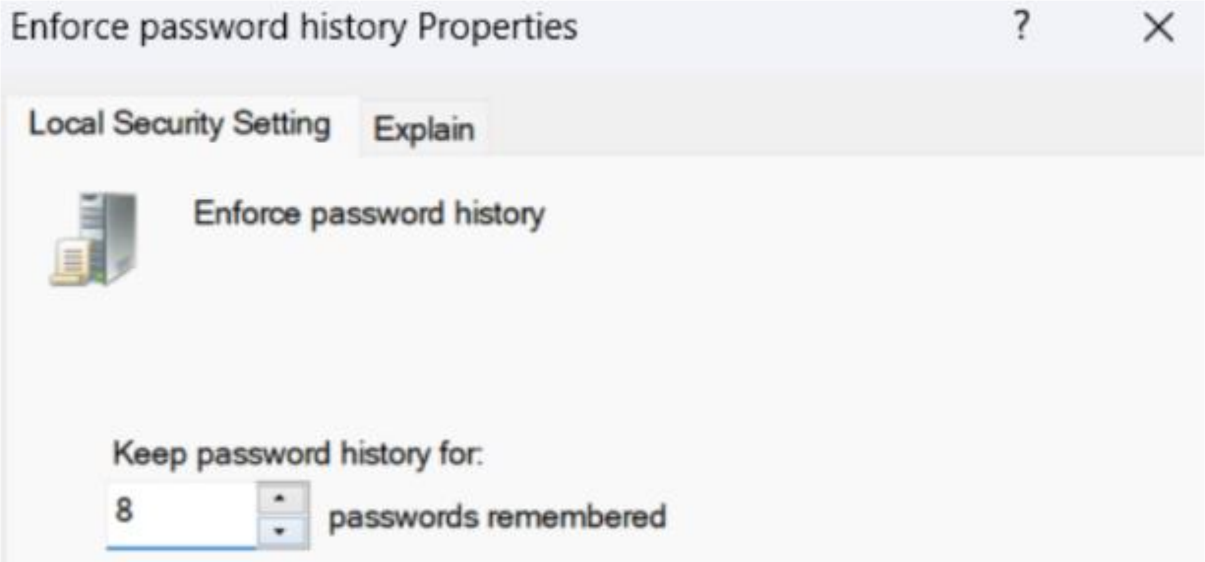
Policies > Password Policy



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) Click on Enforce password history and set it to enabled to require password changes

after a certain number of days (8 days)



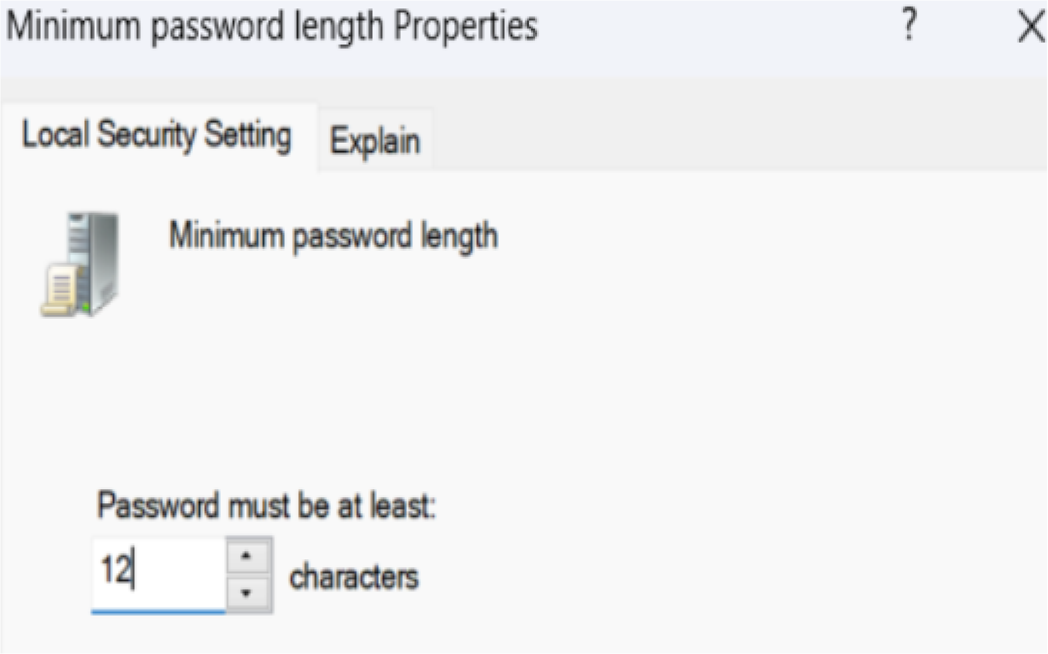
Enforce password history Properties

Enforce password history

Keep password history for:

8 passwords remembered

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

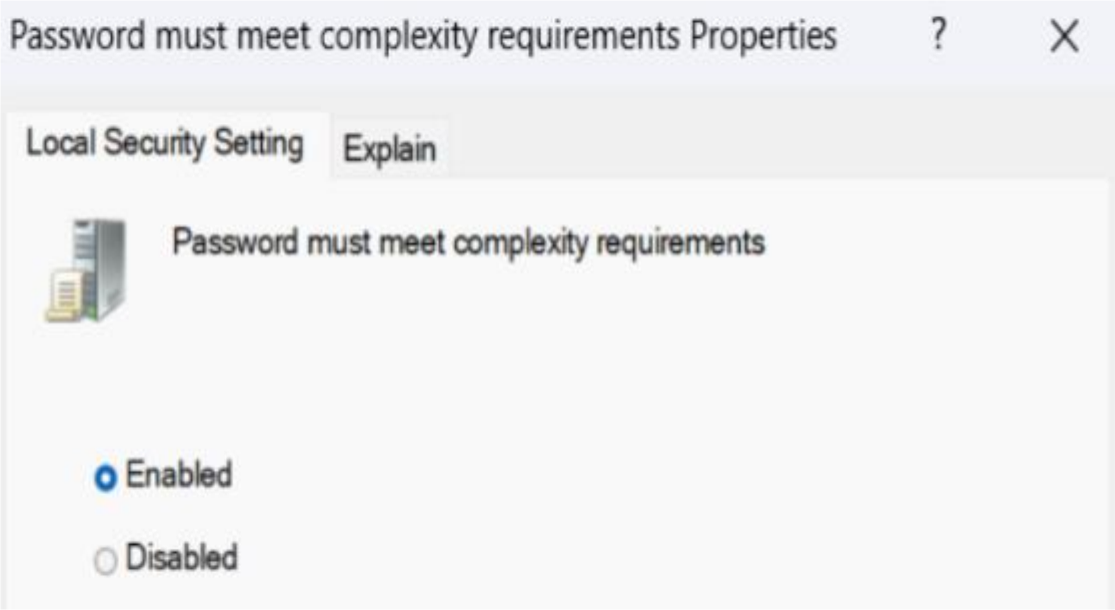


Minimum password length Properties

Minimum password length

Password must be at least:

12 characters



Password must meet complexity requirements Properties

Password must meet complexity requirements

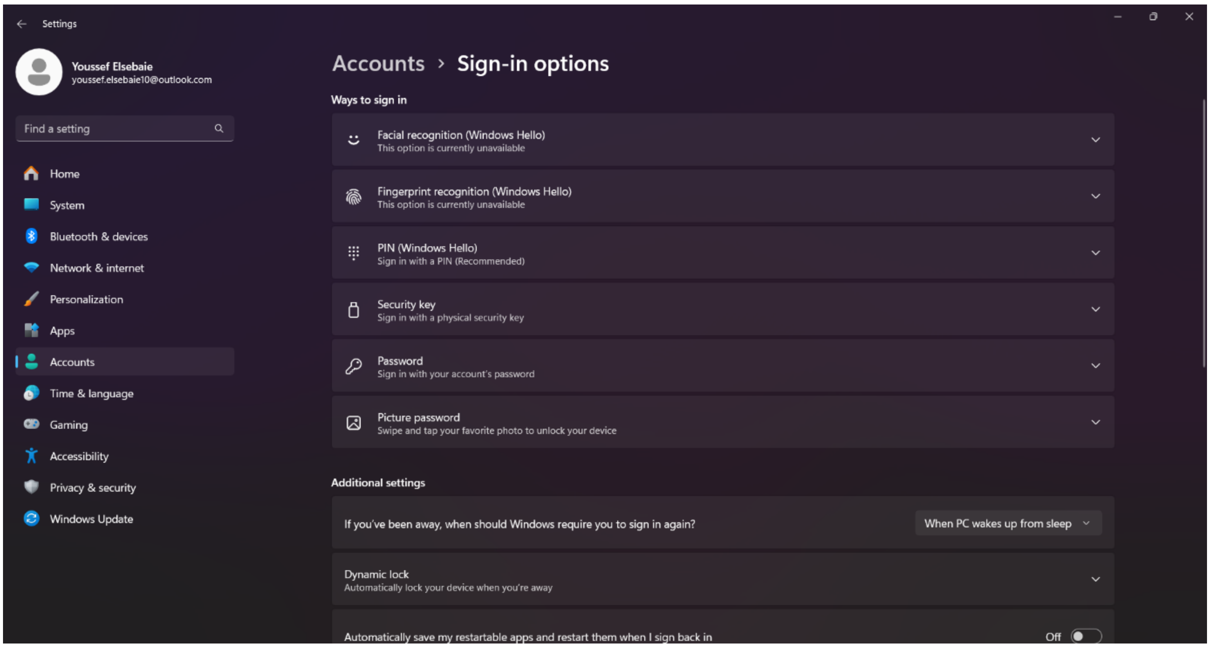
● Enabled

○ Disabled

Enabling multi-factor authentication

1)Open sign-in settings

2)Add a login Password to pc using my Microsoft account also enable Multi-factor Authentication



Accounts › Sign-in options

Ways to sign in

Facial recognition (Windows Hello)
This option is currently unavailable

Fingerprint recognition (Windows Hello)
This option is currently unavailable

PIN (Windows Hello)
Sign in with a PIN (Recommended)

Security key
Sign in with a physical security key

Password
Sign in with your account's password

Picture password
Swipe and tap your favorite photo to unlock your device

Additional settings

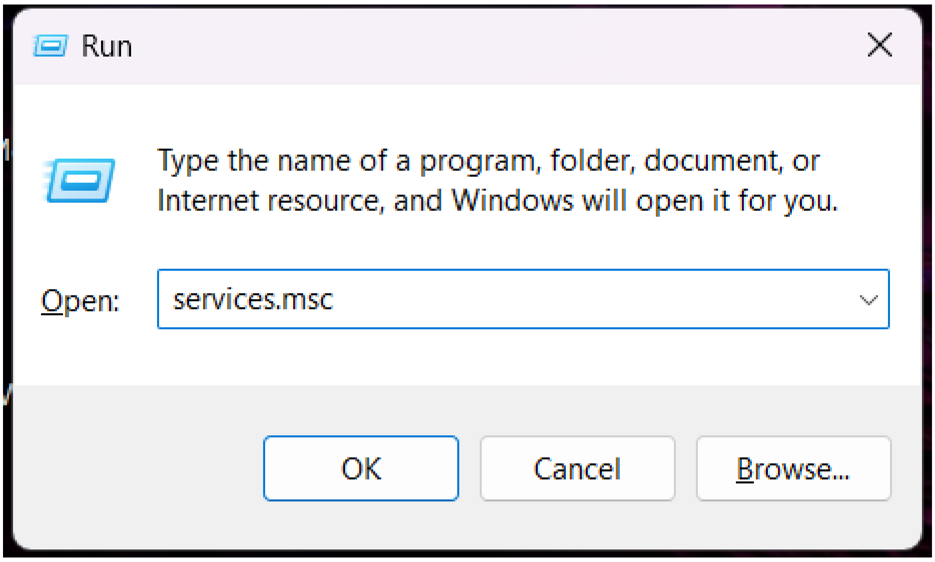
If you've been away, when should Windows require you to sign in again? When PC wakes up from sleep

Dynamic lock
Automatically lock your device when you're away

Automatically save my restartable apps and restart them when I sign back in Off

3.Disabling Unnecessary Services and Applications

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

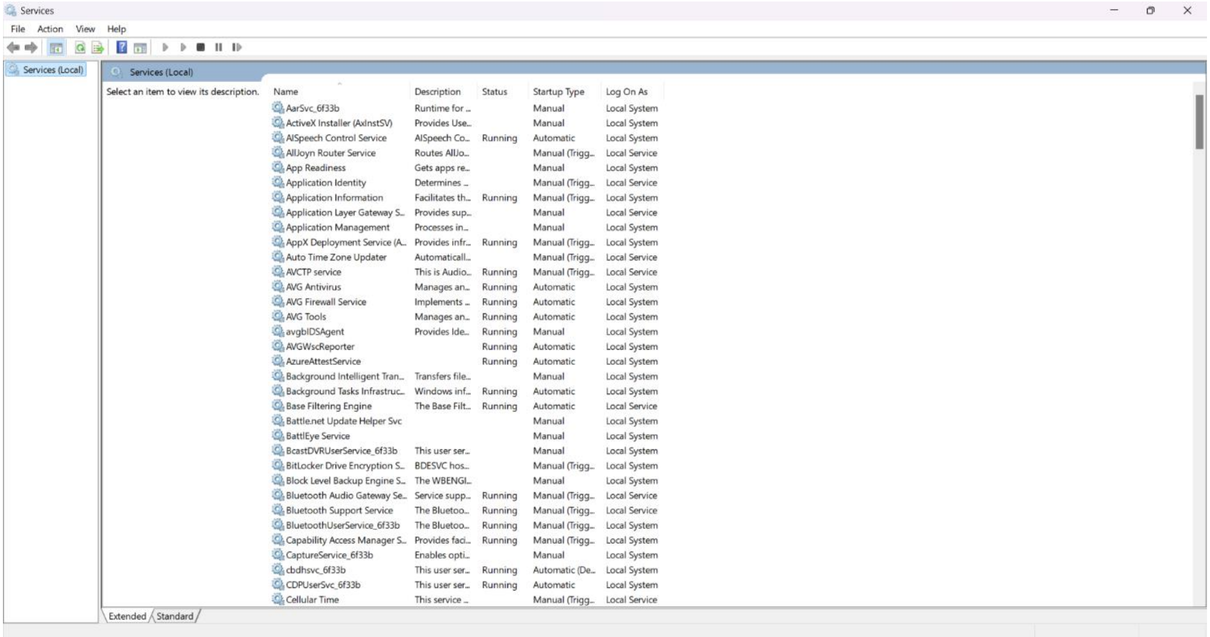


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: services.msc

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

teamviewer.



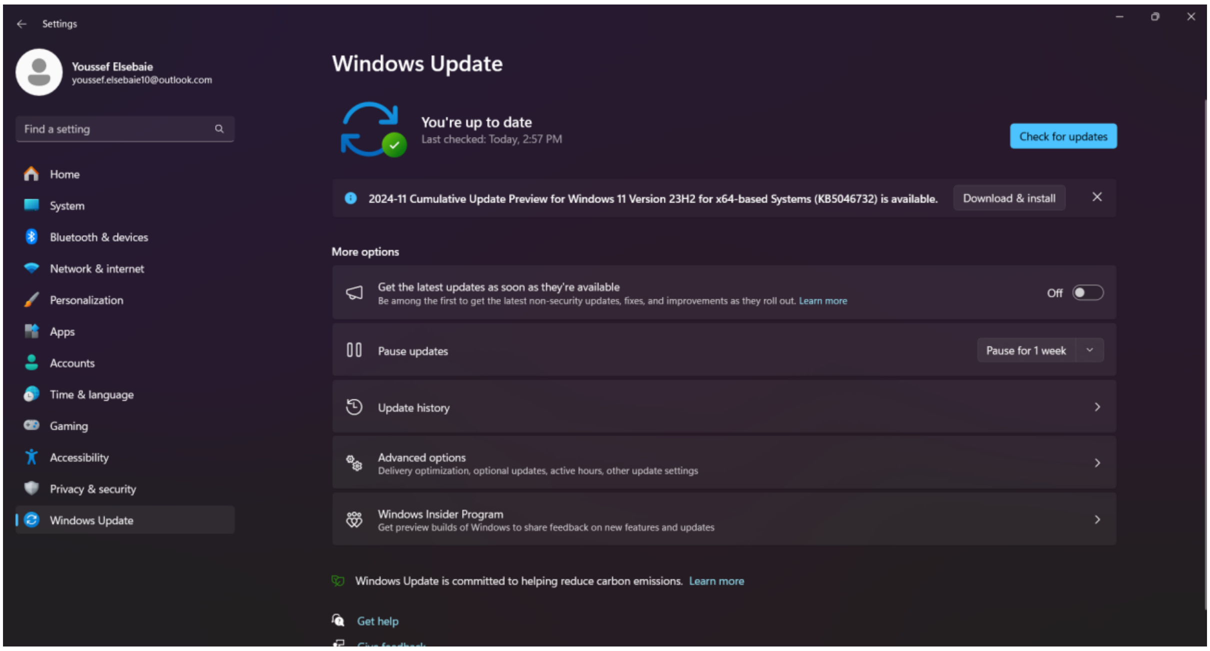
Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
AarSvc_6f33b	Runtime for ...		Manual	Local System
ActiveX Installer (AxInstSV)	Provides Use...		Manual	Local System
AISpeech Control Service	AISpeech Co...	Running	Automatic	Local System
AllJoyn Router Service	Routes AllJo...		Manual (Trigg...	Local Service
App Readiness	Gets apps re...		Manual	Local System
Application Identity	Determines ...		Manual (Trigg...	Local Service
Application Information	Facilitates th...	Running	Manual (Trigg...	Local System
Application Layer Gateway S...	Provides sup...		Manual	Local Service
Application Management	Processes in...		Manual	Local System
AppX Deployment Service (A...	Provides infr...	Running	Manual (Trigg...	Local System
Auto Time Zone Updater	Automaticall...		Manual (Trigg...	Local Service
AVCTP service	This is Audio...	Running	Manual (Trigg...	Local Service
AVG Antivirus	Manages an...	Running	Automatic	Local System
AVG Firewall Service	Implements ...	Running	Automatic	Local System
AVG Tools	Manages an...	Running	Automatic	Local System
avgbIDSAgent	Provides Ide...	Running	Manual	Local System
AVGWscReporter		Running	Automatic	Local System
AzureAttestService		Running	Automatic	Local System
Background Intelligent Tran...	Transfers file...		Manual	Local System
Background Tasks Infrastruc...	Windows inf...	Running	Automatic	Local System
Base Filtering Engine	The Base Filt...	Running	Automatic	Local Service
Battle.net Update Helper Svc			Manual	Local System
BattlEye Service			Manual	Local System
BcastDVRUserService_6f33b	This user ser...		Manual	Local System
BitLocker Drive Encryption S...	BDESVC hos...		Manual (Trigg...	Local System
Block Level Backup Engine S...	The WBENGI...		Manual	Local System
Bluetooth Audio Gateway Se...	Service supp...	Running	Manual (Trigg...	Local Service
Bluetooth Support Service	The Bluetoo...	Running	Manual (Trigg...	Local Service
BluetoothUserService_6f33b	The Bluetoo...	Running	Manual (Trigg...	Local System
Capability Access Manager S...	Provides faci...	Running	Manual (Trigg...	Local System
CaptureService_6f33b	Enables opti...		Manual	Local System
cbdhsvc_6f33b	This user ser...	Running	Automatic (De...	Local System
CDPUserSvc_6f33b	This user ser...	Running	Automatic	Local System
Cellular Time	This service ...		Manual (Trigg...	Local Service

4.Keeping Software Updated With The Latest Security Patches

1) Open Settings > Update & Security > Windows Update

Enable auto checking for update



Windows Update

You're up to date
Last checked: Today, 2:57 PM

2024-11 Cumulative Update Preview for Windows 11 Version 23H2 for x64-based Systems (KB5046732) is available.

Get the latest updates as soon as they're available
Be among the first to get the latest non-security updates, fixes, and improvements as they roll out. Learn more
Off

Pause updates: Pause for 1 week

Advanced options
Delivery optimization, optional updates, active hours, other update settings

Windows Insider Program
Get preview builds of Windows to share feedback on new features and updates

Windows Update is committed to helping reduce carbon emissions. Learn more

Key Security Measures Overview:

1. **Strong Password Policies:**
   - **Implementation:** Set requirements for password length, complexity, and history.
   - **Advantage:** Prevents brute-force attacks and unauthorized access.
2. **Multi-Factor Authentication (MFA):**
   - **Implementation:** Activated MFA on user accounts.
   - **Advantage:** Adds an extra security layer to prevent breaches.
3. **Disabling Unnecessary Services:**
   - **Implementation:** Turned off unused apps and non-essential services.
   - **Advantage:** Reduces the attack surface and potential vulnerabilities.
4. **Regular Updates:**
   - **Implementation:** Enabled automatic updates and ensured systems stay current.
   - **Advantage:** Fixes security flaws and protects against exploits and malware.