Windows Hardening Guide for Users

Name of student
Asaeyl Wali
Razan Rajhi
Raneem Bakour
Haneen Saleem
Dina Bajaifer

Table of Contents

Introduction

Project: How to Secure Your Computer (Windows 11)

What is this guide? This guide gives you the essential steps to install Windows on your device in a way that helps you protect your computer from any possible risks. We chose Windows 11 as our operating system.

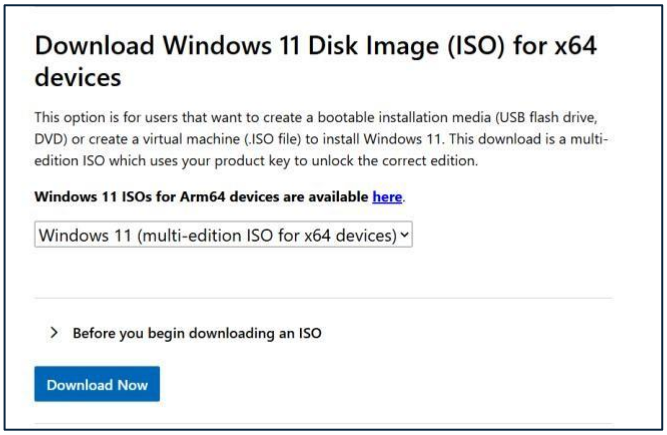
Many people don't know how to avoid viruses or hackers. This guide is a simple manual for beginners. We will show you easy steps to make your computer safe, from secure installation, to service hardening, patches and updates, accounts and policies, and any additional recommendations.

1. Secure Installation

This section describes **how to install Windows 11 in a secure way. The purpose** is to help beginners set up their computers safely from the start. The methods are straightforward and don't require any technical knowledge.

Step 1: Use Official Source to Download Windows

1. Installing Windows 11 should always begin with downloading it from Microsoft's official website, https://www.microsoft.com/en-au/software-download/windows11
2. Go to the **Download Windows 11 Disk Image (ISO)** section and click **download**, then follow the steps as shown in the pictures below. (see figures 1 to 3)



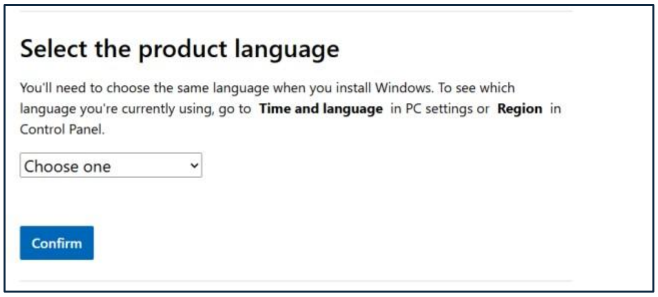
Download Windows 11 Disk Image (ISO) for x64 devices

This option is for users that want to create a bootable installation media (USB flash drive, DVD) or create a virtual machine (.ISO file) to install Windows 11. This download is a multi-edition ISO which uses your product key to unlock the correct edition.

Windows 11 ISOs for Arm64 devices are available here.

Windows 11 (multi-edition ISO for x64 devices)

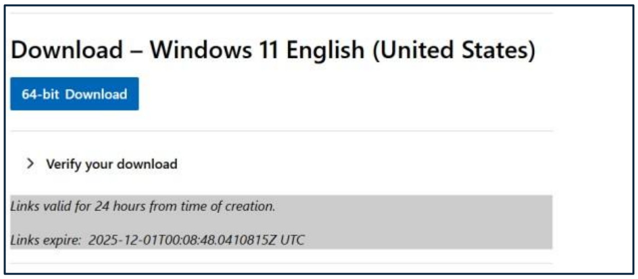
Figure 1 Download Windows ISO



Select the product language

You'll need to choose the same language when you install Windows. To see which language you're currently using, go to **Time and language** in PC settings or **Region** in Control Panel.

Figure 2 Selecting the preferred language



Download – Windows 11 English (United States)

Links valid for 24 hours from time of creation.

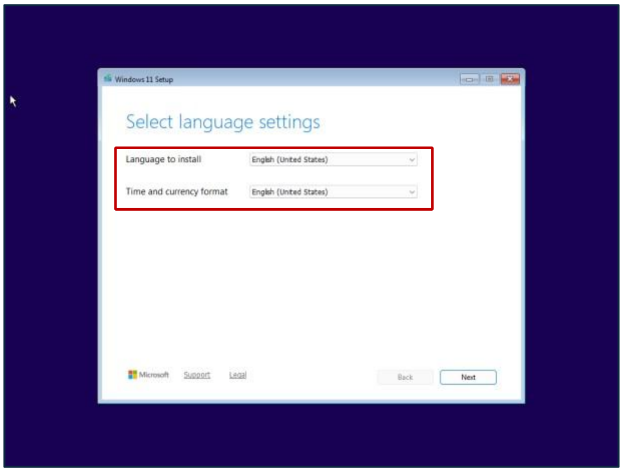
Links expire: 2025-12-01T00:08:48.0410815Z UTC

Figure 3 Downloading the ISO file

Step 2: Select language & Keyboard Settings

After the download is complete, double-click on the ISO file. It will open and launch the Windows Setup window, where you can see the language and keyboard selection., The user picks the language and region settings and selects the appropriate keyboard layout. During the installation.

Choosing the correct language is critical for user understanding of security messages and system notifications, while using the correct keyboard helps to avoid password problems during account creation.

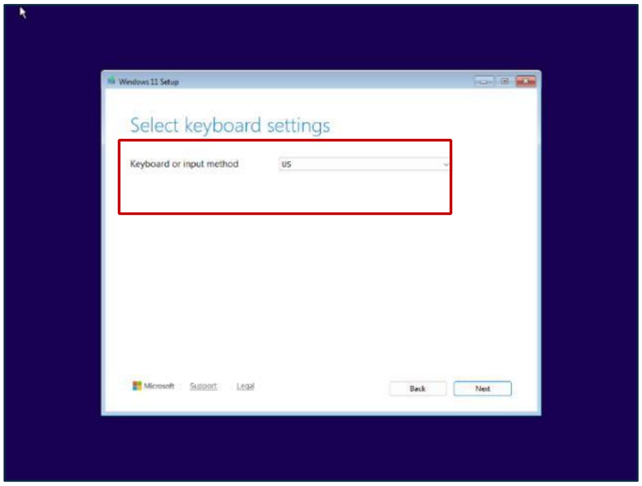


Select language settings

Language to install: English (United States)

Time and currency format: English (United States)

Figure 4 Selecting language settings



Select keyboard settings

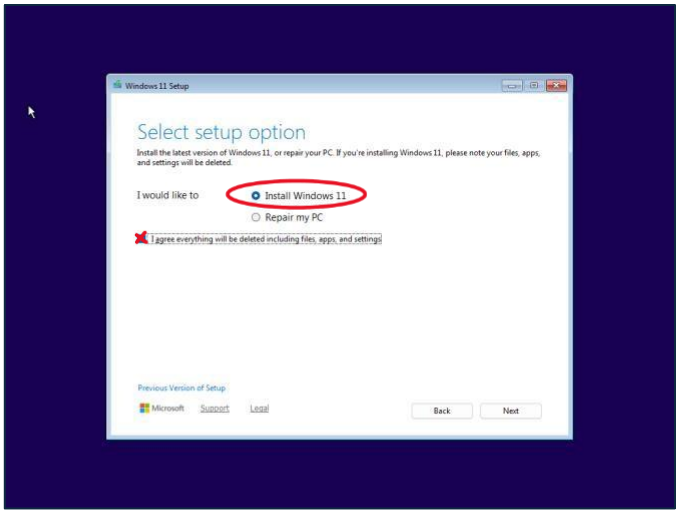
Keyboard or input method: US

Figure 5 Select keyboard settings

Step3: Select Setup Option

Now Choose "Install Windows."

This stage guarantees that the system is installed in a clean and structured manner, which is safer because it removes old files and unnecessary programs.



Select setup option

Install the latest version of Windows 11, or repair your PC. If you're installing Windows 11, please note your files, apps, and settings will be deleted.

I would like to ● Install Windows 11
○ Repair my PC

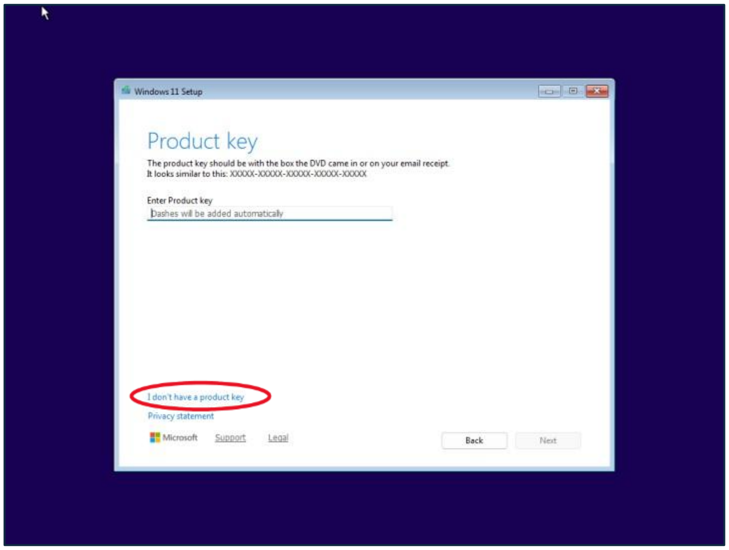
☒ I agree everything will be deleted including files, apps, and settings

Figure 6 selecting the set up options

A clean installation is considered a minimal and secure setup because it does not include any unnecessary or outdated software. This eliminates unneeded programs and decreases potential security threats.

Step4: Product Key

To proceed with the installation, select "I don't have a product key". This allows the installation to continue safely without using unlawful activation tools that are dangerous and may include malware.



Windows 11 Setup

Product key

The product key should be with the box the DVD came in or on your email receipt.
It looks similar to this: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Enter Product key

Dashes will be added automatically

I don't have a product key

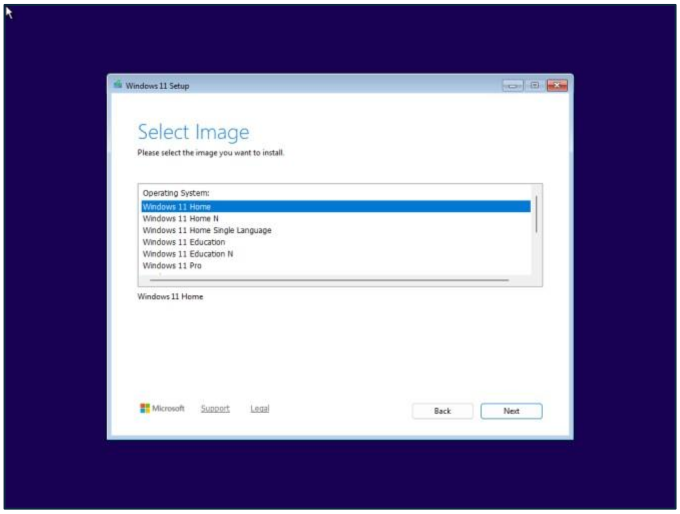
Privacy statement

Figure 7

Step5: Select Windows 11 Edition

Choosing Windows 11 version

Choosing the right edition guarantees compliance with security features like built-in protection measures. .



Windows 11 Setup

Select Image

Please select the image you want to install.

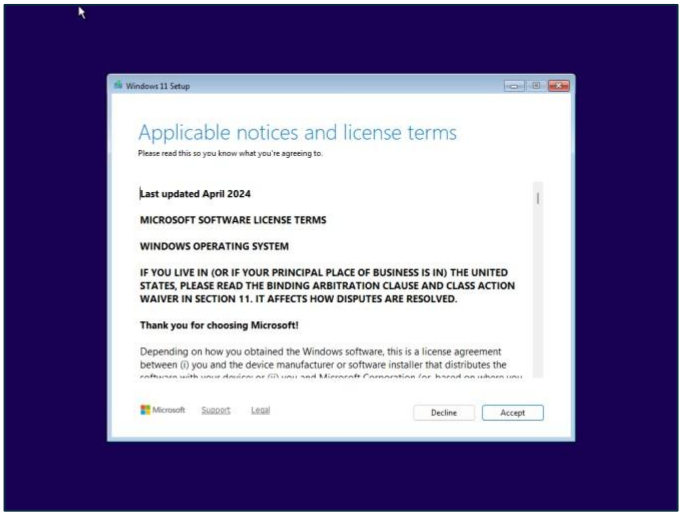
Operating System:
Windows 11 Home
Windows 11 Home N
Windows 11 Home Single Language
Windows 11 Education
Windows 11 Education N
Windows 11 Pro

Windows 11 Home

Figure 8 Selecting windows edition

Step6: License Terms

Accepting the Microsoft licensing agreements. It gives access to Microsoft's official updates and security services.



Applicable notices and license terms

Please read this so you know what you're agreeing to.

Last updated April 2024

MICROSOFT SOFTWARE LICENSE TERMS

WINDOWS OPERATING SYSTEM

IF YOU LIVE IN (OR IF YOUR PRINCIPAL PLACE OF BUSINESS IS IN) THE UNITED STATES, PLEASE READ THE BINDING ARBITRATION CLAUSE AND CLASS ACTION WAIVER IN SECTION 11. IT AFFECTS HOW DISPUTES ARE RESOLVED.

Thank you for choosing Microsoft!

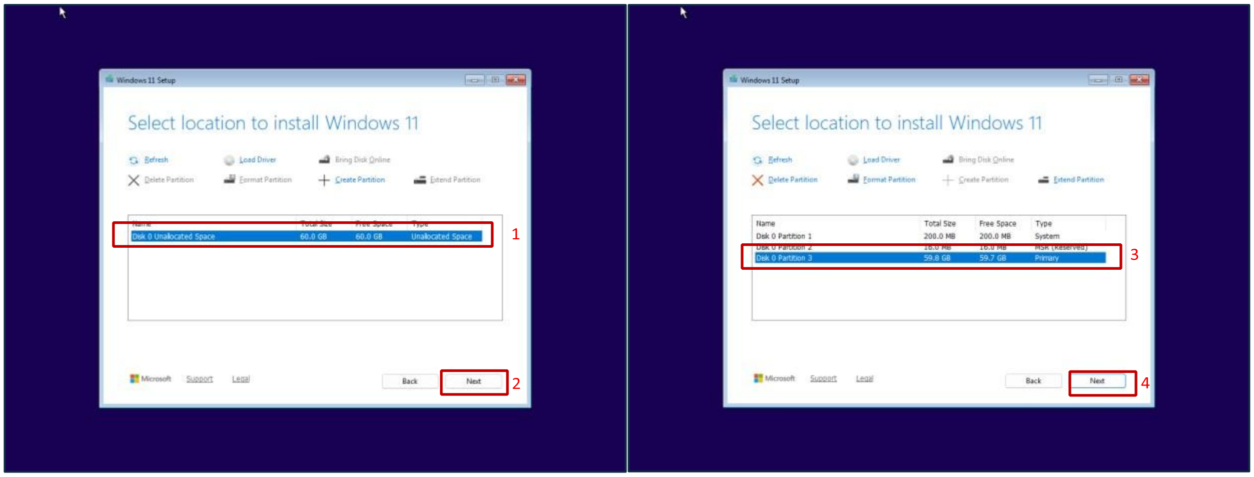
Depending on how you obtained the Windows software, this is a license agreement between (i) you and the device manufacturer or software installer that distributes the

Figure 9 Accepting windows agreement

Step7: Select Location to Install Windows 11

Selecting Drive 0 as the primary disk for installation.

Any old files, viruses, or unsafe settings from earlier systems are removed when Windows is installed on a clean primary drive.



Select location to install Windows 11

Name	Total Size	Free Space	Type
Disk 0 Unallocated Space	60.0 GB	60.0 GB	Unallocated Space

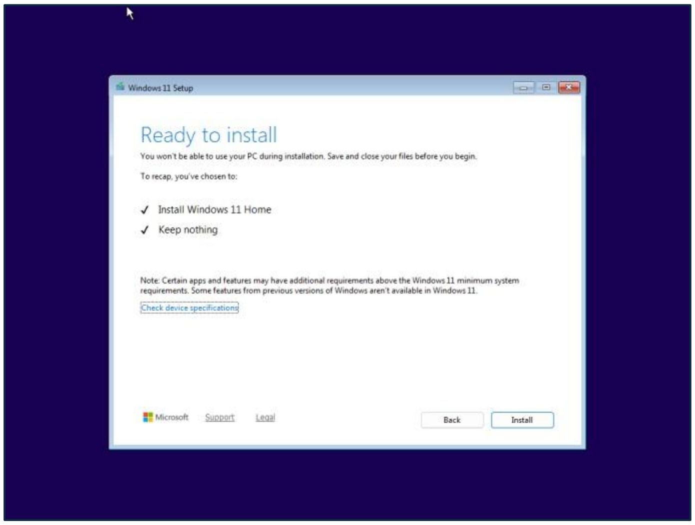
Select location to install Windows 11

Name	Total Size	Free Space	Type
Disk 0 Partition 1	200.0 MB	200.0 MB	System
Disk 0 Partition 2	16.0 MB	16.0 MB	MSR (Reserved)
Disk 0 Partition 3	59.8 GB	59.7 GB	Primary

Figure 10 Selecting the location

Step8: Ready to Install

Before installing Windows, confirm installation options to ensure all settings are correct and to avoid problems like installing on the wrong drive.



Ready to install

You won't be able to use your PC during installation. Save and close your files before you begin.

To recap, you've chosen to:

✓ Install Windows 11 Home

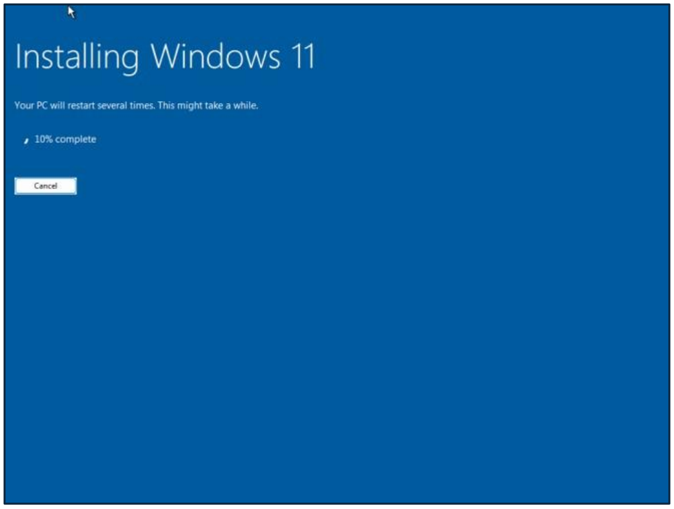
✓ Keep nothing

Note: Certain apps and features may have additional requirements above the Windows 11 minimum system requirements. Some features from previous versions of Windows aren't available in Windows 11.

Figure 11 Installing settings

Step9: Installing Windows 11

Windows files are being set up. The installation of the security system starts here.



Installing Windows 11

Your PC will restart several times. This might take a while.

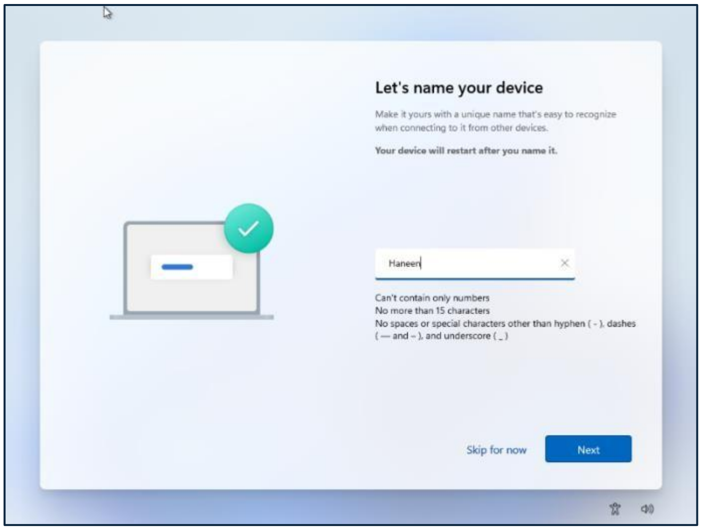
10% complete

Figure 12 Installing process

Step10: Checking for Updates

During setup, Windows is looking for the most recent updates. Then the most recent updates are being installed by Windows.

Installing updates immediately protects the system against recognized weaknesses. This ensures that the system is updated before the first use.



Let's name your device

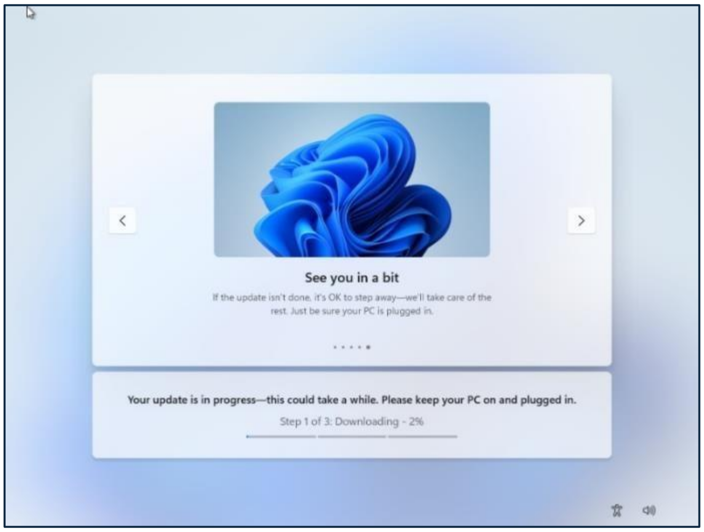
Make it yours with a unique name that's easy to recognize when connecting to it from other devices.

Your device will restart after you name it.

Haneen

Can't contain only numbers
No more than 15 characters
No spaces or special characters other than hyphen (-), dashes (— and –), and underscore (_)

Figure 13 Naming your device



See you in a bit

If the update isn't done, it's OK to step away—we'll take care of the rest. Just be sure your PC is plugged in.

Your update is in progress—this could take a while. Please keep your PC on and plugged in.

Step 1 of 3: Downloading - 2%

Figure 14 Updating

Step11: Successful Installation

After the installation is completed successfully, the Windows 11 desktop displays. This indicates that Windows was successfully installed.

Figure 15 Successful secure installation

2. Service Hardening:

When you start a Windows computer, many small features also start in the background. Some of these features help the device work normally, while others are not needed for everyday use or by normal users. So, the more unnecessary features are active, the more the computer gets exposed to problems. Service hardening means turning off any background features (services) users don't need, so the device becomes safer, easier to manage, and faster. Doing this step reduces the chances of having unwanted programs using these features. It makes the computer protected and safer.

In addition to disabling unnecessary services, sometimes when the computer turns on certain features, it also creates a path or doors that allow programs to talk to other devices or the Internet. If the feature is not needed, then it's better to close that door as well. Keeping extra doors open makes the computer less private and gives higher chances for unwanted actions. Closing these doors makes the computer safer and more focused on what the user actually needs.

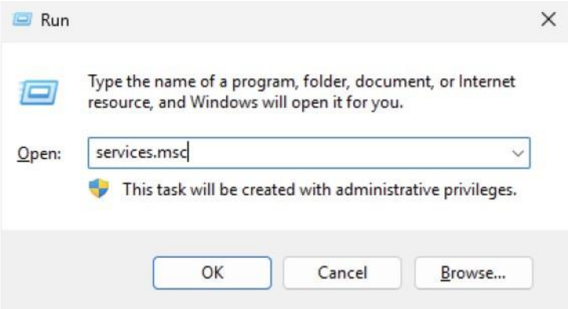
How to disable unnecessary services :

To turn off features that the user doesn't need, the first step is to open a certain place in Windows where all the background features are listed. You can do this by pressing the Windows key and the R key at the same time.

Esc
F1
F2
F3
F4
F5
F6
Tab
Q
W
E
R
T
Y
U
Caps Lock
A
S
D
F
G
H
J
Shift
Z
X
C
V
B
N
Ctrl
Alt
wikiHow

Figure 16 Windows and R keys placement

A tiny box with the name “run” will appear on the left bottom side of the window (see figure 17). You can type services.msc inside the box and press enter.



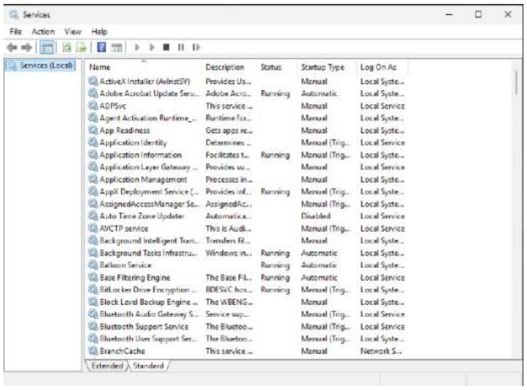
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: services.msc

This task will be created with administrative privileges.

Figure 17 Run Window

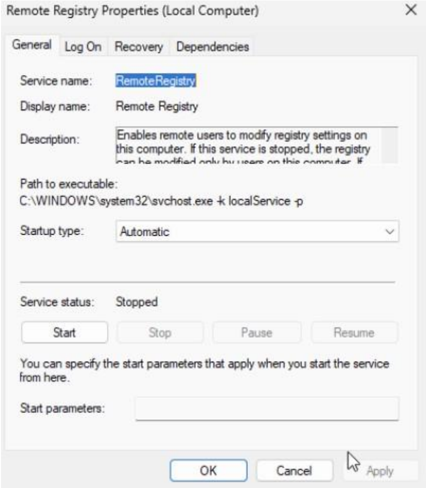
A new window opens, showing many items that run in the background (see figure 18). The user doesn't need to understand everything in that list. You will only change the items that the guide explains.



Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Us...		Manual	Local Syste...
Adobe Acrobat Update Serv...	Adobe Acro...	Running	Automatic	Local Syste...
ADPSvc	This service ...		Manual	Local Service
Agent Activation Runtime_...	Runtime for...		Manual	Local Syste...
App Readiness	Gets apps re...		Manual	Local Syste...
Application Identity	Determines ...		Manual (Trig...	Local Service
Application Information	Facilitates t...	Running	Manual (Trig...	Local Syste...
Application Layer Gateway ...	Provides su...		Manual	Local Service
Application Management	Processes in...		Manual	Local Syste...
AppX Deployment Service (...	Provides inf...	Running	Manual (Trig...	Local Syste...
AssignedAccessManager Se...	AssignedAc...		Manual (Trig...	Local Syste...
Auto Time Zone Updater	Automatica...		Disabled	Local Service
AVCTP service	This is Audi...		Manual (Trig...	Local Service
Background Intelligent Tran...	Transfers fil...		Manual	Local Syste...
Background Tasks Infrastru...	Windows in...	Running	Automatic	Local Syste...
Balloon Service		Running	Automatic	Local Syste...
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
BitLocker Drive Encryption ...	BDESVC hos...	Running	Manual (Trig...	Local Syste...
Block Level Backup Engine ...	The WBENG...		Manual	Local Syste...
Bluetooth Audio Gateway S...	Service sup...		Manual (Trig...	Local Service
Bluetooth Support Service	The Bluetoo...		Manual (Trig...	Local Service
Bluetooth User Support Ser...	The Bluetoo...		Manual (Trig...	Local Syste...
BranchCache	This service ...		Manual	Network S...

Figure 18 Window with background services.

When you double-click on any service in that list, a small window will appear that shows extra details about it (see figure 19).


Remote Registry Properties (Local Computer)

Service name: RemoteRegistry

Display name: Remote Registry

Description: Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If

Path to executable:
C:\WINDOWS\system32\svchost.exe -k localService -p

Startup type: Automatic

Service status: Stopped

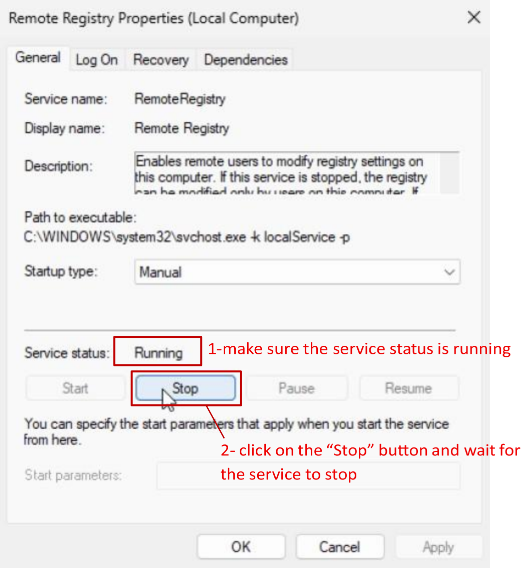
You can specify the start parameters that apply when you start the service from here.

Start parameters:

Figure 19 The service properties

The previous window shows properties of any chosen service. It explains what this service does and how it starts. At the top of the window, you can see the “Service name.” This helps you make sure that you're changing the correct item.

Under the name, there is a short description of what this service does. You don't need to understand all the details in the description, but it gives a simple idea. Below the description, there is a section called “Service Status.” This shows whether the service is running or stopped. In order to stop a service, first check the service status; if it was “running,” then click on the stop button (see figure 20)


Remote Registry Properties (Local Computer)

Service name: RemoteRegistry

Display name: Remote Registry

Description: Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If

Path to executable:
C:\WINDOWS\system32\svchost.exe -k localService -p

Startup type: Manual

Service status: Running

1-make sure the service status is running

You can specify the start parameters that apply when you start the service from here.

2- click on the “Stop” button and wait for the service to stop

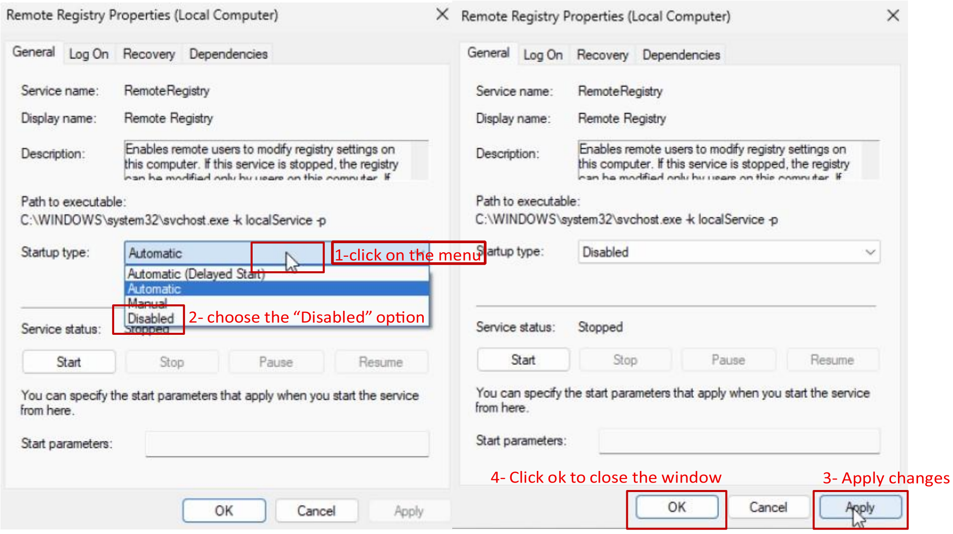
Start parameters:

Figure 20 How to stop a service

One of the most important parts of this window is the Startup Type menu. This menu can control how the service starts. If you set it to automatic, the service starts every time you turn on your computer. If you set it to automatic delayed start, it also starts automatically when you turn on
]

the computer, but a little later. The manual means the service will start only if your computer needs it. Disabled tells the computer not to start this service ever for services that are not needed. Choosing Disabled is the best option, keeping your computer from running unnecessary features in the background.

To disable a service, click on the “Startup Type” menu, then choose “Disable,” then “Apply” in order to save your changes. (see figure 21)



Remote Registry Properties (Local Computer)

Service name: RemoteRegistry

Display name: Remote Registry

Description: Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If

Path to executable:
C:\WINDOWS\system32\svchost.exe -k localService -p

Startup type: Automatic

Automatic (Delayed Start)
Automatic
Manual
Disabled

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

1-click on the menu

2- choose the “Disabled” option

Remote Registry Properties (Local Computer)

Service name: RemoteRegistry

Display name: Remote Registry

Description: Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If

Path to executable:
C:\WINDOWS\system32\svchost.exe -k localService -p

Startup type: Disabled

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

4- Click ok to close the window

3- Apply changes

Figure 21 Startup type menu

Introduction to risky services:

These following services are recommended to be turned off using the method explained above.

Remote registry: a feature that allows outside computers to change settings on your personal computer from far away. Normal home users don't need this type of remote control, so it is safer to keep your settings private. When the service is running, it keeps a small door open that would allow outside devices to reach your device. Turning it off would remove the path to your device and protect the computer from any unwanted changes.

Print Spooler: This is a feature that helps your computer to prepare files for printing. If users don't have a printer, then the service isn't necessary. In the past attackers used this service to enter computers since it gives them privileges. By turning it off, the device becomes safer for users who don't use printing features.

SSTP Discovery: It's a feature that makes your computer look for other devices on the network, like smart TVs or smart washers. Most users don't need their computer for these purposes. And turning on these features would also create extra unnecessary doors. If it stays on, then the computer would constantly send signals. So turning it off closes these unnecessary paths and signals, making the device more private.

Remote Desktop Services: This feature allows someone to control your computer from another device. It could be useful in workplaces, but for home users and solo users, they don't need this remote access. Activating this service keeps the device prepared for any possible access request. So, turning this feature off closes the door for remote access and keeps your computer protected.

UPnP Device Host: This feature allows programs and applications and devices to open doors to your device automatically without asking the user. It can be helpful at some times, but it is not needed for most people because attackers can use these open doors for themselves. Turning the feature off is highly recommended.

Closing unused ports:

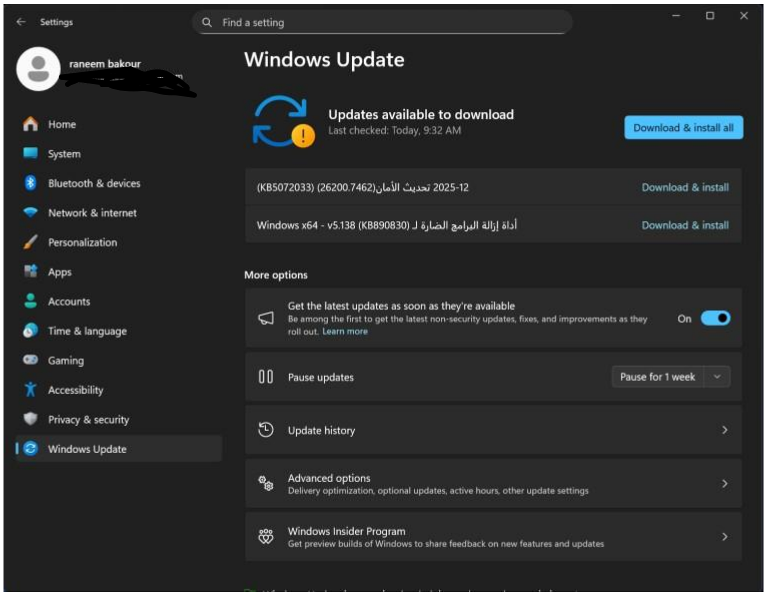
As previously discussed, windows services open doors with other devices or the internet Those doors are known as ports. If a service is no longer needed, the associated port should be closed. When unnecessary services are disabled in the way we showed above, the ports they use automatically close. For example, when you turn off remote desktop services, the ports associated with it also get closed, helping the computer to stay safer without requiring any extra work from the user.
Beginners don't need to manage ports manually. Closing unused ports happens when you disable unnecessary services.

3. Patching and Updates

. **Why do we need updates?** Think of updates like a "check-up" or medicine for your computer. They fix problems and keep your computer healthy

Step 1: Get the Updates

- **What to do:** Click the Windows button and type "Settings". Go to Windows Update. Click the button that says "Check for updates".
- **What happens:** Your computer will look for new repairs from Microsoft and download them.



Settings

Find a setting

raneem bakour [redacted]

Windows Update

Updates available to download
Last checked: Today, 9:32 AM

Download & install all

(KB5072033) (26200.7462)تحديث الأمان 2025-12 — Download & install

Windows x64 - v5.138 (KB890830) أداة إزالة البرامج الضارة لـ — Download & install

More options

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 — On

Pause updates — Pause for 1 week

Update history

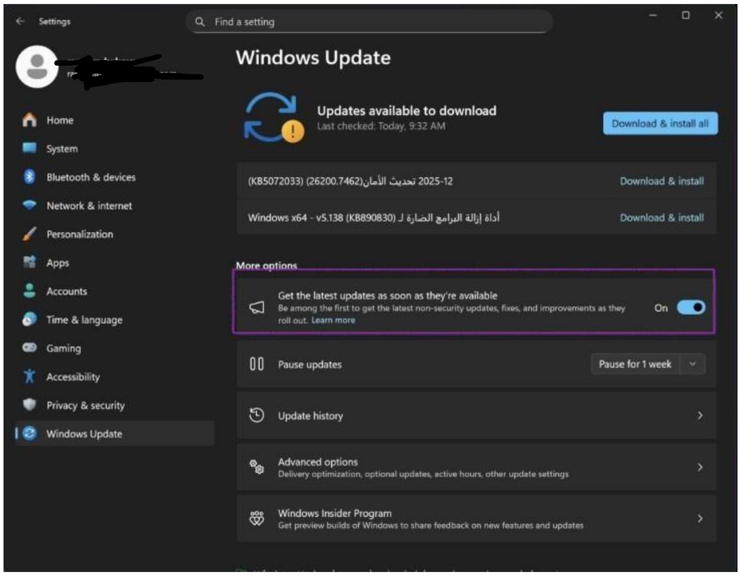
Advanced options
Delivery optimization, optional updates, active hours, other update settings

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

Figure 22 Windows update settings

Step 2: Turn on Automatic Updates

- **What to do:** In the same menu, find the button that says "Get the latest updates soon". Switch it to "On".
- **What happens**: You don't have to remember to update. The computer will do it for you automatically.



Settings

Find a setting

[redacted]

Windows Update

Updates available to download
Last checked: Today, 9:32 AM

Download & install all

(KB5072033) (26200.7462)تحديث الأمان 2025-12 — Download & install

Windows x64 - v5.138 (KB890830) أداة إزالة البرامج الضارة لـ — Download & install

More options

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 — On

Pause updates — Pause for 1 week

Update history

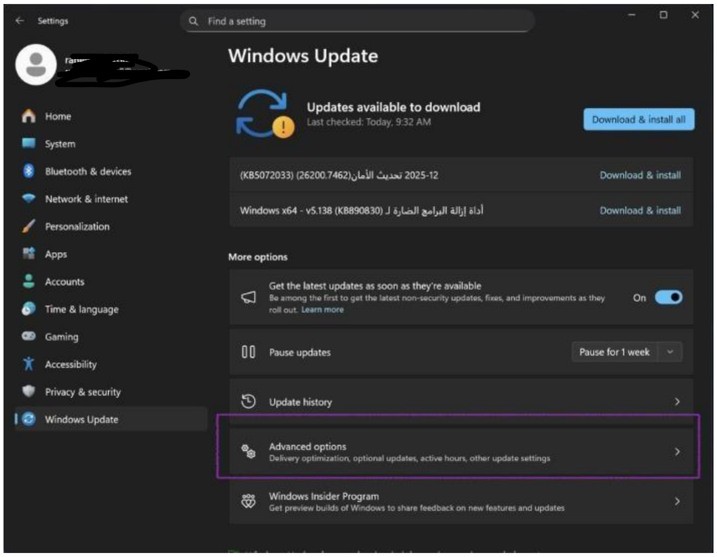
Advanced options
Delivery optimization, optional updates, active hours, other update settings

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

Figure 23 Receiving latest updates

Step 3: Set Work Hours (Active Hours)

- **What to do:** Go to Advanced options and click on Active hours. Pick the time you use the computer (like 8 AM to 5 PM).
- **What happens:** The computer will not restart while you are working. It will wait until you are done.



Windows Update

Updates available to download
Last checked: Today, 9:32 AM

Download & install all

2025-12 تحديث الأمان (26200.7462) (KB5072033) — Download & install

Windows x64 - v5.138 (KB890830) أداة إزالة البرامج الضارة لـ — Download & install

More options

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 — On

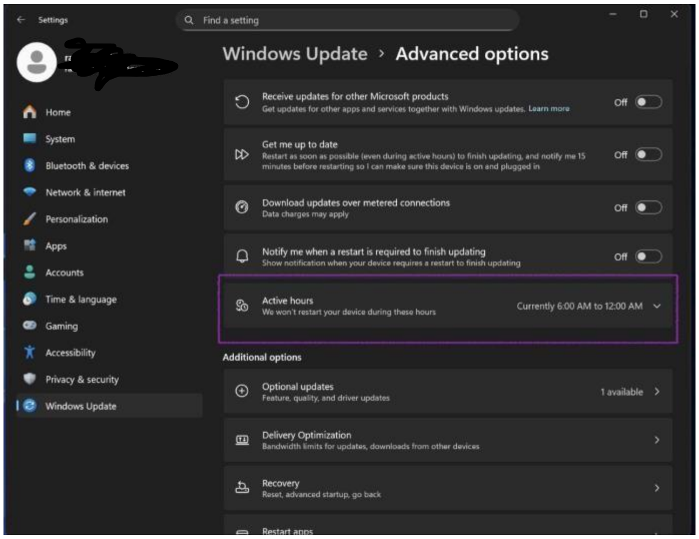
Pause updates — Pause for 1 week

Update history

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

Figure 24 Going to advanced settings



Windows Update › Advanced options

Receive updates for other Microsoft products
Get updates for other apps and services together with Windows updates. Learn more — Off

Get me up to date
Restart as soon as possible (even during active hours) to finish updating, and notify me 15 minutes before restarting so I can make sure this device is on and plugged in — Off

Download updates over metered connections
Data charges may apply — Off

Notify me when a restart is required to finish updating
Show notification when your device requires a restart to finish updating — Off

Active hours
We won't restart your device during these hours — Currently 6:00 AM to 12:00 AM

Additional options

Optional updates
Feature, quality, and driver updates — 1 available

Delivery Optimization
Bandwidth limits for updates, downloads from other devices

Recovery
Reset, advanced startup, go back

Restart apps

Figure 25 Setting work hours

Why is this important?

The Reason: Old software has "holes" or weak spots. Bad people (hackers) use these holes to get into your computer. When you update Windows, you close these holes and keep your files safe.

4. User Accounts and Policies

User accounts and security policies are essential parts of protecting a Windows system. Every person who uses a device must sign in with an account that controls what they can do. When accounts are created and managed correctly, the system becomes safer and easier to use. This section explains account types, how to create them, and how to secure them so beginners can follow every step with confidence.

Overview of Windows User Account Types

Windows provides several types of user accounts. Knowing the differences helps you choose the correct type based on the user's needs.

A **local account** is saved only on your computer. For example, if you create an account called *Student01*, that account can only be used on that one device. This is helpful when you want tight control over who can sign in. It improves security because authentication stays local and does not depend on the internet (authentication is the step where the device asks you to prove your identity, such as entering a password to access the system).

A **Microsoft cloud account** uses an email such as *name@outlook.com* or *name@hotmail.com*. When a user signs in with this account, their settings can sync across devices. Cloud accounts support features like Multi-Factor Authentication (MFA), making them safer for users who frequently access online apps.

A **domain account** is used in larger organizations. For example, if the domain is *school.edu*, a student might sign in with *student01@school.edu*. These accounts are centrally managed, which means administrators can enforce strong security policies on all users at once.

Permission levels also matter (permissions determine what a user is allowed to do after they sign in, such as opening files, installing apps, or changing settings). An **Administrator** can install apps, change system settings, and manage other accounts. A **Standard user** can complete everyday tasks like browsing, working on assignments, and running most applications. A **Guest account** has very limited access and is usually disabled because it creates unnecessary security risks.

For example, if your little brother is using your computer, you should create a standard user account for him instead of letting him use your administrator account. This prevents accidental changes to your system.

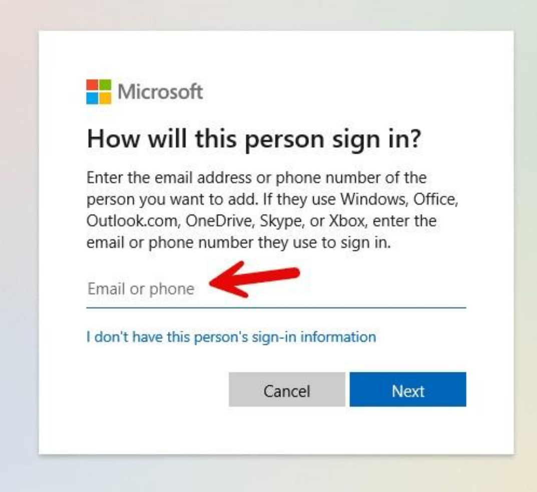
Creating User Accounts in Windows

Windows provides several ways to create user accounts. Choose the method that feels easiest for you.

Creating an account through the Settings app

If you want a simple workflow:

1. Open **Settings → Accounts → Other users**.
2. Select **Add account**.
3. Enter the email address associated with the user’s Microsoft account or create a new one.

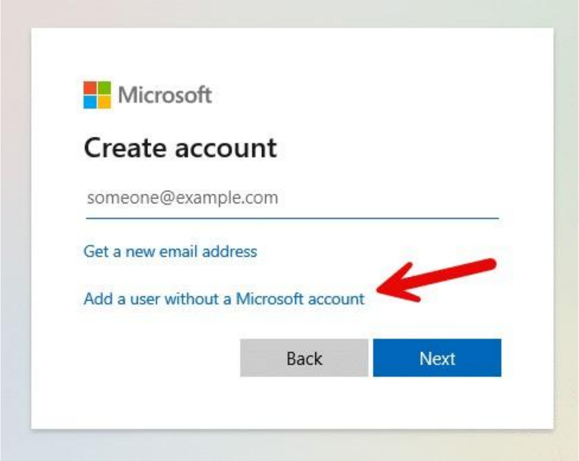


Microsoft

How will this person sign in?

Enter the email address or phone number of the person you want to add. If they use Windows, Office, Outlook.com, OneDrive, Skype, or Xbox, enter the email or phone number they use to sign in.

Figure 26 Using the Settings App to add a Microsoft account on Windows.

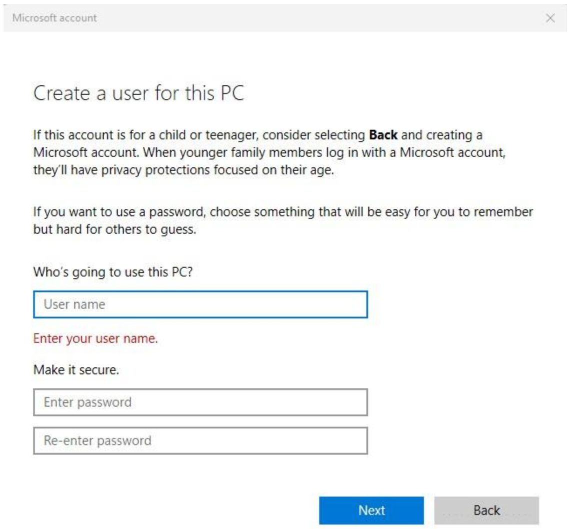


Microsoft

Create account

Figure 27 Selecting "I don’t have this person’s sign-in information" to create a local account.

4. Enter the username and create a strong password (see next subsection).



Create a user for this PC

If this account is for a child or teenager, consider selecting **Back** and creating a Microsoft account. When younger family members log in with a Microsoft account, they'll have privacy protections focused on their age.

If you want to use a password, choose something that will be easy for you to remember but hard for others to guess.

Who's going to use this PC?

Enter your user name.

Make it secure.

Figure 28 Entering a username, setting a strong password, and configuring security questions for the new local account.

This method improves security because you directly set password requirements and recovery questions.

Creating an account through the Control Panel If

you prefer the classic Windows look:

1. Open **Control Panel → User Accounts**.
2. Choose **Manage another account**.
3. Select **Add a new user**.
4. Finish setup in the Settings window.

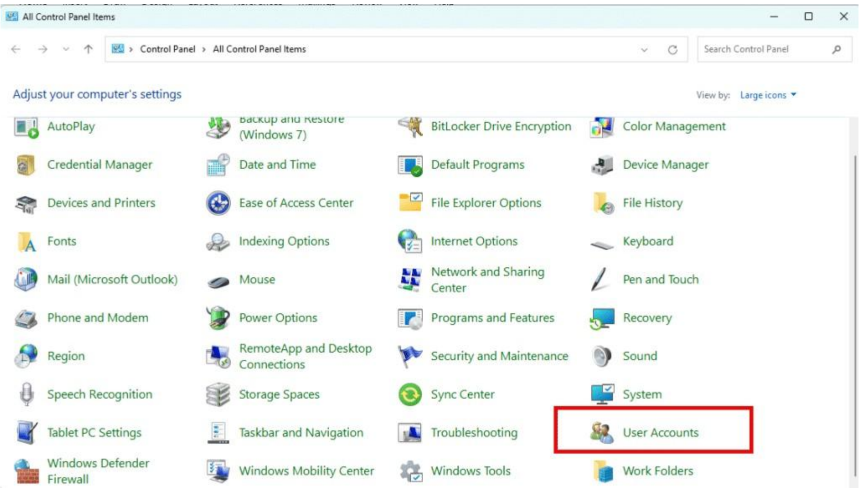
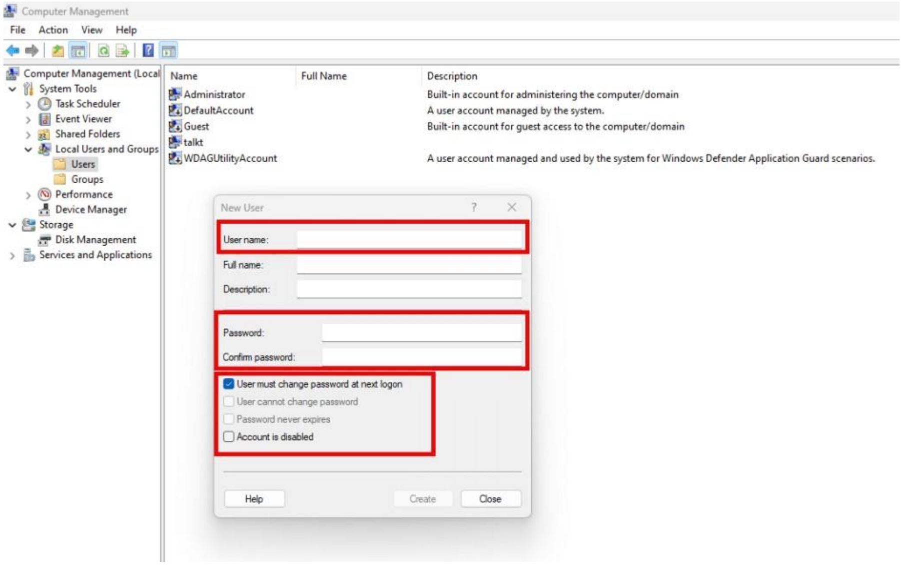


Figure 29 Using the Control Panel to create a new local account via "Manage another account" and linking to Settings.

Creating an account through Computer Management

This method gives more control, especially for multiple users:

1. Open **Computer Management → Local Users and Groups → Users**.
2. Right-click **New User**.
3. Set the username and password.
4. Decide whether the user must change their password at first login.



Name	Full Name	Description
Administrator		Built-in account for administering the computer/domain
DefaultAccount		A user account managed by the system.
Guest		Built-in account for guest access to the computer/domain
talkt		
WDAGUtilityAccount		A user account managed and used by the system for Windows Defender Application Guard scenarios.

☑ User must change password at next logon
☐ User cannot change password
☐ Password never expires
☐ Account is disabled

Figure 30 Using the Computer Management to create a new local account.

This improves security because users create their own private passwords.

Creating accounts using Command Prompt or PowerShell

Advanced users can automate account creation:

- Command Prompt: `net user student123 StrongPass#2025 /add`
- PowerShell:
  ```
  $Password = Read-Host -AsSecureString "Enter Password" New-
  LocalUser -Name "LabUser" -Password $Password
  ```

These tools improve security because they reduce errors and allow consistent setups across many devices.

Password Standards

A secure Windows system depends on strong passwords. Weak passwords are easy to guess or crack. A strong password should have **at least 12 characters**, **mixing uppercase letters**, **lowercase letters**, **numbers**, and **special characters**.

Examples of strong passwords include:

- `BlueSky#2025!Book`
- `RiverStone@4829`
- `Sunset*Cloud+993`
- `MangoTree!2040`

These examples show how you can combine words and symbols to create a password that is long and difficult to guess.

You should avoid anything predictable such as:

- your name (e.g., `Dina2024`)
- your birthdate (e.g., `2005/02/21`)
- simple number patterns (e.g., `12345678` or `11111111`)
- common passwords (e.g., `password123` or `iloveyou`)

Predictable passwords make it much easier for attackers to break into your account using guessing tools or known password lists.

Windows supports **password history rules** that prevent users from reusing old passwords. For example, if Windows is set to remember the last 24 passwords, you cannot switch back to an older, weaker password. This keeps attackers from trying previously leaked passwords.

Windows can also apply **password expiration policies**, which require users to change their passwords after a certain number of days (e.g., every 90 days). This is especially important for administrator accounts because these accounts have the highest permissions.

Windows offers **LAPS (Local Administrator Password Solution)**, which automatically creates a unique, random password for each device's local administrator account. For example, one device may receive the password `Hawk@3921!Moon`, while another receives `Tree&9812$Wind`. This ensures that even if one administrator's password is stolen, it cannot be used to access other machines.

Microsoft cloud accounts should always use **Multi-Factor Authentication (MFA)**. For example, when signing in, you may receive:

- a notification in the Microsoft Authenticator app,
- a text message with a verification code, or
- a prompt to approve the login through your phone.

Even if someone steals your password, they cannot access your account without completing this second step, which greatly improves security.

Principle of Least Privilege (PoLP)

This principle ensures that every user receives only the access they need and nothing more. Giving users minimal privileges helps prevent accidental system changes and reduces the chances of malware spreading throughout the device.

Users should always sign in with a **standard account** for daily work. This protects the system because standard accounts cannot install harmful apps, modify system files, or change important settings. For example, if a user visits a malicious website, the damage is limited because the standard account does not have the authority to install programs silently.

Administrators should keep two separate accounts: **One standard account for normal use** and **one administrator account for managing the system**. This separation ensures that administrative rights are used only when required, lowering exposure to unnecessary risks.

For example, if you are completing homework, checking your email, or browsing the web, you should use your standard account. Only switch to the administrator account when you need to install software, change system settings, or manage other accounts.

Windows supports **Just-In-Time (JIT) access**, which gives elevated permissions only for a specific task and time period. This prevents administrative privileges from being available continuously. For example, if you need to install a driver, JIT grants admin rights for only that installation process.

Additionally, **Just-Enough-Access (JEA)** restricts what administrators can do during elevated tasks. This means even during admin activities, you only receive precise permissions for the specific task you are performing. For example, if you only need to restart a service, JEA can allow that action without granting full administrator privileges.

Regular privilege reviews help remove outdated permissions. This improves security by preventing old, forgotten accounts from having too much access. For example, if a student graduates or an intern leaves, their access should be removed immediately so their accounts cannot be misused later.

User Group Management

Windows manages permissions through groups. Instead of assigning permissions to each user individually, you place users into groups that already have the correct permission levels. This makes administration easier and ensures consistency across all users.

For example, if all science teachers need access to a shared folder, you can create a group called *ScienceTeachers* and add all the teachers to that group. The folder permissions will then apply automatically to everyone in the group. Similarly, if a finance team needs access to sensitive spreadsheets, you could create a group called *FinanceTeam* and assign permissions only to that folder. This prevents unauthorized users from viewing confidential data.

Windows includes built-in groups such as **Administrators**, **Users**, and **Remote Desktop Users**. Assigning permissions through these groups improves security because it keeps user rights consistent, easier to manage, and reduces the risk of accidentally granting too many privileges to one user.

You can also manage permissions at the file or folder level. Right-click a file or folder, select **Properties → Security**, and choose exactly who can **read**, **write**, or **modify** that item. For example, you might give the *MarketingTeam* read-only access to a shared folder while giving the Managers group full control. This method ensures that each user or group can only perform actions appropriate for their role.

Groups should be reviewed regularly. If someone changes jobs, leaves the company, or stops using a device, you should remove them from groups they no longer need. For example, if a teacher moves from the science department to history, remove them from the *ScienceTeachers* group and add them to *HistoryTeachers*. This reduces the risk of unauthorized access and keeps the system organized.

Account Maintenance: Enabling, Disabling, Deleting, and Promoting Accounts

Account maintenance ensures that your system remains secure and organized. Proper maintenance prevents old or inactive accounts from becoming security risks.

Local accounts can be **updated** by changing passwords, usernames, or other profile details through the Settings app or Computer Management. For example, if a student forgets their password, an administrator can reset it to a temporary secure password and require them to change it at next login. Updating account details ensures that only authorized people can access the account.

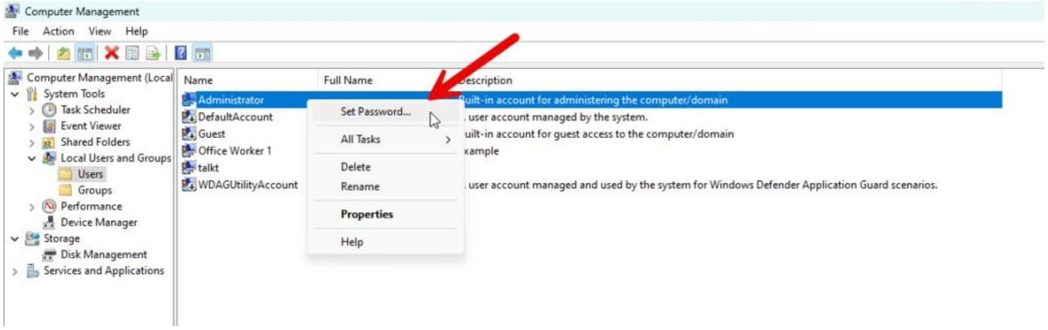


Figure 31 Screenshot showing the Computer Management Console interface. The "Users" folder is selected, and the "Set Password..." option for a local user account is highlighted to demonstrate how to update passwords.

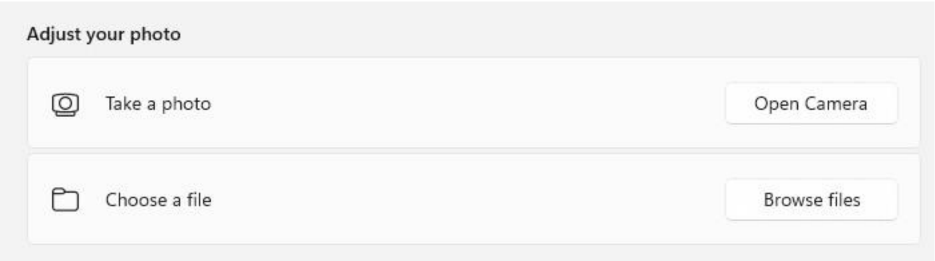
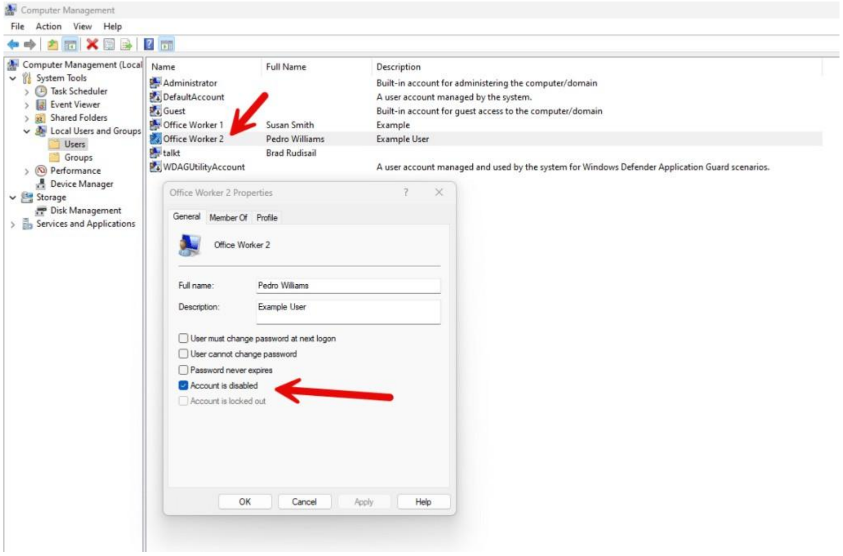


Figure 32 Screenshot of the Settings App account page, highlighting the section where users can update their profile picture and basic account details.

Unused or inactive accounts should be **disabled** rather than deleted immediately. This improves security because attackers cannot use dormant accounts as entry points. For example, if a student completes a course and no longer needs access, disable their account until you are certain it can be safely removed.



Name	Full Name	Description
Administrator		Built-in account for administering the computer/domain
DefaultAccount		A user account managed by the system.
Guest		Built-in account for guest access to the computer/domain
Office Worker 1	Susan Smith	Example
Office Worker 2	Pedro Williams	Example User
talkt	Brad Rudisail	
WDAGUtilityAccount		A user account managed and used by the system for Windows Defender Application Guard scenarios.

Office Worker 2

Full name: Pedro Williams

Description: Example User

☐ User must change password at next logon
☐ User cannot change password
☐ Password never expires
☑ Account is disabled
☐ Account is locked out

Figure 33 Screenshot showing the account Properties window in Computer Management. The "Account is disabled" checkbox is highlighted, illustrating how to disable or enable a local account.

Local accounts created by administrators can be **deleted** when they are no longer needed. For Microsoft cloud accounts, you cannot delete them from the device itself, but you can remove them from the sign-in options to prevent local access. This ensures that users who no longer require access cannot log in.

When a user needs administrative privileges, you can **promote** them by changing their account type or adding them to the Administrators group. This should be done carefully because administrator accounts have full control over the system. For example, only IT staff or trusted technical personnel should be members of the Administrators group, while students, children, or temporary visitors should remain standard users to prevent accidental system changes or security breaches.

Additional Tip: After promoting a user, consider temporarily auditing their activity and reminding them of safe usage practices, especially when handling sensitive files or installing software.

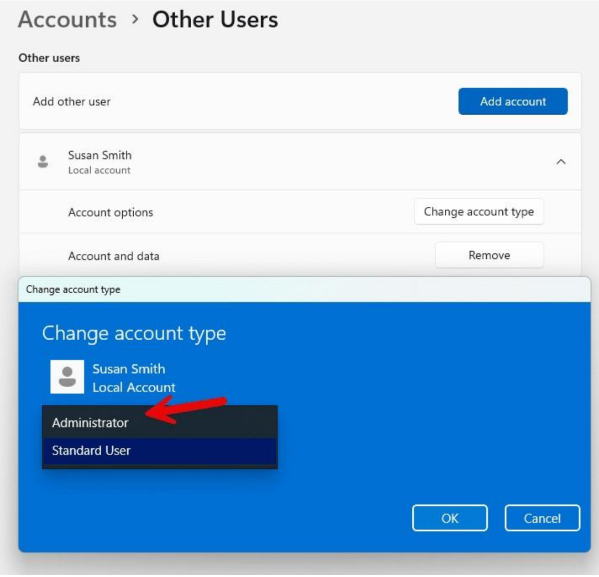
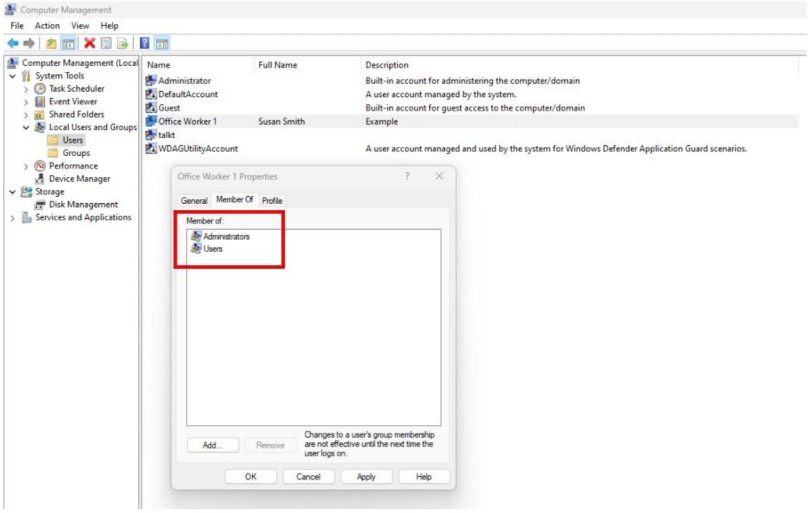


Figure 34 Screenshot of the Settings App, illustrating the process to change a user account type from Standard to Administrator.



Name	Full Name	Description
Administrator		Built-in account for administering the computer/domain
DefaultAccount		A user account managed by the system.
Guest		Built-in account for guest access to the computer/domain
Office Worker 1	Susan Smith	Example
talkt		
WDAGUtilityAccount		A user account managed and used by the system for Windows Defender Application Guard scenarios.

Changes to a user's group membership are not effective until the next time the user logs on.

Figure 35 Screenshot of the Computer Management Console showing a user added to the local Administrators group, demonstrating how to grant administrative privileges safely.

5. Additional Recommendations

In addition to basic security measures, there are several additional recommendations that help improve the security of the user's Windows system and protect their device from common threats.

These recommendations are easy to implement and accessible for non-technical users**.**

1.Enabling the Windows Firewall

It is recommended to keep the Windows Firewall on at all times, since it acts as a filter protecting you from any harm. It monitors the arriving and leaving data and blocks any unauthorized connections. The firewall helps reduce the risk of network attacks and hacking attempts. Users can ensure the firewall is enabled through Windows Security settings.

Settings → Privacy & Security → Windows Security → Firewall & Network Protection

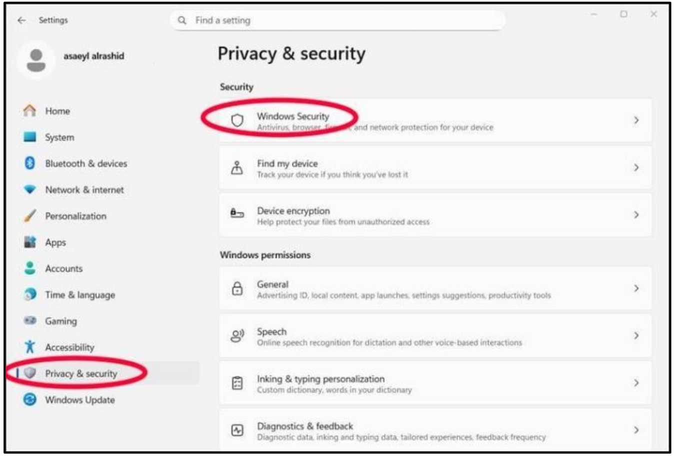

Settings
Find a setting
asaeyl alrashid
Home
System
Bluetooth & devices
Network & internet
Personalization
Apps
Accounts
Time & language
Gaming
Accessibility
Privacy & security
Windows Update
Privacy & security
Security
Windows Security
Antivirus, browser, firewall, and network protection for your device
Find my device
Track your device if you think you've lost it
Device encryption
Help protect your files from unauthorized access
Windows permissions
General
Advertising ID, local content, app launches, settings suggestions, productivity tools
Speech
Online speech recognition for dictation and other voice-based interactions
Inking & typing personalization
Custom dictionary, words in your dictionary
Diagnostics & feedback
Diagnostic data, inking and typing data, tailored experiences, feedback frequency

Figure 36 Accessing Windows security

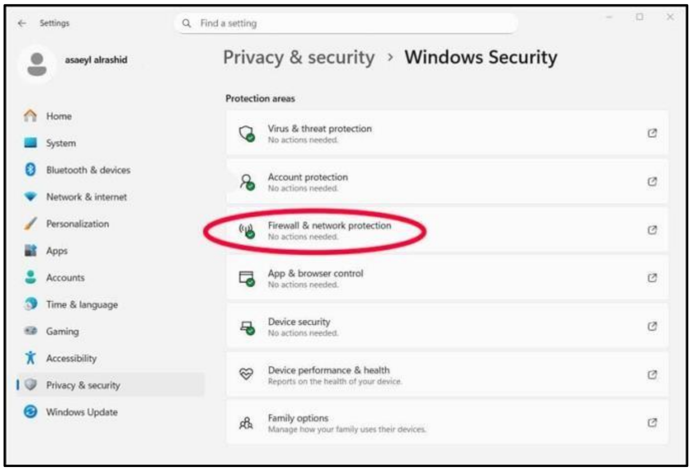


Figure 37 Ensuring firewall is active

In addition to the built-in Windows Firewall, users can use other **optional** security software, such as Norton Antivirus. https://www.norton.com Norton provides extra layers of protection, including:

- an advanced firewall,
- malware protection,
- alerting for hacking attempts
- alerting for unsafe websites.

Using a reliable program like Norton may be suitable for users who require a higher level of protection, while ensuring that any conflicting programs are disabled to avoid performance issues.

2.Enabling and Using Windows Defender Antivirus

Windows Defender is the built-in (embedded in the system) security program for Windows, providing immediate protection against viruses, malware, and ransomware (it is a virus that steals your files and wants a ransom from you to give it back to you). It runs automatically and is continually updated without user involvement. Keeping Windows Defender enabled helps detect threats early and protects your system and data from damage or theft.

You can check if Windows Defender is enabled by going to:

Settings → Privacy & Security → Windows Security → Virus & Threat Protection, where the Real-time Protection option will appear as enabled.

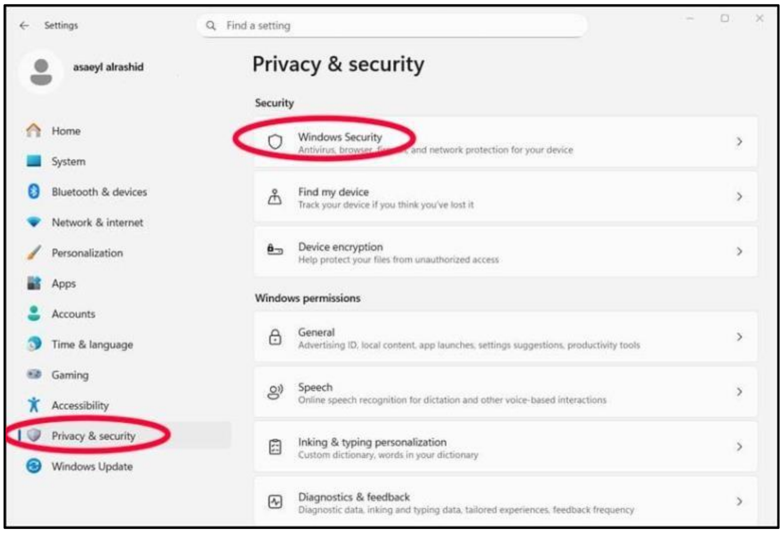
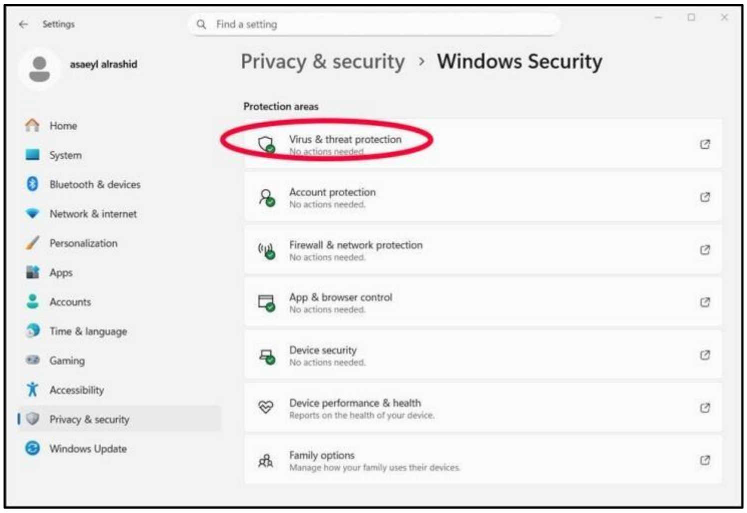

Settings
Find a setting
asaeyl alrashid
Home
System
Bluetooth & devices
Network & internet
Personalization
Apps
Accounts
Time & language
Gaming
Accessibility
Privacy & security
Windows Update
Privacy & security
Security
Windows Security
Antivirus, browser, fi , and network protection for your device
Find my device
Track your device if you think you've lost it
Device encryption
Help protect your files from unauthorized access
Windows permissions
General
Advertising ID, local content, app launches, settings suggestions, productivity tools
Speech
Online speech recognition for dictation and other voice-based interactions
Inking & typing personalization
Custom dictionary, words in your dictionary
Diagnostics & feedback
Diagnostic data, inking and typing data, tailored experiences, feedback frequency

Figure 38 Accessing Windows security



Privacy & security > Windows Security

Protection areas

Virus & threat protection
No actions needed.

Account protection
No actions needed.

Firewall & network protection
No actions needed.

App & browser control
No actions needed.

Device security
No actions needed.

Device performance & health
Reports on the health of your device.

Family options
Manage how your family uses their devices.

Figure 39 Windows virus and threat protection

How do I know it's enabled?

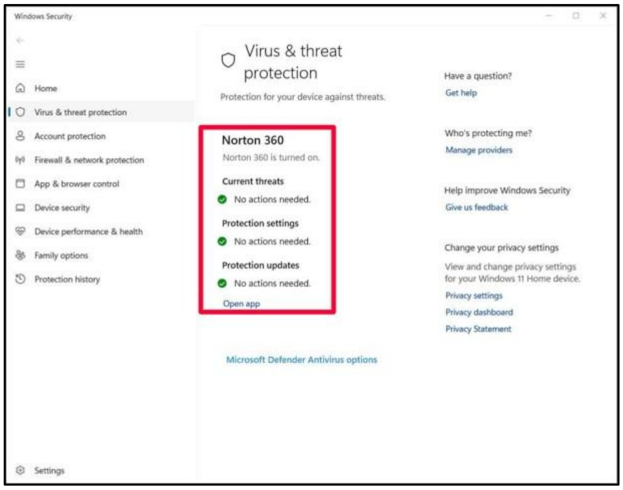
If you see Real-time protection: On

This means Windows Defender is running and enabled. You'll see on the page that your device is Protected.

If it's not enabled:

- Click on Manage settings
- Turn on the Real-time protection option.

If you see a message that another antivirus program is running (like Norton), this is normal because Windows automatically disables Defender to avoid conflicts.



Virus & threat protection

Protection for your device against threats.

Norton 360
Norton 360 is turned on.

Current threats
No actions needed.

Protection settings
No actions needed.

Protection updates
No actions needed.

Open app

Microsoft Defender Antivirus options

Have a question?
Get help

Who's protecting me?
Manage providers

Help improve Windows Security
Give us feedback

Change your privacy settings
View and change privacy settings for your Windows 11 Home device.
Privacy settings
Privacy dashboard
Privacy Statement

Figure 40 Activated antivirus

3.Enabling Automatic Screen Lock

It's recommended to set your device to automatically to lock the screen after a short period of inactivity (the time that you are not working on the device). This prevents unauthorized access if the device is left and not under watch. Setting a password or PIN to unlock the device again helps upgrade account security and protects your personal information.

This setting can be set from: **Settings → Accounts → Sign-in Options**

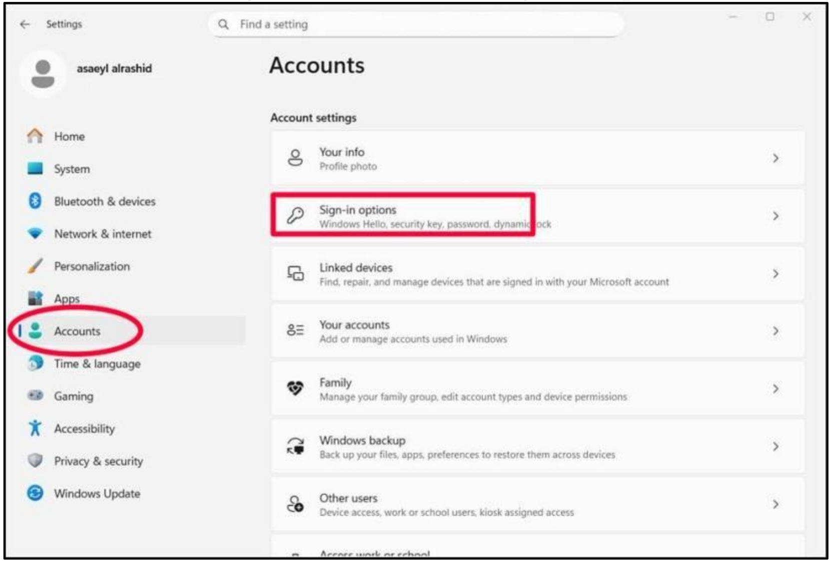
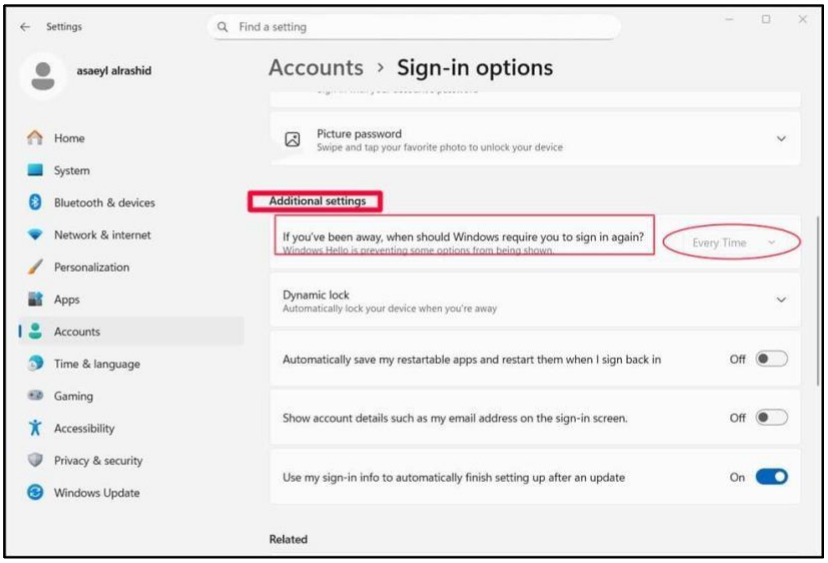

Settings
Find a setting
asaeyl alrashid
Home
System
Bluetooth & devices
Network & internet
Personalization
Apps
Accounts
Time & language
Gaming
Accessibility
Privacy & security
Windows Update
Accounts
Account settings
Your info
Profile photo
Sign-in options
Windows Hello, security key, password, dynamic lock
Linked devices
Find, repair, and manage devices that are signed in with your Microsoft account
Your accounts
Add or manage accounts used in Windows
Family
Manage your family group, edit account types and device permissions
Windows backup
Back up your files, apps, preferences to restore them across devices
Other users
Device access, work or school users, kiosk assigned access
Access work or school

Figure 41 Accessing sign in options



If you've been away, when should Windows require you to sign in again? Every Time
Windows Hello is preventing some options from being shown.

Dynamic lock
Automatically lock your device when you're away

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

Show account details such as my email address on the sign-in screen. Off

Use my sign-in info to automatically finish setting up after an update On

Figure 42 Adjusting sign in settings

Conclusion:

This guide showed simple steps that beginners use in order to secure their Windows computer by starting with a safe installation, setting proper user accounts and passwords, turning off unnecessary services, keeping the system updated, and creating managed user accounts. The device becomes a much safer place. Also, adding protections like firewalls, antiviruses, and automatic screen lock improves security as well.

References:

[1] Microsoft Corporation, “Download Windows 11,” Microsoft, 2024. [Online]. Available: https://www.microsoft.com/en-au/software-download/windows11

[2] Microsoft Support, “Install Windows 11,” Microsoft, 2024. [Online]. Available: https://support.microsoft.com/en-us/windows/install-windows-11

[3] Microsoft Security Compliance, “Windows 11 Security Baseline,” Microsoft Learn, 2024. [Online]. Available: https://learn.microsoft.com/en-us/windows/security/threatprotection/windows-security-baselines

[4] Microsoft Learn, “Security Best Practices for Windows,” Microsoft, 2024. [Online]. Available: https://learn.microsoft.com/en-us/windows/security/

[5] Microsoft, “Windows Firewall documentation,” Microsoft Support, n.d. [Online]. Available: https://support.microsoft.com/en-us/windows/windows-firewall-help

[6] Microsoft, “Microsoft Defender Antivirus overview,” Microsoft Support, n.d. [Online]. Available: https://support.microsoft.com/en-us/windows/microsoft-defender-overview

[7] Microsoft, “Manage Windows sign-in options,” Microsoft Support, n.d. [Online]. Available: https://support.microsoft.com/en-us/windows/manage-sign-in-options

[8] NortonLifeLock, “Norton Antivirus official website,” n.d. [Online]. Available: https://www.norton.com

[9] Center for Internet Security, “CIS Benchmarks,” n.d. [Online]. Available: https://www.cisecurity.org/cis-benchmarks