

Privacy & Security Windows 11

If you are looking for Windows 10 instructions, you can find these [here \(https://www.ebas.ch/en/data-protection-under-windows-10/\)](https://www.ebas.ch/en/data-protection-under-windows-10/).

Windows 11 analyses various personal data. Data affected here are for instance your e-mail address and contents of e-mails received and sent out, personal interests and favourites, purchase and payment data, your personal address book, etc.

Many of these data are also transmitted to Microsoft. Most of these data transmission mechanisms however can be switched off. On the one hand, you should consider certain criteria when first installing Windows 11; on the other, various settings can still be adjusted afterwards. Our instructions are meant to assist you with selecting the correct settings and to protect your data and all your private information in the best possible way.

We have tried to draw up as universally applicable a set of instructions for private users as possible. Nevertheless, the individual configuration options and settings may differ in specific cases. These instructions refer to the options available as at **22nd March 2024**.

Settings during Windows 11 installation

During any Windows 11 installation, you can already make some decisions regarding data protection. You will be asked how extensive you would like the amount of diagnostic data sent back to Microsoft to be. At this point, you can only choose between «Send optional diagnostic data» and «Send required diagnostic data». To avoid Windows sending too many data to Microsoft unintentionally, please select «Send required diagnostic data».

After installation, you can personalise certain settings. Wait until Windows has finished installing, and then change your settings.

Settings after Windows 11 installation

Should you already have installed Windows 11, you can subsequently adjust settings in Windows. You will find the relevant menu under **Start (Windows logo) > Settings (cog) > Privacy & Security**.

Security

Windows Security

Select “Open Windows Security” to access settings.

Virus & threat protection

This is where you can scan your device for viruses and threats under “Current Threats” using the “Quick Scan” option. In addition, you can create settings for your virus and threat protection. Windows Defender will show each time whether you are sufficiently protected by the settings chosen. This is then marked “No actions needed”. If you have antivirus software installed on your device, this is shown here, too. Instead of your settings, this will then link to “current threats”, “virus and threat protection settings”, “virus and threat protection updates” and “ransomware protection”.

Account protection

Microsoft account

You can use a Microsoft account to log into several Microsoft services. Amongst other things, this includes the on-line Office 365 software, the OneDrive cloud service, Teams and phone service and the Xbox Live games platform.

The advantage offered by a Microsoft account is that you are able to log into all Microsoft services using just a single e-mail address and password. You therefore don't have to set up and remember several different user names and passwords. In addition, a Microsoft account facilitates the use of multiple Windows devices: Your activity history, cache, OneDrive plus various settings such as Wi-Fi connections are automatically synchronised on all devices on which you log into your Microsoft account.

The drawback of a Microsoft account is data protection issues. You should be aware that Microsoft also collects data via your account: Locations, calendar entries, search queries, your browser history etc. These data are then for instance used to display suitable, personalised advertisements to you. If you don't want this, it is better to use a local account.

Dynamic lock

Your dynamic lock can be used to automatically have your device locked when away. To do so, you will have to connect your device with a mobile. We recommend setting this as per your requirements.

Firewall & network protection

This shows who and what is accessing your network. You can use Windows Defender to activate your firewall here. If you have antivirus software installed, Windows Defender will leave this task to the antivirus software instead. If you use Windows Defender, it will check whether your chosen settings will sufficiently protect you in its estimation. This is then marked "No actions needed".

App & browser control

Smart App Control

This is where you can set protection and control of your apps. By activating this control, malicious or non-trustworthy apps are detected and blocked to protect your device.

Reputation-based protection

| Option | Our recommendation |
|--|--------------------|
| Check apps and files | On |
| SmartScreen for Microsoft Edge | On |
| Phishing protection | On |
| - Warn me about malicious apps and sites | On |
| - Warn me about password reuse | Tick |
| - Warn me about unsafe password storage | Tick |
| Potentially unwanted app blocking | Tick |
| - Block apps | Tick |

| | |
|--------------------------------------|------|
| - Block downloads | Tick |
| SmartScreen for Microsoft Store apps | On |

Isolated browsing

Depending on your requirements, you can install Microsoft Defender Application Guard here. This will open your Microsoft Edge browser in an isolated browser environment to better protect your device and data against malware.

Exploit protection

Depending on your requirements, you can activate further Exploit protection settings. Windows provides your device with protection settings for regular users as standard.

Device security

Core isolation

| Option | Our recommendation |
|---------------------------------------|--------------------|
| Memory integrity | On |
| Memory access protection | On |
| Microsoft Vulnerable Driver Blocklist | On |

The symbols next to the title show a green, orange or red dot indicating whether everything is in good order.

Security processor

Your security processor, called the trust platform module (TPM), is providing additional encryption for your device.

Secure boot

Secure boot is on, preventing malicious software from loading when your device starts up.

Data encryption

We recommend activating data encryption.

Device performance & health

This is where you find the integrity report status of your device with regard to storage capacity, battery life, apps and software plus the Windows time service.

Family options

Depending on your requirements, you can activate your family settings here. To do so, you are directed to the “Microsoft Family Safety” home page.

Protection history

This is where you find all actions performed recently.

Find my device

We recommend deactivating device search.

Device encryption

We recommend activating device encryption.

For developers

| Option | Our recommendation |
|----------------|--------------------|
| Developer Mode | Off |

| | |
|------------------|-----|
| Device Portal | Off |
| Device discovery | Off |
| File Explorer | Off |
| Remote Desktop | Off |

Windows permissions

General

To protect your device against definite identification based on an advertising ID allocated by Windows, switch the first option “off”.

You should leave the second option “on”. This way, you ensure that websites are displayed in the language set as the Windows system language where possible.

The third option serves for local improvement of Windows and be left switched “on”. Windows can launch apps in frequent use by you more quickly this way.

| Option | Our recommendation |
|--|--------------------|
| Let apps show me personalized ads by using my advertising ID | Off |
| Allow websites to provide locally relevant content by accessing my language list | On |
| Let Windows improve start and search results by tracking app launches | On |
| Show me suggested content in the Settings app | Off |

Speech

Windows and the Cortana voice assistant can analyse your voice and improve personal recommendations that way. Since this allows Windows 11 to spy on your calendar, contact data and similar, you should switch this option off.

| Option | Our recommendation |
|---------------------------|--------------------|
| Online speech recognition | Off |

Inking & typing personalisation

Windows and the Cortana voice assistant can analyse your handwriting and improve personal recommendations that way. Since this allows Windows 11 to spy on your calendar, contact data and similar, you should switch this option off.

| Option | Our recommendation |
|---------------------------------------|--------------------|
| Personal inking and typing dictionary | Off |

Diagnostics & feedback

You cannot completely stop Microsoft from collecting any data. You can choose whether you would like to transmit few or plenty of data. To transmit as few data as possible, please select: «Required diagnostic data».

| Option | Our recommendation |
|-------------------------------|--------------------------------|
| Diagnostic data | Sending required data |
| Send optional diagnostic data | Off |
| Improve inking and typing | Off |
| Tailored experiences | Off |
| View diagnostic data | Depending on your requirements |
| Delete diagnostic data | Depending on your requirements |
| Feedback frequency | Never |

Activity history

Windows analyses which applications you have been working with, and offers a history of your activities.

If you use a Microsoft account and have cloud synchronisation activated, this will allow you to access the same timeline on several devices. If you don't want this, you should switch it off.

| Option | Our recommendation |
|--|--------------------------------|
| Store my activity history on this device | Off |
| Send my activity history to Microsoft | Off |
| Clear activity history | Depending on your requirements |

Search permissions

The SafeSearch function can limit inappropriate contents. Depending on your requirements, you can set this individually (strict, moderate or off). In the "Search permissions" settings, you can also define whether Cloud contents (OneDrive, SharePoint, Outlook data, etc.) should be taken into account for personalised search results. To optimise web search results, Windows Search can also save search histories on your device.

| Option | Our recommendation |
|-------------------------------|--------------------------------|
| SafeSearch | Depending on your requirements |
| Cloud content search | Off |
| Search history on this device | On |

Searching Windows

| Option | Our recommendation |
|--------------------------------------|--------------------------------|
| Respect power settings when indexing | On |
| Find my files | Classic |
| Exclude folders from enhanced search | Depending on your requirements |

App permissions

Location

Location is used by your device to send the location where you are using it to Microsoft. Location detection should be switched off.

If location tracking is active, organizations other than Microsoft can establish your location, too – in particular if you allow apps to access your location.

Scroll down a little bit, and by clicking on the «Delete» button any location data potentially submitted so far already can be removed from your device. Whether Microsoft will also then delete them, is not clear.

Should you have location services activated anyway, you can enable or disable location detection for each of your installed apps individually as needed. Your location data will then potentially be passed on to the provider of all relevant apps you activate this for.

Should you have location services activated anyway, you can enable or disable location detection for each of your installed apps individually as needed. Your location data will then potentially be passed on to the provider of all relevant apps you activate this for.

| Option | Our recommendation |
|--------------------------|--------------------------------|
| Location services | Off |
| Default location | Depending on your requirements |
| Location history | Depending on your requirements |
| Allow location overrider | Off |

Camera

Here you can stop every app automatically given access to your camera. Switch this option off.

Should you have a camera and would like to allow access to individual apps, you should do this for each app and enable or disable access for each one individually.

| Option | Our recommendation |
|---------------|--------------------|
| Camera access | Off |

Microphone

Here you can stop every app automatically given access to your microphone Switch this option off.

Should you have a microphone and would like to allow access to individual apps, you should do this for each app and enable or disable access for each one individually.

| Option | Our recommendation |
|-------------------|--------------------|
| Microphone access | Off |

Voice activation

You can only change this setting if you have allowed access to a microphone above. If this is the case, you can determine whether certain apps are opened and are allowed to record your spoken words.

If you don't want to control your device by your voice, you should switch everything off here.

| Option | Our recommendation |
|---|--------------------|
| Let apps access voice activation services | Off |

Notifications

You can basically enable or disable access to your notifications for all apps generally. If you don't want to generally stop all access, you can enable or disable access for each app individually. Access should only be granted to trustworthy apps.

| Option | Our recommendation |
|---------------------|--------------------------------|
| Notification access | Depending on your requirements |

Account info

Since this access is primarily required for personalised advertising, it is recommended to switch this option off.

| Option | Our recommendation |
|---------------------|--------------------|
| Account info access | Off |

Contacts

You can basically enable or disable access to your contacts for all apps generally. If you don't want to generally stop all access, you can enable or disable access for each app individually. Access should only be granted to trustworthy apps.

| Option | Our recommendation |
|-----------------|--------------------------------|
| Contacts access | Depending on your requirements |

Calendar

You can basically enable or disable access to your calendar for all apps generally. If you don't want to generally stop all access, you can enable or disable access for each app individually. Access should only be granted to trustworthy apps.

| Option | Our recommendation |
|-----------------|--------------------------------|
| Calendar access | Depending on your requirements |

Phone calls

You can basically allow all apps access to your telephone calls or stop them from accessing them. In case you don't want to prohibit access in general, you can allow or prohibit access for every individual app. You should only allow trustworthy apps such access.

| Option | Our recommendation |
|-------------------|--------------------------------|
| Phone call access | Depending on your requirements |

Call history

You can basically enable or disable access to your call history for all apps generally. If you don't want to generally stop all access, you can enable or disable access to every app individually. Access should only be granted to trustworthy apps.

| Option | Our recommendation |
|---------------------|--------------------------------|
| Call history access | Depending on your requirements |

Email

You can basically enable or disable access to your e-mail by all apps generally. If you don't want to generally stop all access, you can enable or disable access to every app individually. Access should only be granted to trustworthy apps.

| Option | Our recommendation |
|--------------|--------------------------------|
| Email access | Depending on your requirements |

Tasks

You can basically enable or disable access to your tasks by all apps generally. If you don't want to generally stop all access, you can enable or disable access to every app individually. Access should only be granted to trustworthy apps.

| Option | Our recommendation |
|--------------|--------------------------------|
| Tasks access | Depending on your requirements |

Messaging

You can basically enable or disable access by all apps to your messages (SMS or MMS) generally. If you don't want to generally stop all access, you can enable or disable access to every app individually. Access should only be granted to trustworthy apps.

| Option | Our recommendation |
|------------------|--------------------------------|
| Messaging access | Depending on your requirements |

Radios

You can basically enable or disable access to your radio controls (Bluetooth, etc.) by all apps generally. If you don't want to generally stop all access, you can enable or disable access to every app individually. Access should only be granted to trustworthy apps.

| Option | Our recommendation |
|----------------------|--------------------------------|
| Radio control access | Depending on your requirements |

Other devices

An automatic exchange of information, for instance inside a public Wi-Fi network, poses a serious security risk. You should therefore switch this option off.

Please note however that contactless payments using a smartphone (under Windows 11 mobile) are no longer possible this way.

| Option | Our recommendation |
|-----------------------------------|--------------------|
| Communicate with unpaired devices | Off |

App diagnostics

As per their default settings, apps also transmit many diagnostic data to Microsoft. It is recommended to switch this option «off».

| Option | Our recommendation |
|-----------------------|--------------------|
| App diagnostic access | Off |

Automatic file downloads

Has been deactivated as per your settings above.

Documents

You can enable or disable access to your document libraries by all apps overall. If you don't want to generally stop all access, you can enable or disable access by every app individually. Access should only be granted to trustworthy apps.

| Option | Our recommendation |
|--------------------------|--------------------------------|
| Documents library access | Depending on your requirements |

Downloads folder

You can enable or disable access to your «Downloads» folder by all apps overall. If you don't want to generally stop all access, you can enable or disable access by every app individually. Access should only be granted to trustworthy apps.

| Option | Our recommendation |
|-------------------------|--------------------------------|
| Downloads folder access | Depending on your requirements |

Music library

You can enable or disable access to your music library by all apps overall. If you don't want to generally stop all access, you can enable or disable access by every app individually. Access should only be granted to trustworthy apps.

| Option | Our recommendation |
|--|--------------------------------|
| Allow access to music libraries on this device | Depending on your requirements |

Pictures

You can enable or disable access to your picture libraries by all apps overall. If you don't want to generally stop all access, you can enable or disable access by every app individually. Access should only be granted to trustworthy apps.

| Option | Our recommendation |
|-------------------------|--------------------------------|
| Pictures library access | Depending on your requirements |

Videos

You can enable or disable access to your video libraries by all apps overall. If you don't want to generally stop all access, you can enable or disable access by every app individually. Access should only be granted to trustworthy apps.

| Option | Our recommendation |
|-----------------------|--------------------------------|
| Videos library access | Depending on your requirements |

File system

You can enable or disable access to all your files, including your documents, images, videos and local OneDrive files, overall. If you don't want to generally stop all access, you can enable or disable access by every app individually. Access should only be granted to trustworthy apps.

| Option | Our recommendation |
|--------------------|--------------------------------|
| File system access | Depending on your requirements |

Screenshot borders

You can enable or disable access to an apps' screenshot borders permission function by all apps overall. If you don't want to generally stop all access, you can enable or disable access by every app individually.

| Option | Our recommendation |
|-----------------------------------|--------------------------------|
| Screenshot border settings access | Depending on your requirements |

Screenshots and apps

You can enable or disable access to an app's screenshot permission function by all apps overall. If you don't want to generally stop all access, you can enable or disable access by every app individually. Access should only be granted to trustworthy apps.

| Option | Our recommendation |
|--------------------|--------------------------------|
| Screenshots access | Depending on your requirements |