

The Ultimate Windows 10 **Security Guide**

Windows 10 was launched in July 2015 in a context infused with talks about security and privacy. As online safety became a priority for an important group of users (often key opinion leaders), Microsoft turned this into a selling point. Windows 10 was boldly described as "the most secure Windows ever."



But is it really so?

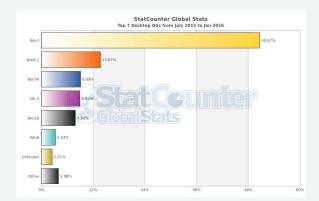
With Windows 10, Microsoft changed their outlook on how the OS was built and how it would be updated. The company decided that the new OS would be an "operating system-as- a-service," which means it will get ongoing updates, both feature and security-related.

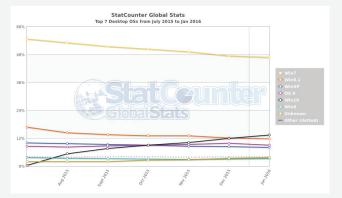
"Today, we're sharing more on security in Windows 10. Windows 10 has more built-in security protections to help safeguard you against viruses, phishing, and malware, it's the most secure Windows ever. New features are now delivered through automatic updates, helping you to stay current and your system to feel fresh, so you're free to do."

Source: Security in Windows 10

While it got mostly positive reviews for new features, user interface, integrations and more, Windows 10 also generated some security and especially some privacy concerns.

If you're a Windows 10 user or plan to upgrade soon, you've come to the right place to find out what you need to do to achieve enhanced data protection.





Source: StatCounter OS statistics

This **Windows 10 security guide** is meant to help you understand what's new about this OS, how you can adjust your security and privacy settings for maximum protection available and which apps can increase e your safety.

If you're looking for a resource that has all the advice and details you need, then this guide is it!

What's new in Windows 10 Security

Microsoft played the security card strong with Windows 10. It was even transformed into a selling point and an incentive to motivate Windows users to upgrade. Consequently, they added a lot of new features that would help make users safer online. Some of these features include:

$\langle \bullet \rangle$	Multi-factor authentication technology;
⊘	Support for biometric authentication through Windows Hello and Windows Passport (more on that below);
⊘	Device encryption with BitLocker and local storage for credentials;
⊘	Improved SmartScreen Filter to single out and block potentially malicious apps;
⊘	Faster security updates and patches;
⊘	Brute-force attack resistance;
⊘	Improved malware resistance;
\bigcirc	Enhanced Protected Mode included in both Microsoft Edge and IE to help protect users against malicious browser extensions;
⊘	A significantly enhanced Windows Defender;
⊘	Trusted Apps in Windows store;
\bigcirc	Reduced browser extension support in Microsoft Edge to reduce vulnerabilities and more

This may sound like a lot of information to take in at once, so let's get to it, step by step.

Don't worry, we won't get too technical. The point here is for everyone to be able to fine tune their Windows 10 settings to obtain a higher degree of online safety and privacy.



Windows 10 Security

1.	Accounts	10
2.	Update & security	21
	Windows Update	21
	Windows Defender	26
	Backup	34
	Recovery	38
	Find my Device	42
3.	BitLocker encryption	47
4.	Trusted apps	52
5.	SmartScreen Filter	56
6.	Microsoft Edge	61
7.	Cyber threats targeting Windows 10	64
0	December and advantage on the few Windows 10	0.0



Windows 10 Privacy

1.	Controversy	71
2.	Terms of service & Privacy policy	74
3.	Privacy settings	75
	General privacy settings	79
	Location privacy settings	81
	Camera privacy settings	83
	Microphone privacy settings	84
	Speech, inking and typing privacy settings	85
	Account info security settings	86
	Contacts privacy settings	88
	Calendar privacy settings	89
	Call history privacy settings	90
	Email privacy settings	91
	Messaging privacy settings	93
	Radios privacy settings	94
	Other devices privacy settings	95
	Feedback and diagnostics privacy settings	96
	Background apps privacy settings	99
4.	Cortana	100
5.	OneDrive	105
6.	Proxy settings	108
7.	VPN settings	111

Windows 10 Security

If you're new to Windows 10 or haven't had the chance to tweak your settings, these resources will help you find all the answers you need.

For every setting, we'll show you what it is, what's new about it, where to find it, how it works and we'll also include additional resources if you want to go in-depth.

Let's get to it, shall we?



What it is

When installing Windows 10, you'll be prompted to either log into your Microsoft account, if you have one, or you can choose to use a local account.

What's new

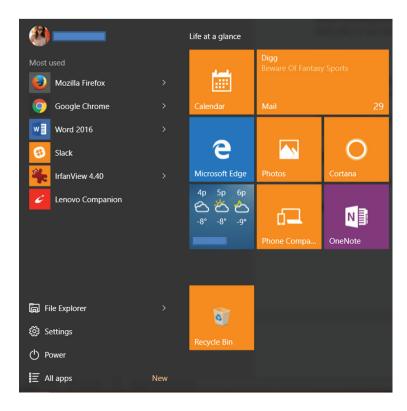
If you choose to use a Microsoft account, you'll be able to synchronize some of your settings between your devices (if you have multiple laptops, PCs or mobile with Windows Phone, but also for your other online accounts, such as Skype, Xbox, Hotmail, Outlook or Office 365).

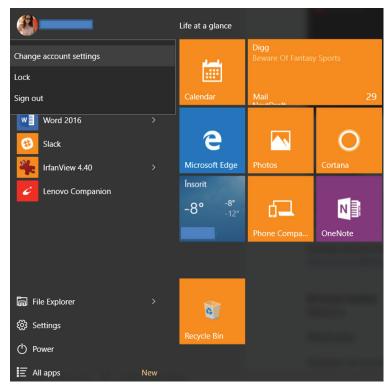
If you'd rather use a local account, you'll find that you're not as limited as you would've been on Windows 8 or 8.1. This is a good option if you only have one device you use Windows 10 on or if you want enhanced privacy.

Where to find it

Click on the Windows icon in the bottom-left corner. Go to the top of the window and click on the username (this can be either the local account or your Microsoft account).





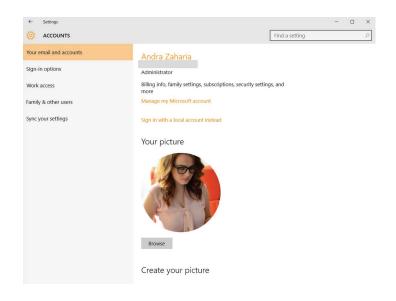


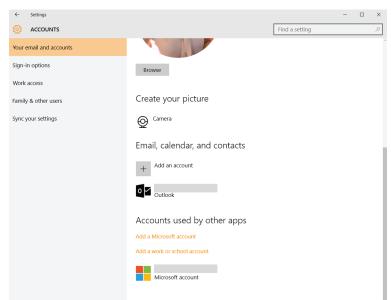


Here, you'll find 3 options:

- Change account settings
- Lock
- **Accounts**
- And Sign out.

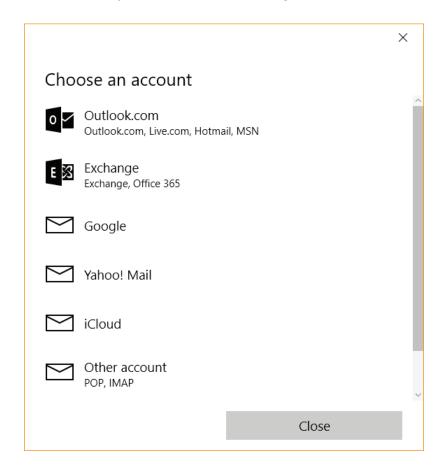
Click on Change account settings to adjust detailed settings such as:





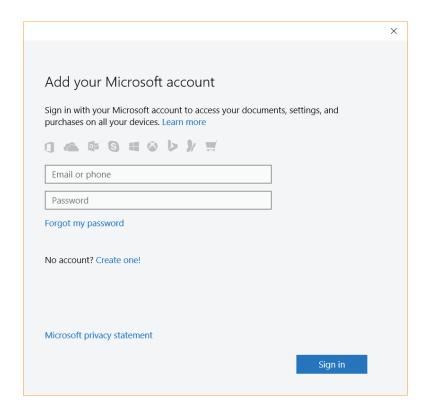


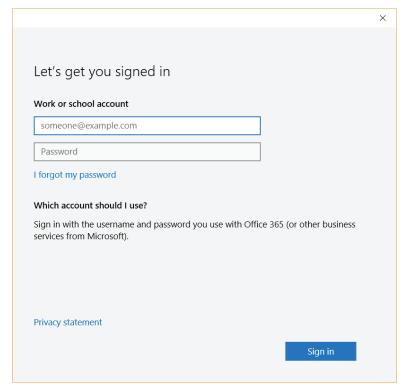
- Billing info, family settings, subscriptions, security settings and more for your Microsoft account (if you chose to log in with it) this setting will take you to
 - https://account.microsoft.com/about, where you can manage all these details;
- Sign in with a local account;
- Choose a picture for your account or create one using your computer's camera;
- Add other accounts to access email, calendar and contacts from; you have the following options:



 You can also add another Microsoft account or a work or school account to your device:









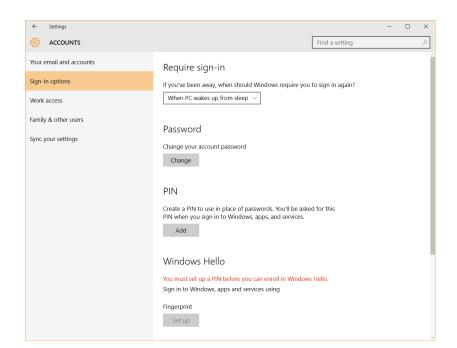
From here you can also customize your sign-in options here, such as:

- Pick when Windows 10 should require you to sign in again;
- Choose or change a password for your account;
- Set up a PIN to use instead of passwords;
- Set up Windows Hello to use biometric-based authentication, such as your fingerprint, instead of passwords;

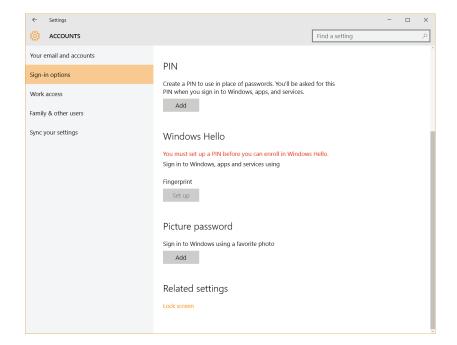
"Windows Hello helps address this challenge with a biometric alternative to passwords which provides enterprise-grade secure instant access to your Windows 10 devices* and Microsoft online services. Using just your finger print or even your face, Windows will greet you by name, providing a fast, secured, password-free way to log in."

Source: Security in Windows 10

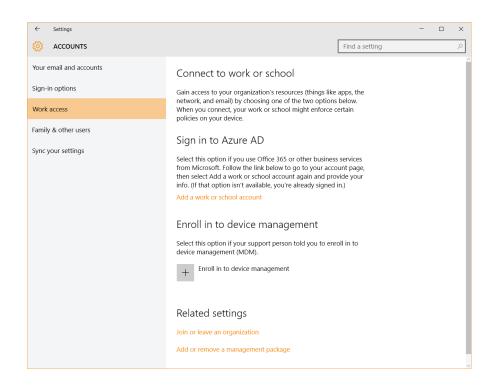
Set up a picture password.





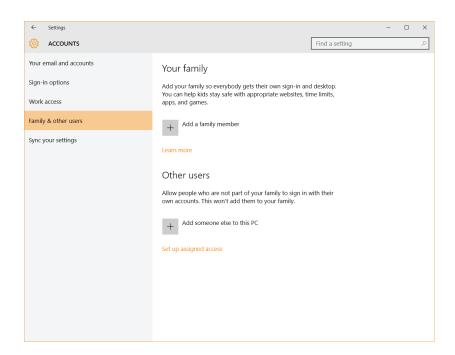


In the "Work access" section you'll be able to connect to your workplace or school account to get access to the data you have stored there.



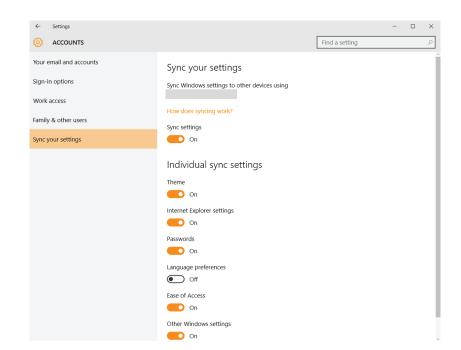


In the "Family & other users" section, you can set up dedicated accounts for your kids or other family members, with settings of their own. Here, you can also create guest accounts with limited access, to keep your system and data safe from intrusion.

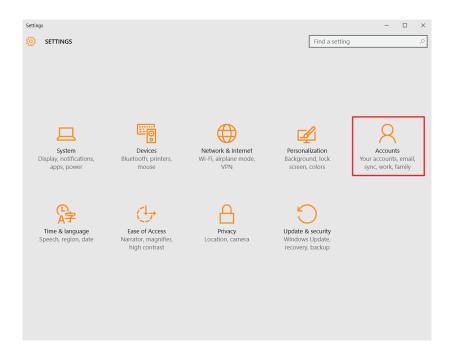


In the "Sync your settings" section, you'll be able to... sync your settings across devices (obviously). You can see, at a glance, what options you have and decide if and what data you want to make available on other devices you own that run Windows 10.





There's also another way to find the Account settings: **Start > Settings** > **Accounts.**





Available on

All Windows 10 versions.

Accounts

How it works

If you choose to use a Microsoft account, you'll be able to sync settings such as: theme preferences, Internet Explorer settings, passwords, language preferences, Ease of Access and other Windows settings across devices.

However, if **you chose to use a local account**, you won't be able to sync settings and preferences across devices. Also, you won't have the possibility to install applications from the Windows Store, because it requires a Microsoft account to do so.

Key takeaway

Set up an account that doesn't have administrator privileges to limit the damages that a potential malware infection can cause. Use a local account if you want to protect your privacy and send as little information to Microsoft as possible.

Settings, tips & tricks

No matter which option you choose, we recommend **setting a strong password** for your Microsoft account or for your local account. Also, if



your computer supports **biometric authentication via Microsoft Hello**, we highly recommend you start using it (today). **Picture passwords** are also a good way to enhance your security, so try out and see what works best for you.

For a more in-depth look at using user accounts on Windows 10, we recommend the following resources:

- Should you use a local or a Microsoft account in Windows 10?
- How to Set Up and Configure User Accounts on Windows 10
- How to manage Microsoft and user accounts in Windows 10



Update & security

This is your go-to section for security-related settings and more. Let's take a peek into what it can help you do.

Windows Update

What it is

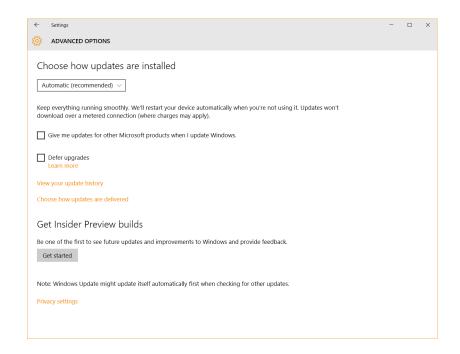
You probably already got it from the name that this is the place where you get your system updates. And it's also where you can choose how to receive and install these updates.

What's new

Windows 10 has been criticized for limiting how users can manage Windows updates. The biggest change is that **users can no longer selectively install updates**. You get them all at once and they can actually be installed automatically or you can choose to be notified to schedule a restart.



Windows Update



You can choose to defer upgrades, but you'll still get security updates automatically (and that's a very good thing):

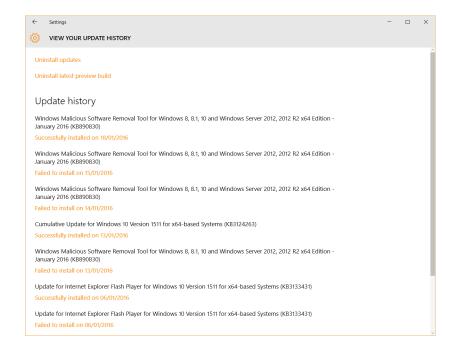
"Some Windows 10 editions let you defer upgrades to your PC. When you defer upgrades, new Windows features won't be downloaded or installed for several months. Deferring upgrades doesn't affect security updates. Note that deferring upgrades will prevent you from getting the latest Windows features as soon as they're available."

Source: Defer upgrades in Windows 10

You may not be able to selectively install updates, but you can still see your full update history in the dedicated section:



Windows Update



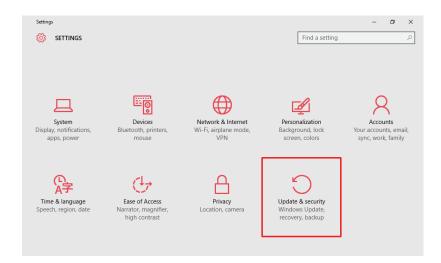
And if you're an early adopter or just plain curious, you can check the "Get Insider Preview Builds" to be part of the first few who get updates and improvements for the OS.

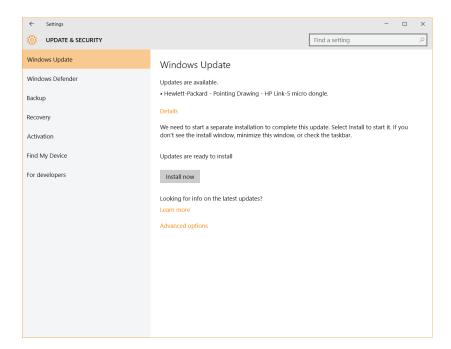
Where to find it

Follow this path to find it: Start > Settings > Update & Security > Windows Update. Clicking on Advanced options takes you to the aforementioned options.



Windows Update





Available on

All Windows 10 versions.

How it works

Well, in Windows 10, updates work by themselves. All you have to do



is sit back and choose when to install them or just let them follow their course and install automatically.

Windows Update

If you really, really want to keep updates from installing automatically, there's a workaround, but we don't recommend it. Keeping your system up to date is crucial to your data's security!

Key takeaway

Windows 10 will install operating system updates automatically, which is a great thing for your security. Keeping your OS and all your apps up to date is crucial for preventing malware infections and other cyber threats.

Settings, tips & tricks

If you want to read more about Windows Update in Windows 10, check out these useful links:

- What You Need to Know About Windows Update on Windows
- **How to Manage Windows Update in Windows 10**



What it is

Windows Defender is a software that attempts to detect and remove malware from your Windows-based computer. Microsoft released Windows Defender as an antispyware program initially, but improved it and made it embedded into the operating system starting with Vista.

What's new

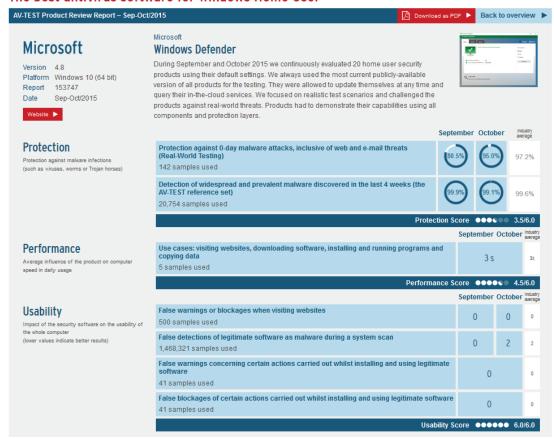
In Windows 10, Windows Defender comes with real-time antivirus capabilities. Another benefit is that it's simple enough to use that anyone can enjoy its benefits. The software runs in the background, scanning your files and offering a basic level of protection for all Windows 10 users.

In terms of protection, you can't expect it to perform the way a paid antivirus would. Here is a **snapshot of the analysis** that AV-TEST performed in October 2015. On Windows 10, Windows Defender scored:



- 3.5/6 in terms of protection effectiveness
- 4.5/6 when it comes to performance
- And 6/6 for usability.

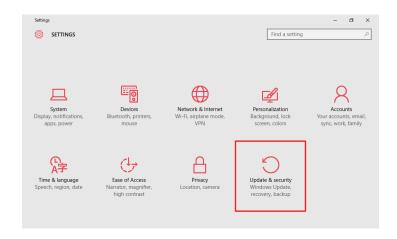
The best antivirus software for Windows Home User

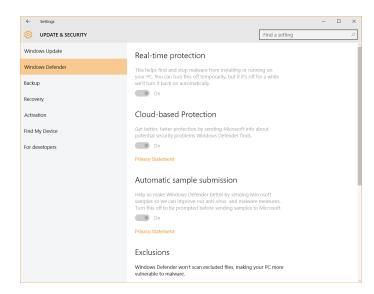


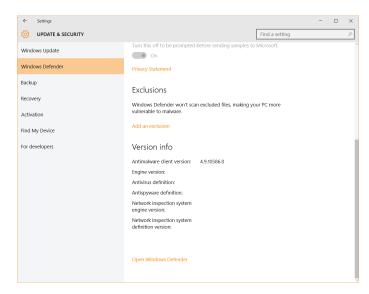
Where to find it

Get there by following this path: **Start > Settings > Update & Security** > **Windows Defender**. Here, you'll be able to tweak the settings to your liking.











Available on

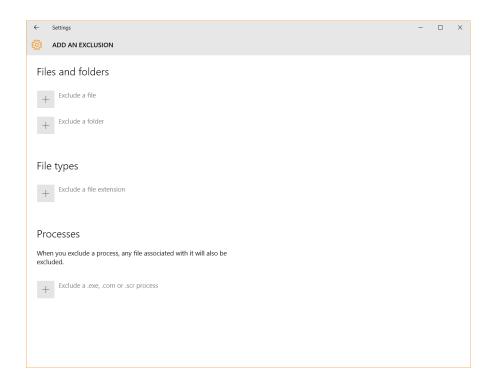
All Windows versions.

Windows Defender

How it works

Windows Defender offers a primary level of protection for your PC by finding and stopping malware from running on your PC. You can also choose to enable Cloud-based protection and Automatic sample submission to send Microsoft data about malware samples. This helps improve your protection and enhances Windows Defender for all users as well.

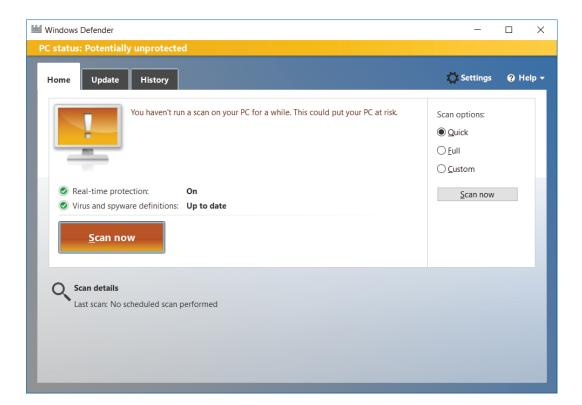
Should you want it, you can select to add exclusions in Windows Defender, but this will make your PC more vulnerable, as those files won't be scanned (obviously).





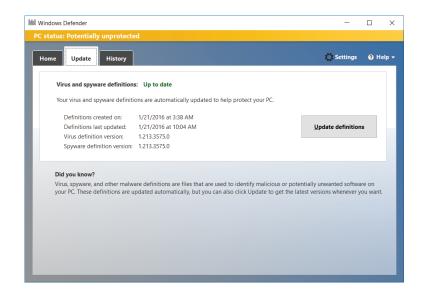
When you open Windows Defender, you'll see that you can perform three types of scans: Quick, Full and Custom. If you choose to use Windows Defender as your antivirus product, we recommend doing a Full scan as often as possible.

If Windows Defender finds any malware or suspicious files, it will clean it up and quarantine the files automatically. Should this happen, you'll get a "Malware detected" notification or a or "Detected threats are being cleaned" one.

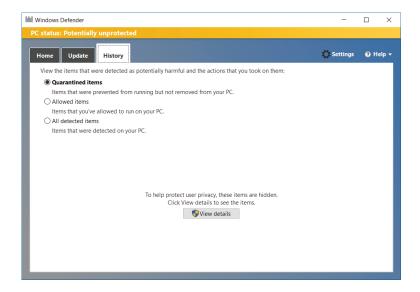


In Windows 10, Defender will get automatic updates, which are delivered automatically via Windows Update.





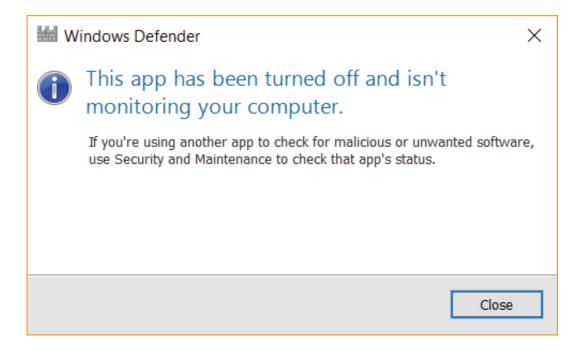
In the History tab in Windows Defender, you'll see a list of quarantined items, allowed items and all detected items on your PC, if you're one to be curious about such details.



If you choose to a different and more effective antivirus solution (highly recommended!), Windows 10 will automatically disable Windows Defender. That's because two antivirus solutions can't coexist on the same operating system.



All the options in Windows Defender will be grayed out and, when you try to open it, you'll get this message:



If you uninstall your antivirus of choice, Windows Defender will automatically turn back on and provide protection for your computer.

An important note is that **you can also use Windows Defender offline**:

"If Windows Defender finds a virus it can't remove, it will prompt you to download and run Windows Defender Offline.

Once your download is complete, your PC will automatically restart into the recovery environment, where Defender will run a more complete scan of your system and remove threats."

Source: Using Windows Defender Offline

Key takeaway



Use Windows Defender as a baseline antivirus to protect your system until you can find a more reliable antivirus solution. But please keep in mind that it can't ensure sufficient protection against advanced cyber threats, such as ransomware.

Settings, tips & tricks

The following articles offer more in-depth advice on how to use Windows 10 or how to manage it to better fit your protection needs:

- How to Use the Built-in Windows Defender Antivirus on Windows 10
- What's the Best Antivirus for Windows 10? (Is Windows **Der Good Enough?)**
- **Picking a Windows 10 Security Package**



What it is

One of our favorite subjects is the constantly disregarded backup. There is no such things as too many backups, so we strongly encourage you to use this feature and some other backup systems as well.

Windows Backup provides a simple way to create a copy of your data on a connected disk drive (external storage device), so you can make sure that your data is safe if something happens to your computer. That something could be a malware infection, theft or physical damage, so don't believe it can't happen to you.

What's new

On Windows 10, the Backup option is extremely easy to use. It also provides a way to start your own backup routine to help keep your data backed-up over time. It's something you'll definitely thank yourself for!

There are two types of backups you can perform:

 File History – useful if you want to back up your documents and other important files, and also the previous versions of



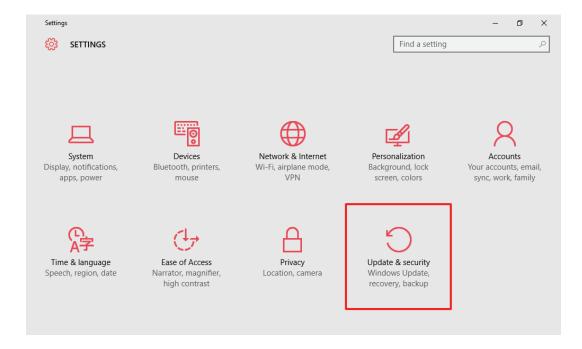
Backup

- those files. This way, you can recover older file versions if you need them
- System image backup this helps you create a full system image backup. You can perform a full system restore from this backup.

For more details on both these options, check out the recommended links at the end of this section.

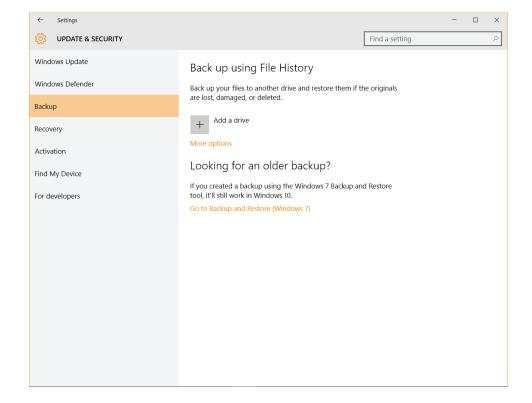
Where to find it

As always, the Start menu is the place you want to begin with. The Backup option is also included in the "Update & security" section in your Settings app on Windows 10.





Backup



Available on

All Windows 10 versions.

How it works

It's super easy to get started, so you really have no excuse for not doing it. Just select an external drive or a network location and then let the app do the work. According to Microsoft:

All set. Every hour, we'll back up everything in your user folder (C:\Us-ers\username). To change which files get backed up or how often back-ups happen, go to More options.

Source: Back up and restore your files



Backup

Key takeaway

Keeping at least one backup of your data is the best insurance you can get that your information will be available in case anything happens to your computer. It's recommended that you keep at least two back-ups of your data, one in the cloud and one on an external hard drive.

Settings, tips & tricks

This small collection of links if exactly what you need to get step-by-step advice on how to back-up your data on Windows 10:

- How to Use All of Windows 10's Backup and Recovery Tools
- How to create an image backup in Windows 10 and restore it, if need be
- **How to use Windows 10's File History backup feature**



What it is

You may find yourself in need to do a system recovery at some point. The cause could be one of the following, as presented by Microsoft:

Recovery options in Windows 10

If you're having problems with your PC, the following table can help you decide which recovery option to use. **Applies to Windows 10** Problem See this section Your PC isn't working well and you recently installed an app, Restore from a system restore point driver, or update. Your PC isn't working well and it's been a while since you Reset your PC installed an app, driver, or update. Your PC won't start and you've created a recovery drive. Use a recovery drive to restore or reset your PC Your PC won't start and you haven't created a recovery drive. Use installation media to restore or reset your PC Your PC won't start, you haven't created a recovery drive, and Use installation media to reinstall Windows 10 resetting your PC didn't work. You want to reinstall your previous operating system. Go back to your previous version of Windows

By using your backup from a restore point, you can revert back to it to fix your potential issue.

What's new

In Windows 10 you get three different recovery options which give you different ways to do a system restore, either a full or a partial one.



Moreover, in case you upgraded to Windows 10, you'll have a month to change your mind and go back to a previous version of Windows.

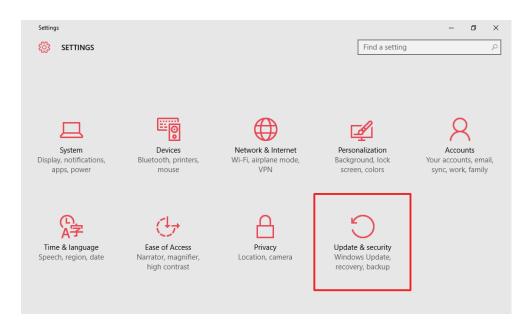
Recovery

This will keep your personal files, but it'll remove apps and drivers installed after the upgrade, as well as any changes you made to settings.

Source: How System Restore & Factory Reset Work in Windows 10

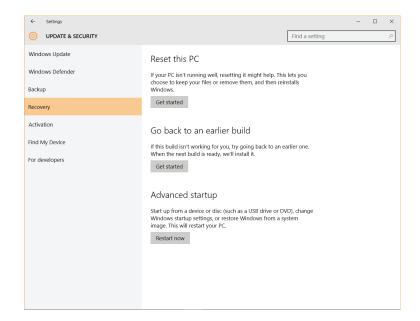
Where to find it

Go to Start > Settings > Update & Security > Recovery to start using any of the three options presented below.





Recovery



Available on

All Windows 10 versions.

How it works

In Windows 10, you have three options:

 Reset this PC – this option lets you keep your files or remove them, and then reinstalls Windows;





Recovery

- Go back to an earlier build if the Windows 10 build you have installed doesn't work for you, you can choose to go back to an earlier one:
- **Advanced startup** you can use a USB drive or a DVD to change the Windows startup settings, or restore Windows from a system image.

Key takeaway

Backing up your data is one of the best things you can do for yourself, but knowing how to recover your data from backups is half of this process. Using the Recovery option offered by Windows 10 will help you save time and effort.

Settings, tips & tricks

If you'd like to explore in detail each of the recovery options that Windows 10 features, these helpful resources will provide all the answers:

- **Recovery options in Windows 10**
- **How System Restore & Factory Reset Work in Windows 10**
- **How to Reset Your Windows 10 PC**



What it is

Losing a device or having it stolen is one of the most terrible things that can happen to your digital life. We all know we shouldn't get so deeply attached to our laptops, smartphones or tablets, but we can't help it. Our stuff is on them and we need that stuff, either for work or personal purposes.

So it's a great thing that the "Find My Device" option was introduced in Windows 10. It works just like it would on a smartphone, if you're familiar with it. You can use "Find my device" to find your laptop if you misplaced it or if it was stolen (which we hope never happens).

This is a free service we recommend you enable (if you're not worried about Microsoft getting your location data).

What's new

The option is entirely new and Microsoft periodically gets your device's location so you can see where your laptop is. And, from our experience, its ability to pinpoint the exact place is quite good.

If you're worried about privacy issues, here is an excerpt from the Windows 10 Privacy Statement:



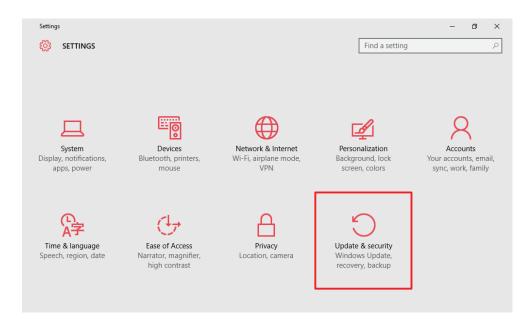
Find my device

"Examples of data we may collect include your name, email address, preferences and interests; location, browsing, search and file history; phone call and SMS data; device configuration and sensor data; voice, text and writing input; and application usage."

Source: Privacy Statement, Data We Collect

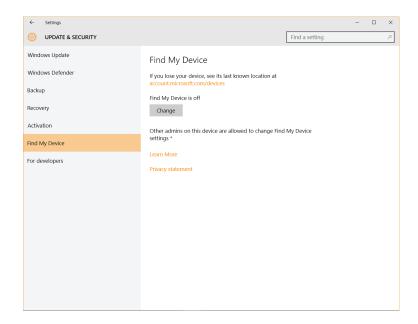
Where to find it

This is how to find the option on your device: Start > Settings > **Update & Security > Find My Device.**





Find my device



Available on

All Windows 10 versions.

How it works

First, in order to set up "Find My Device," you have to be logged into your Microsoft account and log in with administrator rights.

To change settings for Find My Device

Set up Find My Device to save your location every few hours so it's easier to locate your device. To change these settings, make sure you've already turned on the master location setting on your device and signed in on your device using your Microsoft account.

- Sign in to your device as an administrator. 1.
- On your device, go to Start, then select Settings > Update and Security > Find My Device.



Find my device

Turn the Find My Device setting on. 3.

> Save my device's location periodically

To find your device

- Go to account.microsoft.com/devices. If you're prompted to sign in, use the same Microsoft account you used to sign in on your device.
- Choose the device you want to find, and then click Find My Device. 2.
- 3. You'll see a map with your device's location.

Tips from Microsoft:

- Not seeing the latest location? Make sure you're signed in with the same Microsoft account as the administrator on your device.
- Your device only sends its location if it's connected to Wi-Fi and has enough battery power.

Source: Find a lost phone or device

Key takeaway

This feature can help you recover your lost or stolen computer, so it



may be tremendously helpful when you least expect it. You'll have to trade off a bit of your privacy to do so (location data), but, in return, you can end up recovering your device when you most need it.

Find my device

Settings, tips & tricks

Leverage the "Find my device" option to keep your Windows 10 gadgets safe and locate them asap. These links can help provide more details on how to connect to your account and trace your device's whereabouts:

- How to turn on Windows 10's Find My Device feature
- Find a lost phone or device



What it is

BitLocker is a full disk encryption feature integrated into Windows 10 that you can use to protect your data by encrypting it. Using BitLocker is easy, because it's built into the operating system, so there's no need to use additional software to encrypt and decrypt your data.

BitLocker was first introduced to Windows Vista users and had been present on every Windows version ever since.

According to Microsoft:

"BitLocker ensures that data stored on a computer running Windows Vista [in our case, Windows 10] remains encrypted even if the computer is tampered with when the operating system is not running. This helps protect against "offline attacks," attacks made by disabling or circumventing the installed operating system, or made by physically removing the hard drive to attack the data separately."

Source: Windows BitLocker Drive Encryption Step-by-Step Guide



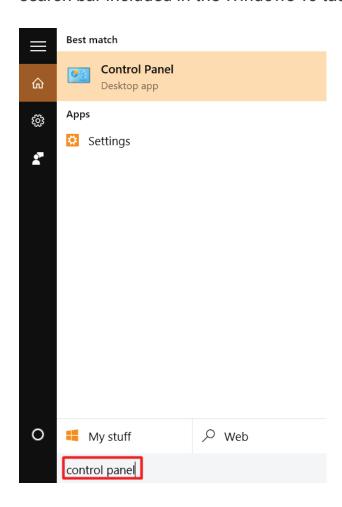
BitLocker encryption

What's new

Here's where it gets a bit technical, but bear with me. In Windows 10, BitLocker supports the XTS-AES encryption algorithm, which makes the encryption stronger. And there are also a few details that only apply to Windows 10 usage in companies, so, if you're interested, you can check out the details on the **Microsoft website**.

Where to find it

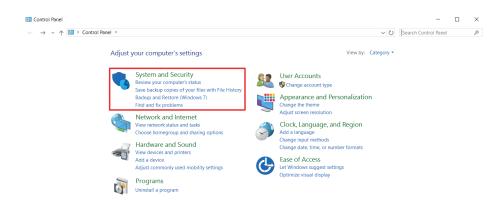
To find your encryption options, search for "control panel" in the search bar included in the Windows 10 taskbar.



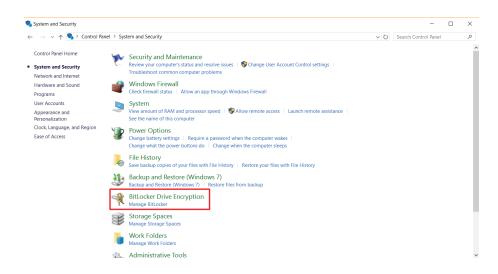


BitLocker encryption

Choose "System and Security":



And then go to BitLocker Drive Encryption:



Available on

BitLocker encryption is available on Windows 10 Pro and Windows 10 Enterprise.



How it works

As Microsoft says:

BitLocker encryption

"You can use BitLocker Drive Encryption to help protect your files on an entire drive. BitLocker can help block hackers from accessing the system files they rely on to discover your password, or from accessing your drive by physically removing it from your PC and installing it in a different one. You can still sign in to Windows and use your files as you normally would."

Source: BitLocker Drive Encryption

There are a few details you should go over before starting to encrypt your drive though, and we've collected them below.

Key takeaway

Encryption is an important safeguard for both your security and your privacy. Keeping your data encrypted will help you protect it against prying eyes and malware attacks of all kinds. It may take a bit to set up your system, but it will be easier to maintain afterwards.

Settings, tips & tricks

Ready to encrypt your hard drive and add an important layer of protection



BitLocker encryption

for your data?

The guides below will help you get set up and master BitLocker encryption like a pro:

- How to enable BitLocker encryption without a TPM chip in Windows
- How to Set Up BitLocker Encryption on Windows
- Windows BitLocker Drive Encryption Step-by-Step Guide



What it is

This is a new feature integrated into the Windows Store. **Long story short:** every application distributed through the Windows Store has to be signed by either Microsoft or by a trusted vendor. This helps reduce the number of dangerous applications that can harm your data's safety or privacy from being sold or distributed through the store.

What's new

The Windows store in its actual form is rather new (it first appeared in this form on Windows 8). So the app vetting process is also recent. You may rush to compare it to the system that Apple uses for its App Store, but Microsoft's approach is probably not as thorough as Apple's.

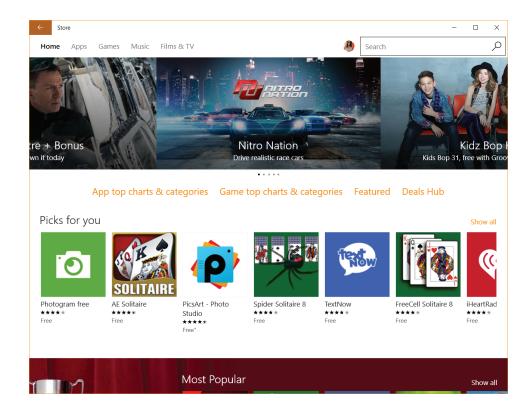
However, this is a security layer that's more than welcome and that hopefully Microsoft will continue to build on.

Where to find it

You can find the Windows Store by clicking on **Start > Store**.



Trusted apps

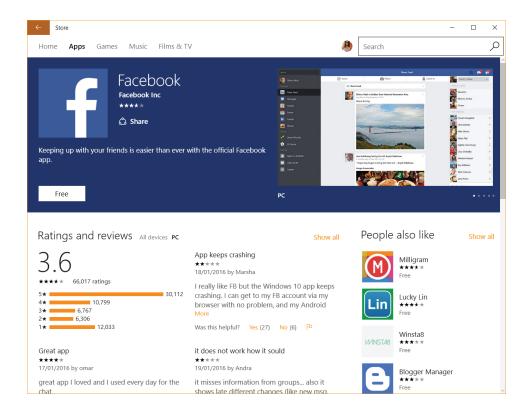


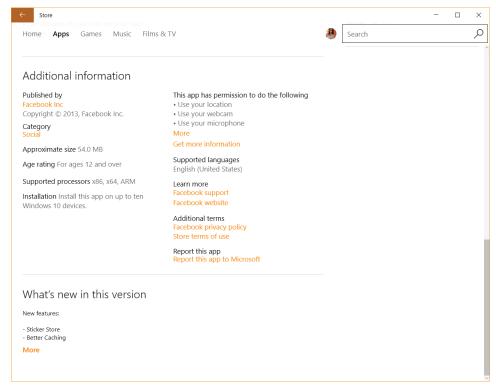
Once you find the app you need, scroll to **Additional information** and check:

- The publisher's name
- Its age rating (especially for protecting your children)
- The type of permissions that the app requires
- If it offers additional links for supplemental information.



Trusted apps







Should an app cause you trouble, you can go to the app's page in the Windows Store and report it to Microsoft, so they can take the appropriate measures.

Trusted apps

Available on

All Windows 10 versions.

How it works

Microsoft or trusted vendors verify the app so that it meets the Microsoft Store security standards. Only after that will they allow it to show up in the store for distribution or sale.

In order to download or buy apps from Windows Store, you'll need to log in with your Microsoft account.

Key takeaway

By knowing which details to check in the Windows Store, you'll be able to avoid installing rogue apps and thus giving cyber criminals a way into your computer. Also, the filter put in place by Microsoft will help keep you protected from most malicious apps.

Settings, tips & tricks

There is not that much information out there about Trusted Apps in Windows Store, but this might help fill in some blanks:

Top Windows 10 Security Features Explained.



What it is

According to Microsoft, SmartScreen Filter is a technology embedded into the Windows Store and in Microsoft Edge that helps protect you against phishing attempts.

What's new

SmartScreen has been around since Windows 8, so there's not much new about it. Read below for more information on how it works.

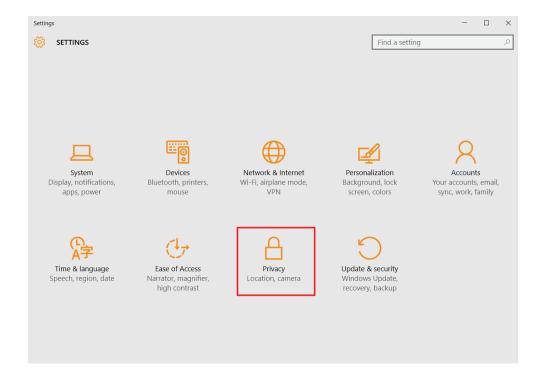
Available on

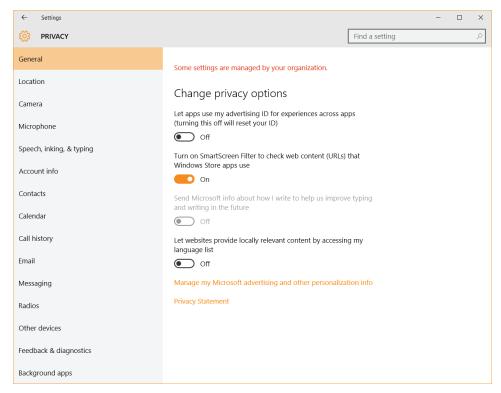
All Windows 10 versions.

Where to find it

You can turn the SmartScreen Filter on and off by going to Start > Settings > Privacy > General. There, you can "Turn on SmartScreen Filter to check web content (URLs) that Windows Store apps use."

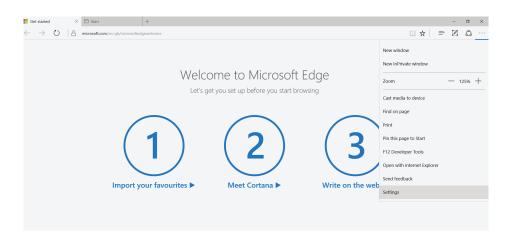


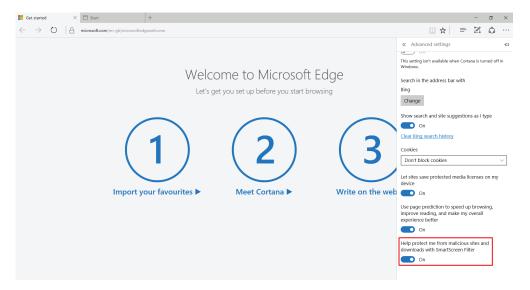






Remember that SmartScreen Filter is also embedded into Microsoft Edge. Here's how to find the option in Microsoft's latest browser. Follow this path: **Edge > Settings > Advanced Settings** and turn on "Help protect me from malicious sites and downloads with SmartScreen Filter."





How it works

According to Microsoft, here's how SmartScreen kicks into action:



- "As you browse the web, **it analyses webpages** and determines if they have any characteristics that might be suspicious. If it finds suspicious webpages, SmartScreen will display a message giving you an opportunity to provide feedback and advising you to proceed with caution.
- SmartScreen Filter checks the sites you visit against a dynamic list of reported phishing sites and malicious software sites. If it finds a match, SmartScreen Filter will show you a warning notifying you that the site has been blocked for your safety.
- SmartScreen Filter checks files that you download from the web against a list of reported malicious software sites and programs known to be unsafe. If it finds a match, SmartScreen Filter will warn you that the download has been blocked for your safety. SmartScreen Filter also checks the files that you download against a list of files that are well known and downloaded by many Internet Explorer users. If the file that you're downloading isn't on that list, SmartScreen Filter will warn you."

Source: SmartScreen Filter: frequently asked questions

Key takeaway

Even though you may find the SmartScreen Filter annoying at first, it's really useful to have it on. We suggest you keep it activated for potential malicious apps that might try to install themselves on your computer.



Settings, tips & tricks

If you're curious to read more on the SmartScreen Filter, here are two resources to help you achieve just that:

- What is the SmartScreen Filter & How Does it Work?
- SmartScreen Filter: frequently asked questions



What it is

Microsoft Edge is the default browser in Windows 10, and its role is to replace Internet Explorer on all devices in the Windows ecosystem.

Edge claims to be a rather safe browser, because of the various integrated security settings and because it limits add-ons and plugins that can have a potential harmful impact.

What's new

Bottom line: quite a lot. We won't get into the details of all the behind-the-scenes action here, but we'll mention some security aspects that you may find useful.

Microsoft Edge no longer support the extensions VML, VB Script, Toolbars, BHOs or ActiveX. For non-techies, this means that Edge is more secure because it gave up on using some technologies that were often exploited by cyber criminals.

Edge also features **increased protection against code injection**, which is essential to protect against a large part of cyber attacks that target browsers (more details in this **Microsoft blogpost**).



The new Microsoft Edge also **includes the SmartScreen Filter feature** that we mentioned earlier, which is meant to protect users against phishing.

Microsoft Edge

What's more, **Edge constantly runs in a partial sandbox**. Sandboxing is a technique used in security to run a program in a controlled and contained environment, so it can't affect other apps or data.

Java is not supported in Edge, but Adobe Flash is and let's not forget that Flash was **one of the most vulnerable and exploited plugins in 2015**.

"Yes, Adobe Flash is supported as a built-in feature of Microsoft Edge. We continue to work closely in partnership with Adobe to provide this version of Flash, which we support and service via Windows Update."

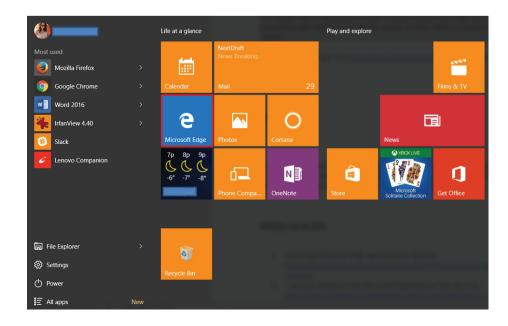
Source: Microsoft Edge FAQ

Where to find it

Just go to the Start menu and you'll find Edge in the "Life at a glance" section, as Microsoft chose to name it.



Microsoft Edge



Key takeaway

Using Microsoft Edge can actually be safer than using Firefox or Chrome, as it doesn't support vulnerable plugins. It can also be protected with an additional security product which has web filtering capabilities and a VPN for enhanced privacy.

Settings, tips & tricks

- Protecting Microsoft Edge against binary injection
- 3 Security Features in the Microsoft Edge Browser that We Love
- A break from the past, part 2: Saying goodbye to ActiveX,
- Microsoft Edge Brings Bigger, Badder Security to Windows 10



Cyber threats targeting Windows 10

Cyber criminals knew Windows 10 was coming and they've prepared for it. The new operating system brought some improvements in terms of security and some changes, but the most vulnerable applications continued to exist.

The most targeted applications you may be using on Windows 10:

- Internet Explorer
- Google Chrome
- Mozilla Firefox
- Oracle Java
- Office Word
- Office Excel
- Adobe Acrobat Reader
- Adobe Flash and Flash plugin

It's no wonder that cyber criminals are keeping up with the times and adapting to Windows 10's specific elements.



Cyber threats targeting Windows 10

"In November 2015, our team at Heimdal Security picked up and analyzed a new variant of the infamous banking Trojan Dyreza.

The results of the analysis show that the info-stealer malware now includes support for Windows 10. This new variant can also hook to Microsoft Edge to collect data and then send it to malicious servers.

Moreover, the new Dyreza variant kills a series of processes linked to endpoint security software, in order to make its infiltration in the system faster and more effective.

The cyber criminals behind Dyreza often spread the malware via "spray & pray" spam campaigns, which are sent to random recipients."

Source: Security Alert: New Dyreza variant supports Windows 10 & Edge

Threats such as ransomware, banking Trojans and data-stealing malware won't go away just because a new OS is released. That's why it's important to know and adjust your security settings to counteract their malicious tactics.

And you're certainly interested in solutions, which we're very keen on offering.



Recommended security apps for Windows 10

Even if it claims to be "the most secure Windows" to date, Windows 10 is surely not impenetrable against cyber attacks. That's why you need additional applications to keep your data and confidential information safe.

There are 5 categories of security-related products we recommend you install:

1. Antivirus

Windows Defender can only offer baseline protection, but you need much more than that. Choose a reliable and strong antivirus product that's placed in the top 5 recommended AVs by experts (independent ones, if possible).

And because we know it's a difficult choice to make, here's a guide to help you pick the right one for your: What Is The Best Antivirus For My



PC? A Step-By-Step Research Guide.

2. Antimalware

Recommended security apps for Windows 10

Antivirus can't provide 100% protection against malware or other cyber attacks. In fact, no security solution can. But if you use complementary solutions, then you can increase your protection against cyber criminals and their malicious tools.

If you're unsure why antivirus is really not good enough, here's a recommended read to help you the big picture: Is Antivirus Dead? Meet The NextGen Anti-Hacking Tools

3. Password manager

You can't have strong security without strong passwords. And it's very often an aspect that users neglect. So much so that **the most used passwords in 2015** probably make cyber criminals laugh.

We've all used the same password more than once, there's no shame in admitting it. But it's crucially important to stop doing it, for your online safety. If attackers break one of them, they will get into all of your accounts.

Here's a top 5 of reaaaally bad passwords that I hope will make you change your ways:

- 1. 123456
- 2. password
- 3. 12345678



4. qwerty

5. 12345

Recommended security apps for Windows 10

So we're obviously not good at passwords, which is why it's great to have some help. Here's a step-by-step plan to help you boost your password security:

Password Security 101: How to Manage Your Credentials Like an Expert in 8 Easy-to-Follow Steps

4. Encryption tools

Encryption is all the rage right now, with talks around it spanning from government to private users. What we know is that encryption is necessary and very useful to protect our data from prying eyes or malicious attempts. Of course, we have to make sure it's done right.

If you don't want to use the built-in BitLocker encryption that comes with Windows 10 (the Pro edition), then there are plenty of alternatives. Here's a guide to help you choose the right encryption tool for you:

9 Free Encryption Software Tools to Protect Your Data

5. Backup solutions

Data backups are exactly like washing your teeth before you go to sleep: you know they're good for you and you should do it more often, but you just can't seem to find the motivation.



With ransomware and other data-stealing malware out there, backups can be life savers! And the same goes for accidentally damaging your computer, having it stolen or what else could happen.

Recommended security apps for Windows 10

So do yourself a big favor and start a backup schedule. You can either do it using the backup tool integrated in Windows 10, or you can choose one of the many options available on the market. Or, even better, you can do both!

How to back up your computer - the best advice in one place

Windows 10 Privacy



Ever since Windows 10 was launched, there have been many polemic discussions around the privacy factor of the new operating system. Microsoft is the type of company that people love to hate, so the privacy issues were expected to cause some ruckus.

Critics and privacy advocates denounced the default settings in Windows 10 for collecting and transmitting user data to Microsoft and its partners.

"Windows 10, by default, has permission to report a huge amount of data back to Microsoft. By clicking through "Express Settings" during installation, you allow Windows 10 to gather up your contacts, calendar details, text and touch input, location data, and a whole lot more. The OS then sends it all back to Microsoft so that it can be used for personalisation and targeted ads."

Source: Windows 10 doesn't offer much privacy by default: Here's how to fix it

Microsoft's Privacy Statement states that:

"Microsoft collects data to operate effectively and provide you the best experiences with our services. You provide some of this data directly,



Controversy

such as when you create a Microsoft account, submit a search query to Bing, speak a voice command to Cortana, upload a document to OneDrive, complete a survey, or contact us for support. We get some of it by recording how you interact with our services by, for example, using technologies like cookies, and receiving error reports or usage data from software running on your device."

"We also obtain data from third parties (including other companies). For example, we supplement the data we collect by purchasing demographic data from other companies. We also use services from other companies to help us determine a location based on your IP address in order to customize certain services to your location."

Source: Microsoft Privacy Statement

Here is what type of data Microsoft can collect via Windows 10:

- Name and contact data
- Credentials
- Demographic data
- Interests and favorites
- Payment data
- Usage data
- Contacts and relationships
- Location data
- Content.

Now, before you go and feel outraged that Microsoft does this, remember that you're sharing at least as much if you have a Facebook account. It's no excuse, but it's customary for companies such as Microsoft to collect this type of data.



Also, this response that Microsoft officials gave may help clear the air a bit.

Controversy

But why are they collecting this much data?

Data such as this is usually used for:

- Customer support
- Product activation
- Service improvement
- Security, safety and dispute resolution
- Business operations.

All this can be quite a hassle to comb through, so let's keep our cool. We'll show you how to adjust your settings to get **the highest possible level of privacy on your Windows 10 device**. Enhanced privacy will also mean improved Windows 10 security, so here's how to do it.



Terms of service & Privacy policy

What it is

You will probably say you don't have time for this, but if you're concerned with your privacy, the place to start is reading the terms of service and the privacy policy associated with Windows 10.

Where to find it

Here's where to find the two documents:

- **Microsoft License Terms**
- **Microsoft Privacy Statement**



What it is

This is the section where you can adjust a myriad of settings to protect your privacy and data from being transmitted to either Microsoft or third parties.

What's new

Because Windows 10 comes with more built-in features that can help your operating system learn more about you, so it can provide more useful help and suggestions, there are quite a few new elements.

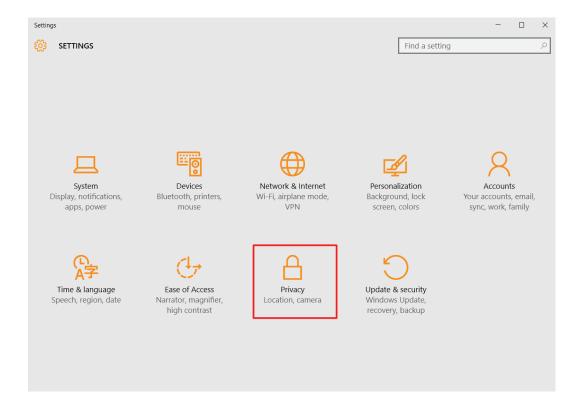
The **Privacy settings** area bundles them up nicely, so let's see what you can do in either section.

Where to find it

It all beings with Start > Settings > Privacy.



Privacy settings



Available on

All Windows 10 versions.

How it works

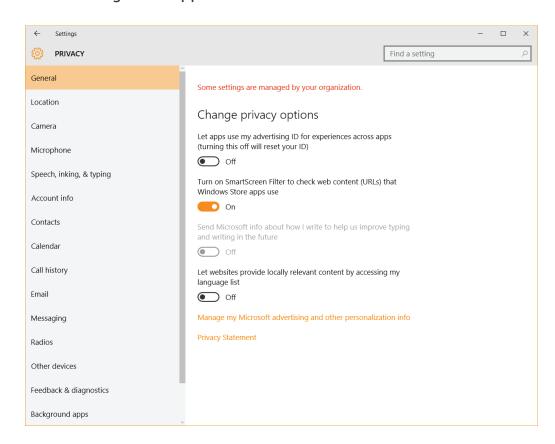
Once you're in, you'll be able to adjust privacy settings such as:

- General
- Location
- Camera
- Microphone
- Speech, inking and typing
- Account info
- Contacts
- Calendar



Privacy settings

- Call history
- Email
- Messaging
- Radios
- Other devices
- Feedback & diagnostics
- Background apps.



Key takeaway

Adjusting your privacy settings in Windows 10 can help you see that the new operating system is not the nightmare that some articles have claimed it is. Spending a bit of time reading about your options and tweaking them to your liking is all you need to do to keep your



data from prying eyes.

Privacy settings

Settings, tips & tricks

We have more than a few recommended links that can give you a hand in better understanding the privacy matters related to Windows 10, so here is a good selection you can rely on:

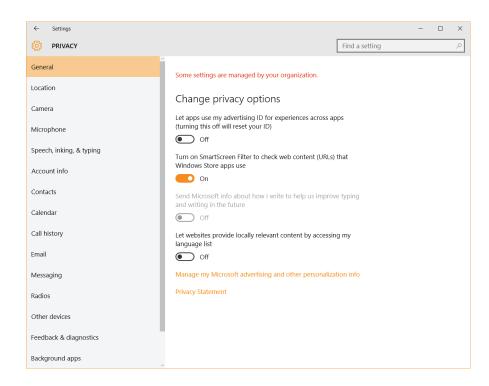
- The Windows 10 privacy settings you need to change right now
- What Windows 10's "Privacy Nightmare" Settings Actually Do
- How to reclaim your privacy in Windows 10, piece by piece



General privacy settings

What we really like about Windows 10 is that the info about each option is well written, clearly and simply, so that anyone can understand it.

For example, these **general privacy settings** don't even need an explanation:





General privacy settings

Generally, you'll find that you have **two major types of settings** you can adjust:

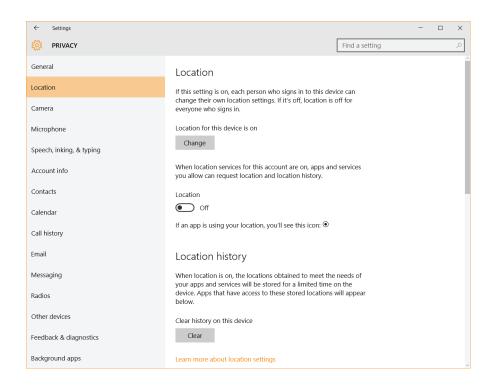
- Turn a feature on or off
- Keep a feature on, but select which apps it can apply to.

Also, each section of the Privacy settings area includes **links to privacy policies specific to that feature**, so you can read more about it, in depth.



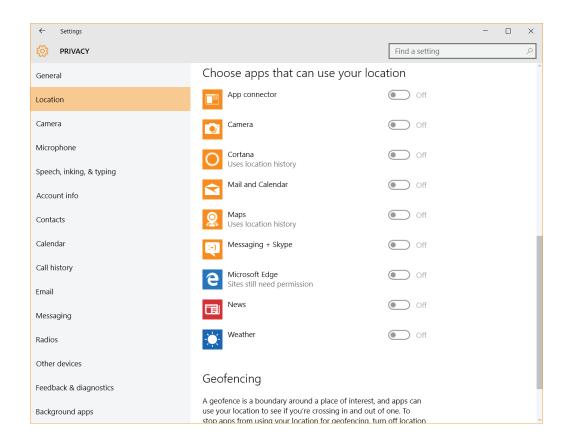
For example, when it comes to **location data**, you can choose to turn it on or off.

If you choose to turn it on, you can also control which applications can use your location information to offer tailored services and suggestions.





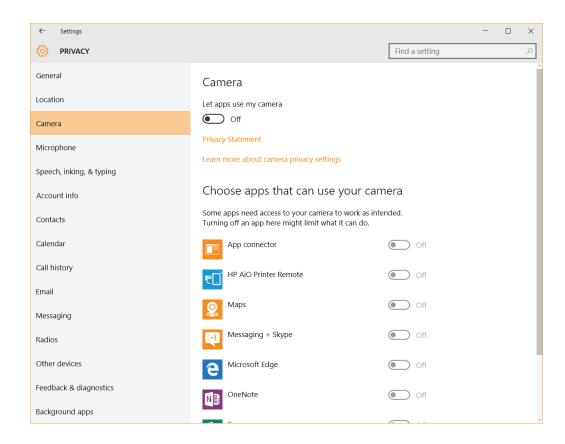
Location privacy settings





Camera privacy settings

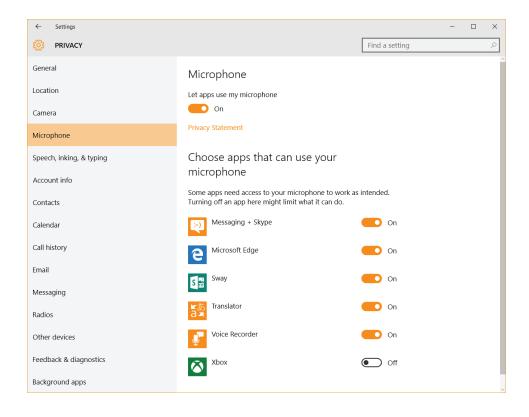
Here's where you decide if any apps can use your camera or if only some of them can.





Microphone privacy settings

When adjusting microphone settings, remember to keep the feature on for any apps that may actually require voice interaction, such as Skype or your voice recorder. This comes from someone who forgot to turn on the setting for Skype and couldn't figure out why it didn't work properly (yes, that person is me).

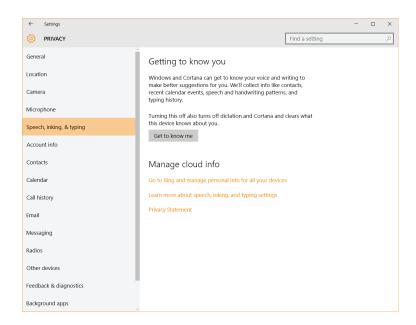




Speech, inking and typing privacy settings

If you want to use Cortana, the personal assistant built into Windows 10, you can help her get to know you by letting her collect information about your speech and writing patterns.

If that sounds too intrusive (or downright creepy) for you, just turn Cortana off and that'll be that. (More on Cortana in a bit.)

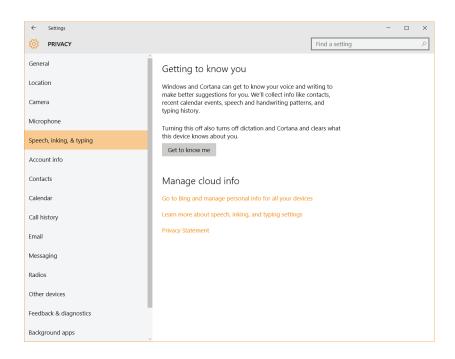




Account info security settings

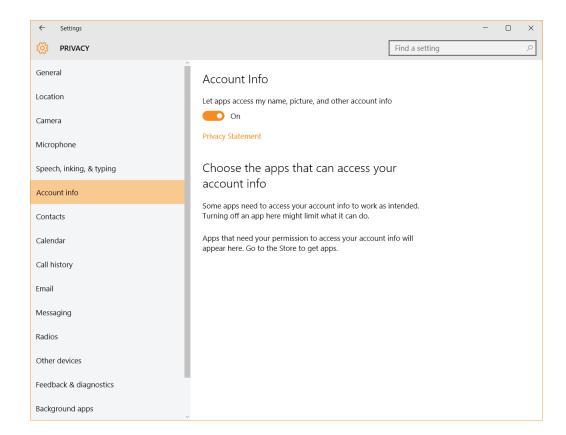
Do you want your apps to use your account information?

This data can include name, birthdate (if you provided one), credit card details and so on. As a security measure, we always recommend you **don't save your credit card information in your account.** If someone breaks into it, it'll be incredibly easy to use your card to make purchases.





Account info security settings



Moreover, it's a great idea to **enable two-step verification** (or two-factor authentication) **for your Microsoft account**. It's a great addition to your security stack and can really help you in case anyone tries to break into your account.

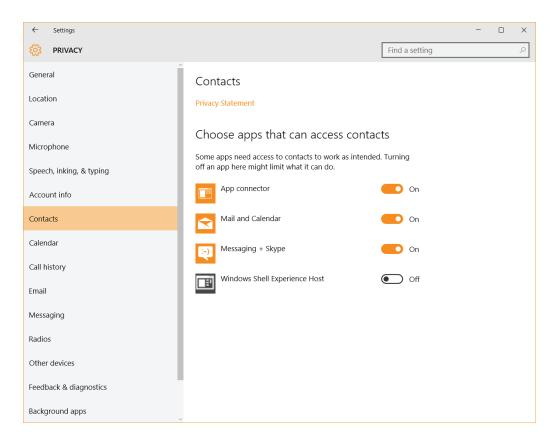
Here's how to do it: How to use two-step verification with your Microsoft account

PS: you can also **set passwords for specific applications**, so that's also something worth looking into.



Contacts privacy settings

Should your applications have access to your contacts? It's up to you.

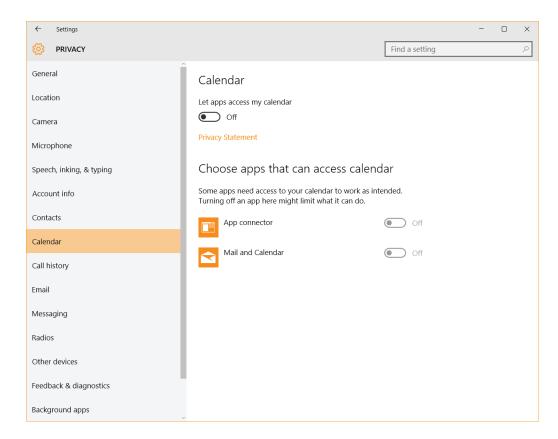




Calendar privacy settings

Do you really need your apps to use your calendar data?

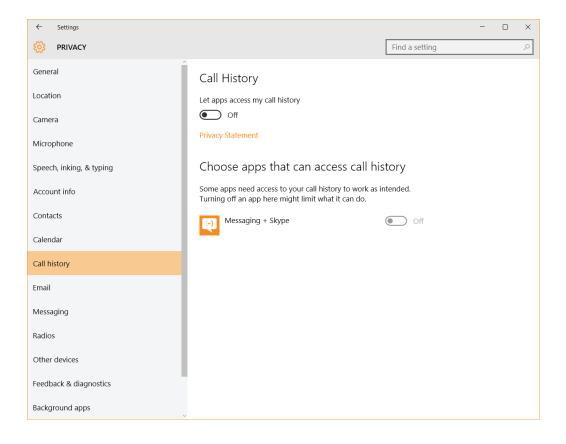
If you don't use Microsoft as your primary email address, we recommend turning this option off altogether.





Call history privacy settings

This is where it gets a little creepy: sharing your call history data feels like a bit more than a simple intrusion to your privacy. At this point, it really starts to feel that you need to pay more attention to the type and amount of information you share.

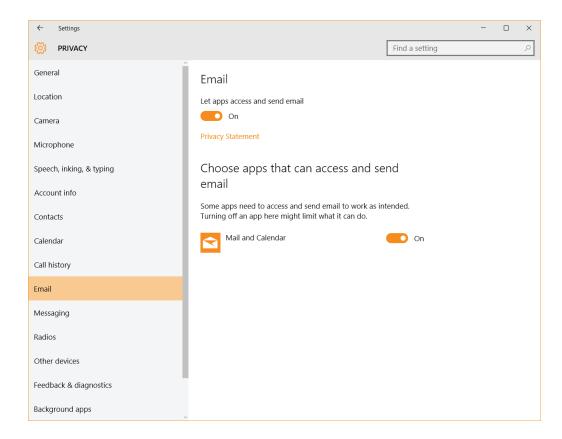




Email privacy settings

Do you use Windows 10 native apps to send email?

If not, there's no point in keeping this feature on.





If you want to strengthen your Windows 10 security, there are plenty of things you can do to make your email accounts more secure.

Email privacy settings

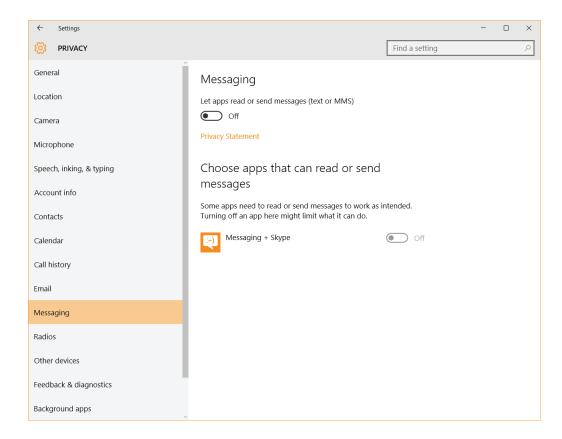
The following steps are just what you need to secure your email account like a pro:

The Complete Guide to E-mail Security



Messaging privacy settings

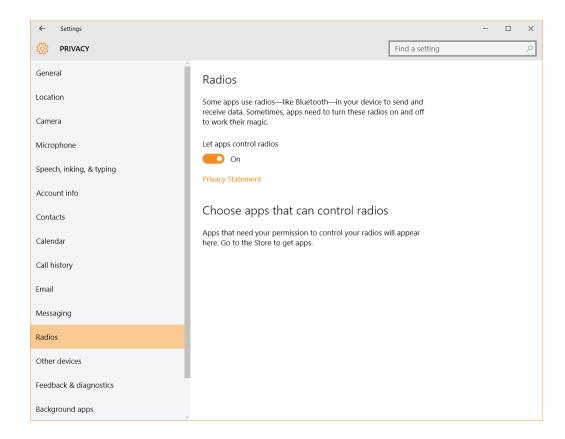
Decide which apps, if any, should be able to read or send messages to your family, friends, coworkers and so on.





Radios privacy settings

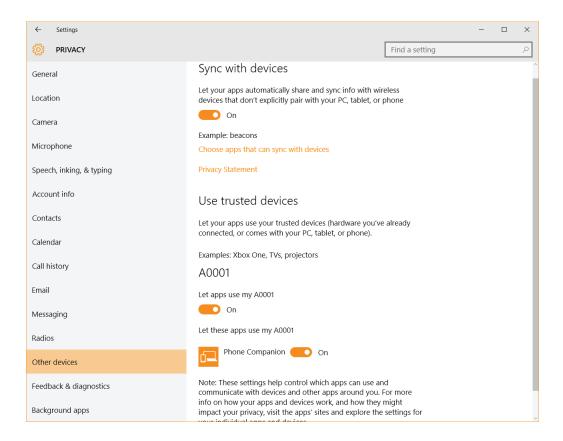
Maybe you'd think this is a harmless setting you don't need to pay attention to, but **Bluetooth** is also a radio-based technology, so do take a look at it.





Other devices privacy settings

This is the place where you choose how your devices can connect to one another to share data. Careful which devices you add to your "trusted" list, because they can represent a security hazard.





Feedback and diagnostics privacy settings

Select how often Windows should ask for feedback. Choose between: Automatically (recommended)

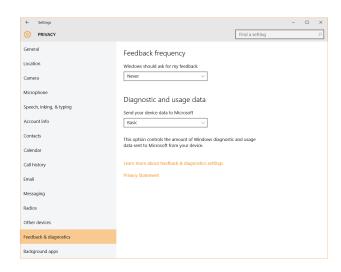
Always

Once a day

Once a week

Never.

How generous do you feel with your time and attention?





Feedback and diagnostics privacy settings When it comes to Diagnostic and usage data, Microsoft doesn't give users the option to provide nothing at all. So you can opt for Basic, Enhanced or Full (recommended).

Buy what do these options mean?

Let's see what the official statement on this feature is:

"As you use Windows, we collect performance and usage information that helps us identify and troubleshoot problems as well as improve our products and services. We recommend that you select Full for this setting.

- Basic information is data that is vital to the operation of Windows. This data helps keep Windows and apps running properly by letting Microsoft know the capabilities of your device, what is installed, and whether Windows is operating correctly. This option also turns on basic error reporting back to Microsoft. If you select this option, we'll be able to provide updates to Windows (through Windows Update, including malicious software protection by the Malicious Software Removal Tool).
- Enhanced data includes all Basic data plus data about how you use Windows, such as how frequently or how long you use certain features or apps and which apps you use most often. This option also lets us collect enhanced diagnostic information, such as the memory state of your device when a system or app crash occurs, which may unintentionally include parts of a document you were working on when a problem occurred. We also use this information to measure reliability of devices, the operating system, and apps. If you select this option, we'll be able to provide you with an enhanced and personalized Windows experience.
- Full data includes all Basic and Enhanced data, and also turns on advanced diagnostic features that collect additional data from your



Feedback and diagnostics privacy settings device, which helps us further troubleshoot and fix problems. When devices experience problems that are difficult to diagnose or replicate with Microsoft's internal testing, Microsoft will randomly select a small number of devices, from those opted into this level and exhibiting the problem, from which to gather all of the data needed to diagnose and fix the problem (including user content that may have triggered the issue). If an error report contains personal data, we won't use that information to identify, contact, or target advertising to you. This is the recommended option for the best Windows experience and the most effective troubleshooting.

Source: Windows 10 feedback, diagnostics, and privacy: FAQ

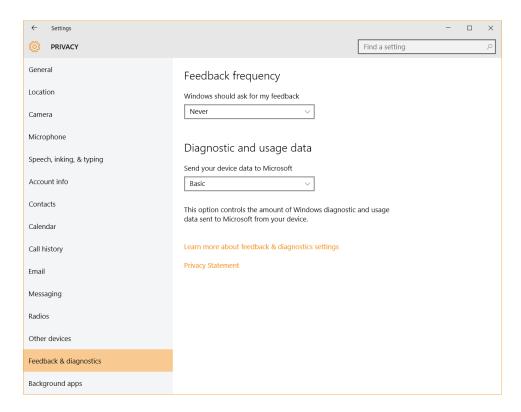
Again, knowledge is power here! Read the details before tweaking your settings, so you can ensure that you have a good grasp of what happens to your data.



Background apps privacy settings

This is the last privacy option in this section which provides the chance to select which applications can receive information send notifications and stay up-to-date, even when you're not using them.

If you don't use it, turn it off – words to live by!





What it is

Cortana is a personal assistant embedded into Windows 10 that can, according to Microsoft:

[...] help you find things on your PC, manage your calendar, track packages, find files, chat with you, and tell jokes. The more you use Cortana, the more personalized your experience will be.

Source: What is Cortana?

The development of Cortana started in 2009 and the personal assistant was first introduced in 2014, but in Windows 10, this really shines. It's even available in multiple languages, such as English, French, German, Italian, Spanish, Chinese, and Japanese.

What's new

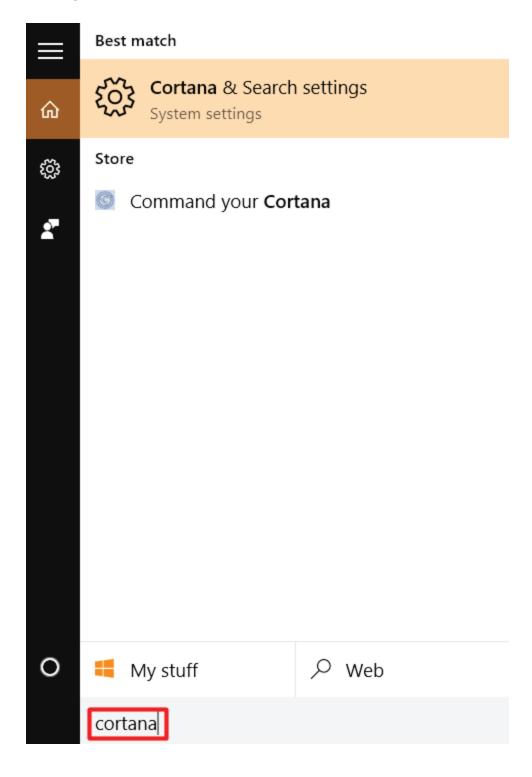
Cortana is entirely new, so not many people know how deeply ingrained in Windows 10 it is, especially when it comes to data collection and interpretation.

Where to find it



In the taskbar, search for "Cortana" in the available search bar and a settings menu will pop up.

Cortana



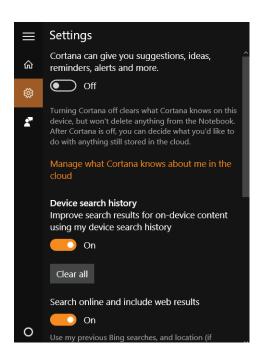


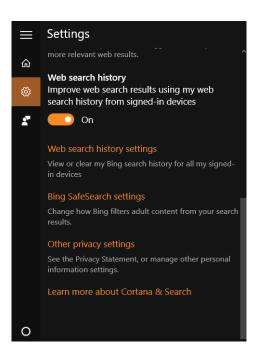
Click on "Cortana & Search settings" and you'll be able to do the following:

Cortana

- Turn Cortana on or off
- Keep your device search history on or turn it off
- Include web results in the searches you make from the search bar included in your taskbar or not
- Give Microsoft access to improve your search results by using your search history from all of the devices you've signed in on.

You can also find a list of helpful links with more information about how Cortana works and how your data is managed when you use it.





This FAQ can help with a lot of useful answers: **Cortana, Search, and privacy: FAQ.**

Available on



All Windows 10 versions.

How it works

Cortana

So Cortana can do a lot of things for you, but it's also a major privacy risk if you're keen about the subject.

For example, Cortana can:

- Set reminders for you
- Retrieve search results activated with voice commands.
- Do calculations and conversions
- Find facts
- Give you updates on the weather
- Offer directions
- Even send email, and much more.

Source: 15 Things You Can Do With Cortana on Windows 10

But doing so will require you to share a lot of your data, so Cortana can learn about you to offer better services.

Key takeaway

Having a personal assistant like Cortana requires you give up a bit of your privacy in return for its services. Read about your options and consider if you find Cortana useful and if you're ready to let her learn about you in order to help you.



Cortana

Settings, tips & tricks

If you're interested in learning more about Cortana and see how she can potentially help you, these links provide a lot of useful information:

- 15 Things You Can Do With Cortana on Windows 10
- How to use Cortana in Windows 10: speak to your PC and make things happen
- Everything You Can Ask Cortana to Do in Windows 10

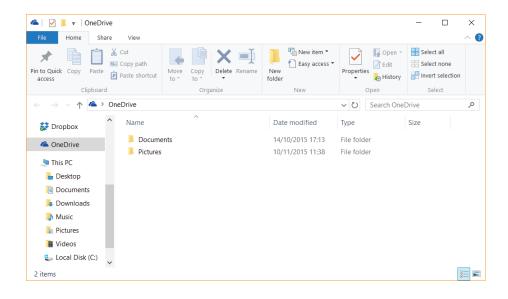


What it is

OneDrive is free online storage that comes with your Microsoft account and it's also included in Windows 10. You can use it to store your files in the cloud and OneDrive makes it available on any Windows device you own and that you've logged into with your account.

Where to find it

The quickest way is to use the search bar located in your taskbar and look for "OneDrive." This will bring up the OneDrive desktop app, which is basically a folder you can put your files into.





Available on

All Windows 10 versions.

OneDrive

How it works

All the data you put in your OneDrive file will automatically sync to the cloud and will then become available on any Windows 10 enabled device you use. It comes with 15GB of free storage for everyone

Key takeaway

OneDrive is a great tool to use as a backup location, but you should decide if it's something you'd like to use or if you'd rather select another cloud solution. Comparing the most used options on the market could help you single out the benefits and disadvantages faster and easier.

Settings, tips & tricks

Want to see how you can best manage your OneDrive application to keep your data safe? Check out the advice in the links below. We even found how you can remove OneDrive, although it's a bit more complicated than expected.

- This Is How OneDrive Works in Windows 10
- Why you should use OneDrive with Windows 10
- How to Disable OneDrive and Remove It from File Explorer on



Windows 10

OneDrive storage plans change in pursuit of productivity and collaboration

OneDrive



If you're not familiar with the term, a proxy server, also known as a proxy is:

"[...] a computer system or router that breaks the connection between sender and receiver. Functioning as a relay between client and server, proxy servers help prevent an attacker from invading a private network and are one of several tools used to build a firewall."

Source: Definition of: proxy server

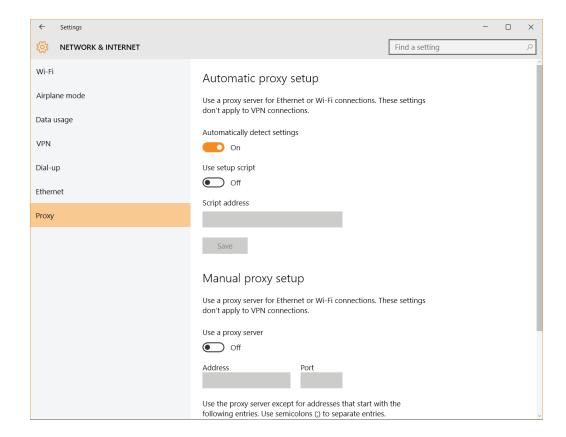
Where to find it

You can start configuring your proxy by going to **Start > Settings > Network & Internet > Proxy**.





Proxy settings



Available on

All Windows 10 versions.

How it works

Once you're in the right place, you'll be able to either use a setup script or do a manual proxy setup. This will help you get an additional privacy and security layer for your device, which comes in very handy.

Key takeaway

Using a proxy may feel old-school, but it can help provide a bit of extra-privacy. Don't rely on it to do what a VPN can do, though. A



pragmatic approach when it comes to security and privacy always works.

Proxy settings

Settings, tips & tricks

If you've never used a proxy before, you can learn all the basics by following the two links below:

- How to Set Up A Proxy Server In Windows 10
- What are the Benefits of Using a Proxy?



What it is

The Wikipedia definition of a VPN is perfect and it will definitely help you understand what a VPN is if you've never heard about it or used one:

"A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, and thus are benefiting from the functionality, security and management policies of the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption."

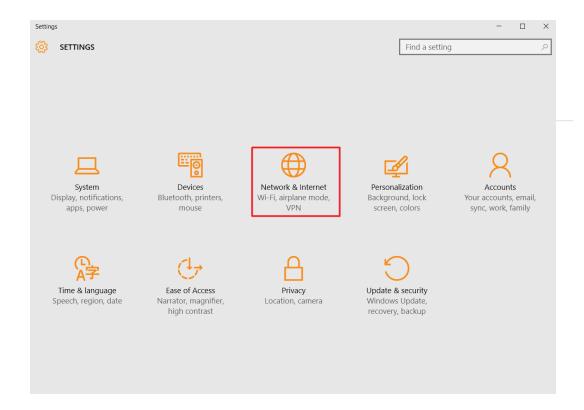
Source: Virtual private network, Wikipedia

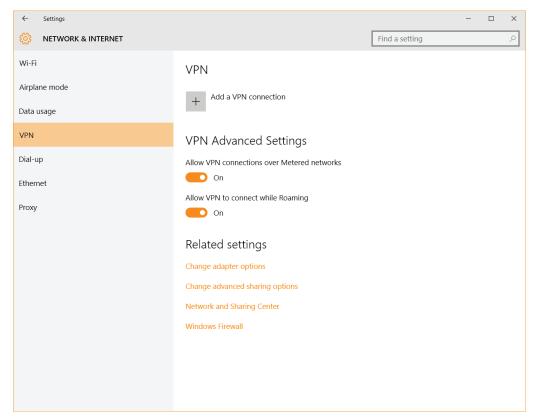
Where to find it

To start setting up your VPN connection, go to: **Start > Settings > Network & Internet > VPN**.



VPN settings







Available on

All Windows 10 versions.

VPN settings

How it works

By setting up a VPN connection, you'll anonymize your Internet traffic so advertisers can't target you with ads. This also makes cyber criminals unable to track your moves around the web.

Using a VPN connection is especially important when you connect to networks that are not your own, but make sure to use adequate cyber security products as well. VPN is dedicated to safeguarding your privacy, not your online security.

Windows doesn't offer a VPN solution of its own, so you'll have to put in the settings corresponding to your VPN product of choice.

Key takeaway

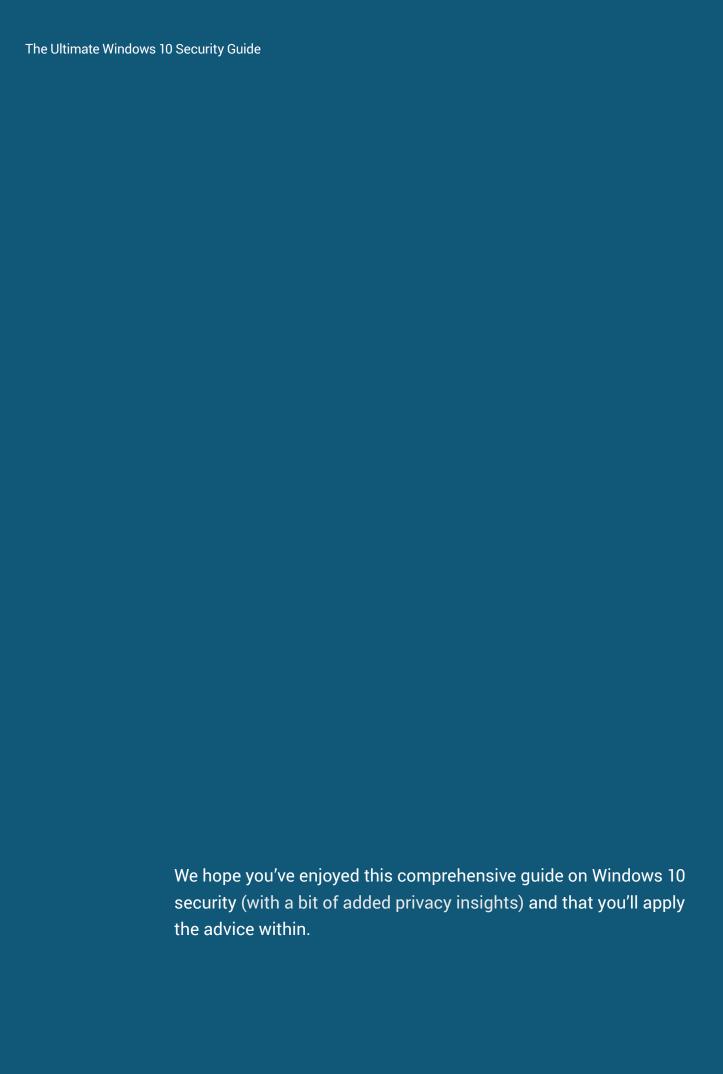
Once you discover the benefits of using a VPN, you may want to make it part of your fresh Windows setup. Security and privacy products work best when you create your own multi-layered system. That doesn't mean you should install all the security products available, but that you should choose the ones that best fit your needs.

Settings, tips & tricks



The go-to guide for setting up your VPN on Windows 10? This one: **How** to Set up a VPN Connection in Windows 10.

VPN settings





We are Heimdal and security is our passion

Since 2011, we have been developing new technologies and providing intelligence to protect over 350,000 users against cyber criminal attacks and data security breaches.

We protect users and companies from cyber-criminal actions, by keeping confidential information and intellectual property safe.

The last years proved that information theft and financial data leakage are major international issues, which continue to create security challenges for organizations, as well as private individuals. That's why our products have been developed: to address the real-world need for a solution against cyber-criminals actions and their malicious tools.



HEIMDAL FREE

We keep you safe from security exploits by automatically and silently updating your vulnerable software applications.



HEIMDAL CORP

We help you manage your network security from a single, easy-to-use interface to keep cyber-criminals and data stealing malware away from your company's sensitive data.



HEIMDAL PRO

We protect you from attacks that antivirus can't block, such as ransomware or sophisticated financial malware. Ensure your system is proactively protected against cyber attacks using Heimdal PRO's intelligence.