

WINDOWS UPDATES AND MAJOR BUILDS

Updates install automatically, and you can't pick and choose

Another big change with Windows 10 is that there will be automatic updates, so there's less chance of you missing an important security update or bug fix. In addition, all Windows 10 systems will be on the same page at all times, whether it's on a computer, a tablet, or a smart phone.

Visit the Windows Update interface (type *windows update* in the search box) and you'll find a single button — *Check for updates*. Click this button and Windows will check for available updates. If it finds any, it will automatically download and install them. Windows will also check for updates in the background and automatically download and install them the moment that they are released by Microsoft.

Unlike on previous versions of Windows, there's no way to select individual updates you want to download. All updates — from security updates and Windows Defender definition updates to optional updates and driver updates — will be installed automatically.

The only option you can control is to select the “Advanced options” link and **uncheck** *Give me updates for other Microsoft products when I update Windows*. This will allow you to disable updates for Microsoft Office and other Microsoft programs.

In Windows 10, Microsoft is committed to rolling out both security updates and feature updates. Most of the installed Modern applications will also automatically update themselves via the Windows Store. Microsoft is thinking of Windows 10 as the last version of Windows, so instead of a Windows 11 or Windows 10.1, we should see future updates and interface changes appear on an ongoing basis.

Accordingly, “Patch Tuesdays” (the second Tuesday of each month) will be a thing of the past. Ironically, the first major upgrade (#1511) to Win 10 took place on a patch Tuesday!

Microsoft also plans on making more use of the “build” system going forward. While small security updates will arrive as individual updates, major upgrades to Windows 10 that include new features will likely arrive as “builds.” A Windows 10 PC can upgrade directly to a new build, which means that old cycle of

downloading updates and rebooting four or five times to ensure you have all the old updates on an out-of-date PC won't be necessary.

But you can choose when to reboot

Click the “Advanced options” link in the Windows Update interface and you'll find two **Choose how updates are installed** options. You can pick *Automatic*, which is the default — Windows will automatically download updates, install them, and schedule a reboot for a time when you aren't using your PC.

You can also choose *Notify to schedule restart*, which will prevent your PC from automatically rebooting without your confirmation. But, either way, those updates will automatically be downloaded and installed.

Peer-to-peer downloads for updates are enabled, even over the Internet

To speed up updating, Windows now uses peer-to-peer downloads for updates. For example, if you have more than one Windows 10 at home, you don't necessarily have to download the same update several times. Instead, the first PC to update would download it and the other PCs could download it from the first PC.

You can control whether peer-to-peer downloads are enabled from the *Choose how updates are delivered link* under **Advanced options**.

By default, Windows 10 enables peer-to-peer downloads over the Internet as well, and your PC will use some of your upload bandwidth to send those Windows updates to other PCs. You can disable this by selecting only “PCs on my local network.” See snipped page below.

If you run Disk Cleanup (type *disk cleanup* at the search bar) and clean up the Windows Update files lying around on your PC to free up space, your PC won't be able to provide peer-to-peer downloads because the files won't be available.



CHOOSE HOW UPDATES ARE DELIVERED

Updates from more than one place

Download Windows updates and apps from other PCs in addition to Microsoft. This can help speed up app and update downloads.

[Learn more](#)

When this is turned on, your PC may also send parts of previously downloaded Windows updates and apps to PCs on your local network, or PCs on the Internet, depending on what's selected below.

Off

Get updates from Microsoft, and get updates from and send updates to

PCs on my local network

PCs on my local network, and PCs on the Internet

You can view your update history and uninstall updates

If there is a problem with your PC, you can uninstall problematic updates afterwards. To view your update history, type *windows updates* at the search box, select “Advanced options,” and select “View your update history.” You’ll see a list of updates, and you can select “Uninstall updates” to view a list of updates you can uninstall.

Microsoft will probably continue rolling out major updates to Windows 10 in the form of “builds” that contain all previous updates. This means that you’ll be unable to avoid updates forever, just as you had to accept an update when it appeared in a

service pack on previous versions of Windows — assuming you wanted to upgrade to that service pack.

In the future, if you have to reset your computer, your updates will follow

When you use the *PC Reset* feature to restore your PC, you won't have to re-download every single Windows update that's ever been released. Instead, the new PC Reset feature will give you a fresh, up-to-date Windows system.

Updates to Modern apps occur automatically

Windows 10 is configured, by default, to automatically update apps in the background, so everything is always up to date. This applies only to Windows 8/10 apps (not legacy apps), of course, but it's a welcome improvement over all earlier editions of Windows.

Securing your legacy software from attack

Tens of millions of people read PDF files using **Adobe Reader**. Unfortunately, hackers have found ways to embed malware in PDF files sent through Adobe Reader that can spring to life when you view the document. (Sumatra PDF is a good alternative!) Two other high-profile hacks have involved Adobe's **Flash Player** and the **Java** software, which for years had been touted as a secure cross-platform application environment. Some serious security holes in Java prompted many pundits to recommend removing it altogether. It seems that new vulnerabilities are discovered in these three pieces of software almost every day.

Software developers issue patches and updates that close these doors to hackers in a never-ending game of us against them. A vulnerability pops up here, hit it with a patch. Another pops up over there, hit it with another patch. Developers provide the patches, but it's up to us to know about these updates and download and apply the patches in a timely manner.

The average computer holds about 80 application programs! Some are pre-installed, and some are downloaded from the Internet. These applications are vulnerable to attack from the cybercriminals.

A good solution is to check all the software on your computer for vulnerabilities using the **Secunia Personal Software Inspector (PSI)**. This free program comes from a trusted security site, and scans your software for known vulnerabilities. It

will tell you which programs need updating and provide links to sites where you can download patches. (http://secunia.com/vulnerability_scanning/personal).