

Automatic Updates and Patching Landing

Automatic Updates and Patching Landing



For more information on securing your data, see [Information Protection @ MIT](#).

On this page:

[Overview](#)

[How to](#)

[Mac OS](#)

[Windows](#)

[Linux/Unix](#)

[Mobile](#)

[Software](#)

[Servers](#)

[Have Questions or Still Need Help?](#)

Overview

An important way to protect your devices is to keep them up to date. Automatic-updates allow your devices to update as soon as new software patches are available - and they're not just for operating systems. Anti-virus software, business applications (Office) and more are important to keep up to date so you have the latest versions with the most current security fixes. To stay informed about the latest IT news and security threats, consider joining the IT Partners and the Security FYI lists.

- [IT Partners](#)
- [Security FYI](#)

How to

Mac OS

- [Configure Automatic Updates on OS X 10.9 or later](#)

Windows

- [IS&T's WAUS: MIT Windows Automatic Update Service](#)
- [MIT Windows Automatic Update Service - WAUS](#)
- [Configure Automatic Updates on a Windows Machine](#)

Linux/Unix

- [Will my workstation automatically upgrade to a new release of Ubuntu?](#)
- [How do I set up Red Hat Network to automatically check for software updates and install them daily?](#)

Mobile

- Most mobile devices will prompt you to take security updates as soon as they are available. Doing so promptly protects you from known exploits.

Software

Many software packages offer automatic updates for security, bug fixes and feature additions. Check the vendor documentation on installation to learn how to turn on automatic updates. Here are some examples of software that has automatic-update options.

- [Sophos Central - How do I update Sophos Anti-Virus?](#)
- [Automatic Updates for Office for Mac](#)
- [Automatic Updates for Office for Windows](#)
- [Web Browsers \(Chrome, Firefox, Opera\)](#)
- [Adobe Software](#)
- [Database Software \(Filemaker\)](#)
- [Virtualization Software \(Vmware\)](#)
- [And more](#)

Servers

It's especially important to be aware of exploits that could compromise servers. If you can't take automatic updates because you need to plan for downtime, join security and patch release email lists for your operating system and software to stay aware of updates. That ensures you know about exploits and the necessary patches to protect your systems.

- [Microsoft Products](#)
- [Apple Products](#)

Have Questions or Still Need Help?

- [Contact the IS&T Service Desk](#)