

ClamAV



Quick Look

ClamAV is a free, open-source antivirus software specifically designed to detect, identify, and block a wide range of malware threats on multiple operating systems, including Windows, macOS, and Linux.

It provides reliable on-demand and scheduled scanning capabilities, as well as real-time file monitoring to ensure continuous protection. ClamAV maintains an extensive and constantly updated virus definition database to combat the latest malware and viruses effectively.

The software integrates smoothly with email servers to automatically scan incoming and outgoing messages for viruses. Its lightweight design ensures minimal impact on system performance, making it suitable for personal devices and large-scale network environments requiring efficient malware defense.

Features

ClamAV is a free, open-source antivirus software that offers reliable malware detection across multiple platforms. Key features include:

- **Supports Windows, macOS, and Linux operating systems**
- **Offers real-time file monitoring for continuous protection**
- **Integrates with email servers for automated virus scanning**

How to Use

Please follow the instructions for your preferred desktop operating system below:



- **Visit the official website:**
<https://www.clamav.net>
- **Go to the “Downloads” section and select the latest Windows version**
- **Download the installer file for your OS:**
 - **Windows:** Download the .exe installer.
- **Install the software:**
 - **Windows:** Double-click the .exe file and follow the setup wizard to complete the installation.
- **Update virus definitions after installation to ensure the latest protection**
- **Run the command or use the built-in updater to download the latest virus signatures.**



- **Visit the official website:**
<https://www.clamav.net>
- **Go to the “Downloads” section and select the version for macOS**
- **Download the installer file for your OS:**
 - **macOS:** Download the .pkg installer.
- **Install the software:**
 - **macOS:** Open the .pkg file and follow the installation steps. If prompted, allow installation under System Settings → Privacy & Security.
- **Update virus definitions after installation to ensure the latest protection**
- **Run the command or use the built-in updater to download the latest virus signatures.**