

What is Bitdefender Webcam Protection and what can it do?

This article is a step-by-step guide to help you get started with Webcam Protection quickly. We'll also cover the module's key features to help you understand how it works and why it's great to use the Webcam Protection feature included in Bitdefender security solutions for Windows. Additionally, we'll highlight tips to help you manage its settings.

Video

- Meet Video & Audio Protection: Secure Your Webcam and Microphone with Bitdefender



What is Bitdefender Webcam Protection?

When it comes to preventing hackers from taking control of your webcam, solutions such as revoking application's privileges, disabling the device's built-in camera, or covering it up are not very practical. This is where Bitdefender Video & Audio Protection comes in. To prevent extortion attempts using sensitive data, our Webcam Protection feature permanently monitors apps that try to access your camera and blocks unknown applications.

How does it work?

Safe and trusted applications are automatically allowed access to the device webcam. An application is considered safe by Bitdefender and allowed by default to access your camera if it has a certain market spread and many users have chosen to allow it.

The behavior is the same regardless of whether your computer has an integrated camera. By default, the “Set application permissions based on community choice” option is enabled, which means that when an application tries to access your camera Bitdefender searches the Cloud for a similar application based on a hash, and if found then the Allow/Block rule selected by most users is applied.

As a safety measure, you will receive a notification each time an untrusted app attempts to gain access to your camera, and you will be able to block it or allow it.

Managing Webcam Protection settings

To activate Webcam Protection, follow these steps:

1. Click **Privacy**, on the left side of the main Bitdefender interface.
2. In the **Video & Audio Protection** pane, click on Settings.
3. Access the **Settings** tab.
4. Use the ON/OFF switch to enable Webcam Protection.



To access the settings menu, click Settings in the Video & Audio Protection pane. From here, you can:

- **Block all access to the webcam**
 - No application will be allowed to gain access to your webcam.
- **Block browsers' access to the webcam**
 - No web browser except Internet Explorer and Microsoft Edge will be allowed to gain access to your webcam.

① **Note**

Due to the Windows Store apps' procedure to run in a single process, Internet Explorer and Microsoft Edge cannot be detected by Bitdefender as web browsers and therefore are excluded from this setting.

- **Set application webcam access based on Bitdefender users' choice**

If most Bitdefender users consider a popular app as being harmless, then its access to the webcam will be automatically set to Allow. If a popular app is considered dangerous by many users, then its access will be automatically set to Block. You will be informed each time one of your installed apps will be listed as blocked by most Bitdefender users.

- **Opt to receive notifications when allowed applications connect to the webcam**

You will be notified each time an allowed app will access your webcam.

How can I protect my webcam from hackers?

Unfortunately, when it comes to webcams, security is often ignored by some producers, who prefer to focus more on economic aspects. This can lead to particularly dangerous situations in which users can become easy targets for hackers looking to access their devices. To protect your webcam against hackers, you should:

- Never use default settings. Make sure you change passwords and other settings once you've installed your device.
- Always keep the firmware up to date.
- Use an adequate security solution, capable of protecting your webcam.