

Temporary workaround for Windows driver blocking

Driver Signature Enforcement - Windows 10 / Windows 11

IMPORTANT WARNING - READ BEFORE STARTING

This procedure is a temporary workaround intended to allow Medcapteurs drivers to operate after the driver blocking issue caused by some Microsoft updates or security policies.

This operation temporarily changes the level of driver control applied by Windows during startup. It may involve risks if the steps are not followed properly.

The customer remains responsible for carrying out this procedure and for the condition of their computer. Medcapteurs informs the customer that this is a sensitive operation and cannot be held responsible if the customer's PC encounters any issue, including Windows access problems, BitLocker recovery key request, startup error, data loss, system malfunction or need for IT intervention.

Before starting, the computer must be connected to AC power, all open work must be saved, and the BitLocker recovery key must be available if the computer is encrypted.

Procedure objective

Use this procedure only as a temporary workaround when Medcapteurs drivers are blocked by Windows. The procedure has one prerequisite, then two parts:

Prerequisite	Check whether BitLocker / Device Encryption is enabled or disabled on the customer's PC.
1	If BitLocker is enabled, disable it by running the provided script with administrator rights.
2	If BitLocker is disabled, go directly to Part 2. Restart Windows with Driver Signature Enforcement temporarily disabled, then install or relaunch the Medcapteurs driver.

Important: disabling driver signature enforcement is temporary. After every full Windows restart, the manipulation must be performed again if the driver needs to be installed or relaunched in this mode.

Prerequisite - Check BitLocker status before any operation

Before running the BitLocker script or changing startup options, check whether BitLocker / Device Encryption is enabled on the customer's PC.

Windows 11 Home	Open Settings > Privacy & security > Device encryption. If the option is missing or shown as Off, go directly to Part 2. If it is On, continue with Part 1.
Windows 11 Pro	Open Control Panel > System and Security > BitLocker Drive Encryption, then check drive C:. If BitLocker is Off, go directly to Part 2. If BitLocker is On, continue with Part 1.
Quick CMD check	Open Command Prompt as administrator and run: <code>manage-bde -status C:</code> . If the status shows Protection Off or Percentage Encrypted: 0.0%, go directly to Part 2.

Decision to take

BitLocker / Device Encryption disabled: do not run the script, go directly to Part 2.

BitLocker / Device Encryption enabled: keep the recovery key available, then complete Part 1 before Part 2.

Part 1 - Disable BitLocker using the provided script

This part must be performed only if the prerequisite confirms that BitLocker or Device Encryption is enabled. If BitLocker is already disabled, go directly to Part 2.

1	Copy the Disable_BitLocker_manage-bde.bat file to the Desktop of the affected PC or to an easily accessible folder.
2	Right-click Disable_BitLocker_manage-bde.bat, then select Run as administrator.
3	If Windows displays a User Account Control prompt, click Yes.
4	The script displays the BitLocker status before any action. When it asks for confirmation, type O, then press Enter.
5	The script runs the command <code>manage-bde -off C:</code> . If the status shows decryption in progress, keep the PC powered on and connected to AC power until completion.
6	To check the status later, open Command Prompt as administrator and run: <code>manage-bde -status C:</code> .

Command executed by the script

```
manage-bde -off C:
```

Manual status check

```
manage-bde -status C:
```

BitLocker warning

Do not force shutdown the PC during decryption.

Do not continue with the next part of the procedure until encryption is fully disabled or until the status is clear.

Keep the BitLocker recovery key available. It may be requested if Windows detects a security, BIOS, TPM or startup change.

The script targets the system drive C:. Do not use it without confirmation if Windows is installed on another drive.

Part 2 - Temporarily disable Windows driver signature enforcement

This part starts Windows once with mandatory driver signature enforcement disabled. This setting is valid for the current session only. [Please follow the steps in the attached video.](#)

1	Open Settings > System > Recovery.
Alternative	Right-click the Windows Start button, select Shut down or sign out, press and hold Shift, then click Restart.
2	Under Advanced startup, click Restart now.
3	After reboot, select Troubleshoot.
4	Select Advanced options.
5	Select Startup Settings.
6	Click Restart.
7	When Startup Settings appears, press F7 or 7 on the keyboard: Disable driver signature enforcement.
8	Windows starts with driver signature enforcement disabled for this session only.
9	Install or relaunch the affected Mediacpteurs driver.
10	Restart the PC normally to automatically re-enable Windows protection.

Remember: after every full PC restart, Windows automatically re-enables driver signature enforcement. If the driver must be installed or relaunched in this mode, this part of the procedure must be performed again.

Final checks and support note

1	BitLocker / Device Encryption status was checked before any operation.
2	If BitLocker was enabled, the script was run as administrator and the status of drive C: was checked.
3	The PC was restarted using Windows Advanced Startup.
4	The F7 / 7 option was selected to temporarily disable driver signature enforcement.
5	The Mediacapture driver was installed or relaunched during this Windows session.
6	After a normal restart, Windows protection is automatically re-enabled.

Support note

If the workaround fails, do not attempt unrelated system changes.

At this stage the remaining solution is to wait for Microsoft to validate the drivers.

This procedure must remain limited to the identified driver blocking issue. It must not be used as a general method for disabling Windows security.