E

Early Launch Anti-Malware (ELAM): How It Works and Fixing Boot Errors

ELAM lets Windows evaluate third-party boot-start drivers before they initialize. Learn how it differs from Secure Boot and how to troubleshoot disabled or failing ELAM protection.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 How ELAM works during Windows startup

02 ELAM driver classifications

03 ELAM vs Secure Boot vs antivirus

04 Why Windows says early launch anti-malware is disabled

05 What “Disable early launch anti-malware protection” does

06 Frequently asked questions

Early Launch Anti-Malware (ELAM) is a Windows security mechanism that allows a specially signed antimalware driver to start before other third-party boot-start drivers. It classifies those early drivers so Windows can decide whether they should initialize. ELAM is designed to block known malicious boot drivers before they gain control at a highly privileged stage of startup.

Short answer: ELAM is an early boot checkpoint, not a complete antivirus scan. It evaluates boot-start drivers and dependent components, then hands protection over to the normal antimalware service as Windows continues loading.

01 How ELAM works during Windows startup

1. The Windows boot loader loads the operating system's boot-critical components.
2. A registered ELAM driver from the antimalware provider loads in the Early-Launch group.
3. Before each third-party boot-start image initializes, Windows supplies information such as its hash and certificate data to ELAM.
4. The ELAM driver classifies the image.
5. Windows combines that classification with the configured driver-load policy to decide whether initialization is allowed.
6. After boot drivers are handled, the ELAM component unloads and the full runtime security service takes over.

02 ELAM driver classifications

Classification	Meaning	Typical default treatment
Known good	The security provider recognizes the driver as trusted	Allowed to initialize
Known bad	The driver matches known malicious data	Blocked

Classification	Meaning	Typical default treatment
Bad but boot-critical	Malicious or untrusted, but blocking it may stop Windows from booting	Handled according to policy
Unknown	There is not enough trusted classification data	Allowed or blocked according to policy

The exact result depends on Windows policy and the antimalware provider. A stricter policy can improve control but may also prevent startup when a legitimate boot driver is unknown or misclassified.

03 ELAM vs Secure Boot vs antivirus

Control	Main purpose
Secure Boot	Verifies trusted signatures in the firmware-to-Windows boot chain
ELAM	Classifies early third-party boot drivers before they initialize
Runtime antivirus or EDR	Scans files, processes, memory, behavior, and activity after the operating system loads

These controls complement one another. Secure Boot being enabled does not prove ELAM is healthy, and ELAM cannot replace ongoing endpoint monitoring. For related startup threats, see bootkit malware and rootkits.

04 Why Windows says early launch anti-malware is disabled

The message may reflect a missing, corrupt, outdated, or incompatible security driver; an incomplete antivirus installation or removal; a policy change; damaged Windows files; or a reporting problem in device-health or management tooling. It does not automatically prove that malware disabled ELAM.

Safe troubleshooting sequence

1. **Record the exact message.** Note the driver filename, security product, error code, and whether the report came from Windows Recovery, Event Viewer, or a management platform.
2. **Restart normally once.** A stale compliance result after hibernation or an incomplete update can clear after a full restart.
3. **Update Windows and the security product.** Obtain drivers and repair tools only from the operating-system, computer, or security vendor.
4. **Check the security product's health.** Confirm that its services and real-time protection are running and that installation or removal did not stop midway.
5. **Review recent driver changes.** Roll back or replace the specific newly installed driver when evidence points to it.
6. **Repair Windows components.** Use supported Windows recovery and system-file repair options before editing boot configuration manually.

05 What “Disable early launch anti-malware protection” does

Windows Startup Settings can offer a one-boot option that bypasses ELAM enforcement. It is intended for diagnosis when an antimalware driver prevents startup. The change is normally temporary for that boot; it is not a repair and it reduces protection during a sensitive startup phase.

If the system boots only with ELAM disabled, identify and repair or remove the incompatible security driver before returning the device to normal use. Do not repeatedly use the bypass on a production system, and do not weaken Secure Boot or driver policy simply to hide the symptom.

06 Frequently asked questions

Is ELAM included in Windows 10 and Windows 11?

Yes. ELAM is part of the Windows boot-protection architecture and works with compatible registered antimalware software.

Can ELAM scan every file on the disk?

No. Its narrow job is to classify boot-start drivers early. Full disk, memory, and behavior scanning occurs through other security components.

Does an ELAM error mean the PC has a rootkit?

Not by itself. Malware is one possibility, but incompatible updates, corrupt drivers, incomplete uninstallations, and reporting errors are also common causes. Investigate the named driver and surrounding changes.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com