AutoKMS: What it is, why it’s risky, and how to remove it

Gridinsoft Help Center

What it is

AutoKMS is riskware-tools that try to fake-license Windows or Office. They often tweak system services and security settings to keep the "activation" alive. That shortcut can open bigger problems: malware bundles, blocked updates, and weakened protection. See details in the AutoKMS threat guide.

Why it’s risky

- Malware piggybacking: many activators come wrapped with trojans or stealers.
- Weakened security: scripts may disable Defender, add exclusions, or stop updates.
- Privacy & trust: tampered systems are harder to audit and easier to abuse.

What you may notice

- Security tools turned off or exclusions added
- Strange scheduled tasks/services named like system components
- Activation pop-ups replaced by other errors or instability

Clean up (quick steps)

- Uninstall the activator and delete its tasks/services.
- Run a full anti-malware scan and reboot.
- Re-enable updates and security features; remove AV exclusions.
- If needed, repair/restore Windows components and re-activate with a legit license.

Prevent it

- Avoid "free" activators; use genuine licensing or approved volume activation.
- Keep Windows and Office updated; don’t disable protection to run scripts.
- Download software only from official sources.