A

AutoKMS: What the Detection Means and How to Remove It Safely

AutoKMS is an unauthorized Microsoft activation tool commonly detected as HackTool or Riskware. Learn why it returns, how to remove scheduled activation components, and verify licensing.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 How to interpret an AutoKMS detection
02 AutoKMS vs legitimate KMS activation
03 Why AutoKMS is risky
04 How to remove AutoKMS safely
05 Why AutoKMS keeps coming back
06 If AutoKMS already ran
07 How to check whether Windows is genuine
08 Frequently asked questions
09 References

AutoKMS is a category of tools that emulate or abuse Microsoft Key Management Service (KMS) activation to activate Windows or Office without an authorized license. Microsoft Defender commonly detects these tools as `HackTool:Win32/AutoKMS`, `HackTool:MSIL/AutoKMS`, or a related variant. Other products may use Riskware, CrackTool, or PUA labels.

The hack-tool label describes the activation bypass; it does not mean every sample is identical. AutoKMS packages are distributed through cracks, repacks, torrents, and unofficial repair shops, and may arrive with password stealers, miners, backdoors, or unwanted software. Keep the item quarantined and review every additional detection separately.

01 How to interpret an AutoKMS detection

Detection context	Likely meaning	Response
HackTool or AutoKMS only, blocked before execution	An unauthorized activation tool was found	Remove it and activate through a legitimate license
AutoKMS returns on a schedule	A scheduled task, service, startup item, or exclusion remains	Remove the persistence and rescan
Trojan, stealer, RAT, miner, or ransomware also appears	The package likely included a separate malicious payload	Isolate the device and perform incident response
Tool was installed by a repair shop or seller	Windows or Office licensing may not be genuine	Preserve purchase records and verify activation with Microsoft or the seller
Authorized enterprise KMS client is present	Normal volume activation does not require AutoKMS cracking tools	Ask the IT team to validate the genuine KMS configuration

02 AutoKMS vs legitimate KMS activation

KMS is a legitimate Microsoft volume-activation method used by organizations. Managed clients contact an authorized organizational KMS host and periodically renew activation. AutoKMS tools imitate or redirect that process on devices that are not entitled to the corresponding volume license.

- A legitimate consumer installation activates with a digital license or product key tied to an authorized purchase.
- A legitimate work device may activate through the organization's KMS or another supported volume-activation method.
- An AutoKMS crack commonly creates a local emulator, service, script, scheduled task, altered configuration, or security exclusion.

Do not assume that any file named KMS is malicious. Confirm the signer, path, organization, activation channel, and exact detection. Likewise, a successful activation message does not prove that an AutoKMS package is safe or licensed.

03 Why AutoKMS is risky

- Packages often instruct users to disable antivirus protection or add exclusions.
- Administrator privileges let the tool change services, tasks, licensing files, firewall rules, and security settings.
- Crack distributors can replace a previously working package with malware while keeping the same name.
- Repeated activation creates persistence that resembles or can conceal malicious behavior.
- Unauthorized licensing can disrupt updates, support, compliance, resale, and organizational audits.

04 How to remove AutoKMS safely

1. **Keep detections quarantined.** Record the full paths, hashes, detection names, times, and whether the tool executed.
2. **Disconnect if other malware is detected.** Use endpoint isolation or take the computer offline when a stealer, RAT, ransomware, or suspicious remote-access tool appears.
3. **Update Defender and run a full scan.** Use Microsoft Defender Offline if the detection returns, protection was disabled, or persistence is suspected.
4. **Remove the original package.** Delete the crack, archive, disk image, installer, and extracted folder from Downloads, email, cloud sync, or torrents.
5. **Review persistence.** Inspect scheduled tasks, services, startup items, recently installed applications, security exclusions, and firewall changes created at the same time. On a managed device, preserve evidence and let IT make changes.
6. **Uninstall unauthorized software.** Remove the cracked Office or Windows installation when required, then reinstall from Microsoft's official channel or an approved organizational source.
7. **Activate legitimately.** Use the digital license, authorized retail key, or employer/school volume activation to which the device is entitled.

05 Why AutoKMS keeps coming back

AutoKMS is often designed to run repeatedly because unauthorized KMS activation must be renewed. A scheduled task or service can recreate a detected file after quarantine. The source may also remain inside an archive, backup, synchronized folder, Recycle Bin, or installer cache.

Compare the path and hash of each alert. Remove the persistence and source, not Defender's internal Protection History or quarantine folders. If the alert action remains incomplete, update protection, restart when prompted, run a full scan, and then use Defender Offline.

06 If AutoKMS already ran

Review whether security was disabled, exclusions were added, administrator credentials were entered, or other payloads executed. From a known-clean device, revoke sessions and change passwords used or stored on the affected computer when credential theft is possible. Reimage from trusted media if a backdoor, stealer, rootkit, or ransomware ran, or if system trust cannot be restored.

07 How to check whether Windows is genuine

- Open Windows Settings and review the Activation page rather than relying on a third-party script.
- Confirm that the installed edition matches the license you purchased.
- For a work or school device, ask the administrator to verify the activation channel and KMS host.
- If a seller promised a genuine license, keep the invoice and contact Microsoft or the marketplace about a counterfeit installation.

08 Frequently asked questions

Is HackTool:Win32/AutoKMS a virus?

It is primarily a hack-tool detection for unauthorized activation, not a self-replicating virus. The package can still contain separate malware, so review all detections and behavior.

Can I allow AutoKMS if Windows is already activated?

No. Remove the tool and persistence, then verify that activation is backed by a valid entitlement. Allowing it maintains unnecessary privileged software and security exceptions.

Will removing AutoKMS deactivate Windows or Office?

Unauthorized activation may expire after removal. That is expected; activate with a legitimate digital license, key, subscription, or organizational method.

09 References

- Microsoft Security Intelligence: AutoKMS detections
- Microsoft: protect your PC from unwanted software

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