GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

D

Data Execution Prevention (DEP) in Windows

Learn how Windows DEP and the processor NX bit block code execution from data memory, how to check DEP, and why disabling it is risky.

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Oct 8, 2026	4 min

CONTENTS

In this guide

01 What does DEP do?

02 How hardware-enforced DEP works

03 What DEP can and cannot stop

04 How to check DEP status in Windows

05 DEP options and application compatibility

06 Should you disable DEP?

07 DEP, NX, ASLR, and antivirus

08 What to do after a DEP alert or crash

Data Execution Prevention (DEP) is a Windows memory-protection feature that marks selected memory pages as non-executable. If a process attempts to run code from a protected data page, Windows raises an access-violation exception and normally terminates the process.

DEP makes common memory-corruption attacks harder, especially attempts to execute injected code from a stack or heap. It is one layer of exploit mitigation, not an antivirus and not a replacement for software updates.

01 What does DEP do?

DEP asks the processor and operating system to prevent instructions from running in memory pages intended only for data. A legitimate program can still request executable memory when needed, but an injected payload placed in a protected stack or heap page cannot simply run. DEP stops that execution path; it does not remove the vulnerable program or prove that the process is otherwise safe.

02 How hardware-enforced DEP works

Modern processors provide a no-execute capability known as NX on AMD systems and XD or execute-disable on Intel systems. Windows uses that processor feature to distinguish memory intended for data from memory permitted to contain executable instructions.

Legitimate applications that generate code at runtime, such as just-in-time compilers, must request appropriate memory permissions. Old or incorrectly written applications may crash when they try to execute code from a data-only page.

03 What DEP can and cannot stop

DEP can block a payload that depends on executing instructions in non-executable data memory. It does not repair the underlying buffer overflow, prevent every control-flow attack, detect phishing, or stop an attacker who already has permission to run a normal executable. Techniques such as return-oriented programming may reuse existing executable code instead of placing new code in a data page.

DEP works best with Address Space Layout Randomization (ASLR), Control Flow Guard, least privilege, endpoint monitoring, and prompt patching.

04 How to check DEP status in Windows

Open PowerShell and query the operating-system properties:

```
Get-CimInstance Win32_OperatingSystem |
  Select-Object DataExecutionPrevention_Available,
                DataExecutionPrevention_Drivers,
                DataExecutionPrevention_SupportPolicy
```

`DataExecutionPrevention_Available` should report `True` when hardware DEP is available. The support-policy values are 0 for AlwaysOff, 1 for AlwaysOn, 2 for OptIn, and 3 for OptOut. Enterprise policy and Windows version can affect the effective settings for individual processes.

05 DEP options and application compatibility

Older Windows interfaces describe OptIn as DEP for essential Windows programs and services and OptOut as DEP for all programs except selected exceptions. Current systems also expose process mitigations through Windows Security and administrative policy. Before changing settings, confirm the affected executable and review vendor guidance.

If a trusted legacy application fails with DEP, update or replace it first. An exception weakens protection for that process and should be narrowly scoped, documented, and removed after the compatibility issue is fixed.

06 Should you disable DEP?

Do not disable DEP globally to troubleshoot one crash. A DEP-related exception can indicate incompatible software, corrupted files, or an active exploitation attempt. Capture the application name and event details, scan the system, install vendor updates, and test the application in a controlled environment.

Commands that alter boot-wide mitigation policy can reduce protection for every process and may conflict with organizational controls. Use them only under documented vendor or administrator direction with a rollback plan.

07 DEP, NX, ASLR, and antivirus

- **DEP/NX** restricts where instructions can execute in memory.
- **ASLR** randomizes the location of executable code and data structures.
- **Control-flow protections** restrict unexpected jumps or calls.
- **Antivirus or EDR** analyzes files, processes, behavior, and other signals.

These controls address different parts of an attack. A system needs layered defenses because no single mitigation blocks every exploit.

08 What to do after a DEP alert or crash

1. Record the process, time, user, error, and recent activity.
2. Update Windows and the affected application from official sources.
3. Run a security scan and review child processes, persistence, and network connections.
4. Test whether the crash reproduces with a clean profile or known-good installation.
5. If exploitation is suspected, isolate the device and follow incident-response procedures rather than creating a DEP exception.

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