



Toshiba EasyGuard™ Secure: Executable Disable Bit

Toshiba EasyGuard™ is the better way to enhanced data security, advanced system protection and easy connectivity. This next-generation computing experience incorporates technologies enabling optimal connectivity and security, Toshiba anti-accident innovations and advanced software utilities for carefree mobile computing.

The 32-bit version of Windows (beginning with Windows XP Service Pack 2 uses the XD-Bit feature as defined by Intel when the notebook processor is running in Physical Address Extension (PAE) mode.

Toshiba EasyGuard™ Four core elements for more confident computing

Protect & Fix

Fortifies vital information and vulnerable components against the stress and hazards mobile computers are exposed to every day.

Connect

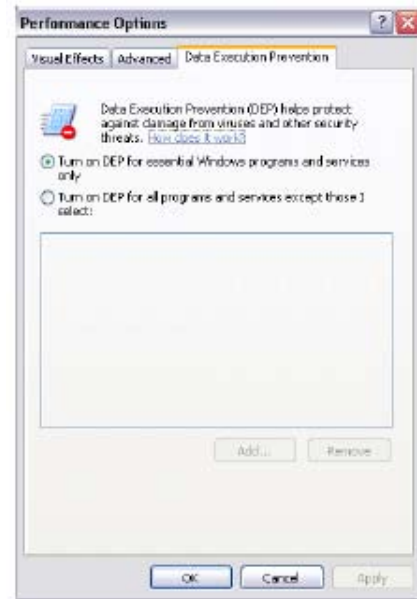
Helps you locate and establish a wired or wireless connection effortlessly and quickly.

Secure

Helps defend your data and your Notebook against loss, theft or viral attack.

Optimise

Allows you to customise the Notebook's system performance so you can be more productive.



What is Execute Disable Bit (XD-Bit)?

Execute Disable Bit (XD-Bit) is a system feature that, if present and enabled, allows the notebook's processor to distinguish between bits of code that should be executed and the ones that cannot be executed because they pose a threat to the system.

When a malicious worm attempts to insert code into the buffer, the processor disables the code execution, preventing damage or worm propagation. In other words, even if infected code is present on the notebook, as long as the processor does not execute it, the code cannot cause any damage. This process of disabling the code execution is called Data Execution Protection or DEP.

What is hardware-enforced DEP and how does it work?

The DEP process can be either hardware-enforced, which requires hardware support, or software-enforced, which provides additional exception handling checking and does not require specific hardware support. Hardware enforced DEP requires a processor capable of executing the feature as defined by Intel for the XD-Bit.

DEP marks all processor memory locations as non-executable unless the location explicitly contains executable code. One class of security attacks attempts to insert and execute code from non-executable memory locations. DEP helps prevent these attacks by intercepting such attempts and raising an exception. DEP also relies on processor hardware to mark memory locations with an attribute indicating that code should not be executed from that location. Windows XP Service Pack 2 recognises this exception and prevents that code from executing.

DEP Configurations for Windows XP SP2

- Opt-in:** DEP is enabled by default for limited system applications and software applications that 'opt-in' and is available on systems with processors capable of hardware-enforced DEP. Technical support may enable DEP for additional applications.
- Opt-out:** DEP is enabled by default for all processes. Users can manually create a list of specific applications that are not DEP-enabled by using System Properties.
- Always On:** Full coverage for the entire system and all processes run with DEP enabled. It is not possible to 'opt-out' of DEP.
- Always Off:** There is no DEP for the system.

Summary of features and benefits

Feature	Benefit
Execute Disable Bit (XD-Bit)	Prevention of buffer overflow virus attacks by enabling the system processor to distinguish between code that can and cannot be executed
Data Execution Protection (DEP)	Process that allows the system processor to disable code execution, thereby preventing virus damage or worm propagation
Four DEP configurations	User flexibility.