Data Execution Prevention

v1.2

Based upon Microsoft TechNet article "Changes to Functionality in Microsoft's Windows XP Service Pack 2," dated August 9, 2004, by Starr Anderson & Vincent Abella.

Introduction

Microsoft's Windows XP Service Pack 2 introduces a set of security technologies that will help improve the ability of computers running Windows XP to withstand malicious attacks, especially those from viruses and worms such as Code Red, Blaster and Sasser.

F-Secure Corporation's Data Security Summary for 2004 reports that there are now in excess of 100,000 recognized viruses, with Sasser being the most recent major epidemic. Released in May 2004, this automatic network worm quickly spread, and reportedly affected three major banks, an Australian Railroad, county hospitals in Sweden, and the European Commission in Brussels, to name a few.

Microsoft's Windows XP Service Pack 2 includes multiple security improvements:

- Network protection
- Memory protection
- Email handling
- Web browsing security
- Computer maintenance

Together, these security technologies help to make it more difficult to attack Windows XP, even if the latest antivirus updates are not applied.

This paper focuses on the aspect of memory protection and how Data Execution Prevention helps lock down the ability for malicious code to propagate through the network. However, you should expect some application behaviors to be incompatible with Data Execution Prevention. Applications that perform dynamic code generation (such as Just-In-Time code generation) that do not explicitly mark generated code with Execute permission may have compatibility issues with Data Execution Prevention.

HP recommends that customers test Windows XP Service Pack 2 before wide scale deployment in their environment.

Data Execution Prevention (DEP)

What does Data Execution Prevention do?

Data Execution Prevention (DEP) is a set of hardware and software technologies that perform checks on memory to help protect against malicious code and viruses. In Windows XP SP2, DEP is enforced by both hardware and software.

Data Execution Prevention Exception Message Box

If an application or driver attempts to execute code from an area where it should not on a DEP-protected computer, Windows displays the following exception error:

Hardware-Enforced DEP

Hardware-enforced DEP marks all memory locations as non-executable (you cannot execute code in this portion of memory) unless the location explicitly contains executable code. There is a class of attacks that attempts to insert and execute code from non-executable memory locations. DEP helps prevent these attacks by intercepting them and displaying the DEP message box.

Hardware-enforced DEP relies on processor hardware to mark memory with an attribute that indicates that code should not be executed from that memory. The actual hardware implementation of DEP varies by processor architecture. However, processors that support hardware-enforced DEP are capable of raising an exception when code is executed from a memory location where it should not be executed.

Both Advanced Micro Devices™ (AMD) and Intel® Corporation have defined and shipped Windows-compatible architectures that support DEP. Beginning with Windows XP Service Pack 2, the 32-bit version of Windows utilizes the no-execute page-protection (NX) processor feature as defined by AMD and the Execute Disable (XD) bit feature as defined by Intel. AMD also refers to this feature as "Enhanced Virus Protection." To use these processor features, the processor must run in Physical Address Extension (PAE) mode. HP ships Windows XP with PAE enabled.

What is PAE?

The XD and NX features require that the processor run in Physical Address Extension (PAE) mode. A 32-bit processor, such as the Intel Pentium 4 (IA32 family), is usually limited to addressing a maximum of 4-GB of memory. This limitation is due to 32 bits of address capability, as follows:

2^{32} = 4,294,967,296 (4 GB)

To address more than 4-GB of memory, Intel created PAE mode. PAE uses an additional 4 bits of addressing, creating a 36-bit address, thereby allowing for the addressing of up to 64-GB of memory, as follows:

2^{36} = 68,719,476,736 (64 GB)

A processor with XD or NX marks memory pages as nonexecutable. This marking consists of a bit in the Page Table Entry (PTE), which is a data structure containing the base physical address and attributes of a page in physical memory. When you use PAE mode, the PTEs are extended from 32 bits to 64 bits, allowing for the additional space required to mark an area as nonexecutable.

Why is this change important? What threats does it help mitigate?

The primary benefit of Data Execution Prevention is the prevention of code execution from data pages such as the default heap, various stacks, and memory pools. A heap is a common pool of memory available to a program. A stack is a set of hardware registers or a reserved amount of memory used for arithmetic calculations or to keep track of internal operations.

In normal system operations, code is not typically executed from the default heap and stack. Hardware-enforced DEP detects code that is running from these locations and raises an exception when execution occurs. If the exception is unhandled, the process is terminated. Execution of code from protected memory in kernel mode results in a bugcheck.

Although terminating a process or causing the system to fail with a bugcheck do not appear to be ideal solutions, they help prevent malicious code from executing. Preventing malicious code from executing on the system may prevent damage to your system or propagation of malicious code whose harmful effects could easily exceed those of a process terminated by a bugcheck.

DEP can help mitigate against a class of security exploits. Specifically, Data Execution Prevention can prevent the exploit in which a virus or other attack injects a process with additional code and then attempts to execute the injected code. On a system with DEP, execution of the injected code results in an exception. Additionally, software-enforced DEP can help mitigate against exploits of exception handling mechanisms within Windows.

A secondary benefit of DEP encourages good engineering and best practices for application and driver developers. Data Execution Prevention forces developers to avoid executing code out of data pages without explicitly marking the pages as executable.

Will my NX- or XD-enabled systems protect me from virus attacks?

XD and NX are promising technologies, but they do not protect against all attacks. You should use XD and NX with antivirus software, firewall, and other security measures to reduce the propagation of viruses and limit the amount of damage they can create.

What are the required components for XD/NX to function?

To take advantage of the XD/NX feature, the following components must support XD/NX:

- Processor
- System BIOS
- Operating system

Processor

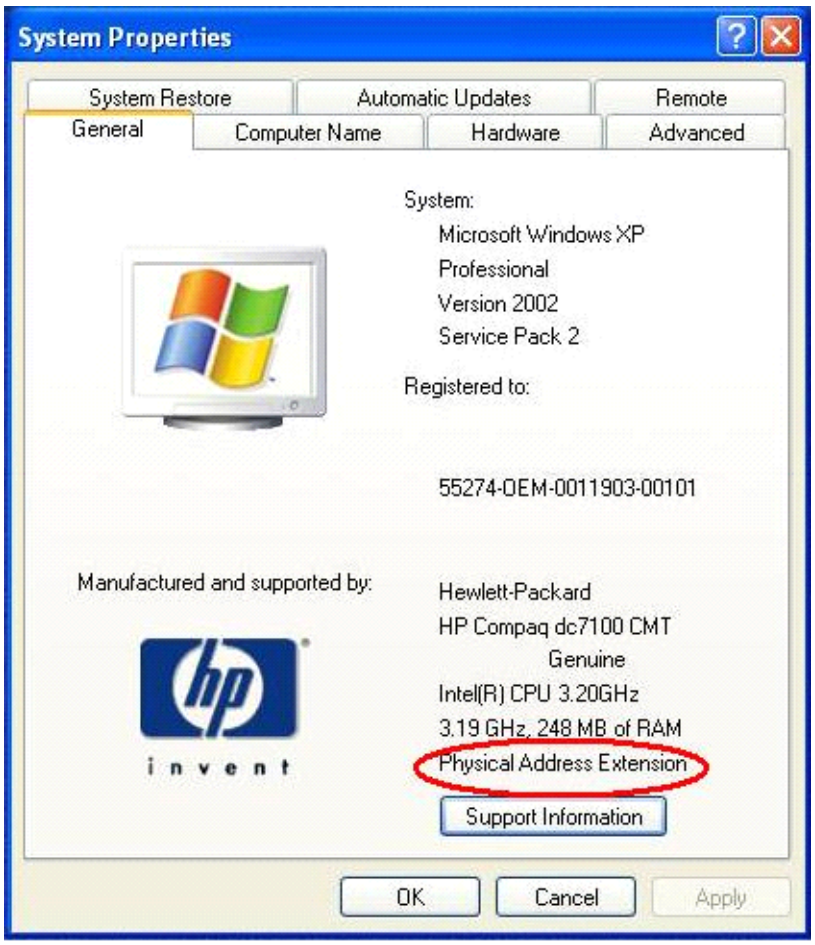
Intel released XD-capable processors for the desktop market starting with the E0 stepping of the "Prescott" Pentium 4 processor. Both Intel Pentium 4 and Celeron processors have XD support. Using Intel's new processor naming scheme, all 6xx, 7xx, and 8xx processors support XD. A majority of 5xx and 3xx processors also support XD.

AMD has released a line of AMD64 processors (Athlon 64, Athlon 64 FX, Turion 64 Mobile Technology, Mobile Athlon 64) which support NX.

Transmeta Efficeon processors using Code Morphing Software (CMS) 6.0.4 or later support NX. Both Intel and AMD have a Windows-compatible method of implementing XD/NX, but their hardware implementation is different. Transmeta Efficeon processors use a virtual implementation compatible with the AMD implementation.

How do I know if I have an XD- or NX- capable processor?

The System Properties window indicates whether PAE is enabled on systems installed with Windows XP SP2 that also have an XD- or NX-capable processor.



System BIOS

- Default XD support is disabled for Intel 915 2004 systems.
- Default XD support is enabled for Intel 945 2005 systems.
- Default NX support is enabled for AMD 2005 systems.
- Default NX support is disabled for Transmeta systems.

The BIOS for Intel 915 and Intel 945 based desktop systems uses the CPUID instruction to look for the Execute Disable bit to determine if XD is supported with the installed processor. If the processor supports XD, then the **Data Execution Prevention** option appears in the Security section of F10 Setup. The user can enable or disable this feature.

AMD processors currently do not have an option to manually disable DEP in F10 Setup. Transmeta processors currently do not have an option to manually enable DEP in F10 Setup.

The **Data Execution Prevention** option is disabled by default in i915-based systems, and enabled by default in i945-based systems. Applications and drivers run without compatibility problems when the XD feature is not enabled.

HP uses the i915 chipset desktop BIOS family in the following product lines (not all systems available in all regions):

- dc5100
- dx6100
- dc7100

HP uses the i945 chipset desktop BIOS family in the following product lines (not all systems available in all regions):

- dc7600
- dx7200

HP uses the ATI Radeon Xpress 200 chipset desktop BIOS family for AMD processors in the following product line (not all systems available in all regions):

- dx5150

The BIOS for the bc1000 disables NX support for the Transmeta processor. There is no option to enable NX.

The following workstations and associated chipsets also support DEP (not all systems available in all regions):

- HP Workstation xw4200 – Intel 925X chipset
- HP Workstation xw6200 – Intel E7525 chipset
- HP Workstation xw8200 – Intel E7525 chipset

These workstations disable DEP by default. However, you can manually enable DEP in BIOS.

Operating System

Microsoft implemented XD/NX support with Windows XP Service Pack 2. All future Microsoft operating systems, including the upcoming "Longhorn" operating system, will have XD/NX support. Previous operating systems do not support the XD/NX features.

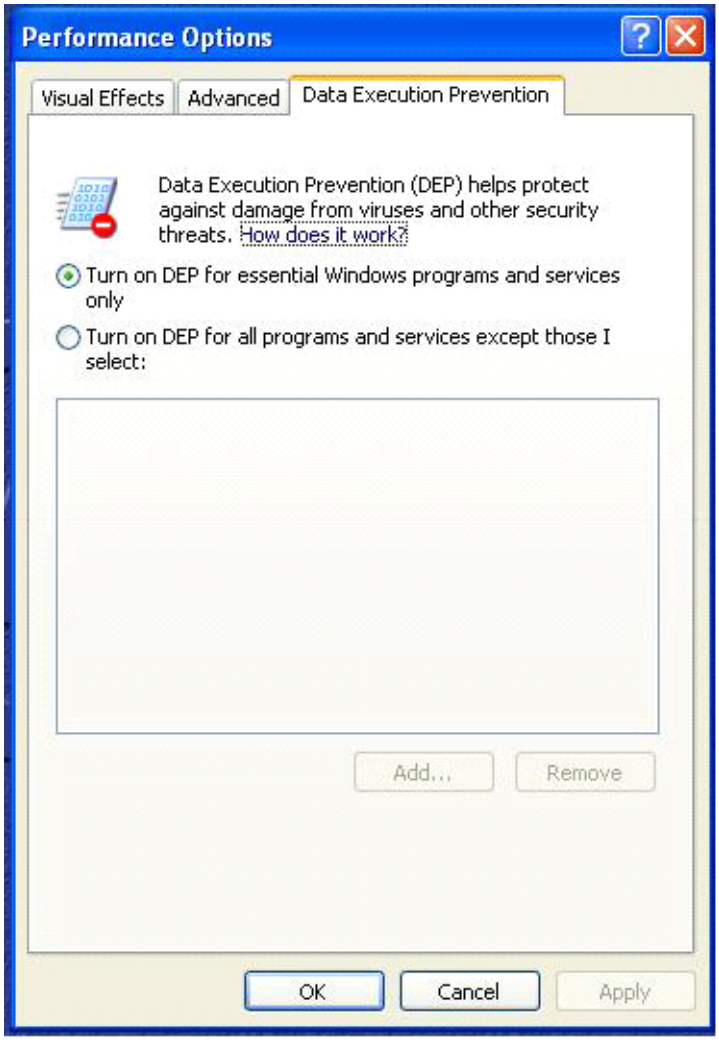
How do I control the DEP functionality on my computer?

Systems installed with Windows XP SP2 include a Data Execution Prevention tab, located at **System Properties > Advanced**. This tab allows the user to enable DEP for either:

- Essential Windows programs and services only - This option equates to the OptIn policy. Applications can enable DEP protection by creating a compatibility shim (a small piece of software added to a program to provide an enhancement) and installing it with the application.
- All program and services except those I select - This option equates to the OptOut policy, which allows a user to select applications for DEP not to affect. This manual application exclusion is useful in working around applications or drivers that do not load or function properly because of DEP.

NOTE: HP ships with Windows XP set to Optin. To prevent Windows XP SP2 from using DEP, set **/NOEXECUTE** to "`alwaysoff`" in the BOOT.INI file.

The following image shows the Data Execution Prevention tab on a system with an XD/NX-enabled processor.



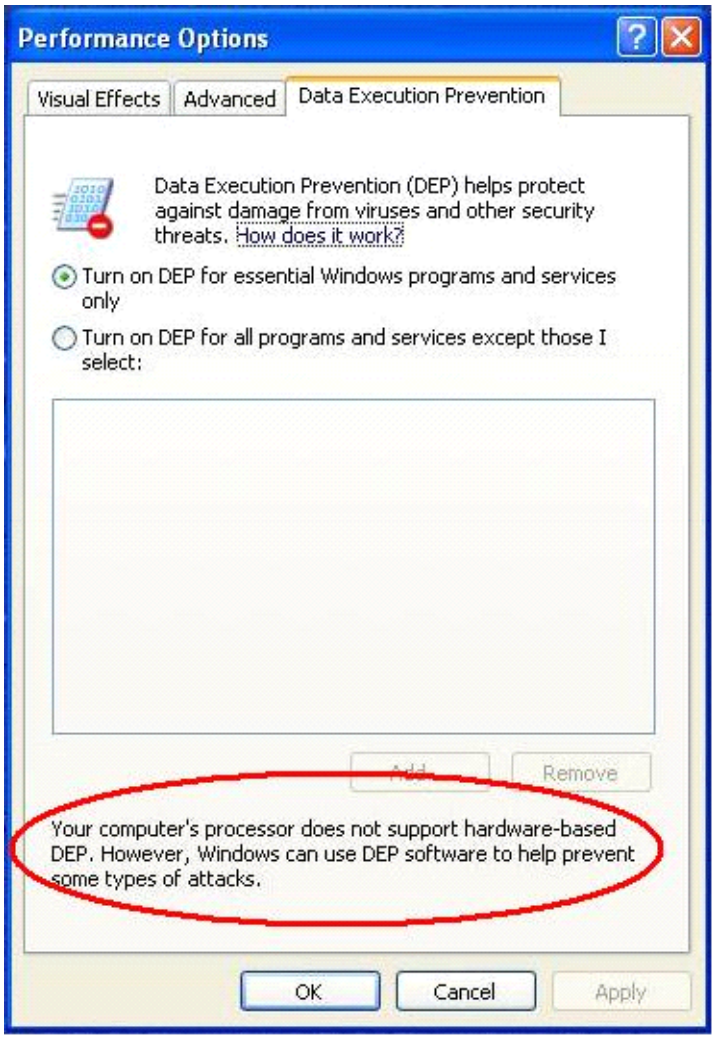
DEP Level Chart

Processor Support	BIOS DEP Setting	OS BOOT.INI Setting	Result
No	N/A	Any Setting	Only software-enforced DEP is available for limited Windows system binaries.
Yes	Disabled	Any Setting	Only software-enforced DEP is available for limited Windows system binaries.
Yes	Enabled	Always On	• Hardware and software-enforced DEP coverage for all Windows binaries, programs, and drivers. • No programs or drivers can be exempted. • System Compatibility Fixes (shims) for DEP do not take effect.
		Always Off	• No hardware or software-enforced DEP is available for any part of the system. • The processor will not run in PAE mode unless a /PAE switch is present in the BOOT.INI.
		OptIn (Default)	• Hardware and software-enforced DEP coverage for limited Windows system binaries by default. • Programs and drivers can be covered by both DEP and NX if they explicitly specify to be covered (opt-in) by creating a shim. • This is the default configuration in the BOOT.INI.
		OptOut	• Hardware and software-enforced DEP coverage for all Windows system binaries, programs, and drivers. • You can exempt programs and drivers if you explicitly specify they are not covered (opt-out). • System Compatibility Fixes (shims) for DEP take effect.

Data Execution Prevention Tab - No XD/NX Processor

The following image shows the Data Execution Prevention tab on a system without an XD/NX-enabled processor. Windows notifies the user that the system does not contain a processor capable of XD/NX, but that software-enforced DEP is available.

NOTE: To prevent Windows XP SP2 from using DEP, set the operating system to `/alwaysoff` in the BOOT.INI file.



Software-Enforced DEP

Software-enforced DEP is a set of DEP security checks built into Windows XP SP2 that can be used with any processor that supports Windows XP SP2. Software-enforced DEP is a more limited form of protection for the exception handling mechanisms in Windows. It is used when hardware-enforced DEP is not available, usually because the processor does not support XD/NX or is disabled in BIOS.

If a program was built with Safe Structured Exception Handling (SafeSEH), then software-enforced DEP can determine if the exception handler is registered in the function table located within the program image file before an exception is dispatched. If a program is not built with SafeSEH, then software-enforced DEP checks whether the exception handler is located within a memory region marked as executable before an exception is dispatched.

Deploying Hardware-Enabled Data Execution Prevention

How will XD/NX impact HP customers?

HP tests its images and deliverables for XD/NX compatibility, including:

- Shipping HP applications
- Operating system image
- Shipping peripheral drivers
- Popular applications and games

Ideally, you should test both hardware and software-enforced DEP. Unfortunately, at this time you can only test hardware-enforced DEP, because Microsoft has not yet supplied the tools to test software-enforced DEP.

You can test hardware-enforced DEP with specialized tests that actively try to execute from data memory space or real world applications. For information about applications that do not function when XD/NX is disabled, see "Known Issues" on page 13.

What about customers who create their own software image?

HP encourages you to perform your own validation if you plan to use proprietary images or software. You should test the following areas to ensure compatibility with DEP:

- Third party drivers
  - Video
  - Network
  - Printer
  - Modem
- Third party applications
  - Benchmarks
  - Productivity Software
  - Games

Customers who set the policy level in BOOT.INI to **AlwaysOn** may encounter multiple software incompatibilities. You cannot exclude applications and drivers from DEP with the **AlwaysOn** policy level.

Advantages of using XD/NX

Enabling XD/NX provides increased protection against viruses that use buffer overflow attacks. This increased protection provides the benefit of increased network security as malicious code cannot propagate or spread to infect more computers. Support staff also benefits from much improved containment and easier eradication of unwanted software.

Disadvantages of using XD/NX

XD/NX compatibility issues can occur for both applications and drivers. Applications that perform dynamic code generation, such as just-in-time (JIT) code generation, that do not mark the generated code with Execute permission, will experience compatibility issues.

Drivers can encounter compatibility issues when running on 32-bit systems with PAE mode enabled. There are several reasons for this:

- Driver does not load because it cannot perform 64-bit addressing.
- Driver does not load because it assumes PAE mode requires more than 4-GB of memory.
- Driver causes problem when it expects a 32-bit PTE, but instead gets a 64-bit PTE.
- Driver cannot DMA properly with a 64-bit physical addresses.

To a lesser extent, some drivers create code in real time. These drivers encounter the same problem as applications that create code in real time as mentioned above.

Conclusion and Recommendation

XD/NX is a useful computer architecture innovation that will reduce the number of viruses that exploit buffer overruns. HP encourages customers who use custom images or third-party software to test software for XD/NX compatibility. Customers have full control as to whether to use XD/NX, either by enabling or disabling XD/NX from the BIOS (F10 Setup), or from the operating system (BOOT.INI).

HP is shipping the following for which the noexecute policy level in BOOT.INI will remain at the default state of OptIn:

- i915 chipset desktop systems with XD disabled in F10 Setup.
- i945 desktop systems with XD enabled by default in F10 Setup.
- Transmeta processor bc1000 computers with NX disabled by default in BIOS.
- AMD processor-based ATI desktop computers with NX enabled by default in BIOS.

To manually turn off DEP, change the state to `/alwaysoff` in the BOOT.INI.

Known Issues

The following table provides a list of drivers and applications for which HP has discovered XD compatibility issues during testing. The table also provides a list of Microsoft Knowledge Base articles that address incompatibilities Microsoft has found during testing.

Application	Effect	Workaround/Solution
3DMark 2001 SE.	Exception error.	Add to exclusion list.
3DMark 2003 SE.	Exception error.	Add to exclusion list.
Adobe Reader 6.0.	Long time to load.	Add to exclusion list.
Adobe Reader 7.0.	Exception error.	Add to exclusion list.
Altiris Deployment Solution Agent.	Does not work properly.	Add to exclusion list.
AMIDIAG Suite 2.0.	Exception error.	Add to exclusion list.
ATI Catalyst Control Center.	Exception error.	Add to exclusion list.
ATI Driver Setup.exe.	Exception error during installation.	Add to exclusion list.
Broadcom Management Apps.	Exception error.	Add to exclusion list.
Content Creation '04 v1.01.	Hang during benchmark.	Add to exclusion list.
CPUID.	Exception error.	Add to exclusion list.
DIVX codec.	Will not install.	Add to exclusion list.
Explorer.exe.	Exception error when opening My Network Places.	Add to exclusion list.
HKCMD (Intel Hotkey).	Exception error.	Add to exclusion list.
HP Diagnostics for Windows.	Exception error.	Add to exclusion list.
IBM Home Page Reader.	Exception error during installation due to Install Shield.	Add to exclusion list for installation, can remove afterwards.
IGFXCFG.EXE module.	Exception error when trying to access Intel Graphics properties.	Add to exclusion list.
Install Shield.	Exception error.	Add to exclusion list.

Application	Effect	Workaround/Solution (Continued)
Intervideo WinDVD.	Exception error during installation and runtime.	Add to exclusion list.
Intervideo WinDVD Creator.	Exception error during installation due to Install Shield.	Add to exclusion list for installation, can remove afterwards.
Java Web Start.	Program does not run, but no exception error.	Add to exclusion list.
JAWS.	Exception error during installation due to Install Shield.	Add to exclusion list for installation, can remove afterwards.
Magazine MM Content Creation Winstone 2004.	Exception error.	Add to exclusion list.
Magic Cursor 2000.	Exception error during installation.	Add to exclusion list.
MAK Software.	Exception error during installation.	Add to exclusion list.
Media Grinder 1.0.	Cannot run Wave, Midi, or MP3 files.	Add to exclusion list.
Microsoft Office Pro 2003.	Exception error.	Add to exclusion list.
Microsoft Office SB 2003.	Exception error.	Add to exclusion list.
Norton Anti-Virus.	Exception error.	Add to exclusion list.
Nvidia Driver Setup.exe.	Exception error during installation.	Add to exclusion list.
PCMark 2004.	Exception error during installation due to Install Shield.	Add to exclusion list for installation, can remove afterwards.
PC Worldbench.	Exception error during installation.	Add to exclusion list for installation, can remove afterwards.
PowerDVD.	Exception error.	Add to exclusion list.
Prime 95.	Exception error.	Add to exclusion list.
Quake 3.	Exception error. If IGD graphics, then shift into 4-bit VGA after the exception.	Add to exclusion list.
Quickbooks.	Exception error.	Add to exclusion list.
Quicken Tour.	Exception error.	Add to exclusion list. Use Quicken Tour v12.1.5.2 C2 or later.

Application	Effect	Workaround/Solution (Continued)
Roxio Cineplayer.	Exception error during installation and runtime.	Add to exclusion list.
Roxio Easy Media Creator.	Exception error during installation and runtime.	Add to exclusion list.
Sysmark 2004.	Exception error during installation and runtime.	Add to exclusion list.
WinDiags.	Exception error.	Add to exclusion list.
Window-Eyes	Exception error during installation due to Install Shield.	Add to exclusion list for installation, can remove afterwards.
Windows Catalog	Exception error.	Add to exclusion list.
Driver	**Effect**	
Creative Audigy 2NX	Exception error during installation.	Add to exclusion list.
HP Deskjet 450ci Driver.	Prints out blank page.	
Microsoft Knowledge Base articles about incompatibilities found during testing:		
http://support.microsoft.com/default.aspx?scid=kb;en-us;884130&Product=winxp		
http://support.microsoft.com/default.aspx?scid=kb;en-us;883775&Product=winxp		
http://support.microsoft.com/default.aspx?scid=kb;en-us;873176&Product=winxp		
http://support.microsoft.com/default.aspx?scid=kb;en-us;878474&Product=winxp		

Frequently Asked Questions

What is XD?

Execute Disable Bit (XD) functionality can prevent certain types of buffer overflow attacks when used with a supporting operating system and system BIOS. XD allows the processor to classify areas in memory where application code can and cannot execute. When a virus or worm attempts to insert code in the buffer, the processor disables code execution, preventing damage or virus or worm propagation.

This feature works with Microsoft's Data Execution Prevention software to help prevent execution of malicious software such as a virus or a worm. The user benefits from increased network security as the malicious code cannot propagate or spread to infect more computers. Support staff also benefits from much improved containment and easier eradication of unwanted software.

What is NX?

NX is the term AMD uses for XD.

What is DEP?

Data Execution Prevention (DEP) is the terminology Microsoft uses for XD and NX. In Windows XP Service Pack 2 (SP2), Microsoft introduced DEP, which is a processor feature that prevents execution of code in memory that is marked as data storage. This limits the "attack surface", specifically for buffer overrun vulnerabilities, where an attacker typically overruns a buffer with code and then executes this code. Unlike a firewall or antivirus program, DEP does not help prevent harmful programs from being installed on your computer. Instead, it monitors your programs to determine whether they use system memory safely.

Windows XP SP2 uses two types of DEP:

- Hardware-enforced DEP - Hardware-enforced DEP provides data protection with hardware (processor) support, requiring use of Windows XP SP2 and a processor that supports XD/NX.
- Software-enforced DEP - Software-enforced DEP is an additional set of DEP security checks built into Windows XP SP2 that can be used with any processor that supports Windows XP SP2. Software-enforced DEP is a more limited form of protection for the exception handling mechanisms in Windows. It is used when hardware-enforced DEP is not available, usually because the processor does not support XD or is disabled in BIOS.

Do they work together or individually?

XD/NX works in conjunction with Microsoft's Data Execution Prevention (DEP) software to help prevent malicious software such as a virus or a worm from executing. The user benefits from increased network security as the malicious code cannot propagate or spread to infect more machines. Support staff also benefit from much improved containment and easier eradication of unwanted software.

How is XD different from NX?

XD and NX are functionally the same, but they use different hardware implementations.

How or where does DEP fit in?

DEP works with XD/NX to help prevent execution of malicious code.

Will an XD or NX processor work without Windows XP SP2?

At this time, XD/NX support requires the following operating systems:

- Windows XP SP2
- Windows Server 2003 SP1
- SUSE Linux 9.2
- Red Hat Enterprise Linux 3 Update 3

What will these technologies do for me?

XD and/or NX potentially reduces the number of viruses that exploit buffer overruns, providing greater overall system security.

What will these technologies change in my systems?

Existing user applications that perform dynamic code generation and do not mark the generated code with Execute permission will encounter problems. Therefore, HP's current deployment strategy is to ship with XD/NX disabled and DEP set for essential Windows programs and services only. Customers are strongly advised to test all end-user applications thoroughly before deploying.

How will these technologies affect my image?

XD/NX will stop any applications or drivers that attempt to execute out of data memory. You should test your images before deploying XD/NX. If a problem does occur with an application/driver associated with a trusted software, you can exclude that software.

Will the new processors, new or updated BIOS, and Windows XP SP2 require a new image qualification?

Once an image is qualified on an XD/NX-enabled platform, that image will function properly for future updates with respect to XD/NX functionality.

Is the BIOS supporting this functionality different from the BIOS HP ships today?

Intel 915 and Transmeta systems ship with XD disabled by default in BIOS. Intel 945 and AMD systems ship with XD enabled by default in BIOS.

Is HP making the BIOS current image friendly?

Yes, you can enable/disable XD in F10 Setup on Intel-based systems.

NX-based systems do not currently allow you to enable or disable XD in F10 Setup.

Are XD and NX enabled or disabled by default?

XD is disabled by default in Intel 915-based computers and enabled by default in Intel 945-based computers.

NX is currently processor-dependent. AMD-based systems are enabled by default. Transmeta-based systems are disabled by default.

If the XD is disabled by default, how do I turn it on?

The BIOS for the i915 chipset-based 2004 and i945-chipset based 2005 desktop systems uses the CPUID instruction to locate the Execute Disable bit to determine if the installed processor supports XD. If XD is supported, then the **Data Execution Prevention** option appears in the Security section of F10 Setup. You can enable or disable this feature.

If I turn XD/NX "on", how will it affect my image?

If the applications and drivers in the image are well programmed (for example, no executing from data space), then everything should work normally. XD/NX may prevent the running of software that is not well programmed.

How do I keep individual users from enabling or disabling the functionality?

Prevention of random enabling or disabling of this functionality occurs using the same methods you use to protect all operating system and BIOS settings. For example, you can use Setup passwords to control who can change items in F10 Setup. Also, you can allow only users with administrator rights to change operating system settings.

Will DEP, XD, or NX keep all viruses out of my system?

No. These technologies address viruses that use buffer overflow types of attacks, and are only a part of a full security system.

Do I still need an antivirus software?

Yes.

Do I still need a firewall?

Yes.

What is needed to make XD or NX functional?

To take advantage of the XD/NX feature, the following components must support XD/NX:

- Processor
- System BIOS
- Operating system

Are the XD-capable processors from Intel also called "J" processors?

Yes, all processors with the "-J" designator include the XD bit. Additionally, several other processors use XD, such as 6xx series processors.

Are the XD-capable processors from Intel a new series - the 600 series?

The following series of Intel processors support XD:

- 3x0 "J"
- 3x1
- 5x0 "J"
- 5x1
- 6xx
- 8xx

Will XD-capable processors cost more?

XD/NX-capable chips will be sold at approximately the same or slightly higher cost compared to versions without XD bit.

When will they start showing up in the HP desktops I purchase?

HP is shipping:

- i915 chipset desktop systems with XD disabled in F10 Setup.
- i945 chipset desktop systems with XD enabled in F10 Setup.

What HP commercial desktops support this technology?

- dc5100
- dc7100
- dc7600
- dx5150
- dx6100
- dx7200
- bc1000

What HP workstations support this technology?

- HP Workstation xw4200
- HP Workstation xw6200
- HP Workstation xw8200

If the processor is changing, is the chipset changing as well?

For Intel-based systems, newer chipsets, starting with the i915 chipset, provide support for XD.

Will the system board change with the processor change?

Intel chipset-based HP system boards support a wide range of Intel processors. You should not have to change system boards when upgrading processors unless the new processor requires:

- Power output that the current system board does not support.
- A different chipset than what is on the system board.

Will my current applications work with this new technology?

In "Known Issues" on page 13, review the table that provides a list of applications currently known to not function properly with XD/NX. The table also lists links to Microsoft Knowledge Base articles about incompatibilities found during XD/NX testing.

How will I know if current applications will work?

If an application conflicts with DEP, you may see the following error message:

```
Data Execution Prevention – Microsoft Windows
To help protect your computer, Windows has closed this program.
Name: program name
Publisher: program publisher
```

To avoid this behavior, contact your program vendor to see if an update is available that enables the program to work correctly with DEP.

What type of support will HP offer for application functionality with this new technology?

HP tests its images and deliverables for XD/NX compatibility, including:

- Shipping HP applications
- Operating system image
- Shipping peripheral drivers
- Popular applications and games

At this time, you can only test hardware-enforced DEP. There is currently no way to reliably test software-enforced DEP. HP encourages you to perform your own validation if you plan to use your own image or proprietary software.

What does it mean when XD/NX is disabled, but the DEP is set for Optin?

The processor does not support XD/NX, therefore software-enforced DEP is used to protect against buffer overflows. Software-enforced DEP provides weaker protection than hardware-enforced DEP.

What viruses was this technology developed to protect against?

XD/NX protects against viruses that exploit buffer overruns. Recent viruses that utilize this attack method include:

- Sasser
- Blaster
- Code Red
- Welchia

Is this part of HP ProtectTools?

No.

Does XD/NX require the Trusted Platform Module (TPM) chip?

No. However, the Embedded Security Manager for ProtectTools does provide security features that can provide additional PC security.

What is the minimum memory requirement for this functionality to work?

XD/NX requires 128 MB of RAM - the minimum memory requirement for Windows XP SP2.

What is the minimum processor speed required

Because XD/NX uses memory tagging, there is no minimum processor speed required for XD/NX to function. The minimum speed XD processor that Intel has released is the 325J Celeron that runs at 2.53GHz.

Currently, all AMD Athlon 64 processors support NX.

Will this affect remote users on my network?

As long as software is properly developed, remote users will not be affected.

What is a shim?

A shim is a small piece of software added to a program to provide an enhancement.

380248-002, 05/2005