DEP Support Statement For GE Fanuc Products Using Proficy Common Licensing

Installs on to XP SP2 and 2003 SP1 can be problematic due to Microsoft's DEP feature, See KB article i023501, for our support statement on DEP here.

Description

When trying to install any GE Fanuc application (i.e. iFIX, iHistorian, Cimplicity, or any 3rd Party application) the install either throws an error, freezes, or doesn't appear to start or complete. You may also experience unexplained system lockups that require a complete reboot of the computer.

Information

*** DEP affects all products using HASP drivers. The HASP driver is included with Proficy Common Licensing, and is a part of all GE Fanuc software products. At this time, GE Fanuc products do not support running with hardware-based DEP turned on. Please read the remainder of this article for further detail of DEP and how to disable DEP.**

Data Execution Prevention (DEP) is a set of hardware and software technologies that perform additional checks on memory to help prevent malicious code from running on a system. Starting with Microsoft Windows XP Service Pack 2 (SP2), DEP is enforced by hardware and by software.

The primary benefit of DEP is to help prevent code execution from data pages. Typically, code is not executed from the default heap and the stack. Hardware-enforced DEP detects code that is running from these locations and raises an exception when execution occurs. Software-enforced DEP can help prevent malicious code from taking advantage of exception-handling mechanisms in Windows.

Hardware-enforced DEP

Hardware-enforced DEP marks all memory locations in a process as non-executable unless the location explicitly contains executable code. A class of attacks exists that tries to insert and run code from non-executable memory locations. DEP helps prevent these attacks by intercepting them and raising an exception.

Hardware-enforced DEP relies on processor hardware to mark memory with

an attribute that indicates that code should not be executed from that memory. DEP functions on a per-virtual memory page basis, and DEP typically changes a bit in the page table entry (PTE) to mark the memory page.

Processor architecture determines how DEP is implemented in hardware and how DEP marks the virtual memory page. However, processors that support hardware-enforced DEP can raise an exception when code is executed from a page that is marked with the appropriate attribute set.

Advanced Micro Devices (AMD) and Intel have defined and shipped Windows-compatible architectures that are compatible with DEP.

Beginning with Windows XP SP2, the 32-bit version of Windows uses one of the following:

The no-execute page-protection (NX) processor feature as defined by AMD.
The Execute Disable Bit (XD) feature as defined by Intel.

If you have an Intel Celeron processor, then only the Intel Celeron D processor supports the Execute Disable Bit. The Intel Celeron R processor does not support this!

To use these processor features, the processor must be running in Physical Address Extension (PAE) mode. However, Windows will automatically enable PAE mode to support DEP. Users do not have to separately enable PAE by using the /PAE boot switch.

Software-enforced DEP

An additional set of Data Execution Prevention security checks have been added to Windows XP SP2. These checks, known as software-enforced DEP, are designed to block malicious code that takes advantage of exception-handling mechanisms in Windows. Software-enforced DEP runs on any processor that can run Windows XP SP2. By default, software-enforced DEP helps protect only limited system binaries, regardless of the hardware-enforced DEP capabilities of the processor.

Benefits

The primary benefit of DEP is that it helps prevent code execution from data pages, such as the default heap pages, various stack pages, and memory pool pages. Typically, code is not executed from the default heap and the 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 will be stopped. Execution of code from protected

memory in kernel mode causes a Stop error.

DEP can help block a class of security intrusions. Specifically, DEP can help block a malicious program in which a virus or other type of attack has injected a process with additional code and then tries to run the injected code. On a system with DEP, execution of the injected code causes an exception. Software-enforced DEP can help block programs that take advantage of exception-handling mechanisms in Windows.

System-wide configuration of DEP

DEP configuration for the system is controlled through switches in the Boot.ini file. If you are logged on as an administrator, you can now easily configure DEP settings by using the System dialog box in Control Panel.

Windows supports four system-wide configurations for both hardware-enforced and software-enforced DEP.

Configuration	Description
OptIn	This setting is the default configuration. On systems with processors that can implement hardware-enforced DEP, DEP is enabled by default for limited system binaries and programs that "opt-in." With this option, only Windows system binaries are covered by DEP by default.
OptOut	DEP is enabled by default for all processes. You can manually create a list of specific programs that do not have DEP applied by using the System dialog box in Control Panel. Information technology (IT) professionals can use the Application Compatibility Toolkit to "opt-out" one or more programs from DEP protection. System compatibility fixes, or shims, for DEP do take effect.
AlwaysOn	This setting provides full DEP coverage for the whole system. All processes always run with DEP applied. The exceptions list to exempt specific programs from DEP protection is not available. System compatibility fixes for DEP do not take effect. Programs that have been opted-out by using the Application Compatibility Toolkit run with DEP applied.
AlwaysOff	This setting does not provide any DEP coverage for any part of the system, regardless of hardware DEP support. The processor does not run in PAE mode unless the /PAE option is present in the Boot.ini file.

Hardware-enforced and software-enforced DEP are configured in the same manner. If the system-wide DEP policy is set to OptIn, the same Windows core binaries and programs will be protected by both hardware-enforced and software-enforced DEP. If the system cannot use hardware-enforced DEP, the Windows core binaries and programs will be protected only by software-enforced DEP.

Similarly, if the system-wide DEP policy is set to OptOut, programs that have been exempted from DEP protection will be exempted from both

hardware-enforced and software-enforced DEP.

The Boot.ini file settings are as follows:

/noexecute=policy_level
Note policy_level is defined as AlwaysOn, AlwaysOff, OptIn, or OptOut.

Existing **/noexecute** settings in the Boot.ini file are not changed when Windows XP SP2 is installed. These settings are also not changed if a Windows operating system image is moved across computers with or without hardware-enforced DEP support.

During installation of Windows XP SP2, the OptIn policy level is enabled by default unless a different policy level is specified in an unattended installation. If the **/noexecute**=policy_level setting is not present in the Boot.ini file for a version of Windows that supports DEP, the behavior is the same as if the **/noexecute**=OptIn setting was included.

If you are logged on as an administrator, you can manually configure DEP to switch between the OptIn and OptOut policies by using the **Data Execution Prevention** tab in System Properties.

The following procedure describes how to manually configure DEP on the computer:

1. Click **Start**, click **Run**, type **sysdm.cpl**, and then click **OK**.
2. On the **Advanced** tab, under **Performance**, click **Settings**.
3. On the **Data Execution Prevention** tab, use one of the following procedures:

? Click Turn on DEP for essential Windows programs and services only to select the OptIn policy.
? Click Turn on DEP for all programs and services except those I select to select the OptOut policy, and then click Add to add the programs that you do not want to use the DEP feature.

4. Click **OK** two times.
IT professionals can control system-wide DEP configuration by using a variety of methods. The Boot.ini file can be modified directly with scripting mechanisms or with the Bootcfg.exe tool that is included in Windows XP SP2.

For unattended installations of Windows XP SP2, you can use the Unattend.txt file to pre-populate a specific DEP configuration. You can use the OSLoadOptionsVar entry in the [Data] section of the Unattend.txt file to specify a system-wide DEP configuration.

Per-program DEP configuration

For the purposes of program compatibility, you can selectively disable DEP for individual 32-bit programs when DEP is set to the OptOut policy level. To do this, use the **Data Execution Prevention** tab in **System Properties** to selectively disable DEP for a program.

For IT professionals, a new program compatibility fix that is named DisableNX is included with Windows XP SP2. The DisableNX compatibility fix disables Data Execution Prevention for the program that the fix is applied to.

The DisableNX compatibility fix can be applied to a program by using the Application Compatibility Toolkit. For more information about Windows application compatibility, see Windows Application Compatibility on the following Microsoft Web site:

http://www.microsoft.com/windows/appcompatibility/default.mspx

Resolution

To turn off the DEP feature

If you need the functionality of the incompatible driver, you can turn off the DEP feature. To do this, follow these steps:

1. Restart your computer.
2. Go into BIOS and disable DEP in BIOS if present. Save and exit.
3. During the restart process, press **F8**.
Note On a computer that is configured to start multiple operating systems, press **F8** when the
Startup menu appears.
4. Use the arrow keys to select a Safe Mode option, and then press **ENTER**.
5. Click **Start**, click **Run**, type **cmd**, and then click **OK**.
6. At the command prompt, type the following, and then press **ENTER**:

bootcfg /raw ?/noexecute=alwaysoff /fastdetect? /id 1

Note If you have multiple start entries or start options, you may have to manually modify the Boot.ini file for your computer. To do this, follow these steps:

a. Click **Start**, click **Run**, type **sysdm.cpl**, and then click **OK**.
b. On the **Advanced** tab, under **Startup and Recovery**, click **Settings**.
c. In the **Startup and Recovery** dialog box, click **Edit**.
d. Change the **/noexecute** option to the following:

/noexecute=alwaysoff

e. On the **File** menu, click **Save**, and then click **Exit**.
f. Click **OK** two times.

7. Restart your computer.