

Tech Note 437

Unable to Open Logger Under Windows® XP SP2, Windows 2003 Server SP1 and SP2

All Tech Notes and KBCD documents and software are provided "as is" without warranty of any kind. See the [Terms of Use](#) for more information.

Topic#: 002130

Created: October 2005

Updated: October 2007

Introduction

The OSConfigurationUtility program for Windows XP Service Pack 2 and Windows Server 2003 Service Pack 1 and Service Pack 2 does not work in all cases when applied to the computers after installing Wonderware Archestra-related software. The issue is mostly seen in computers that come factory-loaded with an OEM version of the operating system, or with computers that have either software or hardware **Data Execution Prevention (DEP)** enabled.

Understanding Data Execution Prevention (DEP)

Data Execution Prevention (DEP) helps prevent damage from viruses and other security threats that run (execute) malicious code from memory locations that only Windows and other programs should use. This type of threat causes damage by taking over one or more memory locations in use by a program. Then it spreads and harms other programs, files, and even your e-mail contacts.

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 if they use system memory safely. To do this, DEP software works alone or with compatible microprocessors to mark some memory locations as "non-executable". If a program tries to run code—malicious or not—from a protected location, DEP closes the program and notifies you.

DEP can take advantage of software and hardware support. To use DEP, your computer must be running Microsoft Windows XP Service Pack 2 (SP2) or later, or Windows Server 2003 Service Pack 1 or later. DEP software alone helps protect against certain types of malicious code attacks. However, to take full advantage of the protection that DEP can offer, your processor must support "execution protection." This is a hardware-based technology designed to mark memory locations as non-executable. If your processor does not support hardware-based DEP, it's a good idea to upgrade

to a processor that offers execution protection features.

How Can I Tell if DEP is Available on My Computer

DEP is accessible through the **System Properties** window of both operating systems.

To access System Properties:

1. Click **Start/Settings**.
2. Select **Control Panel** and double-click the **System** icon.
3. Select the **Advanced** tab.
4. Under **Performance**, click the **Settings** button .
5. Select the **Data Execution Prevention** tab.

Note: By default, DEP is only turned on for essential Windows operating system programs and services (first option). To help protect more programs with DEP, select the **Turn on DEP for all programs and services except those I select** option .

Hardware-Enforced DEP – Physical Address Extension (PAE)

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.

In Windows Server 2003 with SP1 and in Windows XP with SP2, the Data Execution Prevention (DEP) processor features require that the processor run in PAE mode. DEP is a set of hardware and software technologies. These technologies perform additional checks on memory to help prevent malicious code from running on a system.

Starting with Windows XP SP2, the 32-bit versions of Windows use one of the following hardware technologies to implement DEP:

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

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.

Symptoms and Troubleshooting

Unable to Connect to Logger on [computer name]

The primary symptom seen by users is the inability to connect to the ArchestrA Logger Service. When attempting to view the log files in the local machine, the user opens the LogViewer in the System Management Console. Upon selecting the Local node, a pop-up window will display the message: **Unable to connect to Logger on [computer name]**.

Troubleshoot and Disable PAE mode

Warning: This workaround may make your computer or your network more vulnerable to attack by malicious users or by malicious software such as viruses. We do not recommend this workaround but are providing this information so that you can implement this workaround at your own discretion. Use this workaround at your own risk.

To troubleshoot a system, you may have to disable PAE mode on a computer where Windows has automatically enabled PAE mode. In this scenario, you can disable PAE mode by editing the **Boot.ini** file.

To edit the Boot.ini file

1. Click **Start/Run**.
2. Type **sysdm.cpl**, then click **OK**.
3. Select the **Advanced** tab.
4. Click the **Settings** button under **Startup and Recovery**.
5. Under **System Startup**, click the **Edit** button.

The editable contents appear as a .txt file in Notepad or similar editor application.

Disable PAE Mode in Windows XP with SP2

Add the following switches to the Windows XP **Boot.ini** file:

```
/noexecute=alwaysoff /NOPAE
```

For example, the **Boot.ini** file content may appear as follows:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP" /fastdetect /
noexecute=alwaysoff /NOPAE
```

Disable PAE Mode in Windows Server 2003 with SP1

Add the following switches to the Windows Server 2003 **Boot.ini** file:

```
/execute /NOPAE
```

For example, the **Boot.ini** file content may appear as follows:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows Server 2003" /fastdetect /
execute /NOPAE
```

Disable PAE Mode in Windows Server 2003 SP2

Add the following switches to the Windows Server 2003 **Boot.ini** file:

```
/noexecute=alwaysoff
```

For example, the **Boot.ini** file content may appear as follows:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows Server 2003, Enterprise" /
fastdetect /noexecute=alwaysoff
```

References

1. **How to edit the Boot.ini file in Windows XP:** Follow Microsoft's article on making changes to your boot.ini in order to gain access to the file. This article can be found at the following location: <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q289022>
2. **How to prevent the PAE kernel from loading in Windows Server 2003 with Service Pack 1 or in Windows XP with Service Pack:** This article can be found at the following location: <http://support.microsoft.com/default.aspx?scid=kb;en-us;900524>
3. **A detailed description of the Data Execution Prevention (DEP) feature in Windows XP Service Pack 2...:** This article can be found at the following location: <http://support.microsoft.com/>

[kb/875352/](#)

J. Gaines, A. Martinez and B. Shah

Tech Notes are published occasionally by Wonderware Technical Support. Publisher: Invensys Systems, Inc., 26561 Rancho Parkway South, Lake Forest, CA 92630. There is also technical information on our software products at www.wonderware.com/support/mmi

For technical support questions, send an e-mail to support@wonderware.com.



[back to top](#)

©2007 Invensys Systems, Inc. All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, broadcasting, or by any information storage and retrieval system, without permission in writing from Invensys Systems, Inc. [Terms of Use](#).