Find it myself ▷

Ask the community

Get live help

Select the product you need help with

Windows | Internet Explorer | Office | Surface | Xbox | Skype | Windows Phone | More products →

How to disable the Autorun functionality in Windows

Article ID: 967715 - View products that this article applies to.

Support for Windows Vista Service Pack 1 (SP1) ends on July 12, 2011. To continue receiving security updates for Windows, make sure you're running Windows Vista with Service Pack 2 (SP2). For more information, refer to this Microsoft web page: Support is ending for some versions of Windows (http://windows.microsoft.com/en-us/windows/help/end-support-windows-xp-sp2-windows-vista-without-service-packs) .

⊖ SUMMARY

The updates that this article describes fix a problem with the disable Autorun feature. Without these updates, Autorun for a network drive cannot be disabled. Also, the shortcut menu and double-click functionality of Autorun were not disabled even if the steps that were previously provided were followed. This problem is fixed by the updates described in this article. The updates were distributed to the following systems through the Windows Update and Automatic update distribution channels:

- Microsoft Windows 2000
- Windows XP Service Pack 2
- Windows XP Service Pack 3
- Windows Server 2003 Service Pack 1
- Windows Server 2003 Service Pack 2

This article also contains links to download locations where users can obtain these updates.

⊖ MORE INFORMATION

Depending on the version of Windows that you are using, there are different updates that you must have installed to correctly disable the Autorun functionality:

- To disable the Autorun functionality in Windows Vista or in Windows Server 2008, you must have security update 950582 installed (security bulletin MS08-038).
- To disable the Autorun functionality in Windows XP, in Windows Server 2003, or in Windows 2000, you must have security update 950582, update 967715, or update 953252 installed.

  Note Updates 950582, 967715, and 953252 provide the same functionality for Autorun. Update 953252 was repackaged as security update 950582 to provide an additional security update for Windows Vista and Windows Server 2008.

  The following table shows the differences in the three updates:

	Security update 950582	Update 953252	Update 967715
Applicable operating systems	Windows Vista and Windows Server 2008	Windows XP, Windows Server 2003, and Windows 2000	Windows XP, Windows Server 2003, and Windows 2000
Contains security updates	Yes	No	No
Provides the Autorun functionality	Yes	Yes	Yes
Delivery method	Windows Update, Automatic Updates, and Download Center	Download Center	Windows Update, Automatic Updates, and Download Center
Package details	Packages built by using Microsoft Knowledge Base article 950582	Packages built by using Microsoft Knowledge Base article 950582	Packages built by using Microsoft Knowledge Base article 967715

  After the prerequisite updates are installed, you can use the procedures in any of the following sections to disable Autorun features:

  - How to use Group Policy settings to disable all Autorun features
  - How to selectively disable specific Autorun features
  - How to set the HonorAutorunSetting registry key manually

The purpose of Autorun

The main purpose of Autorun is to provide a software response to hardware actions that you start on a computer. Autorun has the following features:

- Double-Click
- Contextual Menu
- AutoPlay

These features are typically called from removable media or from network shares. During AutoPlay, the Autorun.inf file from the media is parsed. This file specifies which commands the system runs. Many companies use this functionality to start their installers.

Default Behavior of Autorun and AutoPlay

Default behavior of AutoPlay on Windows XP-based systems

AutoPlay begins reading from a drive as soon as you insert media into the drive. Therefore, the Setup file of programs and the music on audio media start immediately. Before Windows XP SP2, AutoPlay was disabled by default on removable drives, such as the floppy disk drive (but not the CD drive), and on network drives. Starting with Windows XP SP2, AutoPlay is enabled for removable drives. This includes ZIP drives and some USB mass storage devices. If you enable the settings to disable AutoPlay (the procedure to do this is described in this article), you can disable AutoPlay on a CD drive, on removable media drives, on all drives.

Note This setting appears in both the Computer Configuration and User Configuration folders. If the settings conflict, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Default behavior for Autorun

Autorun commands are generally stored in Autorun.inf files. These commands enable applications to start, start installation programs, or start other routines. In versions of Windows that are earlier than Windows Vista, when media that contains an **Autorun** command is inserted, the system automatically executes the program without requiring user intervention. Because code may be executed without user's knowledge or consent, users may want to disable this feature because of security concerns. The configuration settings that are described in this article give Administrators the ability to selectively or completely disable all Autorun capabilities for systems that run Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008 systems.

The default behavior in Windows Vista and Windows Server 2008 is to prompt the user whether an **Autorun** command is to be run. Changes to these settings are described later in this article. An Administrator can completely disable **Autorun** commands or revert to the pre-Windows Vista behavior of automatically executing the **Autorun** command. If the feature is configured to disable Autorun capabilities, or if this policy is not configured, Windows Vista and Windows Server 2008 will continue to prompt the user whether the **Autorun** command is to be run.

Prerequisites to disable Autorun capabilities

To disable Autorun capabilities, you must install the following updates:

- Update for Windows XP (KB967715)
  http://www.microsoft.com/downloads/details.aspx?FamilyID=c7dbcde3-7814-47c5-849e-e64ecfb35d74 (http://www.microsoft.com/downloads/details.aspx?FamilyID=c7dbcde3-7814-47c5-849e-e64ecfb35d74)
- Update for Windows Server 2003 for Itanium-based Systems (KB967715)
  http://www.microsoft.com/downloads/details.aspx?FamilyID=99423caf-b52b-4ebc-b80c-94ee1ef9f66b (http://www.microsoft.com/downloads/details.aspx?FamilyID=99423caf-b52b-4ebc-b80c-94ee1ef9f66b)
- Update for Windows Server 2003 x64 Edition (KB967715)
  http://www.microsoft.com/downloads/details.aspx?FamilyID=7b866fb7-9bb7-4fce-b395-d0a4ee38a115 (http://www.microsoft.com/downloads/details.aspx?FamilyID=7b866fb7-9bb7-4fce-b395-d0a4ee38a115)
- Update for Windows Server 2003 (KB967715)
  http://www.microsoft.com/downloads/details.aspx?FamilyID=32b845ac-7681-468c-812b-2dcebdae9b40 (http://www.microsoft.com/downloads/details.aspx?FamilyID=32b845ac-7681-468c-812b-2dcebdae9b40)
- Update for Windows XP x64 Edition (KB967715)
  http://www.microsoft.com/downloads/details.aspx?FamilyID=ca802f38-0566-4ac4-8808-6515623c35c5 (http://www.microsoft.com/downloads/details.aspx?FamilyID=ca802f38-0566-4ac4-8808-6515623c35c5)
- Update for Windows 2000 (KB967715)
  http://www.microsoft.com/downloads/details.aspx?FamilyID=3c6039f1-d84d-4294-8457-35aa8b4dcab8 (http://www.microsoft.com/downloads/details.aspx?FamilyID=3c6039f1-d84d-4294-8457-35aa8b4dcab8)
- Windows Vista-based and Windows Server 2008-based systems must have update 950582 (Security bulletin MS08-038 (http://www.microsoft.com/technet/security/bulletin/ms08-038.mspx)) installed to take advantage of the registry key settings that disable Autorun.

After the prerequisites are installed, follow these steps to disable Autorun.

How to use Group Policy settings to disable all Autorun features in Windows Server 2008 or Windows Vista

Use either of the following methods:

Method 1

1. Click **Start** , type **Gpedit.msc** in the **Start Search** box, and then press ENTER.

If you are prompted for an administrator password or for confirmation, type the password, or click **Allow**.

2. Under **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Autoplay Policies**.
3. In the **Details** pane, double-click **Turn off Autoplay**.
4. Click **Enabled**, and then select **All drives** in the **Turn off Autoplay** box to disable Autorun on all drives.
5. Restart the computer.

Method 2

1. Click **Start** , type **Gpedit.msc** in the **Start Search** box, and then press ENTER.

   If you are prompted for an administrator password or for confirmation, type the password, or click **Allow**.
2. Under **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Autoplay Policies**.
3. In the **Details** pane, double-click **Default Behavior for AutoRun**.
4. Click **Enabled**, and then select **Do not execute any autorun commands** in the **Default Autorun behavior** box to disable Autorun on all drives.
5. Restart the computer.

How to use Group Policy settings to disable all Autorun features in Windows Server 2003, Windows XP Professional, and Windows 2000

1. Click **Start**, click **Run**, type **Gpedit.msc** in the **Open** box, and then click **OK**.
2. Under **Computer Configuration**, expand **Administrative Templates**, and then click **System**.
3. In the **Settings** pane, right-click **Turn off Autoplay**, and then click **Properties**.

   Note In Windows 2000, the policy setting is named **Disable Autoplay**.
4. Click **Enabled**, and then select **All drives** in the **Turn off Autoplay** box to disable Autorun on all drives.
5. Click **OK** to close the **Turn off Autoplay Properties** dialog box.
6. Restart the computer.

How to disable or enable all Autorun features in Windows 7 and other operating systems

Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003,or Windows XP

Fix it for me

To disable or enable Autorun automatically, click the appropriate **Fix this problem** link. Then, click **Run** in the **File Download** dialog box and follow the steps in this wizard.

Disable Autorun	**Enable Autorun**
Fix this problem Microsoft Fix it 50471	Fix this problem Microsoft Fix it 50475

Note these wizards may be in English only; however, these automatic fixes also work for other language versions of Windows.

Note If you are not on the computer that has the problem, you can save these automatic fixes to a flash drive or to a CD so that you can run it on the computer that has the problem.

Let me fix it myself

Important This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base:

322756 (http://support.microsoft.com/kb/322756/) How to back up and restore the registry in Windows

To disable Autorun yourself on operating systems that do not include Gpedit.msc, follow these steps:

1. Click **Start**, click **Run**, type **regedit** in the **Open** box, and then click **OK**.
2. Locate and then click the following entry in the registry:
   HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\NoDriveTypeAutorun
3. Right-click **NoDriveTypeAutoRun**, and then click **Modify**.
4. In the **Value data** box, type **0xFF** to disable all types of drives. Or, to selectively disable specific drives, use a different value as described in the "How to selectively disable specific Autorun features" section.

5. Click **OK**, and then exit Registry Editor.
6. Restart the computer.

How to selectively disable specific Autorun features

To selectively disable specific Autorun features, you must change the NoDriveTypeAutoRun entry in one of the following registry key subkeys:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\

The following table shows the settings for the NoDriveTypeAutoRun registry entry.

Value	Meaning
0x1 or 0x80	Disables AutoRun on drives of unknown type
0x4	Disables AutoRun on removable drives
0x8	Disables AutoRun on fixed drives
0x10	Disables AutoRun on network drives
0x20	Disables AutoRun on CD-ROM drives
0x40	Disables AutoRun on RAM disks
0xFF	Disables AutoRun on all kinds of drives

The value of the NoDriveTypeAutoRun registry entry determines which drive or drives the Autorun functionality will be disabled for. For example, if you want to disable Autorun for network drives only, you must set the value of NoDriveTypeAutoRun registry entry to 0x10.

If you want to disable Autorun for multiple drives, you must add the corresponding hexadecimal values to the 0x10 value. For example, if you want to disable Autorun for removable drives and for network drives, you must add 0x4 and 0x10, which is the mathematical addition of 2 hexadecimal values, to determine the value to use. 0x4 + 0x10 = 0x14. Therefore, in this example, you would set the value of the NoDriveTypeAutoRun entry to 0x14.

The default value for the NoDriveTypeAutoRun registry entry varies for different Windows-based operating systems. These default values are listed in the following table.

Operating system	Default value
Windows Server 2008 and Windows Vista	0x91
Windows Server 2003	0x95
Windows XP	0x91
Windows 2000	0x95

Registry entry that is used to control the behavior of the current update

All the fixes in the current update for Windows XP and for Windows Server 2003 are included in the HonorAutorunSetting registry entry in the following subkey:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\

Registry Value

Value	Data type	Range	Default value
HonorAutorunSetting	REG_DWORD	0x0–0xFF	0x01

Note For Windows Server 2003 and Windows XP, all changes of this update are controlled by the HonorAutorunSetting registry entry so that you can revert to the previous configuration if it is required. This entry is not valid for Windows 2000, Windows Vista, or Windows Server 2008 users.

When you install update 967715, the HonorAutorunSetting registry key is created only in the HKEY_LOCAL_MACHINE registry hive. The registry key has a default value of 0x1. This value enables the functionality that is present in the current update. Before you install the current update, this registry key is not present in the system. You can obtain prepackage installation Autorun behavior by manually setting the registry key to 0. To do this, type **0** instead of **1** in step 6 of the following procedures to manually set the registry key. HonorAutorunSetting is always read from the HKEY_LOCAL_MACHINE registry hive even if the HonorAutorunSetting entry is also configured in the HKEY_CURRENT_USER registry hive.

How to set the HonorAutorunSetting registry key manually

Windows Server 2003 and Windows XP

1. Click **Start**, and then click **Run**.
2. In the **Open** box, type **regedit**, and then click **OK**.
3. Locate and then click the following registry subkey:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\

4. Right-click in the right side pane, point to **New**, and then click **DWORD Value**.

5. Type **HonorAutorunSetting**, and then press ENTER.
6. In the **Value data** box, type **1**, click **Hexadecimal** if it is not already selected, and then click **OK**.
7. Exit Registry Editor.
8. Restart the system for the new settings to take effect.

How to prevent Autorun.inf files from being created on shares

To prevent the Autorun feature from being invoked, and to keep any programs from writing Autoun.inf files to mapped network drives, follow these steps:

1. Delete any Autorun.inf files from the root of a mapped network drive.
2. Do not give anyone Create rights to the root of a mapped network drive.

Note After you implement this procedure, Autorun features will not be available from network drives.

How to prevent users from connecting to USB storage devices

The following Microsoft Knowledge Base article contains two methods to prevent users from connecting to a USB storage device:
823732 (http://support.microsoft.com/kb/823732/) How can I prevent users from connecting to a USB storage device?

Note After you implement one of these procedures on a system, USB storage devices no longer function on the system.

Frequently Asked Questions

Does this update change my current Autorun settings?
No. The update does not change the current Autorun settings on your system. Instead, the update lets users correctly enforce Autorun settings.

Is there a change in user experience after this update is installed?
After you install update 967715, you might notice that Autorun features for network drives no longer function. This is because, by default, Autorun on network drives is set to disabled in the registry. After you install the update, a registry key that was already set to disable Autorun on network drives is enforced correctly. This is the only functionality that will change after the update is installed. If a user had disabled Autorun for other drives before the update, they may notice a change in the double-click and contextual menu behavior after the update.

Is this a security vulnerability that requires Microsoft to issue a security update?
No. Disabling the Autorun feature is an optional configuration that some customers may decide to deploy. Update 967715 only resolves the issue with Autorun functionality.

Why am I being redirected to update 967715 when I was looking for update 953252?
Update 953252 and update 967715 offer the same updates. Only the delivery channels for these were different. Update 953252 was released only for Download Center while update 967715 was released for Windows Update, for Automatic Updates, and for the Download Center. To avoid duplication of the same information, you are being redirected to update 967715, which has all the latest information about these updates.

If I have update 950582 or update 953252 installed on my computer, will I be reoffered update 967715?
No, update 967715 is the same update that was released as update 953252 but was packaged under update 950582. Therefore, if Add or Remove Programs shows that update 950582 or update 953252 is installed, you do not require update 967715, and it will not be offered by Windows Update or Automatic Updates.

Do these updates disable Autorun capabilities?
No. The updates that are offered correctly respect the registry key values that disable Autorun capabilities. These updates do not change the registry key values and will continue to respect values that were already set before these updates were installed. If the registry values were not set before you install these updates, then the registry key settings will have to be set appropriately in order to disable Autorun capabilities.

Where are the updates for Windows Vista and Windows Server 2008?
Updates for Windows Vista and Windows Server 2008 were released together with some security updates in security update 950582 (security bulletin MS08-038). In order to take advantage of the registry key settings that disable Autorun, customers who are running Windows Vista or Windows Server 2008-based systems must install security update 950582.

Known issues with this security update

- **Update 967715 is reoffered multiple times**

  Update 967715 may be reoffered if the HonorAutorunSetting registry setting that is described in this article is not added to the registry hive. This issue may occur if some other program that is installed on the computer blocks the update from writing the registry entry. Such software may block the update during the installation of the update or may remove the registry entry after the computer is restarted.

  To resolve this problem, install the update in safe mode. To do this, follow these steps:

  1. Download the update. To do this, follow these steps:

     a. Visit the Microsoft Download Web site:
        http://www.microsoft.com/downloads (http://www.microsoft.com/downloads)

     b. In the **Search for a download** box, type the number of the Knowledge Base article that describes the update, and then click **Go**.
     c. Download the update, and then save it to the desktop.

2. Install the update. To do this, follow these steps:

    a. Double-click the downloaded file to install it.

       If you are prompted to restart the computer, do so.

    b. Visit the Windows Update or Microsoft Update Web site to determine whether the update is offered again. If you are offered the update again, continue to the next step.

3. Install the update in safe mode. Safe mode disables most running processes and services. These services include the Windows Update service. Installing an update in safe mode is a quick test to determine whether an application or process is interfering with the installation. To install the update in safe mode, follow these steps:

    a. Restart the computer.
    b. As the computer starts, press the F8 key.
    c. Use the arrow keys to select **Safe Mode**, and then press ENTER.
    d. Double-click the file that you downloaded in step 1 to install the file.
    e. When the installation is complete, restart the computer.
    f. Visit the Windows Update or Microsoft Update Web site to determine whether the update is offered. Or, wait until Automatic Updates runs again.

⊖ FILE INFORMATION

The English (United States) version of this software update installs files that have the attributes that are listed in the following tables. The dates and times for these files are listed in Coordinated Universal Time (UTC). The dates and times for these files on your local computer are displayed in your local time and with your current daylight saving time (DST) bias. Additionally, the dates and times may change when you perform certain operations on the files.

Windows 2000 file information

For all supported editions of Microsoft Windows 2000 Service Pack 4

File Name	Version	Date	Time	Size	Folder
shell32.dll	5.0.3900.7155	15-Apr-2008	23:13	2,362,640	

Windows XP and Windows Server 2003 file information

- The files that apply to a specific milestone (RTM, SP*n*) and service branch (QFE, GDR) are noted in the "SP requirement" and "Service branch" columns.
- GDR service branches contain only those fixes that are widely released to address widespread, critical issues. QFE service branches contain hotfixes in addition to widely released fixes.
- In addition to the files that are listed in these tables, this software update also installs an associated security catalog file (KB*number*.cat) that is signed with a Microsoft digital signature.

For all supported x86-based versions of Windows XP

File Name	Version	Date	Time	Size	Folder
shell32.dll	6.0.2900.3402	02-Jul-2008	23:46	8,454,656	SP2GDR
shell32.dll	6.0.2900.3402	02-Jul-2008	23:33	8,460,800	SP2QFE
xpsp3res.dll	5.1.2600.3314	14-Feb-2008	19:36	351,744	SP2QFE
shell32.dll	6.0.2900.5622	17-Jun-2008	05:32	8,461,312	SP3GDR
shell32.dll	6.0.2900.5622	17-Jun-2008	05:34	8,461,824	SP3QFE

For all supported x64-based versions of Windows Server 2003 and of Windows XP Professional x64 edition

File Name	Version	Date	Time	Size	CPU	Folder
shell32.dll	6.0.3790.3158	10-Feb-2009	02:12	10,502,144	X64	SP1GDR
wshell32.dll	6.0.3790.3158	10-Feb-2009	02:13	8,384,000	X86	SP1GDR\wow
shell32.dll	6.0.3790.3158	10-Feb-2009	02:12	10,506,240	X64	SP1QFE
w03a2409.dll	5.2.3790.3090	10-Feb-2009	02:12	30,208	X64	SP1QFE
wshell32.dll	6.0.3790.3158	10-Feb-2009	02:12	8,386,560	X86	SP1QFE\wow

ww03a2409.dll	5.2.3790.3090	10-Feb-2009	02:12	29,696	X86	SP1QFE\wow
shell32.dll	6.0.3790.4315	10-Feb-2009	02:21	10,508,288	X64	SP2GDR
wshell32.dll	6.0.3790.4315	10-Feb-2009	02:22	8,360,960	X86	SP2GDR\wow
shell32.dll	6.0.3790.4315	10-Feb-2009	02:12	10,508,800	X64	SP2QFE
wshell32.dll	6.0.3790.4315	10-Feb-2009	02:13	8,361,472	X86	SP2QFE\wow

For all supported x86-based versions of Windows Server 2003

File Name	Version	Date	Time	Size	Folder
shell32.dll	6.0.3790.3158	17-Jun-2008	07:13	8,384,000	SP1GDR
shell32.dll	6.0.3790.3158	17-Jun-2008	07:42	8,386,560	SP1QFE
w03a2409.dll	5.2.3790.3090	13-Feb-2008	20:11	29,696	SP1QFE
shell32.dll	6.0.3790.4315	17-Jun-2008	06:38	8,360,960	SP2GDR
shell32.dll	6.0.3790.4315	17-Jun-2008	07:22	8,361,472	SP2QFE

For all supported IA-64-based versions of Windows Server 2003

File Name	Version	Date	Time	Size	CPU	Folder
shell32.dll	6.0.3790.3158	10-Feb-2009	02:12	13,238,272	IA-64	SP1GDR
wshell32.dll	6.0.3790.3158	10-Feb-2009	02:12	8,384,000	X86	SP1GDR\wow
shell32.dll	6.0.3790.3158	10-Feb-2009	02:12	13,243,904	IA-64	SP1QFE
w03a2409.dll	5.2.3790.3090	10-Feb-2009	02:12	28,672	IA-64	SP1QFE
wshell32.dll	6.0.3790.3158	10-Feb-2009	02:12	8,386,560	X86	SP1QFE\wow
ww03a2409.dll	5.2.3790.3090	10-Feb-2009	02:12	29,696	X86	SP1QFE\wow
shell32.dll	6.0.3790.4315	10-Feb-2009	01:53	13,244,928	IA-64	SP2GDR
wshell32.dll	6.0.3790.4315	10-Feb-2009	01:54	8,360,960	X86	SP2GDR\wow
shell32.dll	6.0.3790.4315	10-Feb-2009	02:12	13,246,464	IA-64	SP2QFE
wshell32.dll	6.0.3790.4315	10-Feb-2009	02:13	8,361,472	X86	SP2QFE\wow

Properties

Article ID: 967715 - Last Review: June 10, 2011 - Revision: 6.3

APPLIES TO

- Windows Server 2008 Datacenter without Hyper-V
- Windows Server 2008 Enterprise without Hyper-V
- Windows Server 2008 for Itanium-Based Systems
- Windows Server 2008 Standard without Hyper-V
- Windows Server 2008 Datacenter
- Windows Server 2008 Enterprise
- Windows Server 2008 Standard
- Windows Web Server 2008
- Windows Vista Service Pack 1, when used with:
  Windows Vista Business
  Windows Vista Enterprise
  Windows Vista Home Basic
  Windows Vista Home Premium
  Windows Vista Starter
  Windows Vista Ultimate
  Windows Vista Enterprise 64-bit Edition
  Windows Vista Home Basic 64-bit Edition
  Windows Vista Home Premium 64-bit Edition
  Windows Vista Ultimate 64-bit Edition
  Windows Vista Business 64-bit Edition

- Windows Vista Business
- Windows Vista Enterprise
- Windows Vista Home Basic
- Windows Vista Home Premium
- Windows Vista Starter
- Windows Vista Ultimate
- Windows Vista Enterprise 64-bit Edition
- Windows Vista Home Basic 64-bit Edition
- Windows Vista Home Premium 64-bit Edition

- Windows Vista Ultimate 64-bit Edition
- Windows Vista Business 64-bit Edition
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 Service Pack 2, when used with:
  Microsoft Windows Server 2003, Standard Edition (32-bit x86)
  Microsoft Windows Server 2003, Enterprise Edition (32-bit x86)
  Microsoft Windows Server 2003, Web Edition
  Microsoft Windows Server 2003, Datacenter Edition (32-bit x86)
  Microsoft Windows Server 2003, Standard x64 Edition
  Microsoft Windows Server 2003, Enterprise x64 Edition
  Microsoft Windows Server 2003, Datacenter x64 Edition
  Microsoft Windows Server 2003, Enterprise Edition for Itanium-based Systems
  Microsoft Windows Server 2003, Datacenter Edition for Itanium-Based Systems
  Microsoft Windows XP Professional x64 Edition

- Microsoft Windows Server 2003 Service Pack 1, when used with:
  Microsoft Windows Server 2003, Standard Edition (32-bit x86)
  Microsoft Windows Server 2003, Enterprise Edition (32-bit x86)
  Microsoft Windows Server 2003, Web Edition
  Microsoft Windows Server 2003, Datacenter Edition (32-bit x86)
  Microsoft Windows Server 2003, Standard x64 Edition
  Microsoft Windows Server 2003, Enterprise x64 Edition
  Microsoft Windows Server 2003, Datacenter x64 Edition
  Microsoft Windows Server 2003, Enterprise Edition for Itanium-based Systems
  Microsoft Windows Server 2003, Datacenter Edition for Itanium-Based Systems

- Microsoft Windows XP Service Pack 2, when used with:
  Microsoft Windows XP Professional
  Microsoft Windows XP Home Edition
  Microsoft Windows XP Tablet PC Edition

- Microsoft Windows XP Service Pack 3, when used with:
  Microsoft Windows XP Home Edition
  Microsoft Windows XP Professional

Keywords: atdownload kbbug kbexpertiseinter kbfix kbPubTypeKC kbsecbulletin kbsecurity kbsecvulnerability kbsurveynew kbfixme kbmsifixme KB967715

⊖ Give Feedback

↑ Back to the top