

Home page setting changes unexpectedly, or you cannot change your home page setting

[View products that this article applies to.](#)

Article ID : 320159

Last Review : June 13, 2006

Revision : 6.2

This article was previously published under Q320159

Important This article contains information about how to modify the registry. Make sure to back up the registry before you modify it. Make sure that you know how to restore the registry if a problem occurs. For more information about how to back up, restore, and modify the registry, click the following article number to view the article in the Microsoft Knowledge Base:

[256986](#) Description of the Microsoft Windows registry

SYMPTOMS

When you use Microsoft Internet Explorer, you may experience any of the following symptoms:

- Your Internet Explorer home page has been changed to a different Web site than the one that you selected.
- You cannot change your home page selection to the Web site that you want.

For example, when you try to change your home page in the **Internet Options** dialog box on the **Tools** menu, you may not be able to type an address in the **Address** box, and the following buttons may be unavailable:

- Use Current
 - Use Default
 - Use Blank
- You reset your home page to the Web site that you want in **Internet Options**, but after you restart your computer your home page selection has again been changed to a different Web site.

[↑ Back to the top](#)

CAUSE

This issue may occur if one or more of the following conditions are true:

- Your computer has been infected with a virus that changed your Internet Explorer home page.

For example, the IRC.Becky.A worm and Trojan.JS.Clid.gen trojan horse viruses change the Internet Explorer home page.

- Code in the form of a malicious attack has been run on your computer.

For example, the JS.Exception.Exploit code may change the Internet Explorer home page.

- You installed third-party software that changed the Internet Explorer home page.

For example, the Xupiter toolbar from Xupiter.com, the SecondPower Multimedia Speedbar from SecondPower.com, and the GoHip! Web browser enhancement from GoHip.com change the Internet Explorer home page. You may be prompted to install one of these programs when you install other programs.

- Your administrator configured your home page by using the Microsoft Internet Explorer Administration Kit (IEAK), Group Policy, System Policy, or manual registry settings, for example, through a logon script.

RESOLUTION

Warning Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall your operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk.

To resolve this issue, follow these steps.

Note If you are running Microsoft Windows NT 4.0, Windows 2000, or Windows XP, you must log on as a user with administrator credentials to follow these steps. If your network system administrator used the IEAK, Group Policy, System Policy, or registry settings to configure your home page, contact your system administrator before you follow these steps:

1. Obtain and run a current antivirus program, with up-to-date virus definitions (signatures), and follow the instructions for cleaning or removing any viruses that are found. Microsoft does not provide software to stop virus infections or to clean infected computers. You may want to contact an antivirus software vendor for more information about how to remove a virus from your computer and how to help prevent future infections. If your computer has been infected, it may be open to additional forms of attack. For more information about how to determine if your computer is infected with a virus, worm, or trojan, how to recover from an infection, how to help prevent future infections from a virus, and how to contact antivirus software vendors, click the following article number to view the article in the Microsoft Knowledge Base:

[129972](#) Computer viruses: description, prevention, and recovery

For more information about how to recover an already compromised system, visit the CERT Coordination Center at the following CERT Web site:

http://www.cert.org/tech_tips/win-UNIX-system_compromise.html

Microsoft provides third-party contact information to help you find technical support. This contact information may change without notice. Microsoft does not guarantee the accuracy of this third-party contact information.

2. Open the Web site that you want to set as your home page in Internet Explorer.
3. Click **Tools**, click **Internet Options**, and then click **Use Current**. Restart your computer, and then restart Internet Explorer. If the issue is resolved, do not follow the remaining steps.
4. Perform a clean boot of your computer. For more information about how to clean boot your operating system, click the following article numbers to view the articles in the Microsoft Knowledge Base:
[310353](#) How to perform a clean boot in Windows XP
[281770](#) How to perform clean-boot troubleshooting for Windows 2000
[267288](#) How to perform a clean boot in Windows Millennium Edition
[192926](#) How to perform clean-boot troubleshooting for Windows 98
[243039](#) How to perform a clean boot in Windows 95
5. Repeat steps 2 and 3.

If the issue is resolved, you have installed third-party software that changed your Internet Explorer home page or code in the form of a malicious attack, such as an unknown virus has been run on your system. One of the startup items that were removed by using the clean boot method is causing the issue. Any startup items that run Regedit.exe or a .reg, .hta, .vbs, or .js file may be the cause of the issue. Leave any such startup items or suspected third-party software turned off, and then continue troubleshooting with the next step.

6. Click **Start**, and then click **Run**.
7. In the **Open** box, type **regedit**, and then click **OK**.
8. In Registry Editor, locate the following subkey, if it exists:
HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel
9. If the **ResetWebSettings** value or the **HomePage** value exists in this key, right-click the values, and then click **Delete**.

Note You may also want to verify any Web site information contained in the **Default_Page_URL**

value and the **Start Page** value in the following registry keys:
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main

HKEY_USERS\Default\Software\Microsoft\Internet Explorer\Main

10. On the **Edit** menu, click **Delete**, and then click **Yes** to confirm the deletion.
11. On the **File** menu or on the **Registry** menu, click **Exit** to quit Registry Editor.
12. Repeat steps 2 and 3. If the issue is resolved, turn on the startup items that you turned off in step 4 except for the items that may be causing the issue for example, commands that run Regedit.exe or a .reg, .hta, .vbs, or .js file. If the issue recurs, you turned on the startup item that was causing the issue. Repeat steps 4 through 11.

Important: After the issue is resolved, follow these steps to help prevent the problem from recurring:

- a. Do not run, save, or download a program from a source that you do not trust.
- b. Regularly use a current antivirus product.
- c. If you are running Microsoft Outlook 2000 or Outlook 98, upgrade to Outlook 2000 SR-2 or later, or install the Outlook 2000 SR-1 Extended E-mail Security update. To install this update, visit the following Microsoft Web site:
<http://office.microsoft.com/Downloads/2000/Out2ksec.aspx>
- d. If you are running Outlook Express, upgrade to Outlook Express 6 or later. Make sure that Active Scripting is turned off for e-mail and block e-mail attachments. For more information about how to do this, click the following article number to view the article in the Microsoft Knowledge Base:
[291387](#) Using virus protection features in Outlook Express 6
- e. If you connect to the Internet directly, use a firewall. For additional information about firewalls, visit the following Microsoft Web site:
<http://www.microsoft.com/security/articles/firewall.asp>
- f. If a virus or code in the form of a malicious attack has been run on your system, delete all Temporary Internet Files, Cookies, and Internet Explorer History items. For more information about how to do this, click the following article numbers to view the articles in the Microsoft Knowledge Base:
[260897](#) How to delete the contents of the Temporary Internet Files folder
[278835](#) How to delete cookie files
[157729](#) How to clear the History entries in Internet Explorer
You may also want to search your hard disk for files that may have been used by the virus or code in the form of a malicious attack and delete these files. For example, files named Rad*.tmp (where * is a random set of letters and numbers), any files containing "regedit" or ".reg" (for example, a file containing "C:\Windows\regedit.exe/s C:\Windows\System\radB9819.tmp"), or Windows.vbs are known to be associated with certain viruses.
- g. Regularly download and install all critical security updates. To do this, visit the following Microsoft Web site:
<http://windowsupdate.microsoft.com>
Some older versions of Windows and Internet Explorer may no longer be supported by Microsoft. As a result, the latest security patches may not be available for these products. For information about which products are still supported, visit the following Microsoft Web site:
<http://support.microsoft.com/?pr=lifecycle>
If your operating system or Internet Explorer version is no longer supported, you may want to upgrade so that you can receive the latest security patches.