

[Continue](#)

HOSTS file, which is necessary to make certain domain redirects, block websites, or remove malicious entries to the HOSTS file unless you open it directly from Notepad or another text editor. To do so: Open Notepad or another text editor like Notepad++. In the text editor, select File > Open and open the HOST file location at C:\Windows\System32\drivers\etc\. Select Text Documents (*.txt) in the bottom-right of the Open window and change it to All Files. This step is required because the HOSTS file doesn't have the .TXT file extension. When files appear in the folder, double click hosts to open it. Edit the HOSTS file and save your changes. In some versions of Windows, you don't have permission to save directly to the etc\ folder. If this is the case, you might see an error like this one when you try to save: *Access to C:\Windows\System32\drivers\etc\ hosts was denied*Cannot create the C:\Windows\System32\drivers\etc\hosts file. Make sure that the path and file name are correct. Instead, you must save the file elsewhere like the Documents or Desktop folder. After saving, go to that folder, copy the HOSTS file, and paste it directly into the location where the HOSTS file should be (C:\Windows\System32\drivers\etc\). You'll be prompted with permission validation and will have to confirm overwriting the file. If you still have trouble saving the modified HOSTS file, check the file's attributes to see if it's been marked read-only. Right-click the file and select Properties to see the attributes. Another option is to open your text editor program as an administrator so that the permissions are already applied to the editor. Then, saving the HOSTS file over the original can be performed without having to verify your admin credentials. If you still can't save to the HOSTS file location, you probably don't have the correct permissions to be editing files in that folder. You should be logged in under an account that has administrative rights over the HOSTS file, which you can check by right-clicking the file and going to the Security tab. The HOSTS file is the virtual equivalent of a phone company's directory assistance. Where directory assistance matches a person's name to a phone number, the HOSTS file maps domain names to IP addresses. Entries in the HOSTS file override DNS entries maintained by the ISP. While this hierarchy might come in handy for regular use, like to block ads or certain malicious IP addresses, its functions also make this file a common target of malware. By modifying it, malware can block access to antivirus updates or force you to a malicious website. Thus, it's a good idea to check the HOSTS file periodically or at least know how to remove false entries. A much easier way to block certain domains from your computer is to use a custom DNS service that supports content filtering or blocklists. Thanks for letting us know! Get the Latest Tech News Delivered Every Day [Subscribe](#) Tell us why!

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017

10/10/2017