Select a Tip ☞ How To: Update the HOSTS file in Windows 10/8 Go!

HostsNews blog & Updates

Blocking Unwanted Connections with a Hosts File

What it does ...

You can use a modified HOSTS file to block ads, banners, 3rd party Cookies, 3rd party page counters, web bugs, and even most hijackers and possibly unwanted programs. This is accomplished by blocking the connection(s) that supplies these little gems. The Hosts file is loaded into memory (cache) at startup, so there is no need to turn on, adjust or change any settings with the exception of the DNS Client service (see below). Windows automatically looks for the existence of a HOSTS file and if found, checks the HOSTS file first for entries to the web page you just requested. The **0.0.0.0** (prefix) is considered the location of your computer, so when an entry listed in the MVPS HOSTS file is requested on a page you are viewing, your computer thinks 0.0.0.0 is the location of the file. When this file is not located it skips onto the next file and thus the ad server is blocked from loading the banner, Cookie, or some unscrupulous tracker, or javascript file.

Example - the following entry **0.0.0.0 ad.doubleclick.net** blocks all files supplied by that DoubleClick Server to the web page you are viewing. This also prevents the server from tracking your movements. Why? ... because in certain cases "Ad Servers" like Doubleclick (and many others) will try silently to open a separate connection on the webpage you are viewing, record your movements then yes ... follow you to additional sites you may visit.

Using a well designed HOSTS file can speed the loading of web pages by not having to wait for these ads, annoying banners, hit counters, etc. to load. This also helps to protect your Privacy and Security by blocking sites that may track your viewing habits, also known as "click-thru tracking" or Data Miners. Simply using a HOSTS file is **not** a cure-all against all the dangers on the Internet, but it **does** provide another very effective "Layer of Protection".

In case you're wondering ... this all happens in microseconds, which is much faster than trying to fetch a file from half way around the world. Another great feature of the HOSTS file is that it is a two-way file, meaning if some parasite does get into your system (usually bundled with other products) the culprit can not get out (call home) as long as the necessary entries exist. This is why it's important to keep your HOSTS file up to Date. Get notified of MVPS HOSTS updates.

Special Note: new Windows 10 users ... the MVPS Hosts file installs just fine, no need to make any changes.

Simply follow the instructions for Windows 10/8

MVPS HOSTS now includes entries for most major parasites, hijackers and unwanted Adware/Spyware programs!

Started providing a HOSTS file in 1998 ... and now celebrating 20 yrs. proudly still the #1 rated HOSTS file on Google ...

To view the HOSTS file in plain text form. (476 kb) (opens in new browser)
Note: The text version also makes a terrific searchable reference for determining possible unwanted connections.

Download: hosts.zip [right-click - Select: Save Target As] [**Updated January-30-2018**]

If you find the MVPS HOSTS file useful ... please consider a donation ...

Important Note: The HOSTS file now contains a change in the prefix in the HOSTS entries to "0.0.0.0" instead of the usual "127.0.0.1".
This was done to resolve a slowdown issue that occurs with the change Microsoft made in the "TCP loopback interface" in Win8.1.

This change in the prefix should not affect everyday users. I've had some feedback that COMODO antivirus, and System Mechanic seems to have issues with the "0.0.0.0" prefix ... to resolve this issue:

You can use the "Replace" function in Notepad to convert the entries, or either of these freeware utilities (see below) has an option for converting the entries from "0.0.0.0" to "127.0.0.1.

This download includes a simple batch file (mvps.bat) that will rename the existing HOSTS file to HOSTS.MVP then copy the included updated HOSTS file to the proper location. For more information please see the Windows version that applies to you ...

Windows 10/8 install instructions see here
Windows 7 requires special instructions see here

When you run the (mvps.bat) batch file - right-click and select: **Run as Administrator**. Once updated you should see another prompt that the task was completed. Some users may see a pop-up from certain Security programs about changes to the HOSTS file. Allow the change ... however if you see this pop-up (changes to the HOSTS file) at any other time ... investigate.

Download Information: (checksum info is on the HOSTS file itself **not** the "hosts.zip")
MD5: 6B3CB66AA8E12586033D9FEA6C906E36 SHA-1: B62A9155DA784BE8E5C2029E0154DB9F00D2F29D

Manual Install Method - Unzip in a "temp" folder and place in the appropriate installed location:

- If you are having trouble downloading or extracting the HOSTS file [click here]
  Note: the below locations are for the typical default paths, edit as needed.

Windows 10/8/7 = **C:\WINDOWS\SYSTEM32\DRIVERS\ETC**

The actual location is defined by the following Registry key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DataBasePath

Windows DNS Client Service

Microsoft has done it again ... making changes to the Operating System, without any kind of explanation. If you upgraded recently to

Microsoft has done it again ... making changes to the Operating System, without any kind of explanation. If you upgraded recently to Windows 10 version 1709, most likely you will be unable to make any changes to the DNS Client, as it is grayed out. However if you had previously Disabled or set to Manual, the DNS Client Service you can still do so. Then to make things even worse ... the work-around Registry entries (see below) no longer apply in Windows 1709 ... they are simply ignored. To check your Windows version ... right-click the Start Menu and select > Run (type) winver (click OK)

thankfully Keith M sends along the following workaround ...

1) From sysinternals.com download the latest version of AUTORUNS -- Set it up to run however you choose, it doesn't require an explicit installation.

2) Run autoruns64.exe as **ADMINISTRATOR** and wait until it finishes it's scan.

3) In the program menu under OPTIONS, uncheck the "**Hide Windows Entries**" option

4) Go to the Services tab, scroll down to the Dnscache entry and clear (uncheck) the checkmark.

5) I'm not sure if it matters, but at this point, in the program menu, I selected FILE / SAVE, to save a copy of the new configuration settings.

6) Close autoruns64, reboot and check the services manager -- DNS Client is disabled.

If you decide that you want the DNS Client service running ... I made a little batch file that will flush the DNS whenever you desire. Open Notepad and enter the following:

ipconfig /flushdns

Then File > Save As > change the file type to All files, and name the batch file to flushdns.bat and place it in your Windows folder. Locate flushdns.bat right-click and select Send To > Desktop as shortcut.

Windows 10 (early versions) /8/7

In most cases the DNS Client Service is not needed, it is recommended to turn it off. These instructions are intended for a **single (home-user) PC**. If your machine is part of a "Domain", check with your IT Dept. **before** applying this work-around. This especially applies to Laptop users who travel or bring their work machines home. Make sure to reset the Service (if needed) prior to connecting (reboot required) to your work Domain ...

To resolve this issue (manually) open the "**Services Editor**"

- Start | Run (type) "**services.msc**" (no quotes)
  Win8 users - Control Panel > Administrative Tools > Services
- Scroll down to "**DNS Client**", Right-click and select: **Properties -** click **Stop**
- Click the drop-down arrow for "**Startup type**"
- Select: **Manual** (recommended) or **Disabled** click Apply/Ok and restart.

Hostsman or Hosts File Editor includes an option to turn off the DNS Service [screenshot]

When set to Manual you can see that the above "Service" is **not** needed (after a little browsing - when set to Manual) by opening the Services Editor again, scroll down to DNS Client and check the "Status" column. It should be blank, if it was needed it would show "Started" in that column. There are several Utilities that can reset the DNS Client for you ... [more info]

Important! If you are using **Network Discovery** then the DNS Client service is required and should **not** be set to either Manual or Disabled.

Workaround for using the MVPS HOSTS file and leaving the DNS Client service enabled (set to: Automatic)

- If you find after a period of time that your browser seems sluggish with the DNS Client service enabled you can manually flush the DNS cache
- Close all browser windows ... open a "Command Prompt" from the Start Menu > All Programs > Accessories > Command Prompt
  Win8 users - Charms Bar > Search > (type) command prompt > Select: Command Promt (left pane) Ok the UAC prompt
- (type) **ipconfig /flushdns** (press Enter) Then close the Command Prompt ...

A better Win10/8/7/Vista/ workaround would be to add two Registry entries to control the amount of time the DNS cache is saved. (KB318803)

- Flush the existing DNS cache (see above)
- Start > Run (type) regedit
  Win8 users - from the Charms Bar, select: Search (type) run and select Run (left pane) and (type) "regedit" (no quotes)
- Navigate to the following location:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters
- Click Edit > New > DWORD Value (type) **MaxCacheTtl**
- Click Edit > New > DWORD Value (type) **MaxNegativeCacheTtl**
- Next right-click on the **MaxCacheTtl** entry (right pane) and select: Modify and change the value to **1**
- The **MaxNegativeCacheTtl entry** should already have a value of **0** (leave it that way - see screenshot)
- Close Regedit and reboot ...
- As usual you should always backup your Registry before editing ... see Regedit Help under "Exporting Registry files"

For all other Questions, Issues and Solutions - see:The HOSTS File FAQ
For detailed Download and Extract Instructions - see: Download Help

Related Utilities

Hosts File Editor ... great little freeware program with all the features of Hostsman ...

HostsMan is a freeware application that lets you manage, Edit and Enable/Disable your Hosts file.
Includes an option to turn off the unneeded DNS Client Service [screenshot]

Includes an option to turn off the unneeded DNS Client Service. [screenshot]
This also has an option to update the existing HOSTS file when needed.
Important! - make sure you select: Default action - Overwrite

Once installed locate the Hostsman location, right-click on "hm.exe" and select: Properties
Click the Compatibility tab and select: "Run as Administrator" [screenshot]

Note: seems abelhadigital.com no longer exists. I have saved a copy of Hostsman, the installer version, since several other sites still offer Hostsman.

Rename the HOSTS file on the fly ... a simple one click batch file.

PowerShell script to automatically download, unzip and update the local host file.

Other Programs using the MVPS HOSTS file

- NOAD
- Virusface

Linux and Mac Users

Although I do not use either Linux or a Mac, I often get requests for "How To" on that system, so here are a few resources:

- Block unwanted advertisements with /etc/hosts file on Linux
- Mac OS X 10.2 or later
- Gas Mask is simple HOSTS File Manager for Mac OS
- Google Search

Various Troubleshooting Articles

- Hosts file is detected as malware in Windows Defender (Win8)
- How do I reset the hosts file back to the default? (Win8/7/Vista/XP)
- You cannot modify the Hosts file in Windows (Win8/7/Vista)

To contribute a listing for our resources, or any other comments: Contact

Donate

If you find the MVPS HOSTS file useful ... please consider a donation ...

Thanks to everyone involved for providing the online update notices for the HOSTS file. These updates are posted to most major security related sites, Newsgroups, and mailing lists, blogs etc. Get notified of MVPS HOSTS updates.

Return Home | Return to Previous Page | Return to Top