



# Blocking Unwanted Parasites with a Hosts File

Select a Tip 

How To: Deal with Unwanted Spyware and Parasites

Go!

[Hosts News blog](#)

```
127.0.0.1 www.adtomi.com 127.0.0.1 www.horseserver.net 127.0.0.1
127.0.0.1 www.baidu.com 127.0.0.1 www.imprenable.net 127.0.0.1
127.0.0.1 www.couponsandc .com 127.0.0.1
127.0.0.1 www.deepcom.com 127.0.0.1
127.0.0.1 www.errorpage40 acker.com 127.0.0.1
127.0.0.1 www.fastfind.org omepage.com 127.0.0.1
127.0.0.1 www.getupdate.com 127.0.0.1 www.msxpsupport.com 127.0.0.1
127.0.0.1 127.0.0.1 www.neededware.com 127.0.0.1
```

**There's no place like 127.0.0.1**

## What it does ...

The [Hosts file](#) contains the mappings of IP addresses to host names. This file is loaded into memory (cache) at startup, then Windows checks the Hosts file **before** it queries any DNS servers, which enables it to override addresses in the DNS. This prevents access to the listed sites by redirecting any connection attempts back to the local (your) machine. Another feature of the HOSTS file is its ability to block other applications from connecting to the Internet, providing the entry exists.

You can use a HOSTS file to block ads, banners, [3rd party Cookies](#), 3rd party page counters, web bugs, and even most [hijackers](#). This is accomplished by blocking the connection(s) that supplies these little gems.

Example - the following entry **127.0.0.1 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.

In many cases 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".

For Windows XP SP2 users you **should** see a Security Center prompt about allowing this connection. [[screenshot](#)]

Simply click No and continue. Yes the prompts can be annoying but at least you'll know, however you should **not** see these prompts if these entries are included in the HOSTS file.

**Note:** this prompt **only** occurs if (example) **\*.doubleclick.net** is included in the "[Restricted Zone](#)".

## More Examples

[AdTech](#) | [BridgeTrack](#) | [Honesty](#) | [Mgnetwork](#) | [ValueClick](#) | [Google AdSense](#) | [Atdmt](#) | [Atdmt](#)

Now here is a 3rd party ad server opening a connection to another 3rd party ad server - [Ad-Flow](#)

More 3rd parties opening other 3rd parties: [Overture](#) | [Overture](#) | [Directtrack](#) | [Directtrack](#) | [RealMedia](#)

**Note:** By placing these type sites in the [Restricted Zone](#) this also cures most "[Back Button](#)" issues.

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

Proudly now the **#1** rated HOSTS file on the Internet! - [Google](#) | [MSN](#) | [Yahoo](#) | [AltaVista](#)

Now regularly featured on the [Kim Komando](#) Radio Show

The MVPS HOSTS file has been selected by [Pricelessware](#) as "*the best of the best in Freeware*" for the 2nd time ...

**Editors Note:** As time has progressed the focus of this project has changed from just blocking ads/banners to protecting the user from the many parasites that now exist on the Internet. It doesn't serve much purpose if you block the ad banner from displaying as most other HOSTS files do, but get hijacked by a parasite from an evil exploit or download contained on the web site. The object is to surf faster while preserving your [Safety, Security and Privacy](#). [[more info](#)]



To view the HOSTS file in plain text form. (605 kb) (opens in 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 August-18-2010**]

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 [readme.txt](#) included in the download.



**Important! Windows Vista requires special instructions**  [see here](#)


**Important! Windows 7 requires special instructions**  [see here](#)

When you run the (mvps.bat) batch file XP users may [see a prompt](#), simply click Run and continue. 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 at any other time ... investigate.

**Download Information:** (checksum info is on the HOSTS file **not** the "hosts.zip")

**MD5:** CCBA5A1E037F4C5D1E8D0ACB3067526 **SHA-1:** 39B9A66E75A0717A7BE81CE47A262DDF8DB69147

**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 7/Vista/XP** = C:\WINDOWS\SYSTEM32\DRIVERS\ETC

**Windows 2K** = C:\WINNT\SYSTEM32\DRIVERS\ETC

The actual location is defined by the following Registry key:

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DataBasePath**

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 127.0.0.1 is considered the location of your computer, so when the entry (example) "**ad.doubleclick.net**" is requested your computer thinks 127.0.0.1 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 ActiveX, or javascript file.

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.

**Editors Note:** in most cases a large HOSTS file (over 135 kb) tends to slow down the machine.

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

- Start | Run (type) "**services.msc**" (no quotes)
- 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. [[more info](#)]

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](#)]

**Editors Note:** The above 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 ...

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

**Possible 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
- (type) **ipconfig /flushdns** (press Enter) Then close the Command Prompt ...

A better Win7/Vista workaround would be to add two Registry entries to control the amount of time the DNS cache is saved.

- Flush the existing DNS cache (see above)
- Start > Run (type) regedit
- 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"

JBF sends along this Tip: IPCOP running a DHCP server needs the DNS Client enabled to function.

**Reset the DNS Client with a simple batch file** (submitted by: Ronny Ong - 2K/XP only)

[DnsManual.bat](#) (resets the DNS Client to Manual) [right-click and select: Save Target As]

[DnsDisabled.bat](#) (resets the DNS Client to Disabled) [right-click and select: Save Target As]

**To use:** double-click on the downloaded file and reboot that's it ...

**For all other Questions, Issues and Solutions** - see: [The HOSTS File FAQ](#)

**For detailed Download and Extract Instructions** - see: [Download Help](#)

**How To Uninstall the MVPS HOSTS file**



## Related Utilities

- [WinPatrol](#) will allow you to lock your HOSTS file and will monitor changes. ★★★★★
- ZoneAlarm Pro and Security Suite users have a "Lock Hosts" file option. However this requires [special instructions](#) to edit **or** update the HOSTS file.



[HostsMan](#) is a freeware application that lets you manage your Hosts file.

Includes an option to turn off the [unneded DNS Client Service](#).

This also has an option to [update the existing HOSTS file](#) when needed.

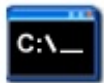
**Important!** - make sure you select: Default action - [Overwrite](#)

Use the Server option to replace the [Action Cancelled](#) message.

**Windows Vista** users ... once installed right-click on "hm.exe" and select: Properties

Click the Compatibility tab and select: "Run as Administrator" [[screenshot](#)]

This step was resolved in 3.2.71 Beta7. Win7 users see their documentation for more info.



[Rename the HOSTS](#) file on the fly ... a simple one click batch file. (Win9x/XP/Vista/Win7)



[HostsXpert](#) is a terrific multi-function Hosts File Manager [[screenshot](#)]

**Note:** no install required, it runs from anywhere ...

**You will need to turn off the DNS Client service manually** [[info here](#)]

When updating the HOSTS file make **sure** to use the Replace option, rather than Merge

---

[Homer](#) is a LocalHost webserver used to replace the [Action Cancelled](#) message.

[Download a custom image](#) for use in Homer.

Simply save (Save Target As) blocked.gif (2 kb) to the "\\Homer\Homer\images\" folder.

---

## Various Troubleshooting Articles

- [You cannot modify the Hosts file in Windows Vista/Win7](#)
- [Options for Using the Ipconfig Diagnostic Utility \(XP\)](#)
- [WinME users - Start | Run \(type\) "winipcfg" \(no quotes\)](#)
- ["The Page Cannot Be Displayed" Error Message \(XP\) \[more info\]](#)
- ["The Page Cannot Be Displayed" Error Message \(2K\)](#)
- [Repairs Winsock 2 settings \(usually spyware related\)](#)
- [How to Reset Internet Protocol \(TCP/IP\) in Windows XP](#)
- [How to Troubleshoot TCP/IP Connectivity with Windows XP](#)
- [How do I reset the hosts file back to the default?](#)

**To contribute a listing for our resources, or any other comments: [Contact](#)**

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.

**This site subscribes to the following: [General Criteria for Detection](#)**

[Return Home](#)

[Return to Previous Page](#)

[Return to Top](#)

Reproduction of information on this site, in any form, is prohibited without express written permission.

Microsoft and or MVPS.org are in no way affiliated with, nor offers endorsement of, this site.

[Website Privacy Policy](#) | [Disclaimer](#)

Copyright © 1998 - 2010 All rights reserved.



This work is licensed under a [Creative Commons License](#) Download this page as a PDF file

<http://www.mvps.org/winhelp2002/hosts.htm>