



How to restore access to Trend Micro and other security sites that have been blocked by malicious software infections

Solution ID: EN-1053403

Product: Client / Server / Messaging Suite for SMB - 2.0; Client / Server Suite for SMB - 2.0; Client Server Messaging Security for SMB - 3.0, 3.5, 3.6; Client/Server Security SMB - 3.0, 3.5, 3.6; HouseCall Server Edition - 6.1, 6.5, 6.6; OfficeScan - 7.0, 7.3, 8.0; PC-cillin Internet Security - 14 Dell, 14.7 Dell, 2005, 2005 Dell, 2006, 2007; ServerProtect for Microsoft Windows - 5.56, 5.58, 5.7; ServerProtect for Novell NetWare - 5.56, 5.58; Trend Micro Anti-Spyware Enterprise Edition - 3.0; Trend Micro Anti-Spyware for SMB - 3.0, 3.2; Trend Micro AntiVirus plus AntiSpyware - 2007, 2008, 2009; Trend Micro Internet Security - 2008, 2009; Trend Micro Internet Security for Dell - 16.6; Trend Micro Internet Security Pro - 2008, 2009; Worry-Free Business Security Advanced - 5.0, 5.1; Worry-Free Business Security Standard - 5.0, 5.1

Operating System: Windows - 2000, 2000 Advanced SP3, 2000 Advanced SP4, 2000 Professional, 2000 Professional Edition - SP4, 2000 Professional/Server with SP1 or above, 2000 series (SP 2), 2000 series (SP3up), 2000 Server, 2000 Server - SP2, 2000 Server - SP4, 2000 Server / Advanced Server with Service Pack 3 , 2000 Server Series SP4, 2000 server/advanced server w/ SP4, 2000 SP2, 2000 SP4, 2000 Standard SP3, 2000 Standard SP4, 2003, 2003 (32-and 64-bit), 2003 Enterprise Edition, 2003 Enterprise SP1, 2003 Enterprise SP2, 2003 R2, 2003 R2 (32-Bit), 2003 SBS SP1, 2003 Server, 2003 Server (SP1 or higher), 2003 Server Series SP1, 2003 SP1, 2003 SP2 (32-Bit), 2003 Standard (SP2 or higher), 2003 Standard 64-Bit, 2003 Standard Edition, 2003 Standard SP1, Live Communications Server 2003 Home Server, NT 4.0 with Service Pack 6a , NT series (SP 6a), NT Server/Workstation 4.0 with SP6a, NT Server/Workstation SP6a, Server 2003 Enterprise Edition, Server 2003 R2, Server 2003 Standard / Enterprise with Service Pack 1 , Server 2003 Standard Edition, Server 2003 Standard Edition - SP1, Server 2003 Standard Enterprise Edition, server 2003 Standard Enterprise Edition SP1, Server 2003 with R2, Server 2003 with SP1, Server 2008 Datacenter, Server 2008 Enterprise, Server 2008 Standard, SharePoint Portal Server 2003, SharePoint Service 2.0, SharePoint Service 2.0 with SP1, Small Business Server 2000, Small Business Server 2003, Storage Server 2003, Vista, Vista - SP1, Vista (32- and 64-bit), Vista (for OfficeScan 8 only), XP, XP - SP1, XP - SP2, XP - SP3, XP (32- and 64-bit), XP Professional Edition (SP 1)

Published: 3/31/2009 7:20 PM

Problem: Recently, malicious software, also known as malware, has resorted to disabling system access to security websites in order to prevent systems from receiving security updates or downloading cleanup tools. This solution will help users to access websites that may have been blocked by malware.

Solution: Malware that blocks access to security-related websites does so by poisoning the DNS cache or modifying the system's hosts file.

To restore access to these websites, you need to stop the client-side DNS cache service. You can do this using a command line or the Service Controller tool. Please see below for instructions:

Stop the Client-Side DNS Cache Service from a Command Line:

1. Click **Start > Run**.
2. Type "cmd" and click **OK** or hit ENTER.

Note: When typing in text such as passwords, filenames, or commands, do not include the quotation marks.

3. Type "net stop dnscache" and press ENTER.
4. Type "Exit" and press ENTER.

Stop the Client-Side DNS Cache Service Using Windows Services:

1. Click **Start > Run**.

2. Type "Services.msc" and click **OK** or hit ENTER.

Note: When typing in text such as passwords, filenames, or commands, do not include the quotation marks.

3. Double-click on the **DNS Client** service and click **Stop**.

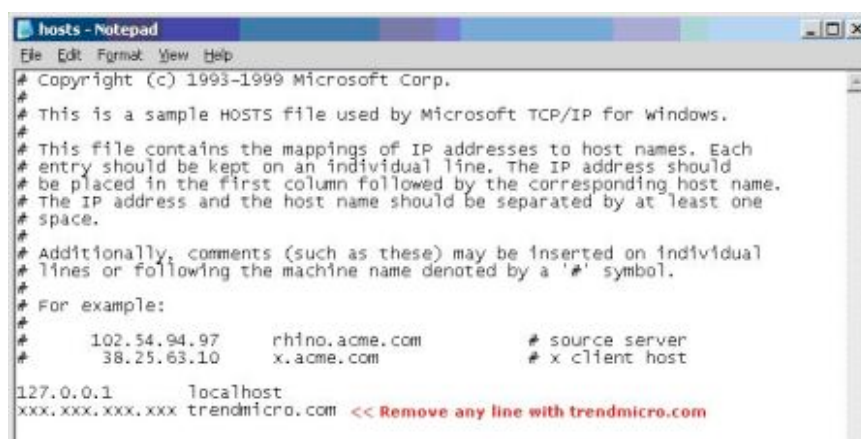
*Note: The name of the Windows DNS Client service may also appear as **Dnscache**.*

For additional details, refer to [Microsoft Knowledge Base article 318803](#).

Note: While the DNS Cache is stopped, user's web browsing experience may be slower than usual due to additional DNS queries needed to resolve the domain names for commonly accessed sites.

- Remove any erroneous entries in the system hosts file
 1. Click **Start > Run**.
 2. Type "notepad.exe %windir%\system32\drivers\etc\hosts"
 3. Remove any line containing "trendmicro.com" in the second column.
 4. Click **File > Save**.

Example:



```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10      x.acme.com           # x client host
#
127.0.0.1       localhost
xxx.xxx.xxx.xxx trendmicro.com << Remove any line with trendmicro.com
```

Once access to Trend Micro site is restored, users should update their products to the latest components and perform a full scan of their system to detect and remove any malware. Once all malware has been removed, restart the DNS Cache service to restore web browsing performance.

To restart the DNS cache service, users can either **restart the computer** or follow one of the procedures below:

- Stop the Client-Side DNS Cache service from a command line:
 1. Click **Start > Run**.
 2. Type "cmd" and then click **OK**.
 3. Type "net start dnscache" and then hit ENTER.
 4. Type "Exit" and then hit ENTER.
- Stop the Client-Side DNS Cache service using Windows Services:
 1. Click **Start > Run**.
 2. Type "Services.msc" and then click **OK**.
 3. Double-click the **DNS Client** service and then click **Start**.

Note: The name of the Windows DNS Client service may also appear as "Dnscache".

Print this page now

Close this window