TinyWall
A lightweight, non-intrusive firewall solution

TinyWall - Frequently Asked Questions

Contents

TinyWall - Frequently Asked Questions....1
General & Installation....1
What are the system requirements to run TinyWall?....1
How does TinyWall compare to other firewall products?....1
Why do I need a software firewall firewall? I already have a hardware firewall....2
How do I uninstall TinyWall?....2
Is TinyWall compatible with other security software?....2
After installation TinyWall is automatically granted internet access. Why?....2
Operating TinyWall....3
I installed TinyWall and now I cannot access the internet. What happened?....3
What is the use of the "Block" profile if TinyWall blocks all applications by default anyway? 3
What is the “Unblock local traffic” option for?....3
What is the difference between port-based and domain-based blocklists?....3
Application Specific Instructions....4
Windows Live applications (Mail, Messenger, Sync etc.)....4
Mozilla Firefox....4
Steam games....4
avast! Antivirus....4
AdMuncher....5
MailWasher....5
Virtual machines....5
Known Issues....6

General & Installation

What are the system requirements to run TinyWall?

TinyWall runs on all versions (including all editions and languages, 32bit and 64bit) of Windows 7 and Windows Vista. However, firewall tampering protection is not active on Windows Vista. Basic tests show that TinyWall also works on Windows 8 CTP. Windows Vista users need to install Microsoft .Net Framework 3.5 SP1 or newer.

How does TinyWall compare to other firewall products?

The traditional task of a firewall is to filter network traffic to ensure that no unwanted network communication takes place. In this regard TinyWall is just as reliable as any other paid firewall. Some other products include a Host-based Intrusion Prevention System (HIPS) which provides additional security, at the cost of incompatibility with some applications and the need for more user intervention. TinyWall does not come with HIPS functionality.

Why do I need a software firewall firewall? I already have a hardware firewall.

Hardware firewalls restrict traffic based on information in the network packets, like ports, hosts and protocols, but they are unable to determine what applications are communicating. If you allow HTTP/80 in your hardware firewall, you will be able to browse the internet, but you've also automatically given internet access to all other kinds of software you might not trust. A software firewall allows you to control applications separately.

Additionally, most consumer hardware firewalls are set up to only filter incoming communication. TinyWall will also let you control network traffic originating from your computer.

How do I uninstall TinyWall?

TinyWall v2 can be uninstalled from the Windows Control Panel just as any other software.

If you are using version 1.0.x, in TinyWall's tray menu go to Manage, select the Maintenance tab and click the Uninstall button there. If this button is greyed out, you first need to select Elevate in the tray menu to make sure you have the necessary privileges.

Is TinyWall compatible with other security software?

- TinyWall is compatible with all antivirus filesystem protections. For possible problems with other protection modules, see the FAQ section about Application Specific Instructions.
- With the exception of Windows Firewall, no other firewall software should be active while TinyWall is installed. Even if two firewall products can technically coexist, it is strongly discouraged to avoid user confusion.
- No compatibility problems have been detected with blocklisting software.
- If you are using HIPS software, make sure not to restrict TinyWall in the HIPS software.

After installation TinyWall is automatically granted internet access. Why?

This is to enable the automatic update checks and the download of updates for TinyWall. TinyWall does not send any information about the user or the computer over the internet. If you still wish to deny TinyWall access to the internet, disable TinyWall on the Special Exceptions tab.

Operating TinyWall

I installed TinyWall and now I cannot access the internet. What happened?

Upon installation TinyWall locks down your PC such that no network communication may take place. Use one of the "Whitelist by ..." options in the tray menu to unblock specific applications.

What is the use of the "Block" profile if TinyWall blocks all applications by default anyway?

TinyWall blocks all applications by default in some of its operation modes, including the "Normal" mode which is the standard mode of operation. The Block profile is useful to explicitly deny network access for an application even when the firewall mode is set to "Allow outgoing".

What is the “Unblock local traffic” option for?

It is an option to easily allow network traffic from/to the local network. It is most useful if you only wish to control internet traffic. When TinyWall is operating in “Normal” mode with this option is unchecked, it will block all traffic except for the defined exceptions. If “Unblock local traffic” is checked, traffic from/to the LAN will be allowed by default even in “Normal” mode. Basically, if this options is enabled, TinyWall behave as if the firewall was mostly disabled only for the local network.

What is the difference between port-based and domain-based blocklists?

Port-based blocklist is implemented as a firewall rule and blocks traffic based on port numbers irrespective of the remote host. Its goal is to undermine some common and known malware that use specific ports. It usually affects only specific (malicious) applications. Domain-based blocklist is implemented as a custom hosts file and blocks specific remote hosts irrespective of the port number. Its goal is to block certain hosts no matter what application tries to communicate with them, and in addition to malware it will also block some forms of internet advertising.

Application Specific Instructions

You might find that even though you have whitelisted the executable of an application, it still cannot connect to the internet. However, the conclusion that TinyWall is not working is probably wrong. This kind of issue is most often caused by whitelisting the wrong executable, or not whitelisting every executable needed for the operation of that particular program. Some applications use multiple executables to connect to the internet. If you do not unblock them all, it might appear that TinyWall is not working. This section is dedicated to list some of the most common applications that are „tricky“ in this respect.

In all of the answers below, if you cannot find the specified file in the „Program Files“ folder, also check in „Program Files (x86)“.

Windows Live applications (Mail, Messenger, Sync etc.)

Make sure to whitelist the following executables in addition to the main .exe of the application:

C:\Program Files\Windows Live\Contacts\wlcomm.exe
C:\Program Files\Common Files\microsoft shared\Windows Live\WLIDSVC.EXE

Mozilla Firefox

Videos, streaming media and some plugins might not work unless you unblock the following executable:

<firefox installation folder>\plugin-container.exe

Steam games

In addition to the main Steam executable, if you want to play games, make sure to whitelist the following executables. Depending on the game some of these files may not actually be present or may not need to be unblocked.

Steam.exe (autodetected by TinyWall)
Game executable (e.g. C:\Program Files\Steam\SteamApps\common\<game>\<game>.exe)
Game launcher (e.g. C:\Program Files\Steam\SteamApps\common\<game>\<game>Launcher.exe)

avast! Antivirus

Some shields of avast! work by redirecting other applications to the local computer, then making the internet connection themselves instead of the original program. As a result, avast! needs to be unblocked instead of your browser, for example, to be able to access the internet. The recommended solution is to unblock the „avast! Antivirus“ service in TinyWall. The downside is that you won‘t be able to control the applications separately that connect over this service. A second solution is to disable the corresponding avast! shield (for example, the Web Shield), but this is not recommended because you‘d loose that protection of avast!.

AdMuncher

AdMuncher works similarly to avast!, redirecting other applications to itself. The solution is to unblock AdMuncher in TinyWall.

MailWasher

MailWasher works similarly to avast!, redirecting other applications to itself. The solution is to unblock MailWasher in TinyWall.

Virtual machines

If you want to access the internet from the guest system of a virtual machine, whitelist the virtual machine software on the host system.

Known Issues

Known issues from version 1 have been resolved in version 2 of TinyWall. This section of the FAQ will be updated if new problems show up that are only going to be addressed in a future version. If you are experiencing strange behavior, be sure to upgrade to the latest version.