TinyWall

A lightweight, non-intrusive firewall solution

TinyWall - Frequently Asked Questions

Contents

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. Windows Vista users need to install Microsoft .Net Framework 3.5 SP1. However, firewall tampering protection is only active on Windows 7.

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.

How do I uninstall TinyWall?

To make sure that TinyWall cannot be removed by 3rd party applications, it is impossible to initiate removal from the Windows Control Panel. Instead, from 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.
- HIPS software should not be active while TinyWall is installed, or 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".

How do I edit the allowed and blocked ports for an application?

TinyWall encourages you to use one or more of the predefined profiles to unblock applications. If none of those profiles fit your needs, you have the option to specify further ports to be whitelisted for an application. In the profile association window for an application, click the "Advanced" button in the bottom left of the window to add custom ports to be whitelisted.

What is the difference between the HTTP(S) and the Web Browser profiles?

The "HTTP(S)" profile, as its name suggests, allows only the HTTP (TCP 80) and HTTPS (TCP 443) protocols. The "Web browser" profile allows, in addition to HTTP(S), some futher ports to support streaming multimedia and some common plugins.

What is the difference between the Outbound and the Blind Trust profiles?

"Outbound" allows an application to initiate TCP/UDP connections to any port of a remote machine. "Blind trust" also allows the application to listen for and accept incoming connection requests from remote machines. For most applications "Outbound" should be more than enough. "Blind trust" is needed for software that also act as a server and you cannot specify the specific ports the program should be allowed to listen on. "Blind trust" is the least tight/secure profile and should only be used when you have no other choice.

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

The issues listed below are the currently known defects. These are expected to be resolved in TinyWall v2.

Virtual machines

Furthermore, under some virtual machine solutions, TinyWall may loose configuration settings upon reboot. This only happens inside the virtual machine.

Windows Remote Desktop

TinyWall does not currently support accepting remote assistance using the default Windows software. However, you can still give remote assistance while using TinyWall.

Windows Home Networks

The „Network“ in Windows Explorer will not function properly while TinyWall is installed. File sharing is still possible when enabled in TinyWall. The recommended way to easily access your files on the network while TinyWall is installed is to mount the remote folder as a network drive locally.