TinyWall
A lightweight, non-intrusive firewall solution

TinyWall - Frequently Asked Questions

Contents

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 incompatiblity with some applications and the need for more user intervention. TinyWall does not come with HIPS functionality.

Is TinyWall compatible with other security software?

- TinyWall should be compatible with all antivirus software. None of the tested antivirus software conflicted with TinyWall.
- 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.

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 usefull 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.

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.

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.

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.