Malwarebytes Windows Firewall Control
User Guide
Version 6.0.2.0
04 March 2019

Notices

Third Party Project Usage

Malwarebytes software is made possible thanks in part to many open source and third party projects. A requirement of many of these projects is that credit is given where credit is due. Information about each third party/open source project used in Malwarebytes software – as well as licenses for each – are available on the following page.

https://www.malwarebytes.com/support/thirdpartynotices/

Sample Code in Documentation

The sample code described herein is provided on an "as is" basis, without warranty of any kind, to the fullest extent permitted by law. Malwarebytes does not warrant or guarantee the individual success developers may have in implementing the sample code on their development platforms. You are solely responsible for testing and maintaining all scripts.

Malwarebytes does not warrant, guarantee or make any representations regarding the use, results of use, accuracy, timeliness or completeness of any data or information relating to the sample code. Malwarebytes disclaims all warranties, express or implied, and in particular, disclaims all warranties of merchantability, fitness for a particular purpose, and warranties related to the code, or any service or software related thereto.

Table of contents

System requirements

Windows Firewall Control is compatible with the x86 and x64 versions of the following operating systems:

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows Server 2012
- Windows Server 2016

Windows Firewall Control is developed by using the Windows Presentation Foundation platform and requires .NET Framework 4.5 or a newer version. It is recommended to install the latest .NET Framework version because newer releases of the .NET Framework include speed improvements and also bug fixes.

The following Windows services must be enabled and running:

- **Windows Firewall** service. Windows Firewall Control is not a firewall by itself and requires Windows Firewall to be running.
- **DNS Client** service. This is required for the notifications system to work properly. If you use a router and this service is stopped, the remote IP address of the blocked connections will be the IP address of the router instead of the real IP address. Also, the log entries that are displayed in **Connections Log** will suffer from the same problem. It is recommended to not disable this Windows service.

Unsupported operating systems

- Windows XP and Windows Server 2003 are not supported and were never supported because Windows Filtering Platform was first introduced in Windows Vista.
- Windows Vista and Windows Server 2008 are not supported.
- Hyper-V Server free editions are not supported since they don't have a GUI. However, Windows Server with Hyper-V role installed is supported since this operating system has a desktop and GUI applications are supported.

- Windows Firewall is incompatible with software proxies, web filtering modules, NDIS drivers, any filtering modules that intercept network packets. These modules may redirect the network traffic to their proxies and the traffic will not reach anymore the Windows Firewall filtering driver. In this case, Windows Firewall rules do not apply correctly because the traffic appears to be made by the proxy, not by the original program. This incompatibility is between software proxies and Windows Firewall itself, not an incompatibility with Windows Firewall Control which does not have any control over this behavior.
- The notifications system is incompatible with old versions of some encryption programs (BoxCryptor, TrueCrypt) because they encrypt the file paths and the real paths can't be determined by Windows Firewall Control. If you use such security programs you have to try for yourself if this problem applies to your configuration or not.
- Due to multiple system configurations and software installed there may be incompatibility problems. Please report them and help to improve Windows Firewall Control.

Windows 10

- The keywords **Internet**, **Intranet**, **PlayTo Renderers**, **Remote Corp Network** which can be set in the Remote Addresses property of a rule from WFwAS are not visible in Windows Firewall Control. This is a problem caused by Windows Firewall API which does not provide these values at all. Editing or duplicating such rules which have these keywords set (for example, the rules from the default group named **Cast to Device functionality**) will remove them. This problem is also visible when exporting/importing partial policy files because this info is missing. However, when exporting/importing a full policy, this info is preserved.

Program parameters

The following command line parameters can be used when launching the file **wfc.exe**. These command line parameters work if the program is not running and also if it is already executing by sending these parameters to the existing running instance. Windows Firewall Control is a single instance application which can't be launched multiple times.

-mp
Open the **Main Panel**. This can be also achieved with a global hot key defined in the **Options** tab.

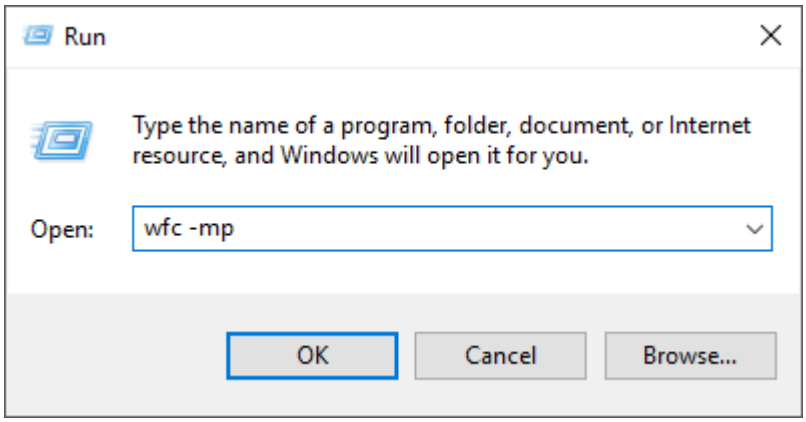
-rp
Open the **Rules Panel**. This can be also achieved with a global hot key defined in the **Options** tab.

-cp
Open the **Connections Log**. This can be also achieved with a global hot key defined in the **Options** tab.

-uninstall or **-u**
Launch the uninstall dialog. This works only if the program is not locked with a password. If the program is locked with a password nothing will happen. In this case please unlock the program and then try again to uninstall it.

-nogpu
Turn off GPU hardware acceleration when rendering WFC and use only the CPU instead. Use this when connecting remotely to a machine where hardware acceleration is not available.

The parameters can be used also in the **Run** dialog with the following syntax. Windows Firewall Control is registered under the App Paths key from Windows Registry, so it can be launched by entering just the exe filename, without the full path.



Keyboard shortcuts

The following keyboard shortcuts are defined and accepted by the program:

Esc or **Middle Mouse Button Click**
Close the active window or dialog. The difference between a window and a dialog is that a window can be resized and moved while a dialog has a fixed location and size.

CTRL + TAB
Switch between the **Rules Panel** and **Connections Log**. If the other window is not yet displayed it will be opened.

F5 or **CTRL + R**
Refresh the firewall rules displayed in the **Rules Panel** or the log entries from the **Connections Log**.

CTRL + F
Move the focus to the search box in **Rules Panel** or **Connections Log**.

ENTER
Open the **Properties Dialog** for the selected entry in **Rules Panel** and **Connections Log**.

F1
Open the user manual. Available in **Main Panel**, **Rules Panel**, **Connections Log**, **Notification Dialog**.

Silent installation

The following command line parameters can be used when launching the installer **wfc6setup.exe** to install/update Windows Firewall Control without requiring any user input. These command line parameters work only if the installer is launched with administrative privileges, otherwise they will be ignored. The parameters can be used in any order and some of them are optional.

-install or **-i**

This will launch the installation without asking the user any input. If the program is already installed and this parameter is used, it will be ignored. The installer will install Windows Firewall Control into the default folder, which is **C:\Program Files\Malwarebytes\Windows Firewall Control**.

-update or **-u**

This will automatically launch the update process without asking the user any input. If the program is not installed and this parameter is used, it will be ignored.

-run or **-r** (optional)

When using the parameters **-i** or **-u**, the installer window will remain open when the process completes. Use this parameter if you want to automatically launch **wfc.exe** and close the installer window.

-close or **-c** (optional)

When using the parameters **-i** or **-u**, the installer window will remain open when the process completes. Use this parameter if you want also to close the installer window without executing **wfc.exe**.

-noshortcuts (optional)

When **-install** parameter is used, use this to disable the creation of Windows Firewall Control shortcuts on Desktop and Start Menu.

-noautostart (optional)

When **-install** parameter is used, use this to disable the creation of Windows Firewall Control entry in the Startup list of Windows.

-norules (optional)

When **-install** parameter is used, use this to disable the creation of **Windows Firewall Control recommended rules**.

To install Windows Firewall Control into a different folder than the default one, for example in **C:\Program Files\ WFC**, you can also specify a custom path:

wfc6setup.exe -i -r "C:\Program Files\WFC" -noshortcuts

- The path must be enclosed in double quotes if it contains empty spaces.
- The folder that you specify doesn't have to exist, it will be created by the installer. However, if the provided path is not valid, the installer will append the provided path to the current execution folder and you may end up installing the program into a sub folder of the current path. So, make sure that the path is valid.
- To proceed with the installation into the default **C:\Program Files\Malwarebytes\Windows Firewall Control** folder, do not specify any folder in the parameters list. Just call: **wfc6setup.exe -i**

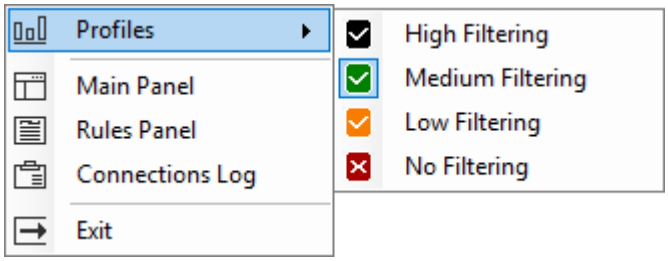
To silently update Windows Firewall Control and automatically launch it, use the following syntax:
wfc5setup.exe -update -run or **wfc5setup.exe -u -r**

User interface

Windows Firewall Control is a system tray application which sits in the notification area, next to the system clock. The icon of the system tray application displays the current profile that is set in the application.

Pressing the left mouse button on the icon will launch the **Main Panel** window.

Pressing the right mouse button on the icon will open the context menu below.



Profiles
Can be used to switch between the filtering profiles of the application.

Main Panel
Can be used to launch the **Main Panel** window.

Rules Panel
Can be used to launch the **Rules Panel** window.

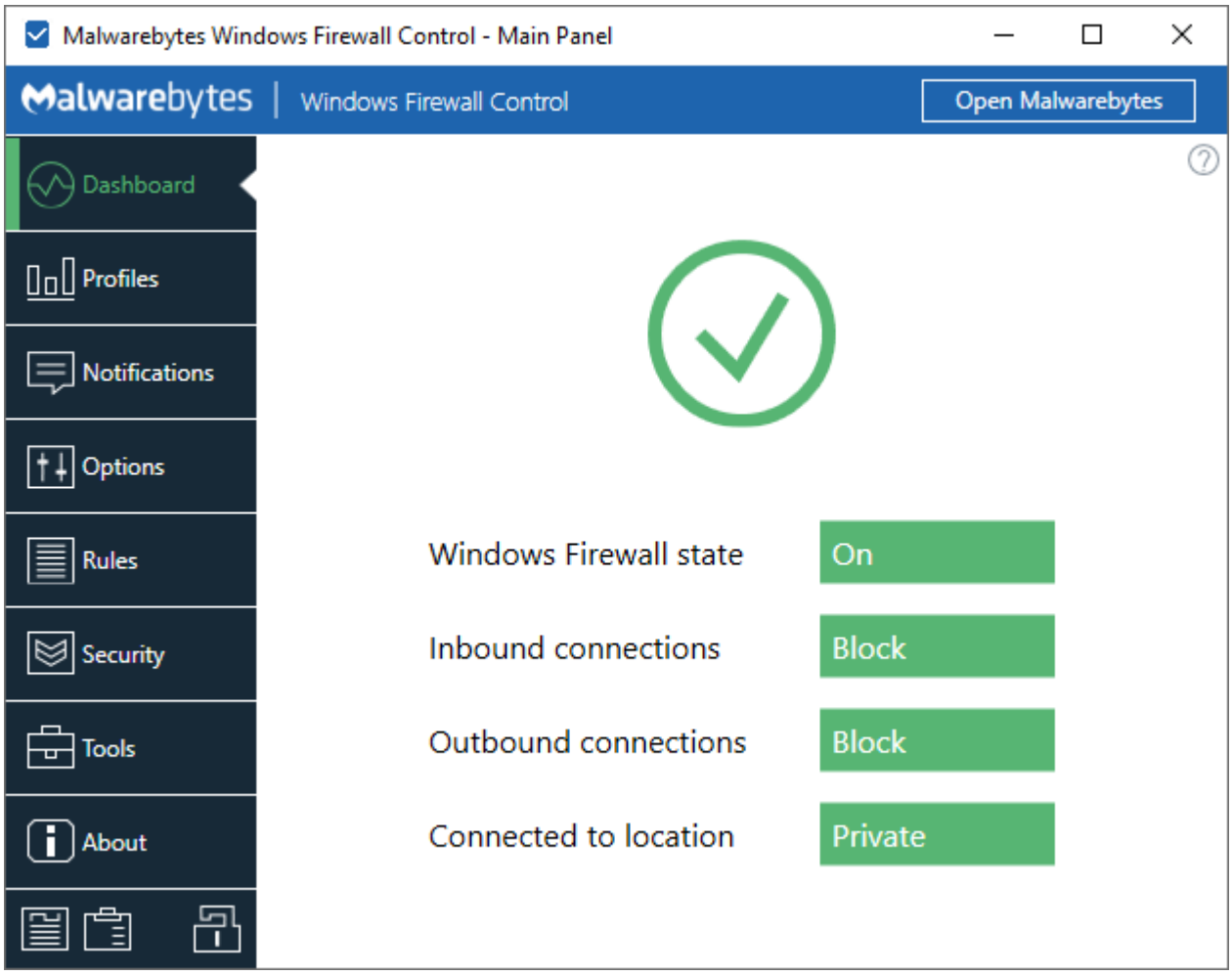
Connections Log
Can be used to launch the **Connections Log** window.

User manual
Can be used to open the online user guide. This context menu item is available only if the system tray application can't connect to Windows Firewall Control service.

Exit
Can be used to exit the system tray application. This will close the process **wfc.exe**. This does not affect the process **wfcs.exe** which is the background Windows service of Windows Firewall Control.

Main Panel

Main Panel is the main place where Windows Firewall Control can be configured. The first tab that is displayed is the **Dashboard tab** which displays the state of Windows Firewall, the status of inbound and outbound connections and the location to which Windows Firewall is located.



The layout of this window contains:

- a list of available tabs on the left side
- buttons on the lower left part of the window
- the content of the active tab on the right side

The following properties are saved when Main Panel window is closed and reused when the window is opened again:

- the size and the location of the window
- the vertical splitter position

The buttons

This will open the **Rules Panel**.

This will open the **Connections Log**.

This will open the lock dialog which can be used to lock the program. By locking the program the following items will become unavailable:

- the Windows Firewall Control interface
- the Windows Firewall Control Panel applet
- the management console snap-in for Windows Firewall with Advanced Security
- the uninstall dialog of Windows Firewall Control

Note that these will be unavailable even if Windows Firewall Control is closed. While the program is locked with a password do not attempt to force the uninstall of Windows Firewall Control by using a 3rd party software because you will not be able to access Windows Firewall interface any more. If you have forgotten your password, read the topic **The program is locked and I can't remember the password** from the **Troubleshooting** section.

Recommendation: Before setting your password, you can view it in plain text by checking the **Show password** check box. In this way you can be sure that you typed the password correctly.

While the application is in locked mode, instead of the default icons that reflect the profiles, the lock icons will be displayed.

The **Profiles tab** can be used to configure the current filtering level.

Filtering level

The filtering level specifies which connections should be allowed or blocked. Windows Firewall Control does not do any packet filtering and this means it does not allow or block any connection. This is done by Windows Firewall based on the firewall rules that are defined.

Inbound connections
In Windows Firewall inbound connections are by default blocked. A program can accept incoming connections only if it has an explicit inbound allow rule that permits the incoming connections to it. Otherwise they are blocked if no rule is defined. Changing the profile in Windows Firewall Control does not affect the filtering of inbound connections.

Outbound connections
When the profile is changed in Windows Firewall Control, only the outbound filtering capabilities of Windows Firewall is changed.

The following profiles are available in the Profiles tab. The profile can be also changed from the context menu of the system tray icon.

High Filtering

- All outbound and inbound connections are blocked. This profile blocks all attempts to connect to and from your computer.
- Windows Firewall does not contain this mode. To achieve this, when this profile is set in WFC, two new firewall rules are added to the firewall, named ***High Filtering profile - Block inbound connections*** and ***High Filtering profile - Block outbound connections*.** These two rules are defined to block all connections for all programs. These are two special rules and cannot be deleted from the Rules Panel. When the profile is switched to another profile, these two rules are automatically removed.

Medium Filtering

- Outbound connections that do not match a rule are blocked.
- Inbound connections that do not match a rule are blocked.
- Only the programs that have an allow rule can initiate outbound connections.
- When this profile is enabled the outbound filtering from Windows Firewall is enabled.
- When this profile is enabled the user must define an allow rule for each program that he wants to allow to connect to the Internet.

Low Filtering

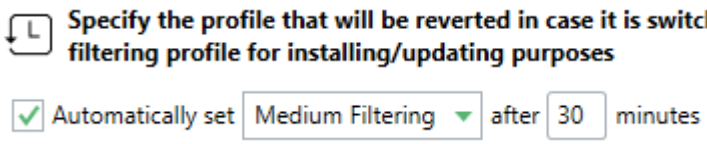
- Outbound connections that do not match a rule are allowed.
- Inbound connections that do not match a rule are blocked.
- Only the programs that have a block rule are blocked from initiating outbound connections.
- When this profile is enabled the outbound filtering from Windows Firewall is disabled and all programs without a block rule can connect to the Internet.
- When this profile is enabled the user must define a block rule for each program that he wants to block from connecting to the Internet.

No Filtering

- Windows Firewall filtering is turned off.

- All programs can connect to the Internet because the inbound and outbound filtering is disabled. This includes programs phoning home, including malware, telemetry traffic, etc.
- Avoid using this profile unless you have another firewall running on your computer.

Revert profile



There are situations when the user may want to disable temporarily the firewall protection:
- While installing a new software without the hassle of creating a new firewall rule for the installer that may download some files from the Internet.
- While debugging connectivity problems to see if the reason why a software can't connect is the firewall or the software itself which can't connect.

Windows Firewall Control can set an internal timer which can revert the **Medium Filtering** or **High Filtering** profile after a predefined period of time which can be set between 1 and 60 minutes. The timer is activated when the check box is checked or when the profile is switched. In the example above, if the profile is switched after 20 minutes, the timer will start again to count to 30 minutes. Also, if the process **wfc.exe** is restarted, this timer is considered to be elapsed immediately because the program doesn't know how much time it was closed.

Is it possible to allow LAN traffic when using High Filtering profile?

High Filtering profile is achieved by creating two generic block rules named ***High Filtering profile - Block inbound connections*** and ***High Filtering profile - Block outbound connections*.** These two special rules are removed automatically when the High Filtering profile is changed to a different profile. To allow the LAN traffic while High Filtering profile is enabled it is possible to modify the remote addresses of these two rules from **Rules Panel**. Note that only the **Remote Addresses** property of these rules can be modified, while other properties are read only.

Let's say the local network uses IP addresses from the following IP range 192.168.0.1-192.168.0.254. We have to set the remote IP addresses of these two rules with the following two IP ranges:

1.1.1.1-192.168.0.0,192.168.0.255-255.255.255.255

This means that the IP addresses from the excluded IP range **192.168.0.1-192.168.0.254** will not be blocked because they are not contained in the block rule, meaning that the LAN traffic will be still allowed while any other connections will be blocked.

The custom IP ranges defined for these two rules are reused when High Filtering is switched on and off until they are updated again.

The **Notifications tab** can be used to configure the notifications system.

Notifications mode

The notifications mode sets which blocked connections will generate notifications that will be displayed to the user. Since Windows Firewall Control displays notifications only for outbound blocked connections, the **Connections Log** can be used to debug connectivity problems if an inbound rule is also required.

The following notifications modes are available in the Notifications tab:

Display notifications

- A new notification is displayed for a blocked outbound connection if there is no matching firewall rule for the program that was blocked. Read below what a matching firewall rule means.

Learning mode

- When this notification level is used and a digitally signed program is blocked, Windows Firewall Control will automatically create an allow rule which will allow all connections of it. The program must retry the connection in order to connect after the allow rule is created. Most programs have a reconnect mechanism which is triggered automatically but some of them don't. If the program does not reconnect automatically, refreshing or restarting the program will make it to try again to connect.
- If a blocked connection is generated by a program that is not digitally signed or the signature is not valid, a new notification will be displayed to the user.
- It is not recommended to leave this notification level enabled for a long time. Use it for a limited period of time to automatically have created allow rules for the programs that are digitally signed.
- If the program is in the notifications exceptions list, then a new outbound allow rule will not be created when using this mode.

Disabled

- The notifications are not displayed to the user. The user has to create manually a new allow rule for each program that he wants to allow to connect to the network.
- When the notifications are disabled and some programs are blocked, the **Connections Log** can be used to debug connectivity problems. Use Connections Log to see the recently blocked connections. This will help to make an idea of what rules are still required based on the processes that were recently blocked.

Notifications exceptions

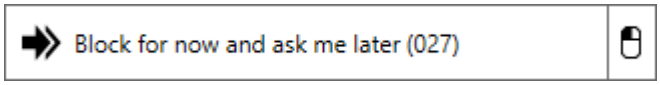
Outbound connections of **svchost.exe** and **System** are generated by the operating system and are related to different functionalities of the operating system, like: Core Networking, File and Printer Sharing, Network Discovery, Telemetry, Windows Update, etc. Because **svchost.exe** is used by all Microsoft Windows services to connect to the network, it may generate endless connections attempts in a very short period of time. Most users are interested in notifications for their custom programs and don't want to be bothered with system notifications. For this reason, certain users may want to disable the notifications of **svchost.exe**, **System** or the notifications of programs which are installed in a certain folder.

Wildcards (*) are not supported. The current algorithm checks if the path of the program that was blocked starts or ends with one of the strings defined in the notifications exceptions list.

Notifications options

Automatic close a notification

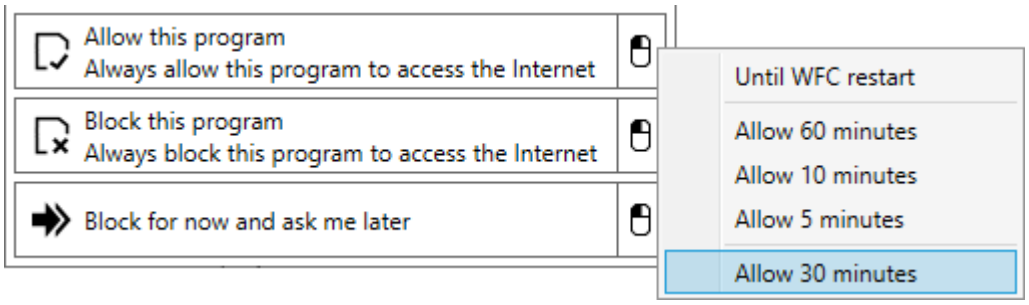
When the notification dialog is displayed on the screen it has a timeout that will automatically close the dialog if there is no user intervention. This timeout is displayed in the **Block for now and ask me later** button from the notification dialog.



This timeout can be set between **1** and **999** seconds. The timeout is automatically removed if the user moves the mouse cursor over the notification dialog or if the timer is set to **0**. If the computer is idle for a long period of time and the user wants to see all notifications that have occurred while he was away from the computer, this timer can be set to **0** to avoid the automatic closing of the notification dialog. However, this is not recommended. Programs that were blocked in the past will be blocked in the future too since they have no rule. These notifications will be displayed again.

Custom timeout for temporary rules

From the notification dialog the user can create a temporary rule that will be automatically removed when it expires. Creating a temporary rule can be made by pressing on the right side button and choosing one of the options from the context menu that appears.



A temporary rule can be set to expire when Windows Firewall Control is restarted, after 60, 10 or 5 minutes. There is also this custom timeout which can be set between 1 and 60 minutes.

Display notifications on top of other windows

A program window is displayed by default with the same priority like any other windows. By having this option enabled, the notification dialog will be displayed on screen on top of the other windows. This includes a full screen video that is playing, a game or an application that is running, etc. This setting does not work for metro style applications because they are running on a different screen than the regular desktop. This setting works for desktop application.

Play a sound when a new notification is generated

It is possible to have an acoustic alert when a new notification is displayed. This can be useful when using metro style applications because the notification dialog can't be displayed on top of metro style applications. The program can play a default sound or a custom sound which must be in **.wav** format. The notification sound can be also played by pressing on the corresponding radio buttons.

Advanced notifications settings

When a new connection is blocked, the notifications system searches through the existing firewall block rules to see if there is a matching block rule for the same file path, which may have blocked the connection. If a matching block rule is found a new notification dialog is not displayed because it means that the user already blocked that connection by a firewall rule and does not want to see again a new notification for it. If a matching rule is not found then a new notification is displayed. The advanced notifications settings can be used to specify which rules should be used when searching for matching rules.

Use allow rules
All blocked connections are logged into the same Security event log of the system. A blocked connection can be blocked by Windows Firewall, by an external program like PeerBlock, by a custom hosts file, etc. Because all blocked connections are logged into the same place and the source is not available, the notification system doesn't know why a connection was blocked. It just receives a blocked connection event and then it searches if there is a firewall rule that is matching the blocked connection. If an allow rule that matches the blocked connection is found a new notification should not be displayed. This setting is useful for scenarios where blocked connections can be generated from multiple sources.

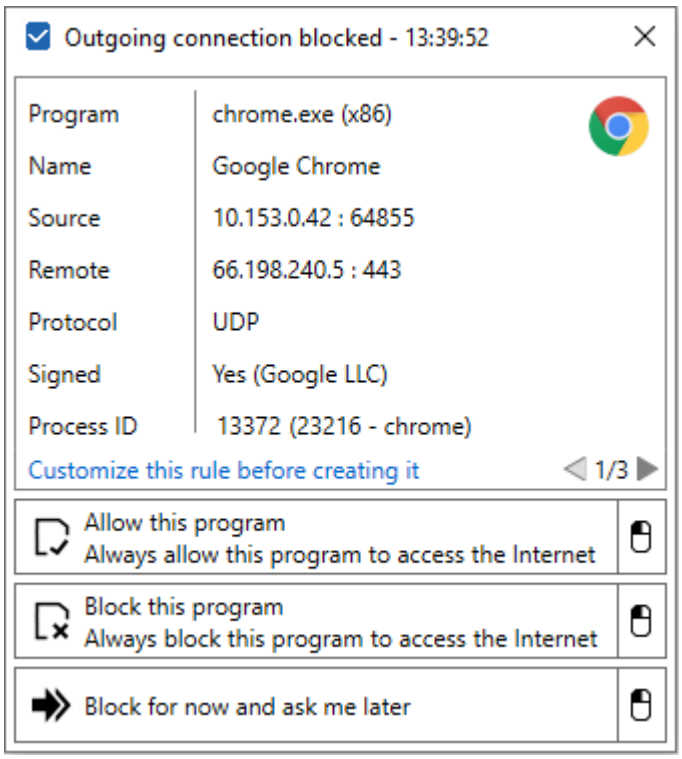
Use generic block rules
When searching for a matching block rule, the notifications system searches through the firewall rules that have the same path as the program that was blocked. But the blocked connection could be a result of a firewall block rule that is applied for all programs. By enabling this setting, the notifications system will extend the search for a matching rule also through the firewall block rules that apply to all programs.

Use disabled rules
This setting will extend the search for matching rules through the disabled rules too. Note that the disabled rules are not applied by Windows Firewall unless they are enabled.

How does the notifications system work?

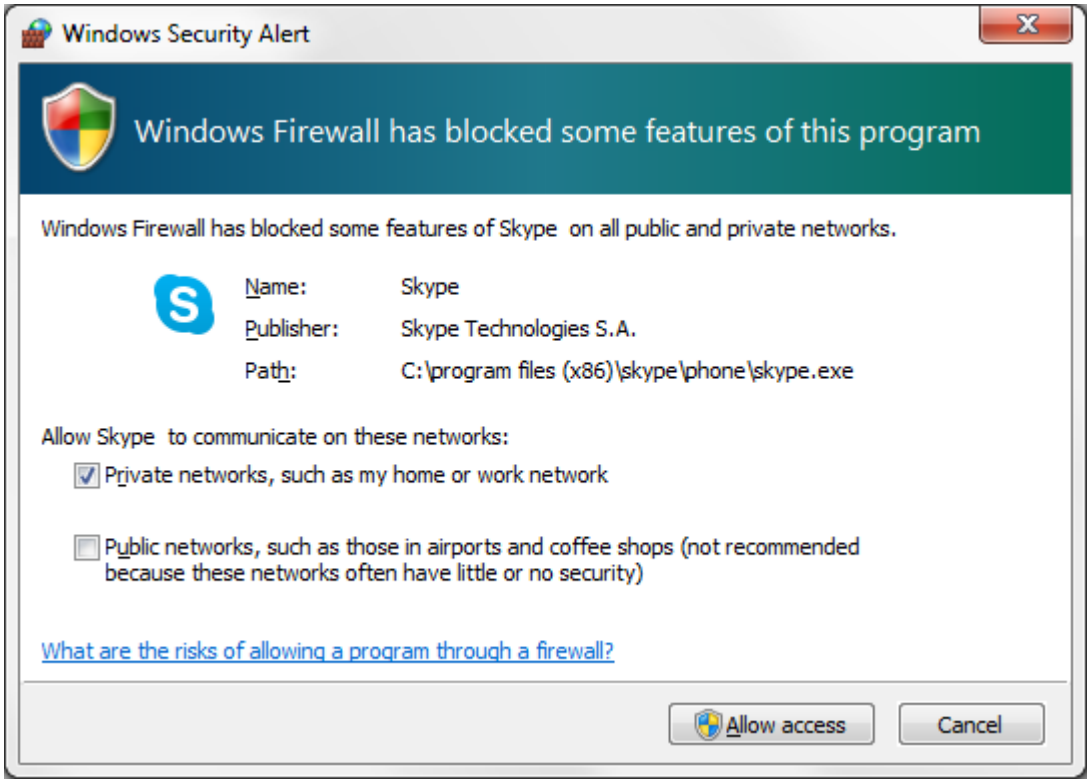
Windows Firewall Control doesn't do any packet filtering to inspect the network traffic. This is done by Windows Filtering Platform. Each time a network packet is dropped, Windows Firewall generates a new event in the Security event log of the system. Windows Firewall Control is subscribed to these events and based on the existing firewall rules it decides if a new notification should be displayed or not. This is done by searching through the existing firewall rules to see if there is a rule that matches the blocked connection that was recorded in the Security event log. The events about a blocked outbound connection are raised after the connection is blocked. This means that a notification dialog is displayed for an already blocked connection, not for a paused connection, therefore the notification dialog can't have an **Allow for now and ask me later** option. After creating an allow rule, the program that was blocked must retry the connection in order to connect based on the newly created allow rule.

The notifications displayed by Windows Firewall Control are for outbound blocked connections and they work only when **Medium Filtering** profile is used. When enabling Medium Filtering profile, the outbound filtering is enabled in Windows Firewall and this means that all programs without an allow rule are blocked by default. The **Connections Log** contains the entries filtered from the Security log of the system. The same entries are the source of notifications displayed by Windows Firewall Control.



Windows Firewall notifications

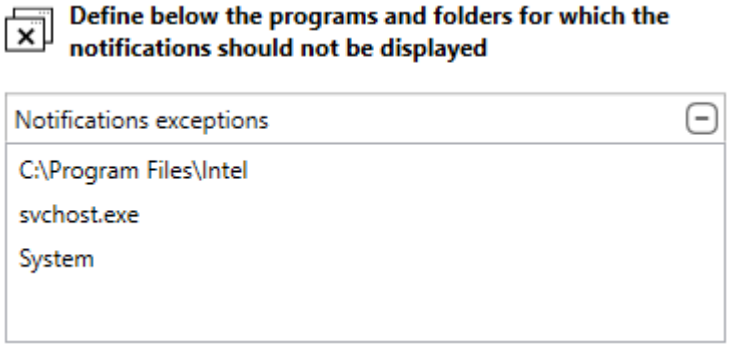
Windows Firewall itself displays security alerts for programs, other than Windows services, that attempt to listen for unsolicited incoming traffic and the incoming traffic is blocked. These security alerts can be disabled from Windows Firewall and are not configurable from Windows Firewall Control.



Pressing the **Allow access** button will create a new inbound allow rule, while pressing the **Cancel** button will create a new inbound block rule.

How to stop entirely the notifications for a program?

Let's say that we have a program for which we already defined an allow rule for a specific IP range only. When this program connects to a different IP a new notification will be displayed for it which is correct. But we don't want to see a new notification for this program because we wanted to allow just a specific IP range and that's all. To disable the unwanted notifications for a program, add a new exception in the notifications exceptions list available in the **Notifications tab**.



In the example above, all blocked connections that have the path starting with **C:\Program Files\Intel** or ending with **svchost.exe** or **System** will not generate a new notification.

Adding a new notification exception can be done also from the notification dialog.

Why there is no "Allow for now and ask me later" button?

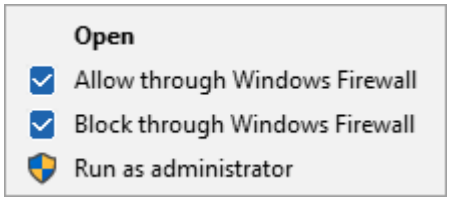
The notifications are displayed for blocked connections, not for paused connections. It is not possible to resume a connection at Windows Firewall Control level because it doesn't do any packet filtering.

Options tab

The **Options tab** can be used to set various program options.

Shell Integration

This setting will add two new entries into the context menu of the executable files and the context menu of shortcuts to the executable files.



Through these two context menu options, the user can create easily a new allow or block rule when browsing through My Computer or from the desktop shortcuts. Multiple files can be selected but not more than 15 files. If more than 15 files are selected, the operating system hides these entries from the context menu. This setting is applied for all user accounts.

When a new rule is created through the shell context menu, a confirmation dialog is displayed above the system clock. If multiple files were selected, the confirmation dialog will be displayed only for the last selected file.

Start automatically at user logon

When this option is checked a new entry is created for **wfc.exe** in Windows Registry under the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

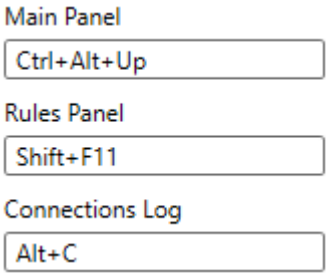
This entry is available to all Windows user accounts and will launch the program for all user accounts.

User interface language

This can be used to change the user interface language. The combo box loads and displays all valid files with the extension **.lng** which are found in the **lang** subfolder. Please note that some translation files may be outdated. Windows Firewall Control installer contains the last versions of the translations that were received from WFC users. The English version (**wfcEN.lng**) is always the most updated. If you have an updated translation file, please send it to support@binisoft.org and it will be included in the next release.

Global Hot-Keys

The global hot keys are keyboard shortcuts that can be used from any program to launch a specific action. They can be used while having no program open on desktop or while other programs are running and have the focus.



The following modifier keys **Ctrl, Alt, Shift** are accepted in any combination with the **A - Z** keys, **Arrow keys** and **F1 - F12** keys. Other keys are not accepted and there is no plan to make them available. The global hot keys are defined for the current user account only.

User settings

Windows Firewall Control stores the program settings in Windows Registry. From the Options tab the user can:

Import user settings from a file

A settings file with the extension **.wfs** must be provided. Importing a settings file will restart the program in order to reload all the global and user settings.

Export user settings to a file

This will export the program settings to a file with the **.wfs** extension. This file uses an XML format and can be edited in any text editor.

Restore all settings to the default values

This will remove all the global and user settings that are stored in Windows Registry regarding Windows Firewall Control and will restart the program with the default values.

The **Rules** tab can be used to specify some default properties for the newly created firewall rules and also for importing and exporting purposes.

Rule direction

A firewall rule can be defined to allow outbound requests for a program which will allow it to connect to the Internet, or can be defined to allow inbound requests which will allow the connection requests that are sent from the network to your computer.

Outbound (recommended)
When creating a new firewall rule from Windows Firewall Control it will be created for outbound connections. These kind of rules are required if you want to allow a program to connect to the network/Internet.

Inbound
When creating a new firewall rule from Windows Firewall Control it will be created for inbound connections. Avoid to create these kind of rules because they allow your computer to be visible and accessible from the network/Internet. Inbound rules are required when you want to be able to ping your computer from another computer or to make it visible into the local network.

Outbound and inbound
When creating a new firewall rule for a program, two rules will be created: one outbound rule and one inbound rule. This is not recommended since not all programs need inbound access. Having an inbound rule for each program that usually needs outbound access is not required.

Rule location

Windows Firewall supports multiple simultaneously active profiles. Each network adapter card attached to a network is assigned one of the following locations:

Domain
The domain location applies to a network when a domain controller is detected for the domain to which the local computer is joined.

Private
The private location applies to a network when it is marked private by the computer administrator and it is not a domain network.

Public
The public location applies to a network when the computer is connected directly to a public network, such as one available in airports and coffee shops.

Import, export or restore firewall rules

Windows Firewall offers the possibility to export and import all the firewall rules through a proprietary format. This file format has the **.wfw** extension. This functionality can be used to export a copy of the firewall rules which can be used on another computer or as a backup copy. The limitation of this import/export is that it works only for the entire set of firewall rules. From the **Rules Panel** the user can also export only a custom set of firewall rules instead of all of

them. For this, Windows Firewall Control uses a different file format which has the extension **.wpw**. This is an XML file format and it can be edited in any text editor.

In order to support importing/exporting through files located on network shares, the import and the export are made through temporary files which are created in the temporary folder.

Import Windows Firewall rules from a file

Importing a policy file has two different results based on the file format that is being imported. Importing a **.wfw** file will overwrite all the existing firewall rules. Importing a **.wpw** file will add the rules contained in the file on top of the existing firewall rules.

Export Windows Firewall rules to a file

Exporting the Windows Firewall set of rules from this place will generate a **.wfw** file. It can be used for backup purposes or for migrating all the firewall rules to another operating system.

Restore Windows Firewall default set of rules

Restoring Windows Firewall default set of rules will overwrite all of the existing firewall rules. The Windows Firewall default set of rules includes the firewall rules that are created when the operating system is installed.

Restore Windows Firewall Control recommended rules

This will recreate a minimal set of firewall rules that are known as **Windows Firewall Control recommended rules**.

How to allow connections only when I'm connected to my VPN?

Regarding VPN only connections, you can create your rules and play with the Location property of the rules. Usually, when the VPN connects, your Location is Public. When you disconnect the VPN you should be back on Private location. Knowing this, you can create two sets of rules which will apply depending on which Location is set at certain time. Since the connect/disconnect of the VPN will change the Location, then you can use this to make two different set of rules which will apply when the VPN is connected/disconnected.

How to find which firewall rule blocked or allowed a connection?

Unfortunately, there is no way to say which rule actually blocked or allowed a connection because when Low Filtering profile is used, meaning that outbound filtering is disabled, all connections without a block rule are allowed. So, there is no rule that allowed the connection. The same applies if Medium Filtering profile is used, meaning that outbound filtering is enabled, all connections without an allow rule are blocked. There is no rule that blocked the connection. In Windows Firewall, multiple firewall rules may match a blocked or allowed connection, so, is not that easy to find out which rule actually blocked or allowed a connection.

Windows Firewall Control recommended rules

Windows Firewall Control recommended rules is a minimal set of firewall rules which can be used with Windows Firewall while the following functionalities are still available:

- Web browsing. An allow rule for the web browser is still required.
- Network discovery - Discover other computers from your network and allow other computers to discover your computer.
- Network printing - Allow printing on a printer from your network.
- PING other computers and respond to PING command.

- Windows time synchronization.
- Windows updates.

These rules are prefixed with **WFC** and can be easily distinguished in **Rules Panel**.

Name	Program	Location	Enabled	Action	Direction	Local ports	Remote addresses	Remote ports	Protocol	Service
WFC - Core Networking - DNS (UDP-Out)	C:\WINDOWS\system32\svchost.exe	All	Yes	Allow	Out			53	UDP	dnscache
WFC - Core Networking - Dynamic Host Configuration...	C:\WINDOWS\system32\svchost.exe	All	Yes	Allow	Out	68		67	UDP	dhcp
WFC - File and Printer Sharing (NB-Session-Out)	System	Domain, Private	Yes	Allow	Out		LocalSubnet	139	TCP	
WFC - File and Printer Sharing (SMB-Out)	System	Domain, Private	Yes	Allow	Out		LocalSubnet	445	TCP	
WFC - File and Printer Sharing (Spooler-Out)	C:\WINDOWS\system32\spoolsv.exe	Domain, Private	Yes	Allow	Out		LocalSubnet		Any	
WFC - Internet Control Message Protocol (ICMPv4-Out)	System	All	Yes	Allow	Out				ICMPv4	
WFC - Internet Control Message Protocol (ICMPv6-Out)	System	All	Yes	Allow	Out				ICMPv6	
WFC - Network Discovery (NB-Name-Out)	System	Domain, Private	Yes	Allow	Out		LocalSubnet	137	UDP	
WFC - Network Discovery (SSDP-Out)	C:\WINDOWS\system32\svchost.exe	Domain, Private	Yes	Allow	Out		LocalSubnet	1900	UDP	Ssdpsrv
WFC - Windows Time Service	C:\WINDOWS\system32\svchost.exe	All	Yes	Allow	Out			123	UDP	W32Time
WFC - Windows Update	C:\WINDOWS\system32\svchost.exe	All	Yes	Allow	Out			80,443	TCP	
WFC - Windows Firewall Control Updater	C:\Program Files\Windows Firewall Control\wfc.exe	All	Yes	Allow	Out			80,443	TCP	
WFC - File and Printer Sharing (SMB-In)	System	Domain, Private	Yes	Allow	In	445	LocalSubnet		TCP	
WFC - Internet Control Message Protocol (ICMPv4-In)	System	All	Yes	Allow	In				ICMPv4	
WFC - Internet Control Message Protocol (ICMPv6-In)	System	All	Yes	Allow	In				ICMPv6	
WFC - Network Discovery (NB-Name-In)	System	Domain, Private	Yes	Allow	In	137	LocalSubnet		UDP	
WFC - Network Discovery (SSDP-In)	C:\WINDOWS\system32\svchost.exe	Domain, Private	Yes	Allow	In	1900	LocalSubnet		UDP	Ssdpsrv

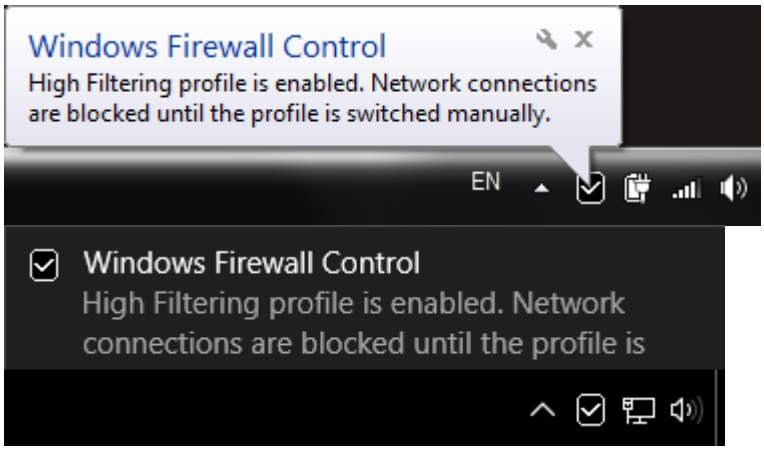
- This minimal set of rules contain only a few outbound and inbound rules. When only these rules are used, some of the features of the operating system may not work unless other required rules are added. This is a minimal set of firewall rules that can be used as a starting point. On top of these firewall rules, add new firewall rules for your custom programs when they require access. All those hundreds of firewall rules that Windows Firewall has by default are not required.
- The recommended inbound rules are required if you want to allow other computers from your network to access your computer. If you don't want other computers to PING your computer or connect to your shared folders, then these inbound rules can be removed.
- The firewall rules for ICMPv4 and ICMPv6 protocols are used strictly for PING command. If you don't use this functionality, they can be removed.

Security tab

The **Security tab** can be used to specify the security enhancements that will be enforced by Windows Firewall Control.

Secure Boot

Secure boot will automatically set High Filtering profile when a system shut down event is detected by the program. The network connections will be blocked at Windows start-up until the user manually changes the profile to another filtering profile. While the High Filtering profile is enabled, when Windows Firewall Control is started, a notification will be displayed informing the user about this.



Secure Profile

In Windows, a software executed with administrative privileges can import a custom policy file and modify outbound and inbound filtering settings of the firewall, or can even disable Windows Firewall. Windows Firewall Control can prevent these external changes. When this feature is enabled, changing the filtering mode of Windows Firewall can be done only through the Windows Firewall Control user interface, from the **Profiles tab**. Also, importing a policy file with the wfw extension is possible only from Windows Firewall Control. This feature is automatically disabled when Windows Firewall Control is uninstalled.

Secure Rules

In Windows, all programs executed with administrative privileges can add Windows Firewall rules. There is no way to prevent this in Windows Firewall. One way to protect against this is to have UAC enabled which will inform the user each time an application requires elevated privileges.

Windows Firewall Control is notified when a new firewall rule is added and can delete or disable any unauthorized rule that is being added by other programs. Any rule which is created with the group name different than the defined authorized group names is considered to be an unauthorized rule. Based on the user choice, these unwanted firewall rules will be deleted or disabled. Disabling the rules instead of deleting them is useful for reviewing purposes because the user has the opportunity to see which programs have this hidden behavior. Usually, a software should not add new firewall rules without asking the user, but unfortunately there are programs that try to enforce their own created firewall rules no matter what. One example is Steam service.

The list of authorized groups contain the following predefined group names which can't be removed:

- **Windows Firewall Control** - This group name is used by default for all firewall rules created from Windows Firewall Control.
- **Temporary Rules** - This group name is used when creating temporary rules from the notification dialog.

When Secure Rules is set to disable unauthorized rules, Windows Firewall Control will automatically disable these rules and will add the "U - " prefix to the rule name. This applies to the newly created firewall rules and to existing ones.

Allow Windows Store rules - Ensures that Windows Store apps are excluded from the logic of Secure Rules. The firewall rules created when a new Windows Store application is installed will not be disabled or deleted.

Import group names from the current existing rules

The group names from the existing firewall rules that are displayed in Rules Panel will be added in alphabetical order to the list of the authorized group names.

Tools tab

The **Tools tab** can be used to launch various system tools and to specify the online services that are used by the program.

System utilities

The existing shortcuts can be used to launch various system utilities. These programs will be started by the Windows Firewall Control service and will be executed with the highest privileges available. The following tools are available:

Windows Firewall with Advanced Security

This will launch the management console snap-in which provides access to Windows Firewall advanced options. This is the integrated user interface of Windows Firewall.

Windows Firewall Control Panel applet

This will launch the control panel applet of Windows Firewall.

Event Viewer

This is a component of the operating system that lets administrators and users view the event logs on a local or remote machine.

Resource Monitor

This is an utility from Windows that displays information about the use of hardware (CPU, memory, disk and network) and software (file handles and modules) resources in real time. This utility can display the current active network connections, which is a feature often requested by Windows Firewall Control users. This is already available and there is no plan to implement this functionality in Windows Firewall Control.

Online services

The user can configure several online services that are used from the **Notifications Dialog**, **Rules Panel** or **Connections Log**. Since there are not many alternatives for these online services, all of them are already defined and the user can only choose which one to use. Custom providers can't be defined by the user.

About tab

The **About tab**, besides the regular info about the program, can be used to update the program.

Check now if a new version is available

This button can be used to check online if a new version of the program is available. This will connect to an XML file from the website and will compare the version specified in that file with the current version of the program. While using Medium Filtering profile, to be able to check for an updated version, a firewall rule for **wfc.exe** is required. This rule should allow all connections on TCP protocol and remote ports 80,443. Windows Firewall Control recommended rules contain a rule named **WFC - Windows Firewall Control Updater** for this purpose.

Automatic check for updates

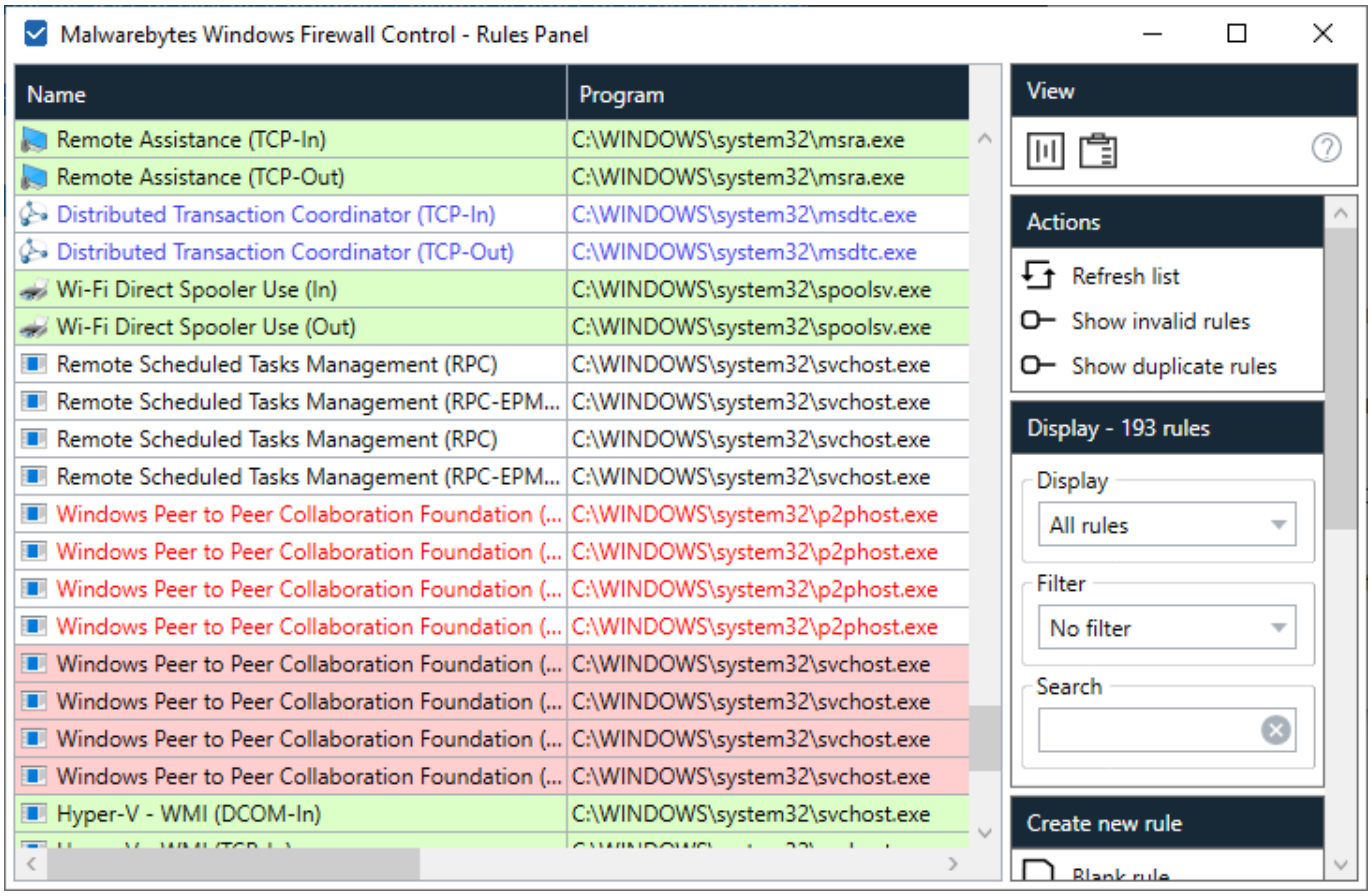
When this option is enabled, the program will check automatically if a new version is available. This is done only once, a minute after the program is started.

Use proxy configuration

This will open a proxy configuration dialog where the user can enter the proxy address, port, username and password. If no proxy configuration is required, leave this check box unchecked.

Rules Panel

Rules Panel offers an integrated an easier way to manage Windows Firewall rules. The firewall rules displayed are the same firewall rules that Windows Firewall uses. There are three color codes used for the firewall rules: **green rules** represent active allow rules, **red rules** represent active block rules, **gray rules** represent the rules that are disabled. Disabled rules are not used until they are enabled. Invalid rules are displayed with **red** text color and temporary rules are displayed with **blue** text color.



The layout of this window contains:

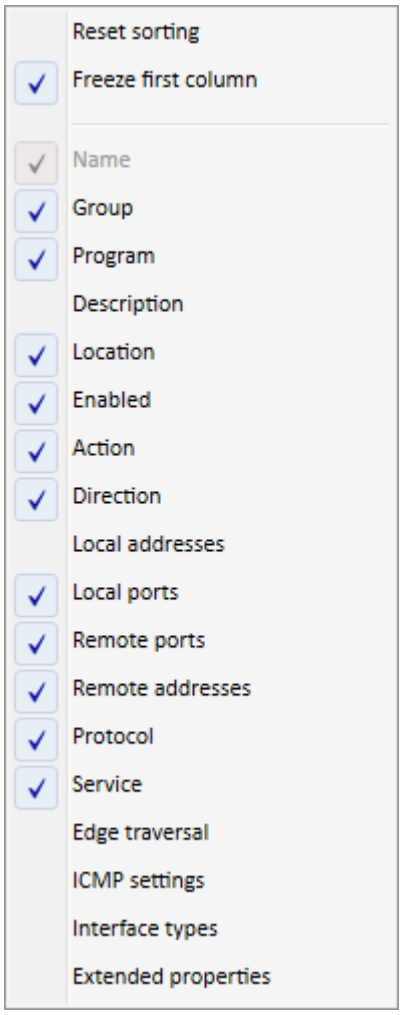
- a data grid on the left side which displays the firewall rules
- a toolbox area on the right side which contains the available actions

The following properties are saved when Rules Panel window is closed and reused when the window is opened again:

- the size and the location of the window
- the columns size, order and visibility
- the last values of the toolbox combo boxes
- the toolbox width

Data grid columns

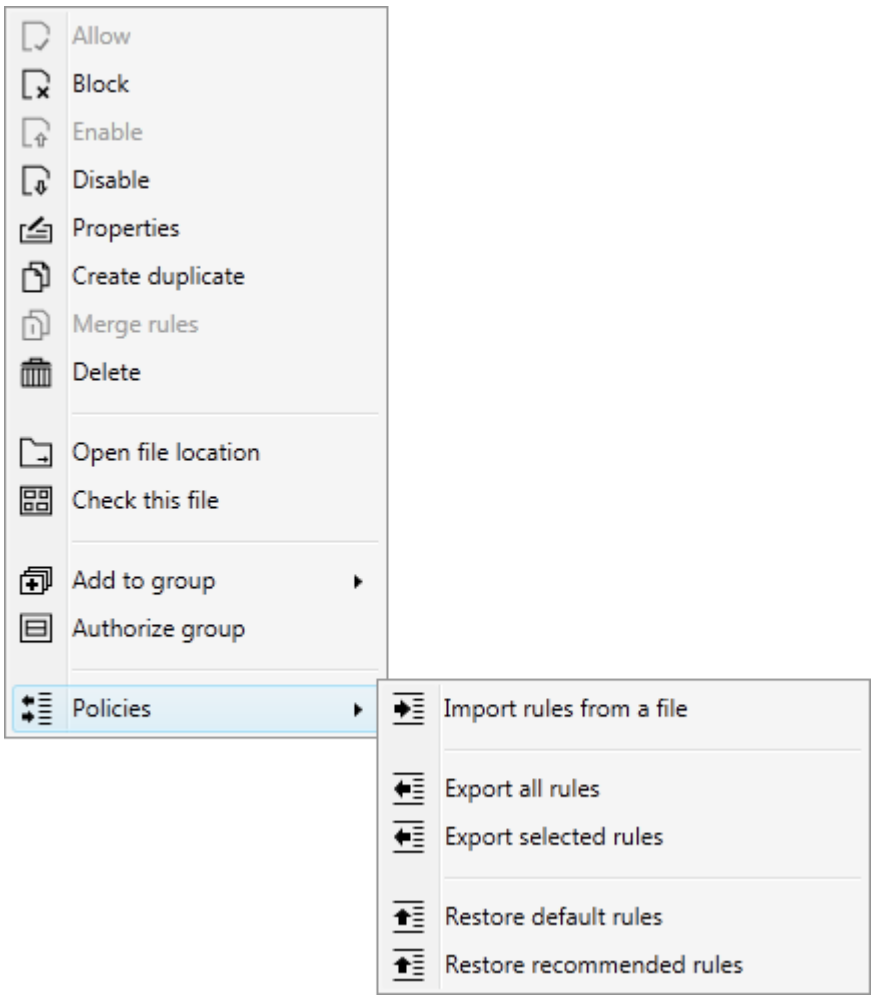
The columns header have a context menu which can be opened by right mouse click. **Reset sorting** menu item can be used to remove any existing sorting. **Freeze first column** menu item can be used to keep always visible the first column. The other menu items can be used to show or hide the data grid columns.



A special mention must be made for the **Extended properties** check box column. A rule with this check box checked informs the user that the rule contains some extra properties which can't be configured from Windows Firewall Control. These extra properties can be found for some Windows 10 firewall rules. These properties can be imported/exported from Windows Firewall Control but they can't be modified.

Rules entries context menu

Each entry from the data grid has a context menu which can be opened by right mouse click. The context menu is available also when selecting multiple entries but based on the selection, some menu items may be disabled or enabled.



Allow
This action will change the selected rules to allow connections. This menu item is disabled if the selected rule is already an allow rule.

Block
This action will change the selected rules to block connections. This menu item is disabled if the selected rule is already a block rule.

Enable
This action will enable the selected rules. This menu item is disabled if the selected rule is already enabled.

Disable
This action will disable the selected rules. This menu item is disabled if the selected rule is already disabled.

Properties
This action will open the **Properties** dialog which can be used to customize an existing rule. This menu item is disabled if multiple rules are selected.

Create duplicate
This action will create a new copy of each of the selected rules.

Merge rules
This action will open the **Merge rules** dialog which can be used to review the rule before the merge. Merging multiple rules is available only for similar rules. The selected rules must have the same: **Program**, **Direction**, **Action**, **Protocol**.

Delete
This action will delete the selected rules.

Open file location
This action will open and select the file from the **Program** column in My Computer.

Check this file
This action will check the file from the **Program** column based on the SHA256 checksum. The check is made with the online service set in the **Tools tab**.

Add to group
This action will set the group name for the selected rules. The list contains **all the group names from the current existing firewall rules** and all **authorized groups names** which are defined in the **Security tab**. The first entry is an empty group name which can be used to unset the group name.

Authorize group
This action will add the group of the selected rule to the list of **authorized groups names** which are defined in the **Security tab** and will enable the selected rule.

Import rules from a file
This action will import a policy file which contains firewall rules. You can read more about the supported file formats in the **Rules tab** section.

Export all rules
This action will export a full policy file in the **.wfw** format. This file will contain all the firewall rules.

Export selected rules
This action will export a partial policy file in the **.wpw** format. This file will contain only the selected firewall rules.

Restore default rules
This action will restore Windows Firewall default set of rules. This will overwrite all of the existing firewall rules.

Restore recommended rules
This action will the Windows Firewall Control recommended firewall rules. You can read more about these rules in the **Rules tab** section.

Toolbox controls

Refresh list button
Based on the applied filters it requests the firewall rules from the Windows Firewall Control service.

Show invalid rules button
Can be used to automatically find and select invalid rules. Are considered invalid rules the rules for which the program does not exist on the disk anymore.

Show duplicate rules button
Can be used to find duplicate rules. The search for duplicate rules is made on the following columns: **Program**, **Location**, **Action**, **Direction**, **Local addresses**, **Local ports**, **Remote ports**, **Remote addresses**, **Protocol**, **Service**, **Edge traversal**, **ICMP settings**, **Interface types**. The following columns are not taken into consideration during the search: **Name**, **Group**, **Description**, **Enabled**. The results contain only the rules for which at least two similar rules were found.

Display combo box
Can be used to filter the firewall rules based on their direction. The user can choose between displaying inbound rules, outbound rules or all rules.

Filter combo box
Can be used to filter the firewall in order to display the rules which are enabled or the ones that are disabled. User created rules are considered the rules created in the group named **Windows Firewall Control**.

Search text box
Can be used to search a string through the firewall rules. The search is made in the following columns: **Name**, **Program**, **Group**, **Local ports**, **Local addresses**, **Remote ports**, **Remote addresses**.

Blank rule
This will open the **Create new rule dialog** allowing the user to define a new rule from scratch.

Browse to allow
This will launch an open file dialog which will create a generic* allow rule for each of the selected files. The following file types are supported: .**exe**, .**dll**, .**bin**, .**setup**, .**scr**, .**tmp**.

Click to allow
This will open a dialog which will wait for the user to click on a program's window in order to create a new generic* allow rule for the program that was clicked.

Browse to block
This will launch an open file dialog which will create a generic* block rule for each of the selected files. **Multiple files are supported.**

Click to block
This will open a dialog which will wait for the user to click on a program's window in order to create a new generic* block rule for the program that was clicked.

Allow button
The same as the context menu item.

Block button
The same as the context menu item.

Enable button
The same as the context menu item.

Disable button
The same as the context menu item.

Properties button
The same as the context menu item.

Create duplicate button
The same as the context menu item.

Merge rules button
The same as the context menu item.

Delete button
The same as the context menu item.

Open file location button
The same as the context menu item.

Check this file button
The same as the context menu item.

*A **generic rule** means a rule for a program that is defined for all locations, all local and remote ports, all local and remote IP addresses, all protocols. A **custom rule** means a rule that is customized with specific values.

Does the program use a different set of firewall rules than Windows Firewall?

Windows Firewall Control is not a firewall by itself. It is just a front end for Windows Firewall which makes things easier and also adds some new extra features. The rules that you see in Rules Panel are the same rules that Windows Firewall uses. These rules are applied even if Windows Firewall Control is not running.

Can I create a rule for all the files from a folder?

No. Windows Firewall does not support wildcards. Because the Windows Firewall rules are applied per path basis you have to create a rule for each program that you want to allow or block. From Windows Firewall Control you can browse for the files for which you want to create a new rule and you can select multiple files at once. This will create a new rule for each file that was selected.

How to allow a program to connect only to the local network?

Define a firewall rule for the required program and open the **Properties Dialog** to edit the rule. Set the **Remote addresses** field to **Custom Addresses** and use the keyword **LocalSubnet**. Many default Windows Firewall rules use the **LocalSubnet** keyword to allow only local network connections. **LocalSubnet** is a special keyword which represents the local network based on the IP Address and the Subnet Mask configuration.

To restrict the allowed connections even more, you can specify an IP range. For example, if your network has IP addresses only in the following range **192.168.0.100-192.168.0.200**, you can specify this IP range in the **Remote addresses** field.

How to allow programs located on mounted drives?

Unfortunately, this is not possible. This is a problem of Windows Firewall itself with the way it handles the actual paths. While outbound filtering is enabled in Windows Firewall, you can't define a working rule for a file located in a mounted drive. This kind of rules can be created, however, they won't work. There is nothing that Windows Firewall Control could fix/extend to support this. The solution is to store the programs for which you want to create working firewall rules on a volume that has a drive letter, otherwise the rules won't work. The fix must come from Microsoft.

How to allow Windows Store apps that have a different path after an update?

When a new version of a Windows Store application that you have installed is receiving an update, the path of the executable file changes. Because Windows Firewall rules are applied per path basis, after such an update a new rule is required. This can become very annoying especially if an application is updated very often. This is how Windows Firewall works and this is not something that Windows Firewall Control can change.

As a workaround, instead of creating a firewall rule for a specific executable file:

- Create a rule that applies to all programs and set an empty group name for this rule. Setting an empty group name is important for the next step.
- Launch Windows Firewall with Advanced Security (**wf.msc**) and edit your newly created rule.
- In the **Programs and Services** tab, press on the **Settings** button under the **Application Packages** group box, select your specific application package and save the rule. Now you will have a working firewall rule, even if the program gets updated and the path changes. Now, you can add this firewall rule in any Group you want.

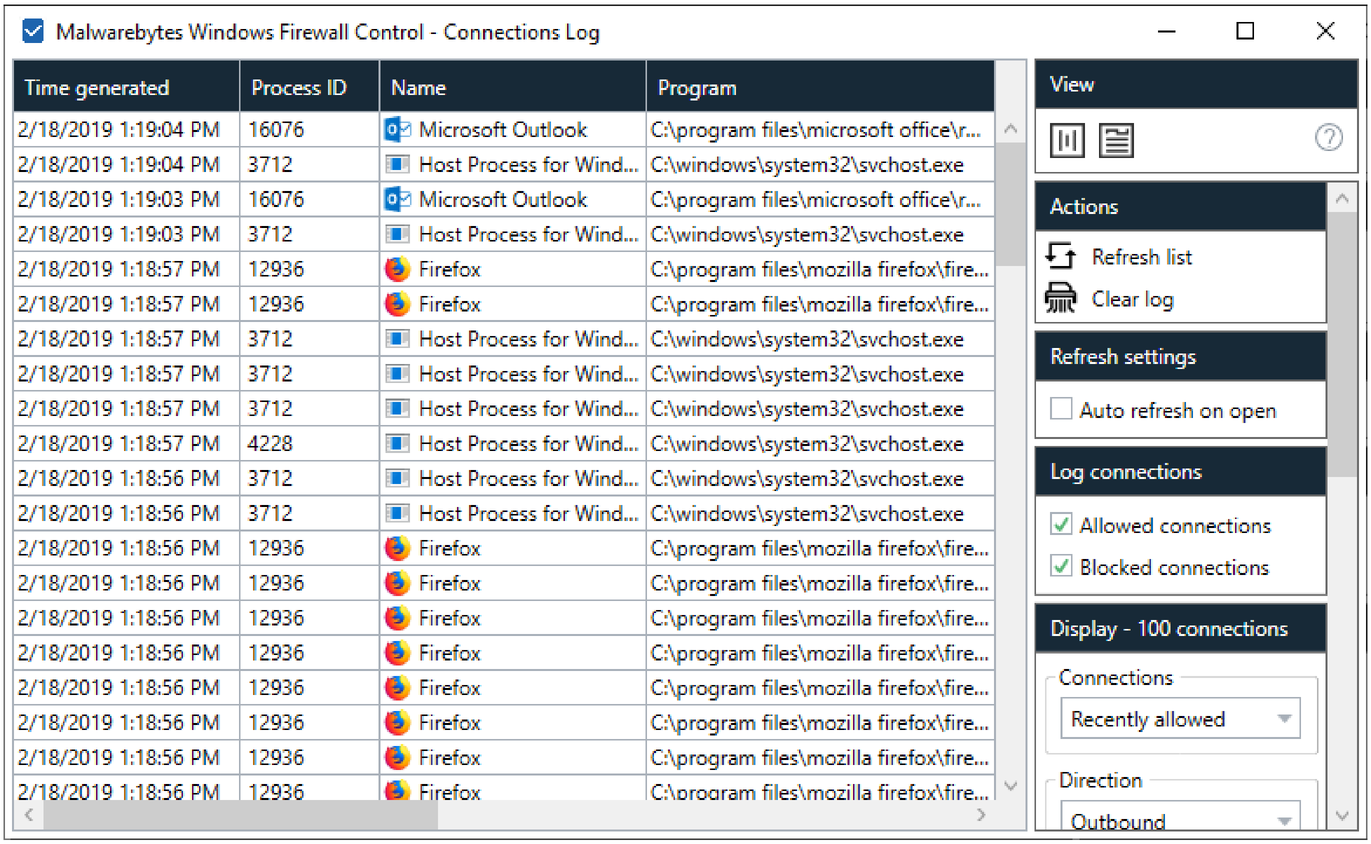
Note: The rules with a group name set can't be modified from Windows Firewall with Advanced Security. Also, the application package can't be set from Windows Firewall Control.

How to create a rule for a program which executes from the temporary folder?

Windows Firewall rules are applied per path basis, so even if you create a rule for an executable file, if this file is executed from a different path (different folder or filename in the temporary folder), a new rule is required for each file path. This is how Windows Firewall works and this is not something that Windows Firewall Control can change. For this scenario the only solution is to use Low Filtering profile when such software is used. You may try to see if you can configure this software to use only a specific port, for example 44444. Then you can create a rule that apply to all programs but which allows only the connections for local port 44444. In this way you can define a working rule for such programs.

Connections Log

Connections Log offers an integrated and easier way to view the Windows Firewall log. The entries are retrieved from the Security event log of the system and contain only Windows Firewall related entries. Depending on the log size (default 20 MB) and the recently network traffic the log can contain entries from the past minutes or from the past days. When the maximum log size is reached, older entries will be overwritten with newer entries. Note that this functionality will display past connections and is not intended to display the current active connections. To see the current network activity, the operating system already contains a tool named **Resource Monitor** which can be launched by executing **resmon.exe**.



The layout of this view contains:

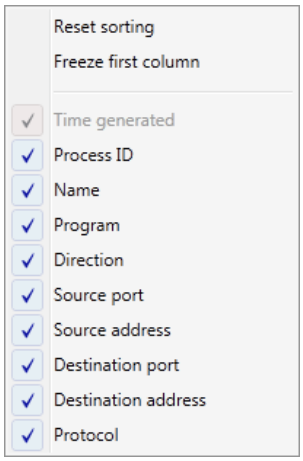
- a data grid on the left side which displays the log entries
- a toolbox area on the right side which contains the available actions

The following properties are saved when Connections Log window is closed and reused when the window is opened again:

- the size and the location of the window
- the columns size, order and visibility
- the last values of the toolbox combo boxes
- the toolbox width

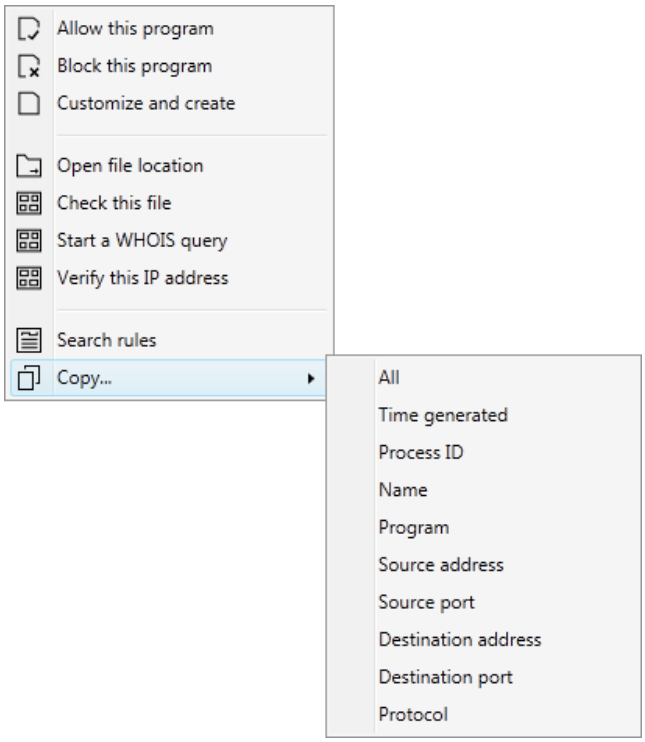
Data grid columns

The columns header have a context menu which can be opened by right mouse click. **Reset sorting** menu item can be used to remove any existing sorting. **Freeze first column** menu item can be used to keep always visible the first column. The other menu items can be used to show or hide the data grid columns.



Log entries context menu

Each entry from the data grid has a context menu which can be opened by right mouse click. The context menu is available also when selecting multiple entries but based on the selection, some menu items may be disabled or enabled.



Allow this program

This action will create a generic* allow rule which for the program that is selected.

Block this program
This action will create a generic* block rule which for the program that is selected.

Customize and create
This action will open the **Customize and create** dialog which can be used to customize the rule before creating it.

Open file location
This action will open and select the file from the **Program** column in My Computer.

Check this file
This action will check the file from the **Program** column based on the SHA256 checksum. The check is made with the online service set in the **Tools tab**.

Start a WHOIS query
This action will start a WHOIS query for the **Remote addresses** column of the log entry. The check is made with the online service set in the **Tools tab**.

Verify this IP address
This action will check online the **Remote addresses** column of the log entry. The check is made with the online service set in the Tools tab.

Search rules
This action will open **Rules Panel** and will automatically search for rules defined for the path displayed in the **Program** column.

Copy
This action will open a submenu which can be used to copy the details of the selected entry to clipboard. This can be used when selecting multiple entries too. For example, to copy all remote addresses from 10 different entries.

*A **generic rule** means a rule for a program that is defined for all locations, all local and remote ports, all local and remote IP addresses, all protocols. A **custom rule** means a rule that is customized with specific values.

Toolbox controls

Refresh list button
Based on the applied filters it requests the log entries from the Windows Firewall Control service. This can take a few seconds or a few minutes, depending on the filters that are used and on the log size.

Clear log button
Can be used to clear the existing entries from the Security log of the system.

Auto refresh on open check box
Enable or disable automatic refresh of the data grid when the window is opened. The last used filters will be used.

Allowed connections check box
Enable or disable the logging of allowed connections in Windows Firewall.

Blocked connections check box
Enable or disable the logging of blocked connections in Windows Firewall. Disabling the logging of blocked connections will also disable the notifications system.

Connections combo box
Can be used to filter the log entries based on the recently allowed or recently blocked connections.

Direction combo box
Can be used to filter the log entries based on the direction of the connections which can be inbound or outbound.

Display combo box
Can be used to choose how many log entries to process from the Security event log. Less entries means faster processing.

Entries combo box
Can be used to filer the log entries to display only the last entry of each program that is found or all of them.

Search text box
Can be used to search a string through the log entries. The search is made in the following columns: **Name**, **Program**, **Source port**, **Source address**, **Destination port**, **Destination address**.

Allow this program button
The same as the context menu item.

Block this program button
The same as the context menu item.

Customize and create button
The same as the context menu item.

Open file location button
The same as the context menu item.

Check this file button
The same as the context menu item.

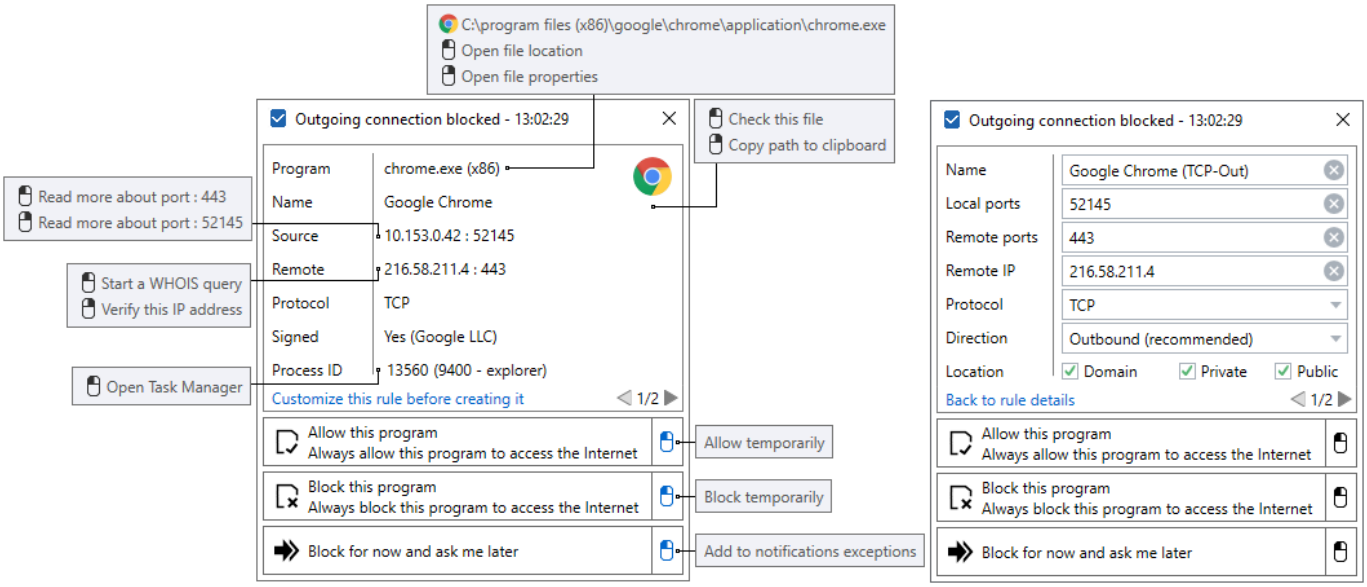
Start a WHOIS query button
The same as the context menu item.

Verify this IP address button
The same as the context menu item.

Notifications Dialog

When the notifications system is enabled and a program without a matching rule is blocked, Windows Firewall Control will display a new notification.

There are several shortcuts available by clicking on the **Program**, **Source**, **Remote**, **Process ID** and the program **Icon**. Just move the mouse cursor over them and check the info from the tool tips that will appear.



Customize this rule before creating it

By default, by choosing one of the options from the notification dialog, a new generic* rule will be created. By using this functionality, the user can customize the rule details (right screenshot) before creating a new rule.

Allow this program

If it is used directly (left screenshot) a new generic* allow rule will be created. If it is used while customizing the rule details (right screenshot) a new customized allow rule will be created.

Block this program

If it is used directly (left screenshot) a new generic* block rule will be created. If it is used while customizing the rule details (right screenshot) a new customized block rule will be created.

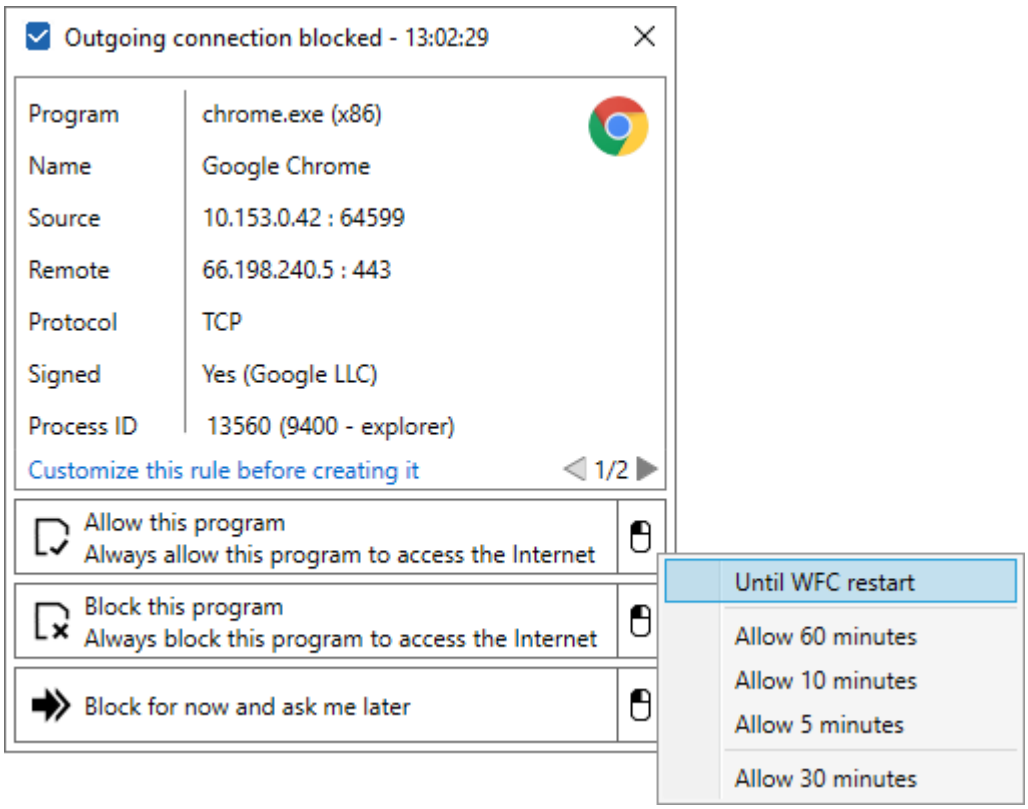
Block for now and ask me later

This will close the dialog without creating a new rule. This has the same functionality as the **Close** button of the dialog.

*A **generic rule** means a rule for a program that is defined for all locations, all local and remote ports, all local and remote IP addresses, all protocols. A **custom rule** means a rule that is customized with specific values.

How to create a temporary rule?

By pressing on the right side buttons in the notification dialog, a context menu will be displayed with multiple options for creating a new temporary rule. There is no option to allow the current instance of the program because Windows Firewall Control is not aware of this information, it doesn't monitor processes.

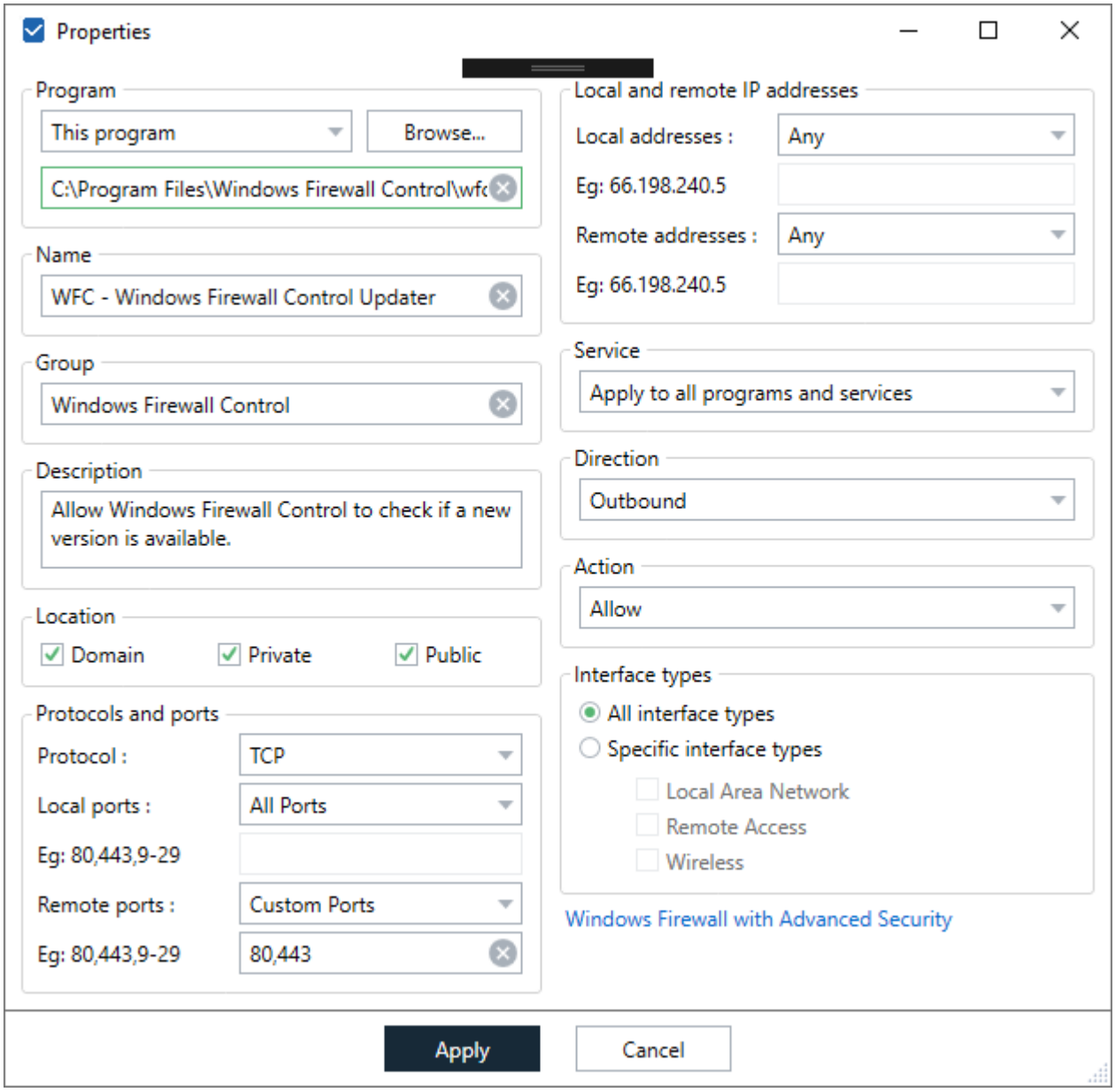


Temporary rules are displayed with blue text in Rules **Panel**.

Name	Group	Program	Location	Enabled	Action	Direction	Local ports	Remote addresses	Remote ports	Protocol	Service
Skype (skype.exe)	Temporary Rules	C:\program files (x86)\skype\phone\skype.exe	All	Yes	Allow	Out				Any	

Properties Dialog

The Properties dialog can be used to edit the details of a firewall rule.



The dialog is displayed in:

- **Rules Panel** when editing an existing rule
- **Rules Panel** when creating a new blank rule
- **Connections Log** when customizing an entry before creating a new rule

Troubleshooting

Due to many system configurations and various programs used, there may be situations when Windows Firewall Control may not work as expected. The cause may be the program code which may not take into consideration a specific case or even a different software which may conflict with Windows Firewall Control or with Windows Firewall itself.

In order to find the problem, try to follow the next steps:

1. Make sure that our software is not blocked by your antivirus or by other security software that you use. Try to temporarily disable them and see if the behavior changes.

2. Try to add **wfc.exe** and **wfcs.exe** into the white list (exceptions list, allowed list, etc) of your antivirus. Some self-defense features, anti executable programs, may block silently our software from execution. Some calls of WFC code involve the use of system tools **netsh.exe** and **auditpol.exe**. Make sure that your antivirus don't block the execution of command line programs that are executed in a CMD window.

3. If you have the possibility, try to install Windows Firewall Control on a different computer or in a virtual machine to see if you can reproduce the same problem on multiple machines.

4. Try to uninstall and reinstall the latest version of Windows Firewall Control and check if the problem is solved.

5. Make sure that you have the latest version of .NET Framework installed. Windows Firewall Control requires .NET Framework 4.5 or a newer version.

6. Please go to Event Viewer (execute **eventvwr.msc**). Under **Applications and Service logs** category, there is a subcategory named **WFC**. There are logged all errors from Windows Firewall Control. If you see errors logged here, from the right panel, use the button named **Save all events** as... to export a **.evtx** file and send it to us to check it.

7. Also in Event Viewer, under **Windows Logs** category, there is a subcategory named **Application**. Here are logged all errors from all programs. Check in this log if there are error entries regarding the files **wfc.exe** or **wfcs.exe**. If so, export a **.evtx** file of this log too and send it to us to check it. We can find here a .NET Framework problem that is causing the problem.

8. If you use a program named **Rivatuner Statistics Server**, open it and set **Application detection level** to None. Otherwise, this software may try to determine the FPS for WFC which uses the GPU to render the user interface.

When sending us an email please provide us as many details of the problem that you have. Write down the exact steps that you did, make a screenshot of the error that you receive, specify your operating system, if it is a virtual machine or a real machine, what other security software you use on the computer. Providing as many relevant details of your scenario will increase the chances to reproduce the problem that you have on our test machines. Then we will be able to provide a solution.

To report a problem regarding Windows Firewall Control send an email to support@binisoft.org. Thank you.

I can't allow Windows Subsystem for Linux through Windows Firewall

Unfortunately, while the outbound filtering is enabled in Windows Firewall (equivalent of Medium Filtering in WFC), WSL can't connect to the network. Microsoft provided a workaround for firewall developers to be able to allow WSL, but this apply to firewall vendors. Since WFC is not a firewall by itself (it is just a front-end which does not do any

packet filtering), it can't implement any fix for this. The fix must come from Microsoft since there is no way to allow Pico (WSL) in Windows Firewall. If you need Linux, I recommend you to use a virtual machine with a full installation of a Linux distribution.

I have enabled the notifications but I do not see them

Notifications are displayed only when **Medium Filtering** profile is used. Make sure that you don't have in your rules list some allow rules that permit all the connections for all programs. These kind of rules will allow anything and there will not be blocked connections. Avoid creating such generic rules. The firewall rules that you create should be targeted to specific files.

To troubleshoot this, make a backup of your rules and then restore Windows Firewall default set of rules. Now you should have only the default rules. Switch to Medium Filtering profile to enable outbound filtering in Windows Firewall and start over with the creation of your rules. Do you see now the notifications ? If the answer is yes, then one or more rules that you had in your previous rules set is responsible for the missing notifications. If you still don't see any notifications, then this may be a symptom generated by software proxies.

I receive duplicate notifications

A new notification is displayed if a new blocked connection does not match (ports, IP addresses, protocol, location) an existing allow rule.

If the rules are matching and you still receive duplicate notifications, it may be a symptom that Windows Firewall filtering does not work correctly. This usually happens when a software proxy from a different security product is used for filtering purposes. Windows Firewall is incompatible with software proxies, web filtering modules, NDIS drivers, any filtering modules that intercepts network packets. They redirect the network traffic to the proxy and the problem is that the traffic does not reach anymore the Windows Firewall filtering driver. In this case, Windows Firewall rules do not apply correctly because the traffic appears to be made by the proxy, not by the original program. Try to disable any software proxies, web filtering modules, NDIS drivers from the 3rd party security products that you use in order to restore the filtering functionality from Windows Firewall. This incompatibility is between software proxies and Windows Firewall, not an incompatibility with Windows Firewall Control which does not have any control over this behavior. Known problems between Windows Firewall and various filtering modules were reported for: Avast WebShield, Avira WebGuard, Kaspersky Internet Security, 360 Total Security, Symantec.

Another source that may cause duplicate notifications to be displayed can be a custom hosts file or a program like PeerBlock that blocks IP addresses based on a blacklist. All blocked connections are logged in the Security event log and will generate new notifications even if they weren't blocked by Windows Firewall. Also check your rules for incompatible rules.

Please read also about the advanced notifications settings from the **Notifications tab**.

My antivirus detects this software as a security threat

An antivirus software is an essential tool that most people need to protect their Windows operating system from malware. Unfortunately, most antivirus companies goes too far with their Virus/Trojan protection, and in many times they classify completely legitimate software as Virus/Trojan/Spyware infection. Windows Firewall Control is a respectable software with a history dating from 2010. If your antivirus detects Windows Firewall Control as a security threat, it is a false positive. To test that this is a false positive, you can scan the suspicious file online on VirusTotal website and see the scan results from more than 50 antivirus vendors.

False positives are actually mistakes made by antivirus and sometimes antispyware programs. The companies that are trying to protect our computers against the threats are under enormous pressure to get the malware identified and a fix created that there isn't enough time except, for very basic testing, before they must release these identifications and fixes. Add to this fact that the authors of the malware are also using the same program compilers and software libraries that often a good program may get misidentified as a bad one. Typically, the protection programs quarantine area that is made to safely hold a malware will allow you to restore these if you don't get impatient and empty it first. If you report the false positive to your protection company, they will be able to correct their mistake. If users will not report a false positive then they cannot be corrected. Please report any false positive regarding Windows Firewall Control to your antivirus vendor in order to get it removed.

What many people fail to realize with the subject of false positives... is that all antivirus and antispyware programs are prone to these. This is because they must also try and detect unknown malware that has just been released also. Its a case of trying to be safe and making a false detection instead of not being safe and letting the systems get infected. Another issue that many do not understand and is why a good program may get detected as a malware after an update is that the authors of the virus's and spyware also use the very same programs and code libraries that normal program authors are using... So many times regular programs have some of the very same code that malware may have.

The user has to ask themselves would they rather their protection program be a little bit paranoid and make a false detection... or would they rather it miss a newly released malware and end up with an infected computer instead.

Ping command returns general failure

A firewall rule is required for **SYSTEM** to allow outbound connections on **ICMPv4** protocol in order to use the PING command. To be able to ping an IPv6 host, a similar rule for **ICMPv6** protocol is also required. Windows Firewall Control recommended rules contain several rules for the ICMPv4 and ICMPv6 protocols for this purpose.

When the notifications system is used make sure that you can be notified about blocked connections of **System** process. If **System** is added in the notifications exceptions list, then the notification will not be displayed.

To debug connectivity problems, when a software is being blocked, use the **Connections Log** to see the recently blocked connections and make an idea of which rule is still required.

The profile changes out of nowhere

This might be a symptom that a 3rd party software changes the outbound filtering in Windows Firewall. To find out which application modifies the Windows Firewall settings, follow the next steps:

- Open Event Viewer, by launching **eventvwr.msc**
- Navigate to the following log name: **Applications and Services Logs -> Microsoft -> Windows -> Windows Firewall With Advanced Security -> Firewall**
- Select the latest events with ID 2003 and check the **Modifying Application**. It contains the software that changed the outbound filtering in Windows Firewall.

Similar to the event above, you can check the events below to find more info:

Event ID 2004 - A rule has been added to the Windows Firewall
Event ID 2005 - A rule has been modified in the Windows Firewall
Event ID 2006 - A rule has been deleted in the Windows Firewall

The program does not start automatically at Windows start-up

When the **Start automatically at user logon** option is checked in the **Options tab** a new entry is created for **wfc.exe** in Windows Registry under the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

This entry is available to all Windows user accounts and will launch the program for all user accounts.

1. Make sure that you don't have multiple places from where **wfc.exe** is executed. The program should be executed only from the key above.

2. Make sure that **wfc.exe** is not blocked from being executed by a 3rd party security software, including Windows Defender.

3. Please verify if the system tray icon is not displayed in the hidden icons area.

4. Check in Task Manager if the process **wfc.exe** is running but the system tray icon is missing or if the process is not running at all.

5. Make sure that the **Run this program as an administrator** check box is not checked in the Compatibility tab of **wfc.exe** file properties. When this check box is checked, UAC will prompt the user if he wants to allow the process to be executed. This kind of user interaction is not allowed during the Windows startup, therefore the program will be ignored and will not be started.

The program is locked and I can't remember the password

While the program is locked with a password, do not attempt to force the uninstall of Windows Firewall Control by using a 3rd party software because you will not be able to access Windows Firewall interface any more. If you forgotten the password used to lock the program interface, follow the next steps to remove a forgotten password:

- Open the lock dialog that you normally use to unlock the program.
- Press on the following key combination on your keyboard: **Right Alt + Right Ctrl + Right Shift + U**
- The lock dialog should close after the key combination was pressed.
- Open the lock dialog again and unlock the program with the following password: **binisoft**

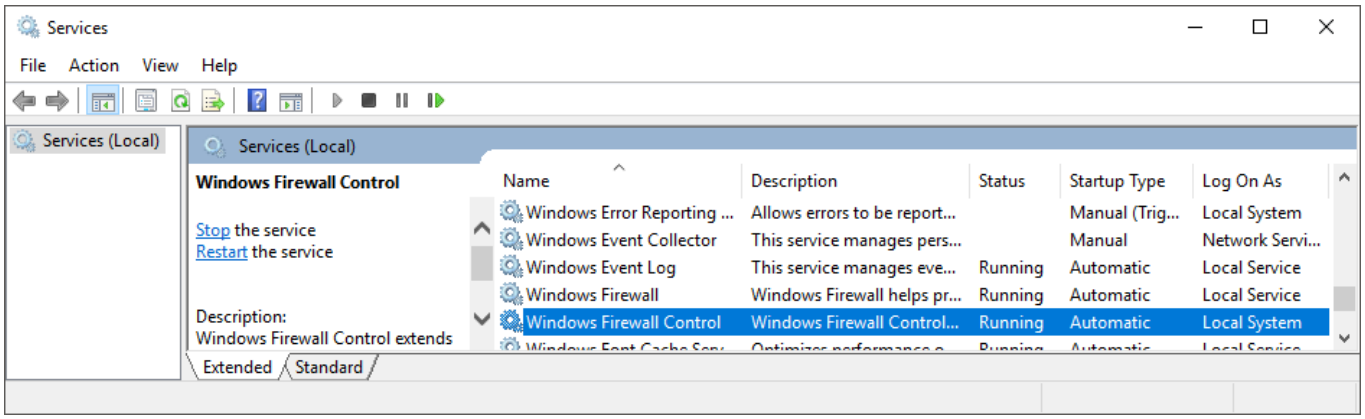
The system tray icon displays an exclamation mark

Windows Firewall Control has two parts. A GUI part which is **wfc.exe** and which runs as a system tray icon in the system tray area and a Windows service which is **wfcs.exe**. These both files can be found in the installation folder of the program, usually
C:\Program Files\Malwarebytes\Windows Firewall Control.

If the connections between the GUI part (**wfc.exe**) and the Windows service (**wfcs.exe**) is not possible, then the icon of the tray application will display an exclamation mark.

There can be multiple causes:

A) The service did not start. Execute **services.msc** and check the status of Windows Firewall Control service. The Startup Type should be **Automatic** and the Status should be **Started**.



For unknown reason, even if the service is set to Automatic startup type, sometimes the service is not started automatically by the operating system. It happens randomly on our systems with SQL Server service. If you manually start the service and the status of the service changes to **Started**, then in a few seconds, the system tray icon should display the icon of the current profile. Now the GUI part could connect to the service and it should work. If the service status is not **Started**, see below.

B) The service did not start because it encountered an error during the startup. In this case it should be an error logged about this in the event log. Please read the Troubleshooting section.

C) A different security software, usually an antivirus, detects a false positive and flags **wfcs.exe** as malware. This action will block the execution of the **wfcs.exe** or **wfc.exe**. It is recommended in this situation to disable temporarily all 3rd party security software to see which one detects WFC as malware. Check the black listed processes from these security programs or even try to add **wfc.exe** and **wfcs.exe** in the white list of these security programs. This behavior can be also caused by anti-executable security programs. Please report any false positive to make sure that this is fixed in a future updated definition file.

The system tray icon displays the profile but the context menu does not work

If the system tray does not launch the **Main Panel** when clicking on it and does not display the context menu on right mouse click, check the logs from the B). If there is no error, then see the C) from the previous answer. This behavior is usually generated by a different security software which blocks Windows Firewall Control.

Make sure that you have the latest version of .NET Framework installed. Windows Firewall Control requires .NET Framework 4.5 or a newer version.

The system tray icon is not displayed even if the program appears in Task Manager

Try to close the process **wfc.exe** from Task Manager and start it again. If the program appears in Task Manager but not in the system tray, check the answers above.

Make sure that you have the latest version of .NET Framework installed. Windows Firewall Control requires .NET Framework 4.5 or a newer version.

The window size and position is not remembered

Windows Firewall Control uses its own mechanism that saves the coordinates of a window when it is closed. These coordinates are restored when the window is reopened. Because the saved coordinates contain absolute values, there are scenarios when these coordinates can't be restored. The default size and position is restored when:

- the window is closed and at least one pixel of it was outside of the screen
- the screen resolution is changed
- a different DPI scaling is used
- the window is closed when a secondary monitor is used and the monitor is removed

Windows Mail can't synchronize folders

This applies to Windows 10 while **Medium Filtering** profile is used in Windows Firewall Control.

1. To allow the Windows Mail application to connect and synchronize your email accounts, you must create an outbound rule for **svchost.exe**.
2. To send an email you have to create an outbound rule for **C:\program files\windowsapps\microsoft.windowscommunicationsapps_17.6002.42251.0_x64__8wekyb3d8bbwe\hxmail.exe**
3. To be able to add a Google account you have to create an outbound rule for **C:\windows\systemapps\microsoft.accountscontrol_cw5n1h2txyewy\accountscontrolhost.exe** and one for **C:\windows\system32\authhost.exe**.

When the notifications system is used make sure that you can be notified about blocked connections of **svchost.exe** process. If **svchost.exe** is added in the notifications exceptions list, then the notification will not be displayed.

To debug connectivity problems, when a software is being blocked, use the **Connections Log** to see the recently blocked connections and make an idea of which rule is still required.

Windows Update does not work

Windows Firewall Control does not block or allow any connection. Windows Firewall does based on the firewall rules that are defined. Windows Update requires an outbound allow rule for **C:\Windows\system32\svchost.exe** on remote ports **80,443** and **TCP** protocol. **Windows Firewall Control recommended rules** contain a rule named **WFC - Windows Update** for this purpose.

When the notifications system is used make sure that you can be notified about blocked connections of **svchost.exe** process. If **svchost.exe** is added in the notifications exceptions list, then the notification will not be displayed.

To debug connectivity problems, when a software is being blocked, use the **Connections Log** to see the recently blocked connections and make an idea of which rule is still required.

When I restart my computer the profile is always set to High Filtering

Make sure that you don't have Secure Boot feature enabled in the **Security tab**.

Make sure you don't have the revert profile enabled to automatically set High Filtering profile in **Profiles tab**.

When **High Filtering** is set, two new firewall rules are added to the firewall, named ***High Filtering profile - Block inbound connections*** and ***High Filtering profile - Block outbound connections*.** These two rules are defined to block all connections for all programs. When the profile is switched to another profile, these two rules are automatically removed. Check in **Rules Panel** if you don't have multiple rules with these names.

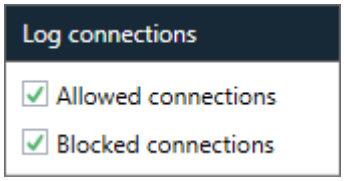
Connections Log entries are missing

The entries are retrieved from the Security event log of the system and contain only Windows Firewall related entries. Events with ID 5156 are logged when a connection is allowed and events with ID 5157 are logged when a connection is blocked. Depending on the log size (default 20 MB) and the recently network traffic the log can contain entries from the past minutes or from the past days. When the maximum log size is reached, older entries will be overwritten with newer entries.

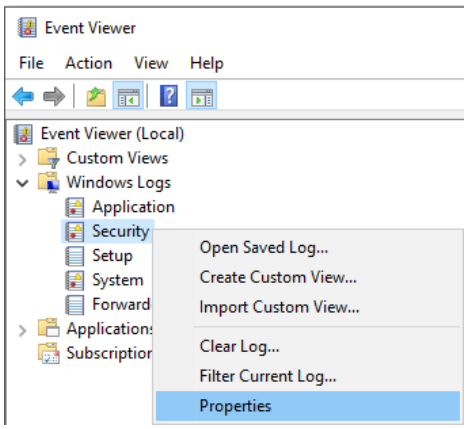
For example, the user chooses to display recently blocked connections and no entries are shown. If recently there were many allowed connections, they filled the entire log and older blocked connections were overwritten. In this case there is nothing to display in Connections Log since there are no records of blocked connections.

You have two possibilities:

- Disable the logging for allowed connections from Connections Log.

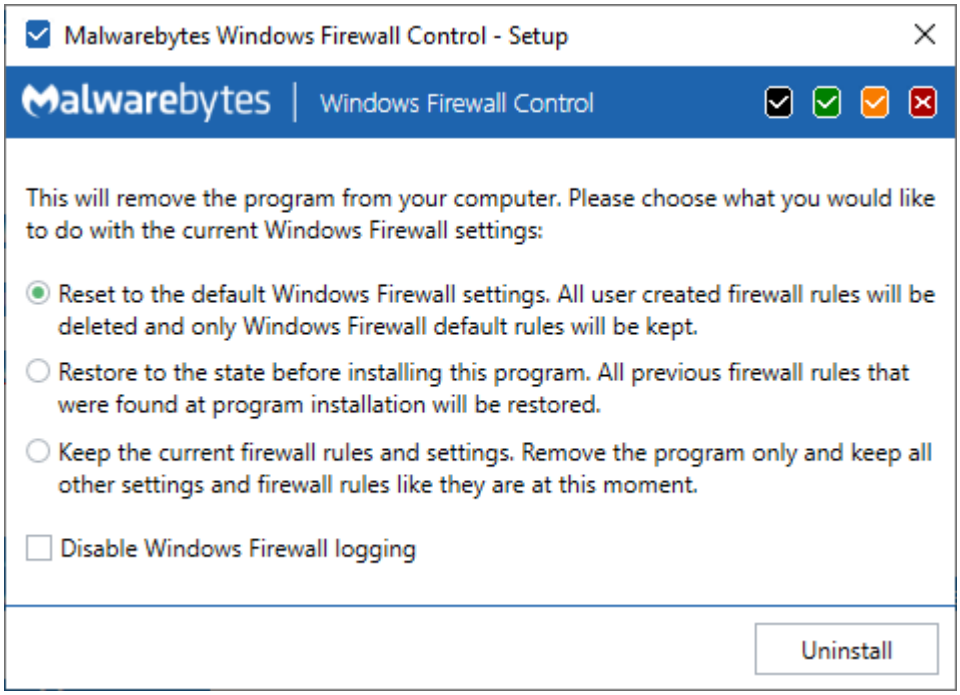


- Increase the Security log size from Event Viewer. In the **Event Viewer** (execute eventvwr.msc) select the **Security** category and from the right click context menu select **Properties.** In the dialog that opens, increase the **Maximum log size** value. Note that an increased log size will make the Connections Log slower since more entries will have to be processed. For best results regarding the performance, the default Security log size is an optimal choice.



Uninstall the program

Windows Firewall Control should be uninstalled from **Programs and Features** available in **Control Panel**. This will launch the file **wfc.exe** with the **-uninstall** parameter and will display the following dialog:



- Avoid using a different method or a specialized software to uninstall Windows Firewall Control because it will not work properly. Windows Firewall Control uses a custom installer and other programs will not know how to properly uninstall it.
- If the program is locked with a password, the uninstall will not be allowed by this method. In this case first unlock the program and then try again to uninstall it. While the program is locked with a password do not attempt to force the uninstall of Windows Firewall Control because you will not be able to access Windows Firewall interface any more. If you have forgotten your password, read the following section **The program is locked and I can't remember the password**.

If for some reason, the uninstall does not start by using the method described above, follow the next steps to manually uninstall the program:

a) Close the process **wfc.exe** by exiting the Windows Firewall Control tray icon or by using Task Manager.

b) Run a **CMD** window with Administrator privileges.

c) Execute the following commands:

sc.exe stop wfcs
sc.exe delete wfcs
reg delete "HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\Windows Firewall Control" /f

d) Delete manually the installation folder. Usually this folder is **C:\Program Files\Malwarebytes\Windows Firewall Control**.

Now your system should be clean of any WFC installation. You can now start again a clean installation of the latest version.

Uninstall options

Reset to the default Windows Firewall settings

All user created firewall rules and settings will be removed and the default Windows Firewall set of rules will be restored. The Windows Firewall default set of rules includes the firewall rules that are created when the operating system is installed.

Restore to the state before installing this program

Before starting the installation, Windows Firewall Control exports the existing firewall rules to a file named **restore.wfw** which is located in the installation folder. When this option is used, the firewall rules that existed before installing Windows Firewall Control will be restored from this file if it exists. The user created firewall rules and the program settings will be removed.

Keep the current firewall rules and settings

Only the files from the installation folder are removed. The user created firewall rules and the program settings remain untouched.

Disable Windows Firewall logging

By default Windows Firewall does not log any connections. The logging is required for the notifications system and for displaying purposes in **Connections Log**. If the program is removed, then the logging is not required anymore and can be disabled. Windows Firewall logging is automatically enabled when Windows Firewall Control is installed.