

WINDOWS FIREWALL CONTROL

Reinvent the wheel? IMPROVE the wheel!

Windows Firewall

The screenshot shows the Windows Defender Firewall with Advanced Security console. The title bar reads "Console1 - [Console Root\Windows Defender Firewall with Advanced Security on Local Computer]". The menu bar includes "File", "Action", "View", "Favorites", "Window", and "Help". The left-hand navigation pane shows a tree view of system components, with "Windows Defender Firewall with Advanced Security" expanded to show "Inbound Rules", "Outbound Rules", "Connection Security Rules", and "Monitoring".

The main content area displays the following information:

- Overview**
- Domain Profile**
 - Windows Defender Firewall is on.
 - Inbound connections that do not match a rule are blocked.
 - Outbound connections that do not match a rule are blocked.
- Private Profile is Active**
 - Windows Defender Firewall is on.
 - Inbound connections that do not match a rule are blocked.
 - Outbound connections that do not match a rule are blocked.
- Public Profile**
 - Windows Defender Firewall is on.
 - Inbound connections that do not match a rule are blocked.
 - Outbound connections that do not match a rule are blocked.
- [Windows Defender Firewall Properties](#)

Below the profiles, there is a section for "Getting Started" with the following content:

- Authenticate communications between computers**

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

 - [Connection Security Rules](#)
- View and create firewall rules**

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

The right-hand pane shows the "Actions" menu for the selected firewall profile, including options like "Import Policy...", "Export Policy...", "Restore Default Policy", "Diagnose / Repair", "View", "New Window from Here", "Refresh", "Properties", and "Help".

WFC-windows firewall control

Advantages

- Easier to control than native interface
- Dynamic – see, control, new programs when they start to access network (or old programs)
- Management easier
 - Add/delete/cull/edit rules
 - View log, create rules from entries

Main interfaces

Malwarebytes | Windows Firewall Control Open Malwarebytes

Dashboard

Profiles

Notifications

Options

Rules

Security

Tools

About

Windows Firewall state: On

Inbound connections: Block

Outbound connections: Block

Connected to location: Private

Right click on task bar icon

Family-friends

G-RA bridge

Profiles

Main Panel

Rules Panel

Connections Log

Exit

High Filtering

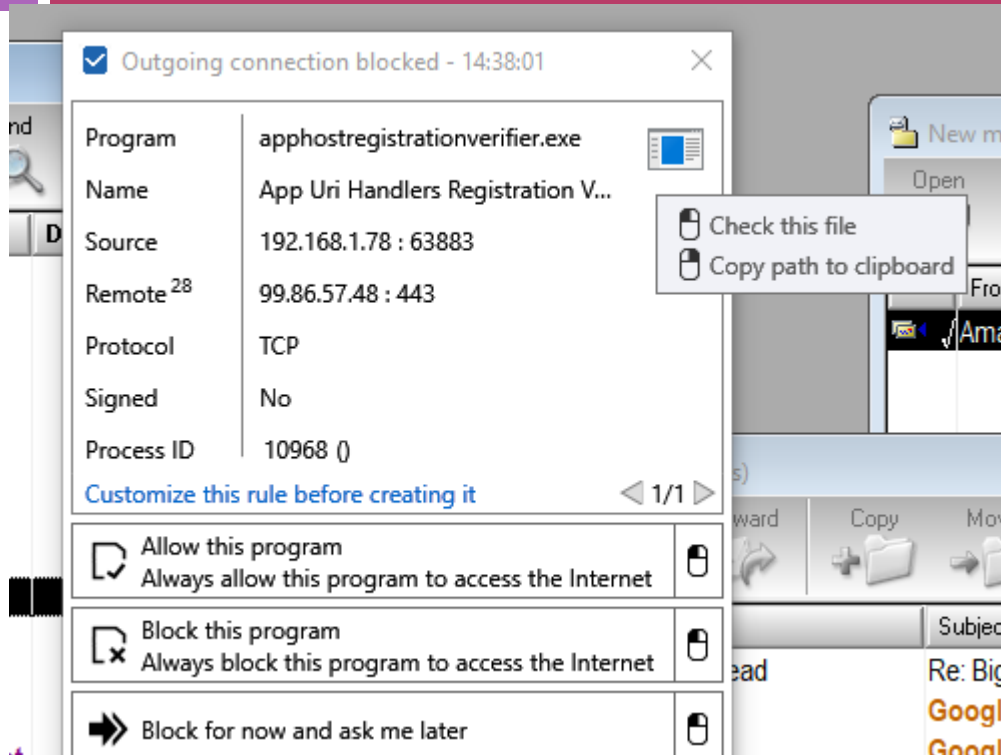
Medium Filtering

Low Filtering

No Filtering

n-bbo

“new program” control

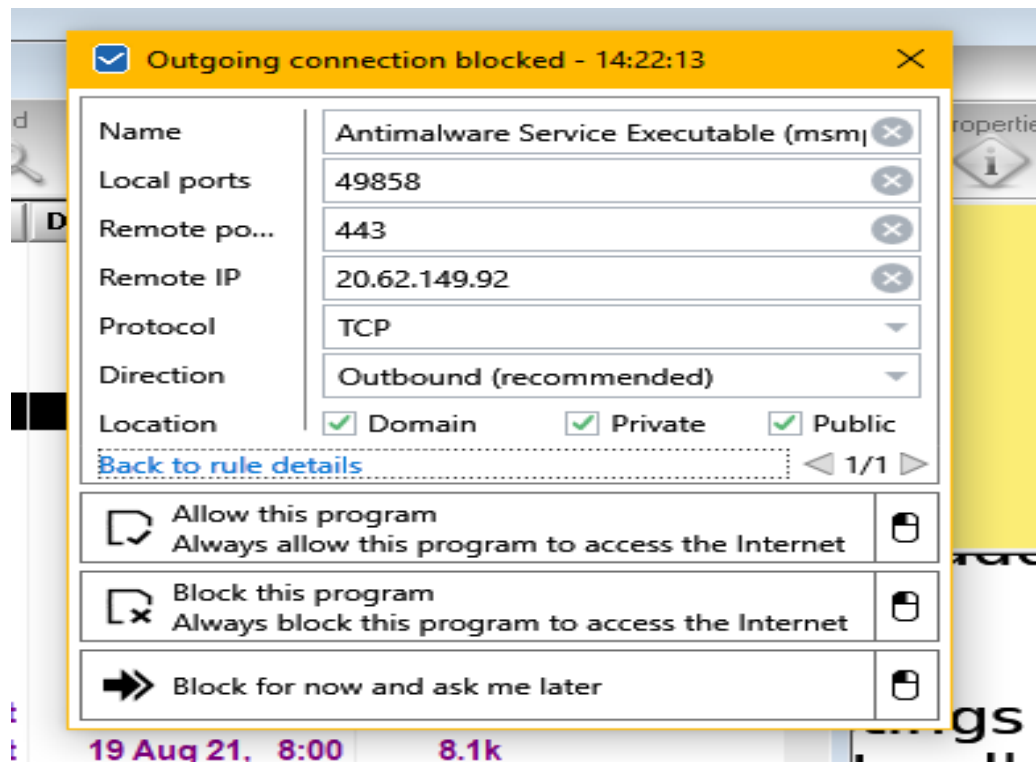


Add program permission to firewall, but can check:

- Vs virus total (opens browser tab)
- Check path to see origin

Can also constrain rule to particular IPs(local/remote), protocol, ports

Program constraints



Rules panel

Group	Name	Program	Location	Ena...	Action	Dir...	Local...	Pro...	Int...
	U - AsusLinkRemoteAgent	C:\WINDOWS\System32\DriverStore\File...	Private, Pub...	No	Allow	In		TCP	All
	U - AsusLinkRemoteAgent	C:\WINDOWS\System32\DriverStore\File...	Private, Pub...	No	Allow	In		TCP	All
Windows Fire...	Opera Internet Browser (opera.exe)	C:\user\ton\appdata\local\program\op...	All	Yes	Allow	Out		Any	All
Windows Fire...	ASUS System Analysis (asusyste...	C:\windows\system32\driverstore\filep...	All	Yes	Allow	Out		Any	All
	U - AsusSync	C:\WINDOWS\System32\DriverStore\File...	Private, Pub...	No	Allow	In		Any	All
	U - AsusLinkRemoteAgent	C:\WINDOWS\System32\DriverStore\File...	Private, Pub...	No	Allow	In		TCP	All
	U - AsusLinkRemoteAgent	C:\WINDOWS\System32\DriverStore\File...	Private, Pub...	No	Allow	In		TCP	All
Windows Fire...	Skype (skype.exe)	C:\program files\windowsapps\microsof...	All	Yes	Allow	Out		Any	All
	U - AsusLinkRemoteAgent	C:\WINDOWS\System32\DriverStore\File...	Private, Pub...	No	Allow	In		UDP	All
	U - AsusSync	C:\WINDOWS\System32\DriverStore\File...	Private, Pub...	No	Allow	In		Any	All
	U - AsusLinkRemoteAgent	C:\WINDOWS\System32\DriverStore\File...	Private, Pub...	No	Allow	In		TCP	All
	U - AsusLinkRemoteAgent	C:\WINDOWS\System32\DriverStore\File...	Private, Pub...	No	Allow	In		TCP	All
Microsoft Edg...	U - Microsoft Edge Beta (mcrs-in)	C:\Program Files (x86)\Microsoft\Edge Be...	All	No	Allow	In	5353	UDP	All
Windows Fire...	Internet Explorer (iexplore.exe)	C:\program files\internet explorer\explor...	All	Yes	Block	Out		Any	All
	U - AsusLinkRemoteAgent	C:\WINDOWS\System32\DriverStore\File...	Private, Pub...	No	Allow	In		UDP	All
	U - AsusLinkRemoteAgent	C:\WINDOWS\System32\DriverStore\File...	Private, Pub...	No	Allow	In		UDP	All
	U - AsusSync	C:\WINDOWS\System32\DriverStore\File...	Private, Pub...	No	Allow	In		Any	All
	U - AsusLinkRemoteAgent	C:\WINDOWS\System32\DriverStore\File...	Private, Pub...	No	Allow	In		UDP	All
	U - AsusSync	C:\WINDOWS\System32\DriverStore\File...	Private, Pub...	No	Allow	In		Any	All
	U - AsusLinkRemoteAgent	C:\WINDOWS\System32\DriverStore\File...	Private, Pub...	No	Allow	In		TCP	All
	U - AsusLinkRemoteAgent	C:\WINDOWS\System32\DriverStore\File...	Private, Pub...	No	Allow	In		UDP	All
	U - AsusSync	C:\WINDOWS\System32\DriverStore\File...	Private, Pub...	No	Allow	In		Any	All
	U - AsusLinkRemoteAgent	C:\WINDOWS\System32\DriverStore\File...	Private, Pub...	No	Allow	In		TCP	All
	U - AsusLinkRemoteAgent	C:\WINDOWS\System32\DriverStore\File...	Private, Pub...	No	Allow	In		UDP	All

Colour coded:
Red – invalid(program missing)
Pink – block
Green – outbound rules

View

Actions

- Refresh list
- Show invalid rules
- Show duplicate rules

Display - 1835 rules

Display

All rules

Filter

No filter

Search

Create new rule

- Blank rule
- Browse to allow
- Click to allow
- Browse to block
- Click to block

Invalid rules - can delete

Group	Name	Program	Location	Ena...	Action	Dir...	Local...	Pro...	Int...
Windows Fire...	AnyStream (anystream.exe)	C:\program files\redfox\anystream\anystr...	All	Yes	Allow	Out	Any	All	
Windows Fire...	WhatsApp (whatsapp.exe)	C:\users\tom\appdata\local\whatsapp\ap...	All	Yes	Allow	Out	Any	All	
Windows Fire...	NVIDIA Install Application (setup...	C:\users\install\appdata\local\temp\invid...	All	Yes	Allow	Out	Any	All	
Windows Fire...	WhatsApp (whatsapp.exe)	C:\users\tom\appdata\local\whatsapp\ap...	All	Yes	Allow	Out	Any	All	
Windows Fire...	Skype (skype.exe)	C:\program files\windowsapps\microsoft...	All	Yes	Allow	Out	Any	All	
Windows Fire...	Tablet Service Deployer/Undeploy...	C:\users\install\appdata\local\temp\7z58...	All	Yes	Allow	Out	Any	All	
Windows Fire...	Skype (skype.exe)	C:\program files\windowsapps\microsoft...	All	Yes	Allow	Out	Any	All	
Windows Fire...	WhatsApp (whatsapp.exe)	C:\users\tom\appdata\local\whatsapp\ap...	All	Yes	Allow	Out	Any	All	
Windows Fire...	WhatsApp (whatsapp.exe)	C:\users\tom\appdata\local\whatsapp\ap...	All	Yes	Allow	Out	Any	All	
	U - DaVinciResolveElements	C:\Program Files\Blackmagic Design\DaVi...	Private	No	Allow	In		Any	All
Windows Fire...	PowerToys Update (powertoys.up...	C:\program files\powertoys\powertoys.u...	All	Yes	Allow	Out	Any	All	
Windows Fire...	MyASUS (myasus.exe)	C:\program files\windowsapps\b9ced6f...	All	Yes	Allow	Out	Any	All	
Windows Fire...	WhatsApp (whatsapp.exe)	C:\users\tom\appdata\local\whatsapp\ap...	All	Yes	Allow	Out	Any	All	
Windows Fire...	GamingServices (gamingervices...	C:\program files\windowsapps\microsoft...	All	Yes	Allow	Out	Any	All	
Windows Fire...	Opera Internet Browser (opera.exe)	C:\users\tom\appdata\local\programs\op...	All	Yes	Allow	Out	Any	All	
Windows Fire...	Opera Internet Browser (opera.exe)	C:\users\tom\appdata\local\programs\op...	All	Yes	Allow	Out	Any	All	
Windows Fire...	(nvidiaisplay.container.exe)	C:\windows\system32\driverstore\filerep...	All	Yes	Allow	Out	Any	All	
Windows Fire...	Opera auto-updater (opera_auto...	C:\users\tom\appdata\local\programs\op...	All	Yes	Allow	Out	Any	All	
Windows Fire...	Opera Installer (installer.exe)	C:\users\tom\appdata\local\temp\opera...	All	Yes	Allow	Out	Any	All	
Windows Fire...	Skype (skype.exe)	C:\program files\windowsapps\microsoft...	All	Yes	Allow	Out	Any	All	
Windows Fire...	Microsoft Malware Protection Co...	C:\programdata\microsoft\windows defe...	All	Yes	Allow	Out	Any	All	
Windows Fire...	Opera auto-updater (opera_auto...	C:\users\tom\appdata\local\programs\op...	All	Yes	Allow	Out	Any	All	
Windows Fire...	Opera Internet Browser (opera.exe)	C:\users\tom\appdata\local\programs\op...	All	Yes	Allow	Out	Any	All	
Windows Fire...	Opera Internet Browser (opera.exe)	C:\users\tom\appdata\local\programs\op...	All	Yes	Allow	Out	TCP	All	

View

Actions

- Refresh list
- Show invalid rules
- Show duplicate rules

Display - 93 rules

Display

All rules

Filter

No filter

Search

Create new rule

- Blank rule
- Browse to allow
- Click to allow
- Browse to block
- Click to block

File verification tools

The screenshot shows the Malwarebytes Windows Firewall Control interface. The top bar includes the Malwarebytes logo, the title "Windows Firewall Control", and an "Open Malwarebytes" button. A left sidebar contains navigation options: Dashboard, Profiles, Notifications, Options, Rules, Security, Tools (highlighted), and About. The main content area features a help icon and a warning: "Use the shortcuts below to launch various system utilities. Note that these programs will be executed with highest privileges available." Below this, several system utilities are listed: Windows Firewall with Advanced Security, Windows Firewall Control Panel applet, Event Viewer, and Resource Monitor. A second section, titled "Specify below the URL services used for various online verifications", lists four URL templates in dropdown menus: "URL to check an IP address reputation" (https://www.ipvoid.com/scan/{0}/), "URL to check a file based on the SHA256 hash of the file" (https://www.virustotal.com/file/{0}/analysis/), "URL to start a WHOIS query" (https://who.is/whois-ip/ip-address/{0}), and "URL to read more about a specific port" (https://www.grc.com/port_{0}.htm).

Notifications

The screenshot shows the Malwarebytes Windows Firewall Control interface. The left sidebar contains navigation options: Dashboard, Profiles, Notifications (selected), Options, Rules, Security, Tools, and About. The main window title is "Windows Firewall Control" with an "Open Malwarebytes" button in the top right. The "Notifications" section is active, showing three radio button options: "Display notifications" (selected), "Learning mode", and "Disabled". Below these are instructions for each mode. A section titled "Define below the programs and folders for which the notifications should not be displayed" contains a list box for "Notifications exceptions" and a text input field "Define here a new exception". The "Notifications options" section includes a numeric input for "Automatically close a notification in" (set to 30 seconds), a numeric input for "Custom timeout for temporary rules is" (set to 10 minutes), and three checked checkboxes: "Display notifications on top of other windows", "Play a sound when a new notification is generated", and "Play default sound". The "Advanced notifications settings" section has three unchecked checkboxes: "Use allow rules when searching for matching rules...", "Use generic block rules when searching for matching rules...", and "Use disabled rules when searching for matching rules...". A "Reset default advanced settings" link is at the bottom.

Malwarebytes | Windows Firewall Control | Open Malwarebytes

Dashboard
Profiles
Notifications
Options
Rules
Security
Tools
About

Notifications mode specifies which blocked outbound connections should be displayed to the user

- Display notifications**
Display notifications for all blocked outbound connections but do not display them for the programs defined as exceptions below
- Learning mode**
Automatically create outbound allow rules for digitally signed programs and display notifications only for unsigned programs.
- Disabled**
Do not display notifications.

Define below the programs and folders for which the notifications should not be displayed

Notifications exceptions

Define here a new exception

Notifications options

Automatically close a notification in seconds.

Custom timeout for temporary rules is minutes

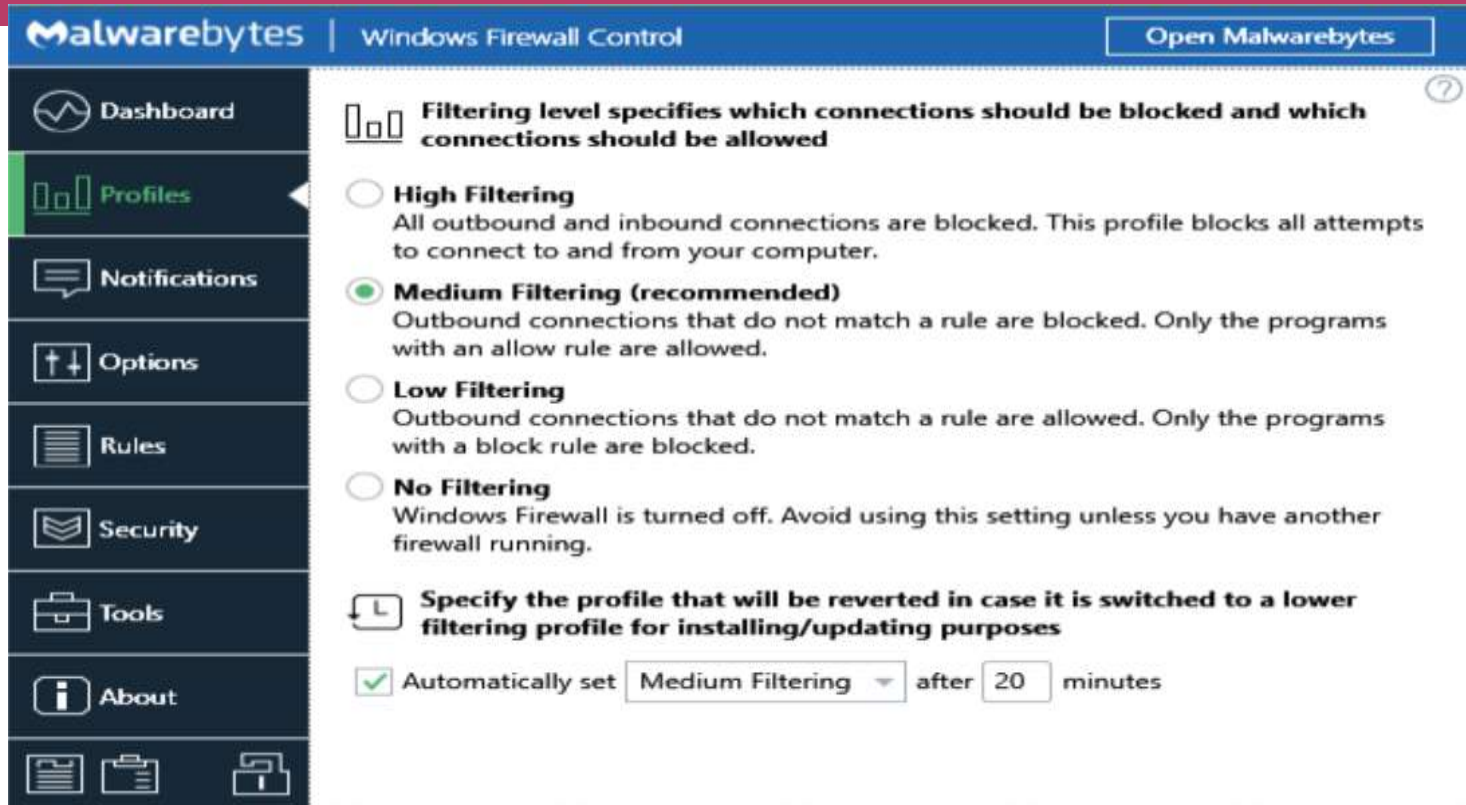
- Display notifications on top of other windows
- Play a sound when a new notification is generated
- Play default sound
- Play custom sound

Advanced notifications settings

- Use allow rules when searching for matching rules. Recommended for compatibility with other security programs if duplicate notifications are displayed.
- Use generic block rules when searching for matching rules. If a block rule that apply to all programs matches the blocked connection, the notifications will not be displayed.
- Use disabled rules when searching for matching rules. If a matching disabled rule is found the notifications will not be displayed.

[Reset default advanced settings](#)

Filtering



The screenshot shows the Malwarebytes Windows Firewall Control application window. The title bar includes the Malwarebytes logo, the text "Windows Firewall Control", and a button labeled "Open Malwarebytes". A dark sidebar on the left contains navigation options: Dashboard, Profiles (highlighted in green), Notifications, Options, Rules, Security, Tools, and About. The main content area features a heading "Filtering level specifies which connections should be blocked and which connections should be allowed" with a bar chart icon and a help icon. Below this are five radio button options: High Filtering, Medium Filtering (recommended), Low Filtering, and No Filtering, each with a descriptive paragraph. A section titled "Specify the profile that will be reverted in case it is switched to a lower filtering profile for installing/updating purposes" includes a checked checkbox and a dropdown menu set to "Medium Filtering" followed by "after 20 minutes".

Malwarebytes | Windows Firewall Control Open Malwarebytes

Filtering level specifies which connections should be blocked and which connections should be allowed

- High Filtering**
All outbound and inbound connections are blocked. This profile blocks all attempts to connect to and from your computer.
- Medium Filtering (recommended)**
Outbound connections that do not match a rule are blocked. Only the programs with an allow rule are allowed.
- Low Filtering**
Outbound connections that do not match a rule are allowed. Only the programs with a block rule are blocked.
- No Filtering**
Windows Firewall is turned off. Avoid using this setting unless you have another firewall running.

Specify the profile that will be reverted in case it is switched to a lower filtering profile for installing/updating purposes

Automatically set Medium Filtering after 20 minutes

Security

The screenshot displays the Malwarebytes Windows Firewall Control application window. The interface is divided into a left sidebar and a main content area. The sidebar contains navigation options: Dashboard, Profiles, Notifications, Options, Rules, Security (highlighted), Tools, and About. The main content area features a top bar with the Malwarebytes logo, the title 'Windows Firewall Control', and an 'Open Malwarebytes' button. Below this, a section titled 'Specify below the security enhancements that will be enforced by Malwarebytes Windows Firewall Control' contains several settings:

- Secure Boot**: Automatically set High Filtering profile at system shut down. At Windows start-up, all network connections will be blocked until the user manually changes the profile.
- Secure Profile**: Protect Windows Firewall state from external tampering. When this feature is enabled, importing firewall rules and changing the filtering mode can be done only through this software.
- Secure Rules**: Enable protection against firewall rules that are not created in the authorized groups defined below. This applies to the newly created firewall rules and to existing ones.
 - Delete unauthorized rules
 - Disable unauthorized rules**
 - Allow Windows Store rules

Below the settings is a list of 'Authorized groups' with a scrollable view:

- Windows Firewall Control
- Temporary Rules
 - @%SystemRoot%\system32\firewallapi.dll,-53500
 - @%SystemRoot%\system32\icsvc.dll,-700
 - @FirewallAPI.dll,-80200

At the bottom, there is a text input field 'Define here a new authorized group' with a plus icon to its right, and a link 'Import group names from the current existing rules'.

Connections Log

Malwarebytes Windows Firewall Control - Connections Log

Time generated	Name	Program
2021-09-08 16:46:12...	Microsoft Net...	C:\programdata\microsoft\windows defender\platform4.18.2108.7-0\nissrv.exe

View

Actions

- Refresh list
- Clear log

Refresh settings

- Auto refresh on open

Log connections

- Allowed connections
- Blocked connections

Display - 1 connections

Connections

Recently blocked

Direction

Outbound

Display

All connections

Entries

All entries

Search

Search

Create new rule

Customize rule from connection log!

Malwarebytes Windows Firewall Control - Connections Log

Time generated	Name	Program
2021-09-08 16:46:12...	Microsoft Network Realtime Inspection Service	C:\programdata\microsoft\windows defender\platform\4.18.2108.7-0\nissrv.exe

Customize and create

Customize and create

Program: This program (Browse...)
C:\programdata\microsoft\windows defender\

Name: Microsoft Network Realtime Inspection Service

Group: Windows Firewall Control

Description:

Location: Domain Private Public

Protocols and ports:
Protocol: TCP
Local ports: Custom Ports (Eg: 80,443,9-29) 49344
Remote ports: Custom Ports (Eg: 80,443,9-29) 443

Local and remote IP addresses:
Local addresses: Custom Addresses (Eg: 66.198.240.5) 192.168.1.78
Remote addresses: Custom Addresses (Eg: 66.198.240.5) 13.68.247.210

Service: Apply to all programs and services

Direction: Outbound

Action: Allow

Interface types:
 All interface types
 Specific interface types
Local Area Network
Remote Access
Wireless

Windows Firewall with Advanced Security

Create Cancel

This can also be done for selected rows

Rules, connections displays can be sorted by clicking the column title.

WFC Advantages

- Uses built-in, trustworthy firewall
- Dynamic – sees new programs
- Powerful – update/create/delete rules based on logs & rules
- Free!
- <https://www.binisoft.org/wfc>