We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking "Manage Cookies" at the bottom of the page. Privacy Statement Third-Party Cookies

Accept

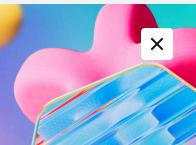
Reject

Manage cookies

### Microsoft Ignite

Nov 19-22, 2024

Register now >



Learn

Product documentation ∨ Development languages ∨

Q Sign in

Windows Server

Get started Failover clustering Management Identity and access Networking Troubleshooting Related products  $\vee$ 

📆 Filter by title

- > Remote access
- > TCP/IP communications
- > Webwindows-client and WebDAV
- Windows Firewall with Advanced Security (WFAS)

Troubleshooting guidance: Windows

Firewall with Advanced Security

Error 0x000006D9 when you share a printer

How to disable stealth mode

UDP communication is blocked

#### Use netsh advfirewall firewall context

- > Windows NIC Teaming (Load Balance Failover)
- > WINS
- > Wireless networking and 802.1X authentication
- > Identify and remediate MaxConcurrentApi issues that affect user authentication
- > Performance
- > Printing
- > Remote Desktop Services
- > Security and Malware
- > Setup, upgrades, and drivers
- > Shell Experience
- > Software Defined Networking
- > System Management Components
- > UserProfiles and Logon
- > Virtualization
- > Windows Security
- > Windows Servicing, Updates and Features on Demand
- > Windows Server End of Support (EoS) FAQ
- > Support Tools

Learn / Troubleshoot / Windows / Windows Server /

## Use netsh advfirewall firewall instead of netsh firewall to control Windows Firewall behavior

Article • 12/26/2023 • 3 contributors

Feedback

#### In this article

Summary

Command example 1: Enable a program

Command example 2: Enable a port

Command example 3: Delete enabled programs or ports

Show 5 more

This article describes how to use the netsh advfirewall firewall context instead of the netsh firewall context to control Windows Firewall behavior.

Original KB number: 947709

### Summary

The netsh advfirewall firewall command-line context is available in Windows Server 2012 R2. This context provides the functionality for controlling Windows Firewall behavior that was provided by the netsh firewall firewall context.

This context also provides functionality for more precise control of firewall rules. These rules include the following per-profile settings:

- Domain
- Private
- Public

The netsh firewall command-line context might be deprecated in a future version of the Windows operating system. We recommend that you use the netsh advfirewall firewall context to control firewall behavior.

(i) Important

Download PDF

If you are a member of the Administrators group, and User Account Control is enabled on your computer, run the commands from a command prompt with elevated permissions. To start a command prompt with elevated permissions, find the icon or Start menu entry that you use to start a command prompt session, right-click it, and then click **Run as administrator**.

Some examples of frequently used commands are provided in the following tables. You can use these examples to help you migrate from the older netsh advfirewall firewall context.

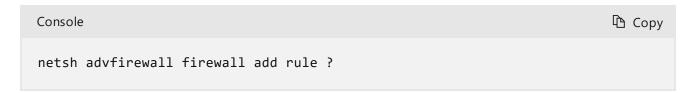
Additionally, the netsh advfirewall commands that you can use to obtain detailed inline help are provided.

### Command example 1: Enable a program

**Expand table** 

Old command	New command
netsh firewall add allowedprogram	netsh advfirewall firewall add rule name="M
<pre>C:\MyApp\MyApp.exe "My Application" ENABLE</pre>	Application" dir=in action=allow
	<pre>program="C:\MyApp\MyApp.exe" enable=yes</pre>
netsh firewall add allowedprogram	netsh advfirewall firewall add rule name="My
<pre>program=C:\MyApp\MyApp.exe name="My</pre>	Application" dir=in action=allow program=
Application" mode=ENABLE scope=CUSTOM	<pre>"C:\MyApp\MyApp.exe" enable=yes</pre>
addresses=157.60.0.1,172.16.0.0/16,LocalSubnet	remoteip=157.60.0.1,172.16.0.0/16,LocalSubne
profile=Domain	profile=domain
netsh firewall add allowedprogram	Run the following commands:
<pre>program=C:\MyApp\MyApp.exe name="My</pre>	netsh advfirewall firewall add rule name="My
Application" mode=ENABLE scope=CUSTOM	Application" dir=in action=allow program=
addresses=157.60.0.1,172.16.0.0/16,LocalSubnet	<pre>"C:\MyApp\MyApp.exe" enable=yes</pre>
profile=ALL	remoteip=157.60.0.1,172.16.0.0/16,LocalSubne
	profile=domain
	netsh advfirewall firewall add rule name="M
	Application" dir=in action=allow
	<pre>program="C:\MyApp\MyApp.exe" enable=yes</pre>
	remoteip=157.60.0.1,172.16.0.0/16,LocalSubne

For more information about how to add firewall rules, run the following command:



### Command example 2: Enable a port

**Expand table** 

Old command	New command
netsh firewall add portopening	netsh advfirewall firewall add rule name= "Open Port 80"
TCP 80 "Open Port 80"	dir=in action=allow protocol=TCP localport=80

For more information about how to add firewall rules, run the following command:

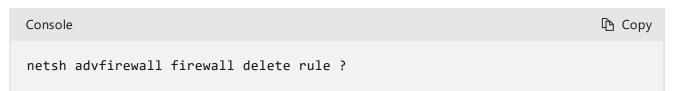
Console	🖺 Сору
netsh advfirewall firewall add rule ?	

# Command example 3: Delete enabled programs or ports

Expand table

Old command	New command
<pre>netsh firewall delete allowedprogram C:\MyApp\MyApp.exe</pre>	<pre>netsh advfirewall firewall delete rule name= rule name program="C:\MyApp\MyApp.exe"</pre>
delete portopening protocol=UDP port=500	<pre>netsh advfirewall firewall delete rule name= rule name protocol=udp localport=500</pre>

For more information about how to delete firewall rules, run the following command:

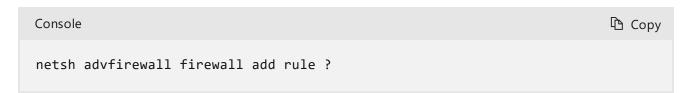


# Command example 4: Configure ICMP settings

Expand table

Old command	New command
netsh firewall set	netsh advfirewall firewall add rule name="ICMP Allow incoming
icmpsetting 8	V4 echo request" protocol=icmpv4:8,any dir=in action=allow
netsh firewall set	netsh advfirewall firewall add rule name= "All ICMP V4"
icmpsetting type=ALL	<pre>protocol=icmpv4:any,any dir=in action=allow</pre>
mode=enable	
netsh firewall set	netsh advfirewall firewall add rule name="Block Type 13 ICMP
icmpsetting 13 disable all	V4" protocol=icmpv4:13,any dir=in action=block

For more information about how to configure ICMP settings, run the following command:



### Command example 5: Set logging

**Expand table** 

Old command	New command
netsh firewall set logging	Run the following commands:
%systemroot%\system32\LogFiles\Firewall\pfirewall.log	netsh advfirewall set currentprofile
4096 ENABLE ENABLE	%systemroot%\system32\LogFiles\Firew
	netsh advfirewall set currentprofile
	maxfilesize 4096
	netsh advfirewall set currentprofile
	droppedconnections enable
	netsh advfirewall set currentprofile
	allowedconnections enable

For more information, run the following command:



If you want to set logging for a particular profile, use one of the following options instead of the currentprofile option:

- Domainprofile
- Privateprofile
- Publicprofile

## Command example 6: Enable Windows firewall

Expand table

Old command	New command
netsh firewall set opmode ENABLE	netsh advfirewall set currentprofile state on
netsh firewall set opmode mode=ENABLE	Run the following commands:
exceptions=enable	Netsh advfirewall set currentprofile state on
	netsh advfirewall set currentprofile
	firewallpolicy blockinboundalways,allowoutbound
netsh firewall set opmode mode=enable	Run the following commands:
exceptions=disable profile=domain	Netsh advfirewall set domainprofile state on
	netsh advfirewall set domainprofile firewallpolicy
	blockinbound, allowoutbound
	Dun the following commands:
netsh firewall set opmode mode=enable	Run the following commands:
netsh firewall set opmode mode=enable profile=ALL	netsh advfirewall set domainprofile state on

For more information, run the following command:



If you want to set the firewall state for a particular profile, use one of the following options instead of the currentprofile option:

- Domainprofile
- Privateprofile
- Publicprofile

## Command example 7: Restore policy defaults

**Expand table** 

Old command	New command
netsh firewall reset	netsh advfirewall reset

For more information, run the following command:

Console Copy

netsh advfirewall reset ?

## Command example 8: Enable specific services

**Expand table** 

Old command	New command
netsh firewall set service FileAndPrint	<pre>netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes</pre>
netsh firewall set service RemoteDesktop enable	<pre>netsh advfirewall firewall set rule group="remote desktop" new enable=Yes</pre>
netsh firewall set service RemoteDesktop enable profile=ALL	Run the following commands:
	<pre>netsh advfirewall firewall set rule group="remote desktop" new enable=Yes profile=domain</pre>
	<pre>netsh advfirewall firewall set rule group="remote desktop" new enable=Yes profile=private</pre>

#### **Feedback**

Provide product feedback  $\ensuremath{\,\boxtimes\,}$ 

#### Additional resources

#### Training

Module

Manage network service settings for Windows devices using PowerShell cmdlets - Training

This module covers the PowerShell modules and cmdlets that are used to configure network settings for Windows devices.

#### Certification

Microsoft Certified: Windows Server Hybrid Administrator Associate - Certifications

As a Windows Server hybrid administrator, you integrate Windows Server environments with Azure services and manage Windows Server in on-premises networks.

Blog ☑

**Previous Versions** 

Manage cookies

Contribute Privacy ☑ Terms of Use Trademarks ☑ © Microsoft 2024