

🔍 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

> Resources

> 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

📄 Download PDF

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.

📘 Important

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 firewall` context to the new `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
<code>netsh firewall add allowedprogram C:\MyApp\MyApp.exe "My Application" ENABLE</code>	<code>netsh advfirewall firewall add rule name="My Application" dir=in action=allow program="C:\MyApp\MyApp.exe" enable=yes</code>
<code>netsh firewall add allowedprogram program=C:\MyApp\MyApp.exe name="My Application" mode=ENABLE scope=CUSTOM addresses=157.60.0.1,172.16.0.0/16,LocalSubnet profile=Domain</code>	<code>netsh advfirewall firewall add rule name="My Application" dir=in action=allow program="C:\MyApp\MyApp.exe" enable=yes remoteip=157.60.0.1,172.16.0.0/16,LocalSubnet profile=domain</code>
<code>netsh firewall add allowedprogram program=C:\MyApp\MyApp.exe name="My Application" mode=ENABLE scope=CUSTOM addresses=157.60.0.1,172.16.0.0/16,LocalSubnet profile=ALL</code>	<div>Run the following commands:</div> <div><code>netsh advfirewall firewall add rule name="My Application" dir=in action=allow program="C:\MyApp\MyApp.exe" enable=yes remoteip=157.60.0.1,172.16.0.0/16,LocalSubnet profile=domain</code></div> <div><code>netsh advfirewall firewall add rule name="My Application" dir=in action=allow program="C:\MyApp\MyApp.exe" enable=yes remoteip=157.60.0.1,172.16.0.0/16,LocalSubnet profile=private</code></div>

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

Console

[Copy](#)

netsh advfirewall firewall add rule ?

Command example 2: Enable a port

[Expand table](#)

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

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

Console

[Copy](#)

netsh advfirewall firewall add rule ?

Command example 3: Delete enabled programs or ports

[Expand table](#)

Old command	New command
-------------	-------------

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

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

ConsoleCopy

netsh advfirewall firewall delete rule ?

Command example 4: Configure ICMP settings

Expand table

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

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

ConsoleCopy

netsh advfirewall firewall add rule ?

Command example 5: Set logging

Expand table

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

For more information, run the following command:

ConsoleCopy

netsh advfirewall set currentprofile ?

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

For more information, run the following command:

Console

netsh advfirewall set currentprofile ?

Copy

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

netsh advfirewall reset ?

Copy


Command example 8: Enable specific services


 Expand table

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

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) 

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.