Netsh Commands for Windows Firewall

By Archiveddocs

Archived: 2026-04-05 14:55:07 UTC

Applies To: Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows Vista

The Netsh commands for Windows Firewall provide a command-line alternative to the capabilities of the Windows Firewall Control Panel utility. By using the Netsh firewall commands, you can configure and view Windows Firewall exceptions and configuration settings.

Important

The **firewall** context of the netsh command-line tool is provided only for backwards-compatibility with earlier versions of Windows. The **firewall** context works on computers that are running Windows® 7, Windows Server® 2008 R2, Windows Vista®, and Windows Server® 2008, but it does not allow you to manage or interact with any of the firewall features that are new to those newer versions of Windows. This context does not allow you to work remotely on a computer to directly configure its firewall.
We recommend that you instead use the **advfirewall** context unless you are using this tool in a mixed environment and must maintain backwards-compatibility with earlier versions of Windows. To use the new firewall features that are included with Windows Vista and later versions of Windows, you must use the **advfirewall** context instead. For more information, see Netsh Commands for Windows Firewall with Advanced Security.
We recommend that you do not use this context on a computer that is running Windows Vista or a later version of Windows, because by using it you can create and modify firewall rules only for the domain and private profiles. Earlier versions of Windows only supported a domain and standard profile. On Windows Vista and later versions of Windows, standard maps to the private profile and domain continues to map to the domain profile. Rules for the public profile can only be manipulated when the computer is actually attached to a public network and the command is run against the "current" profile.
Starting with Windows 7 and Windows Server 2008 R2, if you run any command in the firewall context, the command still works, but is accompanied by the message:
IMPORTANT: “netsh firewall” is deprecated; use “netsh advfirewall firewall” instead. For more information on using “netsh advfirewall firewall” commands instead of “netsh firewall”, see KB article 947709 at https://go.microsoft.com/fwlink/?linkid=121488.

Important

To use the netsh firewall commands remotely on another computer by using the netsh –r parameter, the Remote Registry service must be running on the remote computer. If it is not, then Windows displays a “Network Path Not Found” error message.

You can run these commands from within the netsh tool at the **netsh firewall>** prompt.

For these commands to work at a standard Windows command prompt, you must preface each command with **netsh firewall**, followed by the specific command and parameters as they appear in the syntax below.

Note

If User Account Control is enabled on your computer and you want to run any netsh firewall command that changes the firewall configuration, you must run the command from a command prompt that was started with the **Run as administrator** option. If you try to change the firewall state without having administrator permissions available to the command-line tool, it fails with the message "The requested operation requires elevation."

For more information about **netsh**, see Netsh Overview and Enter a Netsh Context.

Netsh firewall

The following sections describe each command and its syntax.

- add allowedprogram
- set allowedprogram
- delete allowedprogram
- set icmpsetting
- set multicastbroadcastresponse
- set notifications
- set logging
- set opmode
- add portopening
- set portopening
- delete portopening
- set service
- show commands
- reset

Note

In earlier versions of Windows, many of these command accepted a parameter called **interface**. This parameter is not supported in the firewall context in Windows Vista or later versions of Windows.

add allowedprogram

Adds a program-based exception to the firewall.

Syntax

add allowedprogram [**program** =] *PathAndFileName* [**name** =] *ProgramName* [[**mode** =] { **enable** | **disable** }] [[**scope** =] { **all** | **subnet** | **custom** }] [[**addresses** =] { *IPAddress* | *IPRange* | *Subnet* | **localsubnet** }[,…]] [[**profile** =] { **current** | **domain** | **standard** | **all** }]

Parameters

- **[program =]** ***PathAndFileName***
  Required. The path and file name of the program to be added to the firewall exception list. If the path or file name includes spaces, then you must use quotation marks around the path and file name.

- **[name =]** ***ProgramName***
  Required. Friendly name of the program to be added to the list. This value is displayed in the Firewall control panel exception list.

- **[[mode =] { enable | disable }]**
  Specifies whether this exception is currently applied and active on the local computer. The default value is **enable**.

- **[[scope =] { all | subnet | custom }]**
  Specifies the scope of the allowed network traffic from remote computers. **all** indicates that traffic is allowed from any computer, including those on the Internet. **subnet** indicates that traffic is allowed from computers on the local computer's subnet only. **custom** indicates that traffic is allowed from only those computers whose IP address matches the **addresses** parameter. The default value is **all**.

- **[[addresses =] { *IPAddress* | *IPRange* | *Subnet* | localsubnet }[,…]]**
  Specifies a custom list of addresses for the **scope=custom** parameter. Each entry can be:

  - An IPv4 or IPv6 address. For example, **192.168.0.15**.
  - An IPv4 or IPv6 range with start and end addresses separated by a '-'. For example, **192.168.0.1-192.168.0.50**.
  - A subnet indicated by the subnet address and subnet mask separated by a '/'. For example, **192.168.0.0/255.255.255.0**.
  - A subnet indicated by the subnet address and a subnet prefix separated by a '/'. For example, **10.1.0.0/16**.
  - The keyword **localsubnet**, which includes all addresses that are on the local computer's current subnet.

  Multiple entry types can be combined on a command line by separating them with commas: **172.16.0.0/16, 10.0.0.0/255.0.0.0, 21AB:0000:0000:CD30::/60, localsubnet**

- **[[profile** = **] { current** | **domain** | **standard** | **all** } **]**
  Specifies the firewall profile to which the command applies. The firewall profile is determined by the detected network location types accessible through the computer's network adapters.
    - **current** specifies that the command applies to the profile that is currently active on the computer.

Note

On Windows 7 and Windows Server 2008 R2, this option applies to all profiles that are currently active on the computer.

```
 - **domain** specifies that the command applies only to the domain profile.

- **standard** specifies that the command applies only to the private profile.

- **all** specifies that the command applies to all profiles except the private profile.
```

- You must specify **scope=custom** to specify **addresses**. If **scope=custom** is used, then **addresses** cannot be blank.
- To specify the profile associated with the public network location type, you must specify **profile=current** when the computer is attached to a public network.
- The **addresses** parameter cannot contain an unspecified IPv6 address, a loopback address, or a multicast address.

Examples

Each example must be entered as a single command line. The examples may be displayed on multiple lines below for space reasons.

add allowedprogram "C:\My App\MyApp.exe" "My Application" enable

add allowedprogram "C:\My App\MyApp.exe" "My Application" enable custom 157.60.0.1,172.16.0.0/16,21AB:0000:0000:CD30::/60,localsubnet

set allowedprogram

Modifies the settings of an existing program-based exception.

Syntax

set allowedprogram [**program** =] *PathAndFileName* [[**name** =] *ProgramName*]] [[**mode** =] { **enable** | **disable** }] [[**scope** =] { **all** | **subnet** | **custom** }] [[**addresses** =] { *IPAddress* | *IPRange* | *Subnet* | **localsubnet** } [,…]] [[**profile** =] { **current** | **domain** | **standard** | **all** }]

Parameters

- **[program =] *PathAndFileName*]**
  Required. The path and file name of the program whose exception you want to modify. If the path or file name includes spaces, then you must use quotation marks around the path and file name.

- **[[name =] *ProgramName*]**
  Friendly name of the program to be added to the list. This value is displayed in the Firewall control panel exception list.

- **[[mode =] { enable | disable }]**
  Specifies whether this exception is currently applied and active on the local computer.

- **[[scope =] { all | subnet | custom }]**
  Specifies the scope of the allowed network traffic from remote computers. **all** indicates that traffic is allowed from any computer, including those on the Internet. **subnet** indicates that traffic is allowed from computers on the local computer's subnet only. **custom** indicates that traffic is allowed from only those computers whose IP address matches the **addresses** parameter.

- **[[addresses =] { *IPAddress* | *IPRange* | *Subnet* | localsubnet }[,…]]**
  Specifies a custom list of addresses for the **scope=custom** parameter. Each entry can be:

  - An IPv4 or IPv6 address. For example, **192.168.0.15**.
  - An IPv4 or IPv6 range with start and end addresses separated by a '-'. For example, **192.168.0.1-192.168.0.50**.
  - A subnet indicated by the subnet address and subnet mask separated by a '/'. For example, **192.168.0.0/255.255.255.0**.
  - A subnet indicated by the subnet address and a subnet prefix separated by a '/'. For example, **10.1.0.0/16**.
  - The keyword **localsubnet**, which includes all addresses that are on the local computer's current subnet.

  Multiple entry types can be combined on a command line by separating them with commas: **172.16.0.0/16, 10.0.0.0/255.0.0.0, 21AB:0000:0000:CD30::/60, localsubnet**

- **[[profile =] { current | domain | standard | all }]**
  Specifies the firewall profile to which the command applies. The profile is determined by the detected network location types accessible through the computer's network adapters.

  - **current** specifies that the command applies to the profile that is currently active on the computer.

Note

On Windows 7 and Windows Server 2008 R2, this option applies to all profiles that are currently active on the computer.

```
   - **domain** specifies that the command applies only to the domain profile.

  - **standard** specifies that the command applies only to the private profile.

  - **all** specifies that the command applies to all profiles except the private profile.


The default value is **current**.
```

- You must specify at least one parameter other than **program**.
- You must specify **scope=custom** to specify **addresses**. If **scope=custom** is used, then **addresses** cannot be blank.
- To specify the profile associated with the public network location type, you must specify **profile=current** when the computer is attached to a public network.
- The **addresses** parameter cannot contain an unspecified IPv6 address, a loopback address, or a multicast address.

Examples

Each example must be entered as a single command line. The examples may be displayed on multiple lines below for space reasons.

set allowedprogram "C:\My App\MyApp.exe" "My Application" enable

set allowedprogram "C:\My App\MyApp.exe" "My Application" enable custom 157.60.0.1,172.16.0.0/16,10.0.0.0/255.0.0.0,localsubnet

set allowedprogram program="C:\My App\MyApp.exe" name=MyApp mode=enable scope=custom addresses=157.60.0.1,172.16.0.0/16,10.0.0.0/255.0.0.0,localsubnet

delete allowedprogram

Deletes an existing program-based exception.

Syntax

delete allowedprogram [**program =**] *PathAndFileName* [[**profile =**] { **current** | **domain** | **standard** | **all** }]

Parameters

- **[program =]** ***PathAndFileName***
  Required. The path and file name of the program to be deleted from the firewall exception list.
- **[[profile =] { current | domain | standard | all }]**
  Specifies the firewall profile to which the command applies. The profile is determined by the detected network location types accessible through the computer's network adapters.
    - **current** specifies that the command applies to the profile that is currently active on the computer.

Note

On Windows 7 and Windows Server 2008 R2, this option applies to all profiles that are currently active on the computer.

```
 - **domain** specifies that the command applies only to the domain profile.

- **standard** specifies that the command applies only to the private profile.

- **all** specifies that the command applies to all profiles except the private profile.


The default value is **current**.
```

- To specify the profile associated with the public network location type, you must specify **profile=current** when the computer is attached to a public network.

Examples

Each example must be entered as a single command line. The examples may be displayed on multiple lines below for space reasons.

delete allowedprogram C:\MyApp\MyApp.exe

delete allowedprogram program = C:\MyApp\MyApp.exe profile=all

set icmpsetting

Specifies the types of ICMP traffic that are permitted through the firewall.

Syntax

set icmpsetting [**type =**] { **2-5** | **8-9** | **11-13** | **17** | **all** } [[**mode** =] { **enable** | **disable**}] [[**profile=**] { **current** | **domain** | **standard** | **all** }]

Parameters

- **[type =] { 2**-5** | **8**-**9** | **11**-**13** | **17** | **all** }**
  Required. The type of ICMP traffic to allow. The value must be one of the following ICMP message types:
  - **2** - Outbound packet too big.
  - **3** - Outbound destination unreachable.
  - **4** - Outbound source quench.
  - **5** - Redirect.
  - **8** - Inbound echo request (ping).
  - **9** - Inbound router request.
  - **11** - Outbound time exceeded.
  - **12** - Outbound parameter problem.
  - **13** - Inbound timestamp request.
  - **17** - Inbound mask request.
  - **all** - All of the above types.
- **[[mode =] { enable | disable}]**
  Specifies whether this exception is currently applied and active on the local computer. The default value is **enable**.
- **[[profile =] { current | domain | standard | all }]**
  Specifies the firewall profile to which the command applies. The profile is determined by the detected network location types accessible through the computer's network adapters.
  - **current** specifies that the command applies to the profile that is currently active on the computer.

Note

On Windows 7 and Windows Server 2008 R2, this option applies to all profiles that are currently active on the computer.

```
   - **domain** specifies that the command applies only to the domain profile.

  - **standard** specifies that the command applies only to the private profile.

  - **all** specifies that the command applies to all profiles except the private profile.


The default value is **current**.
```

- To specify the profile associated with the public network location type, you must specify **profile=current** when the computer is attached to a public network.

Examples

Each example must be entered as a single command line. The examples may be displayed on multiple lines below for space reasons.

set icmpsetting 8 enable all

set icmpsetting type=all mode=disable

set multicastbroadcastresponse

Specifies whether or not responses to a multicast or broadcast request are allowed through the firewall.

Syntax

set multicastbroadcastresponse [**mode** =] { **enable** | **disable**} [[**profile=**] { **current** | **domain** | **standard** | **all** }]

Parameters

- **[mode =] { enable | disable}**
  Required. Specifies whether to enable or disable responses to multicast or broadcast traffic. The default value is **enable**.
- **[[profile =] { current | domain | standard | all }]**
  Specifies the firewall profile to which the command applies. The profile is determined by the detected network location types accessible through the computer's network adapters.
  - **current** specifies that the command applies to the profile that is currently active on the computer.
  - **domain** specifies that the command applies only to the domain profile.
  - **standard** specifies that the command applies only to the private profile.
  - **all** specifies that the command applies to all profiles except the private profile.

  The default value is **current**.
- To specify the profile associated with the public network location type, you must specify **profile=current** when the computer is attached to a public network.

Examples

Each example must be entered as a single command line. The examples may be displayed on multiple lines below for space reasons.

set multicastbroadcastresponse enable

set multicastbroadcastresponse mode=enable profile=all

set notifications

Specifies whether the firewall displays a pop-up notification to the user when a program attempts to listen on a port.

Syntax

set notifications [**mode** =] { **enable** | **disable**} [[**profile=**] { **current** | **domain** | **standard** | **all** }]

Parameters

- **[mode =] { enable | disable}**
  Required. Specifies whether to enable or disable responses to multicast or broadcast traffic.
- **[[profile =] { current | domain | standard | all }]**
  Specifies the firewall profile to which the command applies. The profile is determined by the detected network location types accessible through the computer's network adapters.
    - **current** specifies that the command applies to the profile that is currently active on the computer.
    - **domain** specifies that the command applies only to the domain profile.
    - **standard** specifies that the command applies only to the private profile.
    - **all** specifies that the command applies to all profiles except the private profile.

  The default value is **current**.
- To specify the profile associated with the public network location type, you must specify **profile=current** when the computer is attached to a public network.

Examples

Each example must be entered as a single command line. The examples may be displayed on multiple lines below for space reasons.

set notifications enable

set notifications disable

set notifications mode=enable profile=current

set logging

Specifies whether the firewall writes information to a log file, and what details are included. This command only affects the currently active profile.

Syntax

set logging [[**filelocation =**] *PathAndFileName*] [[**maxfilesize =**] *Integer*] [[**droppedpackets =**] { **enable** | **disable** }] [[**connections =**] { **enable** | **disable** }]

Parameters

- **[[filelocation =]** ***PathAndFileName*** **]**
  Specifies the path and file name of the file to which the firewall writes its log. The default value is **%windir%\pfirewall.log**.
- **[[maxfilesize =]** ***Integer*** **]**
  Specifies the maximum file size in kilobytes. Must be an integer value from 1 to 32767. The default value is **4096**.
- **[[droppedpackets =] { enable | disable }]**
  Specifies whether to include an entry for each packet dropped by the firewall. The default value is **disable**.
- **[[connections =] { enable | disable }]]**
  Specifies whether to include an entry for each successful connection. The default value is **disable**.
- At least one parameter must be specified.

Examples

Each example must be entered as a single command line. The examples may be displayed on multiple lines below for space reasons.

set logging enable enable

set logging 4096 enable disable

set logging c:\mylogs\mylog.log 4096 enable enable

set opmode

Specifies the operating mode of Windows Firewall.

Syntax

set opmode [**mode =**] { **enable** | **disable** } [[**exceptions =**] { **enable** | **disable** }] [[**profile =**] { **current** | **domain** | **standard** | **all** }]

Parameters

- **[mode =] { enable | disable}**
  Required. Specifies whether to turn the firewall on or off.
- **[[exceptions =] { enable | disable }]**
  Specifies whether the firewall uses any currently defined port and program exceptions that are enabled. If **exceptions=disable**, then all enabled port and program exceptions are ignored. Default is **enable**.
- **[[profile =] { current | domain | standard | all }]**
  Specifies the firewall profile to which the command applies. The profile is determined by the detected network location types accessible through the computer's network adapters.
    - **current** specifies that the command applies to the profile that is currently active on the computer.

Note

On Windows 7 and Windows Server 2008 R2, this option applies to all profiles that are currently active on the computer.

```
 - **domain** specifies that the command applies only to the domain profile.

- **standard** specifies that the command applies only to the private profile.

- **all** specifies that the command applies to all profiles except the private profile.


The default value is **current**.
```

- To specify the profile associated with the public network location type, you must specify **profile=current** when the computer is attached to a public network.

Examples

Each example must be entered as a single command line. The examples may be displayed on multiple lines below for space reasons.

set opmode enable

set opmode mode=enable exceptions=enable

add portopening

Creates a port-based exception.

Syntax

add portopening [**protocol =**] { **tcp** | **udp** | **all** } [**port =**] *Integer* [**name =**] *ExceptionName* [[**mode =**] { **enable** | **disable** }] [[**scope =**] **all** | **subnet** | **custom** }] [[**addresses** =] addresses] [[**profile =**] **current** | **domain** | **standard** | **all** }]

Parameters

- **[protocol =] { tcp | udp | all }**
  Required. Specifies whether the port number refers to TCP, UDP, or both.

- **[port =]** ***Integer***
  Required. Specifies the port number to be excepted. Must be an integer value from 1 to 65535. Only a single value can be specified and port ranges are not supported.

- **[name =]** ***ExceptionName***
  Required. Specifies the name of the exception. This value is displayed in the Firewall control panel exception list.

- **[[mode =] { enable | disable }]**
  Specifies whether this exception is currently applied and active on the local computer.

- **[scope =] { all | subnet | custom }**
  Specifies the scope of the allowed network traffic from remote computers. **all** indicates that traffic is allowed from any computer, including those on the Internet. **subnet** indicates that traffic is allowed from computers on the local computer's subnet only. **custom** indicates that traffic is allowed from only those computers whose IP address matches the **addresses** parameter. The default value is **all**.

- **[addresses =] {** ***IPAddress*** **|** ***IPRange*** **|** ***Subnet*** **| localsubnet }[,…]**
  Specifies a custom list of addresses for the **scope=custom** parameter. Each entry can be:

  - An IPv4 or IPv6 address. For example, **192.168.0.15**.
  - An IPv4 or IPv6 range with start and end addresses separated by a '-'. For example, **192.168.0.1-192.168.0.50**.
  - A subnet indicated by the subnet address and subnet mask separated by a '/'. For example, **192.168.0.0/255.255.255.0**.
  - A subnet indicated by the subnet address and a subnet prefix separated by a '/'. For example, **10.1.0.0/16**.
  - The keyword **localsubnet**, which includes all addresses that are on the local computer's current subnet.

  Multiple entry types can be combined on a command line by separating them with commas: **172.16.0.0/16, 10.0.0.0/255.0.0.0, 21AB:0000:0000:CD30::/60, localsubnet**

- **[profile =] { current | domain | standard | all }**
  Specifies the firewall profile to which the command applies. The profile is determined by the detected network location types accessible through the computer's network adapters.
    - **current** specifies that the command applies to the profile that is currently active on the computer.

Note

On Windows 7 and Windows Server 2008 R2, this option applies to all profiles that are currently active on the computer.

```
 - **domain** specifies that the command applies only to the domain profile.

- **standard** specifies that the command applies only to the private profile.

- **all** specifies that the command applies to all profiles except the private profile.


The default value is **current**.
```

- You must specify **scope=custom** to specify **addresses**. If **scope=custom** is used, then **addresses** cannot be blank.
- To specify the profile associated with the public network location type, you must specify **profile=current** when the computer is attached to a public network.
- The **addresses** parameter cannot contain an unspecified IPv6 address, a loopback address, or a multicast address.

Examples

Each example must be entered as a single command line. The examples may be displayed on multiple lines below for space reasons.

add portopening tcp 80 MyWebPort

add portopening udp 500 "IKE Exception" enable all

add portopening all 53 DNS enable custom 157.60.0.1,172.16.0.0/16,10.0.0.0/255.0.0.0,localsubnet

set portopening

Modifies the settings of an existing port-based exception.

Syntax

set portopening [**protocol =**] { **tcp** | **udp** | **all** } [**port =**] *Integer* [[**name =**] *ExceptionName*]] [[**mode =**] { **enable** | **disable** }] [[**scope =**] **all** | **subnet** | **custom** }] [[**addresses** =] addresses] [[**profile =**] **current** | **domain** | **standard** | **all** }]

Parameters

- **[protocol =] { tcp | udp | all }**
  Required. Specifies whether the port number refers to TCP, UDP, or both.

- **[port =]** ***Integer***
  Required. Specifies the port number of the exception to be modified. Must be an integer value from 1 to 65535. Only a single value can be specified and port ranges are not supported.

- **[[name =]** ***ExceptionName*** **]**
  Specifies the name of the exception. This value is displayed in the Firewall control panel exception list.

- **[[mode =] { enable | disable }]**
  Specifies whether this exception is currently applied and active on the local computer.

- **[scope =] { all | subnet | custom }**
  Specifies the scope of the allowed network traffic from remote computers. **all** indicates that traffic is allowed from any computer, including those on the Internet. **subnet** indicates that traffic is allowed from computers on the local computer's subnet only. **custom** indicates that traffic is allowed from only those computers whose IP address matches the **addresses** parameter.

- **[addresses =] {** ***IPAddress*** **|** ***IPRange*** **|** ***Subnet*** **| localsubnet }[,…]**
  Specifies a custom list of addresses for the **scope=custom** parameter. Each entry can be:

  - An IPv4 or IPv6 address. For example, **192.168.0.15**.
  - An IPv4 or IPv6 range with start and end addresses separated by a '-'. For example, **192.168.0.1-192.168.0.50**.
  - A subnet indicated by the subnet address and subnet mask separated by a '/'. For example, **192.168.0.0/255.255.255.0**.
  - A subnet indicated by the subnet address and a subnet prefix separated by a '/'. For example, **10.1.0.0/16**.
  - The keyword **localsubnet**, which includes all addresses that are on the local computer's current subnet.

  Multiple entry types can be combined on a command line by separating them with commas: **172.16.0.0/16, 10.0.0.0/255.0.0.0, 21AB:0000:0000:CD30::/60, localsubnet**

- **[profile =] { current | domain | standard | all }**
  Specifies the firewall profile to which the command applies. The profile is determined by the detected

network location types accessible through the computer's network adapters.

- **current** specifies that the command applies to the profile that is currently active on the computer.

Note

On Windows 7 and Windows Server 2008 R2, this option applies to all profiles that are currently active on the computer.

```
 - **domain** specifies that the command applies only to the domain profile.

- **standard** specifies that the command applies only to the private profile.

- **all** specifies that the command applies to all profiles except the private profile.
```

- You must specify at least one parameter other than **port** and **protocol**.
- You must specify **scope=custom** to specify **addresses**. If **scope=custom** is used, then **addresses** cannot be blank.
- To specify the profile associated with the public network location type, you must specify **profile=current** when the computer is attached to a public network.
- The **addresses** parameter cannot contain an unspecified IPv6 address, a loopback address, or a multicast address.

Examples

Each example must be entered as a single command line. The examples may be displayed on multiple lines below for space reasons.

set portopening tcp 80 "My Web Port"

set portopening udp 500 "IKE Exception" enable all

set portopening all 53 "DNS Exception" enable custom 157.60.0.1,172.16.0.0/16,10.0.0.0/255.0.0.0,localsubnet

delete portopening

Deletes an existing port-based exception.

Syntax

delete portopening

[**protocol =**] { **tcp** | **udp** | **all** } [**port =**] *Integer* [[**profile =**] **current** | **domain** | **standard** | **all** }]

Parameters

- **[protocol =] { tcp | udp | all }**
  Required. Specifies whether the port number refers to TCP, UDP, or both.
- **[port =]** ***Integer***
  Required. Specifies the port number to be excepted. Must be an integer value from 1 to 65535.
- **[profile =] { current | domain | standard | all }**
  Specifies the firewall profile to which the command applies. The profile is determined by the detected network location types accessible through the computer's network adapters.
  - **current** specifies that the command applies to the profile that is currently active on the computer.
  - **domain** specifies that the command applies only to the domain profile.
  - **standard** specifies that the command applies only to the private profile.
  - **all** specifies that the command applies to all profiles except the private profile.

  The default value is **current**.
- To specify the profile associated with the public network location type, you must specify **profile=current** when the computer is attached to a public network.

Examples

Each example must be entered as a single command line. The examples may be displayed on multiple lines below for space reasons.

delete portopening tcp 80

delete portopening protocol=all port=25

set service

Enables or disables the pre-defined file and printer sharing, remote administration, remote desktop, and UPnP exceptions.

Syntax

set service [**type =**] { **fileandprint** | **remoteadmin** | **remotedesktop** | **upnp** | **all** } [[**mode =**] { **enable** | **disable** }] [[**scope =**] { **all** | **subnet** | **custom** }] [[**addresses =**] { *IPAddress* | *IPRange* | *Subnet* | **localsubnet** } [,…]] [[**profile =**] { **current** | **domain** | **standard** | **all** }]

Parameters

- **[type =] { fileandprint | remoteadmin | remotedesktop | upnp | all }**
  Required. Specifies the service whose pre-defined rules are enabled or disabled. The value must be one of the following:
  - **fileandprint**. The file and printer sharing service.
  - **remoteadmin**. The ability to remotely administer a computer running Windows.
  - **remotedesktop**. The ability to use a Terminal Services client such as Remote Desktop.
  - **upnp**. Universal Plug-and-Play protocol for networked devices.
  - **all**. All of the above services.
- **[[mode =] { enable | disable }]**
  Specifies whether this exception is currently applied and active on the local computer. The default value is **enable**.
- **[[scope =] { all | subnet | custom }]**
  Specifies the scope of the allowed network traffic from remote computers. **all** indicates that traffic is allowed from any computer, including those on the Internet. **subnet** indicates that traffic is allowed from computers on the local computer's subnet only. **custom** indicates that traffic is allowed from only those computers whose IP address matches the **addresses** parameter.
- **[[addresses =] { *IPAddress* | *IPRange* | *Subnet* | localsubnet }[,…]]**
  Specifies a custom list of addresses for the **scope=custom** parameter. Each entry can be:
  - An IPv4 or IPv6 address. For example, **192.168.0.15**.
  - An IPv4 or IPv6 range with start and end addresses separated by a '-'. For example, **192.168.0.1-192.168.0.50**.
  - A subnet indicated by the subnet address and subnet mask separated by a '/'. For example, **192.168.0.0/255.255.255.0**.
  - A subnet indicated by the subnet address and a subnet prefix separated by a '/'. For example, **10.1.0.0/16**.
  - The keyword **localsubnet**, which includes all addresses that are on the local computer's current subnet.

  Multiple entry types can be combined on a command line by separating them with commas: **172.16.0.0/16, 10.0.0.0/255.0.0.0, 21AB:0000:0000:CD30::/60, localsubnet**
- **[[profile =] { current | domain | standard | all }]**
  Specifies the firewall profile to which the command applies. The profile is determined by the detected

network location types accessible through the computer's network adapters.

- **current** specifies that the command applies to the profile that is currently active on the computer.

Note

On Windows 7 and Windows Server 2008 R2, this option applies to all profiles that are currently active on the computer.

```
 - **domain** specifies that the command applies only to the domain profile.

- **standard** specifies that the command applies only to the private profile.

- **all** specifies that the command applies to all profiles except the private profile.


The default value is **current**.
```

- You must specify **scope=custom** to specify **addresses**. If **scope=custom** is used, then **addresses** cannot be blank.
- To specify the profile associated with the public network location type, you must specify **profile=current** when the computer is attached to a public network.
- The **addresses** parameter cannot contain an unspecified IPv6 address, a loopback address, or a multicast address.

Examples

Each example must be entered as a single command line. The examples may be displayed on multiple lines below for space reasons.

set service fileandprint

set service remoteadmin enable subnet

set service type=remotedesktop mode=enable scope=custom addresses=157.60.0.1,172.16.0.0/16,10.0.0.0/255.0.0.0,localsubnet

show commands

The following show commands are used to display the current configuration:

Note

The **show** command cannot be used to see the list of exceptions for the public profile, even if the public profile is the current profile. To see the list of exceptions for the public profile, use the Windows Firewall with Advanced

Security MMC snap-in, and use the **Filter by Profile** option in the Actions pane.

- **show allowedprogram** [[**verbose =**] { **enable** | **disable** }]

  Displays the current list of program exceptions for the domain and standard profiles. Use the parameter **verbose=enable** to see additional details.

- **show config** [[**verbose =**] { **enable** | **disable** }]

  Displays the local configuration information for the domain and standard profiles, including the output of all other **show** commands. Use parameter **verbose=enable** to see additional details.

- **show currentprofile**

  Displays the current profile in use for the network location type.

Note

If the current profile is the public profile, then this command shows the standard profile.

- **show icmpsetting** [[**verbose =**] { **enable** | **disable** }]

  Displays the ICMP settings. Use parameter **verbose=enable** to see additional details.

- **show logging**

  Displays the current logging settings.

Note

If the current profile is the public profile, then this command shows the standard profile.

- **show multicastbroadcastresponse**

  Displays multicast/broadcast response settings for each profile.

- **show notifications**

  Displays whether the firewall displays pop-up notifications for each profile.

- **show opmode**

  Displays the operational mode for the firewall for each profile.

- **show portopening**

  Displays the current list of port exceptions for each profile. Use parameter **verbose=enable** to see additional details.

- **show service**

Displays the service configuration for each profile. Use parameter **verbose=enable** to see additional details.

- **show state**

  Displays the current state information for the firewall. Use parameter **verbose=enable** to see additional details.

reset

Resets the configuration of Windows Firewall to default settings. All manually configured changes are lost. There are no parameters for the reset command.
