



Windows PowerShell Get-Help on Cmdlet 'Remove-NetFirewallHyperVRule'

PS:\>Get-HELP Remove-NetFirewallHyperVRule -Full

NAME

Remove-NetFirewallHyperVRule

SYNOPSIS

Deletes one or more Hyper-V firewall rules that match the specified criteria.

SYNTAX

```
Remove-NetFirewallHyperVRule [-Action {NotConfigured | Allow | Block}] [-AsJob] [-CimSession <CimSession[]>]
[-Direction {Inbound | Outbound}] -DisplayName <String>
[-Enabled {True | False}] [-EnforcementStatus {Unknown | OK | Inactive | Error}] [-Name <String>] [-PolicyStore <String>]
[-PolicyStoreSourceType {None | Local |
MDM}] [-Protocol <String>] [-ThrottleLimit <Int32>] [-VMCreatorId <String>] [<CommonParameters>]
```

DESCRIPTION

Important : Running this cmdlet without parameters removes all Windows Hyper-V firewall rules on the target computer.
Always run this cmdlet with the WhatIf parameter
if you are not targeting a specific Windows Hyper-V Firewall rule.

The Remove-NetFirewallHyperVRule cmdlet permanently deletes a Hyper-V firewall rule to be inactive. This is different from the Disable-NetFirewallHyperVRule cmdlet,

which will only disable the rule. A Disabled rule will not actively modify system behavior, but the rule still exists on the computer so it can be re-enabled later.

This cmdlet removes one or more Hyper-V firewall rules with the Name parameter, DisplayName parameter, or rule properties.

PARAMETERS

-Action <Action>

Specifies that matching Hyper-V firewall rules of the indicated action are removed. The acceptable values for this parameter are: Allow or Block.

- Allow: Network packets that match all criteria specified in this rule are permitted through the firewall. This is the default value. - Block: Network packets

that match all criteria specified in this rule are dropped by the firewall.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-AsJob [<SwitchParameter>]

Runs the cmdlet as a background job. Use this parameter to run commands that take a long time to complete.

Required?	false
Position?	named
Default value	False
Accept pipeline input?	False
Accept wildcard characters?	false

-CimSession <CimSession[]>

Runs the cmdlet in a remote session or on a remote computer. Enter a computer name or a session object, such as the output of a New-CimSession

(<https://go.microsoft.com/fwlink/p/?LinkId=227967>) or

[Get-CimSession](<https://go.microsoft.com/fwlink/p/?LinkId=227966>)cmdlet. The default is the current session on the local computer.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-Direction <Direction>

Specifies that matching Hyper-V firewall rules of the indicated direction are removed. This parameter specifies which direction of traffic to match with this rule. The acceptable values for this parameter are: Inbound or Outbound.

Required?	false
Position?	named
Default value	Inbound
Accept pipeline input?	False
Accept wildcard characters?	false

-DisplayName <String>

Specifies that only matching Hyper-V firewall rules of the indicated display name are removed. Wildcard characters are accepted.

Required?	true
Position?	named
Default value	None
Accept pipeline input?	False

Accept wildcard characters? false

-Enabled <Enabled>

Specifies that matching Hyper-V firewall rules of the indicated state are removed. This parameter specifies that the rule object is administratively enabled or

administratively disabled. The acceptable values for this parameter are: - True: Specifies the rule is currently enabled.

- False: Specifies the rule is currently disabled.

Note that the type of this parameter is not Boolean, therefore ``$true`` and ``$false`` variables are not acceptable values here. Use "True" and "False" text strings

instead.

A disabled rule will not actively modify computer behavior, but the management construct still exists on the computer so it can be re-enabled.

Required? false

Position? named

Default value True

Accept pipeline input? False

Accept wildcard characters? false

-EnforcementStatus <PrimaryStatus[]>

Specifies that firewall rules that match the indicated enforcement status are removed. This parameter specifies the overall status of the rule. - OK: Specifies

that the rule will work as specified.

- PartiallyEnforced: Specifies that one or more parts of the rule will not be enforced.

- NoApplicablePorts: Specifies that the rule is functioning as expected, but there are no ports applicable for this rule and therefore is not active.

- ParsingError: Specifies that the rule is corrupted and the computer is unable to use the rule at all.

- Error: Specifies that the computer is unable to use the rule at all.

Required? false
Position? named
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-Name <String>

Specifies that only matching Hyper-V firewall rules of the indicated name are removed. This name serves as the unique identifier for this rule. This parameter acts just like a file name, in that only one rule with a given name may exist in a policy store at a time.

Required? false
Position? named
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-PolicyStore <String>

Targets the policy store from which to remove the rules. A policy store is a container for firewall policy. The acceptable values for this parameter are: -

PersistentStore: Sometimes called static rules, this store contains the persistent policy for the local computer. This policy is not from GPOs, and has been

created manually or programmatically (during application installation) on the computer. Rules created in this store are attached to the ActiveStore and activated

on the computer immediately. - ActiveStore: This store contains the currently active policy, which is the sum of all policy stores that apply to the computer.

- SystemDefaults: This read-only store contains the default state of firewall rules.

- MDM: This store contains the rules configured via MDM.

By default, the PersistentStore is queried.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-PolicyStoreSourceType <PolicyStoreType[]>

Specifies that Hyper-V firewall rules that match the indicated policy store source type are removed. This parameter value is automatically generated and should

not be modified. The acceptable values for this parameter are: - Local: The object originates from the local store.

- MDM: The object originates from the MDM store.

By default, the local store is queried.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-Protocol <String>

Specifies that only matching Hyper-V firewall rules with the indicated protocol are removed.

The acceptable values for this parameter are: - Protocols by number: 0-255.

- Protocols by name: TCP, UDP, ICMPv4, or ICMPv6.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-ThrottleLimit <Int32>

Specifies the maximum number of concurrent operations that can be established to run the cmdlet. If this parameter is omitted or a value of `0` is entered,

Windows PowerShell calculates an optimum throttle limit for the cmdlet based on the number of CIM cmdlets that are running on the computer.

The throttle limit applies only to the current cmdlet, not to the session or to the computer.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-VMCreatorId <String>

Specifies that only matching Hyper-V firewall rules with the specified VMCreatorId are removed. The format for this value is a GUID enclosed in brackets, such as

'{9E288F02-CE00-4D9E-BE2B-14CE463B0298}'.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False

Accept wildcard characters? false

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, PipelineVariable, and OutVariable. For more information, see about_CommonParameters (<https://go.microsoft.com/fwlink/?LinkID=113216>).

INPUTS

None

OUTPUTS

Microsoft.Management.Infrastructure.CimInstance#root\StandardCimv2\NetFirewallHyperVRule

The `Microsoft.Management.Infrastructure.CimInstance` object is a wrapper class that displays Windows Management Instrumentation (WMI) objects. The path after the pound sign (`#`) provides the namespace and class name for the underlying WMI object.

NOTES

----- EXAMPLE 1 -----

```
PS C:\> Remove-NetFirewallHyperVRule
```

This example retrieves all the Hyper-V firewall rules in the local store and removes them.

----- EXAMPLE 2 -----

```
PS C:\> Remove-NetFirewallHyperVRule -DisplayName 'MyServerIPBlock'
```


This example retrieves all the Hyper-V firewall rules with DisplayName 'MyServerIPBlock' and removes them.

RELATED LINKS

Online

Version:

[https://docs.microsoft.com/powershell/module/netsecurity/remove-netfirewallhypervrule?view=windowsserver2022-ps&wt.m
c_id=ps-gethelp](https://docs.microsoft.com/powershell/module/netsecurity/remove-netfirewallhypervrule?view=windowsserver2022-ps&wt.mc_id=ps-gethelp)

New-NetFirewallHyperVRule

Get-NetFirewallHyperVRule

Enable-NetFirewallHyperVRule

Disable-NetFirewallHyperVRule

Rename-NetFirewallHyperVRule

Set-NetFirewallHyperVRule

Get-NetfirewallHyperVVMCreator