



Windows PowerShell Get-Help on Cmdlet 'New-NetFirewallHyperVVMSetting'

PS:\>Get-HELP New-NetFirewallHyperVVMSetting -Full

NAME

New-NetFirewallHyperVVMSetting

SYNOPSIS

Configures Hyper-V firewall per-VM settings on the target computer.

SYNTAX

```
New-NetFirewallHyperVVMSetting [-AsJob] [-CimSession <CimSession[>] [-DefaultInboundAction {NotConfigured | Allow  
| Block}] [-DefaultOutboundAction {NotConfigured |  
Allow | Block}] [-Enabled {False | True | NotConfigured}] [-LoopbackEnabled {False | True | NotConfigured}]  
[-AllowHostPolicyMerge {False | True | NotConfigured}]  
[-Name <String>] [-ThrottleLimit <Int32>] [<CommonParameters>]
```

DESCRIPTION

The New-NetFirewallHyperVVMSetting cmdlet configures settings for the Hyper-V firewall per-VM settings on the system. These settings are applicable to all Hyper-V firewall ports created by a specific Hyper-V firewall VM creator.

This cmdlet should be used when none of the following are true: a Hyper-V VM creator has registered its VM creator ID with the system, when another Hyper-V setting is

already configured for the specified VM creator ID, or when a Hyper-V firewall port is created with the specified VM creator ID. If any of these is true, the

Set-NetFirewallHyperVVMSetting cmdlet should be used. In other words, this cmdlet can be used to configure policy prior to the application corresponding to the specific VM creator ID running on the system.

PARAMETERS

-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

-DefaultInboundAction <Action>

Specifies how to filter inbound traffic which does not match any Hyper-V firewall rules. The acceptable values for this parameter are: NotConfigured, Allow, or Block.

This setting applies the configuration to all profiles. For configuring at a per-profile granularity, use the `New-NetFirewallHyperVProfile` cmdlet.

- Block: Blocks inbound network traffic that does not match an inbound rule.
- Allow: Allows all inbound network traffic, whether or not it matches an inbound rule.
- NotConfigured: Resets this value back to its default.

The default setting is Block.

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

-DefaultOutboundAction <Action>

Specifies how to filter outbound traffic which does not match any Hyper-V firewall rules. The acceptable values for this parameter are: NotConfigured, Allow, or Block.

This setting applies the configuration to all profiles. For configuring at a per-profile granularity, use the `New-NetFirewallHyperVProfile` cmdlet.

- Block: Blocks outbound network traffic that does not match an outbound rule.
- Allow: Allows all outbound network traffic, whether or not it matches an outbound rule.
- NotConfigured: Resets this value back to its default.

The default setting is Block.

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

-Enabled <GpoBoolean>

Determines whether or not the Hyper-V firewall is active and enforced. The acceptable values for this parameter are: False, True, or NotConfigured.

This setting applies the configuration to all profiles. For configuring at a per-profile granularity, use the ``New-NetFirewallHyperVProfile`` cmdlet.

- True: Enables Windows Hyper-V firewall.
- False: Disables Windows Hyper-V firewall.
- NotConfigured: Resets this value back to its default.

The default setting is True.

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

-LoopbackEnabled <GpoBoolean>

Determines whether or not guest-host loopback traffic is allowed.

The acceptable values for this parameter are: False, True, or NotConfigured.

- True: Hyper-V firewall allows traffic between guest and host.
- False: Hyper-V firewall blocks traffic between guest and host.
- NotConfigured: Resets this value back to its default.

The default setting is False.

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

-AllowHostPolicyMerge <GpoBoolean>

Specifies that the host firewall policy should be merged into the effective policy.

This setting controls whether host firewall profile settings (DefaultInboundAction, DefaultOutboundAction, Enabled, AllowLocalFirewallRules) as well as host

firewall rules (only rules that are IP 5-tuple based, that is, not having any local conditions such as application) should

be applicable to Hyper-V firewall.

Policy configurations may come from many stores. If this setting is True, the following order of precedence is used for determining the effective policy (highest

priority to lowest priority): - Host Firewall Group Policy

- Hyper-V Firewall MDM

- Host Firewall MDM

- Hyper-V Firewall Local

- Host Firewall Local

The acceptable values for this parameter are: False, True, or NotConfigured.

- True: Host firewall rules and settings are applied to the Hyper-V firewall.

- False: Host firewall rules and settings are not applied to Hyper-V firewall

- NotConfigured: Resets this value back to its default.

The default setting is True.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Name <String>

Specifies that the settings are applicable only to the Hyper-V firewall VM creator with the matching ID.

The format for this value is a GUID enclosed in brackets: '{9E288F02-CE00-4D9E-BE2B-14CE463B0298}'.

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

<CommonParameters>

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

INPUTS

None

OUTPUTS

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

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:\> New-NetFirewallHyperVVMSetting -Name '{9E288F02-CE00-4D9E-BE2B-14CE463B0298}' -LoopbackEnabled True
```

This example configures the LoopbackEnabled setting for all Hyper-V firewall ports created by the Hyper-V firewall VM creator specified.

RELATED LINKS

Online

Version:

https://docs.microsoft.com/powershell/module/netsecurity/new-netfirewallhypervvmsetting?view=windowsserver2022-ps&wt.mc_id=ps-gethelp

Get-NetfirewallHyperVRule

Get-NetfirewallHyperVPort

Get-NetfirewallHyperVVMCreator

Get-NetFirewallHyperVVMSetting

Set-NetFirewallHyperVVMSetting

Get-NetFirewallHyperVProfile

New-NetFirewallHyperVProfile

Set-NetFirewallHyperVProfile