Windows PowerShell Get-Help on Cmdlet 'Set-NetFirewallSetting'

PS:\>Get-HELP Set-NetFirewallSetting -Full

NAME

Set-NetFirewallSetting

SYNOPSIS

Modifies the global firewall settings of the target computer.

SYNTAX

Set-NetFirewallSetting [-AllowIPsecThroughNAT {None | Server | Both | NotConfigured}] [-AsJob] [-CertValidationLevel {None | AttemptCrlCheck | RequireCrlCheck |

NotConfigured}] [-CimSession <CimSession[]>] [-Confirm] [-EnablePacketQueuing {None | Inbound | Forward | NotConfigured}] [-EnableStatefulFtp {False | True |

NotConfigured}] [-EnableStatefulPptp {False | True | NotConfigured}] [-Exemptions {None | NeighborDiscovery | Icmp | RouterDiscovery | Dhcp | NotConfigured}]

[-GPOSession <String>] [-KeyEncoding {UTF16 | UTF8 | NotConfigured}] [-MaxSAIdleTimeSeconds <UInt32>] [-PassThru] [-PolicyStore <String>]

[-RemoteMachineTransportAuthorizationList <String>] [-RemoteMachineTunnelAuthorizationList <String>] [-RemoteUserTransportAuthorizationList <String>]

[-RemoteUserTunnelAuthorizationList <String>] [-RequireFullAuthSupport {False | True | NotConfigured}] [-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]

Set-NetFirewallSetting [-AllowIPsecThroughNAT {None | Server | Both | NotConfigured}] [-AsJob] [-CertValidationLevel {None | AttemptCrlCheck | RequireCrlCheck |

NotConfigured}] [-CimSession <CimSession[]>] [-Confirm] [-EnablePacketQueuing {None | Inbound | Forward | NotConfigured}] [-EnableStatefulFtp {False | True |

NotConfigured}] [-EnableStatefulPptp {False | True | NotConfigured}] [-Exemptions {None | NeighborDiscovery | Icmp | RouterDiscovery | Dhcp | NotConfigured}]

-InputObject <CimInstance[]> [-KeyEncoding {UTF16 | UTF8 | NotConfigured}] [-MaxSAIdleTimeSeconds <UInt32>] [-PassThru] [-RemoteMachineTransportAuthorizationList

<String>] [-RemoteMachineTunnelAuthorizationList <String>] [-RemoteUserTransportAuthorizationList <String>] [-RemoteUserTunnelAuthorizationList <String>]

[-RequireFullAuthSupport {False | True | NotConfigured}] [-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Set-NetFirewallSetting cmdlet configures properties that apply to the firewall and IPsec settings, regardless of which network profile is currently in use. This

cmdlet allows the administrator to specify global firewall behavior.

PARAMETERS

-AllowIPsecThroughNAT <IPsecThroughNAT>

Specifies that IPsec configures a security association (SA) when one or both computers involved are behind a network address translation (NAT) device. This

setting indicates on which side NAT traversal should be attempted. The acceptable values for this parameter are: None, Server, Both, or NotConfigured.

- None: Specifies that an SA cannot be negotiated if the server or client computer is behind a NAT device.

- Server: Specifies that an SA can be negotiated if only the server is on a private subnet behind a NAT device.

- Both: Specifies that an SA can be negotiated if the client or server or both of the computers are on private subnets behind one or more NAT devices.

- NotConfigured: Valid only when configuring a GPO.

Removes the setting from the GPO, which results in the policy not changing the value on the computer when the policy is applied.

The default value is None. When managing a GPO, the default setting is NotConfigured.

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

-CertValidationLevel <CRLCheck>

Specifies that IPsec checks the certificates used in authentication against a certificate revocation list (CRL), and how IPsec reacts to a certificate that is

found to be on a CRL. The acceptable values for this parameter are: None, AttemptCrlCheck, RequireCrlCheck, or NotConfigured.

- None: Specifies that IPsec does not perform any CRL checking.

- AttemptCrlCheck: Specifies that IPsec authentication fails only if the certificate is found to be revoked.

- RequireCrlCheck: Specifies that IPsec authentication fails if there is any error during CRL checking, including a failure to retrieve the CRL.

- NotConfigured: Valid only when configuring a GPO.

Removes the setting from the GPO, which results in the policy not changing the value on the computer when the policy is applied.

The default value is None. When managing a GPO, the default setting is NotConfigured.

Required? false
Position? named
Default value None
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

-Confirm [<SwitchParameter>]

Prompts you for confirmation before running the cmdlet.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-EnablePacketQueuing <PacketQueuing>

Specifies how the Windows Firewall with Advanced Security handles packet queuing. This parameter enables inbound or forward packet queuing independently,

allowing the computer is able to evenly distribute CPU load to multiple CPUs for site-to-site IPsec tunnel scenarios. The acceptable values for this parameter

are: None, Inbound, Forward, or NotConfigured.

- None: The firewall tracks the port numbers specified in PORT command requests and in the responses to PASV requests, and then allows the incoming FTP data

traffic entering on the requested port number.

- Inbound: Inbound packet queuing is enabled.

- Forward: Forward packet queuing is enabled.

- NotConfigured: Valid only when configuring a GPO.

Removes the setting from the GPO, which results in the policy not changing the value on the computer when the policy is applied.

The default value when managing a computer running Windows Serverr 2012 is None. When managing a Group Policy Object (GPO), the default setting is NotConfigured.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-EnableStatefulFtp <GpoBoolean>

Configures how Windows Firewall with Advanced Security handles FTP traffic that uses an initial connection on one port to request a data connection on a different

port. This affects both active and passive FTP. If active FTP is used, then the client initiates a connection to the server on TCP port 21 and includes a PORT

command that indicates to the FTP server the port number on which it should respond. A typical firewall on the client would block this new connection as

unsolicited inbound traffic since the packets to the new port are not in response to a request from that port. If passive FTP is used, then the client initiates

a connection to the server on TCP port 21 and includes the PASV command. The server responds on TCP port 21 with a port number that the client must use for

subsequent data transfer. The client then initiates a connection to the server on the specified port. A typical firewall on the FTP server would block this new

incoming data connection as unsolicited inbound traffic since the packets received at the new port are not in response to a request from that port. When this

parameter is True, the firewall examines the PORT and PASV requests for these other port numbers and then allows the corresponding data connection to the port

number that was requested. - True: The firewall tracks the port numbers specified in PORT command requests and in the responses to PASV requests, and then allows

the incoming FTP data traffic entering on the requested port number.

- False: The firewall does not track outgoing PORT commands or PASV responses, and so incoming data connections on the PORT or PASV requested port is blocked as

an unsolicited incoming connection.

- NotConfigured: Valid only when configuring a GPO.

Removes the setting from the GPO, which results in the policy not changing the value on the computer when the policy is applied. The default value is False. The

default value when managing a computer running firstref_vista or firstref_client_7 is True. The default value when managing a computer running firstref_longhorn

or firstref_server_7 is False. When managing a Group Policy Object (GPO), the default value is NotConfigured.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-EnableStatefulPptp <GpoBoolean>

Configures how Windows Firewall with Advanced Security handles PPTP traffic. If a connection is made through TCP port 1723 in nextref_vista, then Windows

Firewall recognizes the connection as being established through PPTP. By default, Windows Firewall uses a stateful PPTP protocol analyzer to determine whether it

can receive packets through the TCP port 1723 connection. Therefore, the stateful PPTP protocol analyzer may reject as not valid any traffic that uses a protocol

other than PPTP. - True: The firewall examines the packets from port 1723 and determines whether the traffic is valid PPTP traffic.

- False: The firewall does not examine the packets from port 1723 to determine whether the traffic is valid PPTP traffic.

- NotConfigured: Valid only when configuring a GPO.

Removes the setting from the GPO, which results in the policy not changing the value on the computer when the policy is applied. The default value is False.

When managing a GPO, the default value is NotConfigured.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Exemptions <TrafficExemption>

Specifies the protocols to be exempted from IPsec requirements. The acceptable values for this parameter are: None,

NeighborDiscovery, Icmp, RouterDiscovery,

Dhcp, or NotConfigured.

- None: No protocols are exempted.

- NeighborDiscovery: Exempt IPv6 Neighbor Discovery protocol traffic.

- Icmp: Exempt ICMP, for both IPv4 and IPv6, protocol traffic.

This option is available on computers that are running Windowsr 7 or nextref_server_7. - RouterDiscovery: Exempt router discovery traffic.

- Dhcp: Exempt DHCP, for both IPv4 and IPv6, protocol traffic.

This option is available on computers that are running Windowsr 7 or nextref_server_7. The default value when managing a local computer that is running Windowsr

7 or nextref_server_7 is NeighborDiscovery,Dhcp. The default value when managing a local computer that is running nextref_vista, nextref_longhorn, Windows XPr,

or Windows Serverr 2003 is NeighborDiscovery.

The default value when managing a GPO is NotConfigured.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-GPOSession <String>

Specifies the network GPO from which to retrieve the rules to be modified. This parameter is used in the same way as the PolicyStore parameter. When modifying

GPOs in Windows PowerShellr, each change to a GPO requires the entire GPO to be loaded, modified, and saved back. On a busy Domain Controller (DC), this can be a

slow and resource-heavy operation. A GPO Session loads a domain GPO onto the local computer and makes all changes in a batch, before saving it back. This reduces

the load on the DC and speeds up the Windows PowerShell cmdlets. To load a GPO Session, use the Open-NetGPO cmdlet. To save a GPO Session, use the Save-NetGPO

cmdlet.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-InputObject <CimInstance[]>

Specifies the input object that is used in a pipeline command.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-KeyEncoding <KeyEncoding>

Specifies the type of key encoding to be used. The acceptable values for this parameter are: UTF16 or UTF8. The default value is UTF8.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-MaxSAIdleTimeSeconds <UInt32>

Specifies the number of minutes that a security association (SA) can stay idle before being deleted. Once deleted, a

new SA must be established before computers

under the scope of the original SA can communicate again. The acceptable values for this parameter are: 300 through 3600 seconds, or NotConfigured.

- A non-zero value, including 300 through 3600, specifies the desired lifetime.

- NotConfigured: Valid only when configuring a GPO.

Removes the setting from the GPO, which results in the policy not changing the value on the computer when the policy is applied. This parameter value is

case-sensitive and NotConfigured can only be specified using dot-notation.

The default value when managing a local computer is 300 seconds (5 minutes). When managing a GPO, the default value is NotConfigured.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-PassThru [<SwitchParameter>]

Returns an object representing the item with which you are working. By default, this cmdlet does not generate any output.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-PolicyStore <String>

Specifies the policy store from which to retrieve the rules to be modified. A policy store is a container for firewall and

IPsec 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.

This is the resultant set of policy (RSOP) for the local computer (the sum of all GPOs that apply to the computer), and the local stores (the PersistentStore, the

static Windows service hardening (WSH), and the configurable WSH). ---- GPOs are also policy stores. Computer GPOs can be specified as follows. ------

`-PolicyStore hostname`.

---- Active Directory GPOs can be specified as follows.

------ `-PolicyStore domain.fqdn.com\GPO_Friendly_Namedomain.fqdn.comGPO_Friendly_Name`.

------ Such as the following.

-------- `-PolicyStore localhost`

-------- `-PolicyStore corp.contoso.com\FirewallPolicy`

---- Active Directory GPOs can be created using the New-GPO cmdlet or the Group Policy Management Console. - RSOP: This read-only store contains the sum of all

GPOs applied to the local computer.

- SystemDefaults: This read-only store contains the default state of firewall rules that ship with Windows Server 2012.

- StaticServiceStore: This read-only store contains all the service restrictions that ship with Windows Server 2012.

Optional and product-dependent features are considered part of Windows Server 2012 for the purposes of WFAS. -ConfigurableServiceStore: This read-write store

contains all the service restrictions that are added for third-party services. In addition, network isolation rules that are created for Windows Store application

containers will appear in this policy store. The default value is PersistentStore. The Set-NetFirewallRule cmdlet cannot be used to add an object to a policy

store. An object can only be added to a policy store at creation time with the Copy-NetFirewallRule cmdlet or with the New-NetFirewallRule cmdlet.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RemoteMachineTransportAuthorizationList <String>

Specifies the computer accounts that are authorized to establish transport connections to the local computer that match this rule. Authorization can override the

per-rule basis and be done at the IPsec layer. The acceptable values for this parameter are:

- None: Specifies that access to the tunnel is not restricted based on computer account.

- <SDDL string>: A string that identifies accounts and the permissions granted or denied to those accounts.

This parameter value is valid on computers that are running Windowsr 7, nextref_server_7, and Windows Server 2012 only, and is ignored on earlier versions of

Windows.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RemoteMachineTunnelAuthorizationList <String>

Specifies the computer accounts that are authorized to establish tunnel connections to the local computer that match this rule. Authorization can override the

per-rule basis and be done at the IPsec layer. The acceptable values for this parameter are:

- None: Specifies that access to the tunnel is not restricted based on computer account.

- <SDDL string>: A string that identifies accounts and the permissions granted or denied to those accounts.

This parameter value is valid on computers that are running Windowsr 7, nextref_server_7, and Windows Server 2012 only, and is ignored on earlier versions of

Windows.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RemoteUserTransportAuthorizationList <String>

Specifies the user accounts that are authorized to establish transport connections to the local computer that match this rule. Authorization can override the

per-rule basis and be done at the IPsec layer. The acceptable values for this parameter are:

- None: Specifies that access to the tunnel is not restricted based on computer account.

- <SDDL string>: A string that identifies accounts and the permissions granted or denied to those accounts.

This parameter value is valid on computers that are running Windowsr 7, nextref_server_7, and Windows Server 2012 only, and is ignored on earlier versions of

Windows.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RemoteUserTunnelAuthorizationList <String>

Specifies the user accounts that are authorized to establish tunnel connections to the local computer that match this rule. Authorization can override the

per-rule basis and be done at the IPsec layer. The acceptable values for this parameter are:

- None: Specifies that access to the tunnel is not restricted based on computer account.

- <SDDL string>: A string that identifies accounts and the permissions granted or denied to those accounts.

This parameter value is valid on computers that are running Windowsr 7, nextref_server_7, and Windows Server 2012 only, and is ignored on earlier versions of

Windows.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RequireFullAuthSupport <GpoBoolean>

Ignores key modules that do not support all of the authentication types present in a rule. If this parameter is set to True, then the behavior is the same as

nextref_vista and Windowsr 7, that the key modules that do not support the entire authentication set will be ignored. If this parameter is set to False, then the

keying modules will try with the subset of configured authentication types that are allowed.

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, then

Windows PowerShellr 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

-WhatIf [<SwitchParameter>]

Shows what would happen if the cmdlet runs. The cmdlet is not run.

Required? false

Position? named

Default value False

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

Microsoft.Management.Infrastructure.CimInstance#root\StandardCimv2\NetFirewallSetting[]

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.

OUTPUTS

Microsoft.Management.Infrastructure.CimInstance#root\StandardCimv2\MSFT_NetServiceFilter[]

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:\>$nfSetting = Get-NetFirewallSetting -PolicyStore corp.contoso.com/gpo_name

PS C:\>Set-NetFirewallSetting -Exemptions RouterDiscovery -InputObject $nfSetting

This cmdlet can be run using only the pipeline.

PS C:\>Get-NetFirewallSetting -PolicyStore corp.contoso.com/gpo_name | Set-NetFirewallSetting -Exemptions RouterDiscovery

This example modifies the global firewall settings of a particular GPO policy store.

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

PS C:\>$computers = New-Object -Typename System.Security.Principal.NTAccount ("corp.contoso.com" "SecureMachineName1")

PS C:\>$SIDofSecureComputerGroup = $computers.Translate([System.Security.Principal.SecurityIdentifier]).Value

PS C:\>$SecureMachineGroupSDDL = "D:(A;;CC;;; $SIDofSecureComputerGroup)"

PS C:\>$nfSetting = Get-NetFirewallSetting -PolicyStore corp.contoso.com/gpo_name

PS C:\>Set-NetFirewallSetting -RemoteMachineTunnelAuthorizationList $SecureMachineGroupSDDL -InputObject $nfSetting

This cmdlet can be run using only the pipeline.

PS C:\>Get-NetFirewallSetting -PolicyStore corp.contoso.com/gpo_name | Set-NetFirewallSetting -RemoteMachineTunnelAuthorizationList $SecureMachineGroupSDDL

This example allows authorization to override the per-rule basis and to be done at the IPsec layer in a GPO.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/netsecurity/set-netfirewallsetting?view=windowsserver2022-ps&wt.mc_id=ps-gethelp

Copy-NetIPsecRule

Get-NetFirewallSetting

New-NetIPsecRule

Open-NetGPO

Save-NetGPO

Set-NetIPsecRule