Full credit is given to all the above companies including the Operating System that this PDF file was generated!

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

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

```
NAME

    Set-NetFirewallProfile


SYNOPSIS

    Configures settings that apply to the per-profile configurations of the Windows Firewall with Advanced Security.



SYNTAX

    Set-NetFirewallProfile [-All] [-AllowInboundRules {False | True | NotConfigured}] [-AllowLocalFirewallRules {False | True |
NotConfigured}] [-AllowLocalIPsecRules
     {False | True | NotConfigured}] [-AllowUnicastResponseToMulticast {False | True | NotConfigured}] [-AllowUserApps
{False | True | NotConfigured}] [-AllowUserPorts
    {False | True | NotConfigured}] [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-DefaultInboundAction {NotConfigured
| Allow | Block}] [-DefaultOutboundAction
     {NotConfigured | Allow | Block}] [-DisabledInterfaceAliases <String[]>] [-EnableStealthModeForIPsec {False | True |
NotConfigured}] [-Enabled {False | True |
     NotConfigured}] [-GPOSession <String>] [-LogAllowed {False | True | NotConfigured}] [-LogBlocked {False | True |
NotConfigured}] [-LogFileName <String>] [-LogIgnored
     {False | True | NotConfigured}] [-LogMaxSizeKilobytes <UInt64>] [-NotifyOnListen {False | True | NotConfigured}]
[-PassThru] [-PolicyStore <String>] [-ThrottleLimit
```

```
    <Int32>] [-WhatIf] [<CommonParameters>]


    Set-NetFirewallProfile [-Name] <String[]> [-AllowInboundRules {False | True | NotConfigured}] [-AllowLocalFirewallRules
{False | True | NotConfigured}]
        [-AllowLocalIPsecRules {False | True | NotConfigured}] [-AllowUnicastResponseToMulticast {False | True |
NotConfigured}] [-AllowUserApps {False | True |
      NotConfigured}] [-AllowUserPorts {False | True | NotConfigured}] [-AsJob] [-CimSession <CimSession[]>] [-Confirm]
[-DefaultInboundAction {NotConfigured | Allow |
          Block}] [-DefaultOutboundAction {NotConfigured | Allow | Block}] [-DisabledInterfaceAliases <String[]>]
[-EnableStealthModeForIPsec {False | True | NotConfigured}]
       [-Enabled {False | True | NotConfigured}] [-GPOSession <String>] [-LogAllowed {False | True | NotConfigured}]
[-LogBlocked {False | True | NotConfigured}]
    [-LogFileName <String>] [-LogIgnored {False | True | NotConfigured}] [-LogMaxSizeKilobytes <UInt64>] [-NotifyOnListen
{False | True | NotConfigured}] [-PassThru]
    [-PolicyStore <String>] [-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]


     Set-NetFirewallProfile [-AllowInboundRules {False | True | NotConfigured}] [-AllowLocalFirewallRules {False | True |
NotConfigured}] [-AllowLocalIPsecRules {False |
    True | NotConfigured}] [-AllowUnicastResponseToMulticast {False | True | NotConfigured}] [-AllowUserApps {False | True
| NotConfigured}] [-AllowUserPorts {False |
    True | NotConfigured}] [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-DefaultInboundAction {NotConfigured | Allow |
Block}] [-DefaultOutboundAction {NotConfigured
     | Allow | Block}] [-DisabledInterfaceAliases <String[]>] [-EnableStealthModeForIPsec {False | True | NotConfigured}]
[-Enabled {False | True | NotConfigured}]
    -InputObject <CimInstance[]> [-LogAllowed {False | True | NotConfigured}] [-LogBlocked {False | True | NotConfigured}]
[-LogFileName <String>] [-LogIgnored {False |
     True | NotConfigured}] [-LogMaxSizeKilobytes <UInt64>] [-NotifyOnListen {False | True | NotConfigured}] [-PassThru]
[-ThrottleLimit <Int32>] [-WhatIf]
    [<CommonParameters>]
```

DESCRIPTION

The Set-NetFirewallProfile cmdlet configures options for the profiles, including domain, public, and private, that are global, or associated with the input rules.

This cmdlet displays information that is presented on the Windows Firewall with Advanced Security Properties page, with the tabs for domain, private, and public

profiles. This cmdlet configures the states, default actions, and logging properties on a per-profile basis.

PARAMETERS

-All [<SwitchParameter>]

Indicates that all of the firewall profiles within the specified policy store are modified.

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

-AllowInboundRules <GpoBoolean>

Specifies that the firewall blocks inbound traffic. If this parameter is set to True, then the administrator will be able to create firewall rules which allow

unsolicited inbound traffic to be accepted. If this parameter is set to False, then firewall rules will be ignored. The acceptable values for this parameter are:

False, True, or NotConfigured.

- True: Inbound firewall rules are allowed. All traffic that does not match a rule will be processed according to the DefaultInboundAction parameter value. -

False: All inbound firewall rules are ignored. All inbound traffic will use the DefaultInboundAction parameter value. If this parameter is set to False and the

DefaultInboundAction parameter is set to Block, then the Windows Firewall is placed into Shields-Up mode on this profile.

- NotConfigured: Valid only when configuring a Group Policy Object (GPO). This parameter 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 setting when managing a computer is True. When managing a GPO, the default setting is NotConfigured.

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

-AllowLocalFirewallRules <GpoBoolean>

Specifies that the local firewall rules should be merged into the effective policy along with Group Policy settings. The acceptable values for this parameter

are: False, True, or NotConfigured.

- True: The firewall rules defined by the local administrator are merged with firewall rules from GPOs and are applied to the computer.

- False: The firewall rules defined by the local administrator are ignored, and only firewall rules from GPOs are applied to the computer.

- NotConfigured: Valid only when configuring a Group Policy Object (GPO).

This parameter 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 setting when managing a computer is True. When managing a GPO, the default setting is NotConfigured.

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

-AllowLocalIPsecRules <GpoBoolean>

Specifies that the local IPsec rules should be merged into the effective policy along with Group Policy settings. The acceptable values for this parameter are:

False, True, or NotConfigured.

- True: The IPsec rules defined by the local administrator are merged with IPsec rules from GPOs and are applied to the computer.

- False: The IPsec rules defined by the local administrator are ignored, and only IPsec rules from GPOs are applied to the computer.

- NotConfigured: Valid only when configuring a Group Policy Object (GPO).

This parameter 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 setting when managing a computer is True. When managing a GPO, the default setting is NotConfigured.

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

-AllowUnicastResponseToMulticast <GpoBoolean>

Allows unicast responses to multi-cast traffic. The acceptable values for this parameter are: False, True, or NotConfigured.

- True: The computer can receive unicast responses to outgoing multi-cast or broadcast messages.

- False: The computer discards unicast responses to outgoing multi-cast or broadcast messages.

- NotConfigured: Valid only when configuring a Group Policy Object (GPO).

This parameter 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 setting when managing a computer is True. When managing a GPO, the default setting is NotConfigured.

Required?   false

Position?   named

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

-AllowUserApps <GpoBoolean>

Determines how the Windows XP policy is applied to the newer Windows Firewall. Defines how to use the policy merge field for older operating systems. Specifies

that traffic from local user applications is allowed through the firewall. The acceptable values for this parameter are: False, True, or NotConfigured.

- True: The traffic from local user applications is allowed.

- False: The traffic from local user applications is blocked.

- NotConfigured: Valid only when Windows PowerShell is configuring a GPO by using this cmdlet.

This parameter removes the setting from the GPO, resulting in the policy not changing the value of the computer when the policy is applied.

Required?   false

Position?   named

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

-AllowUserPorts <GpoBoolean>

Determines how the Windows XP policy is applied to the newer Windows Firewall. Defines how to use the policy merge field for older operating systems. Specifies

that traffic is allowed through local user ports. The acceptable values for this parameter are: False, True, or NotConfigured.

- True: The traffic through local user ports is allowed.

- False: The traffic through local user ports is blocked.

- NotConfigured: Valid only when Windows PowerShell is configuring a GPO by using this cmdlet.

This parameter removes the setting from the GPO, resulting in the policy not changing the value of the computer when the policy is applied.

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
```

-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
```

-DefaultInboundAction <Action>

Specifies how to filter inbound traffic. The acceptable values for this parameter are: NotConfigured, Allow, or Block.

- 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: Valid only when configuring a Group Policy Object (GPO).

This parameter 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 setting when managing a computer is Block. When managing a GPO, the default setting is NotConfigured.

Required?   false

Position?   named

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

-DefaultOutboundAction <Action>

Specifies how to filter outbound traffic. The acceptable values for this parameter are: NotConfigured, Allow, or Block.

- 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: Valid only when configuring a Group Policy Object (GPO).

This parameter 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 setting when managing a computer is Allow. When managing a GPO, the default setting is NotConfigured.

Required?   false

Position?   named

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

-DisabledInterfaceAliases <String[]>

Specifies a list of interfaces on which firewall settings are excluded.

Required?   false

Position?   named

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

-EnableStealthModeForIPsec <GpoBoolean>

Enables stealth mode for IPsec traffic. Stealth mode is a mechanism in Windows Firewall that helps prevent malicious users from discovering information about

network computers and the services that are run. Stealth mode blocks outgoing ICMP unreachable and TCP reset messages for a port when no application is listening

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

Required?   false

Position?   named

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

-Enabled <GpoBoolean>

Allows unicast responses to multi-cast traffic. The acceptable values for this parameter are: False, True, or NotConfigured.

- True: Enables Windows Firewall with Advanced Security when the specified profile is active.

- False: Disables Windows Firewall with Advanced Security when the specified profile is active.

- NotConfigured: Valid only when configuring a Group Policy Object (GPO).

This parameter 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 setting when managing a computer is True. When managing a GPO, the default setting 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

-LogAllowed <GpoBoolean>

Specifies how to log the allowed packets in the location specified by the LogFileName parameter. The acceptable values for this parameter are: False, True, or

NotConfigured.

- True: Windows writes an entry to the log whenever an incoming or outgoing connection is allowed by the policy.

- False: No logging for allowed connections.

- NotConfigured: Valid only when configuring a Group Policy Object (GPO). This parameter 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 setting when managing a computer is False. When managing a GPO, the default setting is NotConfigured.

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

-LogBlocked <GpoBoolean>

Specifies how to log the dropped packets in the location specified by the LogFileName parameter. The acceptable values for this parameter are: False, True, or

NotConfigured.

- True: Windows writes an entry to the log whenever an incoming or outgoing connection is prevented by policy.

- False: No logging for dropped connections.

- NotConfigured: Valid only when configuring a Group Policy Object (GPO).

This parameter 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 setting when managing a computer is False. When managing a GPO, the default setting is NotConfigured.

Required?   false

Position?   named

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

-LogFileName <String>

Specifies the path and filename of the file to which Windows Server 2012 writes log entries. The default setting for managing a computer is

`%windir%\system32\logfiles\firewall\pfirewall.log`. When managing a GPO, the default setting is NotConfigured. To grant write permissions for the log folder to

the Windows Firewall service. - Locate the folder that was specified for the logging file, right-click the file, and then click Properties.

- Select the Security tab, and then click Edit.

- Click Add, in Enter the object names to select, type `NT SERVICE\mpssvc`, and then click OK.

- In the Permissions dialog box, verify that `MpsSvc` has Write access, and then click OK.

Required?   false

Position?   named

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

-LogIgnored <GpoBoolean>

Specifies how to log the ignored packets in the location specified by the LogFileName parameter. The acceptable values for this parameter are: False, True, or

NotConfigured.

- True: Windows writes an entry to the log whenever an incoming or outgoing connection is ignored by policy.

- False: No logging for ignored connections.

- NotConfigured: Valid only when configuring a Group Policy Object (GPO).

This parameter 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 setting when managing a computer is False. When managing a GPO, the default setting is NotConfigured.

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

-LogMaxSizeKilobytes <UInt64>

Specifies the maximum file size of the log, in kilobytes. The acceptable values for this parameter are: 1 through 32767 This parameter specifies in kilobytes the

maximum file size of the log in the location specified by the LogFileName parameter. - NotConfigured: Valid only when configuring a Group Policy Object (GPO).

This parameter 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

setting when managing a computer is 4096. When managing a GPO, the default setting is NotConfigured. This parameter values is case sensitive and NotConfigured

can only be specified using dot-notation.

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

-Name <String[]>

Specifies the network firewall profile objects by profile type to modify. Specifies the profile type. The acceptable values for this parameter are: Domain,

Public, or Private. This parameter accepts multiple values, separated by commas.

Required?   true

Position?   0

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

-NotifyOnListen <GpoBoolean>

Allows the notification of listening for inbound connections by a service. The acceptable values for this parameter are: False, True, or NotConfigured.

- True: Windows notifies the user whenever a program or service starts listening for inbound connections.

- False: Windows does not notify the user whenever a program or service starts listening for inbound connections.

- NotConfigured: Valid only when configuring a Group Policy Object (GPO).

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

computer running firstref_vista and firstref_client_7, then the default value is True. If managing a computer running firstref_longhorn and firstref_server_7,

then the default value is False. If managing a computer running Windows Serverr 2012, then the default value is True. When managing a GPO, the default setting

for all operating systems 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
```

-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\MSFT_NetFirewallProfile[]

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_NetFirewallProfile[]

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:\>Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True
```

This example enables the Windows Firewall on the local computer.

-------------------------- Example 2 --------------------------

```
PS C:\>Set-NetFirewallProfile -DefaultInboundAction Block -DefaultOutboundAction Allow -NotifyOnListen True
-AllowUnicastResponseToMulticast True -LogFileName
%SystemRoot%\System32\LogFiles\Firewall\pfirewall.log
```

This example sets the default inbound and outbound actions, specifies protected network connections, allows notifications to be displayed to the user when a program is blocked from receiving inbound connections. This cmdlet allows unicast response to multi-cast or broadcast network traffic, and specifies logging settings for troubleshooting.

-------------------------- Example 3 --------------------------

```
PS C:\>Set-NetFirewallProfile -Name Domain -DefaultInboundAction Block
```

This example modifies the default inbound action of the domain profile.

-------------------------- Example 4 --------------------------

```
PS C:\>$nfProfile = Get-NetFirewallProfile -Name Private -PolicyStore corp.contoso.com\gpo_name
PS C:\>Set-NetFirewallProfile -AllowUnicastResponseToMulticast True -InputObject $nfProfile
```

This cmdlet can be run using only the pipeline.

```
PS C:\>Get-NetFirewallProfile -Name Private -PolicyStore corp.contoso.com\gpo_name | Set-NetFirewallProfile -AllowUnicastResponseToMulticast True
```

This example modifies the private profile associated with a GPO.

-------------------------- Example 5 --------------------------

```
PS C:\>$nfProfile = Get-NetFirewallRule -DisplayName "Unicast Rule" | Get-NetFirewallProfile
PS C:\>Set-NetFirewallProfile -AllowUnicastResponseToMulticast True -InputObject $nfProfile
```

This cmdlet can be run using only the pipeline.

```
PS C:\>Get-NetFirewallRule -DisplayName "Unicast Rule" | Get-NetFirewallProfile | Set-NetFirewallProfile -AllowUnicastResponseToMulticast True
```

This example modifies the profiles associated with a firewall rule.

RELATED LINKS

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

Copy-NetIPsecRule

Get-NetFirewallProfile

New-NetIPsecRule

Open-NetGPO

Save-NetGPO

Set-NetFirewallRule

Set-NetIPsecRule