



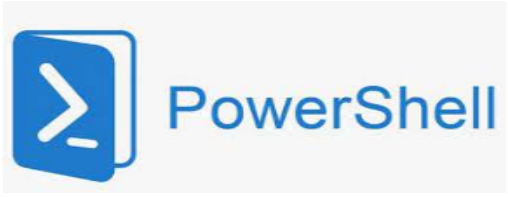



*Full credit is given to the above companies including the OS that this PDF file was generated!*

***PowerShell Get-Help on command 'Set-NetFirewallApplicationFilter'***

***PS C:\Users\wahid> Get-Help Set-NetFirewallApplicationFilter***

NAME

Set-NetFirewallApplicationFilter

SYNOPSIS

Modifies application filter objects, thereby modifying the program and package conditions of the firewall rules.

SYNTAX

Set-NetFirewallApplicationFilter [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-GPOSession <String>] [-Package <String>] [-PassThru] [-PolicyStore <String>] [-Program <String>] [-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]

Set-NetFirewallApplicationFilter [-AsJob] [-CimSession <CimSession[]>] [-Confirm] -InputObject <CimInstance[]> [-Package <String>] [-PassThru] [-Program <String>] [-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Set-NetFirewallApplicationFilter cmdlet modifies the applications

associated with the input firewall rules.

See the Get-NetFirewallApplicationFilter cmdlet for more information on application filters.

To modify the application conditions, two methods can be used starting with the application filters returned by the Get-NetFirewallApplicationFilter cmdlet and optional additional querying. - The application filter objects can be piped to the Get-NetFirewallRule cmdlet, which returns the rule objects associated with the filters. These rules are then piped to the Set-NetFirewallRule cmdlet where the application properties can be configured. - Alternatively, piping the address filter objects directly to this cmdlet allows the Program and Package parameters of the rules to be specified.

PARAMETERS

-AsJob [<SwitchParameter>]

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

-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.

-Confirm [<SwitchParameter>]

Prompts you for confirmation before running the cmdlet.

-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.

-InputObject <CimInstance[]>

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

-Package <String>

Specifies the Windows Store application to which the firewall rule applies. This parameter is specified as a security identifier (SID). Querying for rules with this parameter can only be performed using filter objects.

-PassThru [<SwitchParameter>]

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

-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 Serverr 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 or with the New-NetFirewallRule cmdlet.

-Program <String>

Specifies the path and file name of the program for which the rule allows traffic. This is specified as the full path to an application file.

Querying for rules with this parameter can only be performed using filter objects.

-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.

-WhatIf [<SwitchParameter>]

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

<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).

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

PS C:\>$nfwApplicationFilter = ( Get-FirewallRule -DisplayName "Contoso Messenger" | Get-NetFirewallApplicationFilter )

PS C:\>Set-NetFirewallApplicationFilter -InputObject $nfwApplicationFilter
-Program %SystemRoot%\System32\messenger.exe

This cmdlet can be run using only the pipeline.
PS C:\>Get-FirewallRule -DisplayName "Contoso Messenger" |
Get-NetFirewallApplicationFilter | Set-NetFirewallApplicationFilter -Program
%SystemRoot%\System32\messenger.exe

This cmdlet can be run without using the pipeline.
PS C:\>Set-NetFirewallRule -DisplayName "Contoso Messenger" -Program
%SystemRoot%\System32\messenger.exe

This example changes the application path associated with a particular
firewall rule.
---------- EXAMPLE 2 ----------

PS C:\>$NewPackageSDDL = "S-1-15-2-4292807980-2381230043-3108820062-1451069988-
2614848061-670482394-695399705"

PS C:\>$nfwApplicationFilter = (Get-NetFirewallRule -Group Socialite |
Get-NetFirewallApplicationFilter )

PS C:\>Set-NetFirewallAddressFilter - InputObject $nfwApplicationFilter
-Package $NewPackageSDDL

This cmdlet can be run using only the pipeline.

PS C:\>Get-NetFirewallRule -Group Socialite | Get-NetFirewallApplicationFilter | Set-NetFirewallAddressFilter -Package $NewPackageSDDL

This example modifies the package associated with all related firewall rules for the Socialite Windows Store application.

REMARKS

To see the examples, type: "get-help Set-NetFirewallApplicationFilter -examples".

For more information, type: "get-help Set-NetFirewallApplicationFilter -detailed".

For technical information, type: "get-help Set-NetFirewallApplicationFilter -full".

For online help, type: "get-help Set-NetFirewallApplicationFilter -online"