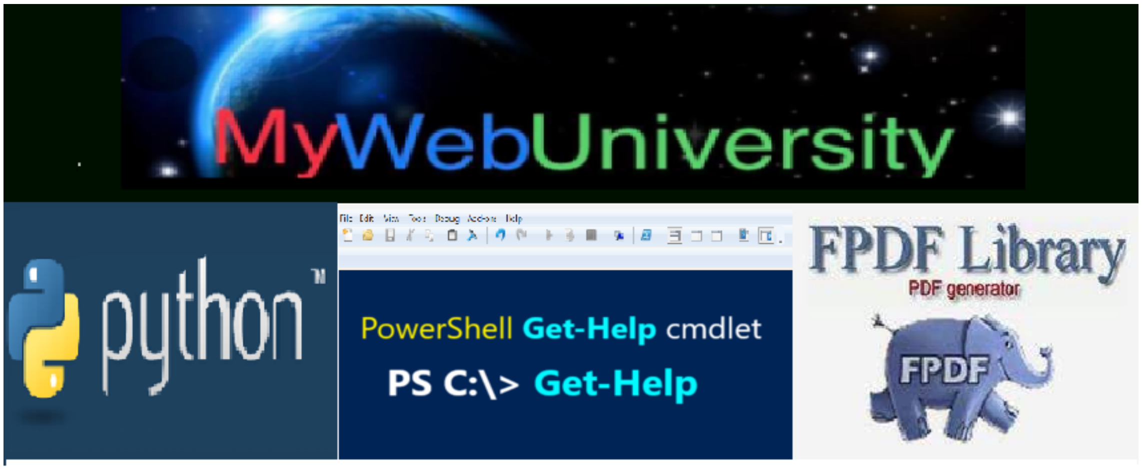

Full credit is given to all the above companies including the Operating System that this PDF file was generated!

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

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

NAME

Get-NetFirewallProfile

SYNOPSIS

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

SYNTAX

Get-NetFirewallProfile [-All] [-AsJob] [-CimSession <CimSession[]>] [-GPOSession <String>] [-PolicyStore <String>] [-ThrottleLimit <Int32>] [<CommonParameters>]

Get-NetFirewallProfile [-AsJob] -AssociatedNetFirewallRule <CimInstance> [-CimSession <CimSession[]>] [-GPOSession <String>] [-PolicyStore <String>] [-ThrottleLimit

<Int32>] [<CommonParameters>]

Get-NetFirewallProfile [-AsJob] -AssociatedNetIPsecMainModeRule <CimInstance> [-CimSession <CimSession[]>] [-GPOSession <String>] [-PolicyStore <String>]

[-ThrottleLimit <Int32>] [<CommonParameters>]

Get-NetFirewallProfile [-AsJob] -AssociatedNetIPsecRule <CimInstance> [-CimSession <CimSession[]>] [-GPOSession

<String>] [-PolicyStore <String>] [-ThrottleLimit <Int32>] [<CommonParameters>]

Get-NetFirewallProfile [-Name] <String[]> [-AsJob] [-CimSession <CimSession[]>] [-GPOSession <String>] [-PolicyStore <String>] [-ThrottleLimit <Int32>] [<CommonParameters>]

DESCRIPTION

The Get-NetFirewallProfile cmdlet displays the currently configured options for a specified profile. 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. The specified profile can be scoped to input rules.

To query for rules scoped to a profile, pipe the profile object into the corresponding cmdlet.

PARAMETERS

-All [<SwitchParameter>]

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

Required? false
Position? named
Default value False
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

-AssociatedNetFirewallRule <CimInstance>

Gets the firewall profile settings associated with the specified firewall rule to be retrieved. This parameter represents a firewall rule, which defines how

traffic is filtered by the firewall. See the New-NetFirewallRule cmdlet for more information.

Required?   true

Position?   named

Default value   None

Accept pipeline input?   True (ByValue)

Accept wildcard characters? false

-AssociatedNetIPsecMainModeRule <CimInstance>

Gets the main mode cryptographic sets that are associated, via the pipeline, with the input main mode rule to be retrieved. This parameter represents a main mode

rule, which alters the behavior of main mode authentications. Main mode negotiation establishes a secure channel between two computers by determining a set of

cryptographic protection suites, exchanging keying material to establish a shared secret key, and authenticating computer and user identities. See the

Get-NetIPsecMainModeRule cmdlet for more information.

Required?   true

Position?   named

Default value   None

Accept pipeline input?   True (ByValue)

Accept wildcard characters? false

-AssociatedNetIPsecRule <CimInstance>

Gets the phase 1 authentication sets that are associated, via the pipeline, with the input IPsec rule to be retrieved. A NetIPsecRule object represents an IPsec

rule, which determines IPsec behavior. An IPsec rule can be associated with Phase1AuthSet, Phase2AuthSet, and

NetIPsecQuickMode cryptographic sets. See the

New-NetIPsecMainModeRule cmdlet for more information.

Required?   true

Position?   named

Default value   None

Accept pipeline input?   True (ByValue)

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

-GPOSession <String>

Specifies the network GPO from which to retrieve the rules to be retrieved. 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

-Name <String[]>

Specifies that only matching firewall rules of the indicated name are retrieved. Wildcard characters are accepted. 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. During group policy processing and policy merge, rules that have the same name but

come from multiple stores being merged, will overwrite one another so that only one exists. This overwriting behavior is desirable if the rules serve the same

purpose. For instance, all of the firewall rules have specific names, so if an administrator can copy these rules to a GPO, and the rules will override the local

versions on a local computer. GPOs can have precedence. So if an administrator has a different or more specific rule with the same name in a higher-precedence

GPO, then it overrides other rules that exist. The default value is a randomly assigned value. When the defaults for main mode encryption need to overridden,

specify the customized parameters and set this parameter value, making this parameter the new default setting for encryption.

Required? true

Position? 0

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-PolicyStore <String>

Specifies the policy store from which to retrieve the rules to be retrieved. 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 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
```

<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_NetConSecRule[]

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.

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

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.

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

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:\>Get-NetFirewallProfile -PolicyStore ActiveStore
```

This example retrieves the active profile conditions on a per profile basis. Running this cmdlet without specifying the policy store retrieves the persistent store.

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

```
PS C:\>Get-NetFirewallProfile -Name Public | Get-NetFirewallRule
```

This example retrieves all the firewall rules scoped to the public profile.

RELATED LINKS

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

Get-NetFirewallRule

Get-NetIPsecRule

New-NetFirewallRule

New-NetIPsecRule

Set-NetFirewallProfile

Set-NetFirewallRule

Set-NetIPsecRule