Windows PowerShell Get-Help on Cmdlet 'Remove-NetIPsecPhase2AuthSet'

PS:\>Get-HELP Remove-NetIPsecPhase2AuthSet -Full

NAME

Remove-NetIPsecPhase2AuthSet

SYNOPSIS

Deletes all of the phase 2 authentication sets that match the specified criteria.

SYNTAX

Remove-NetIPsecPhase2AuthSet [-All] [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-GPOSession <String>] [-PassThru] [-PolicyStore <String>] [-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf] [<CommonParameters>]

Remove-NetIPsecPhase2AuthSet [-AsJob] -AssociatedNetIPsecRule <CimInstance> [-CimSession <CimSession[]>] [-Confirm] [-GPOSession <String>] [-PassThru] [-PolicyStore <String>] [-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf] [<CommonParameters>]

Remove-NetIPsecPhase2AuthSet [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-Description <String[]>] [-DisplayGroup <String[]>] [-GPOSession <String>] [-Group <String[]>] [-PassThru] [-PolicyStore <String>] [-PolicyStoreSource <String[]>] [-PolicyStoreSourceType {None | Local | GroupPolicy | Dynamic | Generated |

Hardcoded}] [-PrimaryStatus {Unknown | OK | Inactive | Error}] [-Status <String[]>] [-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf] [<CommonParameters>]

Remove-NetIPsecPhase2AuthSet [-AsJob] [-CimSession <CimSession[]>] [-Confirm] -DisplayName <String[]> [-GPOSession <String>] [-PassThru] [-PolicyStore <String>]
[-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf] [<CommonParameters>]

Remove-NetIPsecPhase2AuthSet [-Name] <String[]> [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-GPOSession <String>] [-PassThru] [-PolicyStore <String>]
[-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf] [<CommonParameters>]

Remove-NetIPsecPhase2AuthSet [-AsJob] [-CimSession <CimSession[]>] [-Confirm] -InputObject <CimInstance[]> [-PassThru] [-ThrottleLimit <Int32>] [-WhatIf]
[<CommonParameters>]

DESCRIPTION

The Remove-NetIPsecPhase2AuthSet cmdlet permanently deletes one or more phase 2 authentication sets from the specified policy store.

This cmdlet gets one or more authorization sets to be deleted with the Name parameter (default), the DisplayName parameter, the Group parameter, or by associated
IPsec rule. The resulting queried set is deleted from the computer.

PARAMETERS

-All [<SwitchParameter>]

Indicates that all of the phase 2 authentication sets within the specified policy store are removed.

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

-AssociatedNetIPsecRule <CimInstance>

Gets the phase 2 authentication sets that are associated, via the pipeline, with the input IPsec rule to be removed. 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

-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

-Description <String[]>

Specifies that matching phase 2 authentication sets of the indicated description are removed. Wildcard characters are accepted. This parameter provides

information about the phase 2 authentication rule. This parameter specifies a localized, user-facing description of the object.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-DisplayGroup <String[]>

Specifies that only matching phase 2 authentication sets of the indicated group association are removed. Wildcard characters are accepted. The Group parameter

specifies the source string for this parameter. If the value for this parameter is a localizable string, then the Group parameter contains an indirect string.

Rule groups can be used to organize rules by influence and allows batch rule modifications. Using the Set-NetIPsecPhase2AuthSet cmdlet, if the group name is

specified for a set of rules, then all of the rules in that group receive the same set of modifications. It is good practice to

specify the Group parameter with a

universal and world-ready indirect @FirewallAPI name. This parameter cannot be specified upon object creation using the New-NetIPsecPhase2AuthSet cmdlet, but

can be modified using dot notation and the Set-NetIPsecPhase2AuthSet cmdlet.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-DisplayName <String[]>

Specifies that only matching phase 2 authentication sets of the indicated display name are removed. Wildcard characters are accepted. This parameter specifies

the localized, user-facing name of the phase 2 authentication set being created. When creating a set this parameter is required. This parameter value is

locale-dependent. If the object is not modified, this parameter value may change in certain circumstances. When writing scripts in multi-lingual environments, the

Name parameter should be used instead, where the default value is a randomly assigned value. This parameter value cannot be All.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-GPOSession <String>

Specifies the network Group Policy Object (GPO) from which to retrieve the sets to be removed. 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

-Group <String[]>

Specifies that only matching phase 2 authentication sets of the indicated group association are removed. Wildcard characters are accepted. This parameter

specifies the source string for the DisplayGroup parameter. If the DisplayGroup parameter value is a localizable string, then this parameter contains an indirect

string. Rule groups organizes rules by influence and allows batch rule modifications. Using the Set-NetIPsecPhase2AuthSet cmdlet, if the group name is specified

for a set of rules, then all of the rules in that group receive the same set of modifications. It is a good practice to specify this parameter with a universal

and world-ready indirect @FirewallAPI name. The DisplayGroup parameter cannot be specified upon object creation using the New-NetIPsecPhase2AuthSet cmdlet, but

can be modified using dot notation and the Set-NetIPsecPhase2AuthSet 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

-Name <String[]>

Specifies that only matching phase 2 authentication sets of the indicated name are removed. 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. Since GPOs can have precedence, if an administrator gives a rule with a different or more specific rule 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 phase 2

encryption are 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

-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 sets to be removed. 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-NetIPsecPhase2AuthSet 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-NetIPsecPhase2AuthSet cmdlet or with the New-NetIPsecPhase2AuthSet

cmdlet.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-PolicyStoreSource <String[]>

Specifies that phase 2 authentication sets that match the indicated policy store source are removed. This parameter contains a path to the policy store where the

rule originated if the object is retrieved from the ActiveStore with the TracePolicyStoreSource option set. This parameter value is automatically generated and

should not be modified. The monitoring output from this parameter is not completely compatible with the PolicyStore parameter. This parameter value cannot always

be passed into the PolicyStore parameter. Domain GPOs are one example in which this parameter contains only the GPO name, not the domain name.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-PolicyStoreSourceType <PolicyStoreType[]>

Specifies that phase 2 authentication sets that match the indicated policy store source type are removed. This parameter describes the type of policy store where

the rule originated if the object is retrieved from the ActiveStore with the TracePolicyStoreSource option set. This parameter value is automatically generated

and should not be modified. The acceptable values for this parameter are:

- Local: The object originates from the local store.

- GroupPolicy: The object originates from a GPO.

- Dynamic: The object originates from the local runtime state.

This policy store name is not valid for use in the cmdlets, but may appear when monitoring active policy. - Generated: The object was generated automatically.

This policy store name is not valid for use in the cmdlets, but may appear when monitoring active policy. - Hardcoded: The object was hard-coded. This policy

store name is not valid for use in the cmdlets, but may appear when monitoring active policy.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-PrimaryStatus <PrimaryStatus[]>

Specifies that phase 2 authentication sets that match the indicated primary status are removed. This parameter

describes the overall status of the rule. - OK:

Specifies that the rule will work as specified.

- Degraded: Specifies that one or more parts of the rule will not be enforced.

- Error: Specifies that the computer is unable to use the rule at all.

See the Status and StatusCode fields of the object for more detailed status information.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Status <String[]>

Specifies that phase 2 authentication sets that match the indicated status are removed. This parameter describes the status message for the specified status code

value. The status code is a numerical value that indicates any syntax, parsing, or run-time errors in the rule. This parameter value should not be modified.

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

-TracePolicyStore [<SwitchParameter>]

Indicates that the phase 2 authentication sets that match the indicated policy store are removed. This parameter specifies that the name of the source GPO is

queried and set to the PolicyStoreSource parameter value.

Required? false

Position? named

Default value False

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_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_NetIKEP2AuthSet[]

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

None

NOTES

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

PS C:\>Remove-NetIPsecPhase2AuthSet

This example removes all of the static local phase 1 authentication sets. This cmdlet is useful for removing any policy that conflicts with the domain GPO.

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

PS C:\>Remove-NetIPsecPhase2AuthSet -DisplayName "Home LAN - Phase 2 Auth Set"

This example deletes a set based on the localized name.

---------- EXAMPLE 3 ----------

PS C:\>$ipsRule = Get-NetIPsecRule -DisplayName "Transport Mode - Extranet IPv4"

PS C:\>Remove-NetIPsecPhase2AuthSet -InputObject $ipsRule

This example removes all of the phase 2 authentication sets that are associated with an IPsec rule.

RELATED LINKS

Online Version:

https://learn.microsoft.com/powershell/module/netsecurity/remove-netipsecphase2authset?view=windowsserver2022-ps&wt.mc_id=ps-gethelp

Get-NetIPsecRule

New-NetIPsecMainModeRule

New-NetIPsecPhase2AuthSet

Open-NetGPO

Save-NetGPO

Set-NetIPsecPhase2AuthSet