Windows PowerShell Get-Help on Cmdlet 'Disable-NetIPsecMainModeRule'

PS:\>Get-HELP Disable-NetIPsecMainModeRule -Full

NAME

Disable-NetIPsecMainModeRule

SYNOPSIS

Disables a main mode rule.

SYNTAX

Disable-NetIPsecMainModeRule [-All] [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-GPOSession <String>] [-PassThru] [-PolicyStore <String>] [-ThrottleLimit

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

Disable-NetIPsecMainModeRule [-AsJob] -AssociatedNetFirewallAddressFilter <CimInstance> [-CimSession <CimSession[]>] [-Confirm] [-GPOSession <String>] [-PassThru]

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

Disable-NetIPsecMainModeRule [-AsJob] -AssociatedNetFirewallProfile <CimInstance> [-CimSession <CimSession[]>] [-Confirm] [-GPOSession <String>] [-PassThru]

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

Disable-NetIPsecMainModeRule [-AsJob] -AssociatedNetIPsecMainModeCryptoSet <CimInstance> [-CimSession <CimSession[]>] [-Confirm] [-GPOSession <String>] [-PassThru]
[-PolicyStore <String>] [-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf] [<CommonParameters>]

Disable-NetIPsecMainModeRule [-AsJob] -AssociatedNetIPsecPhase1AuthSet <CimInstance> [-CimSession <CimSession[]>] [-Confirm] [-GPOSession <String>] [-PassThru]
[-PolicyStore <String>] [-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf] [<CommonParameters>]

Disable-NetIPsecMainModeRule [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-Description <String[]>] [-DisplayGroup <String[]>] [-Enabled {True | False}]
[-GPOSession <String>] [-Group <String[]>] [-MainModeCryptoSet <String[]>] [-PassThru] [-Phase1AuthSet <String[]>] [-PolicyStore <String>] [-PolicyStoreSource
<String[]>] [-PolicyStoreSourceType {None | Local | GroupPolicy | Dynamic | Generated | Hardcoded}] [-PrimaryStatus {Unknown | OK | Inactive | Error}] [-Status
<String[]>] [-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf] [<CommonParameters>]

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

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

Disable-NetIPsecMainModeRule [-AsJob] [-CimSession <CimSession[]>] [-Confirm] -InputObject <CimInstance[]> [-PassThru] [-ThrottleLimit <Int32>] [-WhatIf]
[<CommonParameters>]

DESCRIPTION

The Disable-NetIPsecMainModeRule cmdlet disables a previously enabled main mode rule to be inactive within the computer or a Group Policy organizational unit. A
disabled rule will no actively modify computer behavior, but the rule still exists on the computer or in a Group Policy

Object (GPO) so it can be re-enabled. This is

different from the Remove-NetIPsecMainModeRule cmdlet, which permanently removes the construct from the computer.

This cmdlet gets one or more main mode rules to be disabled with the Name parameter (default), the DisplayName parameter, rule properties, or by associated filters or

objects. The Enabled parameter value for the resulting queried rules is set to False.

Disabling firewall and IPsec rules can be useful for debugging IPsec policy mismatch issues, but it is easier when the rules are in the local, or persistent, store.

Disabling rules in a GPO container will not take effect until the next time the client applies the GPO. To troubleshoot GPO-based IPsec policy, consider copying all

the rules, and authorization and cryptographic sets from the GPO to a computer that does not have the GPO applied using the corresponding Copy-NetIPsecMainModeRule

cmdlet. This is the way to locally modify the policy, in order to troubleshoot any IPsec problems.

PARAMETERS

-All [<SwitchParameter>]

Indicates that all of the main mode rules within the specified policy store are disabled.

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

-AssociatedNetFirewallAddressFilter <CimInstance>

Gets the main mode rules that are associated with the given address filter to be disabled. A NetFirewallAddressFilter object represents the address conditions

associated with a rule. See the Get-NetFirewallAddressFilter cmdlet for more information.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-AssociatedNetFirewallProfile <CimInstance>

Gets the main mode rules that are associated with the given security filter to be disabled. A NetFirewallSecurityFilter object represents the security conditions

associated with a rule. See the Get-NetFirewallSecurityFilter cmdlet for more information. The security conditions include the Authentication , Encryption ,

LocalUser , RemoteUser , and RemoteMachine parameters.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-AssociatedNetIPsecMainModeCryptoSet <CimInstance>

Gets the main mode rules that are associated, via the pipeline, with the input main mode cryptographic set to be disabled. A NetIPsecMainModeCryptoSet object

represents a main mode cryptographic conditions associated with a main mode rule. This parameter sets the methods for the main mode negotiation by describing the

proposals for encryption. See the Get-NetIPsecMainModeCryptoSet cmdlet for more information. Alternatively, the MainModeCryptoSet parameter can be used for the

same purpose, but does not allow the cryptographic set to be piped into this cmdlet and the set must be specified with the Name parameter.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-AssociatedNetIPsecPhase1AuthSet <CimInstance>

Gets the main mode rules that are associated with the given phase 1 authentication set to be disabled. A NetIPsecPhase1AuthSet object represents the phase 1

authorization set conditions associated with an IPsec or main mode rule. This parameter sets the methods for main mode negotiation by describing the proposals for

computer authentication. See the Get-NetIPsecPhase1AuthSet cmdlet for more information. Alternatively, the Phase1AuthSet parameter can be used for the same

purpose, but does not allow the authentication set to be piped into the cmdlet and the set must be specified with the Name parameter.

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 main mode rules of the indicated description are disabled. Wildcard characters are accepted. This parameter provides information about

the firewall rule. This parameter specifies the localized, user-facing description of the IPsec rule.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-DisplayGroup <String[]>

Specifies that only matching main mode rules of the indicated group association are disabled. 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-NetIPsecMainModeRule cmdlet, if the group name is specified for a set of

rules or sets, then all of the rules or sets in that group receive the same set of modifications. It is good practice to

specify the Group parameter value with a

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

be modified using dot-notation and the Set-NetIPsecMainModeRule cmdlet.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-DisplayName <String[]>

Specifies that only matching main mode rules of the indicated display name are disabled. Wildcard characters are accepted. Specifies the localized, user-facing

name of the firewall rule being created. When creating a rule 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 cannot be set to All.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Enabled <Enabled[]>

Specifies that matching main mode rules of the indicated state are disabled. This parameter specifies that the rule object is administratively enabled or

administratively disabled. The acceptable values for this parameter are: - True: Specifies the rule is currently enabled.

- False: Specifies the rule is currently disabled.

A disabled rule will not actively modify computer behavior, but the management construct still exists on the computer so it can be re-enabled.

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 disabled. 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 main mode rules of the indicated group association are disabled. 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 can be used to organize rules by influence and allows batch rule modifications. Using the Set-NetIPsecMainModeRule cmdlets, if the group name is specified

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

value with a universal and world-ready indirect @FirewallAPI name. The DisplayGroup parameter cannot be specified upon object creation using the

New-NetIPsecMainModeRule cmdlet, but can be modified using dot-notation and the Set-NetIPsecMainModeRule 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

-MainModeCryptoSet <String[]>

Specifies the main mode rules that are associated with the given main mode cryptographic set to be disabled. Specifies, by Name, the main mode cryptographic set

to be associated with the main mode rule. A NetIPsecMainModeCryptoSet object represents a main mode cryptographic conditions associated with a main mode rule.

This parameter sets the methods for main mode negotiation by describing the proposals for encryption. This is only associated with main mode rules. See the

Get-NetIPsecMainModeCryptoSet cmdlet for more information. Alternatively, the AssociatedNetIPsecMainModeCryptoSet parameter can be used for the same purpose, but

is used to pipe the input set into the rule. When specifying cryptographic sets, the Name parameter value of the cryptographic set must be used. The object

cannot be directly passed into the cmdlet.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Name <String[]>

Specifies that only matching main mode rules of the indicated name are disabled. 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, 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

-Phase1AuthSet <String[]>

Specifies the main mode rules that are associated with the given phase 1 authentication set to be disabled. This parameter specifies, by Name, the Phase 1

authentication set to be associated with the main mode rule. A NetIPsecPhase1AuthSet object represents the phase 1 authentication conditions associated with an

IPsec or main mode rule. This parameter sets the methods for main mode negotiation by describing the proposals for computer authentication. See the

New-NetIPsecAuthProposal cmdlet of more information. Alternatively, the AssociatedNetIPsecPhase1AuthSet parameter can be used for the same purpose, but is used to

pipe the input set into the rule.

Required? false

Position? named

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 disabled. 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.

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-NetIPsecMainModeRule 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-NetIPsecMainModeRule

cmdlet or with the New-NetIPsecMainModeRule cmdlet.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-PolicyStoreSource <String[]>

Specifies that main mode rules that match the indicated policy store source are disabled. 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 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 main mode rules that match the indicated primary status are disabled. 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 main mode rules that match the indicated status are disabled. 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 runtime 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 main mode rules that match the indicated policy store are disabled. 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\AssociatedNetIPsecMainModeCryptoSet

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_NetIKEP1AuthSet

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_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.

NOTES

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

PS C:\>Disable-NetIPsecMainModeRule -DisplayName "Main Mode Rule" -PolicyStore domain.contoso.com\gpo

This example disables a main mode rule in a GPO given the localized name.

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

PS C:\>Disable-NetIPsecMainModeRule -Group "DA Client" -PolicyStore ActiveStore

This example disables all of the main mode client DA rules on a local computer.

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

PS C:\>$phase1AuthSet = Get-NetIPsecPhase1AuthSet -DisplayName "Computer Kerb, CA Auth"

PS C:\>Disable-NetIPsecMainModeRule -InputObject $phase1AuthSet

This example disables the main mode rules associated with the specified phase 1 authentication set.

RELATED LINKS

Online Version:

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

Copy-NetIPsecMainModeRule

Get-NetFirewallAddressFilter

Get-NetFirewallSecurityFilter

Get-NetIPsecMainModeCryptoSet

Get-NetIPsecPhase1AuthSet

New-NetIPsecMainModeRule

Open-NetGPO

Remove-NetIPsecMainModeRule

Save-NetGPO

Set-NetIPsecMainModeRule

New-NetIPsecAuthProposal