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

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

NAME

Set-NetIPsecMainModeRule

SYNOPSIS

Modifies existing main mode rules.

SYNTAX

Set-NetIPsecMainModeRule [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-Description <String>] -DisplayGroup <String[]> [-Enabled {True | False}] [-GPOSession

<String>] [-LocalAddress <String[]>] [-MainModeCryptoSet <String>] [-NewDisplayName <String>] [-PassThru] [-Phase1AuthSet <String>] [-Platform <String[]>]

[-PolicyStore <String>] [-Profile {Any | Domain | Private | Public | NotApplicable}] [-RemoteAddress <String[]>] [-ThrottleLimit <Int32>] [-WhatIf]

[<CommonParameters>]

Set-NetIPsecMainModeRule [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-Description <String>] -DisplayName <String[]> [-Enabled {True | False}] [-GPOSession

<String>] [-LocalAddress <String[]>] [-MainModeCryptoSet <String>] [-NewDisplayName <String>] [-PassThru] [-Phase1AuthSet <String>] [-Platform <String[]>]

[-PolicyStore <String>] [-Profile {Any | Domain | Private | Public | NotApplicable}] [-RemoteAddress <String[]>] [-ThrottleLimit <Int32>] [-WhatIf]

[<CommonParameters>]

Set-NetIPsecMainModeRule [-Name] <String[]> [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-Description <String>] [-Enabled {True | False}] [-GPOSession <String>]

[-LocalAddress <String[]>] [-MainModeCryptoSet <String>] [-NewDisplayName <String>] [-PassThru] [-Phase1AuthSet <String>] [-Platform <String[]>] [-PolicyStore

<String>] [-Profile {Any | Domain | Private | Public | NotApplicable}] [-RemoteAddress <String[]>] [-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]

Set-NetIPsecMainModeRule [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-Description <String>] [-Enabled {True | False}] [-GPOSession <String>] -Group <String[]>

[-LocalAddress <String[]>] [-MainModeCryptoSet <String>] [-NewDisplayName <String>] [-PassThru] [-Phase1AuthSet <String>] [-Platform <String[]>] [-PolicyStore

<String>] [-Profile {Any | Domain | Private | Public | NotApplicable}] [-RemoteAddress <String[]>] [-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]

Set-NetIPsecMainModeRule [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-Description <String>] [-Enabled {True | False}] -InputObject <CimInstance[]>

[-LocalAddress <String[]>] [-MainModeCryptoSet <String>] [-NewDisplayName <String>] [-PassThru] [-Phase1AuthSet <String>] [-Platform <String[]>] [-Profile {Any |

Domain | Private | Public | NotApplicable}] [-RemoteAddress <String[]>] [-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Set-NetIPsecMainModeRule cmdlet modifies firewall properties of existing main mode rules. This cmdlet gets one or more main mode rules to be modified with the

Name parameter (default), the DisplayName parameter, or by group association using the DisplayGroup or Group parameters. The rules cannot be queried by property in

this cmdlet. The Get-NetIPsecMainModeRule cmdlet returns the queried objects and pipes the objects into this cmdlet. The remaining parameters specify the properties

of the rule to be modified. When the DisplayGroup or Group parameter is specified, then all of the sets associated with the group receive the same modifications. The

rule parameters modified using the dot-notation are committed using this cmdlet.

To move a rule to a new GPO, copy the existing rule by running the Copy-NetIPsecMainModeRule cmdlet with the NewPolicyStore parameter, then removing the old rule with

the Remove-NetIPsecMainModeRule cmdlet.

Modifying authentication or cryptographic configurations to use the default settings including NetIPsecPhase1AuthSet, NetIPsecMainModeCryptoSet, or with Default flag

enabled must be done by using dot-notation

PARAMETERS

-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

-Description <String>

Specifies that matching main mode rules of the indicated description are modified. Wildcard characters are accepted. This parameter provides information about

the main mode 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 modified. 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 this 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. parameter cannot be specified upon object creation using the

New-NetIPsecMainModeRule cmdlet, but can be modified using

dot-notation and this cmdlet.

Required? true

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 modified. Wildcard characters are accepted. Specifies the localized, user-facing

name of the main mode 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 modified. This parameter specifies that the rule object is administratively enabled or

administratively enabled. 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 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

-Group <String[]>

Specifies that only matching main mode rules of the indicated group association are modified. 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 this 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 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 this cmdlet.

Required? true

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

-LocalAddress <String[]>

Specifies that network packets with matching IP addresses match this rule. This parameter value is the first end point of an IPsec rule and specifies the

computers that are subject to the requirements of this rule. This parameter value is an IPv4 or IPv6 address, hostname, subnet, range, or the following keyword:

Any. The acceptable formats for this parameter are: - Single IPv4 Address: 1.2.3.4

- Single IPv6 Address: fe80::1

- IPv4 Subnet (by network bit count): 1.2.3.4/24

- IPv6 Subnet (by network bit count): fe80::1/48

- IPv4 Subnet (by network mask): 1.2.3.4/255.255.255.0

- IPv4 Range: 1.2.3.4 through 1.2.3.7

- IPv6 Range: fe80::1 through fe80::9

Querying for rules with this parameter can only be performed using filter objects. See the Get-NetFirewallAddressFilter cmdlet for more information.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-MainModeCryptoSet <String>

Gets the IPsec main mode rules that are associated with the given main mode cryptographic set to be modified. 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.

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 modified. 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 the same name in a higher-precedence GPO,

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

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

-NewDisplayName <String>

Specifies the new display name for an IPsec rule.

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

-Phase1AuthSet <String>

Gets the main mode rules that are associated with the given phase 1 authentication set to be modified. 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

-Platform <String[]>

Specifies which version of Windows the associated rule applies. The acceptable format for this parameter is a number in the Major.Minor format. The version

number of 6.0 corresponds to Vista (nextref_vista), 6.1 corresponds to Win7 (Windowsr 7 or firstref_longhorn), and 6.2 corresponds to Win8 (Windowsr 8 or Windows

Server 2012). If + is not specified, then only that version is associated. If + is specified, then that version and later are associated. Querying for rules

with this parameter with the Get-NetIPsecMainModeRule cmdlet cannot be performed.

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 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 system 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 main mode 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. This 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

-Profile <Profile>

Specifies one or more profiles to which the rule is assigned. The rule is active on the local computer only when the specified profile is currently active. This

relationship is many-to-many and can be indirectly modified by the user, by changing the Profiles field on instances of firewall rules. Only one profile is

applied at a time. The acceptable values for this parameter are: Any, Domain, Private, Public, or NotApplicable. The default value is Any. Separate multiple

entries with a comma and do not include any spaces. Use the keyword Any to configure the profile as Private, Public,

Domain in the ConfigurableServiceStore.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RemoteAddress <String[]>

Specifies that network packets with matching IP addresses match this rule. This parameter value is the second end point of an IPsec rule and specifies the

computers that are subject to the requirements of this rule. This parameter value is an IPv4 or IPv6 address, hostname, subnet, range, or the following keyword:

Any. The acceptable formats for this parameter are: - Single IPv4 Address: 1.2.3.4

- Single IPv6 Address: fe80::1

- IPv4 Subnet (by network bit count): 1.2.3.4/24

- IPv6 Subnet (by network bit count): fe80::1/48

- IPv4 Subnet (by network mask): 1.2.3.4/255.255.255.0

- IPv4 Range: 1.2.3.4 through 1.2.3.7

- IPv6 Range: fe80::1 through fe80::9

Querying for rules with this parameter can only be performed using filter objects. See the Get-NetFirewallAddressFilter cmdlet for more information.

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_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:\>$EncAES128 = New-NetIPsecMainModeCryptoProposal -Encryption AES128

PS C:\>$EncDES3 = New-NetIPsecMainModeCryptoProposal -Encryption DES3

PS C:\>$cryptoset = New-NetIPsecMainModeCryptoSet -DisplayName "(DA Client) - Phase 2 Crypto Set" -Proposals $EncAES128,$EncDES3

PS C:\>Set-NetIPsecMainModeRule -DisplayName MainModeRule -MainModeCryptoSet $cryptoset

This example replaces the proposals for an existing main mode rule.

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

PS C:\>Set-NetIPsecMainModeRule -DisplayGroup "DA Client" -Enabled True

PS C:\>Enable-NetIPsecMainModeRule -DisplayGroup "DA Client"

This example shows two ways to enable all of the main mode rules in a predefined group.

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

PS C:\>Set-NetFirewallRule -DisplayName "Tunnel Mode - (DA Client)" -NewDisplayName "Tunnel Mode - Americas (DA Client)"

This example changes the display name for a main mode rule

---------- EXAMPLE 4 ----------

PS C:\>$rule = Get-NetIPsecMainModeRule -DisplayName "Tunnel Mode - (DA Client)"

PS C:\>$rule.MainModeModeCryptoSet = "Default"

PS C:\>Set-NetIPsecMainModeRule -InputObject $rule

This example modifies a main mode rule to use the default encryption method for main mode if a custom one has been previously set to the rule.

RELATED LINKS

Online Version:

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

Copy-NetIPsecMainModeRule

Enable-NetIPsecMainModeRule

Get-NetFirewallAddressFilter

Get-NetIPsecMainModeRule

Open-NetGPO

Remove-NetIPsecMainModeRule

Save-NetGPO

New-NetIPsecAuthProposal