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 'Rename-NetIPsecQuickModeCryptoSet'

PS:\>Get-HELP Rename-NetIPsecQuickModeCryptoSet -Full

NAME

Rename-NetIPsecQuickModeCryptoSet

SYNOPSIS

Renames a single quick mode cryptographic set.

SYNTAX

Rename-NetIPsecQuickModeCryptoSet [-All] [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-GPOSession <String>] -NewName <String> [-PassThru] [-PolicyStore <String>] [-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf] [<CommonParameters>]

Rename-NetIPsecQuickModeCryptoSet [-AsJob] -AssociatedNetIPsecRule <CimInstance> [-CimSession <CimSession[]>] [-Confirm] [-GPOSession <String>] -NewName <String> [-PassThru] [-PolicyStore <String>] [-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf] [<CommonParameters>]

Rename-NetIPsecQuickModeCryptoSet [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-Description <String[]>] [-DisplayGroup <String[]>] [-GPOSession <String>] [-Group <String[]>] -NewName <String> [-PassThru] [-PerfectForwardSecrecyGroup {None | DH1 | DH2 | DH14 | DH19 | DH20 | DH24 | SameAsMainMode}] [-PolicyStore <String>]

[-PolicyStoreSource <String[]>] [-PolicyStoreSourceType {None | Local | GroupPolicy | Dynamic | Generated | Hardcoded}] [-PrimaryStatus {Unknown | OK | Inactive |

Error}] [-Status <String[]>] [-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf] [<CommonParameters>]

Rename-NetIPsecQuickModeCryptoSet [-AsJob] [-CimSession <CimSession[]>] [-Confirm] -DisplayName <String[]> [-GPOSession <String>] -NewName <String> [-PassThru]

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

Rename-NetIPsecQuickModeCryptoSet [-Name] <String[]> [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-GPOSession <String>] -NewName <String> [-PassThru]

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

Rename-NetIPsecQuickModeCryptoSet [-AsJob] [-CimSession <CimSession[]>] [-Confirm] -InputObject <CimInstance[]> -NewName <String> [-PassThru] [-ThrottleLimit <Int32>]

[-WhatIf] [<CommonParameters>]

DESCRIPTION

The Rename-NetIPsecQuickModeCryptoSet cmdlet renames an existing quick mode cryptographic set. When creating a set, if the Name parameter is not specified, then a

randomly generated value is used. This cmdlet specifies a friendly and descriptive rule name. Only one set can be renamed at a time when copying to the same policy

store. This is because only a single set can use the unique identifier, or name, specified by the NewName parameter.

To modify the localized DisplayName parameter, run the Set-NetIPsecQuickModeCryptoSet cmdlet with the NewDisplayName parameter.

The names are unique identifiers for rules, similar to file names. Each name must be unique within a given policy store. If the rules in multiple Group Policy Objects

(GPO) have the same name, then one will overwrite the other based upon GPO precedence. If a rule from a GPO has the same name as a rule from the PersistentStore, then

the rule from the GPO will overwrite the local rule.

To specify a new default quick mode cryptographic set, run this cmdlet to specify the default set with the Name parameter value set to

{E5A5D32A-4BCE-4e4d-B07F-4AB1BA7E5FE1}.

PARAMETERS

-All [<SwitchParameter>]

Indicates that all of the quick mode cryptographic sets within the specified policy store are renamed.

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 quick mode cryptographic sets that are associated, via the pipeline, with the input IPsec rule to be renamed. 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 quick mode cryptographic sets of the indicated description are renamed. Wildcard characters are accepted. This parameter provides information about the quick mode cryptographic sets. 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 quick mode cryptographic sets of the indicated group association are renamed. 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-NetIPsecQuickModeCryptoSet 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-NetIPsecQuickModeCryptoSet cmdlet,

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

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-DisplayName <String[]>

Specifies that only matching quick mode cryptographic sets of the indicated display name are renamed. Wildcard characters are accepted. This parameter specifies

the localized, user-facing name of the quick mode cryptographic 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 GPO from which to retrieve the sets to be renamed. This parameter is used in the same way as the PolicyStore parameter. When you modify a

GPO 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 quick mode cryptographic sets of the indicated group association are renamed. 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-NetIPsecQuickModeCryptoSet 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 this parameter with a

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

New-NetIPsecQuickModeCryptoSet cmdlet, but can be modified using dot notation and the Set-NetIPsecQuickModeCryptoSet 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 quick mode cryptographic sets of the indicated name are renamed. Wildcard characters are accepted. This parameter acts just like a

filename, 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 that 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 quick mode 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

-NewName <String>

Specifies the new name for one or more quick mode cryptographic sets.

Required? true

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

-PerfectForwardSecrecyGroup <DiffieHellmanGroup[]>

Specifies that matching main mode cryptographic sets of the indicated Diffie-Hellman group are renamed. This parameter specifies the Diffie-Hellman group to use

for session key perfect forward secrecy. The acceptable values for this parameter are: None, DH1, DH2, DH14, DH19, DH20, DH24, or SameAsMainMode. The default

value is None.

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 sets to be renamed. 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-NetIPsecQuickModeCryptoSet 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-NetIPsecQuickModeCryptoSet cmdlet or with the

New-NetIPsecQuickModeCryptoSet cmdlet.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-PolicyStoreSource <String[]>

Specifies that quick mode cryptographic sets that match the indicated policy store source are renamed. 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 quick mode cryptographic sets that match the indicated policy store source type are renamed. 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 quick mode cryptographic sets that match the indicated primary status are renamed. 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 quick mode cryptographic sets that match the indicated status are renamed. 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 quick mode cryptographic sets that match the indicated policy store are renamed. 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_NetIKEQMCryptoSet[]

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:\>Rename-NetIPsecQuickModeCryptoSet -Name "{ed8384a9-a78b-4d0d-8f3d-eb5615edb4a0}" -NewName "Exchange HIPAA Server, Any <-> 80 - Phase 2 Crypto Set"

This example renames a quick mode cryptographic set so that the unique identifier is descriptive and user friendly.

RELATED LINKS

Online Version:

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

Copy-NetIPsecQuickModeCryptoSet

Get-NetIPsecRule

New-NetIPsecMainModeRule

New-NetIPsecQuickModeCryptoSet

Open-NetGPO

Remove-NetIPsecQuickModeCryptoSet

Save-NetGPO

Set-NetIPsecQuickModeCryptoSet