## PowerShell Get-Help on command 'Copy-NetIPsecQuickModeCryptoSet'

*PS C:\Users\wahid> Get-Help Copy-NetIPsecQuickModeCryptoSet*

NAME

    Copy-NetIPsecQuickModeCryptoSet

SYNOPSIS

    Copies an entire quick mode cryptographic set to the same or to a different

    policy store.

SYNTAX

    Copy-NetIPsecQuickModeCryptoSet [-All] [-AsJob] [-CimSession <CimSession[]>]

    [-Confirm] [-GPOSession <String>] [-NewGPOSession <String>] [-NewName

    <String>] [-NewPolicyStore <String>] [-PassThru] [-PolicyStore <String>]

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


    Copy-NetIPsecQuickModeCryptoSet [-AsJob] -AssociatedNetIPsecRule <CimInstance>

    [-CimSession <CimSession[]>] [-Confirm] [-GPOSession <String>] [-NewGPOSession

    <String>] [-NewName <String>] [-NewPolicyStore <String>] [-PassThru]

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

    [<CommonParameters>]


    Copy-NetIPsecQuickModeCryptoSet [-AsJob] [-CimSession <CimSession[]>]

[-Confirm] [-Description <String[]>] [-DisplayGroup <String[]>] [-GPOSession <String>] [-Group <String[]>] [-NewGPOSession <String>] [-NewName <String>] [-NewPolicyStore <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>]


Copy-NetIPsecQuickModeCryptoSet [-AsJob] [-CimSession <CimSession[]>] [-Confirm] -DisplayName <String[]> [-GPOSession <String>] [-NewGPOSession <String>] [-NewName <String>] [-NewPolicyStore <String>] [-PassThru] [-PolicyStore <String>] [-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf] [<CommonParameters>]


Copy-NetIPsecQuickModeCryptoSet [-Name] <String[]> [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-GPOSession <String>] [-NewGPOSession <String>] [-NewName <String>] [-NewPolicyStore <String>] [-PassThru] [-PolicyStore <String>] [-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf] [<CommonParameters>]


Copy-NetIPsecQuickModeCryptoSet [-AsJob] [-CimSession <CimSession[]>] [-Confirm] -InputObject <CimInstance[]> [-NewGPOSession <String>] [-NewName <String>] [-NewPolicyStore <String>] [-PassThru] [-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]


DESCRIPTION

The Copy-NetIPsecQuickModeCryptoSet cmdlet copies a main mode cryptographic set, making a complete clone, to a policy store. When a new policy store is not specified, it is copied to the same policy store with a new name specified by the user.

This cmdlet gets one or more cryptographic sets to be duplicated with the Name parameter (default), the DisplayName parameter, set properties, or by the associated filters or objects. The resulting queried set is copied to a new policy store using the NewPolicyStore parameter, a new GPO session using the NewGPOSession parameter, or to the same policy store using the NewName . Only one quick mode cryptographic set can be copied at a time when copying to the same policy store. This is because only a single cryptographic set can use the unique identifier, or name specified by the NewName parameter.

When copying a set to a new policy store, the unique name of the set is preserved. This means that if the same set is attempted to be copied twice, then an error is displayed for the second attempt indicating that the object already exists. To overwrite the target set, run the Remove-NetIPsecQuickModeCryptoSet cmdlet first. If it is possible that the object may already exist, then specify the ErrorAction parameter to silently ignore these errors, instead of running the Remove-NetIPsecQuickModeCryptoSet cmdlet.

PARAMETERS

-All [<SwitchParameter>]

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

-AsJob [<SwitchParameter>]

Runs the cmdlet as a background job. Use this parameter to run commands that take a long time to complete.

-AssociatedNetIPsecRule <CimInstance>

Gets the quick mode cryptographic sets that are associated, via the pipeline, with the input IPsec rule to be copied.  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.

-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.

-Confirm [<SwitchParameter>]

Prompts you for confirmation before running the cmdlet.

-Description <String[]>

Specifies that matching quick mode cryptographic sets of the indicated

description are copied. 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.

-DisplayGroup <String[]>

Specifies that only matching quick mode cryptographic sets of the

indicated group association are copied. 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.

-DisplayName <String[]>

   Specifies that only matching quick mode cryptographic sets of the

   indicated display name are copied. 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.


-GPOSession <String>

   Specifies the network GPO from which to retrieve the sets to be copied.

   This parameter is used in the same way as the PolicyStore parameter. When

   modifying Group Policy Objects (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.


-Group <String[]>

   Specifies that only matching quick mode cryptographic sets of the

   indicated group association are copied. 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 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-NetIPsecQuickModeCryptoSet cmdlet, but can be modified using dot-notation and the Set-NetIPsecQuickModeCryptoSet cmdlet.

-InputObject <CimInstance[]>

Specifies the input object that is used in a pipeline command.

-Name <String[]>

Specifies that only matching quick mode cryptographic sets of the indicated name are copied. 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 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.

-NewGPOSession <String>

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

-NewName <String>

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

-NewPolicyStore <String>

  Specifies the policy store for one or more quick mode cryptographic sets.


-PassThru [<SwitchParameter>]

  Returns an object representing the item with which you are working. By

  default, this cmdlet does not generate any output.


-PerfectForwardSecrecyGroup <DiffieHellmanGroup[]>

  Specifies that matching main mode cryptographic sets of the indicated

  Diffie-Hellman group are copied.  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.


-PolicyStore <String>

  Specifies the policy store from which to retrieve the sets to be copied.

  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
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 this cmdlet or with the New-NetIPsecQuickModeCryptoSet cmdlet.

-PolicyStoreSource <String[]>
Specifies that quick mode cryptographic sets that match the indicated

policy store source are copied.  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.

-PolicyStoreSourceType <PolicyStoreType[]>

Specifies that quick mode cryptographic sets that match the indicated

policy store source type are copied.  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 cmdlets, but may appear

when monitoring active policy.  - Generated: The object was generated

automatically. This policy store name is not valid for use in cmdlets, but

may appear when monitoring active policy.  - Hardcoded: The object was

hard-coded. This policy store name is not valid for use in cmdlets, but

may appear when monitoring active policy.

-PrimaryStatus <PrimaryStatus[]>

Specifies that quick mode cryptographic sets that match the indicated

primary status are copied.  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.

-Status <String[]>

Specifies that quick mode cryptographic sets that match the indicated status are copied.  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.

-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.

-TracePolicyStore [<SwitchParameter>]

Indicates that the quick mode cryptographic sets that match the indicated policy store are copied.  This parameter specifies that the name of the source GPO is queried and set to the PolicyStoreSource parameter value.

-WhatIf [<SwitchParameter>]

   Shows what would happen if the cmdlet runs. The cmdlet is not run.


<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).


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


PS C:\>Copy-NetIPsecQuickModeCryptoSet -DisplayName "Quick Mode Crypto Set"

-NewName "Alternate Quick Mode Crypto Set"


This example copies a quick mode cryptographic set, found by specifying the

localized name, to the current policy store under a new unique identifier.
-------------------------- EXAMPLE 2 --------------------------


PS C:\>$iPsecRule = Get-NetIPsecRule -DisplayName "IPsec Rule: P2Auth +

Crypto" -PolicyStore domain.contoso.com\GPO_name




PS C:\>Copy-NetIPsecPhase1AuthSet -ImportObject $iPsecRule -NewPolicyStore

domain.contoso.com\new_GPO




PS C:\>Copy-NetIPsecPhase2AuthSet -ImportObject $iPsecRule -NewPolicyStore

domain.contoso.com\new_GPO

```
PS C:\>Copy-NetIPsecQuickModeCryptoSet -ImportObject $iPsecRule
-NewPolicyStore domain.contoso.com\new_GPO
```

```
PS C:\>Copy-NetIPsecRule -ImportObject $iPsecRule -NewPolicyStore
domain.contoso.com\new_GPO
```

This accomplishes the same task but takes advantage of caching the GPO to
apply the changes locally.

```
PS C:\>$iPsecRule = Get-NetIPsecRule -DisplayName "IPsec Rule: P2Auth +
Crypto" -PolicyStore domain.contoso.com\GPO_name
```

```
PS C:\>$newGPO = Open-NetGPO -PolicyStore domain.contoso.com\new_GPO
```

```
PS C:\>Copy-NetIPsecPhase1AuthSet -ImportObject $iPsecRule -GPOSession $newGPO
```

```
PS C:\>Copy-NetIPsecPhase2AuthSet -ImportObject $iPsecRule -GPOSession $newGPO
```

```
PS C:\>Copy-NetIPsecQuickModeCryptoSet -ImportObject $iPsecRule -GPOSession
$newGPO
```

```
PS C:\>Copy-NetIPsecRule -ImportObject $iPsecRule -GPOSession $newGPO
```

```
PS C:\>Save-NetGPO -GPOSession $newGPO
```

This example copies an entire IPsec rule and the associated cryptographic sets to a new policy store separately. There is no need to link the newly copied sets to the newly copied rule since the set fields of the rules maintain the Name parameter value of the source.

REMARKS

To see the examples, type: "get-help Copy-NetIPsecQuickModeCryptoSet -examples".

For more information, type: "get-help Copy-NetIPsecQuickModeCryptoSet -detailed".

For technical information, type: "get-help Copy-NetIPsecQuickModeCryptoSet -full".

For online help, type: "get-help Copy-NetIPsecQuickModeCryptoSet -online"