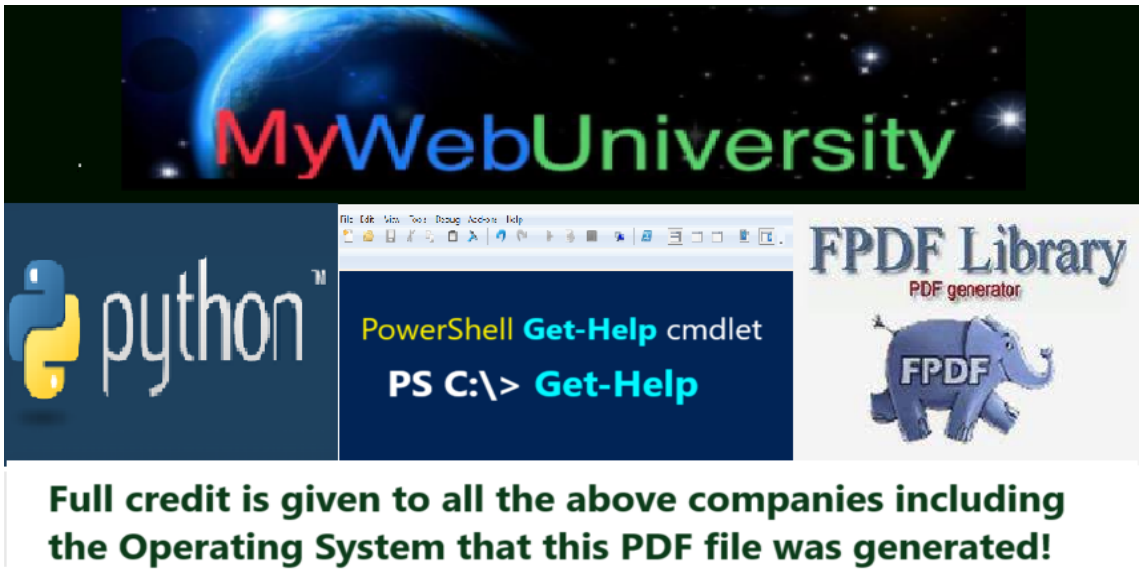

Windows PowerShell Get-Help on Cmdlet 'Set-NetIPsecMainModeCryptoSet'

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

NAME

Set-NetIPsecMainModeCryptoSet

SYNOPSIS

Modifies existing main mode cryptographic sets.

SYNTAX

Set-NetIPsecMainModeCryptoSet [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-Description <String>] -DisplayGroup <String[]> [-ForceDiffieHellman <Boolean>]

[-GPOSession <String>] [-MaxMinutes <UInt32>] [-MaxSessions <UInt32>] [-NewDisplayName <String>] [-PassThru] [-PolicyStore <String>] [-Proposal <CimInstance[]>]

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

Set-NetIPsecMainModeCryptoSet [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-Description <String>] -DisplayName <String[]> [-ForceDiffieHellman <Boolean>]

[-GPOSession <String>] [-MaxMinutes <UInt32>] [-MaxSessions <UInt32>] [-NewDisplayName <String>] [-PassThru] [-PolicyStore <String>] [-Proposal <CimInstance[]>]

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

Set-NetIPsecMainModeCryptoSet [-Name] <String[]> [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-Description <String>] [-ForceDiffieHellman <Boolean>] [-GPOSession

<String>] [-MaxMinutes <UInt32>] [-MaxSessions <UInt32>] [-NewDisplayName <String>] [-PassThru] [-PolicyStore <String>] [-Proposal <CimInstance[]>] [-ThrottleLimit

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

Set-NetIPsecMainModeCryptoSet [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-Description <String>] [-ForceDiffieHellman <Boolean>] [-GPOSession <String>] -Group

<String[]> [-MaxMinutes <UInt32>] [-MaxSessions <UInt32>] [-NewDisplayName <String>] [-PassThru] [-PolicyStore <String>] [-Proposal <CimInstance[]>] [-ThrottleLimit

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

Set-NetIPsecMainModeCryptoSet [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-Description <String>] [-ForceDiffieHellman <Boolean>] -InputObject <CimInstance[]>

[-MaxMinutes <UInt32>] [-MaxSessions <UInt32>] [-NewDisplayName <String>] [-PassThru] [-Proposal <CimInstance[]>] [-ThrottleLimit <Int32>] [-WhatIf]

[<CommonParameters>]

DESCRIPTION

The Set-NetIPsecMainModeCryptoSet cmdlet modifies cryptographic properties for existing main mode cryptographic sets.

This cmdlet gets one or more main mode cryptographic sets to be modified with the Name (default), DisplayName , or by group association using the Group or

DisplayGroup parameter. The sets cannot be queried by property in this cmdlet. The querying can be done by running the Get-NetIPsecMainModeCryptoSet cmdlet, The

Get-NetIPsecMainModeCryptoSet cmdlet returns the cryptographic sets and pipes the sets into this cmdlet, which modifies the sets. The remaining parameters specify the

properties of the set to be modified. When a group is specified, all of the sets associated with the group receive the same modifications. Rule fields are modified

using the dot notation are committed with this cmdlet.

To move a set to a new GPO, copy the existing set by running the Copy-NetIPsecMainModeCryptoSet cmdlet with the NewPolicyStore parameter, then remove the old set by

running the Remove-NetIPsecMainModeCryptoSet cmdlet.

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 cryptographic sets of the indicated description are modified. Wildcard characters are accepted. This parameter provides

information about the main 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 main mode cryptographic sets 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 with a universal

and world-ready indirect @FirewallAPI name. This parameter cannot be specified upon object creation using the New-NetIPsecMainModeCryptoSet 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 cryptographic sets of the indicated display name are modified. Wildcard characters are accepted. This parameter specifies

the localized, user-facing name of a single main mode cryptographic sets. 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 resilient scripts, 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

-ForceDiffieHellman <Boolean>

Indicates that matching main mode cryptographic sets of the indicated value are modified. If this parameter is set to True, then IPsec uses Diffie-Hellman

exchanges to protect the main mode key exchange when AuthIP is used. AuthIP is specified by KeyModule. This provides stronger security for the key exchange. The

default value is False.

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 sets to be modified. 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.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Group <String[]>

Specifies that only matching main mode cryptographic sets 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 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 this parameter with a universal and world-ready

indirect @FirewallAPI name. The DisplayGroup parameter cannot be specified upon object creation using the New-NetIPsecMainModeCryptoSet 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

-MaxMinutes <UInt32>

Specifies that matching main mode cryptographic sets of the indicated maximum lifetime, in minutes, are modified. This parameter specifies the number of minutes

established for a main mode security association before it expires and must be renegotiated. The acceptable values for this parameter are: 0 through 2879.

- A non-zero value specifies the desired minute lifetime.

- NotConfigured: Valid only when configuring a GPO.

Removes the setting from the GPO, which results in the policy not changing the value on the computer when the policy is applied.

The default value is 480 minutes (eight hours). When managing a GPO, the default setting is NotConfigured.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-MaxSessions <UInt32>

Specifies that matching main mode cryptographic sets of the indicated maximum lifetime, in sessions, are modified. This parameter specifies the number of

sessions established for a main mode security association before it expires and must be renegotiated. The acceptable values for this parameter are: 0 through

2147483647.

- A value of zero (0) specifies that there should be no maximum session lifetime.

- A non-zero value specifies the desired session number.

- NotConfigured: Valid only when configuring a GPO.

Removes the setting from the GPO, which results in the policy not changing the value on the computer when the policy is applied.

The default value is zero (0) sessions. When managing a GPO, the default setting is NotConfigured.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Name <String[]>

Specifies that only matching main mode cryptographic sets 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, 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 a main mode cryptographic set.

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

-PolicyStore <String>

Specifies the policy store from which to retrieve the sets 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 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. 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-NetIPsecMainModeCryptoSet cmdlet or with the New-NetIPsecMainModeCryptoSet cmdlet.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Proposal <CimInstance[]>

Associates the specified cryptographic proposal to the corresponding cryptographic set to be used in main mode negotiations. Separate multiple entries with a

comma.

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\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.

OUTPUTS

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.

NOTES

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

PS C:\>$EncAES128 = New-NetIPsecMainModeCryptoProposal -Encryption AES128

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

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

This example replaces the proposals of an existing main mode cryptographic set.

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

PS C:\>Set-NetIPsecMainModeCryptoSet -DisplayGroup "DA Client" -MaxMinutes 240

This example modifies the maximum amount of time the security association is active for a group of main mode cryptographic sets.

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

PS C:\>$proposal1 = New-NetIPsecMainModeCryptoProposal -KeyExchange DH1

PS C:\>$proposal2 = New-NetIPsecMainModeCryptoProposal -KeyExchange DH14

PS C:\>$cryptoset1 = (New-NetIPsecMainModeCryptoSet -DisplayName MainModeCryptoSet -Proposal $proposal1.Name, $proposal2.Name)

PS C:\>$mainModeRule = New-NetIPsecMainModeRule -DisplayName MainModeRule -MainModeCryptoSet $cryptoset1

PS C:\>$mainModeCryptoSet = ($mainModeRule | Get-NetIPsecMainModeCryptoSet)

PS C:\>$mainModeCryptoSet.Proposal[1] = DH19

PS C:\>Set-NetIPsecMainModeCryptoSet -InputObject $mainModeCryptoSet

This version of the cmdlet shows an alternative method to the previous example. The main mode rule setup is the same.

PS C:\>$mainModeRule = New-NetIPsecMainModeRule -DisplayName MainModeRule -MainModeCryptoSet (New-NetIPsecMainModeCryptoSet -DisplayName MainModeCryptoSet -Proposal

(New-NetIPsecMainModeCryptoProposal -KeyExchange DH1),(New-NetIPsecMainModeCryptoProposal -KeyExchange DH14)).Name

PS C:\>$mainModeCryptoSet = ($mainModeRule | Get-NetIPsecMainModeCryptoSet)

PS C:\>$mainModeCryptoSet | Set-NetIPsecMainModeCryptoSet -Proposal (New-NetIPsecMainModeCryptoProposal -KeyExchange DH1), (New-NetIPsecMainModeCryptoProposal
-KeyExchange DH19)

This example shows how to replace a key exchange option of a main mode cryptographic proposal to an existing main mode cryptographic set, given the associated main
mode rule. The key exchange is changed for the second specified cryptographic proposal.

RELATED LINKS

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

Copy-NetIPsecMainModeCryptoSet

Get-NetIPsecMainModeCryptoSet

New-NetIPsecMainModeCryptoSet

New-NetIPsecMainModeRule

Open-NetGPO

Save-NetGPO

Remove-NetIPsecMainModeCryptoSet

New-NetIPsecMainModeCryptoProposal