



Windows PowerShell Get-Help on Cmdlet 'New-AzIpsecPolicy'

PS: \>Get-HELP New-AzIpsecPolicy -Full

WARNING: The names of some imported commands from the module 'Microsoft.Azure.PowerShell.Cmdlets.Network' include unapproved verbs that might make them less discoverable.

To find the commands with unapproved verbs, run the Import-Module command again with the Verbose parameter. For a list of approved verbs, type Get-Verb.

NAME

New-AzIpsecPolicy

SYNOPSIS

Creates an IPsec Policy.

SYNTAX

```

New-AzIpsecPolicy [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -DhGroup {None |
DHGroup1 | DHGroup14 |
DHGroup2 | DHGroup2048 | DHGroup24 | ECP256 | ECP384} -IkeEncryption {DES | DES3 | AES128 | AES192 |
AES256} -IkeIntegrity {MD5 | SHA1 | SHA256 | SHA384}
-IpsecEncryption {None | DES | DES3 | AES128 | AES192 | AES256 | GCMAES128 | GCMAES192 | GCMAES256}
-IpsecIntegrity {MD5 | SHA1 | SHA256 | GCMAES128 | GCMAES192 |
GCMAES256} -PfsGroup {None | PFS1 | PFS2 | PFS2048 | PFS24 | ECP256 | ECP384} [-SADataSize kilobytes]
  
```

<System.Int32>] [-SALifeTimeSeconds <System.Int32>]
[<CommonParameters>]

DESCRIPTION

The New-AzIpsPolicy cmdlet creates an IPSec policy proposal to be used in a virtual network gateway connection.

PARAMETERS

-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>

The credentials, account, tenant, and subscription used for communication with azure.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-DhGroup <System.String>

The DH Groups used in IKE Phase 1 for initial SA

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-IkeEncryption <System.String>

The IKE encryption algorithm (IKE Phase 1)

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-IkeIntegrity <System.String>

The IKE integrity algorithm (IKE Phase 1)

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-IpsecEncryption <System.String>

The IPSec encryption algorithm (IKE Phase 2)

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-IpsecIntegrity <System.String>

The IPSec integrity algorithm (IKE Phase 2)

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-PfsGroup <System.String>

The DH Groups used in IKE Phase 2 for new child SA

Required? true
Position? named
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-SADataSizeKilobytes <System.Int32>

The IPSec Security Association (also called Quick Mode or Phase 2 SA) payload size in KB

Required? false
Position? named
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-SALifeTimeSeconds <System.Int32>

The IPSec Security Association (also called Quick Mode or Phase 2 SA) lifetime in seconds

Required? false
Position? named
Default value None
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 \(https://go.microsoft.com/fwlink/?LinkID=113216\)](https://go.microsoft.com/fwlink/?LinkID=113216).

INPUTS

None

OUTPUTS

Microsoft.Azure.Commands.Network.Models.PSIpsecPolicy

NOTES

----- Example 1 -----

```
$ipsecPolicy = New-AzIpsecPolicy -SALifeTimeSeconds 1000 -SADataSizeKilobytes 2000 -IpsecEncryption
"GCMAES256" -IpsecIntegrity "GCMAES256" -IkeEncryption "AES256"
-IkeIntegrity "SHA256" -DhGroup "DHGroup14" -PfsGroup "PFS2048"
New-AzVirtualNetworkGatewayConnection -ResourceGroupName $rgname -name $vnetConnectionName -location
$location -VirtualNetworkGateway1 $vnetGateway
-LocalNetworkGateway2 $localnetGateway -ConnectionType IPsec -RoutingWeight 3 -SharedKey $sharedKey
-UsePolicyBasedTrafficSelectors $true -IpsecPolicies $ipsecPolicy
```

Creating an IPSec policy to be used for a new virtual network gateway connection.

RELATED LINKS

Online Version: <https://learn.microsoft.com/powershell/module/az.network/new-azipsecpolicy>