



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 'Set-VpnConnectionIPsecConfiguration'

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

NAME

Set-VpnConnectionIPsecConfiguration

SYNOPSIS

Sets the IPsec parameters of a VPN connection.

SYNTAX

```
Set-VpnConnectionIPsecConfiguration [-ConnectionName] <String> [-AuthenticationTransformConstants] {MD596 |  
SHA196 | SHA256128 | GCMAES128 | GCMAES192 | GCMAES256 |  
None} [-CipherTransformConstants] {DES | DES3 | AES128 | AES192 | AES256 | GCMAES128 | GCMAES192 |  
GCMAES256 | None} [-DHGroup] {None | Group1 | Group2 | Group14 |  
ECP256 | ECP384 | Group24} [-EncryptionMethod] {DES | DES3 | AES128 | AES192 | AES256 | GCMAES128 |  
GCMAES256} [-IntegrityCheckMethod] {MD5 | SHA1 | SHA256 | SHA384}  
[-PfsGroup] {None | PFS1 | PFS2 | PFS2048 | ECP256 | ECP384 | PFSMM | PFS24} [-AllUserConnection] [-AsJob]  
[-CimSession <CimSession[]>] [-Confirm] [-Force]  
[-PassThru] [-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]  
  
Set-VpnConnectionIPsecConfiguration [-ConnectionName] <String> [-RevertToDefault] [-AllUserConnection] [-AsJob]  
[-CimSession <CimSession[]>] [-Confirm] [-Force]
```

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

DESCRIPTION

The Set-VpnConnectionIpsecConfiguration cmdlet sets the IPsec parameters of a VPN connection. The settings apply only to IKEv2 and L2TP VPN connections.

PARAMETERS

-AllUserConnection [<SwitchParameter>]

Indicates that the VPN connection being modified is in the global phone book.

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

-AuthenticationTransformConstants <AuthenticationTransformConstants>

Specifies authentication header (AH) transform in the IPsec policy. For more information, see the Set-VpnServerIpsecConfiguration cmdlet. The acceptable values for this parameter are:

- SHA196
- SHA256128
- GCMAES128
- GCMAES192
- GCMAES256
- None

Required? true

Position? 2

Default value None

Accept pipeline input? True (ByPropertyName)

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

-CipherTransformConstants <CipherTransformConstants>

Specifies Encapsulating Security Payload (ESP) cipher transform in the IPsec policy. Acceptable values for this parameter are:

- DES

- DES3

- AES128

- AES192

- AES256

- GCMAES128

- GCMAES192

- GCMAES256

- None

Required? true

Position? 3

Default value None

Accept pipeline input? True (ByPropertyName)

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

-ConnectionName <String>

Specifies the name of a VPN connection profile to modify. To view existing VPN connection profiles, use the Get-VpnConnection cmdlet.

Required? true

Position? 1

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-DHGroup <DHGroup>

Specifies the Diffie-Hellman (DH) Group to use during IKE key exchanges. The acceptable values for this parameter are:

- None

- Group1

- Group2

- Group14

- ECP256

- ECP384

- Group24

Required? true

Position? 4

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-EncryptionMethod <EncryptionMethod>

Specifies the encryption method. The acceptable values for this parameter are:

- DES

- DES3

- AES128

- AES192

- AES256

- GCMAES128

- GCMAES256

Required? true

Position? 5

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Force [<SwitchParameter>]

Forces the command to run without asking for user confirmation.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-IntegrityCheckMethod <IntegrityCheckMethod>

Specifies the integrity check method used to protect data from tampering. The acceptable values for this parameter are:

- MD5

- SHA1

- SHA256

- SHA384

Required? true

Position? 6

Default value None

Accept pipeline input? True (ByPropertyName)

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. If you specify this parameter, the

cmdlet returns the VpnConnection object that contains the VpnConnection configuration settings.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-PfsGroup <PfsGroup>

Specifies the Perfect Forwarding Secrecy (PFS) Group in the IPsec policy. The acceptable values for this parameter are:

- None
- PFS1
- PFS2
- PFS2048
- ECP256
- ECP384
- PFSMM
- PFS24

Required? true
Position? 7
Default value None
Accept pipeline input? True (ByPropertyName)
Accept wildcard characters? false

-RevertToDefault [<SwitchParameter>]

Indicates that the cmdlet sets the IPsec parameters to the default values.

Required? true
Position? 2
Default value False
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 PowerShell 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

OUTPUTS

NOTES

-- Example 1: Set the IPsec configuration for an IKEv2 tunnel --

```
PS C:\> Add-VpnConnection -Name "Contoso" -ServerAddress 176.16.1.2 -TunnelType "Ikev2"
```

```
PS C:\> Set-VpnConnectionIPsecConfiguration -ConnectionName "Contoso" -AuthenticationTransformConstants None  
-CipherTransformConstants AES256 -EncryptionMethod AES256  
-IntegrityCheckMethod SHA384 -PfsGroup None -DHGroup ECP384 -PassThru -Force  
AuthenticationTransformConstants : None
```

CipherTransformConstants : AES256

DHGroup : ECP384

IntegrityCheckMethod : SHA384

PfsGroup : None

EncryptionMethod : AES256

This example sets the IPsec configuration for a VPN connection using IKEv2.

The first command uses the `Add-VpnConnection` cmdlet to add a VPN connection on the server with the address 176.16.1.2. The cmdlet specifies an IKEv2 tunnel.

The second command uses the `Set-VpnConnectionIPsecConfiguration` cmdlet to set the configuration by using the `ConnectionName` parameter. The command also specifies

values for the CipherTransformConstants , EncryptionMethod , IntegrityCheckMethod , and DHGroup parameters.

-- Example 2: Set the IPsec configuration for an L2TP tunnel --

```
PS C:\> Add-VpnConnection -Name "Contoso" -ServerAddress 176.16.1.2 -TunnelType "L2tp"
```

```
PS C:\> Set-VpnConnectionIPsecConfiguration -ConnectionName "Contoso" -AuthenticationTransformConstants None  
-CipherTransformConstants AES128 -EncryptionMethod AES128  
-IntegrityCheckMethod SHA256 -PfsGroup None -DHGroup ECP256 -PassThru -Force  
AuthenticationTransformConstants : None
```

CipherTransformConstants : AES128

DHGroup : ECP256

IntegrityCheckMethod : SHA256

PfsGroup : None

EncryptionMethod : AES128

This example sets the IPsec configuration for an L2TP tunnel.

The first command uses Add-VpnConnection to add a VPN connection on the server with the address 176.16.1.2. The command also specifies an L2TP tunnel.

The second command uses Set-VpnConnectionIPsecConfiguration to set the configuration. The command also specifies values for the CipherTransformConstants ,

EncryptionMethod , IntegrityCheckMethod , and DHGroup parameters.

Example 3: Set the IPsec configuration for an IKEv2 tunnel with 128-bit data blocks

```
PS C:\>Add-VpnConnection -Name "Contoso" -ServerAddress 176.16.1.2 -TunnelType "Ikev2"
```

```
PS C:\> Set-VpnConnectionIPsecConfiguration -ConnectionName "Contoso" -AuthenticationTransformConstants  
GCMAES128 -CipherTransformConstants None -EncryptionMethod
```

AES128 -IntegrityCheckMethod SHA256 -PfsGroup None -DHGroup ECP256 -PassThru -Force

AuthenticationTransformConstants : GCMAES128

CipherTransformConstants : None

DHGroup : ECP256

IntegrityCheckMethod : SHA256

PfsGroup : None

EncryptionMethod : AES128

This example sets the IPsec configuration for an IKEv2 tunnel with authentication transform constants.

The first command uses Add-VpnConnection to add a VPN connection on the server with the address 176.16.1.2. The cmdlet specifies an IKEv2 tunnel.

The second command uses Set-VpnConnectionIPsecConfiguration to set the configuration. The command also specifies values for the CipherTransformConstants ,

EncryptionMethod , IntegrityCheckMethod , and DHGroup parameters, as well as specifying a value for the AuthenticationTransformConstants parameter.

Example 4: Set the IPsec configuration for an IKEv2 tunnel with 256-bit data blocks

```
PS C:\>Add-VpnConnection -Name "Contoso" -ServerAddress 176.16.1.2 -TunnelType "Ikev2"
```

```
PS C:\> Set-VpnConnectionIPsecConfiguration -ConnectionName "Contoso" -AuthenticationTransformConstants GCMAES256 -CipherTransformConstants None -EncryptionMethod
```

```
AES256 -IntegrityCheckMethod SHA384 -PfsGroup None -DHGroup ECP384 -PassThru -Force
```

```
AuthenticationTransformConstants : GCMAES256
```

CipherTransformConstants : None

DHGroup : ECP384

IntegrityCheckMethod : SHA384

PfsGroup : None

EncryptionMethod : AES256

This example sets the IPsec configuration for an IKEv2 tunnel, and specifies authentication transform constants.

The first command uses Add-VpnConnection to add a VPN connection on the server with the address 176.16.1.2. The cmdlet specifies an IKEv2 tunnel.

The second command uses Set-VpnConnectionIPsecConfiguration to set the configuration. The command also specifies values for the CipherTransformConstants ,

EncryptionMethod , IntegrityCheckMethod , and DHGroup parameters, as well as specifying a value for the AuthenticationTransformConstants parameter.

RELATED LINKS

Online

Version:

https://learn.microsoft.com/powershell/module/vpnclient/set-vpnconnectionipsecconfiguration?view=windowsserver2022-ps&wt.mc_id=ps-gethelp
Add-VpnConnection