



Windows PowerShell Get-Help on Cmdlet 'Open-NetGPO'

PS:\>Get-HELP Open-NetGPO -Full

NAME

Open-NetGPO

SYNOPSIS

Creates a cached copy of the Group Policy Object (GPO) to modify locally.

SYNTAX

Open-NetGPO [-PolicyStore] <String> [-AsJob] [-CimSession <CimSession[]>] [-DomainController <String>]
[-ThrottleLimit <Int32>] [<CommonParameters>]

DESCRIPTION

The Open-NetGPO cmdlet caches the Group Policy Object (GPO) so that modifications can be made locally. The changes are batch returned to the policy store with the

Save-NetGPO cmdlet.

If the DomainController parameter value is not a writeable Domain Controller (DC), then the batch updates will not be applied. To help target a writeable DC, use the

cmdlets in the Active Directory module using the Get-Command (<https://go.microsoft.com/fwlink/p/?LinkId=113300>) cmdlet

with the Module parameter set to ActiveDirectory.

An error will result for using this cmdlet when the user is not a domain administrator.

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

-DomainController <String>

Specifies the DC used to target the GPO. If this cmdlet is used without specifying this parameter, then the DC can target a read-only DC (RODC), and lose the

batch changes with Save-NetGPO. To help target a writeable DC, use the cmdlets in the Active Directory module using the Get-Command

(<https://go.microsoft.com/fwlink/p/?LinkId=113309>)cmdlet with the Module parameter set to ActiveDirectory.

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 rules to be stored. 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 Server 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-NetIPsecRule 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 Copy-NetIPsecRule cmdlet or with the New-NetIPsecRule cmdlet.

Required?	true
Position?	0
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 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

<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

None

OUTPUTS

Microsoft.Management.Infrastructure.CimInstance#root\StandardCimv2\GPOSession

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:\>$gpoSession = Open-NetGPO -PolicyStore castle.contoso.com\Win8ClientFirewallPolicy
```

```
PS C:\>Remove-NetFirewallRule -Name BlockIMAccess -GPOSession $gpoSession
```

```
PS C:\>New-NetFirewallRule -Name LimitIMAccess -DisplayName "Contoso Messenger" -Program  
"%ProgramFiles(X86)%\Contoso Messenger\cmmsg.exe" -Action Block -GPOSession  
$gpoSession
```

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

This example replaces one rule in a domain GPO with another using a cached copy of the GPO.

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

```
PS C:\>$domain = "corp.contoso.com"
```

```
PS C:\>$gpo = "corp.contoso.com\FirewallPolicy"
```

```
PS C:\>$pdc = Get-ADDomainController -Discover -Service PrimaryDC -DomainName $domain
```

```
PS C:\>$session = Open-NetGPO -PolicyStore $gpo -DomainController $pdc.Hostname
```

This example shows targeting and opening a writeable DC. This ensures that the batch modifications are made when the GPO is closed.

RELATED LINKS

Online

Version:

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

Get-Command <https://go.microsoft.com/fwlink/p/?LinkId=113309>

New-NetFirewallRule

Remove-NetFirewallRule

Save-NetGPO

New-NetIPsecRule

Set-NetIPsecRule

Get-ADDomainController