
## *Windows PowerShell Get-Help on Cmdlet 'Set-AzFirewallPolicy'*

***PS:\>Get-HELP Set-AzFirewallPolicy -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

Set-AzFirewallPolicy

SYNOPSIS

Saves a modified azure firewall policy

SYNTAX

Set-AzFirewallPolicy [-AsJob] [-BasePolicy <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-DnsSetting <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyDnsSettings>] [-ExplicitProxy <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyExplicitProxy>] [-Identity <Microsoft.Azure.Commands.Network.Models.PSManagedServiceIdentity>] -InputObject <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicy> [-IntrusionDetection <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyIntrusionDetection>] [-Location <System.String>] [-Name <System.String>] [-PrivateRange

<System.String[]>] [-SkuTier {Standard | Premium | Basic}] [-Snat
<Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicySNAT>] [-SqlSetting
<Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicySqlSetting>] [-Tag <System.Collections.Hashtable>]
[-ThreatIntelMode {Alert | Deny | Off}]
[-ThreatIntelWhitelist <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyThreatIntelWhitelist>]
[-TransportSecurityKeyVaultSecretId <System.String>]
[-TransportSecurityName <System.String>] [-UserAssignedIdentityId <System.String>] [-Confirm] [-WhatIf]
[<CommonParameters>]

Set-AzFirewallPolicy [-AsJob] [-BasePolicy <System.String>] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-DnsSetting
<Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyDnsSettings>] [-ExplicitProxy
<Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyExplicitProxy>] [-Identity
<Microsoft.Azure.Commands.Network.Models.PSManagedServiceIdentity>]
[-IntrusionDetection <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyIntrusionDetection>] -Location
<System.String> -Name <System.String> [-PrivateRange
<System.String[]>] -ResourceGroupName <System.String> [-SkuTier {Standard | Premium | Basic}] [-Snat
<Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicySNAT>] [-SqlSetting
<Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicySqlSetting>] [-Tag
<System.Collections.Hashtable>] [-ThreatIntelMode {Alert | Deny | Off}] [-ThreatIntelWhitelist
<Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyThreatIntelWhitelist>]
[-TransportSecurityKeyVaultSecretId <System.String>] [-TransportSecurityName
<System.String>] [-UserAssignedIdentityId <System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

Set-AzFirewallPolicy [-AsJob] [-BasePolicy <System.String>] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-DnsSetting
<Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyDnsSettings>] [-ExplicitProxy
<Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyExplicitProxy>] [-Identity
<Microsoft.Azure.Commands.Network.Models.PSManagedServiceIdentity>]
[-IntrusionDetection <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyIntrusionDetection>] -Location
<System.String> [-PrivateRange <System.String[]>]
-ResourceId <System.String> [-SkuTier {Standard | Premium | Basic}] [-Snat
<Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicySNAT>] [-SqlSetting

<Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicySqlSetting>] [-Tag <System.Collections.Hashtable>] [-ThreatIntelMode {Alert | Deny | Off}]

[-ThreatIntelWhitelist <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyThreatIntelWhitelist>] [-TransportSecurityKeyVaultSecretId <System.String>]

[-TransportSecurityName <System.String>] [-UserAssignedIdentityId <System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Set-AzFirewallPolicy cmdlet updates an Azure Firewall Policy.

PARAMETERS

-AsJob <System.Management.Automation.SwitchParameter>

Run cmdlet in the background

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-BasePolicy <System.String>

The base policy to inherit from

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-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

-DnsSetting <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyDnsSettings>

The DNS Setting

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ExplicitProxy <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyExplicitProxy>

The Explicit Proxy Settings

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Identity <Microsoft.Azure.Commands.Network.Models.PSManagedServiceIdentity>

Firewall Policy Identity to be assigned to Firewall Policy.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-InputObject <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicy>

The AzureFirewall Policy

Required? true

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-IntrusionDetection <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyIntrusionDetection>

The Intrusion Detection Setting

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Location <System.String>

location.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Name <System.String>

The resource name.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? true

-PrivateRange <System.String[]>

The Private IP Range

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ResourceGroupName <System.String>

The resource group name.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? true

-ResourceId <System.String>

The resource Id.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? true

-SkuTier <System.String>

Firewall policy sku tier

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Snat <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicySNAT>

The private IP addresses/IP ranges to which traffic will not be SNAT in Firewall Policy.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SqlSetting <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicySqlSetting>

The SQL related setting

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Tag <System.Collections.Hashtable>

A hashtable which represents resource tags.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ThreatIntelMode <System.String>

The operation mode for Threat Intelligence.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ThreatIntelWhitelist <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyThreatIntelWhitelist>

The allowlist for Threat Intelligence

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-TransportSecurityKeyVaultSecretId <System.String>

Secret Id of (base-64 encoded unencrypted pfx) 'Secret' or 'Certificate' object stored in KeyVault

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-TransportSecurityName <System.String>

Transport security name

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-UserAssignedIdentityId <System.String>

ResourceId of the user assigned identity to be assigned to Firewall Policy.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Confirm <System.Management.Automation.SwitchParameter>

Prompts you for confirmation before running the cmdlet.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-WhatIf <System.Management.Automation.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

System.String

Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicy

System.Collections.Hashtable

OUTPUTS

Microsoft.Azure.Commands.Network.Models.PSAzureFirewall

NOTES

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

Set-AzFirewallPolicy -InputObject $fp

This example sets the firewall policy with the new firewall policy value

---------- Example 2 ----------

Set-AzFirewallPolicy -Name firewallPolicy1 -ResourceGroupName TestRg -Location westcentralus -ThreatIntelMode "Alert"

This example sets the firewall policy with the new threat intel mode

---------- Example 3 ----------

$threatIntelWhitelist = New-AzFirewallPolicyThreatIntelWhitelist -IpAddress 23.46.72.91,192.79.236.79 -FQDN microsoft.com
Set-AzFirewallPolicy -Name firewallPolicy1 -ResourceGroupName TestRg -Location westcentralus -ThreatIntelWhitelist $threatIntelWhitelist

This example sets the firewall policy with the new threat intel allowlist

---------- Example 4 ----------

$exProxy = New-AzFirewallPolicyExplicitProxy -EnableExplicitProxy -HttpPort 100 -HttpsPort 101 -EnablePacFile -PacFilePort 130 -PacFile
"sampleurlfortesting.blob.core.windowsnet/nothing"
Set-AzFirewallPolicy -Name firewallPolicy1 -ResourceGroupName TestRg -Location westcentralus -ExplicitProxy $exProxy

BasePolicy : null
DnsSettings : null
Etag : null
ExplicitProxy
EnableExplicitProxy : true
EnablePacFile : true
HttpPort : 100
HttpsPort : 101

```
 PacFile               : "sampleurlfortesting.blob.core.windowsnet/nothing"
 PacFilePort           : 130
Id                     : null
Identity               : null
IntrusionDetection     : null
Location               : "westcentralus"
Name                   : "firewallPolicy1"
PrivateRange           : null
PrivateRangeText       : "[]"
ProvisioningState      : null
ResourceGroupName      : "TestRg"
ResourceGuid           : null
RuleCollectionGroups   : null
Sku
 Tier                  : "Standard"
Snat
 AutoLearnPrivateRanges : null
 PrivateRanges         : null
SqlSetting             : null
Tag                    : null
TagsTable              : null
ThreatIntelMode        : "Alert"
ThreatIntelWhitelist   : null
TransportSecurity      : null
Type                   : null
```

This example sets the firewall policy with the explicit proxy settings

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.network/set-azfirewallpolicy

New-AzFirewallPolicyExplicitProxy