Windows PowerShell Get-Help on Cmdlet 'Update-AzFrontDoorWafPolicy'

PS:\>Get-HELP Update-AzFrontDoorWafPolicy -Full

NAME

Update-AzFrontDoorWafPolicy

SYNOPSIS

Update WAF policy

SYNTAX

Update-AzFrontDoorWafPolicy [-CustomBlockResponseBody <System.String>] [-CustomBlockResponseStatusCode <System.Nullable`1[System.Int32]>] [-Customrule <Microsoft.Azure.Commands.FrontDoor.Models.PSCustomRule[]>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-EnabledState {Enabled | Disabled}] -InputObject <Microsoft.Azure.Commands.FrontDoor.Models.PSPolicy> [-ManagedRule <Microsoft.Azure.Commands.FrontDoor.Models.PSManagedRule[]>] [-Mode <System.String>] [-RedirectUrl <System.String>] [-RequestBodyCheck <System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

Update-AzFrontDoorWafPolicy [-CustomBlockResponseBody <System.String>] [-CustomBlockResponseStatusCode <System.Nullable`1[System.Int32]>] [-Customrule <Microsoft.Azure.Commands.FrontDoor.Models.PSCustomRule[]>] [-DefaultProfile

<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-EnabledState {Enabled | Disabled}] [-ManagedRule
<Microsoft.Azure.Commands.FrontDoor.Models.PSManagedRule[]>] [-Mode <System.String>] -Name <System.String> [-RedirectUrl <System.String>] [-RequestBodyCheck
<System.String>] -ResourceGroupName <System.String> [-Confirm] [-WhatIf] [<CommonParameters>]

Update-AzFrontDoorWafPolicy [-CustomBlockResponseBody <System.String>] [-CustomBlockResponseStatusCode <System.Nullable`1[System.Int32]>] [-Customrule
<Microsoft.Azure.Commands.FrontDoor.Models.PSCustomRule[]>] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-EnabledState {Enabled | Disabled}] [-ManagedRule
<Microsoft.Azure.Commands.FrontDoor.Models.PSManagedRule[]>] [-Mode <System.String>] [-RedirectUrl <System.String>] [-RequestBodyCheck <System.String>] -ResourceId
<System.String> [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Update-AzFrontDoorWafPolicy cmdlet updates an existing WAF policy. If input parameters are not provided, old parameters from the existing WAF policy will be used.

PARAMETERS

-CustomBlockResponseBody <System.String>

Custom Response Body

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

-CustomBlockResponseStatusCode <System.Nullable`1[System.Int32]>

Custom Response Status Code

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Customrule <Microsoft.Azure.Commands.FrontDoor.Models.PSCustomRule[]>

Custom rules inside the policy

Required? false

Position? named

Default value None

Accept pipeline input? False

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

-EnabledState <Microsoft.Azure.Commands.FrontDoor.Models.PSEnabledState>

Whether the policy is in enabled state or disabled state. Possible values include: 'Disabled', 'Enabled'

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-InputObject <Microsoft.Azure.Commands.FrontDoor.Models.PSPolicy>

The FireWallPolicy object to update.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-ManagedRule <Microsoft.Azure.Commands.FrontDoor.Models.PSManagedRule[]>

Managed rules inside the policy

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Mode <System.String>

Describes if it is in detection mode or prevention mode at policy level. Possible values include:'Prevention', 'Detection'

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Name <System.String>

The name of the FireWallPolicy to update.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RedirectUrl <System.String>

Redirect URL

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RequestBodyCheck <System.String>

Defines if the body should be inspected by managed rules. Possible values include: 'Enabled', 'Disabled'

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ResourceGroupName <System.String>

The resource group to which the FireWallPolicy belongs.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ResourceId <System.String>

Resource Id of the FireWallPolicy to update

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

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

Microsoft.Azure.Commands.FrontDoor.Models.PSPolicy

System.String

OUTPUTS

Microsoft.Azure.Commands.FrontDoor.Models.PSPolicy

NOTES

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

Update-AzFrontDoorWafPolicy -Name $policyName -ResourceGroupName $resourceGroupName -CustomBlockResponseStatusCode 403

Name PolicyMode PolicyEnabledState CustomBlockResponseStatusCode RedirectUrl

---- ---------- ------------------ ---------------------------- -----------

{policyName} Prevention Enabled 403 https://www.bing.com/

Update an existing WAF policy custom status code.

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

Update-AzFrontDoorWafPolicy -Name $policyName -ResourceGroupName $resourceGroupName -Mode Detection

Name PolicyMode PolicyEnabledState CustomBlockResponseStatusCode RedirectUrl

---- ---------- ------------------ ------------------------------ -----------

{policyName} Detection Enabled 403 https://www.bing.com/

Update an existing WAF policy mode.

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

Update-AzFrontDoorWafPolicy -Name $policyName -ResourceGroupName $resourceGroupName -Mode Detection -EnabledState Disabled

Name PolicyMode PolicyEnabledState CustomBlockResponseStatusCode RedirectUrl

---- ---------- ------------------ ------------------------------ -----------

{policyName} Detection Disabled 403 https://www.bing.com/

Update an existing WAF policy enabled state and mode.

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

Get-AzFrontDoorWafPolicy -ResourceGroupName $resourceGroupName | Update-AzFrontDoorWafPolicy -Mode Detection -EnabledState Disabled

Update all WAF policies in $resourceGroupName

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.frontdoor/update-azfrontdoorwafpolicy

New-AzFrontDoorWafPolicy

Get-AzFrontDoorWafPolicy

New-AzFrontDoorWafManagedRuleObject

New-AzFrontDoorWafCustomRuleObject