Windows PowerShell Get-Help on Cmdlet 'Set-AzAlertsSuppressionRule'

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

NAME

Set-AzAlertsSuppressionRule

SYNOPSIS

Create or update an alerts suppression rule.

SYNTAX

Set-AzAlertsSuppressionRule -AlertType <System.String> [-AllOf <Microsoft.Azure.Commands.Security.Models.AlertsSuppressionRules.PSIScopeElement[]>] [-Comment <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-ExpirationDateUtc <System.Nullable`1[System.DateTime]>] -Name <System.String> -Reason <System.String> -State {Enabled | Disabled | Expired | Enabled | Disabled | Expired} [-SuppressionAlertsScope <Microsoft.Azure.Commands.Security.Models.AlertsSuppressionRules.PSSuppressionAlertsScope>] [-Confirm] [-WhatIf] [<CommonParameters>]

Set-AzAlertsSuppressionRule [-AlertType <System.String>] [-AllOf <Microsoft.Azure.Commands.Security.Models.AlertsSuppressionRules.PSIScopeElement[]>] [-Comment

<System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-ExpirationDateUtc <System.Nullable`1[System.DateTime]>] -InputObject <Microsoft.Azure.Commands.Security.Models.AlertsSuppressionRules.PSAlertsSuppressionRule> [-Name <System.String>]
[-Reason <System.String>] [-State {Enabled | Disabled | Expired | Enabled | Disabled | Expired}] [-SuppressionAlertsScope
<Microsoft.Azure.Commands.Security.Models.AlertsSuppressionRules.PSSuppressionAlertsScope>] [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

Create or update an alerts suppression rule.

PARAMETERS

-AlertType <System.String>

Alert type to suppress.

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

-AllOf <Microsoft.Azure.Commands.Security.Models.AlertsSuppressionRules.PSIScopeElement[]>

Scope the suppression rule using specific entities.

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

-Comment <System.String>

Comment.

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

-ExpirationDateUtc <System.Nullable`1[System.DateTime]>

Set an expiration data for the rule, expected to be in a UTC format.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-InputObject <Microsoft.Azure.Commands.Security.Models.AlertsSuppressionRules.PSAlertsSuppressionRule>

Input Object.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-Name <System.String>

Alert suppression rule name, needs to be unique per subscription.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Reason <System.String>

The reason for creating the suppression rule.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-State <Microsoft.Azure.Commands.Security.Models.AlertsSuppressionRules.PSRuleState>

State of the rule, Enabled/Disabled

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SuppressionAlertsScope

<Microsoft.Azure.Commands.Security.Models.AlertsSuppressionRules.PSSuppressionAlertsScope>

Scope the suppression rule using specific entities.

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

Microsoft.Azure.Commands.Security.Models.AlertsSuppressionRules.PSAlertsSuppressionRule

OUTPUTS

Microsoft.Azure.Commands.Security.Models.AlertsSuppressionRules.PSAlertsSuppressionRule

NOTES

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

Set-AzAlertsSuppressionRule -Name "Example" -State Enabled -Comment "Example of a comment" -AlertType "AzureDNS_CurrencyMining" -Reason "Other" -AllOf

@([Microsoft.Azure.Commands.Security.Models.AlertsSuppressionRules.PSScopeElementContains]::new("entities.account.name", "example")) -ExpirationDateUtc

2024-10-17T15:02:24.7511441Z

The above example creates a new suppression rule with the name "Example" to suppress alerts of type (Digital currency mining

activity)[https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-reference] that contains "example" as part of their account name.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.security/set-azalertssuppressionrule