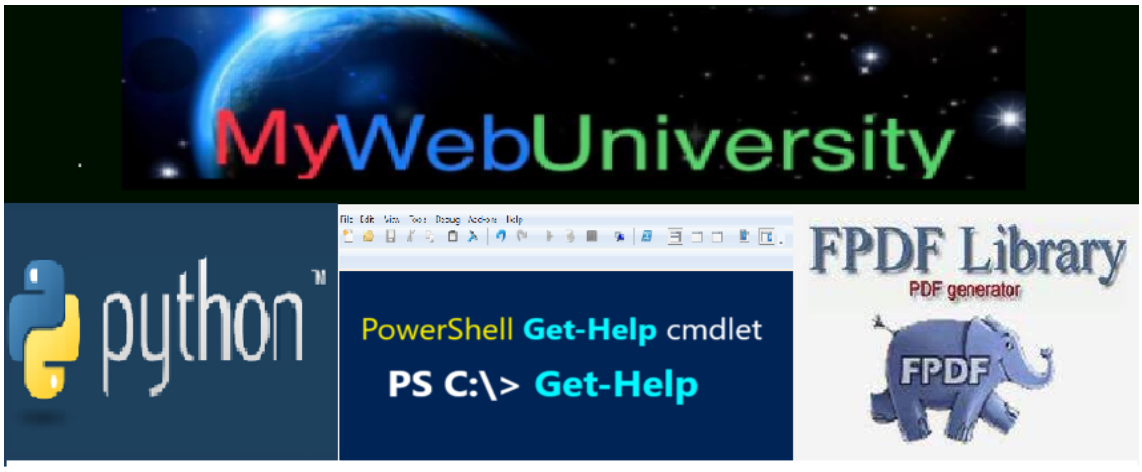

Full credit is given to all the above companies including the Operating System that this PDF file was generated!

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

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

NAME

Set-AzDeviceSecurityGroup

SYNOPSIS

Create or update device security group

SYNTAX

Set-AzDeviceSecurityGroup [-AllowlistRule <Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSAllowlistCustomAlertRule[]>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-DenylistRule <Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSDenylistCustomAlertRule[]>] -HubResourceId <System.String> -Name <System.String> [-ThresholdRule <Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSThresholdCustomAlertRule[]>] [-TimeWindowRule <Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSTimeWindowCustomAlertRule[]>] [-Confirm] [-WhatIf] [<CommonParameters>]

Set-AzDeviceSecurityGroup [-AllowlistRule <Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSAllowlistCustomAlertRule[]>] [-DefaultProfile

<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-DenylistRule
<Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSDenylistCustomAlertRule[]>] -InputObject
<Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSDeviceSecurityGroup> [-ThresholdRule
<Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSThresholdCustomAlertRule[]>]
[-TimeWindowRule
<Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSTimeWindowCustomAlertRule[]>] [-Confirm]
[-WhatIf] [<CommonParameters>]

Set-AzDeviceSecurityGroup [-AllowlistRule
<Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSAllowlistCustomAlertRule[]>] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-DenylistRule
<Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSDenylistCustomAlertRule[]>] -ResourceId
<System.String> [-ThresholdRule
<Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSThresholdCustomAlertRule[]>]
[-TimeWindowRule
<Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSTimeWindowCustomAlertRule[]>] [-Confirm]
[-WhatIf] [<CommonParameters>]

DESCRIPTION

The Set-AzDeviceSecurityGroup cmdlet creates or updates a device security group defined in iot security solution.

PARAMETERS

-AllowlistRule <Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSAllowlistCustomAlertRule[]>

Allow list rules.

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

-DenylistRule <Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSDenylistCustomAlertRule[]>

Deny list rules.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-HubResourceId <System.String>

IoT Hub resource Id.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-InputObject <Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSDeviceSecurityGroup>

Input Object.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-Name <System.String>

Resource name.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ResourceId <System.String>

ID of the security resource that you want to invoke the command on.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ThresholdRule <Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSThresholdCustomAlertRule[]>

Threshold rules.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-TimeWindowRule

<Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSTimeWindowCustomAlertRule[]>

Time window rules.

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.DeviceSecurityGroups.PSThresholdCustomAlertRule[]

Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSTimeWindowCustomAlertRule[]

Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSAllowlistCustomAlertRule[]

Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSDenylistCustomAlertRule[]

Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSDeviceSecurityGroup

System.String

OUTPUTS

Microsoft.Azure.Commands.Security.Models.DeviceSecurityGroups.PSDeviceSecurityGroup

NOTES

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

$TimeWindowSize = New-TimeSpan -Minutes 5

$TimeWindowRule = New-AzDeviceSecurityGroupTimeWindowRuleObject -Type "ActiveConnectionsNotInAllowedRange" -Enabled $true `

-MaxThreshold 30 -MinThreshold 0 -TimeWindowSize $TimeWindowSize

Set-AzDeviceSecurityGroup -Name "MySecurityGroup" `

-HubResourceId "/subscriptions/XXXXXXXX-XXXX-XXXXX-XXXX-XXXXXXXXXXXX/resourceGroups/MyResourceGroup/providers/Microsoft.Devices/IotHubs/MyHub" `

-TimeWindowRule $TimeWindowRules

Id: "/subscriptions/XXXXXXXX-XXXX-XXXXX-XXXX-XXXXXXXXXXXX/resourceGroups/MyResourceGroup/providers/Microsoft.Devices/IotHubs/MyHub/providers/Microsoft.Security/deviceSecurityGroups/MySecurityGroup"

Name: "MySecurityGroup"

Type: "Microsoft.Security/deviceSecurityGroups"

ThresholdRules: []

TimeWindowRules: [

{

RuleType: "ActiveConnectionsNotInAllowedRange"

DisplayName: "Number of active connections is not in allowed range"

Description: "Get an alert when the number of active connections of a device in the time window is not in the allowed range"

IsEnabled: true

MinThreshold: 0

MaxThreshold: 0

TimeWindowSize: "PT5M"

}]

AllowlistRules: [

{

RuleType": "ConnectionToIpNotAllowed",

DisplayName: "Outbound connection to an ip that isn't allowed"

Description: "Get an alert when an outbound connection is created between your device and an ip that isn't allowed"

IsEnabled: false

ValueType: "IpCidr"

```
      AllowlistValues: []
    },
    {
      RuleType: "LocalUserNotAllowed"
      DisplayName: "Login by a local user that isn't allowed"
      Description: "Get an alert when a local user that isn't allowed logins to the device"
      IsEnabled: false
      ValueType: "String"
      AllowlistValues: []
    }]
DenylistRules: []
```

Update existing device security group from IoT Hub

"/subscriptions/XXXXXXXX-XXXX-XXXXX-XXXX-XXXXXXXXXXXX/resourceGroups/MyResourceGroup/providers/Microsoft.Devices/IotHubs/MyHub" with rule type "ActiveConnectionsNotInAllowedRange"

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.security/Set-AzDeviceSecurityGroup