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 'Add-AzWebAppAccessRestrictionRule'

PS:\>Get-HELP Add-AzWebAppAccessRestrictionRule -Full

NAME

Add-AzWebAppAccessRestrictionRule

SYNOPSIS

Adds an Access Restiction rule to an Azure Web App.

SYNTAX

Add-AzWebAppAccessRestrictionRule [-ResourceGroupName] <System.String> [-WebAppName] <System.String> [-Action {Allow | Deny}] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Description <System.String>] [-HttpHeader <System.Collections.Hashtable>]
[-IgnoreMissingServiceEndpoint] [-Name <System.String>] [-PassThru] -Priority <System.UInt32> [-SlotName <System.String>] -SubnetName <System.String> [-TargetScmSite]
-VirtualNetworkName <System.String> [-Confirm] [-WhatIf] [<CommonParameters>]

Add-AzWebAppAccessRestrictionRule [-ResourceGroupName] <System.String> [-WebAppName] <System.String> [-Action {Allow | Deny}] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Description <System.String>] [-HttpHeader <System.Collections.Hashtable>]

[-IgnoreMissingServiceEndpoint] [-Name <System.String>] [-PassThru] -Priority <System.UInt32> [-SlotName <System.String>] -SubnetId <System.String> [-TargetScmSite]
[-Confirm] [-WhatIf] [<CommonParameters>]

Add-AzWebAppAccessRestrictionRule [-ResourceGroupName] <System.String> [-WebAppName] <System.String> [-Action {Allow | Deny}] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Description <System.String>] [-HttpHeader <System.Collections.Hashtable>]
-IpAddress <System.String> [-Name <System.String>] [-PassThru] -Priority <System.UInt32> [-SlotName <System.String>] [-TargetScmSite] [-Confirm] [-WhatIf]
[<CommonParameters>]

Add-AzWebAppAccessRestrictionRule [-ResourceGroupName] <System.String> [-WebAppName] <System.String> [-Action {Allow | Deny}] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Description <System.String>] [-HttpHeader <System.Collections.Hashtable>]
[-Name <System.String>] [-PassThru] -Priority <System.UInt32> -ServiceTag <System.String> [-SlotName <System.String>] [-TargetScmSite] [-Confirm] [-WhatIf]
[<CommonParameters>]

DESCRIPTION

The Add-AzWebAppAccessRestrictionRule cmdlet adds an Access Restriction rule to an Azure Web App.

PARAMETERS

-Action <System.String>

Allow or Deny rule.

Required? false
Position? named
Default value Allow
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

-Description <System.String>

Access Restriction description.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-HttpHeader <System.Collections.Hashtable>

Http header restrictions. Example: -HttpHeader @{'x-azure-fdid' = '7acacb02-47ea-4cd4-b568-5e880e72582e'; 'x-forwarded-host' = 'www.contoso.com',

'app.contoso.com'}

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-IgnoreMissingServiceEndpoint <System.Management.Automation.SwitchParameter>

Specify if Service Endpoint registration at Subnet should be validated.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-IpAddress <System.String>

Ip Address v4 or v6 CIDR range. E.g.: 192.168.0.0/24

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Name <System.String>

Rule Name

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-PassThru <System.Management.Automation.SwitchParameter>

Return the access restriction config object.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Priority <System.UInt32>

Access Restriction priority. E.g.: 500.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ResourceGroupName <System.String>

Resource Group Name

Required? true

Position? 0

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ServiceTag <System.String>

Name of Service Tag

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SlotName <System.String>

Deployment Slot name.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SubnetId <System.String>

ResourceId of Subnet.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SubnetName <System.String>

Name of Subnet.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-TargetScmSite <System.Management.Automation.SwitchParameter>

Rule is aimed for Main site or Scm site.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-VirtualNetworkName <System.String>

Name of Virtual Network.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-WebAppName <System.String>

The name of the web app.

Required? true

Position? 1

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

System.String

OUTPUTS

Microsoft.Azure.Commands.WebApps.Models.PSAccessRestrictionConfig

NOTES

Example 1: Add IpAddress Access Restriction rule to a Web App

```
Add-AzWebAppAccessRestrictionRule -ResourceGroupName "Default-Web-WestUS" -WebAppName "ContosoSite" `
-Name IpRule -Priority 200 -Action Allow -IpAddress 10.10.0.0/8
```

This command adds an access restriction rule with priority 200 and ip range to a Web App named ContosoSite that belongs to the resource group Default-Web-WestUS.

Example 2: Add Subnet Service Endpoint Access Restriction rule to a Web App

```
Add-AzWebAppAccessRestrictionRule -ResourceGroupName "Default-Web-WestUS" -WebAppName "ContosoSite" `
-Name SubnetRule -Priority 300 -Action Allow -SubnetName appgw-subnet -VirtualNetworkName corp-vnet
```

This command adds an access restriction rule with priority 300 and with subnet appgw-subnet in corp-vnet to a Web App named ContosoSite that belongs to the resource group Default-Web-WestUS.

Example 3: Add ServiceTag Access Restriction rule to a Web App

```
Add-AzWebAppAccessRestrictionRule -ResourceGroupName "Default-Web-WestUS" -WebAppName "ContosoSite" `
-Name ServiceTagRule -Priority 200 -Action Allow -ServiceTag AzureFrontDoor.Backend
```

This command adds an access restriction rule with priority 200 and a Service Tag representing the ip scope of Azure Front Door to a Web App named ContosoSite that belongs to the resource group Default-Web-WestUS.

Example 4: Add multi-address Access Restriction rule to a Web App

```
Add-AzWebAppAccessRestrictionRule -ResourceGroupName "Default-Web-WestUS" -WebAppName "ContosoSite" `
-Name MultipleIpRule -Priority 200 -Action Allow -IpAddress "10.10.0.0/8,192.168.0.0/16"
```

This command adds an access restriction rule with priority 200 and two ip ranges to a Web App named ContosoSite that belongs to the resource group Default-Web-WestUS.

Example 5: Add Access Restriction rule with http header to a Web App

```
Add-AzWebAppAccessRestrictionRule -ResourceGroupName "Default-Web-WestUS" -WebAppName "ContosoSite" `
-Name MultipleIpRule -Priority 400 -Action Allow -ServiceTag AzureFrontDoor.Backend `
        -HttpHeader @{'x-forwarded-host' = 'www.contoso.com', 'app.contoso.com'; 'x-azure-fdid' =
'355deb06-47c4-4ba4-9641-c7d7a98b913e'}
```

This command adds an access restriction rule with priority 400 for Service Tag AzureFrontDoor.Backend and further restricts access only to http headers of certain

values to a Web App named ContosoSite that belongs to the resource group Default-Web-WestUS.

RELATED LINKS

Update-AzWebAppAccessRestrictionConfig

Get-AzWebAppAccessRestrictionConfig

Remove-AzWebAppAccessRestrictionRule