
## *Windows PowerShell Get-Help on Cmdlet 'New-AzSecurityConnector'*

***PS:\>Get-HELP New-AzSecurityConnector -Full***

NAME

New-AzSecurityConnector

SYNOPSIS

Create a security connector.

If a security connector is already Created and a subsequent request is issued for the same security connector id, then it will be Created.

SYNTAX

New-AzSecurityConnector -Name <String> -ResourceGroupName <String> [-SubscriptionId <String>] [-EnvironmentData <ISecurityConnectorEnvironment>] [-EnvironmentName
<String>] [-Etag <String>] [-HierarchyIdentifier <String>] [-Kind <String>] [-Location <String>] [-Offering <ICloudOffering[]>] [-Tag <Hashtable>] [-DefaultProfile
<PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>] [-ProxyCredential <PSCredential>]
[-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

DESCRIPTION

Create a security connector.

If a security connector is already Created and a subsequent request is issued for the same security connector id, then it will be Created.

PARAMETERS

-Name <String>

The security connector name.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ResourceGroupName <String>

The name of the resource group within the user's subscription.

The name is case insensitive.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-SubscriptionId <String>

Azure subscription ID

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-EnvironmentData <ISecurityConnectorEnvironment>

The security connector environment data.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-EnvironmentName <String>

The multi cloud resource's cloud name.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Etag <String>

Entity tag is used for comparing two or more entities from the same requested resource.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-HierarchyIdentifier <String>

The multi cloud resource identifier (account id in case of AWS connector, project number in case of GCP connector).

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Kind <String>

Kind of the resource

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Location <String>

Location where the resource is stored

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Offering <ICloudOffering[]>

A collection of offerings for the security connector.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Tag <Hashtable>

A list of key value pairs that describe the resource.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DefaultProfile <PSObject>

The DefaultProfile parameter is not functional.

Use the SubscriptionId parameter when available if executing the cmdlet against a different subscription.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Break [<SwitchParameter>]

Wait for .NET debugger to attach

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-HttpPipelineAppend <SendAsyncStep[]>

SendAsync Pipeline Steps to be appended to the front of the pipeline

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-HttpPipelinePrepend <SendAsyncStep[]>

SendAsync Pipeline Steps to be prepended to the front of the pipeline

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Proxy <Uri>

The URI for the proxy server to use

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ProxyCredential <PSCredential>

Credentials for a proxy server to use for the remote call

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ProxyUseDefaultCredentials [<SwitchParameter>]

Use the default credentials for the proxy

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-WhatIf [<SwitchParameter>]

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Confirm [<SwitchParameter>]

Required? false

Position? named

Default value

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

OUTPUTS

Microsoft.Azure.PowerShell.Cmdlets.Security.Models.ISecurityConnector

NOTES

COMPLEX PARAMETER PROPERTIES

To create the parameters described below, construct a hash table containing the appropriate properties. For information on hash tables, run Get-Help
about_Hash_Tables.

ENVIRONMENTDATA <ISecurityConnectorEnvironment>: The security connector environment data.
EnvironmentType <String>: The type of the environment data.

OFFERING <ICloudOffering[]>: A collection of offerings for the security connector.
OfferingType <String>: The type of the security offering.

---------- EXAMPLE 1 ----------

```
PS C:\>$account = "891376984375"

$arnPrefix = "arn:aws:iam::$($account):role"

$cspmMonitorOffering = New-AzSecurityCspmMonitorAwsOfferingObject -NativeCloudConnectionCloudRoleArn "$arnPrefix/CspmMonitorAws"

$dcspmOffering = New-AzSecurityDefenderCspmAwsOfferingObject `
-VMScannerEnabled $true -ConfigurationScanningMode Default -ConfigurationCloudRoleArn "$arnPrefix/DefenderForCloud-AgentlessScanner" `
-DataSensitivityDiscoveryEnabled $true -DataSensitivityDiscoveryCloudRoleArn "$arnPrefix/SensitiveDataDiscovery" `
-DatabaseDspmEnabled $true -DatabaseDspmCloudRoleArn "$arnPrefix/DefenderForCloud-DataSecurityPostureDB" `
-CiemDiscoveryCloudRoleArn "$arnPrefix/DefenderForCloud-Ciem" -CiemOidcAzureActiveDirectoryAppName "mciem-aws-oidc-connector" -CiemOidcCloudRoleArn
"$arnPrefix/DefenderForCloud-OidcCiem" `
-MdcContainerImageAssessmentEnabled $true -MdcContainerImageAssessmentCloudRoleArn
```

"$arnPrefix/MDCContainersImageAssessmentRole" `

-MdcContainerAgentlessDiscoveryK8SEnabled $true -MdcContainerAgentlessDiscoveryK8SCloudRoleArn "$arnPrefix/MDCContainersAgentlessDiscoveryK8sRole"

$defenderForContainersOffering = New-AzSecurityDefenderForContainersAwsOfferingObject `

-AutoProvisioning $true -KuberneteServiceCloudRoleArn "$arnPrefix/DefenderForCloud-Containers-K8s" -KuberneteScubaReaderCloudRoleArn

"$arnPrefix/DefenderForCloud-DataCollection" `

-KinesiToS3CloudRoleArn "$arnPrefix/DefenderForCloud-Containers-K8s-kinesis-to-s3" -CloudWatchToKinesiCloudRoleArn

"$arnPrefix/DefenderForCloud-Containers-K8s-cloudwatch-to-kinesis" `

-KubeAuditRetentionTime 30 -ScubaExternalId "a47ae0a2-7bf7-482a-897a-7a139d30736c" `

-MdcContainerAgentlessDiscoveryK8SEnabled $true -MdcContainerAgentlessDiscoveryK8SCloudRoleArn "$arnPrefix/MDCContainersAgentlessDiscoveryK8sRole" `

-MdcContainerImageAssessmentEnabled $true -MdcContainerImageAssessmentCloudRoleArn "$arnPrefix/MDCContainersImageAssessmentRole" `

-EnableContainerVulnerabilityAssessment $false

$environment = New-AzSecurityAwsEnvironmentObject -ScanInterval 24

New-AzSecurityConnector -Name "aws-sdktest01" -ResourceGroupName "securityConnectors-tests" `

-EnvironmentData $environment -EnvironmentName AWS -HierarchyIdentifier "$account" `

-Offering @($cspmMonitorOffering, $dcspmOffering, $defenderForContainersOffering) `

-Location "CentralUS"

---------- EXAMPLE 2 ----------

PS C:\>$account = "843025268399"

$emailSuffix = "myproject.iam.gserviceaccount.com"

```
$cspmMonitorOffering = New-AzSecurityCspmMonitorGcpOfferingObject
-NativeCloudConnectionServiceAccountEmailAddress "microsoft-defender-cspm@$emailSuffix"
  -NativeCloudConnectionWorkloadIdentityProviderId "cspm"

  $dcspmOffering = New-AzSecurityDefenderCspmGcpOfferingObject `
    -VMScannerEnabled $true -ConfigurationScanningMode Default -ConfigurationExclusionTag @{key="value"} `
                                                    -MdcContainerAgentlessDiscoveryK8SEnabled $true
-MdcContainerAgentlessDiscoveryK8SServiceAccountEmailAddress "mdc-containers-k8s-operator@$emailSuffix"
  -MdcContainerAgentlessDiscoveryK8SWorkloadIdentityProviderId "containers" `
          -MdcContainerImageAssessmentEnabled $true -MdcContainerImageAssessmentServiceAccountEmailAddress
"mdc-containers-artifact-assess@$emailSuffix"
  -MdcContainerImageAssessmentWorkloadIdentityProviderId "containers" `
                    -DataSensitivityDiscoveryEnabled $true -DataSensitivityDiscoveryServiceAccountEmailAddress
"mdc-data-sec-posture-storage@$emailSuffix"
  -DataSensitivityDiscoveryWorkloadIdentityProviderId "data-security-posture-storage" `
                                -CiemDiscoveryServiceAccountEmailAddress "microsoft-defender-ciem@$emailSuffix"
-CiemDiscoveryAzureActiveDirectoryAppName "mciem-gcp-oidc-app"
  -CiemDiscoveryWorkloadIdentityProviderId "ciem-discovery"

  $defenderForContainersOffering = New-AzSecurityDefenderForContainersGcpOfferingObject `
                    -NativeCloudConnectionServiceAccountEmailAddress "microsoft-defender-containers@$emailSuffix"
-NativeCloudConnectionWorkloadIdentityProviderId "containers" `
    -DataPipelineNativeCloudConnectionServiceAccountEmailAddress "ms-defender-containers-stream@$emailSuffix"
  -DataPipelineNativeCloudConnectionWorkloadIdentityProviderId "containers-streams" `
      -AuditLogsAutoProvisioningFlag $true -DefenderAgentAutoProvisioningFlag $true -PolicyAgentAutoProvisioningFlag
$true `
                                                    -MdcContainerAgentlessDiscoveryK8SEnabled $true
-MdcContainerAgentlessDiscoveryK8SWorkloadIdentityProviderId "containers"
  -MdcContainerAgentlessDiscoveryK8SServiceAccountEmailAddress "mdc-containers-k8s-operator@$emailSuffix" `
          -MdcContainerImageAssessmentEnabled $true -MdcContainerImageAssessmentWorkloadIdentityProviderId
"containers"
  -MdcContainerImageAssessmentServiceAccountEmailAddress "mdc-containers-artifact-assess@$emailSuffix"
```

$environment = New-AzSecurityGcpProjectEnvironmentObject -ScanInterval 24 -ProjectDetailProjectId "asc-sdk-samples" -ProjectDetailProjectNumber "$account"

New-AzSecurityConnector -Name "gcp-sdktest01" -ResourceGroupName "securityConnectors-tests" -EnvironmentData $environment -EnvironmentName GCP -HierarchyIdentifier
"$account" `
-Offering @($cspmMonitorOffering, $dcspmOffering, $defenderForContainersOffering) -Location "CentralUS"

---------- EXAMPLE 3 ----------

PS C:\>New-AzSecurityConnector -ResourceGroupName "securityConnectors-pwsh-tmp" -Name "ado-sdk-pwsh-test03" `

-EnvironmentName AzureDevOps -EnvironmentData (New-AzSecurityAzureDevOpsScopeEnvironmentObject) `
-HierarchyIdentifier ([guid]::NewGuid().ToString()) -Location "CentralUS" `
-Offering @(New-AzSecurityCspmMonitorAzureDevOpsOfferingObject)

---------- EXAMPLE 4 ----------

PS C:\>New-AzSecurityConnector -ResourceGroupName "securityConnectors-pwsh-tmp" -Name "gh-sdk-pwsh-test03" `

-EnvironmentName GitHub -EnvironmentData (New-AzSecurityGitHubScopeEnvironmentObject) `
-HierarchyIdentifier ([guid]::NewGuid().ToString()) -Location "CentralUS" `
-Offering @(New-AzSecurityCspmMonitorGithubOfferingObject)

---------- EXAMPLE 5 ----------

PS C:\>New-AzSecurityConnector -ResourceGroupName "securityConnectors-pwsh-tmp" -Name "gl-sdk-pwsh-test03" `

-EnvironmentName GitLab -EnvironmentData (New-AzSecurityGitLabScopeEnvironmentObject) `

-HierarchyIdentifier ([guid]::NewGuid().ToString()) -Location "CentralUS" `

-Offering @(New-AzSecurityCspmMonitorGitLabOfferingObject)

RELATED LINKS

https://learn.microsoft.com/powershell/module/az.security/new-azsecurityconnector