Azure Sentinel management

Sentinel as a resource

Contents

[Introduction 2](#_Toc75440019)

[OnboardingStates resource 2](#_Toc75440020)

[OnboardingStates resource URI 2](#_Toc75440021)

[OnboardingStates resource body 2](#_Toc75440022)

[OnboardingStates operation group 3](#_Toc75440023)

[Create 3](#_Toc75440024)

[Request 3](#_Toc75440025)

[URI parameters 3](#_Toc75440026)

[Request body 3](#_Toc75440027)

[Response 4](#_Toc75440028)

[Get 4](#_Toc75440029)

[Request 4](#_Toc75440030)

[URI parameters 4](#_Toc75440031)

[Response 4](#_Toc75440032)

[List 5](#_Toc75440033)

[Request 5](#_Toc75440034)

[URI parameters 5](#_Toc75440035)

[Response 5](#_Toc75440036)

[Delete 5](#_Toc75440037)

[Request 5](#_Toc75440038)

[URI parameters 6](#_Toc75440039)

[Response 6](#_Toc75440040)

[ARM templates support 7](#_Toc75440041)

[ARM templates usage for CMK workspaces 8](#_Toc75440042)

[Note on the SecurityInsights solution 9](#_Toc75440043)

# Introduction

Azure Sentinel is a nested resource on top of a Log Analytics workspace resource. This abstraction introduces some complexity in managing the Azure Sentinel resource on its own, since it requires some preliminaries on the workspace and prevents managing the Azure Sentinel resource directly.

To overcome this, we introduce a dedicated endpoint called “OnboardingStates”. This endpoint allows managing the Azure Sentinel instance seamlessly on a workspace through the API. The endpoint provides a single source of truth for performing the different operations required for a complete creation/deletion (aka onboarding/offboarding) of Azure Sentinel on a workspace.

# OnboardingStates resource

The onboardingStates resource is currently supported in the 2021-03-01-preview API version only. You can think of the onboardingStates resource as the Azure Sentinel resource residing in the workspace. You can perform REST API calls on it to manage Azure Sentinel. Since a single Azure Sentinel resource is supported per workspace, there is only one name this resource can have, and it is called “default”. In other words, you can only create or delete the default onboardingStates resource on a Log Analytics workspace.

## OnboardingStates resource URI

The onboardingStates resource has the following URI structure:

https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.OperationalInsights/workspaces/{workspaceName}/providers/  
Microsoft.SecurityInsights/onboardingStates/{sentinelOnboardingStateName}?api-version=2021-03-01-preview

Where sentinelOnboardingStateName is always default.

## OnboardingStates resource body

The onboardingStates resource body consists of a single boolean property called “customerManagedKey”. As the name suggests this boolean is used to indicate whether the workspace being onboarded to Azure Sentinel has the Customer Managed Key (CMK) feature enabled on the workspace. For more information on CMK, see [this document](https://docs.microsoft.com/en-us/azure/sentinel/customer-managed-keys).

{

"properties": {

"customerManagedKey": false

}

}

This property is optional and defaults to false. Therefore, if you are not using CMK, you can simply ignore it and pass an empty properties object in the body.

# OnboardingStates operation group

The onboardingStates resource allows performing the following REST calls on it. The full swagger specification of the resource can be found [here](https://github.com/Azure/azure-rest-api-specs/blob/master/specification/securityinsights/resource-manager/Microsoft.SecurityInsights/preview/2021-03-01-preview/OnboardingStates.json). Example calls and responses can be found [here](https://github.com/Azure/azure-rest-api-specs/tree/master/specification/securityinsights/resource-manager/Microsoft.SecurityInsights/preview/2021-03-01-preview/examples/onboardingStates).

## Create

### Request

PUT

https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.OperationalInsights/workspaces/{workspaceName}/providers/  
Microsoft.SecurityInsights/onboardingStates/{sentinelOnboardingStateName}?api-version=2021-03-01-preview

### URI parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | In | Required | Type | Description |
| subscriptionId | Path | True | String | The Azure subscription ID. |
| resourceGroupName | Path | True | String | The name of the resource group within the user's subscription. The name is case insensitive.  Regex pattern:  ^[-\w\.\_\(\)]+$ |
| workspaceName | Path | True | String | The name of the workspace. |
| sentinelOnboardingStateName | Path | True | String | MUST be equal to default. |
| api-version | Query | True | String | The API version for the operation.  Currently only 2021-03-01-preview is supported. |

### Request body

{

"properties": {

"customerManagedKey": false

}

}

customerManagedKey – Optional. Boolean indicating whether the workspace is using Customer managed key (CMK). Default is false.

### Response

|  |  |
| --- | --- |
| Name | Description |
| 200 OK | OK, operation completed successfully.  Returned when calling PUT on an already onboarded workspace. |
| 201 Created | Created.  Returned when onboarding to Azure Sentinel for the first time on a workspace. |

## Get

### Request

GET

https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.OperationalInsights/workspaces/{workspaceName}/providers/  
Microsoft.SecurityInsights/onboardingStates/{sentinelOnboardingStateName}?api-version=2021-03-01-preview

### URI parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | In | Required | Type | Description |
| subscriptionId | Path | True | String | The Azure subscription ID. |
| resourceGroupName | Path | True | String | The name of the resource group within the user's subscription. The name is case insensitive.  Regex pattern:  ^[-\w\.\_\(\)]+$ |
| workspaceName | Path | True | String | The name of the workspace. |
| sentinelOnboardingStateName | Path | True | String | MUST be equal to default. |
| api-version | Query | True | String | The API version for the operation.  Currently only 2021-03-01-preview is supported. |
|  |  |  |  |  |

### Response

|  |  |
| --- | --- |
| Name | Description |
| 200 OK | OK, operation completed successfully. |

## List

### Request

GET

https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.OperationalInsights/workspaces/{workspaceName}/providers/  
Microsoft.SecurityInsights/onboardingStates?api-version=2021-03-01-preview

### URI parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | In | Required | Type | Description |
| subscriptionId | Path | True | String | The Azure subscription ID |
| resourceGroupName | Path | True | String | The name of the resource group within the user's subscription. The name is case insensitive.  Regex pattern:  ^[-\w\.\_\(\)]+$ |
| workspaceName | Path | True | String | The name of the workspace |
| api-version | Query | True | String | The API version for the operation.  Currently only 2021-03-01-preview is supported |

### Response

|  |  |
| --- | --- |
| Name | Description |
| 200 OK | OK, operation completed successfully. |

## Delete

### Request

DELETE

https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.OperationalInsights/workspaces/{workspaceName}/providers/  
Microsoft.SecurityInsights/onboardingStates/{sentinelOnboardingStateName}?api-version=2021-03-01-preview

### URI parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | In | Required | Type | Description |
| subscriptionId | Path | True | String | The Azure subscription ID. |
| resourceGroupName | Path | True | String | The name of the resource group within the user's subscription. The name is case insensitive.  Regex pattern:  ^[-\w\.\_\(\)]+$ |
| workspaceName | Path | True | String | The name of the workspace. |
| sentinelOnboardingStateName | Path | True | String | MUST be equal to default. |
| api-version | Query | True | String | The API version for the operation.  Currently only 2021-03-01-preview is supported. |
|  |  |  |  |  |

### Response

|  |  |
| --- | --- |
| Name | Description |
| 200 OK | OK, operation completed successfully. |
| 204 No Content | No Content. Returned when calling Delete on either an already offboarded workspace (i.e., Azure Sentinel was already removed), or a workspace which does not have Azure Sentinel at all. |

# ARM templates support

Since the onboardingStates is an Azure resource, it is possible to use ARM (Azure Resource Manager) templates to automate the operations on it.

Below is a simple ARM template to create onboardingStates resource on a workspace (i.e., onboard to Azure Sentinel):

{

"$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",

"contentVersion": "1.0.0.0",

"parameters": {

"workspaceName": {

"type": "string"

}

},

"resources": [

{

"name": "[concat(parameters('workspaceName'),'/Microsoft.SecurityInsights/default')]",

"type": "Microsoft.OperationalInsights/workspaces/providers/onboardingStates",

"apiVersion": "2021-03-01-preview",

"properties": {

},

"dependsOn": [

"[resourceId('Microsoft.OperationalInsights/workspaces', parameters('workspaceName'))]"

]

}

]

}

And this is a more sophisticated ARM template which creates a new Log Analytics workspace and then creates the Azure Sentinel onboardingStates resource on top of it:

{

"$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",

"contentVersion": "1.0.0.0",

"parameters": {

"workspaceName": {

"type": "string"

},

"workspaceLocation": {

"type": "string"

}

},

"resources": [

{

"apiVersion": "2017-03-15-preview",

"name": "[parameters('workspaceName')]",

"location": "[parameters('workspaceLocation')]",

"tags": {},

"type": "Microsoft.OperationalInsights/workspaces",

"properties": {

"sku": {

"name": "pergb2018"

}

}

},

{

"name": "[concat(parameters('workspaceName'),'/Microsoft.SecurityInsights/default')]",

"type": "Microsoft.OperationalInsights/workspaces/providers/onboardingStates",

"apiVersion": "2021-03-01-preview",

"properties": {

},

"dependsOn": [

"[resourceId('Microsoft.OperationalInsights/workspaces', parameters('workspaceName'))]"

]

}

]

}

## ARM templates usage for CMK workspaces

It is possible to use ARM templates for onboarding a CMK workspace to Azure Sentinel, however there are some limitations that you should consider.

Since onboarding a CMK workspace is a process which requires a decent amount of time, mainly for creating the dedicated cosmos DB resource for the customer, the Create request for the onboardingStates resource succeeds but the operation would still run asynchronously in the background.

Due to technical limitations, we currently don not support async operations in the Create REST call. This prevents ARM from orchestrating the steps in the template when needed. As a result, if you attempt to create an onboardingStates resource (i.e., onboard Azure Sentinel to a workspace), and then create a resource that depends on Azure Sentinel (for instance an Analytics rule), the rule creation would fail since Azure Sentinel is not ready yet on the workspace.

Therefore, the usage of ARM templates for CMK workspaces is currently limited to onboarding Azure Sentinel only.

# Note on the SecurityInsights solution

As part of onboarding to Azure Sentinel, the SecurityInsights solution is installed on the Log Analytics workspace. If you had the chance to manage your Azure Sentinel resource(s) using the API in the past, you might have manually installed/removed the SecurityInsights solution on/from the workspace. As part of introducing the new OnboardingStates API, this manual management of the solution will no longer be supported. Hence, you should neither install nor remove the SecurityInsights solution directly. Instead, either use the [Azure Portal](https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard#enable-azure-sentinel-) or the OnboardingStates endpoints to manage Azure Sentinel on a workspace.