# DYNAMICSUMMARY

API version: 2023-03-01-preview

## SUMMARY MODEL

| Field | Type | Description | Required? | Editable? |
|---|---|---|---|---|
| **SummaryName** | String | Name of the summary. Each summary must have a unique name within a Sentinel workspace. | True | |
| **SourceInfo** | Dictionary<string,string> | Source information including runtime attributes, query, and lookback, etc.<br><br>Eaxmple:<br>{"source": "Notebooks",<br>"name": "Scheduled Credential Scan on Log Analytics",<br>"version": "1.0"} | | True |
| **SearchKey** | String | Name of a column in your summary that you expect to use as a join with other data or as a frequent object of searches. For example, ObservableType. | | |
| **Tactics** | List<string><br>Enum:<br>　Reconnaissance,<br>　ResourceDevelopment,<br>　InitialAccess,<br>　Execution,<br>　Persistence,<br>　PrivilegeEscalation,<br>　DefenseEvasion,<br>　CredentialAccess,<br>　Discovery,<br>　LateralMovement,<br>　Collection, | MITRE ATT&CK tactics. | | True |

| | | | | |
|---|---|---|---|---|
| | Exfiltration, CommandAndControl, Impact | | | |
| **Techniques** | List<string> | MITRE ATT&CK techniques | | True |
| **RelationName** | String | Name of the source that generates the summary or is linked to the summary. For example, Hunts, Notebooks, Playbooks, etc. | | |
| **SummaryDescription** | String | Description of the summary | | True |
| **RelationId** | String | Identifier of RelationName if RelationName is used. For example, a Hunting session ID. | | |
| **RawContent** | String | Array of Summary Item Models in JSON. Example: "[{ \"EventTimeUtc\": \"2022-04-16T14:22:08Z\", \"ObservableType\": \"IP\", \"ObservableValue\": \"192.168.0.250\", \"RelationId\" : \"Hunting session 123\", \"SearchKey\" : \"ObservableaType\", \"PackedContent\" : {\"SomeKey\" : \"SomeValue\"} }]" | | |
| **Query** | String | KQL query that is used to summarize data. Example: "SigninLogs   &#124; where ResultType == "50057"   &#124; extend Reason =    case(    ResultType == '50057', 'SigninLogs( Result Code- 50057) - User account is disabled. The account has been disabled by an administrator.',    'Unknown'), Account = UserPrincipalName   &#124; project Computer, Account, Reason, TimeGenerated" | | |

| | | | | |
|---|---|---|---|---|
| **QueryStartDate** | DateTime | Start date of the query | | |
| **QueryEndDate** | DateTime | End date of the query | | |

## SUMMARY ITEM MODEL

| Field | Type | Description | Required | Editable |
|---|---|---|---|---|
| **EventTimeUTC** | DateTime | Datetime of the event when it occurred | | |
| **ObservableType** | String | Type of the observable. For example, it can be an entity like IP **Address**, **Host**, **User account**, or non-entity observable such as a **Hunting query**. | | |
| **ObservableValue** | String | Value of the observable. | | |
| **SearchKey** | String | Real value from a column for quick search. For example, "123.25.25.23" as IP address. | | |
| **Tactics** | List<string><br><br>Enum:<br><br>Reconnaissance,<br><br>ResourceDevelopment,<br><br>InitialAccess,<br><br>Execution,<br><br>Persistence,<br><br>PrivilegeEscalation,<br><br>DefenseEvasion,<br><br>CredentialAccess,<br><br>Discovery,<br><br>LateralMovement,<br><br>Collection,<br><br>Exfiltration, | MITRE ATT&CK | | |

| | | CommandAndControl, Impact, PreAttack, ImpairProcessControl, InhibitResponseFunction | | | |
|---|---|---|---|---|---|
| **Techniques** | List<string> | MITRE ATT&CK | | | |
| **RelationName** | String | Name of the source that generates the summary or is linked to the summary. For example, Hunts, Notebooks, Playbooks, etc. | | | |
| **RelationId** | String | Identifier of RelationName if RelationName is used. For example, a Hunting session ID. | | | |
| **PackedContent** | dynamic | For storing extra columns data by using KQL function pack_all() | | | |

## AUTHENTICATION AND AUTHORIZATION

### AZURE_AUTH

Azure Active Directory OAuth2 Flow

**Type:** oauth2
**Flow:** implicit
**Authorization URL:** https://login.microsoftonline.com/common/oauth2/authorize

### SCOPES

| Name | Description |
|---|---|
| **user_impersonation** | impersonate your user account |

The API supports the following operations.

- Create/Update a summary
- Get a summary
- List summaries
- Delete a summary

## CREATE OR UPDATE

Create or update a Summary.

### HTTP

**PUT**
https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers
/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/
dynamicSummaries/**{summaryId}**?api-version=2023-03-01-preview

### URI PARAMETERS

| Name | In | Required | Type | Description |
|------|-----|----------|------|-------------|
| **resourceGroupName** | Path | True | String | The name of the resource group. The name is not case sensitive. |
| **subscriptionId** | Path | True | String | The ID of the target subscription. |
| **summaryId** | Path | True | String | The ID of the summary |
| **workspaceName** | Path | True | String | The name of the workspace. |
| **api-version** | query | true | string | The API version to use for this operation. |

### REQUEST BODY

| Field | Type | Description | Required |
|---|---|---|---|
| **properties.summaryName** | String | The Summary name | true |
| **properties.sourceInfo** | Dictionary<string,string> | Source information including runtime attributes, query, and lookback | |
| **properties.searchKey** | String | Name of a column in your summary that you expect to use as a join with other data or as a frequent object of searches. For example, ObservableType. | |
| **properties.tactics** | List<string><br><br>Acceptable strings:<br><br>Reconnaissance,<br><br>ResourceDevelopment,<br><br>InitialAccess,<br><br>Execution,<br><br>Persistence,<br><br>PrivilegeEscalation,<br><br>DefenseEvasion,<br><br>CredentialAccess,<br><br>Discovery,<br><br>LateralMovement,<br><br>Collection,<br><br>Exfiltration,<br><br>CommandAndControl,<br><br>Impact | MITRE ATT&CK tactics | |
| **properties.techniques** | List<string> | MITRE ATT&CK techniques | |
| **properties.relationName** | String | Name of the source that generates the summary or is linked to the summary | |
| **properties.summaryDescription** | String | Description of summary | |
| **properties.relationId** | String | Identifier of RelationName if RelationName is used. For example, a Hunting session ID. | |
| **properties.rawContent** | String | Array of Summary Item Models in JSON.<br><br>Example:<br><br>"[{ \"EventTimeUtc\": \"2022-04-16T14:22:08Z\", | |

| | | \"ObservableType\": \"IP\", \"ObservableValue\": \"SomeIp\", \"RelationId\" : \"Some Relation\", \"SearchKey\" : \"Some sear\", \"PackedContent\" : {\"SomeKey\" : \"SomeValue\"} }]" | |
|---|---|---|---|
| **Query** | String | KQL query for summary | |
| **properties.queryStartDate** | DateTime | Start date of the query | |
| **properties.queryEndDate** | DateTime | End date of the query | |

## RESPONSES

| Status Code | Type | Description |
|---|---|---|
| **200 OK** | Summary | OK |
| **201 Created** | Summary | Created |
| **Other status codes** | CloudError | Error response describing why the operation failed. |

## EXAMPLE

Create or update a Summary and bulk creates summary items.

### HTTP: PUT

https://management.azure.com/subscriptions/bd794837-1234-5678-0000-6339bfdb4e6a/resourceGroups/example-rg/providers/Microsoft.OperationalInsights/workspaces/example-ws/providers/Microsoft.SecurityInsights/dynamicSummaries/78f81fdc-0097-0001-8178-a99aec5df9df?api-version=2023-03-01-preview

```json
{
    "properties": {
      "summaryName":"My first Summary",
      "SourceInfo":{"key_1":"val_1", "key_2":"val_2"},
      "summaryDescription":"My new summary",
      "SearchKey":"SomeKey",
      "Tactics":["Reconnaissance","Execution"],
      "Query":"Watchlists | take 13",
      "QueryStartDate":"2023-09-25T14:22:08Z",
      "QueryEndDate":"2023-10-25T14:22:08Z",
      "Techniques":[],
      "RelationId":"sampleRelationId",
      "RelationName":"sampleRelationName",
      "rawContent":"[{ \"EventTimeUtc\": \"2022-05-25T14:22:07Z\", \"ObservableType\": \"IP2\", \"ObservableValue\": \"SomeIp\",
\"RelationId\" : \"Some Relation2.1\", \"SearchKey\" : \"Some search\", \"PackedContent\" : {\"SomeKey\" : \"SomeValue\"} }]"
    }
}
```

## RESPONSE

```json
{
  "id": "/subscriptions/bd794837-1234-5678-0000-6339bfdb4e6a/resourceGroups/example-
rg/providers/Microsoft.OperationalInsights/workspaces/example-ws/providers/Microsoft.SecurityInsights/dynamicsummaries/78f81fdc-2005-1006-
8178-a99aec5df9df",
  "name": "78f81fdc-2005-1006-8178-a99aec5df9df",
  "etag": "\"3d006383-0000-0c00-0000-6392aea10000\"",
  "type": "Microsoft.SecurityInsights/dynamicsummaries",
  "properties": {
    "summaryName": "My first Summary",
    "sourceInfo": {
      "key_1": "val_1",
      "key_2": "val_2"
    },
    "searchKey": "SomeKey",
    "tactics": [
      "Reconnaissance",
      "Execution"
    ],
    "techniques": [],
    "relationName": "sampleRelationName",
    "summaryDescription": "My new summary",
    "relationId": "sampleRelationId",
    "query": "Watchlists | take 13",
    "queryStartDate": "2023-09-25T14:22:08Z",
    "queryEndDate": "2023-10-25T14:22:08Z",
    "tenantId": "dd86d426-8d16-42db-81b7-ab578e110ccd",
    "summaryStatus": "Active",
    "provisioningState": "InProgress"
  }
}
```

## DELETE

Delete a summary.

## HTTP

DELETE

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers
/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/
dynamicSummaries/**{summaryId}**?api-version=2023-03-01-preview

## URI PARAMETERS

| Name | In | Required | Type | Description |
|---|---|---|---|---|
| resourceGroupName | Path | True | String | The name of the resource group. The name is not case sensitive. |
| subscriptionId | Path | True | String | The ID of the target subscription. |
| summaryId | Path | True | String | The ID of the summary |
| workspaceName | Path | True | String | The name of the workspace. |
| api-version | query | true | string | The API version to use for this operation. |

## RESPONSES

| Status Code | Type | Description |
|---|---|---|
| **200 OK** | Summary | OK |
| **204 No Content** | Summary | No Content |
| **Other status codes** | CloudError | Error response describing why the operation failed. |

## EXAMPLE

Delete a summary.

## HTTP: DELETE

https://management.azure.com/subscriptions/bd794837-1234-5678-0000-6339bfdb4e6a/resourceGroups/mamahaj-rg/providers/Microsoft.OperationalInsights/workspaces/mm-watchlistestws/providers/Microsoft.SecurityInsights/dynamicSummaries/78f81fdc-0097-0001-8178-a99aec5df9df?api-version=2023-03-01-preview

## RESPONSE

Status code 200 or status code 204

## GET

Get a summary by the summary ID.

## HTTP

GET

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/dynamicSummaries/**{summaryId}**?api-version=2023-03-01-preview

## URI PARAMETERS

| Name | In | Required | Type | Description |
|------|-----|----------|------|-------------|
| **resourceGroupName** | Path | True | String | The name of the resource group. The name is not case sensitive. |
| **subscriptionId** | Path | True | String | The ID of the target subscription. |
| **summaryId** | Path | True | String | The ID of the summary |

| workspaceName | Path | True | String | The name of the workspace. |
|---|---|---|---|---|
| **api-version** | query | true | string | The API version to use for this operation. |

## RESPONSES

| Status Code | Type | Description |
|---|---|---|
| **200 OK** | Summary | OK |
| **Other status codes** | CloudError | Error response describing why the operation failed. |

## EXAMPLE

### HTTP: GET

https://management.azure.com/subscriptions/bd794837-1234-5678-0000-6339bfdb4e6a/resourceGroups/example-rg/providers/Microsoft.OperationalInsights/workspaces/example-ws/providers/Microsoft.SecurityInsights/dynamicSummaries/78f81fdc-0097-0001-8178-a99aec5df9df?api-version=2023-03-01-preview

### RESPONSE

```json
{
  "id": "/subscriptions/bd794837-1234-5678-0000-6339bfdb4e6a/resourceGroups/example-
rg/providers/Microsoft.OperationalInsights/workspaces/example-ws/providers/Microsoft.SecurityInsights/dynamicsummaries/78f81fdc-2005-1006-
8178-a99aec5df9df",
  "name": "78f81fdc-2005-1006-8178-a99aec5df9df",
  "etag": "\"3d006383-0000-0c00-0000-6392aea10000\"",
  "type": "Microsoft.SecurityInsights/dynamicsummaries",
  "properties": {
    "summaryName": "My first Summary",
    "sourceInfo": {
      "key_1": "val_1",
      "key_2": "val_2"
    },
    "searchKey": "SomeKey",
    "tactics": [
      "Reconnaissance",
      "Execution"
    ],
    "techniques": [],
    "relationName": "sampleRelationName",
    "summaryDescription": "My new summary",
    "relationId": "sampleRelationId",
    "query": "Watchlists | take 13",
    "queryStartDate": "2023-09-25T14:22:08Z",
    "queryEndDate": "2023-10-25T14:22:08Z",
    "tenantId": "dd86d426-8d16-42db-81b7-ab578e110ccd",
    "summaryStatus": "Active",
    "provisioningState": "InProgress"
  }
}
```

## LIST

Get all summaries in a Sentinel workspace.

## HTTP

GET

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers
/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/
dynamicSummaries?api-version=2023-03-01-preview

## URI PARAMETERS

| Name | In | Required | Type | Description |
|---|---|---|---|---|
| **resourceGroupName** | Path | True | String | The name of the resource group. The name is not case sensitive. |

| | | | | |
|---|---|---|---|---|
| **subscriptionId** | Path | True | String | The ID of the target subscription. |
| **workspaceName** | Path | True | String | The name of the Sentinel workspace. |
| **api-version** | query | true | string | The API version to use for this operation. |

| Status Code | Type | Description |
|---|---|---|
| **200 OK** | Summary | OK |
| **Other status codes** | CloudError | Error response describing why the operation failed. |

EXAMPLE

HTTP: GET

https://management.azure.com/subscriptions/bd794837-1234-5678-0000-6339bfdb4e6a
/resourceGroups/example-rg/providers/Microsoft.OperationalInsights/workspaces/example-
ws/providers/Microsoft.SecurityInsights/dynamicSummaries?api-version=2023-03-01-preview

RESPONSE

```
{
  "value": [
    {
      "id": "/subscriptions/bd794837-1234-5678-0000-6339bfdb4e6a/resourceGroups/example-
rg/providers/Microsoft.OperationalInsights/workspaces/example-ws/providers/Microsoft.SecurityInsights/dynamicsummaries/78f81fdc-2005-1006-
8178-a99aec5df9df",
      "name": "78f81fdc-2005-1006-8178-a99aec5df9df",
      "etag": "\"3d006383-0000-0c00-0000-6392aea10000\"",
      "type": "Microsoft.SecurityInsights/dynamicsummaries",
      "properties": {
        "summaryName": "My first Summary",
        "sourceInfo": {
          "key_1": "val_1",
          "key_2": "val_2"
        },
        "searchKey": "SomeKey",
        "tactics": [
          "Reconnaissance",
          "Execution"
        ],
        "techniques": [],
        "relationName": "sampleRelationName",
        "summaryDescription": "My new summary",
        "relationId": "sampleRelationId",
        "query": "Watchlists | take 13",
        "queryStartDate": "2023-09-25T14:22:08Z",
        "queryEndDate": "2023-10-25T14:22:08Z",
        "tenantId": "dd86d426-8d16-42db-81b7-ab578e110ccd",
        "summaryStatus": "Active",
        "provisioningState": "InProgress"
      }
    }
  ]
}
```

## RESTRICTIONS AND LIMITATIONS

Beside all the limits for Log Analytics workspaces here, there are more limits in the DynamicSummaries API usage:

- The maximum size for "summaryName", "searchKey", "relationId", "relationName", "observableValue", "observableType" value is 120 characters.
- The maximum size for "summaryDescription" value is 500 characters.
- The "packedContent" value must be JSON.
- The maximum key name length in "packedContnet" is 45.
- The maximum number of keys in "packedContent" is 50.
- The maximum size of the value per key in "packedContent" is 32KB.
- Currently in *V1* the DynamicSummaries service considers all the items in the upload payload as new items. No deduplication mechanism at the moment.
- Your data in LA expires based on your workspace retention period.
- Currently the summary name is not editable.
- The maximum size of the upload payload is 3.8MB.