SecMaster

# API Reference

**Issue** 06

**Date** 2024-03-20

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

## Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

## Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

# Contents



# 1 Before You Start

## 1.1 Overview

SecMaster is a new generation cloud native security operation platform. Based on years of cloud security experience of Huawei Cloud, it enables integrated and automated security operations through cloud asset management, security situation management, security information and event management, security orchestration and automatic response, to prevent security risks, detect security events, and automatically handle security events.

Before calling SecMaster APIs, ensure that you have understood the concepts related to SecMaster. For more details, see **Service Overview**.

## 1.2 API Calling

SecMaster supports Representational State Transfer (REST) APIs, allowing you to call APIs using HTTPS requests. For details about API calling, see **Calling APIs**.

## 1.3 Endpoints

An endpoint is the **request address** for calling an API. Endpoints vary depending on services and regions. For the endpoints of all services, see **Regions and Endpoints**.

## 1.4 Concepts

- Account

  An account is created upon successful registration with the cloud platform. The account has full access permissions for all of its cloud services and resources. It can be used to reset user passwords and grant user permissions. The account is a payment entity and should not be used to perform routine management. For security purposes, create IAM users under the account and grant them permissions for routine management.

- User

  A user is created using a domain to use cloud services. Each user has its own identity credentials (password and access keys).

  The account name, username, and password will be required for API authentication.

- Region

  Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.

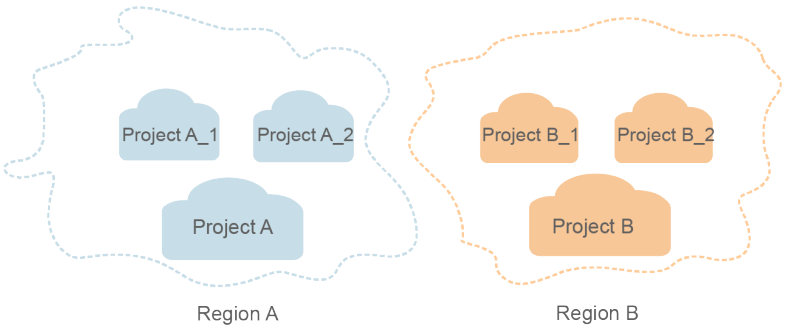
- Availability Zone (AZ)

  An AZ comprises one or multiple physical data centers equipped with independent ventilation, fire, water, and electricity facilities. Compute, network, storage, and other resources in an AZ are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to support cross-AZ high-availability systems.

- Project

  A project corresponds to a region. Projects group and isolate resources (including compute, storage, and network resources) across physical regions. Users can be granted permissions in a default project to access all resources in the region associated with the project. For more refined access control, create subprojects under a project and create resources in the subprojects. Users can then be assigned permissions to access only specific resources in the subprojects.

  **Figure 1-1** Project isolation model

- Enterprise project

  Enterprise projects group and manage resources across regions. Resources in enterprise projects are logically isolated from each other. An enterprise project can contain resources in multiple regions, and resources can be directly transferred between enterprise projects.

  For details about how to obtain enterprise project IDs and features, see **Enterprise Management User Guide**.

# 2 Calling APIs

## 2.1 Making an API Request

This section describes the structure of a REST API request, and uses the IAM API for **obtaining a user token** as an example to demonstrate how to call an API. The obtained token can then be used to authenticate the calling of other APIs.

### Request URI

A request URI is in the following format:

**{URI-scheme} :// {Endpoint} / {resource-path} ? {query-string}**

Although a request URI is included in the request header, most programming languages or frameworks require the request URI to be transmitted separately.

- **URI-scheme**:

  Protocol used to transmit requests. All APIs use HTTPS.
- **Endpoint**:

  Domain name or IP address of the server bearing the REST service. The endpoint varies between services in different regions. It can be obtained from **Regions and Endpoints**.

  For example, the endpoint of IAM in region **CN-Hong Kong** is **iam.ap-southeast-1.myhuaweicloud.com**.
- **resource-path**:

  Access path of an API for performing a specified operation. Obtain the path from the URI of an API. For example, the **resource-path** of the API used to obtain a user token is **/v3/auth/tokens**.
- **query-string**:

  Query parameter, which is optional. Ensure that a question mark (?) is included before each query parameter that is in the format of "Parameter name=Parameter value". For example, **?limit=10** indicates that a maximum of 10 data records will be displayed.

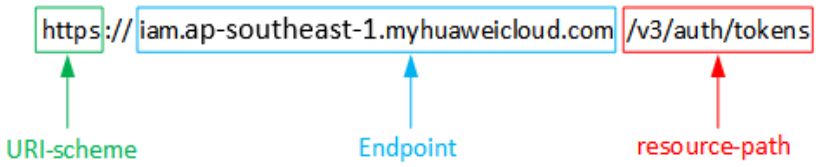
For example, to obtain an IAM token in the **CN-Hong Kong** region, obtain the endpoint of IAM (iam.ap-southeast-1.myhuaweicloud.com)) for this region and

the **resource-path** (**/v3/auth/tokens**) in the URI of the API used to **obtain a user token**. Then, construct the URI as follows:

```
https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
```

**Figure 2-1** Example URI




NOTE

To simplify the URI display in this document, each API is provided only with a **resource-path** and a request method. The **URI-scheme** of all APIs is **HTTPS**, and the endpoints of all APIs in the same region are identical.

## Request Methods

The HTTP protocol defines the following request methods that can be used to send a request to the server:

- **GET**: requests the server to return specified resources.
- **PUT**: requests the server to update specified resources.
- **POST**: requests the server to add resources or perform special operations.
- **DELETE**: requests the server to delete specified resources, for example, an object.
- **HEAD**: same as GET except that the server must return only the response header.
- **PATCH**: requests the server to update partial content of a specified resource. If the resource does not exist, a new resource will be created.

For example, in the case of the API used to **obtain a user token**, the request method is POST. The request is as follows:

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
```

## Request Header

You can also add additional header fields to a request, such as the fields required by a specified URI or HTTP method. For example, to request for the authentication information, add **Content-Type**, which specifies the request body type.

Common request header fields are as follows:

- **Content-Type**: specifies the request body type or format. This field is mandatory and its default value is **application/json**. Other values of this field will be provided for specific APIs if any.
- **X-Auth-Token**: specifies a user token only for token-based API authentication. The user token is a response to the API used to **obtain a user token**. This API is the only one that does not require authentication.

> **NOTE**
>
> In addition to supporting token-based authentication, APIs also support authentication using access key ID/secret access key (AK/SK). During AK/SK-based authentication, an SDK is used to sign the request, and the **Authorization** (signature information) and **X-Sdk-Date** (time when the request is sent) header fields are automatically added to the request.
>
> For more information, see **AK/SK-based Authentication**.

The API used to **obtain a user token** does not require authentication. Therefore, only the **Content-Type** field needs to be added to requests for calling the API. An example of such requests is as follows:

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json
```

## Request Body

The body of a request is often sent in a structured format as specified in the **Content-Type** header field. The request body transfers content except the request header.

The request body varies between APIs. Some APIs do not require the request body, such as the APIs requested using the GET and DELETE methods.

In the case of the API used to **obtain a user token**, the request parameters and parameter description can be obtained from the API request. The following provides an example request with a body included. Set ***username*** to the name of a user, ***domainname*** to the name of the account that the user belongs to, ********* to the user's login password, and ***xxxxxxxxxxxxxxxxx*** to the project name. You can learn more information about projects from **Regions and Endpoints**. Check the value of the **Region** column.

> **NOTE**
>
> The **scope** parameter specifies where a token takes effect. You can set **scope** to an account or a project under an account. In the following example, the token takes effect only for the resources in a specified project. For more information about this API, see **Obtaining a User Token**.

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "username",
                    "password": "*********",
                    "domain": {
                        "name": "domainname"
                    }
                }
            }
        },
        "scope": {
            "project": {
                "name": "xxxxxxxxxxxxxxxxx"
            }
        }
```

```
    }
}
```

If all data required for the API request is available, you can send the request to call the API through **curl**, **Postman**, or coding. In the response to the API used to obtain a user token, **x-subject-token** is the desired user token. This token can then be used to authenticate the calling of other APIs.

# 2.2 Authentication

Requests for calling an API can be authenticated using either of the following methods:

- Token-based authentication: Requests are authenticated using a token.
- AK/SK-based authentication: Requests are authenticated by encrypting the request body using an AK/SK pair. This method is recommended because it provides higher security than token-based authentication.

## Token-based Authentication

NOTE

The validity period of a token is 24 hours. When using a token for authentication, cache it to prevent frequently calling the IAM API used to obtain a user token.

A token specifies temporary permissions in a computer system. During API authentication using a token, the token is added to requests to get permissions for calling the API.

The token can be obtained by calling the required API. For more information, see **Obtaining a User Token**. A project-level token is required for calling this API, that is, **auth.scope** must be set to **project** in the request body. Example:

```
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "username",
                    "password": "********",
                    "domain": {
                        "name": "domainname"
                    }
                }
            }
        },
        "scope": {
            "project": {
                "name": "xxxxxxxx"
            }
        }
    }
}
```

After a token is obtained, the **X-Auth-Token** header field must be added to requests to specify the token when calling other APIs. For example, if the token is **ABCDEFJ....**, **X-Auth-Token: ABCDEFJ....** can be added to a request as follows:

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/projects
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

### AK/SK-based Authentication

NOTE

AK/SK-based authentication supports API requests with a body not larger than 12 MB. For API requests with a larger body, token-based authentication is recommended.

In AK/SK-based authentication, AK/SK is used to sign requests and the signature is then added to the requests for authentication.

- AK: access key ID, which is a unique identifier used in conjunction with a secret access key to sign requests cryptographically.
- SK: secret access key used in conjunction with an AK to sign requests cryptographically. It identifies a request sender and prevents the request from being modified.

In AK/SK-based authentication, you can use an AK/SK to sign requests based on the signature algorithm or use the signing SDK to sign requests. For details about how to sign requests and use the signing SDK, see **API Signature Guide**.

NOTICE

The signing SDK is only used for signing requests and is different from the SDKs provided by services.

## 2.3 Response

### Status Code

After sending a request, you will receive a response, including a status code, response header, and response body.

A status code is a group of digits, ranging from 1xx to 5xx. It indicates the status of a request. For more information, see **Status Codes**.

For example, if status code **201** is returned for calling the API used to **obtain a user token**, the request is successful.

### Response Header

A response header corresponds to a request header, for example, **Content-Type**.

**Figure 2-2** shows the response header fields for the API for **Obtaining a User Token**. The x-subject-token header field is the desired user token. Then, you can use the token to authenticate the calling of other APIs.

**Figure 2-2** Header of the response to the request for obtaining a user token


## (Optional) Response Body

A response body is generally returned in a structured format, corresponding to the **Content-Type** in the response header, and is used to transfer content other than the response header.

The following shows part of the response body for the API to **obtain a user token**. For the sake of space, only part of the content is displayed here.

```
{
    "token": {
        "expires_at": "2019-02-13T06:52:13.855000Z",
        "methods": [
            "password"
        ],
        "catalog": [
            {
                "endpoints": [
                    {
                        "region_id": "xxxxxxxx",
.....
```

If an error occurs during API calling, the system returns an error code and a message to you. The following shows the format of an error response body:

```
{
    "error_msg": "The format of message is error",
    "error_code": "AS.0001"
}
```

In the preceding information, **error_code** is an error code, and **error_msg** describes the error.

# 3 API Overview

You can use all SecMaster functions through VPIs provided by SecMaster.

| Type | Description |
| --- | --- |
| Alarm Rule API | Creates, deletes, views, and enables alarm rules. |
| Alarm API | Creates, deletes, and converts alarms to events. |
| Relationship API | Queries, creates, and deletes relationships. |
| Event API | Creates, updates, and obtains events. |
| Metric API | Queries, creates, and deletes metrics. |
| Playbook API | Queries, creates, and modifies playbooks. |
| Playbook version API | Queries, creates, and updates playbook versions. |
| Playbook review API | Reviews playbooks and queries playbook review results. |
| Playbook rule API | Creates, queries, and deletes playbook rules. |
| Playbook action API | Specifies playbook actions, such as query, creation, and update. |
| Playbook instance API | Queries and operates playbook instances. |

# 4 API

## 4.1 Alert Management

### 4.1.1 Searching for an Alert List

#### Function

Searching for an Alert List

#### Calling Method

For details, see **Calling APIs**.

#### URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/search

**Table 4-1** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

## Request Parameters

**Table 4-2** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **0**<br>Maximum: **2097152** |
| content-type | Yes | String | Content type.<br>Default: **application/json;charset=UTF-8**<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-3** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| limit | No | Integer | Number of records displayed on each page.<br>Minimum: **0**<br>Maximum: **1000** |
| offset | No | Integer | Offset<br>Minimum: **0**<br>Maximum: **1000** |
| sort_by | No | String | Sorting field -- create_time \| update_time<br>Minimum: **0**<br>Maximum: **1000** |
| order | No | String | Sort by -- DESC \| ASC<br>Minimum: **0**<br>Maximum: **1000**<br>Enumeration values:<br>• **DESC**<br>• **ASC** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| from_date | No | String | Search start time, for example, 2023-02-20T00:00:00.000Z<br>Minimum: **0**<br>Maximum: **64** |
| to_date | No | String | Search end time, for example, 2023-02-27T23:59:59.999Z<br>Minimum: **0**<br>Maximum: **64** |
| condition | No | **condition** object | Search condition expression. |

**Table 4-4** condition

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| conditions | No | Array of **conditions** objects | Expression list.<br>Array Length: **0 - 999** |
| logics | No | Array of strings | Expression logic.<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 999** |

**Table 4-5** conditions

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| name | No | String | Expression name.<br>Minimum: **0**<br>Maximum: **64** |
| data | No | Array of strings | Expression content list.<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 999** |

## Response Parameters

**Status code: 200**

**Table 4-6** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-7** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Message<br>Minimum: **0**<br>Maximum: **1024** |
| total | Integer | Total number of alerts.<br>Minimum: **0**<br>Maximum: **10000** |
| limit | Integer | Number of records displayed on each page.<br>Minimum: **0**<br>Maximum: **10000** |
| offset | Integer | Offset<br>Minimum: **0**<br>Maximum: **10000** |
| success | Boolean | Successful or not. |
| data | Array of **ListAlertDetail** objects | Alert list.<br>Array Length: **0 - 10000** |

**Table 4-8** ListAlertDetail

| Parameter | Type | Description |
| --- | --- | --- |
| data_object | **ListAlertRsp** object | Alert details. |
| create_time | String | Create time<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| update_time | String | Update time<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Id value<br>Minimum: **32**<br>Maximum: **64** |
| workspace_id | String | Id value<br>Minimum: **32**<br>Maximum: **64** |
| id | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |
| type | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |
| version | Integer | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |
| format_version | Integer | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |
| dataclass_ref | **dataclass_ref** object | Data class object. |

**Table 4-9** ListAlertRsp

| Parameter | Type | Description |
| --- | --- | --- |
| version | String | Version.<br>Minimum: **1**<br>Maximum: **64** |
| environment | **environment** object | Environment Info |
| data_source | **data_source** object | Data source. |

| Parameter | Type | Description |
| --- | --- | --- |
| first_observed_time | String | Update time<br>Minimum: **0**<br>Maximum: **64** |
| last_observed_time | String | Update time<br>Minimum: **0**<br>Maximum: **64** |
| create_time | String | Create time<br>Minimum: **0**<br>Maximum: **64** |
| arrive_time | String | Update time<br>Minimum: **0**<br>Maximum: **64** |
| title | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |
| description | String | The description, display only<br>Minimum: **0**<br>Maximum: **1024** |
| source_url | String | Incident URL.<br>Minimum: **1**<br>Maximum: **64** |
| count | Integer | Incident occurrences<br>Minimum: **0**<br>Maximum: **5** |
| confidence | Integer | Confidence level<br>Minimum: **0**<br>Maximum: **5** |
| severity | String | Severity.<br>Minimum: **1**<br>Maximum: **64** |
| criticality | Integer | Criticality, which specifies the importance level of the resources involved in an incident.<br>Minimum: **0**<br>Maximum: **5** |
| alert_type | Object | Incident classification. |

| Parameter | Type | Description |
| --- | --- | --- |
| network_list | Array of **network_list** objects | network_list<br>Array Length: **0 - 100** |
| resource_list | Array of **resource_list** objects | network_list<br>Array Length: **0 - 100** |
| remediation | **remediation** object | Remedy measure. |
| verification_state | String | Verification Status<br>Minimum: **1**<br>Maximum: **64** |
| handle_status | String | Incident processing status.<br>Minimum: **1**<br>Maximum: **64** |
| sla | String | sla<br>Minimum: **0**<br>Maximum: **65535** |
| update_time | String | Create time<br>Minimum: **0**<br>Maximum: **64** |
| close_time | String | Create time<br>Minimum: **0**<br>Maximum: **64** |
| chop_phase | String | Period/Handling phase No.<br>Minimum: **4**<br>Maximum: **64** |
| ipdrr_phase | String | Period/Handling phase No.<br>Minimum: **4**<br>Maximum: **64** |
| ppdr_phase | String | Period/Handling phase No.<br>Minimum: **4**<br>Maximum: **64** |
| simulation | String | Whether it is a debugging incident.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| actor | String | Client<br>Minimum: **0**<br>Maximum: **64** |
| owner | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |
| creator | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |
| close_reason | String | Closure Reason<br>Minimum: **32**<br>Maximum: **64** |
| close_comment | String | Closure Reason<br>Minimum: **0**<br>Maximum: **64** |
| malware | **malware** object | Malware |
| system_info | Object | System information. |
| process | Array of **process** objects | Process information.<br>Array Length: **0 - 100** |
| user_info | Array of **user_info** objects | User Details<br>Array Length: **0 - 100** |
| file_info | Array of **file_info** objects | File Information<br>Array Length: **0 - 100** |
| system_alert_table | Object | System information. |
| id | String | Id value<br>Minimum: **32**<br>Maximum: **64** |
| workspace_id | String | workspace id<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-10** environment

| Parameter | Type | Description |
| --- | --- | --- |
| vendor_type | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |
| domain_id | String | Id value<br>Minimum: **32**<br>Maximum: **64** |
| region_id | String | Id value<br>Minimum: **1**<br>Maximum: **64** |
| project_id | String | Id value<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-11** data_source

| Parameter | Type | Description |
| --- | --- | --- |
| source_type | Integer | current page count<br>Minimum: **0**<br>Maximum: **9999** |
| domain_id | String | Id value<br>Minimum: **32**<br>Maximum: **64** |
| project_id | String | Id value<br>Minimum: **32**<br>Maximum: **64** |
| region_id | String | Id value<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-12** network_list

| Parameter | Type | Description |
| --- | --- | --- |
| direction | Object | Direction. The value can be IN or OUT. |

| Parameter | Type | Description |
| --- | --- | --- |
| protocol | String | Protocol. Example- IANA registered name.<br>Minimum: **1**<br>Maximum: **64** |
| src_ip | String | Source IP address<br>Minimum: **0**<br>Maximum: **64** |
| src_port | Integer | Source port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| src_domain | String | Source domain name. The value contains a maximum of 128 characters.<br>Minimum: **0**<br>Maximum: **128** |
| dest_ip | String | Destination IP address<br>Minimum: **0**<br>Maximum: **64** |
| dest_port | String | Destination port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **64** |
| dest_domain | String | Destination domain name. The value contains a maximum of 128 characters.<br>Minimum: **0**<br>Maximum: **128** |
| src_geo | Object | Geographical location of the source IP address. |
| dest_geo | Object | Geographical location of the destination IP address. |

**Table 4-13** resource_list

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Id value<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| name | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |
| type | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |
| domain_id | String | Id value<br>Minimum: **32**<br>Maximum: **64** |
| project_id | String | Id value<br>Minimum: **32**<br>Maximum: **64** |
| region_id | String | Id value<br>Minimum: **0**<br>Maximum: **64** |
| ep_id | String | Id value<br>Minimum: **0**<br>Maximum: **64** |
| ep_name | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |
| tags | String | Id value<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-14** remediation

| Parameter | Type | Description |
| --- | --- | --- |
| recommendation | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |
| url | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-15** malware

| Parameter | Type | Description |
| --- | --- | --- |
| malware_family | String | Malicious family.<br>Minimum: **0**<br>Maximum: **64** |
| malware_class | String | Malware category.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-16** process

| Parameter | Type | Description |
| --- | --- | --- |
| process_name | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |
| process_path | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |
| process_pid | Integer | Id value<br>Minimum: **0**<br>Maximum: **65535** |
| process_uid | Integer | Id value<br>Minimum: **0**<br>Maximum: **65535** |
| process_cmdline | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-17** user_info

| Parameter | Type | Description |
| --- | --- | --- |
| user_id | String | Id value<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| user_name | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-18** file_info

| Parameter | Type | Description |
| --- | --- | --- |
| file_path | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |
| file_content | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |
| file_new_path | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |
| file_hash | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |
| file_md5 | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |
| file_sha256 | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |
| file_attr | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-19** dataclass_ref

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Id value<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| name | String | The name, display only<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 400**

**Table 4-20** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-21** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Example request for querying the alert list. To query the medium-risk alerts in the open state from January 20, 2024 to January 26, 2024, sort the alerts by create time in descending order, return to the first page, with 10 records on each page.

```
{
  "limit" : 10,
  "offset" : 0,
  "sort_by" : "create_time",
  "order" : "DESC",
  "condition" : {
    "conditions" : [ {
      "name" : "severity",
      "data" : [ "severity", "=", "Medium" ]
    }, {
      "name" : "handle_status",
      "data" : [ "handle_status", "=", "Open" ]
    } ],
    "logics" : [ "severity", "and", "handle_status" ]
  },
  "from_date" : "2024-01-20T00:00:00.000Z+0800",
  "to_date" : "2024-01-26T23:59:59.999Z+0800"
}
```

## Example Responses

**Status code: 200**

Response body of the request for searching for alerts.


```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "total" : 41,
  "limit" : 2,
  "offset" : 1,
  "success" : true,
  "data" : [ {
    "data_object" : {
      "version" : "1.0",
      "environment" : {
        "vendor_type" : "MyXXX",
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "data_source" : {
        "source_type" : 3,
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "first_observed_time" : "2021-01-30T23:00:00Z+0800",
      "last_observed_time" : "2021-01-30T23:00:00Z+0800",
      "create_time" : "2021-01-30T23:00:00Z+0800",
      "arrive_time" : "2021-01-30T23:00:00Z+0800",
      "title" : "MyXXX",
      "description" : "This my XXXX",
      "source_url" : "http://xxx",
      "count" : 4,
      "confidence" : 4,
      "severity" : "TIPS",
      "criticality" : 4,
      "alert_type" : { },
      "network_list" : [ {
        "direction" : {
          "IN" : null
        },
        "protocol" : "TCP",
        "src_ip" : "192.168.0.1",
        "src_port" : "1",
        "src_domain" : "xxx",
        "dest_ip" : "192.168.0.1",
        "dest_port" : "1",
        "dest_domain" : "xxx",
        "src_geo" : {
          "latitude" : 90,
          "longitude" : 180
        },
        "dest_geo" : {
          "latitude" : 90,
          "longitude" : 180
        }
      } ],
      "resource_list" : [ {
        "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "name" : "MyXXX",
        "type" : "MyXXX",
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "ep_name" : "MyXXX",
```

```
      "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    } ],
    "remediation" : {
      "recommendation" : "MyXXX",
      "url" : "MyXXX"
    },
    "verification_state" : "Unknown,True_Positive,False_Positive The default value is Unknown.",
    "handle_status" : "Open – enabled.Block – blocked.Closed – closed.The default value is Open.",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "Preparation | Detection and Analysis | Containment, Eradication&Recovery | Post-
Incident-Activity",
    "simulation" : "false",
    "actor" : "Tom",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "False positive; Resolved; Duplicate; Others",
    "close_comment" : "False positive; Resolved; Duplicate; Others",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "Malicious memory occupation."
    },
    "system_info" : { },
    "process" : [ {
      "process_name" : "MyXXX",
      "process_path" : "MyXXX",
      "process_pid" : 123,
      "process_uid" : 123,
      "process_cmdline" : "MyXXX"
    } ],
    "user_info" : [ {
      "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "user_name" : "MyXXX"
    } ],
    "file_info" : [ {
      "file_path" : "MyXXX",
      "file_content" : "MyXXX",
      "file_new_path" : "MyXXX",
      "file_hash" : "MyXXX",
      "file_md5" : "MyXXX",
      "file_sha256" : "MyXXX",
      "file_attr" : "MyXXX"
    } ],
    "system_alert_table" : { },
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
  },
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "id" : "MyXXX",
  "version" : 123,
  "format_version" : 123,
  "dataclass_ref" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX"
  }
 } ]
}
```


## SDK Sample Code

The SDK sample code is as follows.

## Java

Example request for querying the alert list. To query the medium-risk alerts in the open state from January 20, 2024 to January 26, 2024, sort the alerts by create time in descending order, return to the first page, with 10 records on each page.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class ListAlertsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListAlertsRequest request = new ListAlertsRequest();
        DataobjectSearch body = new DataobjectSearch();
        List<String> listConditionLogics = new ArrayList<>();
        listConditionLogics.add("severity");
        listConditionLogics.add("and");
        listConditionLogics.add("handle_status");
        List<String> listConditionsData = new ArrayList<>();
        listConditionsData.add("handle_status");
        listConditionsData.add("=");
        listConditionsData.add("Open");
        List<String> listConditionsData1 = new ArrayList<>();
        listConditionsData1.add("severity");
        listConditionsData1.add("=");
        listConditionsData1.add("Medium");
        List<DataobjectSearchConditionConditions> listConditionConditions = new ArrayList<>();
        listConditionConditions.add(
            new DataobjectSearchConditionConditions()
                .withName("severity")
                .withData(listConditionsData1)
        );
        listConditionConditions.add(
            new DataobjectSearchConditionConditions()
                .withName("handle_status")
                .withData(listConditionsData)
        );
        DataobjectSearchCondition conditionbody = new DataobjectSearchCondition();
        conditionbody.withConditions(listConditionConditions)
            .withLogics(listConditionLogics);
        body.withCondition(conditionbody);
        body.withToDate("2024-01-26T23:59:59.999Z+0800");
```

```
        body.withFromDate("2024-01-20T00:00:00.000Z+0800");
        body.withOrder(DataobjectSearch.OrderEnum.fromValue("DESC"));
        body.withSortBy("create_time");
        body.withOffset(0);
        body.withLimit(10);
        request.withBody(body);
        try {
            ListAlertsResponse response = client.listAlerts(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Example request for querying the alert list. To query the medium-risk alerts in the open state from January 20, 2024 to January 26, 2024, sort the alerts by create time in descending order, return to the first page, with 10 records on each page.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListAlertsRequest()
        listLogicsCondition = [
            "severity",
            "and",
            "handle_status"
        ]
        listDataConditions = [
            "handle_status",
            "=",
            "Open"
        ]
        listDataConditions1 = [
            "severity",
            "=",
            "Medium"
```

```
        ]
        listConditionsCondition = [
            DataobjectSearchConditionConditions(
                name="severity",
                data=listDataConditions1
            ),
            DataobjectSearchConditionConditions(
                name="handle_status",
                data=listDataConditions
            )
        ]
        conditionbody = DataobjectSearchCondition(
            conditions=listConditionsCondition,
            logics=listLogicsCondition
        )
        request.body = DataobjectSearch(
            condition=conditionbody,
            to_date="2024-01-26T23:59:59.999Z+0800",
            from_date="2024-01-20T00:00:00.000Z+0800",
            order="DESC",
            sort_by="create_time",
            offset=0,
            limit=10
        )
        response = client.list_alerts(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Example request for querying the alert list. To query the medium-risk alerts in the open state from January 20, 2024 to January 26, 2024, sort the alerts by create time in descending order, return to the first page, with 10 records on each page.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())
```

```
    request := &model.ListAlertsRequest{}
    var listLogicsCondition = []string{
        "severity",
        "and",
        "handle_status",
    }
    var listDataConditions = []string{
        "handle_status",
        "=",
        "Open",
    }
    var listDataConditions1 = []string{
        "severity",
        "=",
        "Medium",
    }
    nameConditions:= "severity"
    nameConditions1:= "handle_status"
    var listConditionsCondition = []model.DataobjectSearchConditionConditions{
        {
            Name: &nameConditions,
            Data: &listDataConditions1,
        },
        {
            Name: &nameConditions1,
            Data: &listDataConditions,
        },
    }
    conditionbody := &model.DataobjectSearchCondition{
        Conditions: &listConditionsCondition,
        Logics: &listLogicsCondition,
    }
    toDateDataobjectSearch:= "2024-01-26T23:59:59.999Z+0800"
    fromDateDataobjectSearch:= "2024-01-20T00:00:00.000Z+0800"
    orderDataobjectSearch:= model.GetDataobjectSearchOrderEnum().DESC
    sortByDataobjectSearch:= "create_time"
    offsetDataobjectSearch:= int32(0)
    limitDataobjectSearch:= int32(10)
    request.Body = &model.DataobjectSearch{
        Condition: conditionbody,
        ToDate: &toDateDataobjectSearch,
        FromDate: &fromDateDataobjectSearch,
        Order: &orderDataobjectSearch,
        SortBy: &sortByDataobjectSearch,
        Offset: &offsetDataobjectSearch,
        Limit: &limitDataobjectSearch,
    }
    response, err := client.ListAlerts(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

### Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response body of the request for searching for alerts. |
| 400 | Response body for request failures of searching for alerts. |

### Error Codes

See **Error Codes**.

## 4.1.2 Creating an Alert Rule

### Function

Creating an Alert Rule

### Calling Method

For details, see **Calling APIs**.

### URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts

**Table 4-22** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

## Request Parameters

**Table 4-23** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **0**<br>Maximum: **2097152** |
| content-type | Yes | String | Content type.<br>Default: **application/json;charset=UTF-8**<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-24** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| data_object | Yes | **Alert** object | Alert entity information. |

**Table 4-25** Alert

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| version | No | String | Version of the data source of the alert. The value must be one officially released by the Huawei Cloud SSA service.<br>Minimum: **0**<br>Maximum: **64** |
| id | No | String | Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| domain_id | No | String | ID of the account (domain_id) to whom the data is delivered and hosted.<br>Minimum: **0**<br>Maximum: **36** |
| region_id | No | String | ID of the region where the account to whom the data is delivered and hosted belongs to.<br>Minimum: **0**<br>Maximum: **36** |
| workspace_id | No | String | ID of the current workspace.<br>Minimum: **0**<br>Maximum: **36** |
| labels | No | String | Tag (display only)<br>Minimum: **0**<br>Maximum: **1024** |
| environment | No | **environment** object | Coordinates of the environment where the alert was generated. |
| data_source | No | **data_source** object | Source the data is first reported. |
| first_observed_time | No | String | First discovery time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| last_observed_time | No | String | First discovery time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| create_time | No | String | Recording time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| arrive_time | No | String | Data receiving time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| title | No | String | Alert title.<br>Minimum: **0**<br>Maximum: **255** |
| description | No | String | Alert description.<br>Minimum: **0**<br>Maximum: **1024** |
| source_url | No | String | Alert URL, which points to the page of the current incident description in the data source product.<br>Minimum: **0**<br>Maximum: **1024** |
| count | No | Integer | Incident occurrences<br>Minimum: **0**<br>Maximum: **999** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| confidence | No | Integer | Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or incident. Value range -- 0-100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.<br>Minimum: **0**<br>Maximum: **100** |
| severity | No | String | Severity level. Value range: Tips \| Low \| Medium \| High \| Fatal Description:<br>• **0**: TIPS: No threats are found.<br>• **1**: LOW: No actions are required for the threat.<br>• **2**: MEDIUM: The threat needs to be handled but is not urgent.<br>• **3**: HIGH: The threat must be handled preferentially.<br>• **4**: FATAL: The threat must be handled immediately to prevent further damage.<br>Minimum: **3**<br>Maximum: **6**<br>Enumeration values:<br>• **Tips**<br>• **Low**<br>• **Medium**<br>• **High**<br>• **Fatal** |
| criticality | No | Integer | Criticality, which specifies the importance level of the resources involved in an incident. Value range -- 0 to 100. The value 0 indicates that the resource is not critical, and 100 indicates that the resource is critical.<br>Minimum: **0**<br>Maximum: **100** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| alert_type | No | **alert_type** object | Alert classification. For details, see the Alert Type Definition. |
| network_list | No | Array of **network_list** objects | Network Information<br>Array Length: **0 - 999** |
| resource_list | No | Array of **resource_list** objects | Affected resources.<br>Array Length: **0 - 999** |
| remediation | No | **remediation** object | Remedy measure. |
| verification_state | No | String | Verification status, which identifies the accuracy of an incident. The options are as follows: – Unknown – True_Positive – False_Positive Enter Unknown by default.<br>Minimum: **32**<br>Maximum: **64**<br>Enumeration values:<br>• **Unknown**<br>• **True_Positive**<br>• **False_Positive** |
| handle_status | No | String | Incident handling status. The options are as follows:<br>• Open: enabled.<br>• Block: blocked.<br>• Closed: closed. The default value is Open.<br>Minimum: **4**<br>Maximum: **5**<br>Enumeration values:<br>• **Open**<br>• **Block**<br>• **Closed** |
| sla | No | Integer | Risk close time -- Set the acceptable risk duration. Unit -- Hour<br>Minimum: **0**<br>Maximum: **999** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| update_time | No | String | Update time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the alert occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| close_time | No | String | Closing time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| ipdrr_phase | No | String | Period/Handling phase No. Prepartion\|Detection and Analysis\|Containm, Eradication& Recovery\|Post-Incident-Activity<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **Prepartion**<br>• **Detection and Analysis**<br>• **Containm, Eradication& Recovery**<br>• **Post-Incident-Activity** |
| simulation | No | String | Debugging field.<br>Minimum: **0**<br>Maximum: **64** |
| actor | No | String | Alert investigator.<br>Minimum: **0**<br>Maximum: **64** |
| owner | No | String | Owner and service owner.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| creator | No | String | Creator<br>Minimum: **0**<br>Maximum: **64** |
| close_reason | No | String | Close reason.<br>• False positive.<br>• Resolved<br>• Repeated<br>• Other<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **False detection**<br>• **Resolved**<br>• **Repeated**<br>• **Other** |
| close_comment | No | String | Whether to close comment.<br>Minimum: **0**<br>Maximum: **1024** |
| malware | No | **malware** object | Malware |
| system_info | No | Object | System information. |
| process | No | Array of **process** objects | Process information.<br>Array Length: **0 - 999** |
| user_info | No | Array of **user_info** objects | User Details<br>Array Length: **0 - 999** |
| file_info | No | Array of **file_info** objects | Document information.<br>Array Length: **0 - 999** |
| system_alert_table | No | Object | Layout fields in the alerts list. |

**Table 4-26** environment

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| vendor_type | No | String | Environment provider. The value can be **HWCP**, **HWC**, **AWS**, **Azure**, or **GCP**.<br>Minimum: **0**<br>Maximum: **64** |
| domain_id | No | String | Tenant ID.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | No | String | Region ID. **global** is returned for global services.<br>Minimum: **0**<br>Maximum: **64** |
| cross_workspace_id | No | String | ID of the source workspace for the data delivery. If the source workspace ID is null, then the destination workspace account ID is used.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | No | String | Project ID. The default value is null for global services.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-27** data_source

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| source_type | No | Integer | Data source type. The options are as follows-- 1- Huawei product 2- Third-party product 3- Tenant product<br>Minimum: **1**<br>Maximum: **3**<br>Enumeration values:<br>• **1**<br>• **2**<br>• **3** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| domain_id | No | String | Account ID to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | No | String | ID of the project to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | No | String | Region where the data source is located, for example, cn-north1. For details about the value range, see *Regions and Endpoints*.<br>Minimum: **0**<br>Maximum: **64** |
| company_name | No | String | Name of the company to which a data source belongs.<br>Minimum: **0**<br>Maximum: **16** |
| product_name | No | String | Name of the data source.<br>Minimum: **0**<br>Maximum: **24** |
| product_feature | No | String | Name of the feature of the product that detects the incident.<br>Minimum: **0**<br>Maximum: **24** |
| product_module | No | String | Threat detection module list.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-28** alert_type

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| category | No | String | Type<br>Minimum: **0**<br>Maximum: **1024** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| alert_type | No | String | Alert type.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-29** network_list

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| direction | No | String | Direction. The value can be IN or OUT.<br>Minimum: **0**<br>Maximum: **3**<br>Enumeration values:<br>• **IN**<br>• **OUT** |
| protocol | No | String | Protocol, including Layer 7 and Layer 4 protocols. For details, see IANA registered name. https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.<br>Minimum: **0**<br>Maximum: **64** |
| src_ip | No | String | Source IP address<br>Minimum: **0**<br>Maximum: **64** |
| src_port | No | Integer | Source port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| src_domain | No | String | Source domain name.<br>Minimum: **0**<br>Maximum: **128** |
| src_geo | No | **src_geo** object | Geographical location of the source IP address. |
| dest_ip | No | String | Destination IP address<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| dest_port | No | String | Destination port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| dest_domain | No | String | Destination domain name<br>Minimum: **0**<br>Maximum: **128** |
| dest_geo | No | **dest_geo** object | Geographical location of the destination IP address. |

**Table 4-30** src_geo

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| latitude | No | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | No | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | No | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | No | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-31** dest_geo

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| latitude | No | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| longitude | No | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | No | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | No | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-32** resource_list

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| id | No | String | Cloud service resource ID.<br>Minimum: **0**<br>Maximum: **36** |
| name | No | String | Resource name.<br>Minimum: **0**<br>Maximum: **255** |
| type | No | String | Resource type. This parameter references the value of RMS type on Huawei Cloud.<br>Minimum: **0**<br>Maximum: **64** |
| provider | No | String | Cloud service name, which is the same as the provider field in the RMS service.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | No | String | Region ID in Huawei Cloud, for example, cn-north-1.<br>Minimum: **0**<br>Maximum: **36** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| domain_id | No | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | No | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| ep_id | No | String | Specifies the enterprise project ID.<br>Minimum: **0**<br>Maximum: **128** |
| ep_name | No | String | Enterprise Project Name<br>Minimum: **0**<br>Maximum: **128** |
| tags | No | String | Resource tag.<br>1. A maximum of 50 key/value pairs are supported.<br>2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _, :, /,@<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-33** remediation

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| recommendation | No | String | Recommended solution.<br>Minimum: **0**<br>Maximum: **128** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| url | No | String | Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-34** malware

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| malware_family | No | String | Malicious family.<br>Minimum: **0**<br>Maximum: **64** |
| malware_class | No | String | Malware category.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-35** process

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| process_name | No | String | Process name.<br>Minimum: **0**<br>Maximum: **64** |
| process_path | No | String | Process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_pid | No | Integer | Process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_uid | No | Integer | Process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_cmdline | No | String | Process command line.<br>Minimum: **0**<br>Maximum: **128** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| process_parent_name | No | String | Parent process name.<br>Minimum: **0**<br>Maximum: **64** |
| process_parent_path | No | String | Parent process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_parent_pid | No | Integer | Parent process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_parent_uid | No | Integer | Parent process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_parent_cmdline | No | String | Parent process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_child_name | No | String | Subprocess name.<br>Minimum: **0**<br>Maximum: **64** |
| process_child_path | No | String | Subprocess execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_child_pid | No | Integer | Subprocess ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_child_uid | No | Integer | Subprocess user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_child_cmdline | No | String | Subprocess command line<br>Minimum: **0**<br>Maximum: **128** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| process_launche_time | No | String | Incident start time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| process_terminate_time | No | String | Process end time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

**Table 4-36** user_info

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| user_id | No | String | User UID<br>Minimum: **0**<br>Maximum: **36** |
| user_name | No | String | Username<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-37** file_info

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| file_path | No | String | File path/name.<br>Minimum: **0**<br>Maximum: **128** |
| file_content | No | String | File path/name.<br>Minimum: **0**<br>Maximum: **1024** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| file_new_path | No | String | New file path/name.<br>Minimum: **32**<br>Maximum: **64** |
| file_hash | No | String | File Hash<br>Minimum: **0**<br>Maximum: **128** |
| file_md5 | No | String | File MD5<br>Minimum: **0**<br>Maximum: **128** |
| file_sha256 | No | String | File SHA256<br>Minimum: **0**<br>Maximum: **128** |
| file_attr | No | String | File attribute.<br>Minimum: **0**<br>Maximum: **1024** |

## Response Parameters

**Status code: 200**

**Table 4-38** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-39** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Message<br>Minimum: **0**<br>Maximum: **1024** |

| Parameter | Type | Description |
| --- | --- | --- |
| data | **AlertDetail** object | |

**Table 4-40** AlertDetail

| Parameter | Type | Description |
| --- | --- | --- |
| create_time | String | Recording time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| data_object | **Alert** object | Alert entity information. |
| dataclass_ref | **dataclass_ref** object | Data class object. |
| format_version | Integer | Format version.<br>Minimum: **0**<br>Maximum: **999** |
| id | String | Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | String | ID of the current project.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Update time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| version | Integer | Version.<br>Minimum: **0**<br>Maximum: **999** |

| Parameter | Type | Description |
| --- | --- | --- |
| workspace_id | String | ID of the current workspace.<br>Minimum: **0**<br>Maximum: **36** |

**Table 4-41** Alert

| Parameter | Type | Description |
| --- | --- | --- |
| version | String | Version of the data source of the alert. The value must be one officially released by the Huawei Cloud SSA service.<br>Minimum: **0**<br>Maximum: **64** |
| id | String | Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | String | ID of the account (domain_id) to whom the data is delivered and hosted.<br>Minimum: **0**<br>Maximum: **36** |
| region_id | String | ID of the region where the account to whom the data is delivered and hosted belongs to.<br>Minimum: **0**<br>Maximum: **36** |
| workspace_id | String | ID of the current workspace.<br>Minimum: **0**<br>Maximum: **36** |
| labels | String | Tag (display only)<br>Minimum: **0**<br>Maximum: **1024** |
| environment | **environment** object | Coordinates of the environment where the alert was generated. |
| data_source | **data_source** object | Source the data is first reported. |

| Parameter | Type | Description |
| --- | --- | --- |
| first_observed_time | String | First discovery time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| last_observed_time | String | First discovery time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| create_time | String | Recording time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| arrive_time | String | Data receiving time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| title | String | Alert title.<br>Minimum: **0**<br>Maximum: **255** |
| description | String | Alert description.<br>Minimum: **0**<br>Maximum: **1024** |
| source_url | String | Alert URL, which points to the page of the current incident description in the data source product.<br>Minimum: **0**<br>Maximum: **1024** |

| Parameter | Type | Description |
| --- | --- | --- |
| count | Integer | Incident occurrences<br>Minimum: **0**<br>Maximum: **999** |
| confidence | Integer | Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or incident. Value range -- 0-100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.<br>Minimum: **0**<br>Maximum: **100** |
| severity | String | Severity level. Value range: Tips \| Low \| Medium \| High \| Fatal Description:<br>• **0**: TIPS: No threats are found.<br>• **1**: LOW: No actions are required for the threat.<br>• **2**: MEDIUM: The threat needs to be handled but is not urgent.<br>• **3**: HIGH: The threat must be handled preferentially.<br>• **4**: FATAL: The threat must be handled immediately to prevent further damage.<br>Minimum: **3**<br>Maximum: **6**<br>Enumeration values:<br>• **Tips**<br>• **Low**<br>• **Medium**<br>• **High**<br>• **Fatal** |
| criticality | Integer | Criticality, which specifies the importance level of the resources involved in an incident. Value range -- 0 to 100. The value 0 indicates that the resource is not critical, and 100 indicates that the resource is critical.<br>Minimum: **0**<br>Maximum: **100** |
| alert_type | **alert_type** object | Alert classification. For details, see the Alert Type Definition. |
| network_list | Array of **network_list** objects | Network Information<br>Array Length: **0 - 999** |

| Parameter | Type | Description |
| --- | --- | --- |
| resource_list | Array of **resource_list** objects | Affected resources.<br>Array Length: **0 - 999** |
| remediation | **remediation** object | Remedy measure. |
| verification_state | String | Verification status, which identifies the accuracy of an incident. The options are as follows: – Unknown – True_Positive – False_Positive Enter Unknown by default.<br>Minimum: **32**<br>Maximum: **64**<br>Enumeration values:<br>• **Unknown**<br>• **True_Positive**<br>• **False_Positive** |
| handle_status | String | Incident handling status. The options are as follows:<br>• Open: enabled.<br>• Block: blocked.<br>• Closed: closed. The default value is Open.<br>Minimum: **4**<br>Maximum: **5**<br>Enumeration values:<br>• **Open**<br>• **Block**<br>• **Closed** |
| sla | Integer | Risk close time -- Set the acceptable risk duration. Unit -- Hour<br>Minimum: **0**<br>Maximum: **999** |
| update_time | String | Update time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the alert occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |

| Parameter | Type | Description |
| --- | --- | --- |
| close_time | String | Closing time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| ipdrr_phase | String | Period/Handling phase No. Prepartion\| Detection and Analysis\|Containm, Eradication& Recovery\|Post-Incident-Activity<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **Prepartion**<br>• **Detection and Analysis**<br>• **Containm, Eradication& Recovery**<br>• **Post-Incident-Activity** |
| simulation | String | Debugging field.<br>Minimum: **0**<br>Maximum: **64** |
| actor | String | Alert investigator.<br>Minimum: **0**<br>Maximum: **64** |
| owner | String | Owner and service owner.<br>Minimum: **0**<br>Maximum: **64** |
| creator | String | Creator<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| close_reason | String | Close reason.<br>• False positive.<br>• Resolved<br>• Repeated<br>• Other<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **False detection**<br>• **Resolved**<br>• **Repeated**<br>• **Other** |
| close_comment | String | Whether to close comment.<br>Minimum: **0**<br>Maximum: **1024** |
| malware | **malware** object | Malware |
| system_info | Object | System information. |
| process | Array of **process** objects | Process information.<br>Array Length: **0 - 999** |
| user_info | Array of **user_info** objects | User Details<br>Array Length: **0 - 999** |
| file_info | Array of **file_info** objects | Document information.<br>Array Length: **0 - 999** |
| system_alert_table | Object | Layout fields in the alerts list. |

**Table 4-42** environment

| Parameter | Type | Description |
| --- | --- | --- |
| vendor_type | String | Environment provider. The value can be **HWCP**, **HWC**, **AWS**, **Azure**, or **GCP**.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| domain_id | String | Tenant ID.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region ID. **global** is returned for global services.<br>Minimum: **0**<br>Maximum: **64** |
| cross_workspace_id | String | ID of the source workspace for the data delivery. If the source workspace ID is null, then the destination workspace account ID is used.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID. The default value is null for global services.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-43** data_source

| Parameter | Type | Description |
| --- | --- | --- |
| source_type | Integer | Data source type. The options are as follows--1- Huawei product 2- Third-party product 3- Tenant product<br>Minimum: **1**<br>Maximum: **3**<br>Enumeration values:<br>• **1**<br>• **2**<br>• **3** |
| domain_id | String | Account ID to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | String | ID of the project to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| region_id | String | Region where the data source is located, for example, cn-north1. For details about the value range, see *Regions and Endpoints*.<br>Minimum: **0**<br>Maximum: **64** |
| company_name | String | Name of the company to which a data source belongs.<br>Minimum: **0**<br>Maximum: **16** |
| product_name | String | Name of the data source.<br>Minimum: **0**<br>Maximum: **24** |
| product_feature | String | Name of the feature of the product that detects the incident.<br>Minimum: **0**<br>Maximum: **24** |
| product_module | String | Threat detection module list.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-44** alert_type

| Parameter | Type | Description |
| --- | --- | --- |
| category | String | Type<br>Minimum: **0**<br>Maximum: **1024** |
| alert_type | String | Alert type.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-45** network_list

| Parameter | Type | Description |
| --- | --- | --- |
| direction | String | Direction. The value can be IN or OUT.<br>Minimum: **0**<br>Maximum: **3**<br>Enumeration values:<br>• **IN**<br>• **OUT** |
| protocol | String | Protocol, including Layer 7 and Layer 4 protocols. For details, see IANA registered name. https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.<br>Minimum: **0**<br>Maximum: **64** |
| src_ip | String | Source IP address<br>Minimum: **0**<br>Maximum: **64** |
| src_port | Integer | Source port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| src_domain | String | Source domain name.<br>Minimum: **0**<br>Maximum: **128** |
| src_geo | **src_geo** object | Geographical location of the source IP address. |
| dest_ip | String | Destination IP address<br>Minimum: **32**<br>Maximum: **64** |
| dest_port | String | Destination port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| dest_domain | String | Destination domain name<br>Minimum: **0**<br>Maximum: **128** |
| dest_geo | **dest_geo** object | Geographical location of the destination IP address. |

**Table 4-46** src_geo

| Parameter | Type | Description |
| --- | --- | --- |
| latitude | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-47** dest_geo

| Parameter | Type | Description |
| --- | --- | --- |
| latitude | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-48** resource_list

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Cloud service resource ID.<br>Minimum: **0**<br>Maximum: **36** |
| name | String | Resource name.<br>Minimum: **0**<br>Maximum: **255** |
| type | String | Resource type. This parameter references the value of RMS type on Huawei Cloud.<br>Minimum: **0**<br>Maximum: **64** |
| provider | String | Cloud service name, which is the same as the provider field in the RMS service.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region ID in Huawei Cloud, for example, cn-north-1.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| ep_id | String | Specifies the enterprise project ID.<br>Minimum: **0**<br>Maximum: **128** |
| ep_name | String | Enterprise Project Name<br>Minimum: **0**<br>Maximum: **128** |

| Parameter | Type | Description |
| --- | --- | --- |
| tags | String | Resource tag.<br>1. A maximum of 50 key/value pairs are supported.<br>2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _, :, /,@<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-49** remediation

| Parameter | Type | Description |
| --- | --- | --- |
| recommendation | String | Recommended solution.<br>Minimum: **0**<br>Maximum: **128** |
| url | String | Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-50** malware

| Parameter | Type | Description |
| --- | --- | --- |
| malware_family | String | Malicious family.<br>Minimum: **0**<br>Maximum: **64** |
| malware_class | String | Malware category.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-51** process

| Parameter | Type | Description |
| --- | --- | --- |
| process_name | String | Process name.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| process_path | String | Process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_pid | Integer | Process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_uid | Integer | Process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_cmdline | String | Process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_parent_name | String | Parent process name.<br>Minimum: **0**<br>Maximum: **64** |
| process_parent_path | String | Parent process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_parent_pid | Integer | Parent process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_parent_uid | Integer | Parent process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_parent_cmdline | String | Parent process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_child_name | String | Subprocess name.<br>Minimum: **0**<br>Maximum: **64** |
| process_child_path | String | Subprocess execution file path.<br>Minimum: **0**<br>Maximum: **512** |

| Parameter | Type | Description |
| --- | --- | --- |
| process_child_pid | Integer | Subprocess ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_child_uid | Integer | Subprocess user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_child_cmdline | String | Subprocess command line<br>Minimum: **0**<br>Maximum: **128** |
| process_launche_time | String | Incident start time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| process_terminate_time | String | Process end time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

**Table 4-52** user_info

| Parameter | Type | Description |
| --- | --- | --- |
| user_id | String | User UID<br>Minimum: **0**<br>Maximum: **36** |
| user_name | String | Username<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-53** file_info

| Parameter | Type | Description |
| --- | --- | --- |
| file_path | String | File path/name.<br>Minimum: **0**<br>Maximum: **128** |
| file_content | String | File path/name.<br>Minimum: **0**<br>Maximum: **1024** |
| file_new_path | String | New file path/name.<br>Minimum: **32**<br>Maximum: **64** |
| file_hash | String | File Hash<br>Minimum: **0**<br>Maximum: **128** |
| file_md5 | String | File MD5<br>Minimum: **0**<br>Maximum: **128** |
| file_sha256 | String | File SHA256<br>Minimum: **0**<br>Maximum: **128** |
| file_attr | String | File attribute.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-54** dataclass_ref

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Unique identifier of a data class. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| name | String | Data class name.<br>Minimum: **0**<br>Maximum: **36** |

**Status code: 400**

**Table 4-55** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-56** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Create an alarm. Set Alarm Name to MyXXX, Tag to MyXXX, URL to http://xxx, Number of occurrences to 4, Confidence to 4, and Severity to tips.

```
{
  "data_object" : {
    "version" : "1.0",
    "environment" : {
      "vendor_type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "data_source" : {
      "source_type" : 3,
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "product_name" : "test",
      "product_feature" : "test"
    },
    "first_observed_time" : "2021-01-30T23:00:00Z+0800",
    "last_observed_time" : "2021-01-30T23:00:00Z+0800",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "arrive_time" : "2021-01-30T23:00:00Z+0800",
    "title" : "MyXXX",
    "labels" : "MyXXX",
    "description" : "This my XXXX",
    "source_url" : "http://xxx",
    "count" : 4,
    "confidence" : 4,
    "severity" : "TIPS",
    "criticality" : 4,
    "alert_type" : { },
    "network_list" : [ {
      "direction" : {
        "IN" : null
      },
```

```
    "protocol" : "TCP",
    "src_ip" : "192.168.0.1",
    "src_port" : "1",
    "src_domain" : "xxx",
    "dest_ip" : "192.168.0.1",
    "dest_port" : "1",
    "dest_domain" : "xxx",
    "src_geo" : {
      "latitude" : 90,
      "longitude" : 180
    },
    "dest_geo" : {
      "latitude" : 90,
      "longitude" : 180
    }
  } ],
  "resource_list" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "type" : "MyXXX",
    "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "ep_name" : "MyXXX",
    "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  } ],
  "remediation" : {
    "recommendation" : "MyXXX",
    "url" : "MyXXX"
  },
  "verification_state" : "Unknown,True_Positive,False_Positive The default value is Unknown.",
  "handle_status" : "Open – enabled.Block – blocked.Closed – closed.The default value is Open.",
  "sla" : 60000,
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "close_time" : "2021-01-30T23:00:00Z+0800",
  "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm, Eradication& Recovery| Post-Incident-
Activity",
  "simulation" : "false",
  "actor" : "Tom",
  "owner" : "MyXXX",
  "creator" : "MyXXX",
  "close_reason" : "False positive; Resolved; Duplicate; Others",
  "close_comment" : "False positive; Resolved; Duplicate; Others",
  "malware" : {
    "malware_family" : "family",
    "malware_class" : "Malicious memory occupation."
  },
  "system_info" : { },
  "process" : [ {
    "process_name" : "MyXXX",
    "process_path" : "MyXXX",
    "process_pid" : 123,
    "process_uid" : 123,
    "process_cmdline" : "MyXXX"
  } ],
  "user_info" : [ {
    "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "user_name" : "MyXXX"
  } ],
  "file_info" : [ {
    "file_path" : "MyXXX",
    "file_content" : "MyXXX",
    "file_new_path" : "MyXXX",
    "file_hash" : "MyXXX",
    "file_md5" : "MyXXX",
    "file_sha256" : "MyXXX",
    "file_attr" : "MyXXX"
  } ],
```

```
    "system_alert_table" : { },
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
  }
}
```

## Example Responses

### Status code: 200

Response body of the request for creating alerts.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "data_object" : {
      "version" : "1.0",
      "environment" : {
        "vendor_type" : "MyXXX",
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "data_source" : {
        "source_type" : 3,
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "first_observed_time" : "2021-01-30T23:00:00Z+0800",
      "last_observed_time" : "2021-01-30T23:00:00Z+0800",
      "create_time" : "2021-01-30T23:00:00Z+0800",
      "arrive_time" : "2021-01-30T23:00:00Z+0800",
      "title" : "MyXXX",
      "description" : "This my XXXX",
      "source_url" : "http://xxx",
      "count" : 4,
      "confidence" : 4,
      "severity" : "TIPS",
      "criticality" : 4,
      "alert_type" : { },
      "network_list" : [ {
        "direction" : {
          "IN" : null
        },
        "protocol" : "TCP",
        "src_ip" : "192.168.0.1",
        "src_port" : "1",
        "src_domain" : "xxx",
        "dest_ip" : "192.168.0.1",
        "dest_port" : "1",
        "dest_domain" : "xxx",
        "src_geo" : {
          "latitude" : 90,
          "longitude" : 180
        },
        "dest_geo" : {
          "latitude" : 90,
          "longitude" : 180
        }
      } ],
      "resource_list" : [ {
        "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "name" : "MyXXX",
        "type" : "MyXXX",
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
```

```
      "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_name" : "MyXXX",
      "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    } ],
    "remediation" : {
      "recommendation" : "MyXXX",
      "url" : "MyXXX"
    },
    "verification_state" : "Unknown,True_Positive,False_Positive The default value is Unknown.",
    "handle_status" : "Open – enabled.Block – blocked.Closed – closed.The default value is Open.",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "Preparation | Detection and Analysis | Containment, Eradication&Recovery | Post-
Incident-Activity",
    "simulation" : "false",
    "actor" : "Tom",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "False positive; Resolved; Duplicate; Others",
    "close_comment" : "False positive; Resolved; Duplicate; Others",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "Malicious memory occupation."
    },
    "system_info" : { },
    "process" : [ {
      "process_name" : "MyXXX",
      "process_path" : "MyXXX",
      "process_pid" : 123,
      "process_uid" : 123,
      "process_cmdline" : "MyXXX"
    } ],
    "user_info" : [ {
      "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "user_name" : "MyXXX"
    } ],
    "file_info" : [ {
      "file_path" : "MyXXX",
      "file_content" : "MyXXX",
      "file_new_path" : "MyXXX",
      "file_hash" : "MyXXX",
      "file_md5" : "MyXXX",
      "file_sha256" : "MyXXX",
      "file_attr" : "MyXXX"
    } ],
    "system_alert_table" : { },
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
  },
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "id" : "MyXXX",
  "version" : 123,
  "format_version" : 123,
  "dataclass_ref" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX"
  }
 }
}
```


## SDK Sample Code

The SDK sample code is as follows.

## Java

Create an alarm. Set Alarm Name to MyXXX, Tag to MyXXX, URL to http://xxx, Number of occurrences to 4, Confidence to 4, and Severity to tips.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class CreateAlertSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateAlertRequest request = new CreateAlertRequest();
        CreateAlertRequestBody body = new CreateAlertRequestBody();
        List<AlertFileInfo> listDataObjectFileInfo = new ArrayList<>();
        listDataObjectFileInfo.add(
            new AlertFileInfo()
                .withFilePath("MyXXX")
                .withFileContent("MyXXX")
                .withFileNewPath("MyXXX")
                .withFileHash("MyXXX")
                .withFileMd5("MyXXX")
                .withFileSha256("MyXXX")
                .withFileAttr("MyXXX")
        );
        List<AlertUserInfo> listDataObjectUserInfo = new ArrayList<>();
        listDataObjectUserInfo.add(
            new AlertUserInfo()
                .withUserId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withUserName("MyXXX")
        );
        List<AlertProcess> listDataObjectProcess = new ArrayList<>();
        listDataObjectProcess.add(
            new AlertProcess()
                .withProcessName("MyXXX")
                .withProcessPath("MyXXX")
                .withProcessPid(123)
                .withProcessUid(123)
                .withProcessCmdline("MyXXX")
        );
        AlertMalware malwareDataObject = new AlertMalware();
        malwareDataObject.withMalwareFamily("family")
            .withMalwareClass("Malicious memory occupation.");
```

```
AlertRemediation remediationDataObject = new AlertRemediation();
remediationDataObject.withRecommendation("MyXXX")
    .withUrl("MyXXX");
List<AlertResourceList> listDataObjectResourceList = new ArrayList<>();
listDataObjectResourceList.add(
    new AlertResourceList()
        .withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withName("MyXXX")
        .withType("MyXXX")
        .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withEpId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withEpName("MyXXX")
        .withTags("909494e3-558e-46b6-a9eb-07a8e18ca62f")
);
AlertDestGeo destGeoNetworkList = new AlertDestGeo();
destGeoNetworkList.withLatitude(java.math.BigDecimal.valueOf(90))
    .withLongitude(java.math.BigDecimal.valueOf(180));
AlertSrcGeo srcGeoNetworkList = new AlertSrcGeo();
srcGeoNetworkList.withLatitude(java.math.BigDecimal.valueOf(90))
    .withLongitude(java.math.BigDecimal.valueOf(180));
List<AlertNetworkList> listDataObjectNetworkList = new ArrayList<>();
listDataObjectNetworkList.add(
    new AlertNetworkList()
        .withDirection(AlertNetworkList.DirectionEnum.fromValue("{}"))
        .withProtocol("TCP")
        .withSrcIp("192.168.0.1")
        .withSrcPort(1)
        .withSrcDomain("xxx")
        .withSrcGeo(srcGeoNetworkList)
        .withDestIp("192.168.0.1")
        .withDestPort("1")
        .withDestDomain("xxx")
        .withDestGeo(destGeoNetworkList)
);
AlertDataSource dataSourceDataObject = new AlertDataSource();
dataSourceDataObject.withSourceType(3)
    .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withProductName("test")
    .withProductFeature("test");
AlertEnvironment environmentDataObject = new AlertEnvironment();
environmentDataObject.withVendorType("MyXXX")
    .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
Alert dataObjectbody = new Alert();
dataObjectbody.withVersion("1.0")
    .withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withWorkspaceId("909494e3-558e-46b6-a9eb-07a8e18ca620")
    .withLabels("MyXXX")
    .withEnvironment(environmentDataObject)
    .withDataSource(dataSourceDataObject)
    .withFirstObservedTime("2021-01-30T23:00:00Z+0800")
    .withLastObservedTime("2021-01-30T23:00:00Z+0800")
    .withCreateTime("2021-01-30T23:00:00Z+0800")
    .withArriveTime("2021-01-30T23:00:00Z+0800")
    .withTitle("MyXXX")
    .withDescription("This my XXXX")
    .withSourceUrl("http://xxx")
    .withCount(4)
    .withConfidence(4)
    .withSeverity(Alert.SeverityEnum.fromValue("TIPS"))
    .withCriticality(4)
    .withNetworkList(listDataObjectNetworkList)
    .withResourceList(listDataObjectResourceList)
    .withRemediation(remediationDataObject)
```

```
            .withVerificationState(Alert.VerificationStateEnum.fromValue("Unknown,True_Positive,False_Positive
The default value is Unknown."))
            .withHandleStatus(Alert.HandleStatusEnum.fromValue("Open – enabled.Block – blocked.Closed –
closed.The default value is Open."))
            .withSla(60000)
            .withUpdateTime("2021-01-30T23:00:00Z+0800")
            .withCloseTime("2021-01-30T23:00:00Z+0800")
            .withIpdrrPhase(Alert.IpdrrPhaseEnum.fromValue("Prepartion|Detection and Analysis|
Containm,Eradication& Recovery| Post-Incident-Activity"))
            .withSimulation("false")
            .withActor("Tom")
            .withOwner("MyXXX")
            .withCreator("MyXXX")
            .withCloseReason(Alert.CloseReasonEnum.fromValue("False positive; Resolved; Duplicate; Others"))
            .withCloseComment("False positive; Resolved; Duplicate; Others")
            .withMalware(malwareDataObject)
            .withSystemInfo(new Object())
            .withProcess(listDataObjectProcess)
            .withUserInfo(listDataObjectUserInfo)
            .withFileInfo(listDataObjectFileInfo)
            .withSystemAlertTable(new Object());
        body.withDataObject(dataObjectbody);
        request.withBody(body);
        try {
            CreateAlertResponse response = client.createAlert(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Create an alarm. Set Alarm Name to MyXXX, Tag to MyXXX, URL to http://xxx, Number of occurrences to 4, Confidence to 4, and Severity to tips.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
```

```
request = CreateAlertRequest()
listFileInfoDataObject = [
    AlertFileInfo(
        file_path="MyXXX",
        file_content="MyXXX",
        file_new_path="MyXXX",
        file_hash="MyXXX",
        file_md5="MyXXX",
        file_sha256="MyXXX",
        file_attr="MyXXX"
    )
]
listUserInfoDataObject = [
    AlertUserInfo(
        user_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        user_name="MyXXX"
    )
]
listProcessDataObject = [
    AlertProcess(
        process_name="MyXXX",
        process_path="MyXXX",
        process_pid=123,
        process_uid=123,
        process_cmdline="MyXXX"
    )
]
malwareDataObject = AlertMalware(
    malware_family="family",
    malware_class="Malicious memory occupation."
)
remediationDataObject = AlertRemediation(
    recommendation="MyXXX",
    url="MyXXX"
)
listResourceListDataObject = [
    AlertResourceList(
        id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        name="MyXXX",
        type="MyXXX",
        region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        ep_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        ep_name="MyXXX",
        tags="909494e3-558e-46b6-a9eb-07a8e18ca62f"
    )
]
destGeoNetworkList = AlertDestGeo(
    latitude=90,
    longitude=180
)
srcGeoNetworkList = AlertSrcGeo(
    latitude=90,
    longitude=180
)
listNetworkListDataObject = [
    AlertNetworkList(
        direction="{}",
        protocol="TCP",
        src_ip="192.168.0.1",
        src_port=1,
        src_domain="xxx",
        src_geo=srcGeoNetworkList,
        dest_ip="192.168.0.1",
        dest_port="1",
        dest_domain="xxx",
        dest_geo=destGeoNetworkList
    )
```

```
        ]
        dataSourceDataObject = AlertDataSource(
            source_type=3,
            domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            product_name="test",
            product_feature="test"
        )
        environmentDataObject = AlertEnvironment(
            vendor_type="MyXXX",
            domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f"
        )
        dataObjectbody = Alert(
            version="1.0",
            id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            workspace_id="909494e3-558e-46b6-a9eb-07a8e18ca620",
            labels="MyXXX",
            environment=environmentDataObject,
            data_source=dataSourceDataObject,
            first_observed_time="2021-01-30T23:00:00Z+0800",
            last_observed_time="2021-01-30T23:00:00Z+0800",
            create_time="2021-01-30T23:00:00Z+0800",
            arrive_time="2021-01-30T23:00:00Z+0800",
            title="MyXXX",
            description="This my XXXX",
            source_url="http://xxx",
            count=4,
            confidence=4,
            severity="TIPS",
            criticality=4,
            network_list=listNetworkListDataObject,
            resource_list=listResourceListDataObject,
            remediation=remediationDataObject,
            verification_state="Unknown,True_Positive,False_Positive The default value is Unknown.",
            handle_status="Open – enabled.Block – blocked.Closed – closed.The default value is Open.",
            sla=60000,
            update_time="2021-01-30T23:00:00Z+0800",
            close_time="2021-01-30T23:00:00Z+0800",
            ipdrr_phase="Prepartion|Detection and Analysis|Containm,Eradication& Recovery| Post-Incident-
Activity",
            simulation="false",
            actor="Tom",
            owner="MyXXX",
            creator="MyXXX",
            close_reason="False positive; Resolved; Duplicate; Others",
            close_comment="False positive; Resolved; Duplicate; Others",
            malware=malwareDataObject,
            system_info={},
            process=listProcessDataObject,
            user_info=listUserInfoDataObject,
            file_info=listFileInfoDataObject,
            system_alert_table={}
        )
        request.body = CreateAlertRequestBody(
            data_object=dataObjectbody
        )
        response = client.create_alert(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Create an alarm. Set Alarm Name to MyXXX, Tag to MyXXX, URL to http://xxx, Number of occurrences to 4, Confidence to 4, and Severity to tips.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateAlertRequest{}
    filePathFileInfo:= "MyXXX"
    fileContentFileInfo:= "MyXXX"
    fileNewPathFileInfo:= "MyXXX"
    fileHashFileInfo:= "MyXXX"
    fileMd5FileInfo:= "MyXXX"
    fileSha256FileInfo:= "MyXXX"
    fileAttrFileInfo:= "MyXXX"
    var listFileInfoDataObject = []model.AlertFileInfo{
        {
            FilePath: &filePathFileInfo,
            FileContent: &fileContentFileInfo,
            FileNewPath: &fileNewPathFileInfo,
            FileHash: &fileHashFileInfo,
            FileMd5: &fileMd5FileInfo,
            FileSha256: &fileSha256FileInfo,
            FileAttr: &fileAttrFileInfo,
        },
    }
    userIdUserInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    userNameUserInfo:= "MyXXX"
    var listUserInfoDataObject = []model.AlertUserInfo{
        {
            UserId: &userIdUserInfo,
            UserName: &userNameUserInfo,
        },
    }
    processNameProcess:= "MyXXX"
    processPathProcess:= "MyXXX"
    processPidProcess:= int32(123)
    processUidProcess:= int32(123)
    processCmdlineProcess:= "MyXXX"
    var listProcessDataObject = []model.AlertProcess{
        {
```

```
        ProcessName: &processNameProcess,
        ProcessPath: &processPathProcess,
        ProcessPid: &processPidProcess,
        ProcessUid: &processUidProcess,
        ProcessCmdline: &processCmdlineProcess,
    },
}
malwareFamilyMalware:= "family"
malwareClassMalware:= "Malicious memory occupation."
malwareDataObject := &model.AlertMalware{
    MalwareFamily: &malwareFamilyMalware,
    MalwareClass: &malwareClassMalware,
}
recommendationRemediation:= "MyXXX"
urlRemediation:= "MyXXX"
remediationDataObject := &model.AlertRemediation{
    Recommendation: &recommendationRemediation,
    Url: &urlRemediation,
}
idResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
nameResourceList:= "MyXXX"
typeResourceList:= "MyXXX"
regionIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
domainIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
projectIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
epIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
epNameResourceList:= "MyXXX"
tagsResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
var listResourceListDataObject = []model.AlertResourceList{
    {
        Id: &idResourceList,
        Name: &nameResourceList,
        Type: &typeResourceList,
        RegionId: &regionIdResourceList,
        DomainId: &domainIdResourceList,
        ProjectId: &projectIdResourceList,
        EpId: &epIdResourceList,
        EpName: &epNameResourceList,
        Tags: &tagsResourceList,
    },
}
latitudeDestGeo:= float32(90)
longitudeDestGeo:= float32(180)
destGeoNetworkList := &model.AlertDestGeo{
    Latitude: &latitudeDestGeo,
    Longitude: &longitudeDestGeo,
}
latitudeSrcGeo:= float32(90)
longitudeSrcGeo:= float32(180)
srcGeoNetworkList := &model.AlertSrcGeo{
    Latitude: &latitudeSrcGeo,
    Longitude: &longitudeSrcGeo,
}
directionNetworkList:= model.GetAlertNetworkListDirectionEnum().{}
protocolNetworkList:= "TCP"
srcIpNetworkList:= "192.168.0.1"
srcPortNetworkList:= int32(1)
srcDomainNetworkList:= "xxx"
destIpNetworkList:= "192.168.0.1"
destPortNetworkList:= "1"
destDomainNetworkList:= "xxx"
var listNetworkListDataObject = []model.AlertNetworkList{
    {
        Direction: &directionNetworkList,
        Protocol: &protocolNetworkList,
        SrcIp: &srcIpNetworkList,
        SrcPort: &srcPortNetworkList,
        SrcDomain: &srcDomainNetworkList,
        SrcGeo: srcGeoNetworkList,
```

```
            DestIp: &destIpNetworkList,
            DestPort: &destPortNetworkList,
            DestDomain: &destDomainNetworkList,
            DestGeo: destGeoNetworkList,
        },
    }
    sourceTypeDataSource:= int32(3)
    domainIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    projectIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    regionIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    productNameDataSource:= "test"
    productFeatureDataSource:= "test"
    dataSourceDataObject := &model.AlertDataSource{
        SourceType: &sourceTypeDataSource,
        DomainId: &domainIdDataSource,
        ProjectId: &projectIdDataSource,
        RegionId: &regionIdDataSource,
        ProductName: &productNameDataSource,
        ProductFeature: &productFeatureDataSource,
    }
    vendorTypeEnvironment:= "MyXXX"
    domainIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    regionIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    projectIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    environmentDataObject := &model.AlertEnvironment{
        VendorType: &vendorTypeEnvironment,
        DomainId: &domainIdEnvironment,
        RegionId: &regionIdEnvironment,
        ProjectId: &projectIdEnvironment,
    }
    versionDataObject:= "1.0"
    idDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    workspaceIdDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca620"
    labelsDataObject:= "MyXXX"
    firstObservedTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    lastObservedTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    createTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    arriveTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    titleDataObject:= "MyXXX"
    descriptionDataObject:= "This my XXXX"
    sourceUrlDataObject:= "http://xxx"
    countDataObject:= int32(4)
    confidenceDataObject:= int32(4)
    severityDataObject:= model.GetAlertSeverityEnum().TIPS
    criticalityDataObject:= int32(4)
    verificationStateDataObject:=
model.GetAlertVerificationStateEnum().UNKNOWN,TRUE_POSITIVE,FALSE_POSITIVE_THE_DEFAULT_VALUE_I
S_UNKNOWN_
    handleStatusDataObject:= model.GetAlertHandleStatusEnum().OPEN_-_ENABLED_BLOCK_-
_BLOCKED_CLOSED_-_CLOSED_THE_DEFAULT_VALUE_IS_OPEN_
    slaDataObject:= int32(60000)
    updateTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    closeTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    ipdrrPhaseDataObject:= model.GetAlertIpdrrPhaseEnum().PREPARTION|DETECTION_AND_ANALYSIS|
CONTAINM,ERADICATION&_RECOVERY|_POST_INCIDENT_ACTIVITY
    simulationDataObject:= "false"
    actorDataObject:= "Tom"
    ownerDataObject:= "MyXXX"
    creatorDataObject:= "MyXXX"
    closeReasonDataObject:=
model.GetAlertCloseReasonEnum().FALSE_POSITIVE;_RESOLVED;_DUPLICATE;_OTHERS
    closeCommentDataObject:= "False positive; Resolved; Duplicate; Others"
    var systemInfoDataObject interface{} = make(map[string]string)
    var systemAlertTableDataObject interface{} = make(map[string]string)
    dataObjectbody := &model.Alert{
        Version: &versionDataObject,
        Id: &idDataObject,
        WorkspaceId: &workspaceIdDataObject,
        Labels: &labelsDataObject,
```

```
        Environment: environmentDataObject,
        DataSource: dataSourceDataObject,
        FirstObservedTime: &firstObservedTimeDataObject,
        LastObservedTime: &lastObservedTimeDataObject,
        CreateTime: &createTimeDataObject,
        ArriveTime: &arriveTimeDataObject,
        Title: &titleDataObject,
        Description: &descriptionDataObject,
        SourceUrl: &sourceUrlDataObject,
        Count: &countDataObject,
        Confidence: &confidenceDataObject,
        Severity: &severityDataObject,
        Criticality: &criticalityDataObject,
        NetworkList: &listNetworkListDataObject,
        ResourceList: &listResourceListDataObject,
        Remediation: remediationDataObject,
        VerificationState: &verificationStateDataObject,
        HandleStatus: &handleStatusDataObject,
        Sla: &slaDataObject,
        UpdateTime: &updateTimeDataObject,
        CloseTime: &closeTimeDataObject,
        IpdrrPhase: &ipdrrPhaseDataObject,
        Simulation: &simulationDataObject,
        Actor: &actorDataObject,
        Owner: &ownerDataObject,
        Creator: &creatorDataObject,
        CloseReason: &closeReasonDataObject,
        CloseComment: &closeCommentDataObject,
        Malware: malwareDataObject,
        SystemInfo: &systemInfoDataObject,
        Process: &listProcessDataObject,
        UserInfo: &listUserInfoDataObject,
        FileInfo: &listFileInfoDataObject,
        SystemAlertTable: &systemAlertTableDataObject,
    }
    request.Body = &model.CreateAlertRequestBody{
        DataObject: dataObjectbody,
    }
    response, err := client.CreateAlert(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response body of the request for creating alerts. |
| 400 | Response body of the request for creating alerts. |

## Error Codes

See **Error Codes**.

# 4.1.3 Deleting an Alert

## Function

Deleting an Alert

## Calling Method

For details, see **Calling APIs**.

## URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/alerts

**Table 4-57** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

## Request Parameters

**Table 4-58** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **0**<br>Maximum: **2097152** |
| content-type | Yes | String | Content type.<br>Default: **application/json;charset=UTF-8**<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-59** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| batch_ids | No | Array of strings | IDs of deleted alerts<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 999** |

## Response Parameters

**Status code: 200**

**Table 4-60** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-61** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Message<br>Minimum: **0**<br>Maximum: **1024** |
| data | **BatchOperateAlertResult** object | Returned object for batch operation on alerts. |

**Table 4-62** BatchOperateAlertResult

| Parameter | Type | Description |
| --- | --- | --- |
| error_ids | Array of strings | IDs of alerts not transferred to incidents<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 100** |

| Parameter | Type | Description |
| --- | --- | --- |
| success_ids | Array of strings | IDs of alerts transferred to incidents.<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 100** |

**Status code: 400**

**Table 4-63** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-64** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Delete the alert whose ID is 909494e3-558e-46b6-a9eb-07a8e18ca621.

```
{
  "batch_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ]
}
```

## Example Responses

**Status code: 200**

Body of the request for deleting alerts.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "success_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ],
    "error_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ]
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Delete the alert whose ID is 909494e3-558e-46b6-a9eb-07a8e18ca621.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class DeleteAlertSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteAlertRequest request = new DeleteAlertRequest();
        DeleteAlertRequestBody body = new DeleteAlertRequestBody();
        List<String> listbodyBatchIds = new ArrayList<>();
        listbodyBatchIds.add("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withBatchIds(listbodyBatchIds);
        request.withBody(body);
        try {
            DeleteAlertResponse response = client.deleteAlert(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Delete the alert whose ID is 909494e3-558e-46b6-a9eb-07a8e18ca621.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteAlertRequest()
        listBatchIdsbody = [
            "909494e3-558e-46b6-a9eb-07a8e18ca62f"
        ]
        request.body = DeleteAlertRequestBody(
            batch_ids=listBatchIdsbody
        )
        response = client.delete_alert(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Delete the alert whose ID is 909494e3-558e-46b6-a9eb-07a8e18ca621.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
```

```
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

    request := &model.DeleteAlertRequest{}
    var listBatchIdsbody = []string{
        "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    }
    request.Body = &model.DeleteAlertRequestBody{
        BatchIds: &listBatchIdsbody,
    }
    response, err := client.DeleteAlert(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

### More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

### Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Body of the request for deleting alerts. |
| 400 | Response body of the failed request for deleting alerts. |

### Error Codes

See **Error Codes**.

## 4.1.4 This API is used to convert alerts to incidents.

### Function

This API is used to convert alerts to incidents.

### Calling Method

For details, see **Calling APIs**.

### URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/batch-order

**Table 4-65** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

## Request Parameters

**Table 4-66** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **0**<br>Maximum: **2097152** |
| content-type | Yes | String | Content type.<br>Default: **application/json;charset=UTF-8**<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-67** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| ids | No | Array of strings | IDs of the alerts to be converted into incidents.<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 999** |
| incident_content | No | **incident_content** object | Incident details. |

**Table 4-68** incident_content

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| title | No | String | Trace<br>Minimum: **0**<br>Maximum: **255** |
| incident_type | No | **incident_type** object | Incident type. |

**Table 4-69** incident_type

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| id | No | String | Incident type ID<br>Minimum: **0**<br>Maximum: **255** |
| category | No | String | Parent incident type.<br>Minimum: **0**<br>Maximum: **255** |
| incident_type | No | String | Child incident type.<br>Minimum: **0**<br>Maximum: **255** |

## Response Parameters

**Status code: 200**

**Table 4-70** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-71** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| message | String | Error Message<br>Minimum: **0**<br>Maximum: **1024** |
| data | **BatchOperateAlertResult** object | Returned object for batch operation on alerts. |

**Table 4-72** BatchOperateAlertResult

| Parameter | Type | Description |
| --- | --- | --- |
| error_ids | Array of strings | IDs of alerts not transferred to incidents<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 100** |
| success_ids | Array of strings | IDs of alerts transferred to incidents.<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 100** |

**Status code: 400**

**Table 4-73** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-74** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Convert an alert to an incident, set Alert ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, Incident ID to 909494e3-558e-46b6-a9eb-07a8e18ca621, Alert status to Closed, and Mark as Evidence to No.

```
{
  "ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ],
  "incident_content" : {
    "title" : "XXX",
    "incident_type" : {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "category" : "DDoS attack",
      "incident_type" : "DNS protocol attacks"
    }
  }
}
```

## Example Responses

**Status code: 200**

Response body for converting alerts into incidents.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "error_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ],
    "success_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ]
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Convert an alert to an incident, set Alert ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, Incident ID to 909494e3-558e-46b6-a9eb-07a8e18ca621, Alert status to Closed, and Mark as Evidence to No.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class CreateBatchOrderAlertsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
```

```
this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateBatchOrderAlertsRequest request = new CreateBatchOrderAlertsRequest();
        OrderAlert body = new OrderAlert();
        OrderAlertIncidentContentIncidentType incidentTypeIncidentContent = new
OrderAlertIncidentContentIncidentType();
        incidentTypeIncidentContent.withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withCategory("DDoS attack")
            .withIncidentType("DNS protocol attacks");
        OrderAlertIncidentContent incidentContentbody = new OrderAlertIncidentContent();
        incidentContentbody.withTitle("XXX")
            .withIncidentType(incidentTypeIncidentContent);
        List<String> listbodyIds = new ArrayList<>();
        listbodyIds.add("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withIncidentContent(incidentContentbody);
        body.withIds(listbodyIds);
        request.withBody(body);
        try {
            CreateBatchOrderAlertsResponse response = client.createBatchOrderAlerts(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Convert an alert to an incident, set Alert ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, Incident ID to 909494e3-558e-46b6-a9eb-07a8e18ca621, Alert status to Closed, and Mark as Evidence to No.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \
```

```
    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateBatchOrderAlertsRequest()
        incidentTypeIncidentContent = OrderAlertIncidentContentIncidentType(
            id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            category="DDoS attack",
            incident_type="DNS protocol attacks"
        )
        incidentContentbody = OrderAlertIncidentContent(
            title="XXX",
            incident_type=incidentTypeIncidentContent
        )
        listIdsbody = [
            "909494e3-558e-46b6-a9eb-07a8e18ca62f"
        ]
        request.body = OrderAlert(
            incident_content=incidentContentbody,
            ids=listIdsbody
        )
        response = client.create_batch_order_alerts(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Convert an alert to an incident, set Alert ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, Incident ID to 909494e3-558e-46b6-a9eb-07a8e18ca621, Alert status to Closed, and Mark as Evidence to No.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateBatchOrderAlertsRequest{}
```

```
    idIncidentType:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    categoryIncidentType:= "DDoS attack"
    incidentTypeIncidentType:= "DNS protocol attacks"
    incidentTypeIncidentContent := &model.OrderAlertIncidentContentIncidentType{
        Id: &idIncidentType,
        Category: &categoryIncidentType,
        IncidentType: &incidentTypeIncidentType,
    }
    titleIncidentContent:= "XXX"
    incidentContentbody := &model.OrderAlertIncidentContent{
        Title: &titleIncidentContent,
        IncidentType: incidentTypeIncidentContent,
    }
    var listIdsbody = []string{
        "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    }
    request.Body = &model.OrderAlert{
        IncidentContent: incidentContentbody,
        Ids: &listIdsbody,
    }
    response, err := client.CreateBatchOrderAlerts(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response body for converting alerts into incidents. |
| 400 | Response body for failures of converting alerts into incidents. |

## Error Codes

See **Error Codes**.

# 4.1.5 Querying Alert Detail

## Function

Querying Alert Detail

## Calling Method

For details, see **Calling APIs**.

## URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/{alert_id}

**Table 4-75** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| alert_id | Yes | String | Alert ID.<br>Minimum: **32**<br>Maximum: **36** |

## Request Parameters

**Table 4-76** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **0**<br>Maximum: **2097152** |
| content-type | Yes | String | Content type.<br>Default: **application/json;charset=UTF-8**<br>Minimum: **0**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-77** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-78** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Message<br>Minimum: **0**<br>Maximum: **1024** |
| data | **AlertDetail** object | |

**Table 4-79** AlertDetail

| Parameter | Type | Description |
| --- | --- | --- |
| create_time | String | Recording time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| data_object | **Alert** object | Alert entity information. |
| dataclass_ref | **dataclass_ref** object | Data class object. |
| format_version | Integer | Format version.<br>Minimum: **0**<br>Maximum: **999** |
| id | String | Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |

| Parameter | Type | Description |
| --- | --- | --- |
| project_id | String | ID of the current project.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Update time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| version | Integer | Version.<br>Minimum: **0**<br>Maximum: **999** |
| workspace_id | String | ID of the current workspace.<br>Minimum: **0**<br>Maximum: **36** |

**Table 4-80** Alert

| Parameter | Type | Description |
| --- | --- | --- |
| version | String | Version of the data source of the alert. The value must be one officially released by the Huawei Cloud SSA service.<br>Minimum: **0**<br>Maximum: **64** |
| id | String | Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | String | ID of the account (domain_id) to whom the data is delivered and hosted.<br>Minimum: **0**<br>Maximum: **36** |
| region_id | String | ID of the region where the account to whom the data is delivered and hosted belongs to.<br>Minimum: **0**<br>Maximum: **36** |

| Parameter | Type | Description |
| --- | --- | --- |
| workspace_id | String | ID of the current workspace.<br>Minimum: **0**<br>Maximum: **36** |
| labels | String | Tag (display only)<br>Minimum: **0**<br>Maximum: **1024** |
| environment | **environment** object | Coordinates of the environment where the alert was generated. |
| data_source | **data_source** object | Source the data is first reported. |
| first_observed_time | String | First discovery time. The format is ISO 8601-YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| last_observed_time | String | First discovery time. The format is ISO 8601-YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| create_time | String | Recording time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| arrive_time | String | Data receiving time. The format is ISO 8601-YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

| Parameter | Type | Description |
| --- | --- | --- |
| title | String | Alert title.<br>Minimum: **0**<br>Maximum: **255** |
| description | String | Alert description.<br>Minimum: **0**<br>Maximum: **1024** |
| source_url | String | Alert URL, which points to the page of the current incident description in the data source product.<br>Minimum: **0**<br>Maximum: **1024** |
| count | Integer | Incident occurrences<br>Minimum: **0**<br>Maximum: **999** |
| confidence | Integer | Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or incident. Value range -- 0-100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.<br>Minimum: **0**<br>Maximum: **100** |
| severity | String | Severity level. Value range: Tips \| Low \| Medium \| High \| Fatal Description:<br>• **0**: TIPS: No threats are found.<br>• **1**: LOW: No actions are required for the threat.<br>• **2**: MEDIUM: The threat needs to be handled but is not urgent.<br>• **3**: HIGH: The threat must be handled preferentially.<br>• **4**: FATAL: The threat must be handled immediately to prevent further damage.<br>Minimum: **3**<br>Maximum: **6**<br>Enumeration values:<br>• **Tips**<br>• **Low**<br>• **Medium**<br>• **High**<br>• **Fatal** |

| Parameter | Type | Description |
| --- | --- | --- |
| criticality | Integer | Criticality, which specifies the importance level of the resources involved in an incident. Value range -- 0 to 100. The value 0 indicates that the resource is not critical, and 100 indicates that the resource is critical.<br>Minimum: **0**<br>Maximum: **100** |
| alert_type | **alert_type** object | Alert classification. For details, see the Alert Type Definition. |
| network_list | Array of **network_list** objects | Network Information<br>Array Length: **0 - 999** |
| resource_list | Array of **resource_list** objects | Affected resources.<br>Array Length: **0 - 999** |
| remediation | **remediation** object | Remedy measure. |
| verification_state | String | Verification status, which identifies the accuracy of an incident. The options are as follows: – Unknown – True_Positive – False_Positive Enter Unknown by default.<br>Minimum: **32**<br>Maximum: **64**<br>Enumeration values:<br>• **Unknown**<br>• **True_Positive**<br>• **False_Positive** |
| handle_status | String | Incident handling status. The options are as follows:<br>• Open: enabled.<br>• Block: blocked.<br>• Closed: closed. The default value is Open.<br>Minimum: **4**<br>Maximum: **5**<br>Enumeration values:<br>• **Open**<br>• **Block**<br>• **Closed** |

| Parameter | Type | Description |
| --- | --- | --- |
| sla | Integer | Risk close time -- Set the acceptable risk duration. Unit -- Hour<br>Minimum: **0**<br>Maximum: **999** |
| update_time | String | Update time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the alert occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| close_time | String | Closing time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| ipdrr_phase | String | Period/Handling phase No. Prepartion\| Detection and Analysis\|Containm, Eradication& Recovery\|Post-Incident-Activity<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **Prepartion**<br>• **Detection and Analysis**<br>• **Containm, Eradication& Recovery**<br>• **Post-Incident-Activity** |
| simulation | String | Debugging field.<br>Minimum: **0**<br>Maximum: **64** |
| actor | String | Alert investigator.<br>Minimum: **0**<br>Maximum: **64** |
| owner | String | Owner and service owner.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| creator | String | Creator<br>Minimum: **0**<br>Maximum: **64** |
| close_reason | String | Close reason.<br>• False positive.<br>• Resolved<br>• Repeated<br>• Other<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **False detection**<br>• **Resolved**<br>• **Repeated**<br>• **Other** |
| close_comment | String | Whether to close comment.<br>Minimum: **0**<br>Maximum: **1024** |
| malware | **malware** object | Malware |
| system_info | Object | System information. |
| process | Array of **process** objects | Process information.<br>Array Length: **0 - 999** |
| user_info | Array of **user_info** objects | User Details<br>Array Length: **0 - 999** |
| file_info | Array of **file_info** objects | Document information.<br>Array Length: **0 - 999** |
| system_alert_table | Object | Layout fields in the alerts list. |

**Table 4-81** environment

| Parameter | Type | Description |
| --- | --- | --- |
| vendor_type | String | Environment provider. The value can be **HWCP**, **HWC**, **AWS**, **Azure**, or **GCP**.<br>Minimum: **0**<br>Maximum: **64** |
| domain_id | String | Tenant ID.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region ID. **global** is returned for global services.<br>Minimum: **0**<br>Maximum: **64** |
| cross_workspace_id | String | ID of the source workspace for the data delivery. If the source workspace ID is null, then the destination workspace account ID is used.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID. The default value is null for global services.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-82** data_source

| Parameter | Type | Description |
| --- | --- | --- |
| source_type | Integer | Data source type. The options are as follows--1- Huawei product 2- Third-party product 3- Tenant product<br>Minimum: **1**<br>Maximum: **3**<br>Enumeration values:<br>• **1**<br>• **2**<br>• **3** |

| Parameter | Type | Description |
| --- | --- | --- |
| domain_id | String | Account ID to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | String | ID of the project to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region where the data source is located, for example, cn-north1. For details about the value range, see *Regions and Endpoints*.<br>Minimum: **0**<br>Maximum: **64** |
| company_name | String | Name of the company to which a data source belongs.<br>Minimum: **0**<br>Maximum: **16** |
| product_name | String | Name of the data source.<br>Minimum: **0**<br>Maximum: **24** |
| product_feature | String | Name of the feature of the product that detects the incident.<br>Minimum: **0**<br>Maximum: **24** |
| product_module | String | Threat detection module list.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-83** alert_type

| Parameter | Type | Description |
| --- | --- | --- |
| category | String | Type<br>Minimum: **0**<br>Maximum: **1024** |
| alert_type | String | Alert type.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-84** network_list

| Parameter | Type | Description |
| --- | --- | --- |
| direction | String | Direction. The value can be IN or OUT.<br>Minimum: **0**<br>Maximum: **3**<br>Enumeration values:<br>• **IN**<br>• **OUT** |
| protocol | String | Protocol, including Layer 7 and Layer 4 protocols. For details, see IANA registered name. https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.<br>Minimum: **0**<br>Maximum: **64** |
| src_ip | String | Source IP address<br>Minimum: **0**<br>Maximum: **64** |
| src_port | Integer | Source port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| src_domain | String | Source domain name.<br>Minimum: **0**<br>Maximum: **128** |
| src_geo | **src_geo** object | Geographical location of the source IP address. |
| dest_ip | String | Destination IP address<br>Minimum: **32**<br>Maximum: **64** |
| dest_port | String | Destination port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| dest_domain | String | Destination domain name<br>Minimum: **0**<br>Maximum: **128** |
| dest_geo | **dest_geo** object | Geographical location of the destination IP address. |

**Table 4-85** src_geo

| Parameter | Type | Description |
| --- | --- | --- |
| latitude | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-86** dest_geo

| Parameter | Type | Description |
| --- | --- | --- |
| latitude | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-87** resource_list

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Cloud service resource ID.<br>Minimum: **0**<br>Maximum: **36** |
| name | String | Resource name.<br>Minimum: **0**<br>Maximum: **255** |
| type | String | Resource type. This parameter references the value of RMS type on Huawei Cloud.<br>Minimum: **0**<br>Maximum: **64** |
| provider | String | Cloud service name, which is the same as the provider field in the RMS service.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region ID in Huawei Cloud, for example, cn-north-1.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| ep_id | String | Specifies the enterprise project ID.<br>Minimum: **0**<br>Maximum: **128** |
| ep_name | String | Enterprise Project Name<br>Minimum: **0**<br>Maximum: **128** |

| Parameter | Type | Description |
| --- | --- | --- |
| tags | String | Resource tag.<br>1. A maximum of 50 key/value pairs are supported.<br>2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _, :, /,@<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-88** remediation

| Parameter | Type | Description |
| --- | --- | --- |
| recommendation | String | Recommended solution.<br>Minimum: **0**<br>Maximum: **128** |
| url | String | Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-89** malware

| Parameter | Type | Description |
| --- | --- | --- |
| malware_family | String | Malicious family.<br>Minimum: **0**<br>Maximum: **64** |
| malware_class | String | Malware category.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-90** process

| Parameter | Type | Description |
| --- | --- | --- |
| process_name | String | Process name.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| process_path | String | Process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_pid | Integer | Process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_uid | Integer | Process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_cmdline | String | Process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_parent_name | String | Parent process name.<br>Minimum: **0**<br>Maximum: **64** |
| process_parent_path | String | Parent process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_parent_pid | Integer | Parent process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_parent_uid | Integer | Parent process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_parent_cmdline | String | Parent process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_child_name | String | Subprocess name.<br>Minimum: **0**<br>Maximum: **64** |
| process_child_path | String | Subprocess execution file path.<br>Minimum: **0**<br>Maximum: **512** |

| Parameter | Type | Description |
| --- | --- | --- |
| process_child_pid | Integer | Subprocess ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_child_uid | Integer | Subprocess user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_child_cmdline | String | Subprocess command line<br>Minimum: **0**<br>Maximum: **128** |
| process_launche_time | String | Incident start time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| process_terminate_time | String | Process end time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

**Table 4-91** user_info

| Parameter | Type | Description |
| --- | --- | --- |
| user_id | String | User UID<br>Minimum: **0**<br>Maximum: **36** |
| user_name | String | Username<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-92** file_info

| Parameter | Type | Description |
| --- | --- | --- |
| file_path | String | File path/name.<br>Minimum: **0**<br>Maximum: **128** |
| file_content | String | File path/name.<br>Minimum: **0**<br>Maximum: **1024** |
| file_new_path | String | New file path/name.<br>Minimum: **32**<br>Maximum: **64** |
| file_hash | String | File Hash<br>Minimum: **0**<br>Maximum: **128** |
| file_md5 | String | File MD5<br>Minimum: **0**<br>Maximum: **128** |
| file_sha256 | String | File SHA256<br>Minimum: **0**<br>Maximum: **128** |
| file_attr | String | File attribute.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-93** dataclass_ref

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Unique identifier of a data class. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| name | String | Data class name.<br>Minimum: **0**<br>Maximum: **36** |

**Status code: 400**

**Table 4-94** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-95** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Response body for obtaining alert condition details.


```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "data_object" : {
      "version" : "1.0",
      "environment" : {
        "vendor_type" : "MyXXX",
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "data_source" : {
        "source_type" : 3,
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "first_observed_time" : "2021-01-30T23:00:00Z+0800",
      "last_observed_time" : "2021-01-30T23:00:00Z+0800",
      "create_time" : "2021-01-30T23:00:00Z+0800",
      "arrive_time" : "2021-01-30T23:00:00Z+0800",
      "title" : "MyXXX",
      "description" : "This my XXXX",
      "source_url" : "http://xxx",
      "count" : "4",
      "confidence" : 4,
      "severity" : "TIPS",
```

```
    "criticality" : 4,
    "alert_type" : { },
    "network_list" : [ {
      "direction" : {
        "IN" : null
      },
      "protocol" : "TCP",
      "src_ip" : "192.168.0.1",
      "src_port" : "1",
      "src_domain" : "xxx",
      "dest_ip" : "192.168.0.1",
      "dest_port" : "1",
      "dest_domain" : "xxx",
      "src_geo" : {
        "latitude" : 90,
        "longitude" : 180
      },
      "dest_geo" : {
        "latitude" : 90,
        "longitude" : 180
      }
    } ],
    "resource_list" : [ {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "MyXXX",
      "type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_name" : "MyXXX",
      "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    } ],
    "remediation" : {
      "recommendation" : "MyXXX",
      "url" : "MyXXX"
    },
    "verification_state" : "Unknown,True_Positive,False_Positive. The default value is Unknown.",
    "handle_status" : "Open – enabled.Block – blocked.Closed – closed.The default value is Open.",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm, Eradication& Recovery| Post-Incident-
Activity",
    "simulation" : "false",
    "actor" : "Tom",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "False positive; Resolved; Duplicate; Others",
    "close_comment" : "False positive; Resolved; Duplicate; Others",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "Malicious memory occupation."
    },
    "system_info" : { },
    "process" : [ {
      "process_name" : "MyXXX",
      "process_path" : "MyXXX",
      "process_pid" : 123,
      "process_uid" : 123,
      "process_cmdline" : "MyXXX"
    } ],
    "user_info" : [ {
      "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "user_name" : "MyXXX"
    } ],
    "file_info" : [ {
      "file_path" : "MyXXX",
      "file_content" : "MyXXX",
```

```
      "file_new_path" : "MyXXX",
      "file_hash" : "MyXXX",
      "file_md5" : "MyXXX",
      "file_sha256" : "MyXXX",
      "file_attr" : "MyXXX"
     } ],
     "system_alert_table" : { },
     "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
     "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
   },
   "create_time" : "2021-01-30T23:00:00Z+0800",
   "update_time" : "2021-01-30T23:00:00Z+0800",
   "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
   "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
   "id" : "MyXXX",
   "version" : 11,
   "format_version" : 11,
   "dataclass_ref" : {
     "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
     "name" : "MyXXX"
   }
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowAlertSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowAlertRequest request = new ShowAlertRequest();
        try {
            ShowAlertResponse response = client.showAlert(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
```

```
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowAlertRequest()
        response = client.show_alert(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
```

```
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowAlertRequest{}
    response, err := client.ShowAlert(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response body for obtaining alert condition details. |
| 400 | Response body for request failures of obtaining alert condition details. |

## Error Codes

See **Error Codes**.

# 4.1.6 Updating an Alert

## Function

This API is used to edit alerts and update their attributes according to the changes made. The columns that are not changed remain unchanged.

## Calling Method

For details, see **Calling APIs**.

## URI

PUT /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/{alert_id}

**Table 4-96** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| alert_id | Yes | String | Alert ID.<br>Minimum: **32**<br>Maximum: **36** |

## Request Parameters

**Table 4-97** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **0**<br>Maximum: **2097152** |
| content-type | Yes | String | Content type.<br>Default: **application/json;charset=UTF-8**<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-98** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| batch_ids | No | Array of strings | IDs of updated alerts.<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 999** |
| data_object | No | **Alert** object | Alert entity information. |

**Table 4-99** Alert

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| version | No | String | Version of the data source of the alert. The value must be one officially released by the Huawei Cloud SSA service.<br>Minimum: **0**<br>Maximum: **64** |
| id | No | String | Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | No | String | ID of the account (domain_id) to whom the data is delivered and hosted.<br>Minimum: **0**<br>Maximum: **36** |
| region_id | No | String | ID of the region where the account to whom the data is delivered and hosted belongs to.<br>Minimum: **0**<br>Maximum: **36** |
| workspace_id | No | String | ID of the current workspace.<br>Minimum: **0**<br>Maximum: **36** |
| labels | No | String | Tag (display only)<br>Minimum: **0**<br>Maximum: **1024** |
| environment | No | **environment** object | Coordinates of the environment where the alert was generated. |
| data_source | No | **data_source** object | Source the data is first reported. |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| first_observed_time | No | String | First discovery time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| last_observed_time | No | String | First discovery time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| create_time | No | String | Recording time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| arrive_time | No | String | Data receiving time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| title | No | String | Alert title.<br>Minimum: **0**<br>Maximum: **255** |
| description | No | String | Alert description.<br>Minimum: **0**<br>Maximum: **1024** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| source_url | No | String | Alert URL, which points to the page of the current incident description in the data source product.<br>Minimum: **0**<br>Maximum: **1024** |
| count | No | Integer | Incident occurrences<br>Minimum: **0**<br>Maximum: **999** |
| confidence | No | Integer | Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or incident. Value range -- 0-100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.<br>Minimum: **0**<br>Maximum: **100** |
| severity | No | String | Severity level. Value range: Tips \| Low \| Medium \| High \| Fatal Description:<br>• **0**: TIPS: No threats are found.<br>• **1**: LOW: No actions are required for the threat.<br>• **2**: MEDIUM: The threat needs to be handled but is not urgent.<br>• **3**: HIGH: The threat must be handled preferentially.<br>• **4**: FATAL: The threat must be handled immediately to prevent further damage.<br>Minimum: **3**<br>Maximum: **6**<br>Enumeration values:<br>• **Tips**<br>• **Low**<br>• **Medium**<br>• **High**<br>• **Fatal** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| criticality | No | Integer | Criticality, which specifies the importance level of the resources involved in an incident. Value range -- 0 to 100. The value 0 indicates that the resource is not critical, and 100 indicates that the resource is critical.<br>Minimum: **0**<br>Maximum: **100** |
| alert_type | No | **alert_type** object | Alert classification. For details, see the Alert Type Definition. |
| network_list | No | Array of **network_list** objects | Network Information<br>Array Length: **0 - 999** |
| resource_list | No | Array of **resource_list** objects | Affected resources.<br>Array Length: **0 - 999** |
| remediation | No | **remediation** object | Remedy measure. |
| verification_state | No | String | Verification status, which identifies the accuracy of an incident. The options are as follows: – Unknown – True_Positive – False_Positive Enter Unknown by default.<br>Minimum: **32**<br>Maximum: **64**<br>Enumeration values:<br>• **Unknown**<br>• **True_Positive**<br>• **False_Positive** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| handle_status | No | String | Incident handling status. The options are as follows:<br>• Open: enabled.<br>• Block: blocked.<br>• Closed: closed. The default value is Open.<br>Minimum: **4**<br>Maximum: **5**<br>Enumeration values:<br>• **Open**<br>• **Block**<br>• **Closed** |
| sla | No | Integer | Risk close time -- Set the acceptable risk duration. Unit -- Hour<br>Minimum: **0**<br>Maximum: **999** |
| update_time | No | String | Update time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the alert occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| close_time | No | String | Closing time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| ipdrr_phase | No | String | Period/Handling phase No. Prepartion\|Detection and Analysis\|Containm, Eradication& Recovery\|Post-Incident-Activity<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **Prepartion**<br>• **Detection and Analysis**<br>• **Containm, Eradication& Recovery**<br>• **Post-Incident-Activity** |
| simulation | No | String | Debugging field.<br>Minimum: **0**<br>Maximum: **64** |
| actor | No | String | Alert investigator.<br>Minimum: **0**<br>Maximum: **64** |
| owner | No | String | Owner and service owner.<br>Minimum: **0**<br>Maximum: **64** |
| creator | No | String | Creator<br>Minimum: **0**<br>Maximum: **64** |
| close_reason | No | String | Close reason.<br>• False positive.<br>• Resolved<br>• Repeated<br>• Other<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **False detection**<br>• **Resolved**<br>• **Repeated**<br>• **Other** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| close_comment | No | String | Whether to close comment.<br>Minimum: **0**<br>Maximum: **1024** |
| malware | No | **malware** object | Malware |
| system_info | No | Object | System information. |
| process | No | Array of **process** objects | Process information.<br>Array Length: **0 - 999** |
| user_info | No | Array of **user_info** objects | User Details<br>Array Length: **0 - 999** |
| file_info | No | Array of **file_info** objects | Document information.<br>Array Length: **0 - 999** |
| system_alert_table | No | Object | Layout fields in the alerts list. |

**Table 4-100** environment

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| vendor_type | No | String | Environment provider. The value can be **HWCP**, **HWC**, **AWS**, **Azure**, or **GCP**.<br>Minimum: **0**<br>Maximum: **64** |
| domain_id | No | String | Tenant ID.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | No | String | Region ID. **global** is returned for global services.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| cross_workspace_id | No | String | ID of the source workspace for the data delivery. If the source workspace ID is null, then the destination workspace account ID is used.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | No | String | Project ID. The default value is null for global services.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-101** data_source

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| source_type | No | Integer | Data source type. The options are as follows-- 1- Huawei product 2- Third-party product 3- Tenant product<br>Minimum: **1**<br>Maximum: **3**<br>Enumeration values:<br>• **1**<br>• **2**<br>• **3** |
| domain_id | No | String | Account ID to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | No | String | ID of the project to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | No | String | Region where the data source is located, for example, cn-north1. For details about the value range, see *Regions and Endpoints*.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| company_name | No | String | Name of the company to which a data source belongs.<br>Minimum: **0**<br>Maximum: **16** |
| product_name | No | String | Name of the data source.<br>Minimum: **0**<br>Maximum: **24** |
| product_feature | No | String | Name of the feature of the product that detects the incident.<br>Minimum: **0**<br>Maximum: **24** |
| product_module | No | String | Threat detection module list.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-102** alert_type

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| category | No | String | Type<br>Minimum: **0**<br>Maximum: **1024** |
| alert_type | No | String | Alert type.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-103** network_list

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| direction | No | String | Direction. The value can be IN or OUT.<br>Minimum: **0**<br>Maximum: **3**<br>Enumeration values:<br>• **IN**<br>• **OUT** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| protocol | No | String | Protocol, including Layer 7 and Layer 4 protocols. For details, see IANA registered name. https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.<br>Minimum: **0**<br>Maximum: **64** |
| src_ip | No | String | Source IP address<br>Minimum: **0**<br>Maximum: **64** |
| src_port | No | Integer | Source port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| src_domain | No | String | Source domain name.<br>Minimum: **0**<br>Maximum: **128** |
| src_geo | No | **src_geo** object | Geographical location of the source IP address. |
| dest_ip | No | String | Destination IP address<br>Minimum: **32**<br>Maximum: **64** |
| dest_port | No | String | Destination port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| dest_domain | No | String | Destination domain name<br>Minimum: **0**<br>Maximum: **128** |
| dest_geo | No | **dest_geo** object | Geographical location of the destination IP address. |

**Table 4-104** src_geo

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| latitude | No | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | No | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | No | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | No | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-105** dest_geo

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| latitude | No | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | No | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | No | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | No | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-106** resource_list

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| id | No | String | Cloud service resource ID.<br>Minimum: **0**<br>Maximum: **36** |
| name | No | String | Resource name.<br>Minimum: **0**<br>Maximum: **255** |
| type | No | String | Resource type. This parameter references the value of RMS type on Huawei Cloud.<br>Minimum: **0**<br>Maximum: **64** |
| provider | No | String | Cloud service name, which is the same as the provider field in the RMS service.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | No | String | Region ID in Huawei Cloud, for example, cn-north-1.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | No | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | No | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| ep_id | No | String | Specifies the enterprise project ID.<br>Minimum: **0**<br>Maximum: **128** |
| ep_name | No | String | Enterprise Project Name<br>Minimum: **0**<br>Maximum: **128** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| tags | No | String | Resource tag.<br>1. A maximum of 50 key/value pairs are supported.<br>2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _, :, /,@<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-107** remediation

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| recommendation | No | String | Recommended solution.<br>Minimum: **0**<br>Maximum: **128** |
| url | No | String | Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-108** malware

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| malware_family | No | String | Malicious family.<br>Minimum: **0**<br>Maximum: **64** |
| malware_class | No | String | Malware category.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-109** process

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| process_name | No | String | Process name.<br>Minimum: **0**<br>Maximum: **64** |
| process_path | No | String | Process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_pid | No | Integer | Process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_uid | No | Integer | Process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_cmdline | No | String | Process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_parent_name | No | String | Parent process name.<br>Minimum: **0**<br>Maximum: **64** |
| process_parent_path | No | String | Parent process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_parent_pid | No | Integer | Parent process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_parent_uid | No | Integer | Parent process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_parent_cmdline | No | String | Parent process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_child_name | No | String | Subprocess name.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| process_child_path | No | String | Subprocess execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_child_pid | No | Integer | Subprocess ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_child_uid | No | Integer | Subprocess user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_child_cmdline | No | String | Subprocess command line<br>Minimum: **0**<br>Maximum: **128** |
| process_launche_time | No | String | Incident start time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| process_terminate_time | No | String | Process end time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

**Table 4-110** user_info

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| user_id | No | String | User UID<br>Minimum: **0**<br>Maximum: **36** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| user_name | No | String | Username<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-111** file_info

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| file_path | No | String | File path/name.<br>Minimum: **0**<br>Maximum: **128** |
| file_content | No | String | File path/name.<br>Minimum: **0**<br>Maximum: **1024** |
| file_new_path | No | String | New file path/name.<br>Minimum: **32**<br>Maximum: **64** |
| file_hash | No | String | File Hash<br>Minimum: **0**<br>Maximum: **128** |
| file_md5 | No | String | File MD5<br>Minimum: **0**<br>Maximum: **128** |
| file_sha256 | No | String | File SHA256<br>Minimum: **0**<br>Maximum: **128** |
| file_attr | No | String | File attribute.<br>Minimum: **0**<br>Maximum: **1024** |

## Response Parameters

**Status code: 200**

**Table 4-112** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-113** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Message<br>Minimum: **0**<br>Maximum: **1024** |
| data | **AlertDetail** object | |

**Table 4-114** AlertDetail

| Parameter | Type | Description |
| --- | --- | --- |
| create_time | String | Recording time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| data_object | **Alert** object | Alert entity information. |
| dataclass_ref | **dataclass_ref** object | Data class object. |
| format_version | Integer | Format version.<br>Minimum: **0**<br>Maximum: **999** |
| id | String | Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |

| Parameter | Type | Description |
| --- | --- | --- |
| project_id | String | ID of the current project.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Update time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| version | Integer | Version.<br>Minimum: **0**<br>Maximum: **999** |
| workspace_id | String | ID of the current workspace.<br>Minimum: **0**<br>Maximum: **36** |

**Table 4-115** Alert

| Parameter | Type | Description |
| --- | --- | --- |
| version | String | Version of the data source of the alert. The value must be one officially released by the Huawei Cloud SSA service.<br>Minimum: **0**<br>Maximum: **64** |
| id | String | Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | String | ID of the account (domain_id) to whom the data is delivered and hosted.<br>Minimum: **0**<br>Maximum: **36** |
| region_id | String | ID of the region where the account to whom the data is delivered and hosted belongs to.<br>Minimum: **0**<br>Maximum: **36** |

| Parameter | Type | Description |
| --- | --- | --- |
| workspace_id | String | ID of the current workspace.<br>Minimum: **0**<br>Maximum: **36** |
| labels | String | Tag (display only)<br>Minimum: **0**<br>Maximum: **1024** |
| environment | **environment** object | Coordinates of the environment where the alert was generated. |
| data_source | **data_source** object | Source the data is first reported. |
| first_observed_time | String | First discovery time. The format is ISO 8601-YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| last_observed_time | String | First discovery time. The format is ISO 8601-YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| create_time | String | Recording time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| arrive_time | String | Data receiving time. The format is ISO 8601-YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

| Parameter | Type | Description |
| --- | --- | --- |
| title | String | Alert title.<br>Minimum: **0**<br>Maximum: **255** |
| description | String | Alert description.<br>Minimum: **0**<br>Maximum: **1024** |
| source_url | String | Alert URL, which points to the page of the current incident description in the data source product.<br>Minimum: **0**<br>Maximum: **1024** |
| count | Integer | Incident occurrences<br>Minimum: **0**<br>Maximum: **999** |
| confidence | Integer | Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or incident. Value range -- 0-100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.<br>Minimum: **0**<br>Maximum: **100** |
| severity | String | Severity level. Value range: Tips \| Low \| Medium \| High \| Fatal Description:<br>• **0**: TIPS: No threats are found.<br>• **1**: LOW: No actions are required for the threat.<br>• **2**: MEDIUM: The threat needs to be handled but is not urgent.<br>• **3**: HIGH: The threat must be handled preferentially.<br>• **4**: FATAL: The threat must be handled immediately to prevent further damage.<br>Minimum: **3**<br>Maximum: **6**<br>Enumeration values:<br>• **Tips**<br>• **Low**<br>• **Medium**<br>• **High**<br>• **Fatal** |

| Parameter | Type | Description |
| --- | --- | --- |
| criticality | Integer | Criticality, which specifies the importance level of the resources involved in an incident. Value range -- 0 to 100. The value 0 indicates that the resource is not critical, and 100 indicates that the resource is critical.<br>Minimum: **0**<br>Maximum: **100** |
| alert_type | **alert_type** object | Alert classification. For details, see the Alert Type Definition. |
| network_list | Array of **network_list** objects | Network Information<br>Array Length: **0 - 999** |
| resource_list | Array of **resource_list** objects | Affected resources.<br>Array Length: **0 - 999** |
| remediation | **remediation** object | Remedy measure. |
| verification_state | String | Verification status, which identifies the accuracy of an incident. The options are as follows: – Unknown – True_Positive – False_Positive Enter Unknown by default.<br>Minimum: **32**<br>Maximum: **64**<br>Enumeration values:<br>• **Unknown**<br>• **True_Positive**<br>• **False_Positive** |
| handle_status | String | Incident handling status. The options are as follows:<br>• Open: enabled.<br>• Block: blocked.<br>• Closed: closed. The default value is Open.<br>Minimum: **4**<br>Maximum: **5**<br>Enumeration values:<br>• **Open**<br>• **Block**<br>• **Closed** |

| Parameter | Type | Description |
| --- | --- | --- |
| sla | Integer | Risk close time -- Set the acceptable risk duration. Unit -- Hour<br>Minimum: **0**<br>Maximum: **999** |
| update_time | String | Update time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the alert occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| close_time | String | Closing time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| ipdrr_phase | String | Period/Handling phase No. Prepartion\| Detection and Analysis\|Containm, Eradication& Recovery\|Post-Incident-Activity<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **Prepartion**<br>• **Detection and Analysis**<br>• **Containm, Eradication& Recovery**<br>• **Post-Incident-Activity** |
| simulation | String | Debugging field.<br>Minimum: **0**<br>Maximum: **64** |
| actor | String | Alert investigator.<br>Minimum: **0**<br>Maximum: **64** |
| owner | String | Owner and service owner.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| creator | String | Creator<br>Minimum: **0**<br>Maximum: **64** |
| close_reason | String | Close reason.<br>• False positive.<br>• Resolved<br>• Repeated<br>• Other<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **False detection**<br>• **Resolved**<br>• **Repeated**<br>• **Other** |
| close_comment | String | Whether to close comment.<br>Minimum: **0**<br>Maximum: **1024** |
| malware | **malware** object | Malware |
| system_info | Object | System information. |
| process | Array of **process** objects | Process information.<br>Array Length: **0 - 999** |
| user_info | Array of **user_info** objects | User Details<br>Array Length: **0 - 999** |
| file_info | Array of **file_info** objects | Document information.<br>Array Length: **0 - 999** |
| system_alert_table | Object | Layout fields in the alerts list. |

**Table 4-116** environment

| Parameter | Type | Description |
| --- | --- | --- |
| vendor_type | String | Environment provider. The value can be **HWCP**, **HWC**, **AWS**, **Azure**, or **GCP**.<br>Minimum: **0**<br>Maximum: **64** |
| domain_id | String | Tenant ID.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region ID. **global** is returned for global services.<br>Minimum: **0**<br>Maximum: **64** |
| cross_workspace_id | String | ID of the source workspace for the data delivery. If the source workspace ID is null, then the destination workspace account ID is used.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID. The default value is null for global services.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-117** data_source

| Parameter | Type | Description |
| --- | --- | --- |
| source_type | Integer | Data source type. The options are as follows--1- Huawei product 2- Third-party product 3- Tenant product<br>Minimum: **1**<br>Maximum: **3**<br>Enumeration values:<br>• **1**<br>• **2**<br>• **3** |

| Parameter | Type | Description |
| --- | --- | --- |
| domain_id | String | Account ID to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | String | ID of the project to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region where the data source is located, for example, cn-north1. For details about the value range, see *Regions and Endpoints*.<br>Minimum: **0**<br>Maximum: **64** |
| company_name | String | Name of the company to which a data source belongs.<br>Minimum: **0**<br>Maximum: **16** |
| product_name | String | Name of the data source.<br>Minimum: **0**<br>Maximum: **24** |
| product_feature | String | Name of the feature of the product that detects the incident.<br>Minimum: **0**<br>Maximum: **24** |
| product_module | String | Threat detection module list.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-118** alert_type

| Parameter | Type | Description |
| --- | --- | --- |
| category | String | Type<br>Minimum: **0**<br>Maximum: **1024** |
| alert_type | String | Alert type.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-119** network_list

| Parameter | Type | Description |
| --- | --- | --- |
| direction | String | Direction. The value can be IN or OUT.<br>Minimum: **0**<br>Maximum: **3**<br>Enumeration values:<br>• **IN**<br>• **OUT** |
| protocol | String | Protocol, including Layer 7 and Layer 4 protocols. For details, see IANA registered name. https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.<br>Minimum: **0**<br>Maximum: **64** |
| src_ip | String | Source IP address<br>Minimum: **0**<br>Maximum: **64** |
| src_port | Integer | Source port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| src_domain | String | Source domain name.<br>Minimum: **0**<br>Maximum: **128** |
| src_geo | **src_geo** object | Geographical location of the source IP address. |
| dest_ip | String | Destination IP address<br>Minimum: **32**<br>Maximum: **64** |
| dest_port | String | Destination port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| dest_domain | String | Destination domain name<br>Minimum: **0**<br>Maximum: **128** |
| dest_geo | **dest_geo** object | Geographical location of the destination IP address. |

**Table 4-120** src_geo

| Parameter | Type | Description |
| --- | --- | --- |
| latitude | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-121** dest_geo

| Parameter | Type | Description |
| --- | --- | --- |
| latitude | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-122** resource_list

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Cloud service resource ID.<br>Minimum: **0**<br>Maximum: **36** |
| name | String | Resource name.<br>Minimum: **0**<br>Maximum: **255** |
| type | String | Resource type. This parameter references the value of RMS type on Huawei Cloud.<br>Minimum: **0**<br>Maximum: **64** |
| provider | String | Cloud service name, which is the same as the provider field in the RMS service.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region ID in Huawei Cloud, for example, cn-north-1.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| ep_id | String | Specifies the enterprise project ID.<br>Minimum: **0**<br>Maximum: **128** |
| ep_name | String | Enterprise Project Name<br>Minimum: **0**<br>Maximum: **128** |

| Parameter | Type | Description |
| --- | --- | --- |
| tags | String | Resource tag.<br>1. A maximum of 50 key/value pairs are supported.<br>2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _, :, /,@<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-123** remediation

| Parameter | Type | Description |
| --- | --- | --- |
| recommendation | String | Recommended solution.<br>Minimum: **0**<br>Maximum: **128** |
| url | String | Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-124** malware

| Parameter | Type | Description |
| --- | --- | --- |
| malware_family | String | Malicious family.<br>Minimum: **0**<br>Maximum: **64** |
| malware_class | String | Malware category.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-125** process

| Parameter | Type | Description |
| --- | --- | --- |
| process_name | String | Process name.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| process_path | String | Process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_pid | Integer | Process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_uid | Integer | Process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_cmdline | String | Process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_parent_name | String | Parent process name.<br>Minimum: **0**<br>Maximum: **64** |
| process_parent_path | String | Parent process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_parent_pid | Integer | Parent process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_parent_uid | Integer | Parent process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_parent_cmdline | String | Parent process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_child_name | String | Subprocess name.<br>Minimum: **0**<br>Maximum: **64** |
| process_child_path | String | Subprocess execution file path.<br>Minimum: **0**<br>Maximum: **512** |

| Parameter | Type | Description |
| --- | --- | --- |
| process_child_pid | Integer | Subprocess ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_child_uid | Integer | Subprocess user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_child_cmdline | String | Subprocess command line<br>Minimum: **0**<br>Maximum: **128** |
| process_launche_time | String | Incident start time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| process_terminate_time | String | Process end time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

**Table 4-126** user_info

| Parameter | Type | Description |
| --- | --- | --- |
| user_id | String | User UID<br>Minimum: **0**<br>Maximum: **36** |
| user_name | String | Username<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-127** file_info

| Parameter | Type | Description |
| --- | --- | --- |
| file_path | String | File path/name.<br>Minimum: **0**<br>Maximum: **128** |
| file_content | String | File path/name.<br>Minimum: **0**<br>Maximum: **1024** |
| file_new_path | String | New file path/name.<br>Minimum: **32**<br>Maximum: **64** |
| file_hash | String | File Hash<br>Minimum: **0**<br>Maximum: **128** |
| file_md5 | String | File MD5<br>Minimum: **0**<br>Maximum: **128** |
| file_sha256 | String | File SHA256<br>Minimum: **0**<br>Maximum: **128** |
| file_attr | String | File attribute.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-128** dataclass_ref

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Unique identifier of a data class. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| name | String | Data class name.<br>Minimum: **0**<br>Maximum: **36** |

**Status code: 400**

**Table 4-129** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-130** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Update an alert. Set Alert Name to MyXXX, URL to http://xxx, Number of occurrences to 4, Confidence to 4, and Severity to tips.

```
{
  "data_object" : {
    "version" : "1.0",
    "environment" : {
      "vendor_type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "data_source" : {
      "source_type" : 3,
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "first_observed_time" : "2021-01-30T23:00:00Z+0800",
    "last_observed_time" : "2021-01-30T23:00:00Z+0800",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "arrive_time" : "2021-01-30T23:00:00Z+0800",
    "title" : "MyXXX",
    "description" : "This my XXXX",
    "source_url" : "http://xxx",
    "count" : 4,
    "confidence" : 4,
    "severity" : "TIPS",
    "criticality" : 4,
    "alert_type" : { },
    "network_list" : [ {
      "direction" : {
        "IN" : null
      },
      "protocol" : "TCP",
      "src_ip" : "192.168.0.1",
      "src_port" : "1",
```

```
    "src_domain" : "xxx",
    "dest_ip" : "192.168.0.1",
    "dest_port" : "1",
    "dest_domain" : "xxx",
    "src_geo" : {
      "latitude" : 90,
      "longitude" : 180
    },
    "dest_geo" : {
      "latitude" : 90,
      "longitude" : 180
    }
  } ],
  "resource_list" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "type" : "MyXXX",
    "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "ep_name" : "MyXXX",
    "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  } ],
  "remediation" : {
    "recommendation" : "MyXXX",
    "url" : "MyXXX"
  },
  "verification_state" : "Unknown,True_Positive,False_Positive The default value is Unknown.",
  "handle_status" : "Open – enabled.Block – blocked.Closed – closed.The default value is Open.",
  "sla" : 60000,
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "close_time" : "2021-01-30T23:00:00Z+0800",
  "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm, Eradication& Recovery| Post-Incident-
Activity",
  "simulation" : "false",
  "actor" : "Tom",
  "owner" : "MyXXX",
  "creator" : "MyXXX",
  "close_reason" : "False positive; Resolved; Duplicate; Others",
  "close_comment" : "False positive; Resolved; Duplicate; Others",
  "malware" : {
    "malware_family" : "family",
    "malware_class" : "Malicious memory occupation."
  },
  "system_info" : { },
  "process" : [ {
    "process_name" : "MyXXX",
    "process_path" : "MyXXX",
    "process_pid" : 123,
    "process_uid" : 123,
    "process_cmdline" : "MyXXX"
  } ],
  "user_info" : [ {
    "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "user_name" : "MyXXX"
  } ],
  "file_info" : [ {
    "file_path" : "MyXXX",
    "file_content" : "MyXXX",
    "file_new_path" : "MyXXX",
    "file_hash" : "MyXXX",
    "file_md5" : "MyXXX",
    "file_sha256" : "MyXXX",
    "file_attr" : "MyXXX"
  } ],
  "system_alert_table" : { },
  "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
```

```
  }
}
```

## Example Responses

**Status code: 200**

Response body of request for updating alerts.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "data_object" : {
      "version" : "1.0",
      "environment" : {
        "vendor_type" : "MyXXX",
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "data_source" : {
        "source_type" : 3,
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "first_observed_time" : "2021-01-30T23:00:00Z+0800",
      "last_observed_time" : "2021-01-30T23:00:00Z+0800",
      "create_time" : "2021-01-30T23:00:00Z+0800",
      "arrive_time" : "2021-01-30T23:00:00Z+0800",
      "title" : "MyXXX",
      "description" : "This my XXXX",
      "source_url" : "http://xxx",
      "count" : 4,
      "confidence" : 4,
      "severity" : "TIPS",
      "criticality" : 4,
      "alert_type" : { },
      "network_list" : [ {
        "direction" : {
          "IN" : null
        },
        "protocol" : "TCP",
        "src_ip" : "192.168.0.1",
        "src_port" : "1",
        "src_domain" : "xxx",
        "dest_ip" : "192.168.0.1",
        "dest_port" : "1",
        "dest_domain" : "xxx",
        "src_geo" : {
          "latitude" : 90,
          "longitude" : 180
        },
        "dest_geo" : {
          "latitude" : 90,
          "longitude" : 180
        }
      } ],
      "resource_list" : [ {
        "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "name" : "MyXXX",
        "type" : "MyXXX",
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "ep_name" : "MyXXX",
        "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
```

```
    } ],
    "remediation" : {
      "recommendation" : "MyXXX",
      "url" : "MyXXX"
    },
    "verification_state" : "Unknown,True_Positive,False_Positive The default value is Unknown.",
    "handle_status" : "Open – enabled.Block – blocked.Closed – closed.The default value is Open.",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm, Eradication& Recovery| Post-Incident-
Activity",
    "simulation" : "false",
    "actor" : "Tom",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "False positive; Resolved; Duplicate; Others",
    "close_comment" : "False positive; Resolved; Duplicate; Others",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "Malicious memory occupation."
    },
    "system_info" : { },
    "process" : [ {
      "process_name" : "MyXXX",
      "process_path" : "MyXXX",
      "process_pid" : 123,
      "process_uid" : 123,
      "process_cmdline" : "MyXXX"
    } ],
    "user_info" : [ {
      "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "user_name" : "MyXXX"
    } ],
    "file_info" : [ {
      "file_path" : "MyXXX",
      "file_content" : "MyXXX",
      "file_new_path" : "MyXXX",
      "file_hash" : "MyXXX",
      "file_md5" : "MyXXX",
      "file_sha256" : "MyXXX",
      "file_attr" : "MyXXX"
    } ],
    "system_alert_table" : { },
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
  },
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "id" : "MyXXX",
  "version" : 11,
  "format_version" : 11,
  "dataclass_ref" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX"
  }
 }
}
```


## SDK Sample Code

The SDK sample code is as follows.

## Java

Update an alert. Set Alert Name to MyXXX, URL to http://xxx, Number of occurrences to 4, Confidence to 4, and Severity to tips.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class ChangeAlertSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ChangeAlertRequest request = new ChangeAlertRequest();
        ChangeAlertRequestBody body = new ChangeAlertRequestBody();
        List<AlertFileInfo> listDataObjectFileInfo = new ArrayList<>();
        listDataObjectFileInfo.add(
            new AlertFileInfo()
                .withFilePath("MyXXX")
                .withFileContent("MyXXX")
                .withFileNewPath("MyXXX")
                .withFileHash("MyXXX")
                .withFileMd5("MyXXX")
                .withFileSha256("MyXXX")
                .withFileAttr("MyXXX")
        );
        List<AlertUserInfo> listDataObjectUserInfo = new ArrayList<>();
        listDataObjectUserInfo.add(
            new AlertUserInfo()
                .withUserId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withUserName("MyXXX")
        );
        List<AlertProcess> listDataObjectProcess = new ArrayList<>();
        listDataObjectProcess.add(
            new AlertProcess()
                .withProcessName("MyXXX")
                .withProcessPath("MyXXX")
                .withProcessPid(123)
                .withProcessUid(123)
                .withProcessCmdline("MyXXX")
        );
        AlertMalware malwareDataObject = new AlertMalware();
        malwareDataObject.withMalwareFamily("family")
            .withMalwareClass("Malicious memory occupation.");
```

```
        AlertRemediation remediationDataObject = new AlertRemediation();
        remediationDataObject.withRecommendation("MyXXX")
            .withUrl("MyXXX");
        List<AlertResourceList> listDataObjectResourceList = new ArrayList<>();
        listDataObjectResourceList.add(
            new AlertResourceList()
                .withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withName("MyXXX")
                .withType("MyXXX")
                .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withEpId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withEpName("MyXXX")
                .withTags("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        );
        AlertDestGeo destGeoNetworkList = new AlertDestGeo();
        destGeoNetworkList.withLatitude(java.math.BigDecimal.valueOf(90))
            .withLongitude(java.math.BigDecimal.valueOf(180));
        AlertSrcGeo srcGeoNetworkList = new AlertSrcGeo();
        srcGeoNetworkList.withLatitude(java.math.BigDecimal.valueOf(90))
            .withLongitude(java.math.BigDecimal.valueOf(180));
        List<AlertNetworkList> listDataObjectNetworkList = new ArrayList<>();
        listDataObjectNetworkList.add(
            new AlertNetworkList()
                .withDirection(AlertNetworkList.DirectionEnum.fromValue("{}"))
                .withProtocol("TCP")
                .withSrcIp("192.168.0.1")
                .withSrcPort(1)
                .withSrcDomain("xxx")
                .withSrcGeo(srcGeoNetworkList)
                .withDestIp("192.168.0.1")
                .withDestPort("1")
                .withDestDomain("xxx")
                .withDestGeo(destGeoNetworkList)
        );
        AlertDataSource dataSourceDataObject = new AlertDataSource();
        dataSourceDataObject.withSourceType(3)
            .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        AlertEnvironment environmentDataObject = new AlertEnvironment();
        environmentDataObject.withVendorType("MyXXX")
            .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        Alert dataObjectbody = new Alert();
        dataObjectbody.withVersion("1.0")
            .withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withWorkspaceId("909494e3-558e-46b6-a9eb-07a8e18ca620")
            .withEnvironment(environmentDataObject)
            .withDataSource(dataSourceDataObject)
            .withFirstObservedTime("2021-01-30T23:00:00Z+0800")
            .withLastObservedTime("2021-01-30T23:00:00Z+0800")
            .withCreateTime("2021-01-30T23:00:00Z+0800")
            .withArriveTime("2021-01-30T23:00:00Z+0800")
            .withTitle("MyXXX")
            .withDescription("This my XXXX")
            .withSourceUrl("http://xxx")
            .withCount(4)
            .withConfidence(4)
            .withSeverity(Alert.SeverityEnum.fromValue("TIPS"))
            .withCriticality(4)
            .withNetworkList(listDataObjectNetworkList)
            .withResourceList(listDataObjectResourceList)
            .withRemediation(remediationDataObject)
            .withVerificationState(Alert.VerificationStateEnum.fromValue("Unknown,True_Positive,False_Positive
The default value is Unknown."))
            .withHandleStatus(Alert.HandleStatusEnum.fromValue("Open – enabled.Block – blocked.Closed –
```

```
closed.The default value is Open."))
            .withSla(60000)
            .withUpdateTime("2021-01-30T23:00:00Z+0800")
            .withCloseTime("2021-01-30T23:00:00Z+0800")
            .withIpdrrPhase(Alert.IpdrrPhaseEnum.fromValue("Prepartion|Detection and Analysis|
Containm,Eradication& Recovery| Post-Incident-Activity"))
            .withSimulation("false")
            .withActor("Tom")
            .withOwner("MyXXX")
            .withCreator("MyXXX")
            .withCloseReason(Alert.CloseReasonEnum.fromValue("False positive; Resolved; Duplicate; Others"))
            .withCloseComment("False positive; Resolved; Duplicate; Others")
            .withMalware(malwareDataObject)
            .withSystemInfo(new Object())
            .withProcess(listDataObjectProcess)
            .withUserInfo(listDataObjectUserInfo)
            .withFileInfo(listDataObjectFileInfo)
            .withSystemAlertTable(new Object());
        body.withDataObject(dataObjectbody);
        request.withBody(body);
        try {
            ChangeAlertResponse response = client.changeAlert(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Update an alert. Set Alert Name to MyXXX, URL to http://xxx, Number of occurrences to 4, Confidence to 4, and Severity to tips.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ChangeAlertRequest()
        listFileInfoDataObject = [
            AlertFileInfo(
```

```
        file_path="MyXXX",
        file_content="MyXXX",
        file_new_path="MyXXX",
        file_hash="MyXXX",
        file_md5="MyXXX",
        file_sha256="MyXXX",
        file_attr="MyXXX"
    )
]
listUserInfoDataObject = [
    AlertUserInfo(
        user_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        user_name="MyXXX"
    )
]
listProcessDataObject = [
    AlertProcess(
        process_name="MyXXX",
        process_path="MyXXX",
        process_pid=123,
        process_uid=123,
        process_cmdline="MyXXX"
    )
]
malwareDataObject = AlertMalware(
    malware_family="family",
    malware_class="Malicious memory occupation."
)
remediationDataObject = AlertRemediation(
    recommendation="MyXXX",
    url="MyXXX"
)
listResourceListDataObject = [
    AlertResourceList(
        id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        name="MyXXX",
        type="MyXXX",
        region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        ep_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        ep_name="MyXXX",
        tags="909494e3-558e-46b6-a9eb-07a8e18ca62f"
    )
]
destGeoNetworkList = AlertDestGeo(
    latitude=90,
    longitude=180
)
srcGeoNetworkList = AlertSrcGeo(
    latitude=90,
    longitude=180
)
listNetworkListDataObject = [
    AlertNetworkList(
        direction="{}",
        protocol="TCP",
        src_ip="192.168.0.1",
        src_port=1,
        src_domain="xxx",
        src_geo=srcGeoNetworkList,
        dest_ip="192.168.0.1",
        dest_port="1",
        dest_domain="xxx",
        dest_geo=destGeoNetworkList
    )
]
dataSourceDataObject = AlertDataSource(
    source_type=3,
```

```
            domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f"
        )
        environmentDataObject = AlertEnvironment(
            vendor_type="MyXXX",
            domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f"
        )
        dataObjectbody = Alert(
            version="1.0",
            id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            workspace_id="909494e3-558e-46b6-a9eb-07a8e18ca620",
            environment=environmentDataObject,
            data_source=dataSourceDataObject,
            first_observed_time="2021-01-30T23:00:00Z+0800",
            last_observed_time="2021-01-30T23:00:00Z+0800",
            create_time="2021-01-30T23:00:00Z+0800",
            arrive_time="2021-01-30T23:00:00Z+0800",
            title="MyXXX",
            description="This my XXXX",
            source_url="http://xxx",
            count=4,
            confidence=4,
            severity="TIPS",
            criticality=4,
            network_list=listNetworkListDataObject,
            resource_list=listResourceListDataObject,
            remediation=remediationDataObject,
            verification_state="Unknown,True_Positive,False_Positive The default value is Unknown.",
            handle_status="Open – enabled.Block – blocked.Closed – closed.The default value is Open.",
            sla=60000,
            update_time="2021-01-30T23:00:00Z+0800",
            close_time="2021-01-30T23:00:00Z+0800",
            ipdrr_phase="Prepartion|Detection and Analysis|Containm,Eradication& Recovery| Post-Incident-
Activity",
            simulation="false",
            actor="Tom",
            owner="MyXXX",
            creator="MyXXX",
            close_reason="False positive; Resolved; Duplicate; Others",
            close_comment="False positive; Resolved; Duplicate; Others",
            malware=malwareDataObject,
            system_info={},
            process=listProcessDataObject,
            user_info=listUserInfoDataObject,
            file_info=listFileInfoDataObject,
            system_alert_table={}
        )
        request.body = ChangeAlertRequestBody(
            data_object=dataObjectbody
        )
        response = client.change_alert(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Update an alert. Set Alert Name to MyXXX, URL to http://xxx, Number of occurrences to 4, Confidence to 4, and Severity to tips.

```
package main

import (
```

```
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ChangeAlertRequest{}
    filePathFileInfo:= "MyXXX"
    fileContentFileInfo:= "MyXXX"
    fileNewPathFileInfo:= "MyXXX"
    fileHashFileInfo:= "MyXXX"
    fileMd5FileInfo:= "MyXXX"
    fileSha256FileInfo:= "MyXXX"
    fileAttrFileInfo:= "MyXXX"
    var listFileInfoDataObject = []model.AlertFileInfo{
        {
            FilePath: &filePathFileInfo,
            FileContent: &fileContentFileInfo,
            FileNewPath: &fileNewPathFileInfo,
            FileHash: &fileHashFileInfo,
            FileMd5: &fileMd5FileInfo,
            FileSha256: &fileSha256FileInfo,
            FileAttr: &fileAttrFileInfo,
        },
    }
    userIdUserInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    userNameUserInfo:= "MyXXX"
    var listUserInfoDataObject = []model.AlertUserInfo{
        {
            UserId: &userIdUserInfo,
            UserName: &userNameUserInfo,
        },
    }
    processNameProcess:= "MyXXX"
    processPathProcess:= "MyXXX"
    processPidProcess:= int32(123)
    processUidProcess:= int32(123)
    processCmdlineProcess:= "MyXXX"
    var listProcessDataObject = []model.AlertProcess{
        {
            ProcessName: &processNameProcess,
            ProcessPath: &processPathProcess,
            ProcessPid: &processPidProcess,
            ProcessUid: &processUidProcess,
            ProcessCmdline: &processCmdlineProcess,
        },
    }
    malwareFamilyMalware:= "family"
```

```
malwareClassMalware:= "Malicious memory occupation."
malwareDataObject := &model.AlertMalware{
    MalwareFamily: &malwareFamilyMalware,
    MalwareClass: &malwareClassMalware,
}
recommendationRemediation:= "MyXXX"
urlRemediation:= "MyXXX"
remediationDataObject := &model.AlertRemediation{
    Recommendation: &recommendationRemediation,
    Url: &urlRemediation,
}
idResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
nameResourceList:= "MyXXX"
typeResourceList:= "MyXXX"
regionIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
domainIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
projectIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
epIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
epNameResourceList:= "MyXXX"
tagsResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
var listResourceListDataObject = []model.AlertResourceList{
    {
        Id: &idResourceList,
        Name: &nameResourceList,
        Type: &typeResourceList,
        RegionId: &regionIdResourceList,
        DomainId: &domainIdResourceList,
        ProjectId: &projectIdResourceList,
        EpId: &epIdResourceList,
        EpName: &epNameResourceList,
        Tags: &tagsResourceList,
    },
}
latitudeDestGeo:= float32(90)
longitudeDestGeo:= float32(180)
destGeoNetworkList := &model.AlertDestGeo{
    Latitude: &latitudeDestGeo,
    Longitude: &longitudeDestGeo,
}
latitudeSrcGeo:= float32(90)
longitudeSrcGeo:= float32(180)
srcGeoNetworkList := &model.AlertSrcGeo{
    Latitude: &latitudeSrcGeo,
    Longitude: &longitudeSrcGeo,
}
directionNetworkList:= model.GetAlertNetworkListDirectionEnum().{}
protocolNetworkList:= "TCP"
srcIpNetworkList:= "192.168.0.1"
srcPortNetworkList:= int32(1)
srcDomainNetworkList:= "xxx"
destIpNetworkList:= "192.168.0.1"
destPortNetworkList:= "1"
destDomainNetworkList:= "xxx"
var listNetworkListDataObject = []model.AlertNetworkList{
    {
        Direction: &directionNetworkList,
        Protocol: &protocolNetworkList,
        SrcIp: &srcIpNetworkList,
        SrcPort: &srcPortNetworkList,
        SrcDomain: &srcDomainNetworkList,
        SrcGeo: srcGeoNetworkList,
        DestIp: &destIpNetworkList,
        DestPort: &destPortNetworkList,
        DestDomain: &destDomainNetworkList,
        DestGeo: destGeoNetworkList,
    },
}
sourceTypeDataSource:= int32(3)
domainIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
```

```
    projectIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    regionIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    dataSourceDataObject := &model.AlertDataSource{
        SourceType: &sourceTypeDataSource,
        DomainId: &domainIdDataSource,
        ProjectId: &projectIdDataSource,
        RegionId: &regionIdDataSource,
    }
    vendorTypeEnvironment:= "MyXXX"
    domainIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    regionIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    projectIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    environmentDataObject := &model.AlertEnvironment{
        VendorType: &vendorTypeEnvironment,
        DomainId: &domainIdEnvironment,
        RegionId: &regionIdEnvironment,
        ProjectId: &projectIdEnvironment,
    }
    versionDataObject:= "1.0"
    idDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    workspaceIdDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca620"
    firstObservedTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    lastObservedTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    createTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    arriveTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    titleDataObject:= "MyXXX"
    descriptionDataObject:= "This my XXXX"
    sourceUrlDataObject:= "http://xxx"
    countDataObject:= int32(4)
    confidenceDataObject:= int32(4)
    severityDataObject:= model.GetAlertSeverityEnum().TIPS
    criticalityDataObject:= int32(4)
    verificationStateDataObject:=
model.GetAlertVerificationStateEnum().UNKNOWN,TRUE_POSITIVE,FALSE_POSITIVE_THE_DEFAULT_VALUE_I
S_UNKNOWN_
    handleStatusDataObject:= model.GetAlertHandleStatusEnum().OPEN_-_ENABLED_BLOCK_-
_BLOCKED_CLOSED_-_CLOSED_THE_DEFAULT_VALUE_IS_OPEN_
    slaDataObject:= int32(60000)
    updateTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    closeTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    ipdrrPhaseDataObject:= model.GetAlertIpdrrPhaseEnum().PREPARTION|DETECTION_AND_ANALYSIS|
CONTAINM,ERADICATION&_RECOVERY|_POST_INCIDENT_ACTIVITY
    simulationDataObject:= "false"
    actorDataObject:= "Tom"
    ownerDataObject:= "MyXXX"
    creatorDataObject:= "MyXXX"
    closeReasonDataObject:=
model.GetAlertCloseReasonEnum().FALSE_POSITIVE;_RESOLVED;_DUPLICATE;_OTHERS
    closeCommentDataObject:= "False positive; Resolved; Duplicate; Others"
    var systemInfoDataObject interface{} = make(map[string]string)
    var systemAlertTableDataObject interface{} = make(map[string]string)
    dataObjectbody := &model.Alert{
        Version: &versionDataObject,
        Id: &idDataObject,
        WorkspaceId: &workspaceIdDataObject,
        Environment: environmentDataObject,
        DataSource: dataSourceDataObject,
        FirstObservedTime: &firstObservedTimeDataObject,
        LastObservedTime: &lastObservedTimeDataObject,
        CreateTime: &createTimeDataObject,
        ArriveTime: &arriveTimeDataObject,
        Title: &titleDataObject,
        Description: &descriptionDataObject,
        SourceUrl: &sourceUrlDataObject,
        Count: &countDataObject,
        Confidence: &confidenceDataObject,
        Severity: &severityDataObject,
        Criticality: &criticalityDataObject,
        NetworkList: &listNetworkListDataObject,
```

```
        ResourceList: &listResourceListDataObject,
        Remediation: remediationDataObject,
        VerificationState: &verificationStateDataObject,
        HandleStatus: &handleStatusDataObject,
        Sla: &slaDataObject,
        UpdateTime: &updateTimeDataObject,
        CloseTime: &closeTimeDataObject,
        IpdrrPhase: &ipdrrPhaseDataObject,
        Simulation: &simulationDataObject,
        Actor: &actorDataObject,
        Owner: &ownerDataObject,
        Creator: &creatorDataObject,
        CloseReason: &closeReasonDataObject,
        CloseComment: &closeCommentDataObject,
        Malware: malwareDataObject,
        SystemInfo: &systemInfoDataObject,
        Process: &listProcessDataObject,
        UserInfo: &listUserInfoDataObject,
        FileInfo: &listFileInfoDataObject,
        SystemAlertTable: &systemAlertTableDataObject,
    }
    request.Body = &model.ChangeAlertRequestBody{
        DataObject: dataObjectbody,
    }
    response, err := client.ChangeAlert(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

### More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

### Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response body of request for updating alerts. |
| 400 | Response body of failed requests for updating alerts. |

### Error Codes

See **Error Codes**.

# 4.2 Incident Management

## 4.2.1 This API is used to search for the incident list.

### Function

This API is used to search for the incident list.

## Calling Method

For details, see **Calling APIs**.

## URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/search

**Table 4-131** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

## Request Parameters

**Table 4-132** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **0**<br>Maximum: **2097152** |
| content-type | Yes | String | Content type.<br>Default: **application/json;charset=UTF-8**<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-133** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| limit | No | Integer | Number of records displayed on each page.<br>Minimum: **0**<br>Maximum: **1000** |
| offset | No | Integer | Offset<br>Minimum: **0**<br>Maximum: **1000** |
| sort_by | No | String | Sorting field -- create_time \| update_time<br>Minimum: **0**<br>Maximum: **1000** |
| order | No | String | Sort by -- DESC \| ASC<br>Minimum: **0**<br>Maximum: **1000**<br>Enumeration values:<br>• **DESC**<br>• **ASC** |
| from_date | No | String | Search start time, for example, 2023-02-20T00:00:00.000Z<br>Minimum: **0**<br>Maximum: **64** |
| to_date | No | String | Search end time, for example, 2023-02-27T23:59:59.999Z<br>Minimum: **0**<br>Maximum: **64** |
| condition | No | **condition** object | Search condition expression. |

**Table 4-134** condition

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| conditions | No | Array of **conditions** objects | Expression list.<br>Array Length: **0 - 999** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| logics | No | Array of strings | Expression logic.<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 999** |

**Table 4-135** conditions

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| name | No | String | Expression name.<br>Minimum: **0**<br>Maximum: **64** |
| data | No | Array of strings | Expression content list.<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 999** |

## Response Parameters

**Status code: 200**

**Table 4-136** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-137** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Message<br>Minimum: **0**<br>Maximum: **1024** |

| Parameter | Type | Description |
| --- | --- | --- |
| total | Integer | Total number of incidents.<br>Minimum: **0**<br>Maximum: **10000** |
| limit | Integer | Number of records displayed on each page.<br>Minimum: **0**<br>Maximum: **10000** |
| offset | Integer | Offset<br>Minimum: **0**<br>Maximum: **10000** |
| success | Boolean | Successful or not. |
| data | Array of **IncidentDetail** objects | Event List<br>Array Length: **0 - 10000** |

**Table 4-138** IncidentDetail

| Parameter | Type | Description |
| --- | --- | --- |
| create_time | String | Recording time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| data_object | **Incident** object | Incident entity information. |
| dataclass_ref | **dataclass_ref** object | Data class object. |
| format_version | Integer | Format version.<br>Minimum: **0**<br>Maximum: **999** |
| id | String | Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |

| Parameter | Type | Description |
| --- | --- | --- |
| project_id | String | ID of the current project.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Update time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the alert occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| version | Integer | Version.<br>Minimum: **0**<br>Maximum: **999** |
| workspace_id | String | ID of the current workspace.<br>Minimum: **0**<br>Maximum: **36** |

**Table 4-139** Incident

| Parameter | Type | Description |
| --- | --- | --- |
| version | String | Version of the data source of an incident. The version must be one officially released by the Huawei Cloud SSA service.<br>Minimum: **0**<br>Maximum: **64** |
| id | String | Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | String | ID of the account (domain_id) to whom the data is delivered and hosted.<br>Minimum: **0**<br>Maximum: **36** |
| region_id | String | ID of the region where the account to whom the data is delivered and hosted belongs to.<br>Minimum: **0**<br>Maximum: **36** |

| Parameter | Type | Description |
| --- | --- | --- |
| workspace_id | String | ID of the current workspace.<br>Minimum: **0**<br>Maximum: **36** |
| labels | String | Tag (display only)<br>Minimum: **0**<br>Maximum: **1024** |
| environment | **environment** object | Coordinates of the environment where the incident was generated. |
| data_source | **data_source** object | Source the data is first reported. |
| first_observed_time | String | First discovery time. The format is ISO 8601-YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| last_observed_time | String | First discovery time. The format is ISO 8601-YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| create_time | String | Recording time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| arrive_time | String | Data receiving time. The format is ISO 8601-YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

| Parameter | Type | Description |
| --- | --- | --- |
| title | String | Incident title.<br>Minimum: **0**<br>Maximum: **255** |
| description | String | Event Description<br>Minimum: **0**<br>Maximum: **1024** |
| source_url | String | Incident URL, which points to the page of the current incident description in the data source product.<br>Minimum: **0**<br>Maximum: **1024** |
| count | Integer | Incident occurrences<br>Minimum: **0**<br>Maximum: **999** |
| confidence | Integer | Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or incident. Value range -- 0-100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.<br>Minimum: **0**<br>Maximum: **100** |
| severity | String | Severity level. Value range: Tips \| Low \| Medium \| High \| Fatal Description:<br>• **0**: TIPS: No threats are found.<br>• **1**: LOW: No actions are required for the threat.<br>• **2**: MEDIUM: The threat needs to be handled but is not urgent.<br>• **3**: HIGH: The threat must be handled preferentially.<br>• **4**: FATAL: The threat must be handled immediately to prevent further damage.<br>Minimum: **3**<br>Maximum: **6**<br>Enumeration values:<br>• **Tips**<br>• **Low**<br>• **Medium**<br>• **High**<br>• **Fatal** |

| Parameter | Type | Description |
| --- | --- | --- |
| criticality | Integer | Criticality, which specifies the importance level of the resources involved in an incident. Value range -- 0 to 100. The value 0 indicates that the resource is not critical, and 100 indicates that the resource is critical.<br>Minimum: **0**<br>Maximum: **100** |
| incident_type | **incident_type** object | Incident categories. For details, see the Alert Incident Type Definition. |
| network_list | Array of **network_list** objects | Network Information<br>Array Length: **0 - 999** |
| resource_list | Array of **resource_list** objects | Affected resources.<br>Array Length: **0 - 999** |
| remediation | **remediation** object | Remedy measure. |
| verification_state | String | Verification status, which identifies the accuracy of an incident. The options are as follows: – Unknown – True_Positive – False_Positive Enter Unknown by default.<br>Minimum: **32**<br>Maximum: **64**<br>Enumeration values:<br>• **Unknown**<br>• **True_Positive**<br>• **False_Positive** |
| handle_status | String | Incident handling status. The options are as follows:<br>• Open: enabled.<br>• Block: blocked.<br>• Closed: closed. The default value is Open.<br>Minimum: **4**<br>Maximum: **5**<br>Enumeration values:<br>• **Open**<br>• **Block**<br>• **Closed** |

| Parameter | Type | Description |
| --- | --- | --- |
| sla | Integer | Risk close time -- Set the acceptable risk duration. Unit -- Hour<br>Minimum: **0**<br>Maximum: **999** |
| update_time | String | Update time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the alert occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| close_time | String | Closing time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| ipdrr_phase | String | Period/Handling phase No. Prepartion\| Detection and Analysis\|Containm, Eradication& Recovery\|Post-Incident-Activity<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **Prepartion**<br>• **Detection and Analysis**<br>• **Containm, Eradication& Recovery**<br>• **Post-Incident-Activity** |
| simulation | String | Debugging field.<br>Minimum: **0**<br>Maximum: **64** |
| actor | String | Incident investigator.<br>Minimum: **0**<br>Maximum: **64** |
| owner | String | Owner and service owner.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| creator | String | Creator<br>Minimum: **0**<br>Maximum: **64** |
| close_reason | String | Close reason.<br>• False positive.<br>• Resolved<br>• Repeated<br>• Other<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **False detection**<br>• **Resolved**<br>• **Repeated**<br>• **Other** |
| close_comment | String | Whether to close comment.<br>Minimum: **0**<br>Maximum: **1024** |
| malware | **malware** object | Malware |
| system_info | Object | System information. |
| process | Array of **process** objects | Process information.<br>Array Length: **0 - 999** |
| user_info | Array of **user_info** objects | User Details<br>Array Length: **0 - 999** |
| file_info | Array of **file_info** objects | Document Information<br>Array Length: **0 - 999** |
| system_alert_table | Object | Layout fields in the incident list. |

**Table 4-140** environment

| Parameter | Type | Description |
| --- | --- | --- |
| vendor_type | String | Environment provider. The value can be **HWCP**, **HWC**, **AWS**, **Azure**, or **GCP**.<br>Minimum: **0**<br>Maximum: **64** |
| domain_id | String | Tenant ID.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region ID. **global** is returned for global services.<br>Minimum: **0**<br>Maximum: **64** |
| cross_workspace_id | String | ID of the source workspace for the data delivery. If the source workspace ID is null, then the destination workspace account ID is used.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID. The default value is null for global services.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-141** data_source

| Parameter | Type | Description |
| --- | --- | --- |
| source_type | Integer | Data source type. The options are as follows--1- Huawei product 2- Third-party product 3- Tenant product<br>Minimum: **1**<br>Maximum: **3**<br>Enumeration values:<br>• **1**<br>• **2**<br>• **3** |

| Parameter | Type | Description |
| --- | --- | --- |
| domain_id | String | Account ID to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | String | ID of the project to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region where the data source is located, for example, cn-north1. For details about the value range, see *Regions and Endpoints*.<br>Minimum: **0**<br>Maximum: **64** |
| company_name | String | Name of the company to which a data source belongs.<br>Minimum: **0**<br>Maximum: **16** |
| product_name | String | Name of the data source.<br>Minimum: **0**<br>Maximum: **24** |
| product_feature | String | Name of the feature of the product that detects the incident.<br>Minimum: **0**<br>Maximum: **24** |
| product_module | String | Threat detection module list.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-142** incident_type

| Parameter | Type | Description |
| --- | --- | --- |
| category | String | Type<br>Minimum: **0**<br>Maximum: **1024** |
| incident_type | String | Incident type.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-143** network_list

| Parameter | Type | Description |
| --- | --- | --- |
| direction | String | Direction. The value can be IN or OUT.<br>Minimum: **0**<br>Maximum: **3**<br>Enumeration values:<br>• **IN**<br>• **OUT** |
| protocol | String | Protocol, including Layer 7 and Layer 4 protocols. For details, see IANA registered name. https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.<br>Minimum: **0**<br>Maximum: **64** |
| src_ip | String | Source IP address<br>Minimum: **0**<br>Maximum: **64** |
| src_port | Integer | Source port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| src_domain | String | Source domain name.<br>Minimum: **0**<br>Maximum: **128** |
| src_geo | **src_geo** object | Geographical location of the source IP address. |
| dest_ip | String | Destination IP address<br>Minimum: **32**<br>Maximum: **64** |
| dest_port | String | Destination port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| dest_domain | String | Destination domain name<br>Minimum: **0**<br>Maximum: **128** |
| dest_geo | **dest_geo** object | Geographical location of the destination IP address. |

**Table 4-144** src_geo

| Parameter | Type | Description |
| --- | --- | --- |
| latitude | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-145** dest_geo

| Parameter | Type | Description |
| --- | --- | --- |
| latitude | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-146** resource_list

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Cloud service resource ID.<br>Minimum: **0**<br>Maximum: **36** |
| name | String | Resource name.<br>Minimum: **0**<br>Maximum: **255** |
| type | String | Resource type. This parameter references the value of RMS type on Huawei Cloud.<br>Minimum: **0**<br>Maximum: **64** |
| provider | String | Cloud service name, which is the same as the provider field in the RMS service.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region ID in Huawei Cloud, for example, cn-north-1.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| ep_id | String | Specifies the enterprise project ID.<br>Minimum: **0**<br>Maximum: **128** |
| ep_name | String | Enterprise Project Name<br>Minimum: **0**<br>Maximum: **128** |

| Parameter | Type | Description |
| --- | --- | --- |
| tags | String | Resource tag.<br>1. A maximum of 50 key/value pairs are supported.<br>2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _, :, /,@<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-147** remediation

| Parameter | Type | Description |
| --- | --- | --- |
| recommendation | String | Recommended solution.<br>Minimum: **0**<br>Maximum: **128** |
| url | String | Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-148** malware

| Parameter | Type | Description |
| --- | --- | --- |
| malware_family | String | Malicious family.<br>Minimum: **0**<br>Maximum: **64** |
| malware_class | String | Malware category.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-149** process

| Parameter | Type | Description |
| --- | --- | --- |
| process_name | String | Process name.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| process_path | String | Process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_pid | Integer | Process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_uid | Integer | Process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_cmdline | String | Process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_parent_name | String | Parent process name.<br>Minimum: **0**<br>Maximum: **64** |
| process_parent_path | String | Parent process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_parent_pid | Integer | Parent process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_parent_uid | Integer | Parent process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_parent_cmdline | String | Parent process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_child_name | String | Subprocess name.<br>Minimum: **0**<br>Maximum: **64** |
| process_child_path | String | Subprocess execution file path.<br>Minimum: **0**<br>Maximum: **512** |

| Parameter | Type | Description |
| --- | --- | --- |
| process_child_pid | Integer | Subprocess ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_child_uid | Integer | Subprocess user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_child_cmdline | String | Subprocess command line<br>Minimum: **0**<br>Maximum: **128** |
| process_launche_time | String | Incident start time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| process_terminate_time | String | Process end time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

**Table 4-150** user_info

| Parameter | Type | Description |
| --- | --- | --- |
| user_id | String | User UID<br>Minimum: **0**<br>Maximum: **36** |
| user_name | String | Username<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-151** file_info

| Parameter | Type | Description |
| --- | --- | --- |
| file_path | String | File path/name.<br>Minimum: **0**<br>Maximum: **128** |
| file_content | String | File path/name.<br>Minimum: **0**<br>Maximum: **1024** |
| file_new_path | String | New file path/name.<br>Minimum: **32**<br>Maximum: **64** |
| file_hash | String | File Hash<br>Minimum: **0**<br>Maximum: **128** |
| file_md5 | String | File MD5<br>Minimum: **0**<br>Maximum: **128** |
| file_sha256 | String | File SHA256<br>Minimum: **0**<br>Maximum: **128** |
| file_attr | String | File attribute.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-152** dataclass_ref

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Unique identifier of a data class. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| name | String | Data class name.<br>Minimum: **0**<br>Maximum: **36** |

**Status code: 400**

**Table 4-153** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-154** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Example request for querying the incident list. To query the medium-risk incidents in the open state from January 20, 2024 to January 26, 2024, sort the incidents by create time in descending order, return to the first page, with 10 records on each page.

```
{
  "limit" : 10,
  "offset" : 0,
  "sort_by" : "create_time",
  "order" : "DESC",
  "condition" : {
    "conditions" : [ {
      "name" : "severity",
      "data" : [ "severity", "=", "Medium" ]
    }, {
      "name" : "handle_status",
      "data" : [ "handle_status", "=", "Open" ]
    } ],
    "logics" : [ "severity", "and", "handle_status" ]
  },
  "from_date" : "2024-01-20T00:00:00.000Z+0800",
  "to_date" : "2024-01-26T23:59:59.999Z+0800"
}
```

## Example Responses

**Status code: 200**

Response body of the request for querying the incident list.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "total" : 41,
  "limit" : 2,
```

```
"offset" : 1,
"success" : true,
"data" : [ {
  "data_object" : {
    "version" : "1.0",
    "environment" : {
      "vendor_type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "data_source" : {
      "source_type" : 3,
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "first_observed_time" : "2021-01-30T23:00:00Z+0800",
    "last_observed_time" : "2021-01-30T23:00:00Z+0800",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "arrive_time" : "2021-01-30T23:00:00Z+0800",
    "title" : "MyXXX",
    "description" : "This my XXXX",
    "source_url" : "http://xxx",
    "count" : 4,
    "confidence" : 4,
    "severity" : "TIPS",
    "criticality" : 4,
    "incident_type" : { },
    "network_list" : [ {
      "direction" : {
        "IN" : null
      },
      "protocol" : "TCP",
      "src_ip" : "192.168.0.1",
      "src_port" : "1",
      "src_domain" : "xxx",
      "dest_ip" : "192.168.0.1",
      "dest_port" : "1",
      "dest_domain" : "xxx",
      "src_geo" : {
        "latitude" : 90,
        "longitude" : 180
      },
      "dest_geo" : {
        "latitude" : 90,
        "longitude" : 180
      }
    } ],
    "resource_list" : [ {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "MyXXX",
      "type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_name" : "MyXXX",
      "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    } ],
    "remediation" : {
      "recommendation" : "MyXXX",
      "url" : "MyXXX"
    },
    "verification_state" : "Unknown,True_Positive,False_Positive The default value is Unknown.",
    "handle_status" : "Open – enabled.Block – blocked.Closed – closed.The default value is Open.",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
```

```
    "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm, Eradication& Recovery| Post-Incident-
Activity",
    "simulation" : "false",
    "actor" : "Tom",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "False positive; Resolved; Duplicate; Others",
    "close_comment" : "False positive; Resolved; Duplicate; Others",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "Malicious memory occupation."
    },
    "system_info" : { },
    "process" : [ {
      "process_name" : "MyXXX",
      "process_path" : "MyXXX",
      "process_pid" : 123,
      "process_uid" : 123,
      "process_cmdline" : "MyXXX"
    } ],
    "user_info" : [ {
      "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "user_name" : "MyXXX"
    } ],
    "file_info" : [ {
      "file_path" : "MyXXX",
      "file_content" : "MyXXX",
      "file_new_path" : "MyXXX",
      "file_hash" : "MyXXX",
      "file_md5" : "MyXXX",
      "file_sha256" : "MyXXX",
      "file_attr" : "MyXXX"
    } ],
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
  },
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
 } ]
}
```


## SDK Sample Code

The SDK sample code is as follows.

## Java

Example request for querying the incident list. To query the medium-risk incidents in the open state from January 20, 2024 to January 26, 2024, sort the incidents by create time in descending order, return to the first page, with 10 records on each page.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;
```

```
public class ListIncidentsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListIncidentsRequest request = new ListIncidentsRequest();
        DataobjectSearch body = new DataobjectSearch();
        List<String> listConditionLogics = new ArrayList<>();
        listConditionLogics.add("severity");
        listConditionLogics.add("and");
        listConditionLogics.add("handle_status");
        List<String> listConditionsData = new ArrayList<>();
        listConditionsData.add("handle_status");
        listConditionsData.add("=");
        listConditionsData.add("Open");
        List<String> listConditionsData1 = new ArrayList<>();
        listConditionsData1.add("severity");
        listConditionsData1.add("=");
        listConditionsData1.add("Medium");
        List<DataobjectSearchConditionConditions> listConditionConditions = new ArrayList<>();
        listConditionConditions.add(
            new DataobjectSearchConditionConditions()
                .withName("severity")
                .withData(listConditionsData1)
        );
        listConditionConditions.add(
            new DataobjectSearchConditionConditions()
                .withName("handle_status")
                .withData(listConditionsData)
        );
        DataobjectSearchCondition conditionbody = new DataobjectSearchCondition();
        conditionbody.withConditions(listConditionConditions)
            .withLogics(listConditionLogics);
        body.withCondition(conditionbody);
        body.withToDate("2024-01-26T23:59:59.999Z+0800");
        body.withFromDate("2024-01-20T00:00:00.000Z+0800");
        body.withOrder(DataobjectSearch.OrderEnum.fromValue("DESC"));
        body.withSortBy("create_time");
        body.withOffset(0);
        body.withLimit(10);
        request.withBody(body);
        try {
            ListIncidentsResponse response = client.listIncidents(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
```

```
        }
    }
}
```

## Python

Example request for querying the incident list. To query the medium-risk incidents in the open state from January 20, 2024 to January 26, 2024, sort the incidents by create time in descending order, return to the first page, with 10 records on each page.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListIncidentsRequest()
        listLogicsCondition = [
            "severity",
            "and",
            "handle_status"
        ]
        listDataConditions = [
            "handle_status",
            "=",
            "Open"
        ]
        listDataConditions1 = [
            "severity",
            "=",
            "Medium"
        ]
        listConditionsCondition = [
            DataobjectSearchConditionConditions(
                name="severity",
                data=listDataConditions1
            ),
            DataobjectSearchConditionConditions(
                name="handle_status",
                data=listDataConditions
            )
        ]
        conditionbody = DataobjectSearchCondition(
            conditions=listConditionsCondition,
            logics=listLogicsCondition
        )
        request.body = DataobjectSearch(
            condition=conditionbody,
            to_date="2024-01-26T23:59:59.999Z+0800",
```

```
            from_date="2024-01-20T00:00:00.000Z+0800",
            order="DESC",
            sort_by="create_time",
            offset=0,
            limit=10
        )
        response = client.list_incidents(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Example request for querying the incident list. To query the medium-risk incidents in the open state from January 20, 2024 to January 26, 2024, sort the incidents by create time in descending order, return to the first page, with 10 records on each page.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListIncidentsRequest{}
    var listLogicsCondition = []string{
        "severity",
        "and",
        "handle_status",
    }
    var listDataConditions = []string{
        "handle_status",
        "=",
        "Open",
    }
    var listDataConditions1 = []string{
        "severity",
        "=",
        "Medium",
    }
    nameConditions:= "severity"
```

```
    nameConditions1:= "handle_status"
    var listConditionsCondition = []model.DataobjectSearchConditionConditions{
        {
            Name: &nameConditions,
            Data: &listDataConditions1,
        },
        {
            Name: &nameConditions1,
            Data: &listDataConditions,
        },
    }
    conditionbody := &model.DataobjectSearchCondition{
        Conditions: &listConditionsCondition,
        Logics: &listLogicsCondition,
    }
    toDateDataobjectSearch:= "2024-01-26T23:59:59.999Z+0800"
    fromDateDataobjectSearch:= "2024-01-20T00:00:00.000Z+0800"
    orderDataobjectSearch:= model.GetDataobjectSearchOrderEnum().DESC
    sortByDataobjectSearch:= "create_time"
    offsetDataobjectSearch:= int32(0)
    limitDataobjectSearch:= int32(10)
    request.Body = &model.DataobjectSearch{
        Condition: conditionbody,
        ToDate: &toDateDataobjectSearch,
        FromDate: &fromDateDataobjectSearch,
        Order: &orderDataobjectSearch,
        SortBy: &sortByDataobjectSearch,
        Offset: &offsetDataobjectSearch,
        Limit: &limitDataobjectSearch,
    }
    response, err := client.ListIncidents(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response body of the request for querying the incident list. |
| 400 | Response body of the failed requests for querying the incident list. |

## Error Codes

See **Error Codes**.

# 4.2.2 Creating an Incident

## Function

Creating an Incident

## Calling Method

For details, see **Calling APIs**.

## URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/incidents

**Table 4-155** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

## Request Parameters

**Table 4-156** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **0**<br>Maximum: **2097152** |
| content-type | Yes | String | Content type.<br>Default: **application/json;charset=UTF-8**<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-157** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| data_object | No | **Incident** object | Incident entity information. |

**Table 4-158** Incident

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| version | No | String | Version of the data source of an incident. The version must be one officially released by the Huawei Cloud SSA service.<br>Minimum: **0**<br>Maximum: **64** |
| id | No | String | Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | No | String | ID of the account (domain_id) to whom the data is delivered and hosted.<br>Minimum: **0**<br>Maximum: **36** |
| region_id | No | String | ID of the region where the account to whom the data is delivered and hosted belongs to.<br>Minimum: **0**<br>Maximum: **36** |
| workspace_id | No | String | ID of the current workspace.<br>Minimum: **0**<br>Maximum: **36** |
| labels | No | String | Tag (display only)<br>Minimum: **0**<br>Maximum: **1024** |
| environment | No | **environment** object | Coordinates of the environment where the incident was generated. |
| data_source | No | **data_source** object | Source the data is first reported. |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| first_observed_time | No | String | First discovery time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| last_observed_time | No | String | First discovery time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| create_time | No | String | Recording time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| arrive_time | No | String | Data receiving time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| title | No | String | Incident title.<br>Minimum: **0**<br>Maximum: **255** |
| description | No | String | Event Description<br>Minimum: **0**<br>Maximum: **1024** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| source_url | No | String | Incident URL, which points to the page of the current incident description in the data source product.<br>Minimum: **0**<br>Maximum: **1024** |
| count | No | Integer | Incident occurrences<br>Minimum: **0**<br>Maximum: **999** |
| confidence | No | Integer | Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or incident. Value range -- 0-100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.<br>Minimum: **0**<br>Maximum: **100** |
| severity | No | String | Severity level. Value range: Tips \| Low \| Medium \| High \| Fatal Description:<br>• **0**: TIPS: No threats are found.<br>• **1**: LOW: No actions are required for the threat.<br>• **2**: MEDIUM: The threat needs to be handled but is not urgent.<br>• **3**: HIGH: The threat must be handled preferentially.<br>• **4**: FATAL: The threat must be handled immediately to prevent further damage.<br>Minimum: **3**<br>Maximum: **6**<br>Enumeration values:<br>• **Tips**<br>• **Low**<br>• **Medium**<br>• **High**<br>• **Fatal** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| criticality | No | Integer | Criticality, which specifies the importance level of the resources involved in an incident. Value range -- 0 to 100. The value 0 indicates that the resource is not critical, and 100 indicates that the resource is critical.<br>Minimum: **0**<br>Maximum: **100** |
| incident_type | No | **incident_type** object | Incident categories. For details, see the Alert Incident Type Definition. |
| network_list | No | Array of **network_list** objects | Network Information<br>Array Length: **0 - 999** |
| resource_list | No | Array of **resource_list** objects | Affected resources.<br>Array Length: **0 - 999** |
| remediation | No | **remediation** object | Remedy measure. |
| verification_state | No | String | Verification status, which identifies the accuracy of an incident. The options are as follows: – Unknown – True_Positive – False_Positive Enter Unknown by default.<br>Minimum: **32**<br>Maximum: **64**<br>Enumeration values:<br>• **Unknown**<br>• **True_Positive**<br>• **False_Positive** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| handle_status | No | String | Incident handling status. The options are as follows:<br>• Open: enabled.<br>• Block: blocked.<br>• Closed: closed. The default value is Open.<br>Minimum: **4**<br>Maximum: **5**<br>Enumeration values:<br>• **Open**<br>• **Block**<br>• **Closed** |
| sla | No | Integer | Risk close time -- Set the acceptable risk duration. Unit -- Hour<br>Minimum: **0**<br>Maximum: **999** |
| update_time | No | String | Update time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the alert occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| close_time | No | String | Closing time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| ipdrr_phase | No | String | Period/Handling phase No. Prepartion\|Detection and Analysis\|Containm, Eradication& Recovery\|Post-Incident-Activity<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **Prepartion**<br>• **Detection and Analysis**<br>• **Containm, Eradication& Recovery**<br>• **Post-Incident-Activity** |
| simulation | No | String | Debugging field.<br>Minimum: **0**<br>Maximum: **64** |
| actor | No | String | Incident investigator.<br>Minimum: **0**<br>Maximum: **64** |
| owner | No | String | Owner and service owner.<br>Minimum: **0**<br>Maximum: **64** |
| creator | No | String | Creator<br>Minimum: **0**<br>Maximum: **64** |
| close_reason | No | String | Close reason.<br>• False positive.<br>• Resolved<br>• Repeated<br>• Other<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **False detection**<br>• **Resolved**<br>• **Repeated**<br>• **Other** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| close_comment | No | String | Whether to close comment.<br>Minimum: **0**<br>Maximum: **1024** |
| malware | No | **malware** object | Malware |
| system_info | No | Object | System information. |
| process | No | Array of **process** objects | Process information.<br>Array Length: **0 - 999** |
| user_info | No | Array of **user_info** objects | User Details<br>Array Length: **0 - 999** |
| file_info | No | Array of **file_info** objects | Document Information<br>Array Length: **0 - 999** |
| system_alert_table | No | Object | Layout fields in the incident list. |

**Table 4-159** environment

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| vendor_type | No | String | Environment provider. The value can be **HWCP**, **HWC**, **AWS**, **Azure**, or **GCP**.<br>Minimum: **0**<br>Maximum: **64** |
| domain_id | No | String | Tenant ID.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | No | String | Region ID. **global** is returned for global services.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| cross_workspace_id | No | String | ID of the source workspace for the data delivery. If the source workspace ID is null, then the destination workspace account ID is used.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | No | String | Project ID. The default value is null for global services.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-160** data_source

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| source_type | No | Integer | Data source type. The options are as follows-- 1- Huawei product 2- Third-party product 3- Tenant product<br>Minimum: **1**<br>Maximum: **3**<br>Enumeration values:<br>• **1**<br>• **2**<br>• **3** |
| domain_id | No | String | Account ID to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | No | String | ID of the project to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | No | String | Region where the data source is located, for example, cn-north1. For details about the value range, see *Regions and Endpoints*.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| company_name | No | String | Name of the company to which a data source belongs.<br>Minimum: **0**<br>Maximum: **16** |
| product_name | No | String | Name of the data source.<br>Minimum: **0**<br>Maximum: **24** |
| product_feature | No | String | Name of the feature of the product that detects the incident.<br>Minimum: **0**<br>Maximum: **24** |
| product_module | No | String | Threat detection module list.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-161** incident_type

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| category | No | String | Type<br>Minimum: **0**<br>Maximum: **1024** |
| incident_type | No | String | Incident type.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-162** network_list

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| direction | No | String | Direction. The value can be IN or OUT.<br>Minimum: **0**<br>Maximum: **3**<br>Enumeration values:<br>• **IN**<br>• **OUT** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| protocol | No | String | Protocol, including Layer 7 and Layer 4 protocols. For details, see IANA registered name. https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.<br>Minimum: **0**<br>Maximum: **64** |
| src_ip | No | String | Source IP address<br>Minimum: **0**<br>Maximum: **64** |
| src_port | No | Integer | Source port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| src_domain | No | String | Source domain name.<br>Minimum: **0**<br>Maximum: **128** |
| src_geo | No | **src_geo** object | Geographical location of the source IP address. |
| dest_ip | No | String | Destination IP address<br>Minimum: **32**<br>Maximum: **64** |
| dest_port | No | String | Destination port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| dest_domain | No | String | Destination domain name<br>Minimum: **0**<br>Maximum: **128** |
| dest_geo | No | **dest_geo** object | Geographical location of the destination IP address. |

**Table 4-163** src_geo

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| latitude | No | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | No | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | No | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | No | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-164** dest_geo

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| latitude | No | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | No | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | No | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | No | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-165** resource_list

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| id | No | String | Cloud service resource ID.<br>Minimum: **0**<br>Maximum: **36** |
| name | No | String | Resource name.<br>Minimum: **0**<br>Maximum: **255** |
| type | No | String | Resource type. This parameter references the value of RMS type on Huawei Cloud.<br>Minimum: **0**<br>Maximum: **64** |
| provider | No | String | Cloud service name, which is the same as the provider field in the RMS service.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | No | String | Region ID in Huawei Cloud, for example, cn-north-1.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | No | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | No | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| ep_id | No | String | Specifies the enterprise project ID.<br>Minimum: **0**<br>Maximum: **128** |
| ep_name | No | String | Enterprise Project Name<br>Minimum: **0**<br>Maximum: **128** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| tags | No | String | Resource tag.<br>1. A maximum of 50 key/value pairs are supported.<br>2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _, :, /,@<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-166** remediation

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| recommendation | No | String | Recommended solution.<br>Minimum: **0**<br>Maximum: **128** |
| url | No | String | Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-167** malware

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| malware_family | No | String | Malicious family.<br>Minimum: **0**<br>Maximum: **64** |
| malware_class | No | String | Malware category.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-168** process

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| process_name | No | String | Process name.<br>Minimum: **0**<br>Maximum: **64** |
| process_path | No | String | Process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_pid | No | Integer | Process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_uid | No | Integer | Process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_cmdline | No | String | Process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_parent_name | No | String | Parent process name.<br>Minimum: **0**<br>Maximum: **64** |
| process_parent_path | No | String | Parent process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_parent_pid | No | Integer | Parent process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_parent_uid | No | Integer | Parent process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_parent_cmdline | No | String | Parent process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_child_name | No | String | Subprocess name.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| process_child_path | No | String | Subprocess execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_child_pid | No | Integer | Subprocess ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_child_uid | No | Integer | Subprocess user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_child_cmdline | No | String | Subprocess command line<br>Minimum: **0**<br>Maximum: **128** |
| process_launche_time | No | String | Incident start time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| process_terminate_time | No | String | Process end time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

**Table 4-169** user_info

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| user_id | No | String | User UID<br>Minimum: **0**<br>Maximum: **36** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| user_name | No | String | Username<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-170** file_info

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| file_path | No | String | File path/name.<br>Minimum: **0**<br>Maximum: **128** |
| file_content | No | String | File path/name.<br>Minimum: **0**<br>Maximum: **1024** |
| file_new_path | No | String | New file path/name.<br>Minimum: **32**<br>Maximum: **64** |
| file_hash | No | String | File Hash<br>Minimum: **0**<br>Maximum: **128** |
| file_md5 | No | String | File MD5<br>Minimum: **0**<br>Maximum: **128** |
| file_sha256 | No | String | File SHA256<br>Minimum: **0**<br>Maximum: **128** |
| file_attr | No | String | File attribute.<br>Minimum: **0**<br>Maximum: **1024** |

## Response Parameters

**Status code: 200**

**Table 4-171** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-172** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Message<br>Minimum: **0**<br>Maximum: **1024** |
| data | **IncidentDetail** object | |

**Table 4-173** IncidentDetail

| Parameter | Type | Description |
| --- | --- | --- |
| create_time | String | Recording time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| data_object | **Incident** object | Incident entity information. |
| dataclass_ref | **dataclass_ref** object | Data class object. |
| format_version | Integer | Format version.<br>Minimum: **0**<br>Maximum: **999** |
| id | String | Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |

| Parameter | Type | Description |
| --- | --- | --- |
| project_id | String | ID of the current project.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Update time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the alert occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| version | Integer | Version.<br>Minimum: **0**<br>Maximum: **999** |
| workspace_id | String | ID of the current workspace.<br>Minimum: **0**<br>Maximum: **36** |

**Table 4-174** Incident

| Parameter | Type | Description |
| --- | --- | --- |
| version | String | Version of the data source of an incident. The version must be one officially released by the Huawei Cloud SSA service.<br>Minimum: **0**<br>Maximum: **64** |
| id | String | Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | String | ID of the account (domain_id) to whom the data is delivered and hosted.<br>Minimum: **0**<br>Maximum: **36** |
| region_id | String | ID of the region where the account to whom the data is delivered and hosted belongs to.<br>Minimum: **0**<br>Maximum: **36** |

| Parameter | Type | Description |
| --- | --- | --- |
| workspace_id | String | ID of the current workspace.<br>Minimum: **0**<br>Maximum: **36** |
| labels | String | Tag (display only)<br>Minimum: **0**<br>Maximum: **1024** |
| environment | **environment** object | Coordinates of the environment where the incident was generated. |
| data_source | **data_source** object | Source the data is first reported. |
| first_observed_time | String | First discovery time. The format is ISO 8601-YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| last_observed_time | String | First discovery time. The format is ISO 8601-YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| create_time | String | Recording time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| arrive_time | String | Data receiving time. The format is ISO 8601-YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

| Parameter | Type | Description |
| --- | --- | --- |
| title | String | Incident title.<br>Minimum: **0**<br>Maximum: **255** |
| description | String | Event Description<br>Minimum: **0**<br>Maximum: **1024** |
| source_url | String | Incident URL, which points to the page of the current incident description in the data source product.<br>Minimum: **0**<br>Maximum: **1024** |
| count | Integer | Incident occurrences<br>Minimum: **0**<br>Maximum: **999** |
| confidence | Integer | Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or incident. Value range -- 0-100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.<br>Minimum: **0**<br>Maximum: **100** |
| severity | String | Severity level. Value range: Tips \| Low \| Medium \| High \| Fatal Description:<br>• **0**: TIPS: No threats are found.<br>• **1**: LOW: No actions are required for the threat.<br>• **2**: MEDIUM: The threat needs to be handled but is not urgent.<br>• **3**: HIGH: The threat must be handled preferentially.<br>• **4**: FATAL: The threat must be handled immediately to prevent further damage.<br>Minimum: **3**<br>Maximum: **6**<br>Enumeration values:<br>• **Tips**<br>• **Low**<br>• **Medium**<br>• **High**<br>• **Fatal** |

| Parameter | Type | Description |
| --- | --- | --- |
| criticality | Integer | Criticality, which specifies the importance level of the resources involved in an incident. Value range -- 0 to 100. The value 0 indicates that the resource is not critical, and 100 indicates that the resource is critical.<br>Minimum: **0**<br>Maximum: **100** |
| incident_type | **incident_type** object | Incident categories. For details, see the Alert Incident Type Definition. |
| network_list | Array of **network_list** objects | Network Information<br>Array Length: **0 - 999** |
| resource_list | Array of **resource_list** objects | Affected resources.<br>Array Length: **0 - 999** |
| remediation | **remediation** object | Remedy measure. |
| verification_state | String | Verification status, which identifies the accuracy of an incident. The options are as follows: – Unknown – True_Positive – False_Positive Enter Unknown by default.<br>Minimum: **32**<br>Maximum: **64**<br>Enumeration values:<br>• **Unknown**<br>• **True_Positive**<br>• **False_Positive** |
| handle_status | String | Incident handling status. The options are as follows:<br>• Open: enabled.<br>• Block: blocked.<br>• Closed: closed. The default value is Open.<br>Minimum: **4**<br>Maximum: **5**<br>Enumeration values:<br>• **Open**<br>• **Block**<br>• **Closed** |

| Parameter | Type | Description |
| --- | --- | --- |
| sla | Integer | Risk close time -- Set the acceptable risk duration. Unit -- Hour<br>Minimum: **0**<br>Maximum: **999** |
| update_time | String | Update time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the alert occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| close_time | String | Closing time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| ipdrr_phase | String | Period/Handling phase No. Prepartion\| Detection and Analysis\|Containm, Eradication& Recovery\|Post-Incident-Activity<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **Prepartion**<br>• **Detection and Analysis**<br>• **Containm, Eradication& Recovery**<br>• **Post-Incident-Activity** |
| simulation | String | Debugging field.<br>Minimum: **0**<br>Maximum: **64** |
| actor | String | Incident investigator.<br>Minimum: **0**<br>Maximum: **64** |
| owner | String | Owner and service owner.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| creator | String | Creator<br>Minimum: **0**<br>Maximum: **64** |
| close_reason | String | Close reason.<br>• False positive.<br>• Resolved<br>• Repeated<br>• Other<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **False detection**<br>• **Resolved**<br>• **Repeated**<br>• **Other** |
| close_comment | String | Whether to close comment.<br>Minimum: **0**<br>Maximum: **1024** |
| malware | **malware** object | Malware |
| system_info | Object | System information. |
| process | Array of **process** objects | Process information.<br>Array Length: **0 - 999** |
| user_info | Array of **user_info** objects | User Details<br>Array Length: **0 - 999** |
| file_info | Array of **file_info** objects | Document Information<br>Array Length: **0 - 999** |
| system_alert_table | Object | Layout fields in the incident list. |

**Table 4-175** environment

| Parameter | Type | Description |
| --- | --- | --- |
| vendor_type | String | Environment provider. The value can be **HWCP**, **HWC**, **AWS**, **Azure**, or **GCP**.<br>Minimum: **0**<br>Maximum: **64** |
| domain_id | String | Tenant ID.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region ID. **global** is returned for global services.<br>Minimum: **0**<br>Maximum: **64** |
| cross_workspace_id | String | ID of the source workspace for the data delivery. If the source workspace ID is null, then the destination workspace account ID is used.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID. The default value is null for global services.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-176** data_source

| Parameter | Type | Description |
| --- | --- | --- |
| source_type | Integer | Data source type. The options are as follows--1- Huawei product 2- Third-party product 3- Tenant product<br>Minimum: **1**<br>Maximum: **3**<br>Enumeration values:<br>• **1**<br>• **2**<br>• **3** |

| Parameter | Type | Description |
| --- | --- | --- |
| domain_id | String | Account ID to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | String | ID of the project to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region where the data source is located, for example, cn-north1. For details about the value range, see *Regions and Endpoints*.<br>Minimum: **0**<br>Maximum: **64** |
| company_name | String | Name of the company to which a data source belongs.<br>Minimum: **0**<br>Maximum: **16** |
| product_name | String | Name of the data source.<br>Minimum: **0**<br>Maximum: **24** |
| product_feature | String | Name of the feature of the product that detects the incident.<br>Minimum: **0**<br>Maximum: **24** |
| product_module | String | Threat detection module list.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-177** incident_type

| Parameter | Type | Description |
| --- | --- | --- |
| category | String | Type<br>Minimum: **0**<br>Maximum: **1024** |
| incident_type | String | Incident type.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-178** network_list

| Parameter | Type | Description |
| --- | --- | --- |
| direction | String | Direction. The value can be IN or OUT.<br>Minimum: **0**<br>Maximum: **3**<br>Enumeration values:<br>• **IN**<br>• **OUT** |
| protocol | String | Protocol, including Layer 7 and Layer 4 protocols. For details, see IANA registered name. https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.<br>Minimum: **0**<br>Maximum: **64** |
| src_ip | String | Source IP address<br>Minimum: **0**<br>Maximum: **64** |
| src_port | Integer | Source port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| src_domain | String | Source domain name.<br>Minimum: **0**<br>Maximum: **128** |
| src_geo | **src_geo** object | Geographical location of the source IP address. |
| dest_ip | String | Destination IP address<br>Minimum: **32**<br>Maximum: **64** |
| dest_port | String | Destination port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| dest_domain | String | Destination domain name<br>Minimum: **0**<br>Maximum: **128** |
| dest_geo | **dest_geo** object | Geographical location of the destination IP address. |

**Table 4-179** src_geo

| Parameter | Type | Description |
| --- | --- | --- |
| latitude | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-180** dest_geo

| Parameter | Type | Description |
| --- | --- | --- |
| latitude | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-181** resource_list

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Cloud service resource ID.<br>Minimum: **0**<br>Maximum: **36** |
| name | String | Resource name.<br>Minimum: **0**<br>Maximum: **255** |
| type | String | Resource type. This parameter references the value of RMS type on Huawei Cloud.<br>Minimum: **0**<br>Maximum: **64** |
| provider | String | Cloud service name, which is the same as the provider field in the RMS service.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region ID in Huawei Cloud, for example, cn-north-1.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| ep_id | String | Specifies the enterprise project ID.<br>Minimum: **0**<br>Maximum: **128** |
| ep_name | String | Enterprise Project Name<br>Minimum: **0**<br>Maximum: **128** |

| Parameter | Type | Description |
| --- | --- | --- |
| tags | String | Resource tag.<br>1. A maximum of 50 key/value pairs are supported.<br>2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _, :, /,@<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-182** remediation

| Parameter | Type | Description |
| --- | --- | --- |
| recommendation | String | Recommended solution.<br>Minimum: **0**<br>Maximum: **128** |
| url | String | Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-183** malware

| Parameter | Type | Description |
| --- | --- | --- |
| malware_family | String | Malicious family.<br>Minimum: **0**<br>Maximum: **64** |
| malware_class | String | Malware category.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-184** process

| Parameter | Type | Description |
| --- | --- | --- |
| process_name | String | Process name.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| process_path | String | Process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_pid | Integer | Process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_uid | Integer | Process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_cmdline | String | Process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_parent_name | String | Parent process name.<br>Minimum: **0**<br>Maximum: **64** |
| process_parent_path | String | Parent process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_parent_pid | Integer | Parent process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_parent_uid | Integer | Parent process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_parent_cmdline | String | Parent process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_child_name | String | Subprocess name.<br>Minimum: **0**<br>Maximum: **64** |
| process_child_path | String | Subprocess execution file path.<br>Minimum: **0**<br>Maximum: **512** |

| Parameter | Type | Description |
| --- | --- | --- |
| process_child_pid | Integer | Subprocess ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_child_uid | Integer | Subprocess user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_child_cmdline | String | Subprocess command line<br>Minimum: **0**<br>Maximum: **128** |
| process_launche_time | String | Incident start time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| process_terminate_time | String | Process end time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

**Table 4-185** user_info

| Parameter | Type | Description |
| --- | --- | --- |
| user_id | String | User UID<br>Minimum: **0**<br>Maximum: **36** |
| user_name | String | Username<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-186** file_info

| Parameter | Type | Description |
| --- | --- | --- |
| file_path | String | File path/name.<br>Minimum: **0**<br>Maximum: **128** |
| file_content | String | File path/name.<br>Minimum: **0**<br>Maximum: **1024** |
| file_new_path | String | New file path/name.<br>Minimum: **32**<br>Maximum: **64** |
| file_hash | String | File Hash<br>Minimum: **0**<br>Maximum: **128** |
| file_md5 | String | File MD5<br>Minimum: **0**<br>Maximum: **128** |
| file_sha256 | String | File SHA256<br>Minimum: **0**<br>Maximum: **128** |
| file_attr | String | File attribute.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-187** dataclass_ref

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Unique identifier of a data class. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| name | String | Data class name.<br>Minimum: **0**<br>Maximum: **36** |

**Status code: 400**

**Table 4-188** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-189** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Create an incident. Set the incident title to MyXXX, tag to MyXXX, severity to tips, and occurrence times to 4.

```
{
  "data_object" : {
    "version" : "1.0",
    "environment" : {
      "vendor_type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "data_source" : {
      "source_type" : 3,
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "product_name" : "test",
      "product_feature" : "test"
    },
    "first_observed_time" : "2021-01-30T23:00:00Z+0800",
    "last_observed_time" : "2021-01-30T23:00:00Z+0800",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "arrive_time" : "2021-01-30T23:00:00Z+0800",
    "title" : "MyXXX",
    "labels" : "MyXXX",
    "description" : "This my XXXX",
    "source_url" : "http://xxx",
    "count" : 4,
    "confidence" : 4,
    "severity" : "TIPS",
    "criticality" : 4,
    "incident_type" : {
      "incident_type" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "category" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "network_list" : [ {
```

```
    "direction" : {
      "IN" : null
    },
    "protocol" : "TCP",
    "src_ip" : "192.168.0.1",
    "src_port" : "1",
    "src_domain" : "xxx",
    "dest_ip" : "192.168.0.1",
    "dest_port" : "1",
    "dest_domain" : "xxx",
    "src_geo" : {
      "latitude" : 90,
      "longitude" : 180
    },
    "dest_geo" : {
      "latitude" : 90,
      "longitude" : 180
    }
  } ],
  "resource_list" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "type" : "MyXXX",
    "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "ep_name" : "MyXXX",
    "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  } ],
  "remediation" : {
    "recommendation" : "MyXXX",
    "url" : "MyXXX"
  },
  "verification_state" : "Unknown,True_Positive,False_Positive The default value is Unknown.",
  "handle_status" : "Open – enabled.Block – blocked.Closed – closed.The default value is Open.",
  "sla" : 60000,
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "close_time" : "2021-01-30T23:00:00Z+0800",
  "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm, Eradication& Recovery| Post-Incident-
Activity",
  "simulation" : "false",
  "actor" : "Tom",
  "owner" : "MyXXX",
  "creator" : "MyXXX",
  "close_reason" : "False positive; Resolved; Duplicate; Others",
  "close_comment" : "False positive; Resolved; Duplicate; Others",
  "malware" : {
    "malware_family" : "family",
    "malware_class" : "Malicious memory occupation."
  },
  "system_info" : { },
  "process" : [ {
    "process_name" : "MyXXX",
    "process_path" : "MyXXX",
    "process_pid" : 123,
    "process_uid" : 123,
    "process_cmdline" : "MyXXX"
  } ],
  "user_info" : [ {
    "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "user_name" : "MyXXX"
  } ],
  "file_info" : [ {
    "file_path" : "MyXXX",
    "file_content" : "MyXXX",
    "file_new_path" : "MyXXX",
    "file_hash" : "MyXXX",
    "file_md5" : "MyXXX",
```

```
    "file_sha256" : "MyXXX",
    "file_attr" : "MyXXX"
   } ],
   "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
   "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
  }
}
```

## Example Responses

### Status code: 200

Response body for the requests for creating incidents.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "data_object" : {
      "version" : "1.0",
      "environment" : {
        "vendor_type" : "MyXXX",
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "data_source" : {
        "source_type" : 3,
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "first_observed_time" : "2021-01-30T23:00:00Z+0800",
      "last_observed_time" : "2021-01-30T23:00:00Z+0800",
      "create_time" : "2021-01-30T23:00:00Z+0800",
      "arrive_time" : "2021-01-30T23:00:00Z+0800",
      "title" : "MyXXX",
      "description" : "This my XXXX",
      "source_url" : "http://xxx",
      "count" : 4,
      "confidence" : 4,
      "severity" : "TIPS",
      "criticality" : 4,
      "incident_type" : { },
      "network_list" : [ {
        "direction" : {
          "IN" : null
        },
        "protocol" : "TCP",
        "src_ip" : "192.168.0.1",
        "src_port" : "1",
        "src_domain" : "xxx",
        "dest_ip" : "192.168.0.1",
        "dest_port" : "1",
        "dest_domain" : "xxx",
        "src_geo" : {
          "latitude" : 90,
          "longitude" : 180
        },
        "dest_geo" : {
          "latitude" : 90,
          "longitude" : 180
        }
      } ],
      "resource_list" : [ {
        "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "name" : "MyXXX",
        "type" : "MyXXX",
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
```

```
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_name" : "MyXXX",
      "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
     } ],
     "remediation" : {
      "recommendation" : "MyXXX",
      "url" : "MyXXX"
     },
     "verification_state" : "Unknown,True_Positive,False_Positive The default value is Unknown.",
     "handle_status" : "Open – enabled.Block – blocked.Closed – closed.The default value is Open.",
     "sla" : 60000,
     "update_time" : "2021-01-30T23:00:00Z+0800",
     "close_time" : "2021-01-30T23:00:00Z+0800",
     "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm, Eradication& Recovery| Post-Incident-
Activity",
     "simulation" : "false",
     "actor" : "Tom",
     "owner" : "MyXXX",
     "creator" : "MyXXX",
     "close_reason" : "False positive; Resolved; Duplicate; Others",
     "close_comment" : "False positive; Resolved; Duplicate; Others",
     "malware" : {
      "malware_family" : "family",
      "malware_class" : "Malicious memory occupation."
     },
     "system_info" : { },
     "process" : [ {
      "process_name" : "MyXXX",
      "process_path" : "MyXXX",
      "process_pid" : 123,
      "process_uid" : 123,
      "process_cmdline" : "MyXXX"
     } ],
     "user_info" : [ {
      "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "user_name" : "MyXXX"
     } ],
     "file_info" : [ {
      "file_path" : "MyXXX",
      "file_content" : "MyXXX",
      "file_new_path" : "MyXXX",
      "file_hash" : "MyXXX",
      "file_md5" : "MyXXX",
      "file_sha256" : "MyXXX",
      "file_attr" : "MyXXX"
     } ],
     "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
     "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
    },
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  }
}
```


## SDK Sample Code

The SDK sample code is as follows.

## Java

Create an incident. Set the incident title to MyXXX, tag to MyXXX, severity to tips, and occurrence times to 4.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class CreateIncidentSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateIncidentRequest request = new CreateIncidentRequest();
        CreateIncidentRequestBody body = new CreateIncidentRequestBody();
        List<IncidentFileInfo> listDataObjectFileInfo = new ArrayList<>();
        listDataObjectFileInfo.add(
            new IncidentFileInfo()
                .withFilePath("MyXXX")
                .withFileContent("MyXXX")
                .withFileNewPath("MyXXX")
                .withFileHash("MyXXX")
                .withFileMd5("MyXXX")
                .withFileSha256("MyXXX")
                .withFileAttr("MyXXX")
        );
        List<IncidentUserInfo> listDataObjectUserInfo = new ArrayList<>();
        listDataObjectUserInfo.add(
            new IncidentUserInfo()
                .withUserId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withUserName("MyXXX")
        );
        List<IncidentProcess> listDataObjectProcess = new ArrayList<>();
        listDataObjectProcess.add(
            new IncidentProcess()
                .withProcessName("MyXXX")
                .withProcessPath("MyXXX")
                .withProcessPid(123)
                .withProcessUid(123)
                .withProcessCmdline("MyXXX")
        );
        IncidentMalware malwareDataObject = new IncidentMalware();
        malwareDataObject.withMalwareFamily("family")
            .withMalwareClass("Malicious memory occupation.");
        IncidentRemediation remediationDataObject = new IncidentRemediation();
        remediationDataObject.withRecommendation("MyXXX")
            .withUrl("MyXXX");
        List<IncidentResourceList> listDataObjectResourceList = new ArrayList<>();
        listDataObjectResourceList.add(
```

```
        new IncidentResourceList()
            .withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withName("MyXXX")
            .withType("MyXXX")
            .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withEpId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withEpName("MyXXX")
            .withTags("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    );
    IncidentDestGeo destGeoNetworkList = new IncidentDestGeo();
    destGeoNetworkList.withLatitude(java.math.BigDecimal.valueOf(90))
        .withLongitude(java.math.BigDecimal.valueOf(180));
    IncidentSrcGeo srcGeoNetworkList = new IncidentSrcGeo();
    srcGeoNetworkList.withLatitude(java.math.BigDecimal.valueOf(90))
        .withLongitude(java.math.BigDecimal.valueOf(180));
    List<IncidentNetworkList> listDataObjectNetworkList = new ArrayList<>();
    listDataObjectNetworkList.add(
        new IncidentNetworkList()
            .withDirection(IncidentNetworkList.DirectionEnum.fromValue("{}"))
            .withProtocol("TCP")
            .withSrcIp("192.168.0.1")
            .withSrcPort(1)
            .withSrcDomain("xxx")
            .withSrcGeo(srcGeoNetworkList)
            .withDestIp("192.168.0.1")
            .withDestPort("1")
            .withDestDomain("xxx")
            .withDestGeo(destGeoNetworkList)
    );
    IncidentIncidentType incidentTypeDataObject = new IncidentIncidentType();
    incidentTypeDataObject.withCategory("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withIncidentType("909494e3-558e-46b6-a9eb-07a8e18ca62f");
    IncidentDataSource dataSourceDataObject = new IncidentDataSource();
    dataSourceDataObject.withSourceType(3)
        .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withProductName("test")
        .withProductFeature("test");
    IncidentEnvironment environmentDataObject = new IncidentEnvironment();
    environmentDataObject.withVendorType("MyXXX")
        .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
    Incident dataObjectbody = new Incident();
    dataObjectbody.withVersion("1.0")
        .withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withWorkspaceId("909494e3-558e-46b6-a9eb-07a8e18ca620")
        .withLabels("MyXXX")
        .withEnvironment(environmentDataObject)
        .withDataSource(dataSourceDataObject)
        .withFirstObservedTime("2021-01-30T23:00:00Z+0800")
        .withLastObservedTime("2021-01-30T23:00:00Z+0800")
        .withCreateTime("2021-01-30T23:00:00Z+0800")
        .withArriveTime("2021-01-30T23:00:00Z+0800")
        .withTitle("MyXXX")
        .withDescription("This my XXXX")
        .withSourceUrl("http://xxx")
        .withCount(4)
        .withConfidence(4)
        .withSeverity(Incident.SeverityEnum.fromValue("TIPS"))
        .withCriticality(4)
        .withIncidentType(incidentTypeDataObject)
        .withNetworkList(listDataObjectNetworkList)
        .withResourceList(listDataObjectResourceList)
        .withRemediation(remediationDataObject)
        .withVerificationState(Incident.VerificationStateEnum.fromValue("Unknown,True_Positive,False_Posit
```

```
ive The default value is Unknown."))
            .withHandleStatus(Incident.HandleStatusEnum.fromValue("Open – enabled.Block – blocked.Closed
– closed.The default value is Open."))
            .withSla(60000)
            .withUpdateTime("2021-01-30T23:00:00Z+0800")
            .withCloseTime("2021-01-30T23:00:00Z+0800")
            .withIpdrrPhase(Incident.IpdrrPhaseEnum.fromValue("Prepartion|Detection and Analysis|
Containm,Eradication& Recovery| Post-Incident-Activity"))
            .withSimulation("false")
            .withActor("Tom")
            .withOwner("MyXXX")
            .withCreator("MyXXX")
            .withCloseReason(Incident.CloseReasonEnum.fromValue("False positive; Resolved; Duplicate;
Others"))
            .withCloseComment("False positive; Resolved; Duplicate; Others")
            .withMalware(malwareDataObject)
            .withSystemInfo(new Object())
            .withProcess(listDataObjectProcess)
            .withUserInfo(listDataObjectUserInfo)
            .withFileInfo(listDataObjectFileInfo);
        body.withDataObject(dataObjectbody);
        request.withBody(body);
        try {
            CreateIncidentResponse response = client.createIncident(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Create an incident. Set the incident title to MyXXX, tag to MyXXX, severity to tips, and occurrence times to 4.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateIncidentRequest()
```

```
listFileInfoDataObject = [
    IncidentFileInfo(
        file_path="MyXXX",
        file_content="MyXXX",
        file_new_path="MyXXX",
        file_hash="MyXXX",
        file_md5="MyXXX",
        file_sha256="MyXXX",
        file_attr="MyXXX"
    )
]
listUserInfoDataObject = [
    IncidentUserInfo(
        user_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        user_name="MyXXX"
    )
]
listProcessDataObject = [
    IncidentProcess(
        process_name="MyXXX",
        process_path="MyXXX",
        process_pid=123,
        process_uid=123,
        process_cmdline="MyXXX"
    )
]
malwareDataObject = IncidentMalware(
    malware_family="family",
    malware_class="Malicious memory occupation."
)
remediationDataObject = IncidentRemediation(
    recommendation="MyXXX",
    url="MyXXX"
)
listResourceListDataObject = [
    IncidentResourceList(
        id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        name="MyXXX",
        type="MyXXX",
        region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        ep_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        ep_name="MyXXX",
        tags="909494e3-558e-46b6-a9eb-07a8e18ca62f"
    )
]
destGeoNetworkList = IncidentDestGeo(
    latitude=90,
    longitude=180
)
srcGeoNetworkList = IncidentSrcGeo(
    latitude=90,
    longitude=180
)
listNetworkListDataObject = [
    IncidentNetworkList(
        direction="{}",
        protocol="TCP",
        src_ip="192.168.0.1",
        src_port=1,
        src_domain="xxx",
        src_geo=srcGeoNetworkList,
        dest_ip="192.168.0.1",
        dest_port="1",
        dest_domain="xxx",
        dest_geo=destGeoNetworkList
    )
]
```

```
        incidentTypeDataObject = IncidentIncidentType(
            category="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            incident_type="909494e3-558e-46b6-a9eb-07a8e18ca62f"
        )
        dataSourceDataObject = IncidentDataSource(
            source_type=3,
            domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            product_name="test",
            product_feature="test"
        )
        environmentDataObject = IncidentEnvironment(
            vendor_type="MyXXX",
            domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f"
        )
        dataObjectbody = Incident(
            version="1.0",
            id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            workspace_id="909494e3-558e-46b6-a9eb-07a8e18ca620",
            labels="MyXXX",
            environment=environmentDataObject,
            data_source=dataSourceDataObject,
            first_observed_time="2021-01-30T23:00:00Z+0800",
            last_observed_time="2021-01-30T23:00:00Z+0800",
            create_time="2021-01-30T23:00:00Z+0800",
            arrive_time="2021-01-30T23:00:00Z+0800",
            title="MyXXX",
            description="This my XXXX",
            source_url="http://xxx",
            count=4,
            confidence=4,
            severity="TIPS",
            criticality=4,
            incident_type=incidentTypeDataObject,
            network_list=listNetworkListDataObject,
            resource_list=listResourceListDataObject,
            remediation=remediationDataObject,
            verification_state="Unknown,True_Positive,False_Positive The default value is Unknown.",
            handle_status="Open – enabled.Block – blocked.Closed – closed.The default value is Open.",
            sla=60000,
            update_time="2021-01-30T23:00:00Z+0800",
            close_time="2021-01-30T23:00:00Z+0800",
            ipdrr_phase="Prepartion|Detection and Analysis|Containm,Eradication& Recovery| Post-Incident-
Activity",
            simulation="false",
            actor="Tom",
            owner="MyXXX",
            creator="MyXXX",
            close_reason="False positive; Resolved; Duplicate; Others",
            close_comment="False positive; Resolved; Duplicate; Others",
            malware=malwareDataObject,
            system_info={},
            process=listProcessDataObject,
            user_info=listUserInfoDataObject,
            file_info=listFileInfoDataObject
        )
        request.body = CreateIncidentRequestBody(
            data_object=dataObjectbody
        )
        response = client.create_incident(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Create an incident. Set the incident title to MyXXX, tag to MyXXX, severity to tips, and occurrence times to 4.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateIncidentRequest{}
    filePathFileInfo:= "MyXXX"
    fileContentFileInfo:= "MyXXX"
    fileNewPathFileInfo:= "MyXXX"
    fileHashFileInfo:= "MyXXX"
    fileMd5FileInfo:= "MyXXX"
    fileSha256FileInfo:= "MyXXX"
    fileAttrFileInfo:= "MyXXX"
    var listFileInfoDataObject = []model.IncidentFileInfo{
        {
            FilePath: &filePathFileInfo,
            FileContent: &fileContentFileInfo,
            FileNewPath: &fileNewPathFileInfo,
            FileHash: &fileHashFileInfo,
            FileMd5: &fileMd5FileInfo,
            FileSha256: &fileSha256FileInfo,
            FileAttr: &fileAttrFileInfo,
        },
    }
    userIdUserInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    userNameUserInfo:= "MyXXX"
    var listUserInfoDataObject = []model.IncidentUserInfo{
        {
            UserId: &userIdUserInfo,
            UserName: &userNameUserInfo,
        },
    }
    processNameProcess:= "MyXXX"
    processPathProcess:= "MyXXX"
    processPidProcess:= int32(123)
    processUidProcess:= int32(123)
    processCmdlineProcess:= "MyXXX"
    var listProcessDataObject = []model.IncidentProcess{
        {
```

```
        ProcessName: &processNameProcess,
        ProcessPath: &processPathProcess,
        ProcessPid: &processPidProcess,
        ProcessUid: &processUidProcess,
        ProcessCmdline: &processCmdlineProcess,
    },
}
malwareFamilyMalware:= "family"
malwareClassMalware:= "Malicious memory occupation."
malwareDataObject := &model.IncidentMalware{
    MalwareFamily: &malwareFamilyMalware,
    MalwareClass: &malwareClassMalware,
}
recommendationRemediation:= "MyXXX"
urlRemediation:= "MyXXX"
remediationDataObject := &model.IncidentRemediation{
    Recommendation: &recommendationRemediation,
    Url: &urlRemediation,
}
idResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
nameResourceList:= "MyXXX"
typeResourceList:= "MyXXX"
regionIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
domainIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
projectIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
epIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
epNameResourceList:= "MyXXX"
tagsResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
var listResourceListDataObject = []model.IncidentResourceList{
    {
        Id: &idResourceList,
        Name: &nameResourceList,
        Type: &typeResourceList,
        RegionId: &regionIdResourceList,
        DomainId: &domainIdResourceList,
        ProjectId: &projectIdResourceList,
        EpId: &epIdResourceList,
        EpName: &epNameResourceList,
        Tags: &tagsResourceList,
    },
}
latitudeDestGeo:= float32(90)
longitudeDestGeo:= float32(180)
destGeoNetworkList := &model.IncidentDestGeo{
    Latitude: &latitudeDestGeo,
    Longitude: &longitudeDestGeo,
}
latitudeSrcGeo:= float32(90)
longitudeSrcGeo:= float32(180)
srcGeoNetworkList := &model.IncidentSrcGeo{
    Latitude: &latitudeSrcGeo,
    Longitude: &longitudeSrcGeo,
}
directionNetworkList:= model.GetIncidentNetworkListDirectionEnum().{}
protocolNetworkList:= "TCP"
srcIpNetworkList:= "192.168.0.1"
srcPortNetworkList:= int32(1)
srcDomainNetworkList:= "xxx"
destIpNetworkList:= "192.168.0.1"
destPortNetworkList:= "1"
destDomainNetworkList:= "xxx"
var listNetworkListDataObject = []model.IncidentNetworkList{
    {
        Direction: &directionNetworkList,
        Protocol: &protocolNetworkList,
        SrcIp: &srcIpNetworkList,
        SrcPort: &srcPortNetworkList,
        SrcDomain: &srcDomainNetworkList,
        SrcGeo: srcGeoNetworkList,
```

```
            DestIp: &destIpNetworkList,
            DestPort: &destPortNetworkList,
            DestDomain: &destDomainNetworkList,
            DestGeo: destGeoNetworkList,
        },
    }
    categoryIncidentType:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    incidentTypeIncidentType:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    incidentTypeDataObject := &model.IncidentIncidentType{
        Category: &categoryIncidentType,
        IncidentType: &incidentTypeIncidentType,
    }
    sourceTypeDataSource:= int32(3)
    domainIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    projectIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    regionIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    productNameDataSource:= "test"
    productFeatureDataSource:= "test"
    dataSourceDataObject := &model.IncidentDataSource{
        SourceType: &sourceTypeDataSource,
        DomainId: &domainIdDataSource,
        ProjectId: &projectIdDataSource,
        RegionId: &regionIdDataSource,
        ProductName: &productNameDataSource,
        ProductFeature: &productFeatureDataSource,
    }
    vendorTypeEnvironment:= "MyXXX"
    domainIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    regionIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    projectIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    environmentDataObject := &model.IncidentEnvironment{
        VendorType: &vendorTypeEnvironment,
        DomainId: &domainIdEnvironment,
        RegionId: &regionIdEnvironment,
        ProjectId: &projectIdEnvironment,
    }
    versionDataObject:= "1.0"
    idDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    workspaceIdDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca620"
    labelsDataObject:= "MyXXX"
    firstObservedTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    lastObservedTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    createTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    arriveTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    titleDataObject:= "MyXXX"
    descriptionDataObject:= "This my XXXX"
    sourceUrlDataObject:= "http://xxx"
    countDataObject:= int32(4)
    confidenceDataObject:= int32(4)
    severityDataObject:= model.GetIncidentSeverityEnum().TIPS
    criticalityDataObject:= int32(4)
    verificationStateDataObject:=
model.GetIncidentVerificationStateEnum().UNKNOWN,TRUE_POSITIVE,FALSE_POSITIVE_THE_DEFAULT_VAL
UE_IS_UNKNOWN_
    handleStatusDataObject:= model.GetIncidentHandleStatusEnum().OPEN_-_ENABLED_BLOCK_-
_BLOCKED_CLOSED_-_CLOSED_THE_DEFAULT_VALUE_IS_OPEN_
    slaDataObject:= int32(60000)
    updateTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    closeTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    ipdrrPhaseDataObject:= model.GetIncidentIpdrrPhaseEnum().PREPARTION|DETECTION_AND_ANALYSIS|
CONTAINM,ERADICATION&_RECOVERY|_POST_INCIDENT_ACTIVITY
    simulationDataObject:= "false"
    actorDataObject:= "Tom"
    ownerDataObject:= "MyXXX"
    creatorDataObject:= "MyXXX"
    closeReasonDataObject:=
model.GetIncidentCloseReasonEnum().FALSE_POSITIVE;_RESOLVED;_DUPLICATE;_OTHERS
    closeCommentDataObject:= "False positive; Resolved; Duplicate; Others"
    var systemInfoDataObject interface{} = make(map[string]string)
```

```
    dataObjectbody := &model.Incident{
        Version: &versionDataObject,
        Id: &idDataObject,
        WorkspaceId: &workspaceIdDataObject,
        Labels: &labelsDataObject,
        Environment: environmentDataObject,
        DataSource: dataSourceDataObject,
        FirstObservedTime: &firstObservedTimeDataObject,
        LastObservedTime: &lastObservedTimeDataObject,
        CreateTime: &createTimeDataObject,
        ArriveTime: &arriveTimeDataObject,
        Title: &titleDataObject,
        Description: &descriptionDataObject,
        SourceUrl: &sourceUrlDataObject,
        Count: &countDataObject,
        Confidence: &confidenceDataObject,
        Severity: &severityDataObject,
        Criticality: &criticalityDataObject,
        IncidentType: incidentTypeDataObject,
        NetworkList: &listNetworkListDataObject,
        ResourceList: &listResourceListDataObject,
        Remediation: remediationDataObject,
        VerificationState: &verificationStateDataObject,
        HandleStatus: &handleStatusDataObject,
        Sla: &slaDataObject,
        UpdateTime: &updateTimeDataObject,
        CloseTime: &closeTimeDataObject,
        IpdrrPhase: &ipdrrPhaseDataObject,
        Simulation: &simulationDataObject,
        Actor: &actorDataObject,
        Owner: &ownerDataObject,
        Creator: &creatorDataObject,
        CloseReason: &closeReasonDataObject,
        CloseComment: &closeCommentDataObject,
        Malware: malwareDataObject,
        SystemInfo: &systemInfoDataObject,
        Process: &listProcessDataObject,
        UserInfo: &listUserInfoDataObject,
        FileInfo: &listFileInfoDataObject,
    }
    request.Body = &model.CreateIncidentRequestBody{
        DataObject: dataObjectbody,
    }
    response, err := client.CreateIncident(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response body for the requests for creating incidents. |
| 400 | Response body for failed requests for creating incidents. |

## Error Codes

See **Error Codes**.

# 4.2.3 Deleting an Incident

## Function

Deleting an Incident

## Calling Method

For details, see **Calling APIs**.

## URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/incidents

**Table 4-190** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

## Request Parameters

**Table 4-191** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **0**<br>Maximum: **2097152** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| content-type | Yes | String | Content type.<br>Default: **application/json;charset=UTF-8**<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-192** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| batch_ids | No | Array of strings | IDs of deleted alerts.<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 999** |

## Response Parameters

**Status code: 200**

**Table 4-193** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-194** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Message<br>Minimum: **0**<br>Maximum: **1024** |
| data | **data** object | Returned object for batch deleting incidents. |

**Table 4-195** data

| Parameter | Type | Description |
| --- | --- | --- |
| error_ids | Array of strings | IDs of alerts not transferred to incidents<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 100** |
| success_ids | Array of strings | IDs of alerts transferred to incidents.<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 100** |

**Status code: 400**

**Table 4-196** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-197** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Delete the incident whose ID is 909494e3-558e-46b6-a9eb-07a8e18ca621.

```
{
  "batch_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ]
}
```

## Example Responses

**Status code: 200**

The incident deletion result is returned.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "error_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ],
    "success_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ]
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Delete the incident whose ID is 909494e3-558e-46b6-a9eb-07a8e18ca621.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class DeleteIncidentSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteIncidentRequest request = new DeleteIncidentRequest();
        DeleteIncidentRequestBody body = new DeleteIncidentRequestBody();
        List<String> listbodyBatchIds = new ArrayList<>();
        listbodyBatchIds.add("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withBatchIds(listbodyBatchIds);
        request.withBody(body);
        try {
            DeleteIncidentResponse response = client.deleteIncident(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
```

```
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Delete the incident whose ID is 909494e3-558e-46b6-a9eb-07a8e18ca621.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteIncidentRequest()
        listBatchIdsbody = [
            "909494e3-558e-46b6-a9eb-07a8e18ca62f"
        ]
        request.body = DeleteIncidentRequestBody(
            batch_ids=listBatchIdsbody
        )
        response = client.delete_incident(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Delete the incident whose ID is 909494e3-558e-46b6-a9eb-07a8e18ca621.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
```

```
example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteIncidentRequest{}
    var listBatchIdsbody = []string{
        "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    }
    request.Body = &model.DeleteIncidentRequestBody{
        BatchIds: &listBatchIdsbody,
    }
    response, err := client.DeleteIncident(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | The incident deletion result is returned. |
| 400 | Response body for failed requests for deleting incidents. |

## Error Codes

See **Error Codes**.

# 4.2.4 Obtaining Details of an Incident

## Function

This API is used to obtain details of an incident.

## Calling Method

For details, see **Calling APIs**.

## URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/{incident_id}

**Table 4-198** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| incident_id | Yes | String | Incident ID.<br>Minimum: **32**<br>Maximum: **36** |

## Request Parameters

**Table 4-199** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **0**<br>Maximum: **2097152** |
| content-type | Yes | String | Content type.<br>Default: **application/json;charset=UTF-8**<br>Minimum: **0**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-200** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Message<br>Minimum: **0**<br>Maximum: **1024** |
| data | **IncidentDetail** object | |

**Table 4-201** IncidentDetail

| Parameter | Type | Description |
| --- | --- | --- |
| create_time | String | Recording time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| data_object | **Incident** object | Incident entity information. |
| dataclass_ref | **dataclass_ref** object | Data class object. |
| format_version | Integer | Format version.<br>Minimum: **0**<br>Maximum: **999** |
| id | String | Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | String | ID of the current project.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| update_time | String | Update time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the alert occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| version | Integer | Version.<br>Minimum: **0**<br>Maximum: **999** |
| workspace_id | String | ID of the current workspace.<br>Minimum: **0**<br>Maximum: **36** |

**Table 4-202** Incident

| Parameter | Type | Description |
| --- | --- | --- |
| version | String | Version of the data source of an incident. The version must be one officially released by the Huawei Cloud SSA service.<br>Minimum: **0**<br>Maximum: **64** |
| id | String | Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | String | ID of the account (domain_id) to whom the data is delivered and hosted.<br>Minimum: **0**<br>Maximum: **36** |
| region_id | String | ID of the region where the account to whom the data is delivered and hosted belongs to.<br>Minimum: **0**<br>Maximum: **36** |
| workspace_id | String | ID of the current workspace.<br>Minimum: **0**<br>Maximum: **36** |

| Parameter | Type | Description |
| --- | --- | --- |
| labels | String | Tag (display only)<br>Minimum: **0**<br>Maximum: **1024** |
| environment | **environment** object | Coordinates of the environment where the incident was generated. |
| data_source | **data_source** object | Source the data is first reported. |
| first_observed_time | String | First discovery time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| last_observed_time | String | First discovery time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| create_time | String | Recording time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| arrive_time | String | Data receiving time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| title | String | Incident title.<br>Minimum: **0**<br>Maximum: **255** |

| Parameter | Type | Description |
| --- | --- | --- |
| description | String | Event Description<br>Minimum: **0**<br>Maximum: **1024** |
| source_url | String | Incident URL, which points to the page of the current incident description in the data source product.<br>Minimum: **0**<br>Maximum: **1024** |
| count | Integer | Incident occurrences<br>Minimum: **0**<br>Maximum: **999** |
| confidence | Integer | Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or incident. Value range -- 0-100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.<br>Minimum: **0**<br>Maximum: **100** |
| severity | String | Severity level. Value range: Tips \| Low \| Medium \| High \| Fatal Description:<br>• **0**: TIPS: No threats are found.<br>• **1**: LOW: No actions are required for the threat.<br>• **2**: MEDIUM: The threat needs to be handled but is not urgent.<br>• **3**: HIGH: The threat must be handled preferentially.<br>• **4**: FATAL: The threat must be handled immediately to prevent further damage.<br>Minimum: **3**<br>Maximum: **6**<br>Enumeration values:<br>• **Tips**<br>• **Low**<br>• **Medium**<br>• **High**<br>• **Fatal** |

| Parameter | Type | Description |
| --- | --- | --- |
| criticality | Integer | Criticality, which specifies the importance level of the resources involved in an incident. Value range -- 0 to 100. The value 0 indicates that the resource is not critical, and 100 indicates that the resource is critical.<br>Minimum: **0**<br>Maximum: **100** |
| incident_type | **incident_type** object | Incident categories. For details, see the Alert Incident Type Definition. |
| network_list | Array of **network_list** objects | Network Information<br>Array Length: **0 - 999** |
| resource_list | Array of **resource_list** objects | Affected resources.<br>Array Length: **0 - 999** |
| remediation | **remediation** object | Remedy measure. |
| verification_state | String | Verification status, which identifies the accuracy of an incident. The options are as follows: – Unknown – True_Positive – False_Positive Enter Unknown by default.<br>Minimum: **32**<br>Maximum: **64**<br>Enumeration values:<br>• **Unknown**<br>• **True_Positive**<br>• **False_Positive** |
| handle_status | String | Incident handling status. The options are as follows:<br>• Open: enabled.<br>• Block: blocked.<br>• Closed: closed. The default value is Open.<br>Minimum: **4**<br>Maximum: **5**<br>Enumeration values:<br>• **Open**<br>• **Block**<br>• **Closed** |

| Parameter | Type | Description |
| --- | --- | --- |
| sla | Integer | Risk close time -- Set the acceptable risk duration. Unit -- Hour<br>Minimum: **0**<br>Maximum: **999** |
| update_time | String | Update time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the alert occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| close_time | String | Closing time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| ipdrr_phase | String | Period/Handling phase No. Prepartion\| Detection and Analysis\|Containm, Eradication& Recovery\|Post-Incident-Activity<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **Prepartion**<br>• **Detection and Analysis**<br>• **Containm, Eradication& Recovery**<br>• **Post-Incident-Activity** |
| simulation | String | Debugging field.<br>Minimum: **0**<br>Maximum: **64** |
| actor | String | Incident investigator.<br>Minimum: **0**<br>Maximum: **64** |
| owner | String | Owner and service owner.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| creator | String | Creator<br>Minimum: **0**<br>Maximum: **64** |
| close_reason | String | Close reason.<br>• False positive.<br>• Resolved<br>• Repeated<br>• Other<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **False detection**<br>• **Resolved**<br>• **Repeated**<br>• **Other** |
| close_comment | String | Whether to close comment.<br>Minimum: **0**<br>Maximum: **1024** |
| malware | **malware** object | Malware |
| system_info | Object | System information. |
| process | Array of **process** objects | Process information.<br>Array Length: **0 - 999** |
| user_info | Array of **user_info** objects | User Details<br>Array Length: **0 - 999** |
| file_info | Array of **file_info** objects | Document Information<br>Array Length: **0 - 999** |
| system_alert_table | Object | Layout fields in the incident list. |

**Table 4-203** environment

| Parameter | Type | Description |
| --- | --- | --- |
| vendor_type | String | Environment provider. The value can be **HWCP**, **HWC**, **AWS**, **Azure**, or **GCP**.<br>Minimum: **0**<br>Maximum: **64** |
| domain_id | String | Tenant ID.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region ID. **global** is returned for global services.<br>Minimum: **0**<br>Maximum: **64** |
| cross_workspace_id | String | ID of the source workspace for the data delivery. If the source workspace ID is null, then the destination workspace account ID is used.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID. The default value is null for global services.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-204** data_source

| Parameter | Type | Description |
| --- | --- | --- |
| source_type | Integer | Data source type. The options are as follows--1- Huawei product 2- Third-party product 3- Tenant product<br>Minimum: **1**<br>Maximum: **3**<br>Enumeration values:<br>• **1**<br>• **2**<br>• **3** |

| Parameter | Type | Description |
| --- | --- | --- |
| domain_id | String | Account ID to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | String | ID of the project to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region where the data source is located, for example, cn-north1. For details about the value range, see *Regions and Endpoints*.<br>Minimum: **0**<br>Maximum: **64** |
| company_name | String | Name of the company to which a data source belongs.<br>Minimum: **0**<br>Maximum: **16** |
| product_name | String | Name of the data source.<br>Minimum: **0**<br>Maximum: **24** |
| product_feature | String | Name of the feature of the product that detects the incident.<br>Minimum: **0**<br>Maximum: **24** |
| product_module | String | Threat detection module list.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-205** incident_type

| Parameter | Type | Description |
| --- | --- | --- |
| category | String | Type<br>Minimum: **0**<br>Maximum: **1024** |
| incident_type | String | Incident type.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-206** network_list

| Parameter | Type | Description |
| --- | --- | --- |
| direction | String | Direction. The value can be IN or OUT.<br>Minimum: **0**<br>Maximum: **3**<br>Enumeration values:<br>• **IN**<br>• **OUT** |
| protocol | String | Protocol, including Layer 7 and Layer 4 protocols. For details, see IANA registered name. https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.<br>Minimum: **0**<br>Maximum: **64** |
| src_ip | String | Source IP address<br>Minimum: **0**<br>Maximum: **64** |
| src_port | Integer | Source port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| src_domain | String | Source domain name.<br>Minimum: **0**<br>Maximum: **128** |
| src_geo | **src_geo** object | Geographical location of the source IP address. |
| dest_ip | String | Destination IP address<br>Minimum: **32**<br>Maximum: **64** |
| dest_port | String | Destination port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| dest_domain | String | Destination domain name<br>Minimum: **0**<br>Maximum: **128** |
| dest_geo | **dest_geo** object | Geographical location of the destination IP address. |

**Table 4-207** src_geo

| Parameter | Type | Description |
| --- | --- | --- |
| latitude | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-208** dest_geo

| Parameter | Type | Description |
| --- | --- | --- |
| latitude | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-209** resource_list

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Cloud service resource ID.<br>Minimum: **0**<br>Maximum: **36** |
| name | String | Resource name.<br>Minimum: **0**<br>Maximum: **255** |
| type | String | Resource type. This parameter references the value of RMS type on Huawei Cloud.<br>Minimum: **0**<br>Maximum: **64** |
| provider | String | Cloud service name, which is the same as the provider field in the RMS service.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region ID in Huawei Cloud, for example, cn-north-1.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| ep_id | String | Specifies the enterprise project ID.<br>Minimum: **0**<br>Maximum: **128** |
| ep_name | String | Enterprise Project Name<br>Minimum: **0**<br>Maximum: **128** |

| Parameter | Type | Description |
| --- | --- | --- |
| tags | String | Resource tag.<br>1. A maximum of 50 key/value pairs are supported.<br>2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _, :, /,@<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-210** remediation

| Parameter | Type | Description |
| --- | --- | --- |
| recommendation | String | Recommended solution.<br>Minimum: **0**<br>Maximum: **128** |
| url | String | Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-211** malware

| Parameter | Type | Description |
| --- | --- | --- |
| malware_family | String | Malicious family.<br>Minimum: **0**<br>Maximum: **64** |
| malware_class | String | Malware category.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-212** process

| Parameter | Type | Description |
| --- | --- | --- |
| process_name | String | Process name.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| process_path | String | Process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_pid | Integer | Process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_uid | Integer | Process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_cmdline | String | Process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_parent_name | String | Parent process name.<br>Minimum: **0**<br>Maximum: **64** |
| process_parent_path | String | Parent process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_parent_pid | Integer | Parent process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_parent_uid | Integer | Parent process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_parent_cmdline | String | Parent process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_child_name | String | Subprocess name.<br>Minimum: **0**<br>Maximum: **64** |
| process_child_path | String | Subprocess execution file path.<br>Minimum: **0**<br>Maximum: **512** |

| Parameter | Type | Description |
| --- | --- | --- |
| process_child_pid | Integer | Subprocess ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_child_uid | Integer | Subprocess user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_child_cmdline | String | Subprocess command line<br>Minimum: **0**<br>Maximum: **128** |
| process_launche_time | String | Incident start time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| process_terminate_time | String | Process end time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

**Table 4-213** user_info

| Parameter | Type | Description |
| --- | --- | --- |
| user_id | String | User UID<br>Minimum: **0**<br>Maximum: **36** |
| user_name | String | Username<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-214** file_info

| Parameter | Type | Description |
| --- | --- | --- |
| file_path | String | File path/name.<br>Minimum: **0**<br>Maximum: **128** |
| file_content | String | File path/name.<br>Minimum: **0**<br>Maximum: **1024** |
| file_new_path | String | New file path/name.<br>Minimum: **32**<br>Maximum: **64** |
| file_hash | String | File Hash<br>Minimum: **0**<br>Maximum: **128** |
| file_md5 | String | File MD5<br>Minimum: **0**<br>Maximum: **128** |
| file_sha256 | String | File SHA256<br>Minimum: **0**<br>Maximum: **128** |
| file_attr | String | File attribute.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-215** dataclass_ref

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Unique identifier of a data class. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| name | String | Data class name.<br>Minimum: **0**<br>Maximum: **36** |

**Status code: 400**

**Table 4-216** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Response body for requests for obtaining incident details.


```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "data_object" : {
      "version" : "1.0",
      "environment" : {
        "vendor_type" : "MyXXX",
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "data_source" : {
        "source_type" : 3,
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "first_observed_time" : "2021-01-30T23:00:00Z+0800",
      "last_observed_time" : "2021-01-30T23:00:00Z+0800",
      "create_time" : "2021-01-30T23:00:00Z+0800",
      "arrive_time" : "2021-01-30T23:00:00Z+0800",
      "title" : "MyXXX",
      "description" : "This my XXXX",
      "source_url" : "http://xxx",
      "count" : "4",
      "confidence" : 4,
      "severity" : "TIPS",
      "criticality" : 4,
      "incident_type" : { },
      "network_list" : [ {
        "direction" : {
          "IN" : null
        },
        "protocol" : "TCP",
        "src_ip" : "192.168.0.1",
        "src_port" : "1",
        "src_domain" : "xxx",
        "dest_ip" : "192.168.0.1",
```

```
      "dest_port" : "1",
      "dest_domain" : "xxx",
      "src_geo" : {
        "latitude" : 90,
        "longitude" : 180
      },
      "dest_geo" : {
        "latitude" : 90,
        "longitude" : 180
      }
    } ],
    "resource_list" : [ {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "MyXXX",
      "type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_name" : "MyXXX",
      "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    } ],
    "remediation" : {
      "recommendation" : "MyXXX",
      "url" : "MyXXX"
    },
    "verification_state" : "Unknown,True_Positive,False_Positive The default value is Unknown.",
    "handle_status" : "Open – enabled.Block – blocked.Closed – closed.The default value is Open.",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm, Eradication& Recovery| Post-Incident-
Activity",
    "simulation" : "false",
    "actor" : "Tom",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "False positive; Resolved; Duplicate; Others",
    "close_comment" : "False positive; Resolved; Duplicate; Others",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "Malicious memory occupation."
    },
    "system_info" : { },
    "process" : [ {
      "process_name" : "MyXXX",
      "process_path" : "MyXXX",
      "process_pid" : 123,
      "process_uid" : 123,
      "process_cmdline" : "MyXXX"
    } ],
    "user_info" : [ {
      "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "user_name" : "MyXXX"
    } ],
    "file_info" : [ {
      "file_path" : "MyXXX",
      "file_content" : "MyXXX",
      "file_new_path" : "MyXXX",
      "file_hash" : "MyXXX",
      "file_md5" : "MyXXX",
      "file_sha256" : "MyXXX",
      "file_attr" : "MyXXX"
    } ],
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
  },
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800",
```

```
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowIncidentSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowIncidentRequest request = new ShowIncidentRequest();
        try {
            ShowIncidentResponse response = client.showIncident(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
```

```
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowIncidentRequest()
        response = client.show_incident(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowIncidentRequest{}
    response, err := client.ShowIncident(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

### More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

### Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response body for requests for obtaining incident details. |
| 400 | Response body for failed requests for obtaining incident details. |

### Error Codes

See **Error Codes**.

## 4.2.5 Updating an Incident

### Function

This API is used to modify an incident and update its attributes according to the changes made. The columns that are not changed remain unchanged.

### Calling Method

For details, see **Calling APIs**.

### URI

PUT /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/{incident_id}

**Table 4-217** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| incident_id | Yes | String | Incident ID.<br>Minimum: **32**<br>Maximum: **36** |

## Request Parameters

**Table 4-218** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **0**<br>Maximum: **2097152** |
| content-type | Yes | String | Content type.<br>Default: **application/json;charset=UTF-8**<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-219** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| batch_ids | No | Array of strings | IDs of updated alerts.<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 999** |
| data_object | No | **Incident** object | Incident entity information. |

**Table 4-220** Incident

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| version | No | String | Version of the data source of an incident. The version must be one officially released by the Huawei Cloud SSA service.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| id | No | String | Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | No | String | ID of the account (domain_id) to whom the data is delivered and hosted.<br>Minimum: **0**<br>Maximum: **36** |
| region_id | No | String | ID of the region where the account to whom the data is delivered and hosted belongs to.<br>Minimum: **0**<br>Maximum: **36** |
| workspace_id | No | String | ID of the current workspace.<br>Minimum: **0**<br>Maximum: **36** |
| labels | No | String | Tag (display only)<br>Minimum: **0**<br>Maximum: **1024** |
| environment | No | **environment** object | Coordinates of the environment where the incident was generated. |
| data_source | No | **data_source** object | Source the data is first reported. |
| first_observed_time | No | String | First discovery time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| last_observed_time | No | String | First discovery time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| create_time | No | String | Recording time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| arrive_time | No | String | Data receiving time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| title | No | String | Incident title.<br>Minimum: **0**<br>Maximum: **255** |
| description | No | String | Event Description<br>Minimum: **0**<br>Maximum: **1024** |
| source_url | No | String | Incident URL, which points to the page of the current incident description in the data source product.<br>Minimum: **0**<br>Maximum: **1024** |
| count | No | Integer | Incident occurrences<br>Minimum: **0**<br>Maximum: **999** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| confidence | No | Integer | Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or incident. Value range -- 0-100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.<br>Minimum: **0**<br>Maximum: **100** |
| severity | No | String | Severity level. Value range: Tips \| Low \| Medium \| High \| Fatal Description:<br>• **0**: TIPS: No threats are found.<br>• **1**: LOW: No actions are required for the threat.<br>• **2**: MEDIUM: The threat needs to be handled but is not urgent.<br>• **3**: HIGH: The threat must be handled preferentially.<br>• **4**: FATAL: The threat must be handled immediately to prevent further damage.<br>Minimum: **3**<br>Maximum: **6**<br>Enumeration values:<br>• **Tips**<br>• **Low**<br>• **Medium**<br>• **High**<br>• **Fatal** |
| criticality | No | Integer | Criticality, which specifies the importance level of the resources involved in an incident. Value range -- 0 to 100. The value 0 indicates that the resource is not critical, and 100 indicates that the resource is critical.<br>Minimum: **0**<br>Maximum: **100** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| incident_type | No | **incident_type** object | Incident categories. For details, see the Alert Incident Type Definition. |
| network_list | No | Array of **network_list** objects | Network Information<br>Array Length: **0 - 999** |
| resource_list | No | Array of **resource_list** objects | Affected resources.<br>Array Length: **0 - 999** |
| remediation | No | **remediation** object | Remedy measure. |
| verification_state | No | String | Verification status, which identifies the accuracy of an incident. The options are as follows: – Unknown – True_Positive – False_Positive Enter Unknown by default.<br>Minimum: **32**<br>Maximum: **64**<br>Enumeration values:<br>• **Unknown**<br>• **True_Positive**<br>• **False_Positive** |
| handle_status | No | String | Incident handling status. The options are as follows:<br>• Open: enabled.<br>• Block: blocked.<br>• Closed: closed. The default value is Open.<br>Minimum: **4**<br>Maximum: **5**<br>Enumeration values:<br>• **Open**<br>• **Block**<br>• **Closed** |
| sla | No | Integer | Risk close time -- Set the acceptable risk duration. Unit -- Hour<br>Minimum: **0**<br>Maximum: **999** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| update_time | No | String | Update time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the alert occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| close_time | No | String | Closing time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| ipdrr_phase | No | String | Period/Handling phase No. Prepartion\|Detection and Analysis\|Containm, Eradication& Recovery\|Post-Incident-Activity<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **Prepartion**<br>• **Detection and Analysis**<br>• **Containm, Eradication& Recovery**<br>• **Post-Incident-Activity** |
| simulation | No | String | Debugging field.<br>Minimum: **0**<br>Maximum: **64** |
| actor | No | String | Incident investigator.<br>Minimum: **0**<br>Maximum: **64** |
| owner | No | String | Owner and service owner.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| creator | No | String | Creator<br>Minimum: **0**<br>Maximum: **64** |
| close_reason | No | String | Close reason.<br>• False positive.<br>• Resolved<br>• Repeated<br>• Other<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **False detection**<br>• **Resolved**<br>• **Repeated**<br>• **Other** |
| close_comment | No | String | Whether to close comment.<br>Minimum: **0**<br>Maximum: **1024** |
| malware | No | **malware** object | Malware |
| system_info | No | Object | System information. |
| process | No | Array of **process** objects | Process information.<br>Array Length: **0 - 999** |
| user_info | No | Array of **user_info** objects | User Details<br>Array Length: **0 - 999** |
| file_info | No | Array of **file_info** objects | Document Information<br>Array Length: **0 - 999** |
| system_alert_table | No | Object | Layout fields in the incident list. |

**Table 4-221** environment

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| vendor_type | No | String | Environment provider. The value can be **HWCP**, **HWC**, **AWS**, **Azure**, or **GCP**.<br>Minimum: **0**<br>Maximum: **64** |
| domain_id | No | String | Tenant ID.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | No | String | Region ID. **global** is returned for global services.<br>Minimum: **0**<br>Maximum: **64** |
| cross_workspace_id | No | String | ID of the source workspace for the data delivery. If the source workspace ID is null, then the destination workspace account ID is used.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | No | String | Project ID. The default value is null for global services.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-222** data_source

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| source_type | No | Integer | Data source type. The options are as follows-- 1- Huawei product 2- Third-party product 3- Tenant product<br>Minimum: **1**<br>Maximum: **3**<br>Enumeration values:<br>• **1**<br>• **2**<br>• **3** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| domain_id | No | String | Account ID to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | No | String | ID of the project to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | No | String | Region where the data source is located, for example, cn-north1. For details about the value range, see *Regions and Endpoints*.<br>Minimum: **0**<br>Maximum: **64** |
| company_name | No | String | Name of the company to which a data source belongs.<br>Minimum: **0**<br>Maximum: **16** |
| product_name | No | String | Name of the data source.<br>Minimum: **0**<br>Maximum: **24** |
| product_feature | No | String | Name of the feature of the product that detects the incident.<br>Minimum: **0**<br>Maximum: **24** |
| product_module | No | String | Threat detection module list.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-223** incident_type

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| category | No | String | Type<br>Minimum: **0**<br>Maximum: **1024** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| incident_type | No | String | Incident type.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-224** network_list

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| direction | No | String | Direction. The value can be IN or OUT.<br>Minimum: **0**<br>Maximum: **3**<br>Enumeration values:<br>• **IN**<br>• **OUT** |
| protocol | No | String | Protocol, including Layer 7 and Layer 4 protocols. For details, see IANA registered name. https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.<br>Minimum: **0**<br>Maximum: **64** |
| src_ip | No | String | Source IP address<br>Minimum: **0**<br>Maximum: **64** |
| src_port | No | Integer | Source port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| src_domain | No | String | Source domain name.<br>Minimum: **0**<br>Maximum: **128** |
| src_geo | No | **src_geo** object | Geographical location of the source IP address. |
| dest_ip | No | String | Destination IP address<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| dest_port | No | String | Destination port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| dest_domain | No | String | Destination domain name<br>Minimum: **0**<br>Maximum: **128** |
| dest_geo | No | **dest_geo** object | Geographical location of the destination IP address. |

**Table 4-225** src_geo

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| latitude | No | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | No | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | No | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | No | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-226** dest_geo

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| latitude | No | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| longitude | No | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | No | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | No | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-227** resource_list

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| id | No | String | Cloud service resource ID.<br>Minimum: **0**<br>Maximum: **36** |
| name | No | String | Resource name.<br>Minimum: **0**<br>Maximum: **255** |
| type | No | String | Resource type. This parameter references the value of RMS type on Huawei Cloud.<br>Minimum: **0**<br>Maximum: **64** |
| provider | No | String | Cloud service name, which is the same as the provider field in the RMS service.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | No | String | Region ID in Huawei Cloud, for example, cn-north-1.<br>Minimum: **0**<br>Maximum: **36** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| domain_id | No | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | No | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| ep_id | No | String | Specifies the enterprise project ID.<br>Minimum: **0**<br>Maximum: **128** |
| ep_name | No | String | Enterprise Project Name<br>Minimum: **0**<br>Maximum: **128** |
| tags | No | String | Resource tag.<br>1. A maximum of 50 key/value pairs are supported.<br>2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _, :, /,@<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-228** remediation

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| recommendation | No | String | Recommended solution.<br>Minimum: **0**<br>Maximum: **128** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| url | No | String | Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-229** malware

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| malware_family | No | String | Malicious family.<br>Minimum: **0**<br>Maximum: **64** |
| malware_class | No | String | Malware category.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-230** process

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| process_name | No | String | Process name.<br>Minimum: **0**<br>Maximum: **64** |
| process_path | No | String | Process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_pid | No | Integer | Process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_uid | No | Integer | Process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_cmdline | No | String | Process command line.<br>Minimum: **0**<br>Maximum: **128** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| process_parent_name | No | String | Parent process name.<br>Minimum: **0**<br>Maximum: **64** |
| process_parent_path | No | String | Parent process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_parent_pid | No | Integer | Parent process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_parent_uid | No | Integer | Parent process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_parent_cmdline | No | String | Parent process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_child_name | No | String | Subprocess name.<br>Minimum: **0**<br>Maximum: **64** |
| process_child_path | No | String | Subprocess execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_child_pid | No | Integer | Subprocess ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_child_uid | No | Integer | Subprocess user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_child_cmdline | No | String | Subprocess command line<br>Minimum: **0**<br>Maximum: **128** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| process_launche_time | No | String | Incident start time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| process_terminate_time | No | String | Process end time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

**Table 4-231** user_info

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| user_id | No | String | User UID<br>Minimum: **0**<br>Maximum: **36** |
| user_name | No | String | Username<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-232** file_info

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| file_path | No | String | File path/name.<br>Minimum: **0**<br>Maximum: **128** |
| file_content | No | String | File path/name.<br>Minimum: **0**<br>Maximum: **1024** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| file_new_path | No | String | New file path/name.<br>Minimum: **32**<br>Maximum: **64** |
| file_hash | No | String | File Hash<br>Minimum: **0**<br>Maximum: **128** |
| file_md5 | No | String | File MD5<br>Minimum: **0**<br>Maximum: **128** |
| file_sha256 | No | String | File SHA256<br>Minimum: **0**<br>Maximum: **128** |
| file_attr | No | String | File attribute.<br>Minimum: **0**<br>Maximum: **1024** |

## Response Parameters

**Status code: 200**

**Table 4-233** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-234** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Message<br>Minimum: **0**<br>Maximum: **1024** |

| Parameter | Type | Description |
| --- | --- | --- |
| data | IncidentDetail object | |

**Table 4-235** IncidentDetail

| Parameter | Type | Description |
| --- | --- | --- |
| create_time | String | Recording time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| data_object | Incident object | Incident entity information. |
| dataclass_ref | dataclass_ref object | Data class object. |
| format_version | Integer | Format version.<br>Minimum: **0**<br>Maximum: **999** |
| id | String | Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | String | ID of the current project.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Update time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the alert occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| version | Integer | Version.<br>Minimum: **0**<br>Maximum: **999** |

| Parameter | Type | Description |
| --- | --- | --- |
| workspace_id | String | ID of the current workspace.<br>Minimum: **0**<br>Maximum: **36** |

**Table 4-236** Incident

| Parameter | Type | Description |
| --- | --- | --- |
| version | String | Version of the data source of an incident. The version must be one officially released by the Huawei Cloud SSA service.<br>Minimum: **0**<br>Maximum: **64** |
| id | String | Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | String | ID of the account (domain_id) to whom the data is delivered and hosted.<br>Minimum: **0**<br>Maximum: **36** |
| region_id | String | ID of the region where the account to whom the data is delivered and hosted belongs to.<br>Minimum: **0**<br>Maximum: **36** |
| workspace_id | String | ID of the current workspace.<br>Minimum: **0**<br>Maximum: **36** |
| labels | String | Tag (display only)<br>Minimum: **0**<br>Maximum: **1024** |
| environment | **environment** object | Coordinates of the environment where the incident was generated. |
| data_source | **data_source** object | Source the data is first reported. |

| Parameter | Type | Description |
| --- | --- | --- |
| first_observed_time | String | First discovery time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| last_observed_time | String | First discovery time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| create_time | String | Recording time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| arrive_time | String | Data receiving time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| title | String | Incident title.<br>Minimum: **0**<br>Maximum: **255** |
| description | String | Event Description<br>Minimum: **0**<br>Maximum: **1024** |
| source_url | String | Incident URL, which points to the page of the current incident description in the data source product.<br>Minimum: **0**<br>Maximum: **1024** |

| Parameter | Type | Description |
| --- | --- | --- |
| count | Integer | Incident occurrences<br>Minimum: **0**<br>Maximum: **999** |
| confidence | Integer | Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or incident. Value range -- 0-100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.<br>Minimum: **0**<br>Maximum: **100** |
| severity | String | Severity level. Value range: Tips \| Low \| Medium \| High \| Fatal Description:<br>• **0**: TIPS: No threats are found.<br>• **1**: LOW: No actions are required for the threat.<br>• **2**: MEDIUM: The threat needs to be handled but is not urgent.<br>• **3**: HIGH: The threat must be handled preferentially.<br>• **4**: FATAL: The threat must be handled immediately to prevent further damage.<br>Minimum: **3**<br>Maximum: **6**<br>Enumeration values:<br>• **Tips**<br>• **Low**<br>• **Medium**<br>• **High**<br>• **Fatal** |
| criticality | Integer | Criticality, which specifies the importance level of the resources involved in an incident. Value range -- 0 to 100. The value 0 indicates that the resource is not critical, and 100 indicates that the resource is critical.<br>Minimum: **0**<br>Maximum: **100** |
| incident_type | **incident_type** object | Incident categories. For details, see the Alert Incident Type Definition. |
| network_list | Array of **network_list** objects | Network Information<br>Array Length: **0 - 999** |

| Parameter | Type | Description |
| --- | --- | --- |
| resource_list | Array of **resource_list** objects | Affected resources.<br>Array Length: **0 - 999** |
| remediation | **remediation** object | Remedy measure. |
| verification_state | String | Verification status, which identifies the accuracy of an incident. The options are as follows: – Unknown – True_Positive – False_Positive Enter Unknown by default.<br>Minimum: **32**<br>Maximum: **64**<br>Enumeration values:<br>• **Unknown**<br>• **True_Positive**<br>• **False_Positive** |
| handle_status | String | Incident handling status. The options are as follows:<br>• Open: enabled.<br>• Block: blocked.<br>• Closed: closed. The default value is Open.<br>Minimum: **4**<br>Maximum: **5**<br>Enumeration values:<br>• **Open**<br>• **Block**<br>• **Closed** |
| sla | Integer | Risk close time -- Set the acceptable risk duration. Unit -- Hour<br>Minimum: **0**<br>Maximum: **999** |
| update_time | String | Update time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the alert occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |

| Parameter | Type | Description |
| --- | --- | --- |
| close_time | String | Closing time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| ipdrr_phase | String | Period/Handling phase No. Prepartion\| Detection and Analysis\|Containm, Eradication& Recovery\|Post-Incident-Activity<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **Prepartion**<br>• **Detection and Analysis**<br>• **Containm, Eradication& Recovery**<br>• **Post-Incident-Activity** |
| simulation | String | Debugging field.<br>Minimum: **0**<br>Maximum: **64** |
| actor | String | Incident investigator.<br>Minimum: **0**<br>Maximum: **64** |
| owner | String | Owner and service owner.<br>Minimum: **0**<br>Maximum: **64** |
| creator | String | Creator<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| close_reason | String | Close reason.<br>• False positive.<br>• Resolved<br>• Repeated<br>• Other<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **False detection**<br>• **Resolved**<br>• **Repeated**<br>• **Other** |
| close_comment | String | Whether to close comment.<br>Minimum: **0**<br>Maximum: **1024** |
| malware | **malware** object | Malware |
| system_info | Object | System information. |
| process | Array of **process** objects | Process information.<br>Array Length: **0 - 999** |
| user_info | Array of **user_info** objects | User Details<br>Array Length: **0 - 999** |
| file_info | Array of **file_info** objects | Document Information<br>Array Length: **0 - 999** |
| system_alert_table | Object | Layout fields in the incident list. |

**Table 4-237** environment

| Parameter | Type | Description |
| --- | --- | --- |
| vendor_type | String | Environment provider. The value can be **HWCP**, **HWC**, **AWS**, **Azure**, or **GCP**.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| domain_id | String | Tenant ID.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region ID. **global** is returned for global services.<br>Minimum: **0**<br>Maximum: **64** |
| cross_workspace_id | String | ID of the source workspace for the data delivery. If the source workspace ID is null, then the destination workspace account ID is used.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID. The default value is null for global services.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-238** data_source

| Parameter | Type | Description |
| --- | --- | --- |
| source_type | Integer | Data source type. The options are as follows--1- Huawei product 2- Third-party product 3- Tenant product<br>Minimum: **1**<br>Maximum: **3**<br>Enumeration values:<br>• **1**<br>• **2**<br>• **3** |
| domain_id | String | Account ID to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | String | ID of the project to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| region_id | String | Region where the data source is located, for example, cn-north1. For details about the value range, see *Regions and Endpoints*.<br>Minimum: **0**<br>Maximum: **64** |
| company_name | String | Name of the company to which a data source belongs.<br>Minimum: **0**<br>Maximum: **16** |
| product_name | String | Name of the data source.<br>Minimum: **0**<br>Maximum: **24** |
| product_feature | String | Name of the feature of the product that detects the incident.<br>Minimum: **0**<br>Maximum: **24** |
| product_module | String | Threat detection module list.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-239** incident_type

| Parameter | Type | Description |
| --- | --- | --- |
| category | String | Type<br>Minimum: **0**<br>Maximum: **1024** |
| incident_type | String | Incident type.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-240** network_list

| Parameter | Type | Description |
| --- | --- | --- |
| direction | String | Direction. The value can be IN or OUT.<br>Minimum: **0**<br>Maximum: **3**<br>Enumeration values:<br>• **IN**<br>• **OUT** |
| protocol | String | Protocol, including Layer 7 and Layer 4 protocols. For details, see IANA registered name. https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.<br>Minimum: **0**<br>Maximum: **64** |
| src_ip | String | Source IP address<br>Minimum: **0**<br>Maximum: **64** |
| src_port | Integer | Source port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| src_domain | String | Source domain name.<br>Minimum: **0**<br>Maximum: **128** |
| src_geo | **src_geo** object | Geographical location of the source IP address. |
| dest_ip | String | Destination IP address<br>Minimum: **32**<br>Maximum: **64** |
| dest_port | String | Destination port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| dest_domain | String | Destination domain name<br>Minimum: **0**<br>Maximum: **128** |
| dest_geo | **dest_geo** object | Geographical location of the destination IP address. |

**Table 4-241** src_geo

| Parameter | Type | Description |
| --- | --- | --- |
| latitude | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-242** dest_geo

| Parameter | Type | Description |
| --- | --- | --- |
| latitude | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-243** resource_list

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Cloud service resource ID.<br>Minimum: **0**<br>Maximum: **36** |
| name | String | Resource name.<br>Minimum: **0**<br>Maximum: **255** |
| type | String | Resource type. This parameter references the value of RMS type on Huawei Cloud.<br>Minimum: **0**<br>Maximum: **64** |
| provider | String | Cloud service name, which is the same as the provider field in the RMS service.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region ID in Huawei Cloud, for example, cn-north-1.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| ep_id | String | Specifies the enterprise project ID.<br>Minimum: **0**<br>Maximum: **128** |
| ep_name | String | Enterprise Project Name<br>Minimum: **0**<br>Maximum: **128** |

| Parameter | Type | Description |
| --- | --- | --- |
| tags | String | Resource tag.<br>1. A maximum of 50 key/value pairs are supported.<br>2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _, :, /,@<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-244** remediation

| Parameter | Type | Description |
| --- | --- | --- |
| recommendation | String | Recommended solution.<br>Minimum: **0**<br>Maximum: **128** |
| url | String | Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-245** malware

| Parameter | Type | Description |
| --- | --- | --- |
| malware_family | String | Malicious family.<br>Minimum: **0**<br>Maximum: **64** |
| malware_class | String | Malware category.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-246** process

| Parameter | Type | Description |
| --- | --- | --- |
| process_name | String | Process name.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| process_path | String | Process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_pid | Integer | Process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_uid | Integer | Process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_cmdline | String | Process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_parent_name | String | Parent process name.<br>Minimum: **0**<br>Maximum: **64** |
| process_parent_path | String | Parent process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_parent_pid | Integer | Parent process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_parent_uid | Integer | Parent process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_parent_cmdline | String | Parent process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_child_name | String | Subprocess name.<br>Minimum: **0**<br>Maximum: **64** |
| process_child_path | String | Subprocess execution file path.<br>Minimum: **0**<br>Maximum: **512** |

| Parameter | Type | Description |
| --- | --- | --- |
| process_child_pid | Integer | Subprocess ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_child_uid | Integer | Subprocess user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_child_cmdline | String | Subprocess command line<br>Minimum: **0**<br>Maximum: **128** |
| process_launche_time | String | Incident start time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| process_terminate_time | String | Process end time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

**Table 4-247** user_info

| Parameter | Type | Description |
| --- | --- | --- |
| user_id | String | User UID<br>Minimum: **0**<br>Maximum: **36** |
| user_name | String | Username<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-248** file_info

| Parameter | Type | Description |
| --- | --- | --- |
| file_path | String | File path/name.<br>Minimum: **0**<br>Maximum: **128** |
| file_content | String | File path/name.<br>Minimum: **0**<br>Maximum: **1024** |
| file_new_path | String | New file path/name.<br>Minimum: **32**<br>Maximum: **64** |
| file_hash | String | File Hash<br>Minimum: **0**<br>Maximum: **128** |
| file_md5 | String | File MD5<br>Minimum: **0**<br>Maximum: **128** |
| file_sha256 | String | File SHA256<br>Minimum: **0**<br>Maximum: **128** |
| file_attr | String | File attribute.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-249** dataclass_ref

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Unique identifier of a data class. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| name | String | Data class name.<br>Minimum: **0**<br>Maximum: **36** |

**Status code: 400**

**Table 4-250** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-251** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Update an incident. Set the incident title to MyXXX, URL to http://xxx, occurrence times to 4, and confidence to 4.

```
{
  "data_object" : {
    "version" : "1.0",
    "environment" : {
      "vendor_type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "data_source" : {
      "source_type" : 3,
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "first_observed_time" : "2021-01-30T23:00:00Z+0800",
    "last_observed_time" : "2021-01-30T23:00:00Z+0800",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "arrive_time" : "2021-01-30T23:00:00Z+0800",
    "title" : "MyXXX",
    "description" : "This my XXXX",
    "source_url" : "http://xxx",
    "count" : 4,
    "confidence" : 4,
    "severity" : "TIPS",
    "criticality" : 4,
    "incident_type" : { },
    "network_list" : [ {
      "direction" : {
        "IN" : null
      },
      "protocol" : "TCP",
      "src_ip" : "192.168.0.1",
      "src_port" : "1",
```

```
    "src_domain" : "xxx",
    "dest_ip" : "192.168.0.1",
    "dest_port" : "1",
    "dest_domain" : "xxx",
    "src_geo" : {
      "latitude" : 90,
      "longitude" : 180
    },
    "dest_geo" : {
      "latitude" : 90,
      "longitude" : 180
    }
  } ],
  "resource_list" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "type" : "MyXXX",
    "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "ep_name" : "MyXXX",
    "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  } ],
  "remediation" : {
    "recommendation" : "MyXXX",
    "url" : "MyXXX"
  },
  "verification_state" : "Unknown,True_Positive,False_Positive The default value is Unknown.",
  "handle_status" : "Open – enabled.Block – blocked.Closed – closed.The default value is Open.",
  "sla" : 60000,
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "close_time" : "2021-01-30T23:00:00Z+0800",
  "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm, Eradication& Recovery| Post-Incident-
Activity",
  "simulation" : "false",
  "actor" : "Tom",
  "owner" : "MyXXX",
  "creator" : "MyXXX",
  "close_reason" : "False positive; Resolved; Duplicate; Others",
  "close_comment" : "False positive; Resolved; Duplicate; Others",
  "malware" : {
    "malware_family" : "family",
    "malware_class" : "Malicious memory occupation."
  },
  "system_info" : { },
  "process" : [ {
    "process_name" : "MyXXX",
    "process_path" : "MyXXX",
    "process_pid" : 123,
    "process_uid" : 123,
    "process_cmdline" : "MyXXX"
  } ],
  "user_info" : [ {
    "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "user_name" : "MyXXX"
  } ],
  "file_info" : [ {
    "file_path" : "MyXXX",
    "file_content" : "MyXXX",
    "file_new_path" : "MyXXX",
    "file_hash" : "MyXXX",
    "file_md5" : "MyXXX",
    "file_sha256" : "MyXXX",
    "file_attr" : "MyXXX"
  } ],
  "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
```

```
 }
}
```

## Example Responses

**Status code: 200**

Response body of the request for updating incidents.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "data_object" : {
      "version" : "1.0",
      "environment" : {
        "vendor_type" : "MyXXX",
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "data_source" : {
        "source_type" : 3,
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "first_observed_time" : "2021-01-30T23:00:00Z+0800",
      "last_observed_time" : "2021-01-30T23:00:00Z+0800",
      "create_time" : "2021-01-30T23:00:00Z+0800",
      "arrive_time" : "2021-01-30T23:00:00Z+0800",
      "title" : "MyXXX",
      "description" : "This my XXXX",
      "source_url" : "http://xxx",
      "count" : 4,
      "confidence" : 4,
      "severity" : "TIPS",
      "criticality" : 4,
      "incident_type" : { },
      "network_list" : [ {
        "direction" : {
          "IN" : null
        },
        "protocol" : "TCP",
        "src_ip" : "192.168.0.1",
        "src_port" : "1",
        "src_domain" : "xxx",
        "dest_ip" : "192.168.0.1",
        "dest_port" : "1",
        "dest_domain" : "xxx",
        "src_geo" : {
          "latitude" : 90,
          "longitude" : 180
        },
        "dest_geo" : {
          "latitude" : 90,
          "longitude" : 180
        }
      } ],
      "resource_list" : [ {
        "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "name" : "MyXXX",
        "type" : "MyXXX",
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "ep_name" : "MyXXX",
        "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
```

```
    } ],
    "remediation" : {
      "recommendation" : "MyXXX",
      "url" : "MyXXX"
    },
    "verification_state" : "Unknown,True_Positive,False_Positive The default value is Unknown.",
    "handle_status" : "Open – enabled.Block – blocked.Closed – closed.The default value is Open.",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm, Eradication& Recovery| Post-Incident-
Activity",
    "simulation" : "false",
    "actor" : "Tom",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "False positive; Resolved; Duplicate; Others",
    "close_comment" : "False positive; Resolved; Duplicate; Others",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "Malicious memory occupation."
    },
    "system_info" : { },
    "process" : [ {
      "process_name" : "MyXXX",
      "process_path" : "MyXXX",
      "process_pid" : 123,
      "process_uid" : 123,
      "process_cmdline" : "MyXXX"
    } ],
    "user_info" : [ {
      "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "user_name" : "MyXXX"
    } ],
    "file_info" : [ {
      "file_path" : "MyXXX",
      "file_content" : "MyXXX",
      "file_new_path" : "MyXXX",
      "file_hash" : "MyXXX",
      "file_md5" : "MyXXX",
      "file_sha256" : "MyXXX",
      "file_attr" : "MyXXX"
    } ],
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
  },
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
 }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Update an incident. Set the incident title to MyXXX, URL to http://xxx, occurrence times to 4, and confidence to 4.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
```

```
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class ChangeIncidentSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ChangeIncidentRequest request = new ChangeIncidentRequest();
        ChangeIncidentRequestBody body = new ChangeIncidentRequestBody();
        List<IncidentFileInfo> listDataObjectFileInfo = new ArrayList<>();
        listDataObjectFileInfo.add(
            new IncidentFileInfo()
                .withFilePath("MyXXX")
                .withFileContent("MyXXX")
                .withFileNewPath("MyXXX")
                .withFileHash("MyXXX")
                .withFileMd5("MyXXX")
                .withFileSha256("MyXXX")
                .withFileAttr("MyXXX")
        );
        List<IncidentUserInfo> listDataObjectUserInfo = new ArrayList<>();
        listDataObjectUserInfo.add(
            new IncidentUserInfo()
                .withUserId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withUserName("MyXXX")
        );
        List<IncidentProcess> listDataObjectProcess = new ArrayList<>();
        listDataObjectProcess.add(
            new IncidentProcess()
                .withProcessName("MyXXX")
                .withProcessPath("MyXXX")
                .withProcessPid(123)
                .withProcessUid(123)
                .withProcessCmdline("MyXXX")
        );
        IncidentMalware malwareDataObject = new IncidentMalware();
        malwareDataObject.withMalwareFamily("family")
            .withMalwareClass("Malicious memory occupation.");
        IncidentRemediation remediationDataObject = new IncidentRemediation();
        remediationDataObject.withRecommendation("MyXXX")
            .withUrl("MyXXX");
        List<IncidentResourceList> listDataObjectResourceList = new ArrayList<>();
        listDataObjectResourceList.add(
            new IncidentResourceList()
                .withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withName("MyXXX")
                .withType("MyXXX")
                .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
```

```
            .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withEpId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withEpName("MyXXX")
            .withTags("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        );
        IncidentDestGeo destGeoNetworkList = new IncidentDestGeo();
        destGeoNetworkList.withLatitude(java.math.BigDecimal.valueOf(90))
            .withLongitude(java.math.BigDecimal.valueOf(180));
        IncidentSrcGeo srcGeoNetworkList = new IncidentSrcGeo();
        srcGeoNetworkList.withLatitude(java.math.BigDecimal.valueOf(90))
            .withLongitude(java.math.BigDecimal.valueOf(180));
        List<IncidentNetworkList> listDataObjectNetworkList = new ArrayList<>();
        listDataObjectNetworkList.add(
            new IncidentNetworkList()
                .withDirection(IncidentNetworkList.DirectionEnum.fromValue("{}"))
                .withProtocol("TCP")
                .withSrcIp("192.168.0.1")
                .withSrcPort(1)
                .withSrcDomain("xxx")
                .withSrcGeo(srcGeoNetworkList)
                .withDestIp("192.168.0.1")
                .withDestPort("1")
                .withDestDomain("xxx")
                .withDestGeo(destGeoNetworkList)
        );
        IncidentDataSource dataSourceDataObject = new IncidentDataSource();
        dataSourceDataObject.withSourceType(3)
            .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        IncidentEnvironment environmentDataObject = new IncidentEnvironment();
        environmentDataObject.withVendorType("MyXXX")
            .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        Incident dataObjectbody = new Incident();
        dataObjectbody.withVersion("1.0")
            .withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withWorkspaceId("909494e3-558e-46b6-a9eb-07a8e18ca620")
            .withEnvironment(environmentDataObject)
            .withDataSource(dataSourceDataObject)
            .withFirstObservedTime("2021-01-30T23:00:00Z+0800")
            .withLastObservedTime("2021-01-30T23:00:00Z+0800")
            .withCreateTime("2021-01-30T23:00:00Z+0800")
            .withArriveTime("2021-01-30T23:00:00Z+0800")
            .withTitle("MyXXX")
            .withDescription("This my XXXX")
            .withSourceUrl("http://xxx")
            .withCount(4)
            .withConfidence(4)
            .withSeverity(Incident.SeverityEnum.fromValue("TIPS"))
            .withCriticality(4)
            .withNetworkList(listDataObjectNetworkList)
            .withResourceList(listDataObjectResourceList)
            .withRemediation(remediationDataObject)
            .withVerificationState(Incident.VerificationStateEnum.fromValue("Unknown,True_Positive,False_Posit
ive The default value is Unknown."))
            .withHandleStatus(Incident.HandleStatusEnum.fromValue("Open – enabled.Block – blocked.Closed
– closed.The default value is Open."))
            .withSla(60000)
            .withUpdateTime("2021-01-30T23:00:00Z+0800")
            .withCloseTime("2021-01-30T23:00:00Z+0800")
            .withIpdrrPhase(Incident.IpdrrPhaseEnum.fromValue("Prepartion|Detection and Analysis|
Containm,Eradication& Recovery| Post-Incident-Activity"))
            .withSimulation("false")
            .withActor("Tom")
            .withOwner("MyXXX")
            .withCreator("MyXXX")
```

```
            .withCloseReason(Incident.CloseReasonEnum.fromValue("False positive; Resolved; Duplicate;
Others"))
            .withCloseComment("False positive; Resolved; Duplicate; Others")
            .withMalware(malwareDataObject)
            .withSystemInfo(new Object())
            .withProcess(listDataObjectProcess)
            .withUserInfo(listDataObjectUserInfo)
            .withFileInfo(listDataObjectFileInfo);
        body.withDataObject(dataObjectbody);
        request.withBody(body);
        try {
            ChangeIncidentResponse response = client.changeIncident(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Update an incident. Set the incident title to MyXXX, URL to http://xxx, occurrence times to 4, and confidence to 4.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ChangeIncidentRequest()
        listFileInfoDataObject = [
            IncidentFileInfo(
                file_path="MyXXX",
                file_content="MyXXX",
                file_new_path="MyXXX",
                file_hash="MyXXX",
                file_md5="MyXXX",
                file_sha256="MyXXX",
                file_attr="MyXXX"
            )
        ]
        listUserInfoDataObject = [
```

```
    IncidentUserInfo(
        user_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        user_name="MyXXX"
    )
]
listProcessDataObject = [
    IncidentProcess(
        process_name="MyXXX",
        process_path="MyXXX",
        process_pid=123,
        process_uid=123,
        process_cmdline="MyXXX"
    )
]
malwareDataObject = IncidentMalware(
    malware_family="family",
    malware_class="Malicious memory occupation."
)
remediationDataObject = IncidentRemediation(
    recommendation="MyXXX",
    url="MyXXX"
)
listResourceListDataObject = [
    IncidentResourceList(
        id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        name="MyXXX",
        type="MyXXX",
        region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        ep_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        ep_name="MyXXX",
        tags="909494e3-558e-46b6-a9eb-07a8e18ca62f"
    )
]
destGeoNetworkList = IncidentDestGeo(
    latitude=90,
    longitude=180
)
srcGeoNetworkList = IncidentSrcGeo(
    latitude=90,
    longitude=180
)
listNetworkListDataObject = [
    IncidentNetworkList(
        direction="{}",
        protocol="TCP",
        src_ip="192.168.0.1",
        src_port=1,
        src_domain="xxx",
        src_geo=srcGeoNetworkList,
        dest_ip="192.168.0.1",
        dest_port="1",
        dest_domain="xxx",
        dest_geo=destGeoNetworkList
    )
]
dataSourceDataObject = IncidentDataSource(
    source_type=3,
    domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
    project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
    region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f"
)
environmentDataObject = IncidentEnvironment(
    vendor_type="MyXXX",
    domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
    region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
    project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f"
)
```

```
        dataObjectbody = Incident(
            version="1.0",
            id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            workspace_id="909494e3-558e-46b6-a9eb-07a8e18ca620",
            environment=environmentDataObject,
            data_source=dataSourceDataObject,
            first_observed_time="2021-01-30T23:00:00Z+0800",
            last_observed_time="2021-01-30T23:00:00Z+0800",
            create_time="2021-01-30T23:00:00Z+0800",
            arrive_time="2021-01-30T23:00:00Z+0800",
            title="MyXXX",
            description="This my XXXX",
            source_url="http://xxx",
            count=4,
            confidence=4,
            severity="TIPS",
            criticality=4,
            network_list=listNetworkListDataObject,
            resource_list=listResourceListDataObject,
            remediation=remediationDataObject,
            verification_state="Unknown,True_Positive,False_Positive The default value is Unknown.",
            handle_status="Open – enabled.Block – blocked.Closed – closed.The default value is Open.",
            sla=60000,
            update_time="2021-01-30T23:00:00Z+0800",
            close_time="2021-01-30T23:00:00Z+0800",
            ipdrr_phase="Prepartion|Detection and Analysis|Containm,Eradication& Recovery| Post-Incident-
Activity",
            simulation="false",
            actor="Tom",
            owner="MyXXX",
            creator="MyXXX",
            close_reason="False positive; Resolved; Duplicate; Others",
            close_comment="False positive; Resolved; Duplicate; Others",
            malware=malwareDataObject,
            system_info={},
            process=listProcessDataObject,
            user_info=listUserInfoDataObject,
            file_info=listFileInfoDataObject
        )
        request.body = ChangeIncidentRequestBody(
            data_object=dataObjectbody
        )
        response = client.change_incident(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Update an incident. Set the incident title to MyXXX, URL to http://xxx, occurrence times to 4, and confidence to 4.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
variables and decrypted during use to ensure security.
```

```
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ChangeIncidentRequest{}
    filePathFileInfo:= "MyXXX"
    fileContentFileInfo:= "MyXXX"
    fileNewPathFileInfo:= "MyXXX"
    fileHashFileInfo:= "MyXXX"
    fileMd5FileInfo:= "MyXXX"
    fileSha256FileInfo:= "MyXXX"
    fileAttrFileInfo:= "MyXXX"
    var listFileInfoDataObject = []model.IncidentFileInfo{
        {
            FilePath: &filePathFileInfo,
            FileContent: &fileContentFileInfo,
            FileNewPath: &fileNewPathFileInfo,
            FileHash: &fileHashFileInfo,
            FileMd5: &fileMd5FileInfo,
            FileSha256: &fileSha256FileInfo,
            FileAttr: &fileAttrFileInfo,
        },
    }
    userIdUserInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    userNameUserInfo:= "MyXXX"
    var listUserInfoDataObject = []model.IncidentUserInfo{
        {
            UserId: &userIdUserInfo,
            UserName: &userNameUserInfo,
        },
    }
    processNameProcess:= "MyXXX"
    processPathProcess:= "MyXXX"
    processPidProcess:= int32(123)
    processUidProcess:= int32(123)
    processCmdlineProcess:= "MyXXX"
    var listProcessDataObject = []model.IncidentProcess{
        {
            ProcessName: &processNameProcess,
            ProcessPath: &processPathProcess,
            ProcessPid: &processPidProcess,
            ProcessUid: &processUidProcess,
            ProcessCmdline: &processCmdlineProcess,
        },
    }
    malwareFamilyMalware:= "family"
    malwareClassMalware:= "Malicious memory occupation."
    malwareDataObject := &model.IncidentMalware{
        MalwareFamily: &malwareFamilyMalware,
        MalwareClass: &malwareClassMalware,
    }
    recommendationRemediation:= "MyXXX"
    urlRemediation:= "MyXXX"
    remediationDataObject := &model.IncidentRemediation{
        Recommendation: &recommendationRemediation,
        Url: &urlRemediation,
    }
```

```
idResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
nameResourceList:= "MyXXX"
typeResourceList:= "MyXXX"
regionIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
domainIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
projectIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
epIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
epNameResourceList:= "MyXXX"
tagsResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
var listResourceListDataObject = []model.IncidentResourceList{
    {
        Id: &idResourceList,
        Name: &nameResourceList,
        Type: &typeResourceList,
        RegionId: &regionIdResourceList,
        DomainId: &domainIdResourceList,
        ProjectId: &projectIdResourceList,
        EpId: &epIdResourceList,
        EpName: &epNameResourceList,
        Tags: &tagsResourceList,
    },
}
latitudeDestGeo:= float32(90)
longitudeDestGeo:= float32(180)
destGeoNetworkList := &model.IncidentDestGeo{
    Latitude: &latitudeDestGeo,
    Longitude: &longitudeDestGeo,
}
latitudeSrcGeo:= float32(90)
longitudeSrcGeo:= float32(180)
srcGeoNetworkList := &model.IncidentSrcGeo{
    Latitude: &latitudeSrcGeo,
    Longitude: &longitudeSrcGeo,
}
directionNetworkList:= model.GetIncidentNetworkListDirectionEnum().{}
protocolNetworkList:= "TCP"
srcIpNetworkList:= "192.168.0.1"
srcPortNetworkList:= int32(1)
srcDomainNetworkList:= "xxx"
destIpNetworkList:= "192.168.0.1"
destPortNetworkList:= "1"
destDomainNetworkList:= "xxx"
var listNetworkListDataObject = []model.IncidentNetworkList{
    {
        Direction: &directionNetworkList,
        Protocol: &protocolNetworkList,
        SrcIp: &srcIpNetworkList,
        SrcPort: &srcPortNetworkList,
        SrcDomain: &srcDomainNetworkList,
        SrcGeo: srcGeoNetworkList,
        DestIp: &destIpNetworkList,
        DestPort: &destPortNetworkList,
        DestDomain: &destDomainNetworkList,
        DestGeo: destGeoNetworkList,
    },
}
sourceTypeDataSource:= int32(3)
domainIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
projectIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
regionIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
dataSourceDataObject := &model.IncidentDataSource{
    SourceType: &sourceTypeDataSource,
    DomainId: &domainIdDataSource,
    ProjectId: &projectIdDataSource,
    RegionId: &regionIdDataSource,
}
vendorTypeEnvironment:= "MyXXX"
domainIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
regionIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
```

```
    projectIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    environmentDataObject := &model.IncidentEnvironment{
        VendorType: &vendorTypeEnvironment,
        DomainId: &domainIdEnvironment,
        RegionId: &regionIdEnvironment,
        ProjectId: &projectIdEnvironment,
    }
    versionDataObject:= "1.0"
    idDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    workspaceIdDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca620"
    firstObservedTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    lastObservedTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    createTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    arriveTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    titleDataObject:= "MyXXX"
    descriptionDataObject:= "This my XXXX"
    sourceUrlDataObject:= "http://xxx"
    countDataObject:= int32(4)
    confidenceDataObject:= int32(4)
    severityDataObject:= model.GetIncidentSeverityEnum().TIPS
    criticalityDataObject:= int32(4)
    verificationStateDataObject:=
model.GetIncidentVerificationStateEnum().UNKNOWN,TRUE_POSITIVE,FALSE_POSITIVE_THE_DEFAULT_VAL
UE_IS_UNKNOWN_
    handleStatusDataObject:= model.GetIncidentHandleStatusEnum().OPEN_-_ENABLED_BLOCK_-
_BLOCKED_CLOSED_-_CLOSED_THE_DEFAULT_VALUE_IS_OPEN_
    slaDataObject:= int32(60000)
    updateTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    closeTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    ipdrrPhaseDataObject:= model.GetIncidentIpdrrPhaseEnum().PREPARTION|DETECTION_AND_ANALYSIS|
CONTAINM,ERADICATION&_RECOVERY|_POST_INCIDENT_ACTIVITY
    simulationDataObject:= "false"
    actorDataObject:= "Tom"
    ownerDataObject:= "MyXXX"
    creatorDataObject:= "MyXXX"
    closeReasonDataObject:=
model.GetIncidentCloseReasonEnum().FALSE_POSITIVE;_RESOLVED;_DUPLICATE;_OTHERS
    closeCommentDataObject:= "False positive; Resolved; Duplicate; Others"
    var systemInfoDataObject interface{} = make(map[string]string)
    dataObjectbody := &model.Incident{
        Version: &versionDataObject,
        Id: &idDataObject,
        WorkspaceId: &workspaceIdDataObject,
        Environment: environmentDataObject,
        DataSource: dataSourceDataObject,
        FirstObservedTime: &firstObservedTimeDataObject,
        LastObservedTime: &lastObservedTimeDataObject,
        CreateTime: &createTimeDataObject,
        ArriveTime: &arriveTimeDataObject,
        Title: &titleDataObject,
        Description: &descriptionDataObject,
        SourceUrl: &sourceUrlDataObject,
        Count: &countDataObject,
        Confidence: &confidenceDataObject,
        Severity: &severityDataObject,
        Criticality: &criticalityDataObject,
        NetworkList: &listNetworkListDataObject,
        ResourceList: &listResourceListDataObject,
        Remediation: remediationDataObject,
        VerificationState: &verificationStateDataObject,
        HandleStatus: &handleStatusDataObject,
        Sla: &slaDataObject,
        UpdateTime: &updateTimeDataObject,
        CloseTime: &closeTimeDataObject,
        IpdrrPhase: &ipdrrPhaseDataObject,
        Simulation: &simulationDataObject,
        Actor: &actorDataObject,
        Owner: &ownerDataObject,
        Creator: &creatorDataObject,
```

```
        CloseReason: &closeReasonDataObject,
        CloseComment: &closeCommentDataObject,
        Malware: malwareDataObject,
        SystemInfo: &systemInfoDataObject,
        Process: &listProcessDataObject,
        UserInfo: &listUserInfoDataObject,
        FileInfo: &listFileInfoDataObject,
    }
    request.Body = &model.ChangeIncidentRequestBody{
        DataObject: dataObjectbody,
    }
    response, err := client.ChangeIncident(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

### More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

### Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response body of the request for updating incidents. |
| 400 | Response body of the failed request for updating incidents. |

### Error Codes

See **Error Codes**.

## 4.3 Indicator Management

### 4.3.1 This API is used to query the intelligence indicator list.

### Function

This API is used to query the intelligence indicator list.

### Calling Method

For details, see **Calling APIs**.

### URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/search

**Table 4-252** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **1**<br>Maximum: **1024** |

## Request Parameters

**Table 4-253** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | Token of the tenant.<br>Minimum: **32**<br>Maximum: **65535** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-254** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| ids | No | Array of strings | List of indicator IDs.<br>Minimum: **32**<br>Maximum: **64**<br>Array Length: **0 - 999** |
| name | No | String | Indicator name.<br>Minimum: **0**<br>Maximum: **64** |
| dataclass_id | No | String | Data class ID.<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| condition | Yes | **condition** object | Search condition expression. |
| offset | Yes | Integer | request offset, from 0<br>Minimum: **0**<br>Maximum: **999999**<br>Default: **0** |
| limit | Yes | Integer | request limit size<br>Minimum: **1**<br>Maximum: **999999** |
| sort_by | No | String | sort by property, create_time.<br>Minimum: **1**<br>Maximum: **64** |
| from_date | No | String | Query start time, for example, 2024-01-20T00:00:00.000Z +0800<br>Minimum: **0**<br>Maximum: **64** |
| to_date | No | String | Query end time, for example, 2024-01-26T23:59:59.999Z +0800<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-255** condition

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| conditions | No | Array of **conditions** objects | Expression list.<br>Array Length: **0 - 999** |
| logics | No | Array of strings | Expression logic.<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 999** |

**Table 4-256** conditions

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| name | No | String | Expression name.<br>Minimum: **0**<br>Maximum: **64** |
| data | No | Array of strings | Expression content list.<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 999** |

## Response Parameters

**Status code: 200**

**Table 4-257** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-258** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **32**<br>Maximum: **64** |
| message | String | Error Message<br>Minimum: **1**<br>Maximum: **32** |
| total | Integer | Total<br>Minimum: **0**<br>Maximum: **99999** |
| data | Array of **IndicatorDetail** objects | List of indicators.<br>Array Length: **0 - 100** |

**Table 4-259** IndicatorDetail

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Indicator ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Indicator name.<br>Minimum: **0**<br>Maximum: **64** |
| data_object | **IndicatorDataObjectDetail** object | Indicator details |
| workspace_id | String | Workspace ID<br>Minimum: **32**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| dataclass_ref | **DataClassRefPojo** object | Data class object information. |
| create_time | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-260** IndicatorDataObjectDetail

| Parameter | Type | Description |
| --- | --- | --- |
| indicator_type | **indicator_type** object | Indicator type object. |
| value | String | Value, for example, ip url domain.<br>Minimum: **0**<br>Maximum: **256** |
| update_time | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| create_time | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |
| environment | **environment** object | Environment Info |
| data_source | **data_source** object | Data source. |
| first_report_time | String | First Occurred At<br>Minimum: **0**<br>Maximum: **64** |
| is_deleted | Boolean | Delete |
| last_report_time | String | Last occurred.<br>Minimum: **0**<br>Maximum: **64** |
| granular_marking | Integer | Confidentiality level. 1 -- First discovery; 2 -- Self-produced data; 3 -- Purchase required; and 4 -- Direct query from the external network.<br>Minimum: **1**<br>Maximum: **4** |
| name | String | Name.<br>Minimum: **1**<br>Maximum: **64** |
| id | String | Indicator ID.<br>Minimum: **1**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **1**<br>Maximum: **64** |
| revoked | Boolean | Whether to discard. |
| status | String | Status. The options are Open, Closed, and Revoked.<br>Minimum: **1**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| verdict | String | Threat degree. The options are Black, White, and Gray.<br>Minimum: **1**<br>Maximum: **64** |
| workspace_id | String | Workspace ID<br>Minimum: **1**<br>Maximum: **64** |
| confidence | Integer | Confidence. The value range is 80 to 100.<br>Minimum: **80**<br>Maximum: **100** |

**Table 4-261** indicator_type

| Parameter | Type | Description |
| --- | --- | --- |
| indicator_type | String | Indicator type.<br>Minimum: **1**<br>Maximum: **32** |
| id | String | Indicator type ID.<br>Minimum: **1**<br>Maximum: **64** |
| category | String | Table of Contents<br>Minimum: **1**<br>Maximum: **64** |
| layout_id | String | Layout ID.<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-262** environment

| Parameter | Type | Description |
| --- | --- | --- |
| vendor_type | String | Environment suppliers, such as HWC, AWS, and Azure.<br>Minimum: **0**<br>Maximum: **1024** |

| Parameter | Type | Description |
| --- | --- | --- |
| domain_id | String | Tenant ID.<br>Minimum: **32**<br>Maximum: **64** |
| region_id | String | Region ID<br>Minimum: **1**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-263** data_source

| Parameter | Type | Description |
| --- | --- | --- |
| source_type | Integer | Data source type. The options are as follows--1- Huawei product 2- Third-party product 3-Tenant product<br>Minimum: **0**<br>Maximum: **9999** |
| domain_id | String | Tenant ID.<br>Minimum: **32**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| region_id | String | Region ID<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-264** DataClassRefPojo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Data class ID.<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| name | String | Data class name.<br>Minimum: **0**<br>Maximum: **64** |

**Status code: 400**

**Table 4-265** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-266** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Query the intelligence indicator list. IDs are id1 and id2; Name is indicator name; Type is DATA_SOURCE; Data class ID is 28f61af50fc9452aa0ed5ea25c3cc3d3; Offset is 0. A maximum of 10 indicators can be included, and sorted by create_time.

```
{
  "ids" : [ "id1", "id2" ],
  "name" : "Indicator name.",
  "dataclass_id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
  "condition" : {
    "conditions" : [ {
      "name" : "title",
      "data" : [ "title", "=", "Incident" ]
    } ],
    "logics" : [ "title" ]
  },
  "offset" : 0,
  "limit" : 10,
  "sort_by" : "create_time",
  "from_date" : "2024-01-20T00:00:00.000Z+0800",
  "to_date" : "2024-01-26T23:59:59.999Z+0800"
}
```

## Example Responses

**Status code: 200**

Response when the request is successful.


```
{
  "code" : "00000000",
  "data" : [ {
    "create_time" : "2023-07-24T20:54:19Z+0800",
    "data_object" : {
      "indicator_type" : {
        "layout_id" : "20e45c85-8192-3142-bfc8-54b784a80c69",
        "indicator_type" : "ipv6",
        "id" : "ac794b2dfab9fe8c0676587301a636d3",
        "category" : "ipv6"
      },
      "revoked" : false,
      "workspace_id" : "d5baeef8-3e75-4e91-9826-fb208ac58987",
      "update_time" : "2023-07-24T20:54:19.038Z+0800",
      "project_id" : "15645222e8744afa985c93dab6341da6",
      "first_report_time" : "2023-07-31T20:54:12.000Z+0800",
      "id" : "ff61d1f8-0de4-4077-9e9b-e312f6829c6d",
      "granular_marking" : 1,
      "value" : "{}",
      "create_time" : "2023-07-24T20:54:19.038Z+0800",
      "confidence" : 80,
      "last_report_time" : "2023-07-25T20:54:15.000Z+0800",
      "data_source" : {
        "domain_id" : "ac7438b990ef4a37b741004eb45e8bf4",
        "project_id" : "15645222e8744afa985c93dab6341da6",
        "region_id" : "cn-XXX-7",
        "source_type" : 1
      },
      "environment" : {
        "domain_id" : "ac7438b990ef4a37b741004eb45e8bf4",
        "project_id" : "15645222e8744afa985c93dab6341da6",
        "region_id" : "cn-xxx-7",
        "vendor_type" : "xxx"
      },
      "verdict" : "Black",
      "name" : "test",
      "status" : "Open"
    },
    "dataclass_ref" : {
      "id" : "97ccf890-7480-31f6-a961-cf8da1f2f040",
      "name" : "name"
    },
    "id" : "ff61d1f8-0de4-4077-9e9b-e312f6829c6d",
    "update_time" : "2023-07-24T20:54:19Z+0800"
  } ],
  "message" : "",
  "total" : 2
}
```


## SDK Sample Code

The SDK sample code is as follows.

## Java

Query the intelligence indicator list. IDs are id1 and id2; Name is indicator name; Type is DATA_SOURCE; Data class ID is 28f61af50fc9452aa0ed5ea25c3cc3d3; Offset is 0. A maximum of 10 indicators can be included, and sorted by create_time.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class ListIndicatorsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListIndicatorsRequest request = new ListIndicatorsRequest();
        IndicatorListSearchRequest body = new IndicatorListSearchRequest();
        List<String> listConditionLogics = new ArrayList<>();
        listConditionLogics.add("title");
        List<String> listConditionsData = new ArrayList<>();
        listConditionsData.add("title");
        listConditionsData.add("=");
        listConditionsData.add("Incident");
        List<IndicatorListSearchRequestConditionConditions> listConditionConditions = new ArrayList<>();
        listConditionConditions.add(
            new IndicatorListSearchRequestConditionConditions()
                .withName("title")
                .withData(listConditionsData)
        );
        IndicatorListSearchRequestCondition conditionbody = new IndicatorListSearchRequestCondition();
        conditionbody.withConditions(listConditionConditions)
            .withLogics(listConditionLogics);
        List<String> listbodyIds = new ArrayList<>();
        listbodyIds.add("id1");
        listbodyIds.add("id2");
        body.withToDate("2024-01-26T23:59:59.999Z+0800");
        body.withFromDate("2024-01-20T00:00:00.000Z+0800");
        body.withSortBy("create_time");
        body.withLimit(10);
        body.withOffset(0);
        body.withCondition(conditionbody);
        body.withDataclassId("28f61af50fc9452aa0ed5ea25c3cc3d3");
        body.withName("Indicator name.");
        body.withIds(listbodyIds);
        request.withBody(body);
        try {
            ListIndicatorsResponse response = client.listIndicators(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
```

```
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Query the intelligence indicator list. IDs are id1 and id2; Name is indicator name; Type is DATA_SOURCE; Data class ID is 28f61af50fc9452aa0ed5ea25c3cc3d3; Offset is 0. A maximum of 10 indicators can be included, and sorted by create_time.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListIndicatorsRequest()
        listLogicsCondition = [
            "title"
        ]
        listDataConditions = [
            "title",
            "=",
            "Incident"
        ]
        listConditionsCondition = [
            IndicatorListSearchRequestConditionConditions(
                name="title",
                data=listDataConditions
            )
        ]
        conditionbody = IndicatorListSearchRequestCondition(
            conditions=listConditionsCondition,
            logics=listLogicsCondition
        )
        listIdsbody = [
            "id1",
            "id2"
        ]
        request.body = IndicatorListSearchRequest(
            to_date="2024-01-26T23:59:59.999Z+0800",
            from_date="2024-01-20T00:00:00.000Z+0800",
```

```
        sort_by="create_time",
        limit=10,
        offset=0,
        condition=conditionbody,
        dataclass_id="28f61af50fc9452aa0ed5ea25c3cc3d3",
        name="Indicator name.",
        ids=listIdsbody
    )
    response = client.list_indicators(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

Query the intelligence indicator list. IDs are id1 and id2; Name is indicator name; Type is DATA_SOURCE; Data class ID is 28f61af50fc9452aa0ed5ea25c3cc3d3; Offset is 0. A maximum of 10 indicators can be included, and sorted by create_time.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListIndicatorsRequest{}
    var listLogicsCondition = []string{
        "title",
    }
    var listDataConditions = []string{
        "title",
        "=",
        "Incident",
    }
    nameConditions:= "title"
    var listConditionsCondition = []model.IndicatorListSearchRequestConditionConditions{
        {
            Name: &nameConditions,
            Data: &listDataConditions,
        },
```

```
    }
    conditionbody := &model.IndicatorListSearchRequestCondition{
        Conditions: &listConditionsCondition,
        Logics: &listLogicsCondition,
    }
    var listIdsbody = []string{
        "id1",
        "id2",
    }
    toDateIndicatorListSearchRequest:= "2024-01-26T23:59:59.999Z+0800"
    fromDateIndicatorListSearchRequest:= "2024-01-20T00:00:00.000Z+0800"
    sortByIndicatorListSearchRequest:= "create_time"
    dataclassIdIndicatorListSearchRequest:= "28f61af50fc9452aa0ed5ea25c3cc3d3"
    nameIndicatorListSearchRequest:= "Indicator name."
    request.Body = &model.IndicatorListSearchRequest{
        ToDate: &toDateIndicatorListSearchRequest,
        FromDate: &fromDateIndicatorListSearchRequest,
        SortBy: &sortByIndicatorListSearchRequest,
        Limit: int32(10),
        Offset: int32(0),
        Condition: conditionbody,
        DataclassId: &dataclassIdIndicatorListSearchRequest,
        Name: &nameIndicatorListSearchRequest,
        Ids: &listIdsbody,
    }
    response, err := client.ListIndicators(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

## Error Codes

See **Error Codes**.

# 4.3.2 Creating an Indicator

## Function

Creating an Indicator

## Calling Method

For details, see **Calling APIs**.

## URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/indicators

**Table 4-267** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **1**<br>Maximum: **1024** |

## Request Parameters

**Table 4-268** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | Token of the tenant.<br>Minimum: **32**<br>Maximum: **65535** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-269** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| data_object | Yes | **CreateIndicatorDetail** object | Indicator details. |

**Table 4-270** CreateIndicatorDetail

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| data_source | Yes | **data_source** object | Data source. |
| verdict | Yes | String | Threat Rating<br>Minimum: **1**<br>Maximum: **64** |
| confidence | No | Integer | Confidence level<br>Minimum: **0**<br>Maximum: **99** |
| status | No | String | Status<br>Minimum: **1**<br>Maximum: **64** |
| labels | No | String | Tag.<br>Minimum: **1**<br>Maximum: **64** |
| value | Yes | String | Value.<br>Minimum: **1**<br>Maximum: **128** |
| granular_marking | Yes | String | Confidentiality level. 1 -- First discovery; 2 -- Self-produced data; 3 -- Purchase required; and 4 -- Direct query from the external network.<br>Minimum: **1**<br>Maximum: **64** |
| environment | Yes | **environment** object | Environment Info |
| defanged | Yes | Boolean | Still valid?<br>Default: **false**<br>Enumeration values:<br>• **true**<br>• **false** |
| first_report_time | Yes | String | First Occurred At<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| last_report_time | No | String | Last occurred.<br>Minimum: **0**<br>Maximum: **64** |
| id | No | String | Indicator ID.<br>Minimum: **32**<br>Maximum: **64** |
| indicator_type | Yes | **indicator_type** object | Indicator type statistics. |
| name | Yes | String | Indicator name.<br>Minimum: **0**<br>Maximum: **64** |
| dataclass_id | No | String | Data class ID.<br>Minimum: **32**<br>Maximum: **64** |
| data_object | No | **IndicatorDataObjectDetail** object | Indicator details |
| workspace_id | Yes | String | workspace id<br>Minimum: **32**<br>Maximum: **64** |
| project_id | No | String | Project id value<br>Minimum: **32**<br>Maximum: **64** |
| layout_id | No | String | Layout ID.<br>Minimum: **0**<br>Maximum: **64** |
| dataclass | No | **DataClassRefPojo** object | Data class object information. |
| create_time | No | String | Create time<br>Minimum: **0**<br>Maximum: **64** |
| update_time | No | String | Update time<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-271** data_source

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| source_type | Yes | Integer | current page count<br>Minimum: **0**<br>Maximum: **9999** |
| domain_id | Yes | String | Id value<br>Minimum: **32**<br>Maximum: **64** |
| project_id | Yes | String | Id value<br>Minimum: **32**<br>Maximum: **64** |
| region_id | Yes | String | Id value<br>Minimum: **1**<br>Maximum: **64** |
| product_name | Yes | String | Id value<br>Minimum: **1**<br>Maximum: **64** |
| product_feature | Yes | String | Id value<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-272** environment

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| vendor_type | Yes | String | Environment suppliers, such as HWC/AWS.<br>Minimum: **0**<br>Maximum: **1024** |
| domain_id | Yes | String | Tenant ID.<br>Minimum: **32**<br>Maximum: **64** |
| region_id | Yes | String | Region ID<br>Minimum: **1**<br>Maximum: **64** |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-273** indicator_type

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| indicator_type | Yes | String | Metric Type<br>Minimum: **1**<br>Maximum: **32** |
| id | Yes | String | Indicator type ID.<br>Minimum: **1**<br>Maximum: **64** |
| category | Yes | String | Table of Contents<br>Minimum: **1**<br>Maximum: **64** |
| layout_id | Yes | String | Layout ID.<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-274** IndicatorDataObjectDetail

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| indicator_type | No | **indicator_type** object | Indicator type object. |
| value | No | String | Value, for example, ip url domain.<br>Minimum: **0**<br>Maximum: **256** |
| update_time | No | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |
| create_time | No | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |
| environment | No | **environment** object | Environment Info |
| data_source | No | **data_source** object | Data source. |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| first_report_time | No | String | First Occurred At<br>Minimum: **0**<br>Maximum: **64** |
| is_deleted | No | Boolean | Delete |
| last_report_time | No | String | Last occurred.<br>Minimum: **0**<br>Maximum: **64** |
| granular_marking | No | Integer | Confidentiality level. 1 -- First discovery; 2 -- Self-produced data; 3 -- Purchase required; and 4 -- Direct query from the external network.<br>Minimum: **1**<br>Maximum: **4** |
| name | No | String | Name.<br>Minimum: **1**<br>Maximum: **64** |
| id | No | String | Indicator ID.<br>Minimum: **1**<br>Maximum: **64** |
| project_id | No | String | Project ID.<br>Minimum: **1**<br>Maximum: **64** |
| revoked | No | Boolean | Whether to discard. |
| status | No | String | Status. The options are Open, Closed, and Revoked.<br>Minimum: **1**<br>Maximum: **64** |
| verdict | No | String | Threat degree. The options are Black, White, and Gray.<br>Minimum: **1**<br>Maximum: **64** |
| workspace_id | No | String | Workspace ID<br>Minimum: **1**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| confidence | No | Integer | Confidence. The value range is 80 to 100.<br>Minimum: **80**<br>Maximum: **100** |

**Table 4-275** indicator_type

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| indicator_type | No | String | Indicator type.<br>Minimum: **1**<br>Maximum: **32** |
| id | No | String | Indicator type ID.<br>Minimum: **1**<br>Maximum: **64** |
| category | No | String | Table of Contents<br>Minimum: **1**<br>Maximum: **64** |
| layout_id | No | String | Layout ID.<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-276** environment

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| vendor_type | No | String | Environment suppliers, such as HWC, AWS, and Azure.<br>Minimum: **0**<br>Maximum: **1024** |
| domain_id | No | String | Tenant ID.<br>Minimum: **32**<br>Maximum: **64** |
| region_id | No | String | Region ID<br>Minimum: **1**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | No | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-277** data_source

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| source_type | No | Integer | Data source type. The options are as follows-- 1- Huawei product 2- Third-party product 3- Tenant product<br>Minimum: **0**<br>Maximum: **9999** |
| domain_id | No | String | Tenant ID.<br>Minimum: **32**<br>Maximum: **64** |
| project_id | No | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| region_id | No | String | Region ID<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-278** DataClassRefPojo

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| id | Yes | String | Data class ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | No | String | Data class name.<br>Minimum: **0**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-279** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-280** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **32**<br>Maximum: **64** |
| message | String | Error Message<br>Minimum: **1**<br>Maximum: **32** |
| data | **IndicatorDetail** object | Indicator details. |

**Table 4-281** IndicatorDetail

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Indicator ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Indicator name.<br>Minimum: **0**<br>Maximum: **64** |
| data_object | **IndicatorDataObjectDetail** object | Indicator details |
| workspace_id | String | Workspace ID<br>Minimum: **32**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| dataclass_ref | **DataClassRefPojo** object | Data class object information. |

| Parameter | Type | Description |
| --- | --- | --- |
| create_time | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-282** IndicatorDataObjectDetail

| Parameter | Type | Description |
| --- | --- | --- |
| indicator_type | **indicator_type** object | Indicator type object. |
| value | String | Value, for example, ip url domain.<br>Minimum: **0**<br>Maximum: **256** |
| update_time | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |
| create_time | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |
| environment | **environment** object | Environment Info |
| data_source | **data_source** object | Data source. |
| first_report_time | String | First Occurred At<br>Minimum: **0**<br>Maximum: **64** |
| is_deleted | Boolean | Delete |
| last_report_time | String | Last occurred.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| granular_marking | Integer | Confidentiality level. 1 -- First discovery; 2 -- Self-produced data; 3 -- Purchase required; and 4 -- Direct query from the external network.<br>Minimum: **1**<br>Maximum: **4** |
| name | String | Name.<br>Minimum: **1**<br>Maximum: **64** |
| id | String | Indicator ID.<br>Minimum: **1**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **1**<br>Maximum: **64** |
| revoked | Boolean | Whether to discard. |
| status | String | Status. The options are Open, Closed, and Revoked.<br>Minimum: **1**<br>Maximum: **64** |
| verdict | String | Threat degree. The options are Black, White, and Gray.<br>Minimum: **1**<br>Maximum: **64** |
| workspace_id | String | Workspace ID<br>Minimum: **1**<br>Maximum: **64** |
| confidence | Integer | Confidence. The value range is 80 to 100.<br>Minimum: **80**<br>Maximum: **100** |

**Table 4-283** indicator_type

| Parameter | Type | Description |
| --- | --- | --- |
| indicator_type | String | Indicator type.<br>Minimum: **1**<br>Maximum: **32** |

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Indicator type ID.<br>Minimum: **1**<br>Maximum: **64** |
| category | String | Table of Contents<br>Minimum: **1**<br>Maximum: **64** |
| layout_id | String | Layout ID.<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-284** environment

| Parameter | Type | Description |
| --- | --- | --- |
| vendor_type | String | Environment suppliers, such as HWC, AWS, and Azure.<br>Minimum: **0**<br>Maximum: **1024** |
| domain_id | String | Tenant ID.<br>Minimum: **32**<br>Maximum: **64** |
| region_id | String | Region ID<br>Minimum: **1**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-285** data_source

| Parameter | Type | Description |
| --- | --- | --- |
| source_type | Integer | Data source type. The options are as follows--1- Huawei product 2- Third-party product 3- Tenant product<br>Minimum: **0**<br>Maximum: **9999** |

| Parameter | Type | Description |
| --- | --- | --- |
| domain_id | String | Tenant ID.<br>Minimum: **32**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| region_id | String | Region ID<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-286** DataClassRefPojo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Data class ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Data class name.<br>Minimum: **0**<br>Maximum: **64** |

**Status code: 400**

**Table 4-287** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-288** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Create an indicator. The indicator name is Indicator Name, indicator version is 1, indicator type is DATA_SOURCE, and Trigger Flag is NO.

```
{
  "data_object" : {
    "data_source" : {
      "source_type" : 3,
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "product_name" : "test",
      "product_feature" : "test"
    },
    "verdict" : "BLACK",
    "confidence" : 4,
    "status" : "OPEN",
    "labels" : "OPEN",
    "value" : "{}",
    "granular_marking" : "1",
    "environment" : {
      "vendor_type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "defanged" : false,
    "first_report_time" : "2021-01-30T23:00:00Z+0800",
    "last_report_time" : "2021-01-30T23:00:00Z+0800",
    "id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
    "indicator_type" : { },
    "name" : "Indicator name.",
    "dataclass_id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
    "data_object" : {
      "indicator_type" : { },
      "value" : "ip"
    },
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "layout_id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
    "dataclass" : {
      "id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
      "name" : "Name."
    },
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800"
  }
}
```

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
    "name" : "Indicator name.",
    "data_object" : {
      "indicator_type" : {
        "layout_id" : "4e2d7f64-a66d-3236-a8c1-704636ced9a7",
        "indicator_type" : "ipv6",
        "id" : "ac794b2dfab9fe8c0676587301a636d3",
        "category" : "ipv6"
      },
      "value" : "ip",
      "data_source" : {
        "domain_id" : "ac7438b990ef4a37b741004eb45e8bf4",
        "project_id" : "5b8bb3c888db498f9eeaf1023f7ba597",
        "region_id" : "cn-xxx-7",
        "source_type" : 1
      },
      "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "granular_marking" : 1,
      "first_report_time" : "2023-07-04T16:47:01Z+0800",
      "status" : "Open"
    },
    "dataclass_ref" : {
      "id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
      "name" : "Name."
    },
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800"
  }
}
```


## SDK Sample Code

The SDK sample code is as follows.

## Java

Create an indicator. The indicator name is Indicator Name, indicator version is 1, indicator type is DATA_SOURCE, and Trigger Flag is NO.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class CreateIndicatorSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
```

```
        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateIndicatorRequest request = new CreateIndicatorRequest();
        IndicatorCreateRequest body = new IndicatorCreateRequest();
        DataClassRefPojo dataclassDataObject = new DataClassRefPojo();
        dataclassDataObject.withId("28f61af50fc9452aa0ed5ea25c3cc3d3")
            .withName("Name.");
        IndicatorDataObjectDetail dataObjectDataObject = new IndicatorDataObjectDetail();
        dataObjectDataObject.withValue("ip");
        CreateIndicatorDetailEnvironment environmentDataObject = new CreateIndicatorDetailEnvironment();
        environmentDataObject.withVendorType("MyXXX")
            .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        CreateIndicatorDetailDataSource dataSourceDataObject = new CreateIndicatorDetailDataSource();
        dataSourceDataObject.withSourceType(3)
            .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withProductName("test")
            .withProductFeature("test");
        CreateIndicatorDetail dataObjectbody = new CreateIndicatorDetail();
        dataObjectbody.withDataSource(dataSourceDataObject)
            .withVerdict("BLACK")
            .withConfidence(4)
            .withStatus("OPEN")
            .withLabels("OPEN")
            .withValue("{}")
            .withGranularMarking("1")
            .withEnvironment(environmentDataObject)
            .withDefanged(false)
            .withFirstReportTime("2021-01-30T23:00:00Z+0800")
            .withLastReportTime("2021-01-30T23:00:00Z+0800")
            .withId("28f61af50fc9452aa0ed5ea25c3cc3d3")
            .withName("Indicator name.")
            .withDataclassId("28f61af50fc9452aa0ed5ea25c3cc3d3")
            .withDataObject(dataObjectDataObject)
            .withWorkspaceId("909494e3-558e-46b6-a9eb-07a8e18ca620")
            .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withLayoutId("28f61af50fc9452aa0ed5ea25c3cc3d3")
            .withDataclass(dataclassDataObject)
            .withCreateTime("2021-01-30T23:00:00Z+0800")
            .withUpdateTime("2021-01-30T23:00:00Z+0800");
        body.withDataObject(dataObjectbody);
        request.withBody(body);
        try {
            CreateIndicatorResponse response = client.createIndicator(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Create an indicator. The indicator name is Indicator Name, indicator version is 1, indicator type is DATA_SOURCE, and Trigger Flag is NO.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateIndicatorRequest()
        dataclassDataObject = DataClassRefPojo(
            id="28f61af50fc9452aa0ed5ea25c3cc3d3",
            name="Name."
        )
        dataObjectDataObject = IndicatorDataObjectDetail(
            value="ip"
        )
        environmentDataObject = CreateIndicatorDetailEnvironment(
            vendor_type="MyXXX",
            domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f"
        )
        dataSourceDataObject = CreateIndicatorDetailDataSource(
            source_type=3,
            domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            product_name="test",
            product_feature="test"
        )
        dataObjectbody = CreateIndicatorDetail(
            data_source=dataSourceDataObject,
            verdict="BLACK",
            confidence=4,
            status="OPEN",
            labels="OPEN",
            value="{}",
            granular_marking="1",
            environment=environmentDataObject,
            defanged=False,
            first_report_time="2021-01-30T23:00:00Z+0800",
            last_report_time="2021-01-30T23:00:00Z+0800",
            id="28f61af50fc9452aa0ed5ea25c3cc3d3",
            name="Indicator name.",
            dataclass_id="28f61af50fc9452aa0ed5ea25c3cc3d3",
            data_object=dataObjectDataObject,
            workspace_id="909494e3-558e-46b6-a9eb-07a8e18ca620",
            project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
```

```
        layout_id="28f61af50fc9452aa0ed5ea25c3cc3d3",
        dataclass=dataclassDataObject,
        create_time="2021-01-30T23:00:00Z+0800",
        update_time="2021-01-30T23:00:00Z+0800"
    )
    request.body = IndicatorCreateRequest(
        data_object=dataObjectbody
    )
    response = client.create_indicator(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

Create an indicator. The indicator name is Indicator Name, indicator version is 1, indicator type is DATA_SOURCE, and Trigger Flag is NO.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateIndicatorRequest{}
    nameDataclass:= "Name."
    dataclassDataObject := &model.DataClassRefPojo{
        Id: "28f61af50fc9452aa0ed5ea25c3cc3d3",
        Name: &nameDataclass,
    }
    valueDataObject:= "ip"
    dataObjectDataObject := &model.IndicatorDataObjectDetail{
        Value: &valueDataObject,
    }
    environmentDataObject := &model.CreateIndicatorDetailEnvironment{
        VendorType: "MyXXX",
        DomainId: "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        RegionId: "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        ProjectId: "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    }
    dataSourceDataObject := &model.CreateIndicatorDetailDataSource{
        SourceType: int32(3),
```

```
        DomainId: "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        ProjectId: "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        RegionId: "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        ProductName: "test",
        ProductFeature: "test",
    }
    confidenceDataObject:= int32(4)
    statusDataObject:= "OPEN"
    labelsDataObject:= "OPEN"
    lastReportTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    idDataObject:= "28f61af50fc9452aa0ed5ea25c3cc3d3"
    dataclassIdDataObject:= "28f61af50fc9452aa0ed5ea25c3cc3d3"
    projectIdDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    layoutIdDataObject:= "28f61af50fc9452aa0ed5ea25c3cc3d3"
    createTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    updateTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    dataObjectbody := &model.CreateIndicatorDetail{
        DataSource: dataSourceDataObject,
        Verdict: "BLACK",
        Confidence: &confidenceDataObject,
        Status: &statusDataObject,
        Labels: &labelsDataObject,
        Value: "{}",
        GranularMarking: "1",
        Environment: environmentDataObject,
        Defanged: false,
        FirstReportTime: "2021-01-30T23:00:00Z+0800",
        LastReportTime: &lastReportTimeDataObject,
        Id: &idDataObject,
        Name: "Indicator name.",
        DataclassId: &dataclassIdDataObject,
        DataObject: dataObjectDataObject,
        WorkspaceId: "909494e3-558e-46b6-a9eb-07a8e18ca620",
        ProjectId: &projectIdDataObject,
        LayoutId: &layoutIdDataObject,
        Dataclass: dataclassDataObject,
        CreateTime: &createTimeDataObject,
        UpdateTime: &updateTimeDataObject,
    }
    request.Body = &model.IndicatorCreateRequest{
        DataObject: dataObjectbody,
    }
    response, err := client.CreateIndicator(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

## Error Codes

See **Error Codes**.

# 4.3.3 This API is used to delete an indicator.

## Function

This API is used to delete an indicator.

## Calling Method

For details, see **Calling APIs**.

## URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/indicators

**Table 4-289** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **1**<br>Maximum: **1024** |

## Request Parameters

**Table 4-290** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | Token of the tenant.<br>Minimum: **32**<br>Maximum: **65535** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-291** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| batch_ids | No | Array of strings | List of indicator IDs.<br>Minimum: **32**<br>Maximum: **64**<br>Array Length: **0 - 999** |

## Response Parameters

**Status code: 200**

**Table 4-292** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-293** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **32**<br>Maximum: **64** |
| message | String | Error Message<br>Minimum: **1**<br>Maximum: **32** |
| data | **IndicatorBatchOperateResponse** object | Intelligence response parameters |

**Table 4-294** IndicatorBatchOperateResponse

| Parameter | Type | Description |
| --- | --- | --- |
| success_ids | Array of strings | Succeeded IDs.<br>Minimum: **32**<br>Maximum: **64**<br>Array Length: **0 - 999** |

| Parameter | Type | Description |
| --- | --- | --- |
| error_ids | Array of strings | Failed IDs.<br>Minimum: **32**<br>Maximum: **64**<br>Array Length: **0 - 999** |

**Status code: 400**

**Table 4-295** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-296** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Delete an indicator. Its batch ID is 909494e3-558e-46b6-a9eb-07a8e18ca62f.

```
{
  "batch_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ]
}
```

## Example Responses

**Status code: 200**

Response succeeded.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "success_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ],
    "error_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ]
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Delete an indicator. Its batch ID is 909494e3-558e-46b6-a9eb-07a8e18ca62f.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class DeleteIndicatorSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteIndicatorRequest request = new DeleteIndicatorRequest();
        DeleteIndicatorRequestBody body = new DeleteIndicatorRequestBody();
        List<String> listbodyBatchIds = new ArrayList<>();
        listbodyBatchIds.add("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withBatchIds(listbodyBatchIds);
        request.withBody(body);
        try {
            DeleteIndicatorResponse response = client.deleteIndicator(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Delete an indicator. Its batch ID is 909494e3-558e-46b6-a9eb-07a8e18ca62f.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteIndicatorRequest()
        listBatchIdsbody = [
            "909494e3-558e-46b6-a9eb-07a8e18ca62f"
        ]
        request.body = DeleteIndicatorRequestBody(
            batch_ids=listBatchIdsbody
        )
        response = client.delete_indicator(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Delete an indicator. Its batch ID is 909494e3-558e-46b6-a9eb-07a8e18ca62f.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
```

```
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteIndicatorRequest{}
    var listBatchIdsbody = []string{
        "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    }
    request.Body = &model.DeleteIndicatorRequestBody{
        BatchIds: &listBatchIdsbody,
    }
    response, err := client.DeleteIndicator(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response succeeded. |
| 400 | Response upon a request failure |

## Error Codes

See **Error Codes**.

# 4.3.4 Querying Indicator Details

## Function

Querying Indicator Details

## Calling Method

For details, see **Calling APIs**.

## URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/{indicator_id}

**Table 4-297** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **1**<br>Maximum: **1024** |
| indicator_id | Yes | String | Intelligence indicator ID.<br>Minimum: **32**<br>Maximum: **64** |

## Request Parameters

**Table 4-298** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | Token of the tenant.<br>Minimum: **32**<br>Maximum: **65535** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-299** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-300** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **32**<br>Maximum: **64** |
| message | String | Error Message<br>Minimum: **1**<br>Maximum: **32** |
| data | **IndicatorDetail** object | Indicator details. |

**Table 4-301** IndicatorDetail

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Indicator ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Indicator name.<br>Minimum: **0**<br>Maximum: **64** |
| data_object | **IndicatorDataObjectDetail** object | Indicator details |
| workspace_id | String | Workspace ID<br>Minimum: **32**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| dataclass_ref | **DataClassRefPojo** object | Data class object information. |
| create_time | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-302** IndicatorDataObjectDetail

| Parameter | Type | Description |
| --- | --- | --- |
| indicator_type | **indicator_type** object | Indicator type object. |
| value | String | Value, for example, ip url domain.<br>Minimum: **0**<br>Maximum: **256** |
| update_time | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |
| create_time | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |
| environment | **environment** object | Environment Info |
| data_source | **data_source** object | Data source. |
| first_report_time | String | First Occurred At<br>Minimum: **0**<br>Maximum: **64** |
| is_deleted | Boolean | Delete |
| last_report_time | String | Last occurred.<br>Minimum: **0**<br>Maximum: **64** |
| granular_marking | Integer | Confidentiality level. 1 -- First discovery; 2 -- Self-produced data; 3 -- Purchase required; and 4 -- Direct query from the external network.<br>Minimum: **1**<br>Maximum: **4** |
| name | String | Name.<br>Minimum: **1**<br>Maximum: **64** |
| id | String | Indicator ID.<br>Minimum: **1**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| project_id | String | Project ID.<br>Minimum: **1**<br>Maximum: **64** |
| revoked | Boolean | Whether to discard. |
| status | String | Status. The options are Open, Closed, and Revoked.<br>Minimum: **1**<br>Maximum: **64** |
| verdict | String | Threat degree. The options are Black, White, and Gray.<br>Minimum: **1**<br>Maximum: **64** |
| workspace_id | String | Workspace ID<br>Minimum: **1**<br>Maximum: **64** |
| confidence | Integer | Confidence. The value range is 80 to 100.<br>Minimum: **80**<br>Maximum: **100** |

**Table 4-303** indicator_type

| Parameter | Type | Description |
| --- | --- | --- |
| indicator_type | String | Indicator type.<br>Minimum: **1**<br>Maximum: **32** |
| id | String | Indicator type ID.<br>Minimum: **1**<br>Maximum: **64** |
| category | String | Table of Contents<br>Minimum: **1**<br>Maximum: **64** |
| layout_id | String | Layout ID.<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-304** environment

| Parameter | Type | Description |
| --- | --- | --- |
| vendor_type | String | Environment suppliers, such as HWC, AWS, and Azure.<br>Minimum: **0**<br>Maximum: **1024** |
| domain_id | String | Tenant ID.<br>Minimum: **32**<br>Maximum: **64** |
| region_id | String | Region ID<br>Minimum: **1**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-305** data_source

| Parameter | Type | Description |
| --- | --- | --- |
| source_type | Integer | Data source type. The options are as follows--1- Huawei product 2- Third-party product 3- Tenant product<br>Minimum: **0**<br>Maximum: **9999** |
| domain_id | String | Tenant ID.<br>Minimum: **32**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| region_id | String | Region ID<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-306** DataClassRefPojo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Data class ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Data class name.<br>Minimum: **0**<br>Maximum: **64** |

**Status code: 400**

**Table 4-307** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-308** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
    "name" : "Indicator name.",
```

```
  "data_object" : {
    "indicator_type" : {
      "layout_id" : "4e2d7f64-a66d-3236-a8c1-704636ced9a7",
      "indicator_type" : "ipv6",
      "id" : "ac794b2dfab9fe8c0676587301a636d3",
      "category" : "ipv6"
    },
    "value" : "ip",
    "data_source" : {
      "domain_id" : "ac7438b990ef4a37b741004eb45e8bf4",
      "project_id" : "5b8bb3c888db498f9eeaf1023f7ba597",
      "region_id" : "cn-xxx-7",
      "source_type" : 1
    },
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "granular_marking" : 1,
    "first_report_time" : "2023-07-04T16:47:01Z+0800",
    "status" : "Open"
  },
  "dataclass_ref" : {
    "id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
    "name" : "Name."
  },
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800"
 }
}
```


## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowIndicatorDetailSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowIndicatorDetailRequest request = new ShowIndicatorDetailRequest();
        try {
```

```
            ShowIndicatorDetailResponse response = client.showIndicatorDetail(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowIndicatorDetailRequest()
        response = client.show_indicator_detail(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
```

```
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowIndicatorDetailRequest{}
    response, err := client.ShowIndicatorDetail(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

## Error Codes

See **Error Codes**.

# 4.3.5 Updating Indicators

## Function

Updating Indicators

## Calling Method

For details, see **Calling APIs**.

## URI

PUT /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/{indicator_id}

**Table 4-309** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **1**<br>Maximum: **1024** |
| indicator_id | Yes | String | Indicator ID.<br>Minimum: **32**<br>Maximum: **64** |

## Request Parameters

**Table 4-310** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | Token of the tenant.<br>Minimum: **32**<br>Maximum: **65535** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-311** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| data_object | No | **IndicatorDataObjectDetail** object | Indicator details |

**Table 4-312** IndicatorDataObjectDetail

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| indicator_type | No | **indicator_type** object | Indicator type object. |
| value | No | String | Value, for example, ip url domain.<br>Minimum: **0**<br>Maximum: **256** |
| update_time | No | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |
| create_time | No | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |
| environment | No | **environment** object | Environment Info |
| data_source | No | **data_source** object | Data source. |
| first_report_time | No | String | First Occurred At<br>Minimum: **0**<br>Maximum: **64** |
| is_deleted | No | Boolean | Delete |
| last_report_time | No | String | Last occurred.<br>Minimum: **0**<br>Maximum: **64** |
| granular_marking | No | Integer | Confidentiality level. 1 -- First discovery; 2 -- Self-produced data; 3 -- Purchase required; and 4 -- Direct query from the external network.<br>Minimum: **1**<br>Maximum: **4** |
| name | No | String | Name.<br>Minimum: **1**<br>Maximum: **64** |
| id | No | String | Indicator ID.<br>Minimum: **1**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | No | String | Project ID.<br>Minimum: **1**<br>Maximum: **64** |
| revoked | No | Boolean | Whether to discard. |
| status | No | String | Status. The options are Open, Closed, and Revoked.<br>Minimum: **1**<br>Maximum: **64** |
| verdict | No | String | Threat degree. The options are Black, White, and Gray.<br>Minimum: **1**<br>Maximum: **64** |
| workspace_id | No | String | Workspace ID<br>Minimum: **1**<br>Maximum: **64** |
| confidence | No | Integer | Confidence. The value range is 80 to 100.<br>Minimum: **80**<br>Maximum: **100** |

**Table 4-313** indicator_type

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| indicator_type | No | String | Indicator type.<br>Minimum: **1**<br>Maximum: **32** |
| id | No | String | Indicator type ID.<br>Minimum: **1**<br>Maximum: **64** |
| category | No | String | Table of Contents<br>Minimum: **1**<br>Maximum: **64** |
| layout_id | No | String | Layout ID.<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-314** environment

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| vendor_type | No | String | Environment suppliers, such as HWC, AWS, and Azure.<br>Minimum: **0**<br>Maximum: **1024** |
| domain_id | No | String | Tenant ID.<br>Minimum: **32**<br>Maximum: **64** |
| region_id | No | String | Region ID<br>Minimum: **1**<br>Maximum: **64** |
| project_id | No | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-315** data_source

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| source_type | No | Integer | Data source type. The options are as follows-- 1- Huawei product 2- Third-party product 3- Tenant product<br>Minimum: **0**<br>Maximum: **9999** |
| domain_id | No | String | Tenant ID.<br>Minimum: **32**<br>Maximum: **64** |
| project_id | No | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| region_id | No | String | Region ID<br>Minimum: **1**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-316** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-317** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **32**<br>Maximum: **64** |
| message | String | Error Message<br>Minimum: **1**<br>Maximum: **32** |
| data | **IndicatorDetail** object | Indicator details. |

**Table 4-318** IndicatorDetail

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Indicator ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Indicator name.<br>Minimum: **0**<br>Maximum: **64** |
| data_object | **IndicatorDataObjectDetail** object | Indicator details |
| workspace_id | String | Workspace ID<br>Minimum: **32**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| dataclass_ref | **DataClassRefPojo** object | Data class object information. |

| Parameter | Type | Description |
| --- | --- | --- |
| create_time | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-319** IndicatorDataObjectDetail

| Parameter | Type | Description |
| --- | --- | --- |
| indicator_type | **indicator_type** object | Indicator type object. |
| value | String | Value, for example, ip url domain.<br>Minimum: **0**<br>Maximum: **256** |
| update_time | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |
| create_time | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |
| environment | **environment** object | Environment Info |
| data_source | **data_source** object | Data source. |
| first_report_time | String | First Occurred At<br>Minimum: **0**<br>Maximum: **64** |
| is_deleted | Boolean | Delete |
| last_report_time | String | Last occurred.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| granular_marking | Integer | Confidentiality level. 1 -- First discovery; 2 -- Self-produced data; 3 -- Purchase required; and 4 -- Direct query from the external network.<br>Minimum: **1**<br>Maximum: **4** |
| name | String | Name.<br>Minimum: **1**<br>Maximum: **64** |
| id | String | Indicator ID.<br>Minimum: **1**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **1**<br>Maximum: **64** |
| revoked | Boolean | Whether to discard. |
| status | String | Status. The options are Open, Closed, and Revoked.<br>Minimum: **1**<br>Maximum: **64** |
| verdict | String | Threat degree. The options are Black, White, and Gray.<br>Minimum: **1**<br>Maximum: **64** |
| workspace_id | String | Workspace ID<br>Minimum: **1**<br>Maximum: **64** |
| confidence | Integer | Confidence. The value range is 80 to 100.<br>Minimum: **80**<br>Maximum: **100** |

**Table 4-320** indicator_type

| Parameter | Type | Description |
| --- | --- | --- |
| indicator_type | String | Indicator type.<br>Minimum: **1**<br>Maximum: **32** |

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Indicator type ID.<br>Minimum: **1**<br>Maximum: **64** |
| category | String | Table of Contents<br>Minimum: **1**<br>Maximum: **64** |
| layout_id | String | Layout ID.<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-321** environment

| Parameter | Type | Description |
| --- | --- | --- |
| vendor_type | String | Environment suppliers, such as HWC, AWS, and Azure.<br>Minimum: **0**<br>Maximum: **1024** |
| domain_id | String | Tenant ID.<br>Minimum: **32**<br>Maximum: **64** |
| region_id | String | Region ID<br>Minimum: **1**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-322** data_source

| Parameter | Type | Description |
| --- | --- | --- |
| source_type | Integer | Data source type. The options are as follows--1- Huawei product 2- Third-party product 3-Tenant product<br>Minimum: **0**<br>Maximum: **9999** |

| Parameter | Type | Description |
| --- | --- | --- |
| domain_id | String | Tenant ID.<br>Minimum: **32**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| region_id | String | Region ID<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-323** DataClassRefPojo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Data class ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Data class name.<br>Minimum: **0**<br>Maximum: **64** |

**Status code: 400**

**Table 4-324** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-325** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Update an indicator. Set the trigger flag to No and value to IP.

```
{
  "data_object" : {
    "indicator_type" : {
      "layout_id" : "4e2d7f64-a66d-3236-a8c1-704636ced9a7",
      "indicator_type" : "ipv6",
      "id" : "ac794b2dfab9fe8c0676587301a636d3",
      "category" : "ipv6"
    },
    "value" : "ip",
    "data_source" : {
      "domain_id" : "ac7438b990ef4a37b741004eb45e8bf4",
      "project_id" : "5b8bb3c888db498f9eeaf1023f7ba597",
      "region_id" : "cn-xxx-7",
      "source_type" : 1
    },
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "granular_marking" : 1,
    "first_report_time" : "2023-07-04T16:47:01Z+0800",
    "status" : "Open"
  }
}
```

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
    "name" : "Indicator name.",
    "data_object" : {
      "indicator_type" : {
        "layout_id" : "4e2d7f64-a66d-3236-a8c1-704636ced9a7",
        "indicator_type" : "ipv6",
        "id" : "ac794b2dfab9fe8c0676587301a636d3",
        "category" : "ipv6"
      },
      "value" : "ip",
      "data_source" : {
        "domain_id" : "ac7438b990ef4a37b741004eb45e8bf4",
        "project_id" : "5b8bb3c888db498f9eeaf1023f7ba597",
        "region_id" : "cn-xxx-7",
        "source_type" : 1
      },
      "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "granular_marking" : 1,
      "first_report_time" : "2023-07-04T16:47:01Z+0800",
```

```
    "status" : "Open"
  },
  "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "dataclass_ref" : {
    "id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
    "name" : "Name."
  },
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800"
 }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Update an indicator. Set the trigger flag to No and value to IP.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class UpdateIndicatorSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdateIndicatorRequest request = new UpdateIndicatorRequest();
        UpdateIndicatorRequestBody body = new UpdateIndicatorRequestBody();
        IndicatorDataObjectDetailDataSource dataSourceDataObject = new IndicatorDataObjectDetailDataSource();
        dataSourceDataObject.withSourceType(1)
            .withDomainId("ac7438b990ef4a37b741004eb45e8bf4")
            .withProjectId("5b8bb3c888db498f9eeaf1023f7ba597")
            .withRegionId("cn-xxx-7");
        IndicatorDataObjectDetailIndicatorType indicatorTypeDataObject = new IndicatorDataObjectDetailIndicatorType();
        indicatorTypeDataObject.withIndicatorType("ipv6")
            .withId("ac794b2dfab9fe8c0676587301a636d3")
            .withCategory("ipv6")
            .withLayoutId("4e2d7f64-a66d-3236-a8c1-704636ced9a7");
        IndicatorDataObjectDetail dataObjectbody = new IndicatorDataObjectDetail();
```

```
        dataObjectbody.withIndicatorType(indicatorTypeDataObject)
            .withValue("ip")
            .withDataSource(dataSourceDataObject)
            .withFirstReportTime("2023-07-04T16:47:01Z+0800")
            .withGranularMarking(1)
            .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withStatus("Open")
            .withWorkspaceId("909494e3-558e-46b6-a9eb-07a8e18ca620");
        body.withDataObject(dataObjectbody);
        request.withBody(body);
        try {
            UpdateIndicatorResponse response = client.updateIndicator(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Update an indicator. Set the trigger flag to No and value to IP.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateIndicatorRequest()
        dataSourceDataObject = IndicatorDataObjectDetailDataSource(
            source_type=1,
            domain_id="ac7438b990ef4a37b741004eb45e8bf4",
            project_id="5b8bb3c888db498f9eeaf1023f7ba597",
            region_id="cn-xxx-7"
        )
        indicatorTypeDataObject = IndicatorDataObjectDetailIndicatorType(
            indicator_type="ipv6",
            id="ac794b2dfab9fe8c0676587301a636d3",
            category="ipv6",
            layout_id="4e2d7f64-a66d-3236-a8c1-704636ced9a7"
        )
        dataObjectbody = IndicatorDataObjectDetail(
```

```
        indicator_type=indicatorTypeDataObject,
        value="ip",
        data_source=dataSourceDataObject,
        first_report_time="2023-07-04T16:47:01Z+0800",
        granular_marking=1,
        project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        status="Open",
        workspace_id="909494e3-558e-46b6-a9eb-07a8e18ca620"
    )
    request.body = UpdateIndicatorRequestBody(
        data_object=dataObjectbody
    )
    response = client.update_indicator(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

Update an indicator. Set the trigger flag to No and value to IP.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateIndicatorRequest{}
    sourceTypeDataSource:= int32(1)
    domainIdDataSource:= "ac7438b990ef4a37b741004eb45e8bf4"
    projectIdDataSource:= "5b8bb3c888db498f9eeaf1023f7ba597"
    regionIdDataSource:= "cn-xxx-7"
    dataSourceDataObject := &model.IndicatorDataObjectDetailDataSource{
        SourceType: &sourceTypeDataSource,
        DomainId: &domainIdDataSource,
        ProjectId: &projectIdDataSource,
        RegionId: &regionIdDataSource,
    }
    indicatorTypeIndicatorType:= "ipv6"
    idIndicatorType:= "ac794b2dfab9fe8c0676587301a636d3"
    categoryIndicatorType:= "ipv6"
    layoutIdIndicatorType:= "4e2d7f64-a66d-3236-a8c1-704636ced9a7"
```

```
    indicatorTypeDataObject := &model.IndicatorDataObjectDetailIndicatorType{
        IndicatorType: &indicatorTypeIndicatorType,
        Id: &idIndicatorType,
        Category: &categoryIndicatorType,
        LayoutId: &layoutIdIndicatorType,
    }
    valueDataObject:= "ip"
    firstReportTimeDataObject:= "2023-07-04T16:47:01Z+0800"
    granularMarkingDataObject:= int32(1)
    projectIdDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    statusDataObject:= "Open"
    workspaceIdDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca620"
    dataObjectbody := &model.IndicatorDataObjectDetail{
        IndicatorType: indicatorTypeDataObject,
        Value: &valueDataObject,
        DataSource: dataSourceDataObject,
        FirstReportTime: &firstReportTimeDataObject,
        GranularMarking: &granularMarkingDataObject,
        ProjectId: &projectIdDataObject,
        Status: &statusDataObject,
        WorkspaceId: &workspaceIdDataObject,
    }
    request.Body = &model.UpdateIndicatorRequestBody{
        DataObject: dataObjectbody,
    }
    response, err := client.UpdateIndicator(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

## Error Codes

See **Error Codes**.

# 4.4 Playbook Management

# 4.4.1 Playbook Running Monitoring

## Function

Playbook Running Monitoring

## Calling Method

For details, see **Calling APIs**.

## URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}/monitor

**Table 4-326** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| playbook_id | Yes | String | Playbook ID.<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-327** Query Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| start_time | Yes | String | Start time.The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. For example, 2021-01-30T23:00:00Z+0800. Time zone is where the playbook instances occured. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **18**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| version_query_type | Yes | String | Playbook version type. The options are ALL, VALID, and DELETED.<br>Minimum: **1**<br>Maximum: **20**<br>Enumeration values:<br>• **ALL:all, VALID:valid, DELETED:deleted.** |
| end_time | Yes | String | End time.The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Time zone. For example, 2021-01-30T23:00:00Z+0800. Time zone is where the playbook instances occured. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **18**<br>Maximum: **64** |

## Request Parameters

**Table 4-328** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-329** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-330** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Error Message<br>Minimum: **1**<br>Maximum: **32** |
| data | **PlaybookInstanceMonitorDetail** object | Playbook monitoring details. |

**Table 4-331** PlaybookInstanceMonitorDetail

| Parameter | Type | Description |
| --- | --- | --- |
| total_instance_run_num | Integer | Total running times.<br>Minimum: **0**<br>Maximum: **99999999** |
| schedule_instance_run_num | Integer | Scheduled executions.<br>Minimum: **0**<br>Maximum: **99999999** |
| event_instance_run_num | Integer | Time-triggered executions.<br>Minimum: **0**<br>Maximum: **99999999** |
| average_run_time | Number | Average duration.<br>Minimum: **0**<br>Maximum: **9999999999** |

| Parameter | Type | Description |
| --- | --- | --- |
| min_run_time_instance | **PlaybookInstanceRunStatistics** object | Workflow with the shortest running duration. |
| max_run_time_instance | **PlaybookInstanceRunStatistics** object | Workflow with the longest running duration. |
| total_instance_num | Integer | Total number of playbook instances.<br>Minimum: **0**<br>Maximum: **99999999** |
| success_instance_num | Integer | Number of successful instances.<br>Minimum: **0**<br>Maximum: **99999999** |
| fail_instance_num | Integer | Failed instances.<br>Minimum: **0**<br>Maximum: **99999999** |
| terminate_instance_num | Integer | Number of terminated instances.<br>Minimum: **0**<br>Maximum: **99999999** |
| running_instance_num | Integer | Number of running instances.<br>Minimum: **0**<br>Maximum: **99999999** |

**Table 4-332** PlaybookInstanceRunStatistics

| Parameter | Type | Description |
| --- | --- | --- |
| playbook_instance_id | String | Playbook instance ID.<br>Minimum: **0**<br>Maximum: **64** |
| playbook_instance_name | String | Playbook instance name.<br>Minimum: **0**<br>Maximum: **64** |
| playbook_instance_run_time | Number | Playbook instance running time.<br>Minimum: **0**<br>Maximum: **9999999999** |

**Status code: 400**

**Table 4-333** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-334** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "code" : "00000000",
  "message" : "",
  "data" : {
    "total_instance_run_num" : "Unknown Type: in",
    "schedule_instance_run_num" : 99999999,
    "event_instance_run_num" : 99999999,
    "average_run_time" : 9999999999,
    "min_run_time_instance" : {
      "playbook_instance_id" : "string",
      "playbook_instance_name" : "string",
      "playbook_instance_run_time" : 9999999999
    },
    "max_run_time_instance" : {
      "playbook_instance_id" : "string",
      "playbook_instance_name" : "string",
      "playbook_instance_run_time" : 9999999999
    },
    "total_instance_num" : 99999999,
    "success_instance_num" : 99999999,
    "fail_instance_num" : 99999999,
    "terminate_instance_num" : 99999999,
    "running_instance_num" : 99999999
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowPlaybookMonitorsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPlaybookMonitorsRequest request = new ShowPlaybookMonitorsRequest();
        request.withStartTime("<start_time>");

request.withVersionQueryType(ShowPlaybookMonitorsRequest.VersionQueryTypeEnum.fromValue("<version_query_type>"));
        request.withEndTime("<end_time>");
        try {
            ShowPlaybookMonitorsResponse response = client.showPlaybookMonitors(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *
```

```
if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowPlaybookMonitorsRequest()
        request.start_time = "<start_time>"
        request.version_query_type = "<version_query_type>"
        request.end_time = "<end_time>"
        response = client.show_playbook_monitors(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowPlaybookMonitorsRequest{}
    request.StartTime = "<start_time>"
    request.VersionQueryType = model.GetShowPlaybookMonitorsRequestVersionQueryTypeEnum().<VERSION_QUERY_TYPE>
    request.EndTime = "<end_time>"
    response, err := client.ShowPlaybookMonitors(request)
    if err == nil {
```

```
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

## Error Codes

See **Error Codes**.

# 4.4.2 Querying Playbook Statistic Data

## Function

This API is used to obtain playbook statistics.

## Calling Method

For details, see **Calling APIs**.

## URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/statistics

**Table 4-335** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

## Request Parameters

**Table 4-336** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-337** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-338** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Error Message<br>Minimum: **1**<br>Maximum: **32** |
| data | **PlaybookStatisticDetail** object | Playbook statistic information. |

**Table 4-339** PlaybookStatisticDetail

| Parameter | Type | Description |
| --- | --- | --- |
| unapproved_num | Integer | Number of unapproved playbooks.<br>Minimum: **0**<br>Maximum: **99999999** |
| disabled_num | Integer | Number of playbooks that are not enabled.<br>Minimum: **0**<br>Maximum: **99999999** |
| enabled_num | Integer | Number of enabled playbooks.<br>Minimum: **0**<br>Maximum: **99999999** |

**Status code: 400**

**Table 4-340** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-341** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "unapproved_num" : 99999999,
    "disabled_num" : 99999999,
    "enabled_num" : 99999999
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowPlaybookStatisticsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPlaybookStatisticsRequest request = new ShowPlaybookStatisticsRequest();
        try {
            ShowPlaybookStatisticsResponse response = client.showPlaybookStatistics(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowPlaybookStatisticsRequest()
        response = client.show_playbook_statistics(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowPlaybookStatisticsRequest{}
    response, err := client.ShowPlaybookStatistics(request)
```

```
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

## Error Codes

See **Error Codes**.

# 4.4.3 Querying the Playbook List

## Function

Querying the Playbook List

## Calling Method

For details, see **Calling APIs**.

## URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks

**Table 4-342** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

**Table 4-343** Query Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| search_txt | No | String | Keyword<br>Minimum: **32**<br>Maximum: **36** |
| enabled | No | Boolean | Whether to enable. |
| offset | Yes | Integer | Indicates the page number. Start position of the query result. The value starts from 0.<br>Minimum: **0**<br>Maximum: **999999**<br>Default: **0** |
| limit | Yes | Integer | The maximum number of records can be returned on each page for a pagination query. The value starts from 1.<br>Minimum: **1**<br>Maximum: **999999** |
| description | No | String | Playbook description.<br>Minimum: **0**<br>Maximum: **64** |
| dataclass_name | No | String | Data class name.<br>Minimum: **0**<br>Maximum: **64** |
| name | No | String | Playbook name.<br>Minimum: **0**<br>Maximum: **64** |

## Request Parameters

**Table 4-344** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-345** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-346** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Response message information<br>Minimum: **1**<br>Maximum: **32** |
| total | Integer | Total records.<br>Minimum: **0**<br>Maximum: **99999** |

| Parameter | Type | Description |
| --- | --- | --- |
| size | Integer | Records on each page.<br>Minimum: **0**<br>Maximum: **9999** |
| page | Integer | Current page.<br>Minimum: **0**<br>Maximum: **100** |
| data | Array of **PlaybookInfo** objects | Playbook list information.<br>Array Length: **0 - 100000000** |

**Table 4-347** PlaybookInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Playbook name.<br>Minimum: **0**<br>Maximum: **1024** |
| description | String | Provides supplementary information about the resource.<br>Minimum: **0**<br>Maximum: **1024** |
| create_time | String | Playbook creation time.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Playbook update time.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| version_id | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |
| enabled | Boolean | Whether to enable. |

| Parameter | Type | Description |
| --- | --- | --- |
| workspace_id | String | Workspace ID<br>Minimum: **32**<br>Maximum: **64** |
| approve_role | String | Reviewer role.<br>Minimum: **0**<br>Maximum: **64** |
| user_role | String | Role<br>Minimum: **0**<br>Maximum: **64** |
| edit_role | String | Edit Role for Account<br>Minimum: **0**<br>Maximum: **64** |
| owner_id | String | ID<br>Minimum: **32**<br>Maximum: **64** |
| version | String | Version No.<br>Minimum: **32**<br>Maximum: **64** |
| dataclass_name | String | Data class name.<br>Minimum: **0**<br>Maximum: **64** |
| dataclass_id | String | Data class ID.<br>Minimum: **1**<br>Maximum: **64** |
| unaudited_version_id | String | ID of the playbook version to be reviewed.<br>Minimum: **1**<br>Maximum: **64** |
| reject_version_id | String | ID of the rejected playbook version.<br>Minimum: **1**<br>Maximum: **64** |

**Status code: 400**

**Table 4-348** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-349** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Response parameters for successful playbook list query.


```
{
  "code" : 0,
  "message" : null,
  "total" : 41,
  "page" : 10,
  "data" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "description" : "This my XXXX",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "enabled" : true,
    "workspace_id" : "string",
    "approve_role" : "approve",
    "user_role" : "string",
    "edit_role" : "editor",
    "owner_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1",
    "dataclass_name" : "string",
    "dataclass_id" : "string",
    "unaudited_version_id" : "string",
    "reject_version_id" : "string"
  } ]
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListPlaybooksSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListPlaybooksRequest request = new ListPlaybooksRequest();
        request.withSearchTxt("<search_txt>");
        request.withEnabled(<enabled>);
        request.withOffset(<offset>);
        request.withLimit(<limit>);
        request.withDescription("<description>");
        request.withDataclassName("<dataclass_name>");
        request.withName("<name>");
        try {
            ListPlaybooksResponse response = client.listPlaybooks(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
```

```
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListPlaybooksRequest()
        request.search_txt = "<search_txt>"
        request.enabled = <Enabled>
        request.offset = <offset>
        request.limit = <limit>
        request.description = "<description>"
        request.dataclass_name = "<dataclass_name>"
        request.name = "<name>"
        response = client.list_playbooks(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListPlaybooksRequest{}
```

```
    searchTxtRequest:= "<search_txt>"
    request.SearchTxt = &searchTxtRequest
    enabledRequest:= <enabled>
    request.Enabled = &enabledRequest
    request.Offset = int32(<offset>)
    request.Limit = int32(<limit>)
    descriptionRequest:= "<description>"
    request.Description = &descriptionRequest
    dataclassNameRequest:= "<dataclass_name>"
    request.DataclassName = &dataclassNameRequest
    nameRequest:= "<name>"
    request.Name = &nameRequest
    response, err := client.ListPlaybooks(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response parameters for successful playbook list query. |
| 400 | Response parameters for failed requests. |

## Error Codes

See **Error Codes**.

# 4.4.4 Creating a Playbook

## Function

Creating a Playbook

## Calling Method

For details, see **Calling APIs**.

## URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks

**Table 4-350** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

## Request Parameters

**Table 4-351** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-352** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| name | Yes | String | Playbook name.<br>Minimum: **0**<br>Maximum: **1024** |
| description | No | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **0**<br>Maximum: **2097152** |
| enabled | No | Boolean | Whether to enable the function. The default value is false. |

## Response Parameters

**Status code: 200**

**Table 4-353** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-354** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Error Message<br>Minimum: **1**<br>Maximum: **32** |
| data | **PlaybookInfo** object | Playbook details. |

**Table 4-355** PlaybookInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook ID.<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| name | String | Playbook name.<br>Minimum: **0**<br>Maximum: **1024** |
| description | String | Provides supplementary information about the resource.<br>Minimum: **0**<br>Maximum: **1024** |
| create_time | String | Playbook creation time.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Playbook update time.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| version_id | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |
| enabled | Boolean | Whether to enable. |
| workspace_id | String | Workspace ID<br>Minimum: **32**<br>Maximum: **64** |
| approve_role | String | Reviewer role.<br>Minimum: **0**<br>Maximum: **64** |
| user_role | String | Role<br>Minimum: **0**<br>Maximum: **64** |
| edit_role | String | Edit Role for Account<br>Minimum: **0**<br>Maximum: **64** |
| owner_id | String | ID<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| version | String | Version No.<br>Minimum: **32**<br>Maximum: **64** |
| dataclass_name | String | Data class name.<br>Minimum: **0**<br>Maximum: **64** |
| dataclass_id | String | Data class ID.<br>Minimum: **1**<br>Maximum: **64** |
| unaudited_version_id | String | ID of the playbook version to be reviewed.<br>Minimum: **1**<br>Maximum: **64** |
| reject_version_id | String | ID of the rejected playbook version.<br>Minimum: **1**<br>Maximum: **64** |

**Status code: 400**

**Table 4-356** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-357** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Create a playbook. Name is MyXXX; workspace ID is string; approver is approve; and status is enabled.

```
{
  "name" : "MyXXX",
  "description" : "This my XXXX",
  "workspace_id" : "string",
  "enabled" : true
}
```

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "description" : "This my XXXX",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "enabled" : true,
    "workspace_id" : "string",
    "approve_role" : "approve",
    "user_role" : "string",
    "edit_role" : "editor",
    "owner_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1",
    "dataclass_name" : "string",
    "dataclass_id" : "string",
    "unaudited_version_id" : "string",
    "reject_version_id" : "string"
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Create a playbook. Name is MyXXX; workspace ID is string; approver is approve; and status is enabled.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class CreatePlaybookSolution {
```

```
    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreatePlaybookRequest request = new CreatePlaybookRequest();
        CreatePlaybookInfo body = new CreatePlaybookInfo();
        body.withEnabled(true);
        body.withWorkspaceId("string");
        body.withDescription("This my XXXX");
        body.withName("MyXXX");
        request.withBody(body);
        try {
            CreatePlaybookResponse response = client.createPlaybook(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Create a playbook. Name is MyXXX; workspace ID is string; approver is approve; and status is enabled.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()
```

```
    try:
        request = CreatePlaybookRequest()
        request.body = CreatePlaybookInfo(
            enabled=True,
            workspace_id="string",
            description="This my XXXX",
            name="MyXXX"
        )
        response = client.create_playbook(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Create a playbook. Name is MyXXX; workspace ID is string; approver is approve; and status is enabled.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreatePlaybookRequest{}
    enabledCreatePlaybookInfo:= true
    descriptionCreatePlaybookInfo:= "This my XXXX"
    request.Body = &model.CreatePlaybookInfo{
        Enabled: &enabledCreatePlaybookInfo,
        WorkspaceId: "string",
        Description: &descriptionCreatePlaybookInfo,
        Name: "MyXXX",
    }
    response, err := client.CreatePlaybook(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

### More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

### Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

### Error Codes

See **Error Codes**.

## 4.4.5 Querying Playbook Details

### Function

Querying Playbook Details

### Calling Method

For details, see **Calling APIs**.

### URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}

**Table 4-358** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| playbook_id | Yes | String | ID of playbook<br>Minimum: **32**<br>Maximum: **64** |

## Request Parameters

**Table 4-359** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-360** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-361** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Error Message<br>Minimum: **1**<br>Maximum: **32** |
| data | **PlaybookInfo** object | Playbook details. |

**Table 4-362** PlaybookInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Playbook name.<br>Minimum: **0**<br>Maximum: **1024** |
| description | String | Provides supplementary information about the resource.<br>Minimum: **0**<br>Maximum: **1024** |
| create_time | String | Playbook creation time.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Playbook update time.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| version_id | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |
| enabled | Boolean | Whether to enable. |
| workspace_id | String | Workspace ID<br>Minimum: **32**<br>Maximum: **64** |
| approve_role | String | Reviewer role.<br>Minimum: **0**<br>Maximum: **64** |
| user_role | String | Role<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| edit_role | String | Edit Role for Account<br>Minimum: **0**<br>Maximum: **64** |
| owner_id | String | ID<br>Minimum: **32**<br>Maximum: **64** |
| version | String | Version No.<br>Minimum: **32**<br>Maximum: **64** |
| dataclass_name | String | Data class name.<br>Minimum: **0**<br>Maximum: **64** |
| dataclass_id | String | Data class ID.<br>Minimum: **1**<br>Maximum: **64** |
| unaudited_version_id | String | ID of the playbook version to be reviewed.<br>Minimum: **1**<br>Maximum: **64** |
| reject_version_id | String | ID of the rejected playbook version.<br>Minimum: **1**<br>Maximum: **64** |

**Status code: 400**

**Table 4-363** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-364** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "description" : "This my XXXX",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "enabled" : true,
    "workspace_id" : "string",
    "approve_role" : "approve",
    "user_role" : "string",
    "edit_role" : "editor",
    "owner_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1",
    "dataclass_name" : "string",
    "dataclass_id" : "string",
    "unaudited_version_id" : "string",
    "reject_version_id" : "string"
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowPlaybookSolution {
```

```
    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPlaybookRequest request = new ShowPlaybookRequest();
        try {
            ShowPlaybookResponse response = client.showPlaybook(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowPlaybookRequest()
        response = client.show_playbook(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
```

```
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowPlaybookRequest{}
    response, err := client.ShowPlaybook(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

## Error Codes

See **Error Codes**.

# 4.4.6 Deleting a Playbook

## Function

Deleting a Playbook

## Calling Method

For details, see **Calling APIs**.

## URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}

**Table 4-365** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| playbook_id | Yes | String | ID of playbook<br>Minimum: **32**<br>Maximum: **64** |

## Request Parameters

**Table 4-366** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-367** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-368** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Error Message<br>Minimum: **1**<br>Maximum: **32** |
| data | **PlaybookInfo** object | Playbook details. |

**Table 4-369** PlaybookInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook ID.<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| name | String | Playbook name.<br>Minimum: **0**<br>Maximum: **1024** |
| description | String | Provides supplementary information about the resource.<br>Minimum: **0**<br>Maximum: **1024** |
| create_time | String | Playbook creation time.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Playbook update time.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| version_id | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |
| enabled | Boolean | Whether to enable. |
| workspace_id | String | Workspace ID<br>Minimum: **32**<br>Maximum: **64** |
| approve_role | String | Reviewer role.<br>Minimum: **0**<br>Maximum: **64** |
| user_role | String | Role<br>Minimum: **0**<br>Maximum: **64** |
| edit_role | String | Edit Role for Account<br>Minimum: **0**<br>Maximum: **64** |
| owner_id | String | ID<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| version | String | Version No.<br>Minimum: **32**<br>Maximum: **64** |
| dataclass_name | String | Data class name.<br>Minimum: **0**<br>Maximum: **64** |
| dataclass_id | String | Data class ID.<br>Minimum: **1**<br>Maximum: **64** |
| unaudited_version_id | String | ID of the playbook version to be reviewed.<br>Minimum: **1**<br>Maximum: **64** |
| reject_version_id | String | ID of the rejected playbook version.<br>Minimum: **1**<br>Maximum: **64** |

**Status code: 400**

**Table 4-370** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-371** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "description" : "This my XXXX",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "enabled" : true,
    "workspace_id" : "string",
    "approve_role" : "approve",
    "user_role" : "string",
    "edit_role" : "editor",
    "owner_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1",
    "dataclass_name" : "string",
    "dataclass_id" : "string",
    "unaudited_version_id" : "string",
    "reject_version_id" : "string"
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class DeletePlaybookSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
```

```
            .withSk(sk);

    SecMasterClient client = SecMasterClient.newBuilder()
            .withCredential(auth)
            .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
            .build();
    DeletePlaybookRequest request = new DeletePlaybookRequest();
    try {
        DeletePlaybookResponse response = client.deletePlaybook(request);
        System.out.println(response.toString());
    } catch (ConnectionException e) {
        e.printStackTrace();
    } catch (RequestTimeoutException e) {
        e.printStackTrace();
    } catch (ServiceResponseException e) {
        e.printStackTrace();
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
  }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeletePlaybookRequest()
        response = client.delete_playbook(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
```

```
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeletePlaybookRequest{}
    response, err := client.DeletePlaybook(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

## Error Codes

See **Error Codes**.

# 4.4.7 Modifying a Playbook

## Function

Modifying a Playbook

## Calling Method

For details, see **Calling APIs**.

## URI

PUT /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}

**Table 4-372** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| playbook_id | Yes | String | Playbook ID.<br>Minimum: **32**<br>Maximum: **64** |

## Request Parameters

**Table 4-373** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-374** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| name | No | String | Playbook name.<br>Minimum: **0**<br>Maximum: **1024** |
| description | No | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |
| enabled | No | Boolean | Whether to enable. |
| active_version_id | No | String | ID of the enabled playbook version.<br>Minimum: **32**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-375** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-376** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Error Message<br>Minimum: **1**<br>Maximum: **32** |
| data | **PlaybookInfo** object | Playbook details. |

**Table 4-377** PlaybookInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Playbook name.<br>Minimum: **0**<br>Maximum: **1024** |
| description | String | Provides supplementary information about the resource.<br>Minimum: **0**<br>Maximum: **1024** |
| create_time | String | Playbook creation time.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Playbook update time.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| version_id | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |
| enabled | Boolean | Whether to enable. |
| workspace_id | String | Workspace ID<br>Minimum: **32**<br>Maximum: **64** |
| approve_role | String | Reviewer role.<br>Minimum: **0**<br>Maximum: **64** |
| user_role | String | Role<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| edit_role | String | Edit Role for Account<br>Minimum: **0**<br>Maximum: **64** |
| owner_id | String | ID<br>Minimum: **32**<br>Maximum: **64** |
| version | String | Version No.<br>Minimum: **32**<br>Maximum: **64** |
| dataclass_name | String | Data class name.<br>Minimum: **0**<br>Maximum: **64** |
| dataclass_id | String | Data class ID.<br>Minimum: **1**<br>Maximum: **64** |
| unaudited_version_id | String | ID of the playbook version to be reviewed.<br>Minimum: **1**<br>Maximum: **64** |
| reject_version_id | String | ID of the rejected playbook version.<br>Minimum: **1**<br>Maximum: **64** |

**Status code: 400**

**Table 4-378** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-379** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Modify a playbook. Name is MyXXX; Description is This my XXXX; Status is Enabled, and playbook ID is active_version_id.

```
{
  "name" : "MyXXX",
  "description" : "This my XXXX",
  "enabled" : true,
  "active_version_id" : "active_version_id"
}
```

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "description" : "This my XXXX",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "enabled" : true,
    "workspace_id" : "string",
    "approve_role" : "approve",
    "user_role" : "string",
    "edit_role" : "editor",
    "owner_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1",
    "dataclass_name" : "string",
    "dataclass_id" : "string",
    "unaudited_version_id" : "string",
    "reject_version_id" : "string"
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Modify a playbook. Name is MyXXX; Description is This my XXXX; Status is Enabled, and playbook ID is active_version_id.

```
package com.huaweicloud.sdk.test;
```

```
import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class UpdatePlaybookSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdatePlaybookRequest request = new UpdatePlaybookRequest();
        ModifyPlaybookInfo body = new ModifyPlaybookInfo();
        body.withActiveVersionId("active_version_id");
        body.withEnabled(true);
        body.withDescription("This my XXXX");
        body.withName("MyXXX");
        request.withBody(body);
        try {
            UpdatePlaybookResponse response = client.updatePlaybook(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Modify a playbook. Name is MyXXX; Description is This my XXXX; Status is Enabled, and playbook ID is active_version_id.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
```

```
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdatePlaybookRequest()
        request.body = ModifyPlaybookInfo(
            active_version_id="active_version_id",
            enabled=True,
            description="This my XXXX",
            name="MyXXX"
        )
        response = client.update_playbook(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Modify a playbook. Name is MyXXX; Description is This my XXXX; Status is Enabled, and playbook ID is active_version_id.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdatePlaybookRequest{}
    activeVersionIdModifyPlaybookInfo:= "active_version_id"
    enabledModifyPlaybookInfo:= true
    descriptionModifyPlaybookInfo:= "This my XXXX"
    nameModifyPlaybookInfo:= "MyXXX"
    request.Body = &model.ModifyPlaybookInfo{
```

```
        ActiveVersionId: &activeVersionIdModifyPlaybookInfo,
        Enabled: &enabledModifyPlaybookInfo,
        Description: &descriptionModifyPlaybookInfo,
        Name: &nameModifyPlaybookInfo,
    }
    response, err := client.UpdatePlaybook(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

### More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

### Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

### Error Codes

See **Error Codes**.

# 4.5 Alert Rule Management

## 4.5.1 Listing Alert Rules

### Function

List alert rules

### Calling Method

For details, see **Calling APIs**.

### URI

GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules

**Table 4-380** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID. Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID. Workspace ID.<br>Minimum: **32**<br>Maximum: **36** |

**Table 4-381** Query Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| offset | Yes | Long | The query offset. Offset.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| limit | Yes | Long | Number of bucket groups Limit.<br>Minimum: **10**<br>Maximum: **50** |
| sort_key | No | String | Sorting field. Sort key<br>Minimum: **1**<br>Maximum: **256** |
| sort_dir | No | String | Sort direction, asc or desc.<br>Enumeration values:<br>• **asc**<br>• **desc** |
| pipe_id | No | String | Pipeline ID.Pipe ID.<br>Minimum: **36**<br>Maximum: **36** |
| rule_name | No | String | Alert rule name.<br>Minimum: **1**<br>Maximum: **256** |
| rule_id | No | String | Alert rule ID.<br>Minimum: **36**<br>Maximum: **36** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| status | No | Array | Status. The options are as follows - Enabled - Disabled<br>Minimum: **1**<br>Maximum: **256**<br>Array Length: **1 - 2**<br>Enumeration values:<br>• **ENABLED**<br>• **DISABLED** |
| severity | No | Array | Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.<br>Array Length: **1 - 5**<br>Enumeration values:<br>• **TIPS**<br>• **LOW**<br>• **MEDIUM**<br>• **HIGH**<br>• **FATAL** |

## Request Parameters

**Table 4-382** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. You can obtain the token by calling the IAM API used to obtain a user token. Token of an IAM user. To obtain it, call the corresponding IAM API.<br>Minimum: **1**<br>Maximum: **2097152** |

## Response Parameters

**Status code: 200**

**Table 4-383** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

**Table 4-384** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| count | Long | Total number. Total count.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| records | Array of **AlertRule** objects | Alert models. Alert rules.<br>Array Length: **0 - 100** |

**Table 4-385** AlertRule

| Parameter | Type | Description |
| --- | --- | --- |
| rule_id | String | Alert rule ID.<br>Minimum: **36**<br>Maximum: **36** |
| pipe_id | String | Pipeline ID.Pipe ID.<br>Minimum: **36**<br>Maximum: **36** |
| pipe_name | String | Data pipeline name.Pipe name.<br>Minimum: **5**<br>Maximum: **63** |
| create_by | String | Created by. Created by.<br>Minimum: **1**<br>Maximum: **255** |
| create_time | Long | Creation time. Create time.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| update_by | String | Updated by. Update by.<br>Minimum: **1**<br>Maximum: **255** |

| Parameter | Type | Description |
| --- | --- | --- |
| update_time | Long | Update time. Update time.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| delete_time | Long | The deletion time. Delete time.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| rule_name | String | Alert rule name.<br>Minimum: **1**<br>Maximum: **255** |
| query | String | Query.<br>Minimum: **1**<br>Maximum: **1024** |
| query_type | String | SQL query syntax. Query type. SQL.<br>Default: **SQL**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **SQL** |
| status | String | Status. The options are as follows - Enabled - Disabled<br>Default: **ENABLED**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **ENABLED**<br>• **DISABLED** |
| severity | String | Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.<br>Default: **TIPS**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **TIPS**<br>• **LOW**<br>• **MEDIUM**<br>• **HIGH**<br>• **FATAL** |

| Parameter | Type | Description |
| --- | --- | --- |
| custom_properties | Map<String,String> | Custom extension information. Custom properties. |
| event_grouping | Boolean | Alert group. Alert group.<br>Default: **true** |
| schedule | **Schedule** object | |
| triggers | Array of **AlertRuleTrigger** objects | Alert triggering rules. Alert triggers.<br>Array Length: **1 - 5** |

**Table 4-386** Schedule

| Parameter | Type | Description |
| --- | --- | --- |
| frequency_interval | Integer | Scheduling interval. Frequency interval.<br>Minimum: **1**<br>Maximum: **60** |
| frequency_unit | String | The unit of the scheduling interval. The value can be minute, hour, or day. Frequency unit. MINUTE, HOUR, DAY.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **MINUTE**<br>• **HOUR**<br>• **DAY** |
| period_interval | Integer | Time window interval. Period interval.<br>Minimum: **1**<br>Maximum: **60** |
| period_unit | String | Time Window unit. The value can be minute, hour, or day. Period unit. MINUTE, HOUR, DAY.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **MINUTE**<br>• **HOUR**<br>• **DAY** |

| Parameter | Type | Description |
| --- | --- | --- |
| delay_interval | Integer | The delay interval. Delay interval<br>Minimum: **0**<br>Maximum: **10**<br>Default: **0** |
| overtime_interval | Integer | Timeout interval. Overtime interval<br>Minimum: **0**<br>Maximum: **10**<br>Default: **10** |

**Table 4-387** AlertRuleTrigger

| Parameter | Type | Description |
| --- | --- | --- |
| mode | String | Number of modes. Mode. COUNT.<br>Default: **COUNT**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **COUNT** |
| operator | String | Operator, which can be equal to, not equal to, greater than, or less than. operator. EQ equal, NE not equal, GT greater than, LT less than.<br>Default: **GT**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **EQ**<br>• **NE**<br>• **GT**<br>• **LT** |
| expression | String | expression<br>Minimum: **1**<br>Maximum: **255** |

| Parameter | Type | Description |
| --- | --- | --- |
| severity | String | Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **TIPS**<br>• **LOW**<br>• **MEDIUM**<br>• **HIGH**<br>• **FATAL** |
| accumulated_times | Integer | accumulated_times<br>Minimum: **1**<br>Maximum: **1000**<br>Default: **1** |

**Status code: 400**

**Table 4-388** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

## Example Requests

None

## Example Responses

**Status code: 200**

Success


```
{
  "count" : 9223372036854776000,
  "records" : [ {
    "rule_id" : "443a0117-1aa4-4595-ad4a-796fad4d4950",
    "pipe_id" : "772fb35b-83bc-46c9-a0b1-ebe31070a889",
    "create_by" : "582dd19dd99d4505a1d7929dc943b169",
    "create_time" : 1665221214,
    "update_by" : "582dd19dd99d4505a1d7929dc943b169",
    "update_time" : 1665221214,
    "delete_time" : 0,
    "rule_name" : "Alert rule",
    "query" : "* | select status, count(*) as count group by status",
```

```
    "query_type" : "SQL",
    "status" : "ENABLED",
    "severity" : "TIPS",
    "custom_properties" : {
      "references" : "https://localhost/references",
      "maintainer" : "isap"
    },
    "event_grouping" : true,
    "schedule" : {
      "frequency_interval" : 5,
      "frequency_unit" : "MINUTE",
      "period_interval" : 5,
      "period_unit" : "MINUTE",
      "delay_interval" : 2,
      "overtime_interval" : 10
    },
    "triggers" : [ {
      "mode" : "COUNT",
      "operator" : "GT",
      "expression" : 10,
      "severity" : "TIPS"
    } ]
  } ]
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class ListAlertRulesSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListAlertRulesRequest request = new ListAlertRulesRequest();
        request.withOffset(<offset>L);
        request.withLimit(<limit>L);
        request.withSortKey("<sort_key>");
```

```
        request.withSortDir(ListAlertRulesRequest.SortDirEnum.fromValue("<sort_dir>"));
        request.withPipeId("<pipe_id>");
        request.withRuleName("<rule_name>");
        request.withRuleId("<rule_id>");
        request.withStatus();
        request.withSeverity();
        try {
            ListAlertRulesResponse response = client.listAlertRules(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListAlertRulesRequest()
        request.offset = <offset>
        request.limit = <limit>
        request.sort_key = "<sort_key>"
        request.sort_dir = "<sort_dir>"
        request.pipe_id = "<pipe_id>"
        request.rule_name = "<rule_name>"
        request.rule_id = "<rule_id>"
        request.status =
        request.severity =
        response = client.list_alert_rules(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListAlertRulesRequest{}
    request.Offset = int64(<offset>)
    request.Limit = int64(<limit>)
    sortKeyRequest:= "<sort_key>"
    request.SortKey = &sortKeyRequest
    sortDirRequest:= model.GetListAlertRulesRequestSortDirEnum().<SORT_DIR>
    request.SortDir = &sortDirRequest
    pipeIdRequest:= "<pipe_id>"
    request.PipeId = &pipeIdRequest
    ruleNameRequest:= "<rule_name>"
    request.RuleName = &ruleNameRequest
    ruleIdRequest:= "<rule_id>"
    request.RuleId = &ruleIdRequest
    response, err := client.ListAlertRules(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Success |

| Status Code | Description |
| --- | --- |
| 400 | Bad Request |

### Error Codes

See **Error Codes**.

## 4.5.2 Creating an Alert Rule

### Function

Create alert rule

### Calling Method

For details, see **Calling APIs**.

### URI

POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules

**Table 4-389** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID. Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID. Workspace ID.<br>Minimum: **32**<br>Maximum: **36** |

## Request Parameters

**Table 4-390** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. You can obtain the token by calling the IAM API used to obtain a user token. Token of an IAM user. To obtain it, call the corresponding IAM API.<br>Minimum: **1**<br>Maximum: **2097152** |

**Table 4-391** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| pipe_id | Yes | String | Pipeline ID.Pipe ID.<br>Minimum: **36**<br>Maximum: **36** |
| rule_name | Yes | String | Alert rule name. Alert rule name.<br>Minimum: **1**<br>Maximum: **255** |
| description | No | String | Link description.Description.<br>Minimum: **0**<br>Maximum: **1024** |
| query | Yes | String | Query statement. Query.<br>Minimum: **1**<br>Maximum: **1024** |
| query_type | No | String | SQL query syntax. Query type. SQL.<br>Default: **SQL**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **SQL** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| status | No | String | Status. The options are as follows - Enabled - Disabled<br>Default: **ENABLED**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **ENABLED**<br>• **DISABLED** |
| severity | No | String | Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.<br>Default: **TIPS**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **TIPS**<br>• **LOW**<br>• **MEDIUM**<br>• **HIGH**<br>• **FATAL** |
| custom_properties | No | Map<String,String> | Custom extension information. Custom properties. |
| alert_type | No | Map<String,String> | Alert type. Alert type. |
| event_grouping | No | Boolean | Alert group. Alert group.<br>Default: **true** |
| suspression | No | Boolean | Alert containment. Suppression.<br>Default: **true** |
| simulation | No | Boolean | Simulated alerts. Simulation.<br>Default: **true** |
| schedule | Yes | **Schedule** object | |
| triggers | Yes | Array of **AlertRuleTrigger** objects | Alert triggering rules. Alert triggers.<br>Array Length: **1 - 5** |

**Table 4-392** Schedule

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| frequency_interval | Yes | Integer | Scheduling interval. Frequency interval.<br>Minimum: **1**<br>Maximum: **60** |
| frequency_unit | Yes | String | The unit of the scheduling interval. The value can be minute, hour, or day. Frequency unit. MINUTE, HOUR, DAY.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **MINUTE**<br>• **HOUR**<br>• **DAY** |
| period_interval | Yes | Integer | Time window interval. Period interval.<br>Minimum: **1**<br>Maximum: **60** |
| period_unit | Yes | String | Time Window unit. The value can be minute, hour, or day. Period unit. MINUTE, HOUR, DAY.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **MINUTE**<br>• **HOUR**<br>• **DAY** |
| delay_interval | No | Integer | The delay interval. Delay interval<br>Minimum: **0**<br>Maximum: **10**<br>Default: **0** |
| overtime_interval | No | Integer | Timeout interval. Overtime interval<br>Minimum: **0**<br>Maximum: **10**<br>Default: **10** |

**Table 4-393** AlertRuleTrigger

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| mode | No | String | Number of modes. Mode. COUNT.<br>Default: **COUNT**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **COUNT** |
| operator | No | String | Operator, which can be equal to, not equal to, greater than, or less than. operator. EQ equal, NE not equal, GT greater than, LT less than.<br>Default: **GT**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **EQ**<br>• **NE**<br>• **GT**<br>• **LT** |
| expression | Yes | String | expression<br>Minimum: **1**<br>Maximum: **255** |
| severity | No | String | Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **TIPS**<br>• **LOW**<br>• **MEDIUM**<br>• **HIGH**<br>• **FATAL** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| accumulated_times | No | Integer | accumulated_times<br>Minimum: **1**<br>Maximum: **1000**<br>Default: **1** |

## Response Parameters

**Status code: 200**

**Table 4-394** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

**Table 4-395** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| rule_id | String | Alert rule ID.<br>Minimum: **36**<br>Maximum: **36** |
| pipe_id | String | Pipeline ID.Pipe ID.<br>Minimum: **36**<br>Maximum: **36** |
| pipe_name | String | Data pipeline name.Pipe name.<br>Minimum: **5**<br>Maximum: **63** |
| create_by | String | Created by. Created by.<br>Minimum: **1**<br>Maximum: **255** |
| create_time | Long | Creation time. Create time.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| update_by | String | Updated by. Update by.<br>Minimum: **1**<br>Maximum: **255** |

| Parameter | Type | Description |
| --- | --- | --- |
| update_time | Long | Update time. Update time.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| delete_time | Long | The deletion time. Delete time.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| rule_name | String | Alert rule name.<br>Minimum: **1**<br>Maximum: **255** |
| query | String | Query.<br>Minimum: **1**<br>Maximum: **1024** |
| query_type | String | SQL query syntax. Query type. SQL.<br>Default: **SQL**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **SQL** |
| status | String | Status. The options are as follows - Enabled - Disabled<br>Default: **ENABLED**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **ENABLED**<br>• **DISABLED** |
| severity | String | Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.<br>Default: **TIPS**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **TIPS**<br>• **LOW**<br>• **MEDIUM**<br>• **HIGH**<br>• **FATAL** |

| Parameter | Type | Description |
| --- | --- | --- |
| custom_properties | Map<String,String> | Custom extension information. Custom properties. |
| event_grouping | Boolean | Alert group. Alert group.<br>Default: **true** |
| schedule | **Schedule** object | |
| triggers | Array of **AlertRuleTrigger** objects | Alert triggering rules. Alert triggers.<br>Array Length: **1 - 5** |

**Table 4-396** Schedule

| Parameter | Type | Description |
| --- | --- | --- |
| frequency_interval | Integer | Scheduling interval. Frequency interval.<br>Minimum: **1**<br>Maximum: **60** |
| frequency_unit | String | The unit of the scheduling interval. The value can be minute, hour, or day. Frequency unit. MINUTE, HOUR, DAY.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **MINUTE**<br>• **HOUR**<br>• **DAY** |
| period_interval | Integer | Time window interval. Period interval.<br>Minimum: **1**<br>Maximum: **60** |
| period_unit | String | Time Window unit. The value can be minute, hour, or day. Period unit. MINUTE, HOUR, DAY.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **MINUTE**<br>• **HOUR**<br>• **DAY** |

| Parameter | Type | Description |
| --- | --- | --- |
| delay_interval | Integer | The delay interval. Delay interval<br>Minimum: **0**<br>Maximum: **10**<br>Default: **0** |
| overtime_interval | Integer | Timeout interval. Overtime interval<br>Minimum: **0**<br>Maximum: **10**<br>Default: **10** |

**Table 4-397** AlertRuleTrigger

| Parameter | Type | Description |
| --- | --- | --- |
| mode | String | Number of modes. Mode. COUNT.<br>Default: **COUNT**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **COUNT** |
| operator | String | Operator, which can be equal to, not equal to, greater than, or less than. operator. EQ equal, NE not equal, GT greater than, LT less than.<br>Default: **GT**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **EQ**<br>• **NE**<br>• **GT**<br>• **LT** |
| expression | String | expression<br>Minimum: **1**<br>Maximum: **255** |

| Parameter | Type | Description |
| --- | --- | --- |
| severity | String | Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **TIPS**<br>• **LOW**<br>• **MEDIUM**<br>• **HIGH**<br>• **FATAL** |
| accumulated_times | Integer | accumulated_times<br>Minimum: **1**<br>Maximum: **1000**<br>Default: **1** |

**Status code: 400**

**Table 4-398** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

## Example Requests

Create an alarm rule whose ID is 772fb35b-83bc-46c9-a0b1-ebe31070a889, Name is Alert rule, Query type is SQL, and Status is Enabled.D331

```
{
  "pipe_id" : "772fb35b-83bc-46c9-a0b1-ebe31070a889",
  "rule_name" : "Alert rule",
  "description" : "An alert rule",
  "query" : "* | select status, count(*) as count group by status",
  "query_type" : "SQL",
  "status" : "ENABLED",
  "severity" : "TIPS",
  "custom_properties" : {
    "references" : "https://localhost/references",
    "maintainer" : "isap"
  },
  "event_grouping" : true,
  "suspression" : true,
  "schedule" : {
    "frequency_interval" : 5,
    "frequency_unit" : "MINUTE",
    "period_interval" : 5,
```

```
    "period_unit" : "MINUTE",
    "delay_interval" : 2,
    "overtime_interval" : 10
  },
  "triggers" : [ {
    "mode" : "COUNT",
    "operator" : "GT",
    "expression" : 10,
    "severity" : "TIPS"
  } ]
}
```

## Example Responses

**Status code: 200**

Success

```
{
  "rule_id" : "443a0117-1aa4-4595-ad4a-796fad4d4950",
  "pipe_id" : "772fb35b-83bc-46c9-a0b1-ebe31070a889",
  "create_by" : "582dd19dd99d4505a1d7929dc943b169",
  "create_time" : 1665221214,
  "update_by" : "582dd19dd99d4505a1d7929dc943b169",
  "update_time" : 1665221214,
  "delete_time" : 0,
  "rule_name" : "Alert rule",
  "query" : "* | select status, count(*) as count group by status",
  "query_type" : "SQL",
  "status" : "ENABLED",
  "severity" : "TIPS",
  "custom_properties" : {
    "references" : "https://localhost/references",
    "maintainer" : "isap"
  },
  "event_grouping" : true,
  "schedule" : {
    "frequency_interval" : 5,
    "frequency_unit" : "MINUTE",
    "period_interval" : 5,
    "period_unit" : "MINUTE",
    "delay_interval" : 2,
    "overtime_interval" : 10
  },
  "triggers" : [ {
    "mode" : "COUNT",
    "operator" : "GT",
    "expression" : 10,
    "severity" : "TIPS"
  } ]
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Create an alarm rule whose ID is 772fb35b-83bc-46c9-a0b1-ebe31070a889, Name is Alert rule, Query type is SQL, and Status is Enabled.D331

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
```

```
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;
import java.util.Map;
import java.util.HashMap;

public class CreateAlertRuleSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateAlertRuleRequest request = new CreateAlertRuleRequest();
        CreateAlertRuleRequestBody body = new CreateAlertRuleRequestBody();
        List<AlertRuleTrigger> listbodyTriggers = new ArrayList<>();
        listbodyTriggers.add(
            new AlertRuleTrigger()
                .withMode(AlertRuleTrigger.ModeEnum.fromValue("COUNT"))
                .withOperator(AlertRuleTrigger.OperatorEnum.fromValue("GT"))
                .withExpression("10")
                .withSeverity(AlertRuleTrigger.SeverityEnum.fromValue("TIPS"))
        );
        Schedule schedulebody = new Schedule();
        schedulebody.withFrequencyInterval(5)
            .withFrequencyUnit(Schedule.FrequencyUnitEnum.fromValue("MINUTE"))
            .withPeriodInterval(5)
            .withPeriodUnit(Schedule.PeriodUnitEnum.fromValue("MINUTE"))
            .withDelayInterval(2)
            .withOvertimeInterval(10);
        Map<String, String> listbodyCustomProperties = new HashMap<>();
        listbodyCustomProperties.put("references", "https://localhost/references");
        listbodyCustomProperties.put("maintainer", "isap");
        body.withTriggers(listbodyTriggers);
        body.withSchedule(schedulebody);
        body.withSuspression(true);
        body.withEventGrouping(true);
        body.withCustomProperties(listbodyCustomProperties);
        body.withSeverity(CreateAlertRuleRequestBody.SeverityEnum.fromValue("TIPS"));
        body.withStatus(CreateAlertRuleRequestBody.StatusEnum.fromValue("ENABLED"));
        body.withQueryType(CreateAlertRuleRequestBody.QueryTypeEnum.fromValue("SQL"));
        body.withQuery("* | select status, count(*) as count group by status");
        body.withDescription("An alert rule");
        body.withRuleName("Alert rule");
        body.withPipeId("772fb35b-83bc-46c9-a0b1-ebe31070a889");
        request.withBody(body);
        try {
            CreateAlertRuleResponse response = client.createAlertRule(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
```

```
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Create an alarm rule whose ID is 772fb35b-83bc-46c9-a0b1-ebe31070a889, Name is Alert rule, Query type is SQL, and Status is Enabled.D331

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateAlertRuleRequest()
        listTriggersbody = [
            AlertRuleTrigger(
                mode="COUNT",
                operator="GT",
                expression="10",
                severity="TIPS"
            )
        ]
        schedulebody = Schedule(
            frequency_interval=5,
            frequency_unit="MINUTE",
            period_interval=5,
            period_unit="MINUTE",
            delay_interval=2,
            overtime_interval=10
        )
        listCustomPropertiesbody = {
            "references": "https://localhost/references",
            "maintainer": "isap"
        }
        request.body = CreateAlertRuleRequestBody(
            triggers=listTriggersbody,
            schedule=schedulebody,
            suspression=True,
            event_grouping=True,
            custom_properties=listCustomPropertiesbody,
            severity="TIPS",
            status="ENABLED",
```

```
        query_type="SQL",
        query="* | select status, count(*) as count group by status",
        description="An alert rule",
        rule_name="Alert rule",
        pipe_id="772fb35b-83bc-46c9-a0b1-ebe31070a889"
    )
    response = client.create_alert_rule(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

Create an alarm rule whose ID is 772fb35b-83bc-46c9-a0b1-ebe31070a889, Name is Alert rule, Query type is SQL, and Status is Enabled.D331

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateAlertRuleRequest{}
    modeTriggers:= model.GetAlertRuleTriggerModeEnum().COUNT
    operatorTriggers:= model.GetAlertRuleTriggerOperatorEnum().GT
    severityTriggers:= model.GetAlertRuleTriggerSeverityEnum().TIPS
    var listTriggersbody = []model.AlertRuleTrigger{
        {
            Mode: &modeTriggers,
            Operator: &operatorTriggers,
            Expression: "10",
            Severity: &severityTriggers,
        },
    }
    delayIntervalSchedule:= int32(2)
    overtimeIntervalSchedule:= int32(10)
    schedulebody := &model.Schedule{
        FrequencyInterval: int32(5),
        FrequencyUnit: model.GetScheduleFrequencyUnitEnum().MINUTE,
        PeriodInterval: int32(5),
        PeriodUnit: model.GetSchedulePeriodUnitEnum().MINUTE,
        DelayInterval: &delayIntervalSchedule,
```

```
        OvertimeInterval: &overtimeIntervalSchedule,
    }
    var listCustomPropertiesbody = map[string]string{
        "references": "https://localhost/references",
        "maintainer": "isap",
    }
    suspressionCreateAlertRuleRequestBody:= true
    eventGroupingCreateAlertRuleRequestBody:= true
    severityCreateAlertRuleRequestBody:= model.GetCreateAlertRuleRequestBodySeverityEnum().TIPS
    statusCreateAlertRuleRequestBody:= model.GetCreateAlertRuleRequestBodyStatusEnum().ENABLED
    queryTypeCreateAlertRuleRequestBody:= model.GetCreateAlertRuleRequestBodyQueryTypeEnum().SQL
    descriptionCreateAlertRuleRequestBody:= "An alert rule"
    request.Body = &model.CreateAlertRuleRequestBody{
        Triggers: listTriggersbody,
        Schedule: schedulebody,
        Suspression: &suspressionCreateAlertRuleRequestBody,
        EventGrouping: &eventGroupingCreateAlertRuleRequestBody,
        CustomProperties: listCustomPropertiesbody,
        Severity: &severityCreateAlertRuleRequestBody,
        Status: &statusCreateAlertRuleRequestBody,
        QueryType: &queryTypeCreateAlertRuleRequestBody,
        Query: "* | select status, count(*) as count group by status",
        Description: &descriptionCreateAlertRuleRequestBody,
        RuleName: "Alert rule",
        PipeId: "772fb35b-83bc-46c9-a0b1-ebe31070a889",
    }
    response, err := client.CreateAlertRule(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Success |
| 400 | Bad Request |

## Error Codes

See **Error Codes**.

# 4.5.3 Deleting an Alert Rule

## Function

Delete alert rule

## Calling Method

For details, see **Calling APIs**.

## URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules

**Table 4-399** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID. Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID. Workspace ID.<br>Minimum: **32**<br>Maximum: **36** |

## Request Parameters

**Table 4-400** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. You can obtain the token by calling the IAM API used to obtain a user token. Token of an IAM user. To obtain it, call the corresponding IAM API.<br>Minimum: **1**<br>Maximum: **2097152** |

**Table 4-401** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| [items] | Yes | Array of strings | Array of Alert rule ID |

## Response Parameters

**Status code: 200**

**Table 4-402** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

**Table 4-403** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| rule_id | String | Alert rule ID.<br>Minimum: **36**<br>Maximum: **36** |
| delete_time | Long | The deletion time. Delete time.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |

**Status code: 400**

**Table 4-404** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

## Example Requests

This API is used to delete an alert role. The request body is Array of Alert rule ID.

```
[ "612b7f41-da89-495b-a6a1-fdf14e4cc794" ]
```

## Example Responses

**Status code: 200**

Success

```
{
  "rule_id" : "443a0117-1aa4-4595-ad4a-796fad4d4950",
  "delete_time" : 1665221214
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

This API is used to delete an alert role. The request body is Array of Alert rule ID.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class DeleteAlertRuleSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteAlertRuleRequest request = new DeleteAlertRuleRequest();
        List<String> listbodyBody = new ArrayList<>();
        listbodyBody.add("612b7f41-da89-495b-a6a1-fdf14e4cc794");
        request.withBody(listbodyBody);
        try {
            DeleteAlertRuleResponse response = client.deleteAlertRule(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

This API is used to delete an alert role. The request body is Array of Alert rule ID.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *
```

```
if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteAlertRuleRequest()
        listBodybody = [
            "612b7f41-da89-495b-a6a1-fdf14e4cc794"
        ]
        request.body = listBodybody
        response = client.delete_alert_rule(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

This API is used to delete an alert role. The request body is Array of Alert rule ID.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteAlertRuleRequest{}
    var listBodybody = []string{
        "612b7f41-da89-495b-a6a1-fdf14e4cc794",
    }
```

```
    request.Body = &listBodybody
    response, err := client.DeleteAlertRule(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Success |
| 400 | Bad Request |

## Error Codes

See **Error Codes**.

# 4.5.4 Querying an Alert Rule

## Function

Querying an Alert Rule

## Calling Method

For details, see **Calling APIs**.

## URI

GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/{rule_id}

**Table 4-405** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID. Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID. Workspace ID.<br>Minimum: **32**<br>Maximum: **36** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| rule_id | Yes | String | Alert rule ID.<br>Minimum: **36**<br>Maximum: **36** |

## Request Parameters

**Table 4-406** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. You can obtain the token by calling the IAM API used to obtain a user token. Token of an IAM user. To obtain it, call the corresponding IAM API.<br>Minimum: **1**<br>Maximum: **2097152** |

## Response Parameters

**Status code: 200**

**Table 4-407** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

**Table 4-408** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| rule_id | String | Alert rule ID.<br>Minimum: **36**<br>Maximum: **36** |
| pipe_id | String | Pipeline ID.Pipe ID.<br>Minimum: **36**<br>Maximum: **36** |

| Parameter | Type | Description |
| --- | --- | --- |
| pipe_name | String | Data pipeline name.Pipe name.<br>Minimum: **5**<br>Maximum: **63** |
| create_by | String | Created by. Created by.<br>Minimum: **1**<br>Maximum: **255** |
| create_time | Long | Creation time. Create time.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| update_by | String | Updated by. Update by.<br>Minimum: **1**<br>Maximum: **255** |
| update_time | Long | Update time. Update time.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| delete_time | Long | The deletion time. Delete time.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| rule_name | String | Alert rule name.<br>Minimum: **1**<br>Maximum: **255** |
| query | String | Query.<br>Minimum: **1**<br>Maximum: **1024** |
| query_type | String | SQL query syntax. Query type. SQL.<br>Default: **SQL**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **SQL** |

| Parameter | Type | Description |
| --- | --- | --- |
| status | String | Status. The options are as follows - Enabled - Disabled<br>Default: **ENABLED**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **ENABLED**<br>• **DISABLED** |
| severity | String | Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.<br>Default: **TIPS**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **TIPS**<br>• **LOW**<br>• **MEDIUM**<br>• **HIGH**<br>• **FATAL** |
| custom_properties | Map<String,String> | Custom extension information. Custom properties. |
| event_grouping | Boolean | Alert group. Alert group.<br>Default: **true** |
| schedule | **Schedule** object | |
| triggers | Array of **AlertRuleTrigger** objects | Alert triggering rules. Alert triggers.<br>Array Length: **1 - 5** |

**Table 4-409** Schedule

| Parameter | Type | Description |
| --- | --- | --- |
| frequency_interval | Integer | Scheduling interval. Frequency interval.<br>Minimum: **1**<br>Maximum: **60** |

| Parameter | Type | Description |
| --- | --- | --- |
| frequency_unit | String | The unit of the scheduling interval. The value can be minute, hour, or day. Frequency unit. MINUTE, HOUR, DAY.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **MINUTE**<br>• **HOUR**<br>• **DAY** |
| period_interval | Integer | Time window interval. Period interval.<br>Minimum: **1**<br>Maximum: **60** |
| period_unit | String | Time Window unit. The value can be minute, hour, or day. Period unit. MINUTE, HOUR, DAY.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **MINUTE**<br>• **HOUR**<br>• **DAY** |
| delay_interval | Integer | The delay interval. Delay interval<br>Minimum: **0**<br>Maximum: **10**<br>Default: **0** |
| overtime_interval | Integer | Timeout interval. Overtime interval<br>Minimum: **0**<br>Maximum: **10**<br>Default: **10** |

**Table 4-410** AlertRuleTrigger

| Parameter | Type | Description |
| --- | --- | --- |
| mode | String | Number of modes. Mode. COUNT.<br>Default: **COUNT**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **COUNT** |
| operator | String | Operator, which can be equal to, not equal to, greater than, or less than. operator. EQ equal, NE not equal, GT greater than, LT less than.<br>Default: **GT**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **EQ**<br>• **NE**<br>• **GT**<br>• **LT** |
| expression | String | expression<br>Minimum: **1**<br>Maximum: **255** |
| severity | String | Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **TIPS**<br>• **LOW**<br>• **MEDIUM**<br>• **HIGH**<br>• **FATAL** |
| accumulated_times | Integer | accumulated_times<br>Minimum: **1**<br>Maximum: **1000**<br>Default: **1** |

**Status code: 400**

**Table 4-411** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

## Example Requests

None

## Example Responses

**Status code: 200**

Success

```
{
  "rule_id" : "443a0117-1aa4-4595-ad4a-796fad4d4950",
  "pipe_id" : "772fb35b-83bc-46c9-a0b1-ebe31070a889",
  "create_by" : "582dd19dd99d4505a1d7929dc943b169",
  "create_time" : 1665221214,
  "update_by" : "582dd19dd99d4505a1d7929dc943b169",
  "update_time" : 1665221214,
  "delete_time" : 0,
  "rule_name" : "Alert rule",
  "query" : "* | select status, count(*) as count group by status",
  "query_type" : "SQL",
  "status" : "ENABLED",
  "severity" : "TIPS",
  "custom_properties" : {
    "references" : "https://localhost/references",
    "maintainer" : "isap"
  },
  "event_grouping" : true,
  "schedule" : {
    "frequency_interval" : 5,
    "frequency_unit" : "MINUTE",
    "period_interval" : 5,
    "period_unit" : "MINUTE",
    "delay_interval" : 2,
    "overtime_interval" : 10
  },
  "triggers" : [ {
    "mode" : "COUNT",
    "operator" : "GT",
    "expression" : 10,
    "severity" : "TIPS"
  } ]
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
```

```
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowAlertRuleSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowAlertRuleRequest request = new ShowAlertRuleRequest();
        try {
            ShowAlertRuleResponse response = client.showAlertRule(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()
```

```
    try:
        request = ShowAlertRuleRequest()
        response = client.show_alert_rule(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowAlertRuleRequest{}
    response, err := client.ShowAlertRule(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Success |
| 400 | Bad Request |

### Error Codes

See **Error Codes**.

## 4.5.5 Updating an Alert Rule

### Function

Update alert rule

### Calling Method

For details, see **Calling APIs**.

### URI

PUT /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/{rule_id}

**Table 4-412** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID. Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID. Workspace ID.<br>Minimum: **32**<br>Maximum: **36** |
| rule_id | Yes | String | Alert rule ID.<br>Minimum: **36**<br>Maximum: **36** |

## Request Parameters

**Table 4-413** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. You can obtain the token by calling the IAM API used to obtain a user token. Token of an IAM user. To obtain it, call the corresponding IAM API.<br>Minimum: **1**<br>Maximum: **2097152** |

**Table 4-414** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| rule_name | No | String | Alert rule name.<br>Minimum: **1**<br>Maximum: **255** |
| description | No | String | Description.Description.<br>Minimum: **0**<br>Maximum: **1024** |
| query | No | String | Query.<br>Minimum: **1**<br>Maximum: **1024** |
| query_type | No | String | SQL query syntax. Query type. SQL.<br>Default: **SQL**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **SQL** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| status | No | String | Status. The options are as follows - Enabled - Disabled<br>Default: **ENABLED**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **ENABLED**<br>• **DISABLED** |
| severity | No | String | Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.<br>Default: **TIPS**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **TIPS**<br>• **LOW**<br>• **MEDIUM**<br>• **HIGH**<br>• **FATAL** |
| custom_properties | No | Map<String,String> | Custom extension information. Custom properties. |
| alert_type | No | Map<String,String> | Alert type. Alert type. |
| event_grouping | No | Boolean | Alert group. Alert group.<br>Default: **true** |
| suppression | No | Boolean | Alert containment. Suppression<br>Default: **true** |
| simulation | No | Boolean | Simulated alerts. Simulation.<br>Default: **true** |
| schedule | No | **Schedule** object | |
| triggers | No | Array of **AlertRuleTrigger** objects | Alert triggering rules. Alert triggers.<br>Array Length: **1 - 5** |

**Table 4-415** Schedule

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| frequency_interval | Yes | Integer | Scheduling interval. Frequency interval.<br>Minimum: **1**<br>Maximum: **60** |
| frequency_unit | Yes | String | The unit of the scheduling interval. The value can be minute, hour, or day. Frequency unit. MINUTE, HOUR, DAY.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **MINUTE**<br>• **HOUR**<br>• **DAY** |
| period_interval | Yes | Integer | Time window interval. Period interval.<br>Minimum: **1**<br>Maximum: **60** |
| period_unit | Yes | String | Time Window unit. The value can be minute, hour, or day. Period unit. MINUTE, HOUR, DAY.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **MINUTE**<br>• **HOUR**<br>• **DAY** |
| delay_interval | No | Integer | The delay interval. Delay interval<br>Minimum: **0**<br>Maximum: **10**<br>Default: **0** |
| overtime_interval | No | Integer | Timeout interval. Overtime interval<br>Minimum: **0**<br>Maximum: **10**<br>Default: **10** |

**Table 4-416** AlertRuleTrigger

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| mode | No | String | Number of modes. Mode. COUNT.<br>Default: **COUNT**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **COUNT** |
| operator | No | String | Operator, which can be equal to, not equal to, greater than, or less than. operator. EQ equal, NE not equal, GT greater than, LT less than.<br>Default: **GT**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **EQ**<br>• **NE**<br>• **GT**<br>• **LT** |
| expression | Yes | String | expression<br>Minimum: **1**<br>Maximum: **255** |
| severity | No | String | Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **TIPS**<br>• **LOW**<br>• **MEDIUM**<br>• **HIGH**<br>• **FATAL** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| accumulated_times | No | Integer | accumulated_times<br>Minimum: **1**<br>Maximum: **1000**<br>Default: **1** |

## Response Parameters

**Status code: 200**

**Table 4-417** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

**Table 4-418** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| rule_id | String | Alert rule ID.<br>Minimum: **36**<br>Maximum: **36** |
| pipe_id | String | Pipeline ID.Pipe ID.<br>Minimum: **36**<br>Maximum: **36** |
| pipe_name | String | Data pipeline name.Pipe name.<br>Minimum: **5**<br>Maximum: **63** |
| create_by | String | Created by. Created by.<br>Minimum: **1**<br>Maximum: **255** |
| create_time | Long | Creation time. Create time.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| update_by | String | Updated by. Update by.<br>Minimum: **1**<br>Maximum: **255** |

| Parameter | Type | Description |
| --- | --- | --- |
| update_time | Long | Update time. Update time.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| delete_time | Long | The deletion time. Delete time.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| rule_name | String | Alert rule name.<br>Minimum: **1**<br>Maximum: **255** |
| query | String | Query.<br>Minimum: **1**<br>Maximum: **1024** |
| query_type | String | SQL query syntax. Query type. SQL.<br>Default: **SQL**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **SQL** |
| status | String | Status. The options are as follows - Enabled - Disabled<br>Default: **ENABLED**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **ENABLED**<br>• **DISABLED** |
| severity | String | Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.<br>Default: **TIPS**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **TIPS**<br>• **LOW**<br>• **MEDIUM**<br>• **HIGH**<br>• **FATAL** |

| Parameter | Type | Description |
| --- | --- | --- |
| custom_properties | Map<String,String> | Custom extension information. Custom properties. |
| event_grouping | Boolean | Alert group. Alert group.<br>Default: **true** |
| schedule | **Schedule** object | |
| triggers | Array of **AlertRuleTrigger** objects | Alert triggering rules. Alert triggers.<br>Array Length: **1 - 5** |

**Table 4-419** Schedule

| Parameter | Type | Description |
| --- | --- | --- |
| frequency_interval | Integer | Scheduling interval. Frequency interval.<br>Minimum: **1**<br>Maximum: **60** |
| frequency_unit | String | The unit of the scheduling interval. The value can be minute, hour, or day. Frequency unit. MINUTE, HOUR, DAY.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **MINUTE**<br>• **HOUR**<br>• **DAY** |
| period_interval | Integer | Time window interval. Period interval.<br>Minimum: **1**<br>Maximum: **60** |
| period_unit | String | Time Window unit. The value can be minute, hour, or day. Period unit. MINUTE, HOUR, DAY.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **MINUTE**<br>• **HOUR**<br>• **DAY** |

| Parameter | Type | Description |
| --- | --- | --- |
| delay_interval | Integer | The delay interval. Delay interval<br>Minimum: **0**<br>Maximum: **10**<br>Default: **0** |
| overtime_interval | Integer | Timeout interval. Overtime interval<br>Minimum: **0**<br>Maximum: **10**<br>Default: **10** |

**Table 4-420** AlertRuleTrigger

| Parameter | Type | Description |
| --- | --- | --- |
| mode | String | Number of modes. Mode. COUNT.<br>Default: **COUNT**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **COUNT** |
| operator | String | Operator, which can be equal to, not equal to, greater than, or less than. operator. EQ equal, NE not equal, GT greater than, LT less than.<br>Default: **GT**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **EQ**<br>• **NE**<br>• **GT**<br>• **LT** |
| expression | String | expression<br>Minimum: **1**<br>Maximum: **255** |

| Parameter | Type | Description |
| --- | --- | --- |
| severity | String | Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **TIPS**<br>• **LOW**<br>• **MEDIUM**<br>• **HIGH**<br>• **FATAL** |
| accumulated_times | Integer | accumulated_times<br>Minimum: **1**<br>Maximum: **1000**<br>Default: **1** |

**Status code: 400**

**Table 4-421** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

## Example Requests

Update an alert rule whose name is Alert rule, query type is SQL, status is Enabled, and Severity is Warning.

```
{
  "rule_name" : "Alert rule",
  "query" : "* | select status, count(*) as count group by status",
  "query_type" : "SQL",
  "status" : "ENABLED",
  "severity" : "TIPS",
  "custom_properties" : {
    "references" : "https://localhost/references",
    "maintainer" : "isap"
  },
  "event_grouping" : true,
  "schedule" : {
    "frequency_interval" : 5,
    "frequency_unit" : "MINUTE",
    "period_interval" : 5,
    "period_unit" : "MINUTE",
    "delay_interval" : 2,
    "overtime_interval" : 10
```

```
  },
  "triggers" : [ {
    "mode" : "COUNT",
    "operator" : "GT",
    "expression" : 10,
    "severity" : "TIPS"
  } ]
}
```

## Example Responses

**Status code: 200**

Success

```
{
  "rule_id" : "443a0117-1aa4-4595-ad4a-796fad4d4950",
  "pipe_id" : "772fb35b-83bc-46c9-a0b1-ebe31070a889",
  "create_by" : "582dd19dd99d4505a1d7929dc943b169",
  "create_time" : 1665221214,
  "update_by" : "582dd19dd99d4505a1d7929dc943b169",
  "update_time" : 1665221214,
  "delete_time" : 0,
  "rule_name" : "Alert rule",
  "query" : "* | select status, count(*) as count group by status",
  "query_type" : "SQL",
  "status" : "ENABLED",
  "severity" : "TIPS",
  "custom_properties" : {
    "references" : "https://localhost/references",
    "maintainer" : "isap"
  },
  "event_grouping" : true,
  "schedule" : {
    "frequency_interval" : 5,
    "frequency_unit" : "MINUTE",
    "period_interval" : 5,
    "period_unit" : "MINUTE",
    "delay_interval" : 2,
    "overtime_interval" : 10
  },
  "triggers" : [ {
    "mode" : "COUNT",
    "operator" : "GT",
    "expression" : 10,
    "severity" : "TIPS"
  } ]
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Update an alert rule whose name is Alert rule, query type is SQL, status is Enabled, and Severity is Warning.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
```

```
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;
import java.util.Map;
import java.util.HashMap;

public class UpdateAlertRuleSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdateAlertRuleRequest request = new UpdateAlertRuleRequest();
        UpdateAlertRuleRequestBody body = new UpdateAlertRuleRequestBody();
        List<AlertRuleTrigger> listbodyTriggers = new ArrayList<>();
        listbodyTriggers.add(
            new AlertRuleTrigger()
                .withMode(AlertRuleTrigger.ModeEnum.fromValue("COUNT"))
                .withOperator(AlertRuleTrigger.OperatorEnum.fromValue("GT"))
                .withExpression("10")
                .withSeverity(AlertRuleTrigger.SeverityEnum.fromValue("TIPS"))
        );
        Schedule schedulebody = new Schedule();
        schedulebody.withFrequencyInterval(5)
            .withFrequencyUnit(Schedule.FrequencyUnitEnum.fromValue("MINUTE"))
            .withPeriodInterval(5)
            .withPeriodUnit(Schedule.PeriodUnitEnum.fromValue("MINUTE"))
            .withDelayInterval(2)
            .withOvertimeInterval(10);
        Map<String, String> listbodyCustomProperties = new HashMap<>();
        listbodyCustomProperties.put("references", "https://localhost/references");
        listbodyCustomProperties.put("maintainer", "isap");
        body.withTriggers(listbodyTriggers);
        body.withSchedule(schedulebody);
        body.withEventGrouping(true);
        body.withCustomProperties(listbodyCustomProperties);
        body.withSeverity(UpdateAlertRuleRequestBody.SeverityEnum.fromValue("TIPS"));
        body.withStatus(UpdateAlertRuleRequestBody.StatusEnum.fromValue("ENABLED"));
        body.withQueryType(UpdateAlertRuleRequestBody.QueryTypeEnum.fromValue("SQL"));
        body.withQuery("* | select status, count(*) as count group by status");
        body.withRuleName("Alert rule");
        request.withBody(body);
        try {
            UpdateAlertRuleResponse response = client.updateAlertRule(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
```

```
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Update an alert rule whose name is Alert rule, query type is SQL, status is Enabled, and Severity is Warning.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateAlertRuleRequest()
        listTriggersbody = [
            AlertRuleTrigger(
                mode="COUNT",
                operator="GT",
                expression="10",
                severity="TIPS"
            )
        ]
        schedulebody = Schedule(
            frequency_interval=5,
            frequency_unit="MINUTE",
            period_interval=5,
            period_unit="MINUTE",
            delay_interval=2,
            overtime_interval=10
        )
        listCustomPropertiesbody = {
            "references": "https://localhost/references",
            "maintainer": "isap"
        }
        request.body = UpdateAlertRuleRequestBody(
            triggers=listTriggersbody,
            schedule=schedulebody,
            event_grouping=True,
            custom_properties=listCustomPropertiesbody,
            severity="TIPS",
            status="ENABLED",
            query_type="SQL",
            query="* | select status, count(*) as count group by status",
            rule_name="Alert rule"
        )
        response = client.update_alert_rule(request)
        print(response)
    except exceptions.ClientRequestException as e:
```

```
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Update an alert rule whose name is Alert rule, query type is SQL, status is Enabled, and Severity is Warning.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateAlertRuleRequest{}
    modeTriggers:= model.GetAlertRuleTriggerModeEnum().COUNT
    operatorTriggers:= model.GetAlertRuleTriggerOperatorEnum().GT
    severityTriggers:= model.GetAlertRuleTriggerSeverityEnum().TIPS
    var listTriggersbody = []model.AlertRuleTrigger{
        {
            Mode: &modeTriggers,
            Operator: &operatorTriggers,
            Expression: "10",
            Severity: &severityTriggers,
        },
    }
    delayIntervalSchedule:= int32(2)
    overtimeIntervalSchedule:= int32(10)
    schedulebody := &model.Schedule{
        FrequencyInterval: int32(5),
        FrequencyUnit: model.GetScheduleFrequencyUnitEnum().MINUTE,
        PeriodInterval: int32(5),
        PeriodUnit: model.GetSchedulePeriodUnitEnum().MINUTE,
        DelayInterval: &delayIntervalSchedule,
        OvertimeInterval: &overtimeIntervalSchedule,
    }
    var listCustomPropertiesbody = map[string]string{
        "references": "https://localhost/references",
        "maintainer": "isap",
    }
    eventGroupingUpdateAlertRuleRequestBody:= true
    severityUpdateAlertRuleRequestBody:= model.GetUpdateAlertRuleRequestBodySeverityEnum().TIPS
    statusUpdateAlertRuleRequestBody:= model.GetUpdateAlertRuleRequestBodyStatusEnum().ENABLED
```

```
    queryTypeUpdateAlertRuleRequestBody:= model.GetUpdateAlertRuleRequestBodyQueryTypeEnum().SQL
    queryUpdateAlertRuleRequestBody:= "* | select status, count(*) as count group by status"
    ruleNameUpdateAlertRuleRequestBody:= "Alert rule"
    request.Body = &model.UpdateAlertRuleRequestBody{
        Triggers: &listTriggersbody,
        Schedule: schedulebody,
        EventGrouping: &eventGroupingUpdateAlertRuleRequestBody,
        CustomProperties: listCustomPropertiesbody,
        Severity: &severityUpdateAlertRuleRequestBody,
        Status: &statusUpdateAlertRuleRequestBody,
        QueryType: &queryTypeUpdateAlertRuleRequestBody,
        Query: &queryUpdateAlertRuleRequestBody,
        RuleName: &ruleNameUpdateAlertRuleRequestBody,
    }
    response, err := client.UpdateAlertRule(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Success |
| 400 | Bad Request |

## Error Codes

See **Error Codes**.

# 4.5.6 Simulating an Alert Rule

## Function

Simulate alert rule

## Calling Method

For details, see **Calling APIs**.

## URI

POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/simulation

**Table 4-422** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID. Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID. Workspace ID.<br>Minimum: **32**<br>Maximum: **36** |

## Request Parameters

**Table 4-423** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. You can obtain the token by calling the IAM API used to obtain a user token. Token of an IAM user. To obtain it, call the corresponding IAM API.<br>Minimum: **1**<br>Maximum: **2097152** |

**Table 4-424** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| pipe_id | Yes | String | Pipeline ID.Pipe ID.<br>Minimum: **36**<br>Maximum: **36** |
| query | Yes | String | Query.<br>Minimum: **1**<br>Maximum: **1024** |
| query_type | No | String | SQL query syntax. Query type. SQL.<br>Default: **SQL**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **SQL** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| from | Yes | Long | Start time.Start time.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| to | Yes | Long | End time.End time.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| event_grouping | No | Boolean | Alert group. Incident group.<br>Default: **true** |
| triggers | Yes | Array of **AlertRuleTrigger** objects | Alert triggering rules. Alert triggers.<br>Array Length: **1 - 5** |

**Table 4-425** AlertRuleTrigger

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| mode | No | String | Number of modes. Mode. COUNT.<br>Default: **COUNT**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **COUNT** |
| operator | No | String | Operator, which can be equal to, not equal to, greater than, or less than. operator. EQ equal, NE not equal, GT greater than, LT less than.<br>Default: **GT**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **EQ**<br>• **NE**<br>• **GT**<br>• **LT** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| expression | Yes | String | expression<br>Minimum: **1**<br>Maximum: **255** |
| severity | No | String | Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **TIPS**<br>• **LOW**<br>• **MEDIUM**<br>• **HIGH**<br>• **FATAL** |
| accumulated_times | No | Integer | accumulated_times<br>Minimum: **1**<br>Maximum: **1000**<br>Default: **1** |

## Response Parameters

**Status code: 200**

**Table 4-426** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

**Table 4-427** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| alert_count | Integer | Number of alarms. Alert count.<br>Minimum: **0**<br>Maximum: **100** |

| Parameter | Type | Description |
| --- | --- | --- |
| severity | String | Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.<br>Minimum: **1**<br>Maximum: **64** |

**Status code: 400**

**Table 4-428** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

## Example Requests

Simulate an alarm rule. The ID of the pipe to which the alarm rule belongs is ead2769b-afb0-45dd-b9fa-a2953e6ac82f, the query type is SQL, and the severity is Warning.

```
{
  "pipe_id" : "ead2769b-afb0-45dd-b9fa-a2953e6ac82f",
  "query" : "* | select status, count(*) as count group by status",
  "query_type" : "SQL",
  "event_grouping" : true,
  "from" : 1665221214000,
  "to" : 1665546370000,
  "triggers" : [ {
    "mode" : "COUNT",
    "operator" : "GT",
    "expression" : 10,
    "severity" : "TIPS"
  } ]
}
```

## Example Responses

**Status code: 200**

Success

```
{
  "alert_count" : 100,
  "severity" : "TIPS"
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Simulate an alarm rule. The ID of the pipe to which the alarm rule belongs is ead2769b-afb0-45dd-b9fa-a2953e6ac82f, the query type is SQL, and the severity is Warning.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class CreateAlertRuleSimulationSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateAlertRuleSimulationRequest request = new CreateAlertRuleSimulationRequest();
        CreateAlertRuleSimulationRequestBody body = new CreateAlertRuleSimulationRequestBody();
        List<AlertRuleTrigger> listbodyTriggers = new ArrayList<>();
        listbodyTriggers.add(
            new AlertRuleTrigger()
                .withMode(AlertRuleTrigger.ModeEnum.fromValue("COUNT"))
                .withOperator(AlertRuleTrigger.OperatorEnum.fromValue("GT"))
                .withExpression("10")
                .withSeverity(AlertRuleTrigger.SeverityEnum.fromValue("TIPS"))
        );
        body.withTriggers(listbodyTriggers);
        body.withEventGrouping(true);
        body.withTo(1665546370000L);
        body.withFrom(1665221214000L);
        body.withQueryType(CreateAlertRuleSimulationRequestBody.QueryTypeEnum.fromValue("SQL"));
        body.withQuery("* | select status, count(*) as count group by status");
        body.withPipeId("ead2769b-afb0-45dd-b9fa-a2953e6ac82f");
        request.withBody(body);
        try {
            CreateAlertRuleSimulationResponse response = client.createAlertRuleSimulation(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
```

```
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Simulate an alarm rule. The ID of the pipe to which the alarm rule belongs is ead2769b-afb0-45dd-b9fa-a2953e6ac82f, the query type is SQL, and the severity is Warning.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateAlertRuleSimulationRequest()
        listTriggersbody = [
            AlertRuleTrigger(
                mode="COUNT",
                operator="GT",
                expression="10",
                severity="TIPS"
            )
        ]
        request.body = CreateAlertRuleSimulationRequestBody(
            triggers=listTriggersbody,
            event_grouping=True,
            to=1665546370000,
            _from=1665221214000,
            query_type="SQL",
            query="* | select status, count(*) as count group by status",
            pipe_id="ead2769b-afb0-45dd-b9fa-a2953e6ac82f"
        )
        response = client.create_alert_rule_simulation(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Simulate an alarm rule. The ID of the pipe to which the alarm rule belongs is ead2769b-afb0-45dd-b9fa-a2953e6ac82f, the query type is SQL, and the severity is Warning.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateAlertRuleSimulationRequest{}
    modeTriggers:= model.GetAlertRuleTriggerModeEnum().COUNT
    operatorTriggers:= model.GetAlertRuleTriggerOperatorEnum().GT
    severityTriggers:= model.GetAlertRuleTriggerSeverityEnum().TIPS
    var listTriggersbody = []model.AlertRuleTrigger{
        {
            Mode: &modeTriggers,
            Operator: &operatorTriggers,
            Expression: "10",
            Severity: &severityTriggers,
        },
    }
    eventGroupingCreateAlertRuleSimulationRequestBody:= true
    queryTypeCreateAlertRuleSimulationRequestBody:= model.GetCreateAlertRuleSimulationRequestBodyQueryTypeEnum().SQL
    request.Body = &model.CreateAlertRuleSimulationRequestBody{
        Triggers: listTriggersbody,
        EventGrouping: &eventGroupingCreateAlertRuleSimulationRequestBody,
        To: int64(1665546370000),
        From: int64(1665221214000),
        QueryType: &queryTypeCreateAlertRuleSimulationRequestBody,
        Query: "* | select status, count(*) as count group by status",
        PipeId: "ead2769b-afb0-45dd-b9fa-a2953e6ac82f",
    }
    response, err := client.CreateAlertRuleSimulation(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

### Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Success |
| 400 | Bad Request |

### Error Codes

See **Error Codes**.

## 4.5.7 Total number of alert rules.

### Function

List alert rule metrics

### Calling Method

For details, see **Calling APIs**.

### URI

GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/metrics

**Table 4-429** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID. Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID. Workspace ID.<br>Minimum: **32**<br>Maximum: **36** |

## Request Parameters

**Table 4-430** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. You can obtain the token by calling the IAM API used to obtain a user token. Token of an IAM user. To obtain it, call the corresponding IAM API.<br>Minimum: **1**<br>Maximum: **2097152** |

## Response Parameters

**Status code: 200**

**Table 4-431** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

**Table 4-432** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| category | String | Indicator type and number of groups. Metric category. GROUP_COUNT.<br>Enumeration values:<br>• **GROUP_COUNT** |
| metric | Map<String,Number> | Indicator value. Metric value. |

**Status code: 400**

**Table 4-433** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

## Example Requests

None

## Example Responses

**Status code: 200**

Success

- Example 1

```
{
  "category" : {
    "GROUP_COUNT" : null
  },
  "metric" : null
}
```

- Example 2

```
{
  "category" : "GROUP_COUNT",
  "metric" : {
    "ENABLED" : 8,
    "DISABLED" : 2
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListAlertRuleMetricsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
```

```
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListAlertRuleMetricsRequest request = new ListAlertRuleMetricsRequest();
        try {
            ListAlertRuleMetricsResponse response = client.listAlertRuleMetrics(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListAlertRuleMetricsRequest()
        response = client.list_alert_rule_metrics(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
```

```
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListAlertRuleMetricsRequest{}
    response, err := client.ListAlertRuleMetrics(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Success |
| 400 | Bad Request |

## Error Codes

See **Error Codes**.

# 4.5.8 Enabling an Alert Rule

## Function

Enable alert rule

## Calling Method

For details, see **Calling APIs**.

## URI

POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/enable

**Table 4-434** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID. Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID. Workspace ID.<br>Minimum: **32**<br>Maximum: **36** |

## Request Parameters

**Table 4-435** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. You can obtain the token by calling the IAM API used to obtain a user token. Token of an IAM user. To obtain it, call the corresponding IAM API.<br>Minimum: **1**<br>Maximum: **2097152** |

**Table 4-436** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| [items] | Yes | Array of strings | EnableAlertRuleRequestBody |

## Response Parameters

**Status code: 200**

**Table 4-437** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

**Table 4-438** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| rule_id | String | Alert rule ID.<br>Minimum: **36**<br>Maximum: **36** |
| status | String | Status. The options are as follows - Enabled - Disabled<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **ENABLED**<br>• **DISABLED** |

**Status code: 400**

**Table 4-439** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

## Example Requests

Enabling rule 123123

```
[ "123123" ]
```

## Example Responses

**Status code: 200**

Success

```
{
  "rule_id" : "443a0117-1aa4-4595-ad4a-796fad4d4950",
```

```
  "status" : "ENABLED"
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Enabling rule 123123

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class EnableAlertRuleSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        EnableAlertRuleRequest request = new EnableAlertRuleRequest();
        List<String> listbodyBody = new ArrayList<>();
        listbodyBody.add("123123");
        request.withBody(listbodyBody);
        try {
            EnableAlertRuleResponse response = client.enableAlertRule(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

### Enabling rule 123123

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = EnableAlertRuleRequest()
        listBodybody = [
            "123123"
        ]
        request.body = listBodybody
        response = client.enable_alert_rule(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

### Enabling rule 123123

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()
```

```
    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.EnableAlertRuleRequest{}
    var listBodybody = []string{
        "123123",
    }
    request.Body = &listBodybody
    response, err := client.EnableAlertRule(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Success |
| 400 | Bad Request |

## Error Codes

See **Error Codes**.

# 4.5.9 Disabling an Alert Rule

## Function

Disable alert rule

## Calling Method

For details, see **Calling APIs**.

## URI

POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/disable

**Table 4-440** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID. Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID. Workspace ID.<br>Minimum: **32**<br>Maximum: **36** |

## Request Parameters

**Table 4-441** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. You can obtain the token by calling the IAM API used to obtain a user token. Token of an IAM user. To obtain it, call the corresponding IAM API.<br>Minimum: **1**<br>Maximum: **2097152** |

**Table 4-442** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| [items] | Yes | Array of strings | DisableAlertRuleRequestBody |

## Response Parameters

**Status code: 200**

**Table 4-443** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

**Table 4-444** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| rule_id | String | Alert rule ID.<br>Minimum: **36**<br>Maximum: **36** |
| status | String | Status. The options are as follows - Enabled - Disabled<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **ENABLED**<br>• **DISABLED** |

**Status code: 400**

**Table 4-445** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

## Example Requests

Disabling rule 123123

```
[ "123123" ]
```

## Example Responses

**Status code: 200**

Success

```
{
  "rule_id" : "443a0117-1aa4-4595-ad4a-796fad4d4950",
  "status" : "ENABLED"
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Disabling rule 123123

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class DisableAlertRuleSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DisableAlertRuleRequest request = new DisableAlertRuleRequest();
        List<String> listbodyBody = new ArrayList<>();
        listbodyBody.add("123123");
        request.withBody(listbodyBody);
        try {
            DisableAlertRuleResponse response = client.disableAlertRule(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

### Disabling rule 123123

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
```

```
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DisableAlertRuleRequest()
        listBodybody = [
            "123123"
        ]
        request.body = listBodybody
        response = client.disable_alert_rule(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

### Disabling rule 123123

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DisableAlertRuleRequest{}
    var listBodybody = []string{
        "123123",
    }
    request.Body = &listBodybody
    response, err := client.DisableAlertRule(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
```

```
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Success |
| 400 | Bad Request |

## Error Codes

See **Error Codes**.

# 4.5.10 Listing Alert Rule Templates

## Function

List alert rule templates

## Calling Method

For details, see **Calling APIs**.

## URI

GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/templates

**Table 4-446** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID. Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID. Workspace ID.<br>Minimum: **32**<br>Maximum: **36** |

**Table 4-447** Query Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| offset | Yes | Long | The query offset. Offset.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| limit | Yes | Long | Number of bucket groups Limit.<br>Minimum: **10**<br>Maximum: **50** |
| sort_key | No | String | Sorting field. Sort key<br>Minimum: **1**<br>Maximum: **256** |
| sort_dir | No | String | Sort direction, asc or desc.<br>Enumeration values:<br>• **asc**<br>• **desc** |
| severity | No | Array | Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.<br>Array Length: **1 - 5**<br>Enumeration values:<br>• **TIPS**<br>• **LOW**<br>• **MEDIUM**<br>• **HIGH**<br>• **FATAL** |

## Request Parameters

**Table 4-448** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. You can obtain the token by calling the IAM API used to obtain a user token. Token of an IAM user. To obtain it, call the corresponding IAM API.<br>Minimum: **1**<br>Maximum: **2097152** |

## Response Parameters

**Status code: 200**

**Table 4-449** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

**Table 4-450** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| count | Long | Total number. Total count.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| records | Array of **AlertRuleTemplate** objects | Alert rule template. Alert rule templates.<br>Array Length: **0 - 100** |

**Table 4-451** AlertRuleTemplate

| Parameter | Type | Description |
| --- | --- | --- |
| template_id | String | Alert rule template ID. Alert rule template ID.<br>Minimum: **36**<br>Maximum: **36** |
| update_time | Long | Update time. Update time.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| template_name | String | Alert rule template ID. Alert rule template ID.<br>Minimum: **1**<br>Maximum: **255** |
| data_source | String | Data source. Data source.<br>Minimum: **1**<br>Maximum: **255** |
| version | String | Version. Version<br>Minimum: **1**<br>Maximum: **255** |
| query | String | Query.<br>Minimum: **1**<br>Maximum: **1024** |
| query_type | String | SQL query syntax, SQL. Query type. SQL.<br>Default: **SQL**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **SQL** |
| severity | String | Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.<br>Default: **TIPS**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **TIPS**<br>• **LOW**<br>• **MEDIUM**<br>• **HIGH**<br>• **FATAL** |

| Parameter | Type | Description |
| --- | --- | --- |
| custom_properties | Map<String,String> | Custom extension information. Custom properties. |
| event_grouping | Boolean | Alert group. Alert group.<br>Default: **true** |
| schedule | **Schedule** object | |
| triggers | Array of **AlertRuleTrigger** objects | Alert triggering rules. Alert triggers.<br>Array Length: **1 - 5** |

**Table 4-452** Schedule

| Parameter | Type | Description |
| --- | --- | --- |
| frequency_interval | Integer | Scheduling interval. Frequency interval.<br>Minimum: **1**<br>Maximum: **60** |
| frequency_unit | String | The unit of the scheduling interval. The value can be minute, hour, or day. Frequency unit. MINUTE, HOUR, DAY.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **MINUTE**<br>• **HOUR**<br>• **DAY** |
| period_interval | Integer | Time window interval. Period interval.<br>Minimum: **1**<br>Maximum: **60** |
| period_unit | String | Time Window unit. The value can be minute, hour, or day. Period unit. MINUTE, HOUR, DAY.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **MINUTE**<br>• **HOUR**<br>• **DAY** |

| Parameter | Type | Description |
| --- | --- | --- |
| delay_interval | Integer | The delay interval. Delay interval<br>Minimum: **0**<br>Maximum: **10**<br>Default: **0** |
| overtime_interval | Integer | Timeout interval. Overtime interval<br>Minimum: **0**<br>Maximum: **10**<br>Default: **10** |

**Table 4-453** AlertRuleTrigger

| Parameter | Type | Description |
| --- | --- | --- |
| mode | String | Number of modes. Mode. COUNT.<br>Default: **COUNT**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **COUNT** |
| operator | String | Operator, which can be equal to, not equal to, greater than, or less than. operator. EQ equal, NE not equal, GT greater than, LT less than.<br>Default: **GT**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **EQ**<br>• **NE**<br>• **GT**<br>• **LT** |
| expression | String | expression<br>Minimum: **1**<br>Maximum: **255** |

| Parameter | Type | Description |
| --- | --- | --- |
| severity | String | Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **TIPS**<br>• **LOW**<br>• **MEDIUM**<br>• **HIGH**<br>• **FATAL** |
| accumulated_times | Integer | accumulated_times<br>Minimum: **1**<br>Maximum: **1000**<br>Default: **1** |

**Status code: 400**

**Table 4-454** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

## Example Requests

None

## Example Responses

**Status code: 200**

Success

```
{
  "count" : 9223372036854776000,
  "records" : [ {
    "template_id" : "443a0117-1aa4-4595-ad4a-796fad4d4950",
    "update_time" : 1665221214,
    "template_name" : "Alert rule template",
    "data_source" : "sec_hss_vul",
    "version" : "1.0.0",
    "query" : "* | select status, count(*) as count group by status",
    "query_type" : "SQL",
    "severity" : "TIPS",
    "custom_properties" : {
```

```
    "references" : "https://localhost/references",
    "maintainer" : "isap"
   },
   "event_grouping" : true,
   "schedule" : {
    "frequency_interval" : 5,
    "frequency_unit" : "MINUTE",
    "period_interval" : 5,
    "period_unit" : "MINUTE",
    "delay_interval" : 2,
    "overtime_interval" : 10
   },
   "triggers" : [ {
    "mode" : "COUNT",
    "operator" : "GT",
    "expression" : 10,
    "severity" : "TIPS"
   } ]
  } ]
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class ListAlertRuleTemplatesSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListAlertRuleTemplatesRequest request = new ListAlertRuleTemplatesRequest();
        request.withOffset(<offset>L);
        request.withLimit(<limit>L);
        request.withSortKey("<sort_key>");
        request.withSortDir(ListAlertRuleTemplatesRequest.SortDirEnum.fromValue("<sort_dir>"));
        request.withSeverity();
        try {
            ListAlertRuleTemplatesResponse response = client.listAlertRuleTemplates(request);
```

```
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListAlertRuleTemplatesRequest()
        request.offset = <offset>
        request.limit = <limit>
        request.sort_key = "<sort_key>"
        request.sort_dir = "<sort_dir>"
        request.severity =
        response = client.list_alert_rule_templates(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
```

```
risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListAlertRuleTemplatesRequest{}
 request.Offset = int64(<offset>)
 request.Limit = int64(<limit>)
 sortKeyRequest:= "<sort_key>"
 request.SortKey = &sortKeyRequest
 sortDirRequest:= model.GetListAlertRuleTemplatesRequestSortDirEnum().<SORT_DIR>
 request.SortDir = &sortDirRequest
    response, err := client.ListAlertRuleTemplates(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Success |
| 400 | Bad Request |

## Error Codes

See **Error Codes**.

# 4.5.11 Viewing Alert Rule Templates

## Function

List alert rule templates

## Calling Method

For details, see **Calling APIs**.

## URI

GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/templates/{template_id}

**Table 4-455** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID. Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID. Workspace ID.<br>Minimum: **32**<br>Maximum: **36** |
| template_id | Yes | String | Alert rule template ID. Alert rule template ID.<br>Minimum: **36**<br>Maximum: **36** |

## Request Parameters

**Table 4-456** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. You can obtain the token by calling the IAM API used to obtain a user token. Token of an IAM user. To obtain it, call the corresponding IAM API.<br>Minimum: **1**<br>Maximum: **2097152** |

## Response Parameters

**Status code: 200**

**Table 4-457** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

**Table 4-458** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| template_id | String | Alert rule template ID. Alert rule template ID.<br>Minimum: **36**<br>Maximum: **36** |
| update_time | Long | Update time.<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| template_name | String | Alert rule template ID. Alert rule template ID.<br>Minimum: **1**<br>Maximum: **255** |
| data_source | String | Data source. Data source.<br>Minimum: **1**<br>Maximum: **255** |
| version | String | Version. Version<br>Minimum: **1**<br>Maximum: **255** |
| query | String | Query.<br>Minimum: **1**<br>Maximum: **1024** |
| query_type | String | SQL query syntax, SQL. Query type. SQL.<br>Default: **SQL**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **SQL** |

| Parameter | Type | Description |
| --- | --- | --- |
| severity | String | Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.<br>Default: **TIPS**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **TIPS**<br>• **LOW**<br>• **MEDIUM**<br>• **HIGH**<br>• **FATAL** |
| custom_properties | Map<String,String> | Custom extension information. Custom properties. |
| event_grouping | Boolean | Alert group. Alert group.<br>Default: **true** |
| schedule | **Schedule** object | |
| triggers | Array of **AlertRuleTrigger** objects | Alert triggering rules. Alert triggers.<br>Array Length: **1 - 5** |

**Table 4-459** Schedule

| Parameter | Type | Description |
| --- | --- | --- |
| frequency_interval | Integer | Scheduling interval. Frequency interval.<br>Minimum: **1**<br>Maximum: **60** |
| frequency_unit | String | The unit of the scheduling interval. The value can be minute, hour, or day. Frequency unit. MINUTE, HOUR, DAY.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **MINUTE**<br>• **HOUR**<br>• **DAY** |

| Parameter | Type | Description |
| --- | --- | --- |
| period_interval | Integer | Time window interval. Period interval.<br>Minimum: **1**<br>Maximum: **60** |
| period_unit | String | Time Window unit. The value can be minute, hour, or day. Period unit. MINUTE, HOUR, DAY.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **MINUTE**<br>• **HOUR**<br>• **DAY** |
| delay_interval | Integer | The delay interval. Delay interval<br>Minimum: **0**<br>Maximum: **10**<br>Default: **0** |
| overtime_interval | Integer | Timeout interval. Overtime interval<br>Minimum: **0**<br>Maximum: **10**<br>Default: **10** |

**Table 4-460** AlertRuleTrigger

| Parameter | Type | Description |
| --- | --- | --- |
| mode | String | Number of modes. Mode. COUNT.<br>Default: **COUNT**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **COUNT** |

| Parameter | Type | Description |
| --- | --- | --- |
| operator | String | Operator, which can be equal to, not equal to, greater than, or less than. operator. EQ equal, NE not equal, GT greater than, LT less than.<br>Default: **GT**<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **EQ**<br>• **NE**<br>• **GT**<br>• **LT** |
| expression | String | expression<br>Minimum: **1**<br>Maximum: **255** |
| severity | String | Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.<br>Minimum: **1**<br>Maximum: **255**<br>Enumeration values:<br>• **TIPS**<br>• **LOW**<br>• **MEDIUM**<br>• **HIGH**<br>• **FATAL** |
| accumulated_times | Integer | accumulated_times<br>Minimum: **1**<br>Maximum: **1000**<br>Default: **1** |

**Status code: 400**

**Table 4-461** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname. |

## Example Requests

None

## Example Responses

**Status code: 200**

Success

```
{
  "template_id" : "443a0117-1aa4-4595-ad4a-796fad4d4950",
  "update_time" : 1665221214,
  "template_name" : "Alert rule template",
  "data_source" : "sec_hss_vul",
  "version" : "1.0.0",
  "query" : "* | select status, count(*) as count group by status",
  "query_type" : "SQL",
  "severity" : "TIPS",
  "custom_properties" : {
    "references" : "https://localhost/references",
    "maintainer" : "isap"
  },
  "event_grouping" : true,
  "schedule" : {
    "frequency_interval" : 5,
    "frequency_unit" : "MINUTE",
    "period_interval" : 5,
    "period_unit" : "MINUTE",
    "delay_interval" : 2,
    "overtime_interval" : 10
  },
  "triggers" : [ {
    "mode" : "COUNT",
    "operator" : "GT",
    "expression" : 10,
    "severity" : "TIPS"
  } ]
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowAlertRuleTemplateSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
```

```
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowAlertRuleTemplateRequest request = new ShowAlertRuleTemplateRequest();
        try {
            ShowAlertRuleTemplateResponse response = client.showAlertRuleTemplate(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowAlertRuleTemplateRequest()
        response = client.show_alert_rule_template(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
```

```
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowAlertRuleTemplateRequest{}
    response, err := client.ShowAlertRuleTemplate(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Success |
| 400 | Bad Request |

## Error Codes

See **Error Codes**.

# 4.6 Playbook Version Management

# 4.6.1 Cloning a Playbook and Its Version

## Function

Cloning a Playbook and Its Version

## Calling Method

For details, see **Calling APIs**.

## URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/clone

**Table 4-462** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| version_id | Yes | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |

## Request Parameters

**Table 4-463** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-464** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| name | No | String | Name.<br>Minimum: **32**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-465** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-466** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Error message<br>Minimum: **1**<br>Maximum: **32** |
| data | **PlaybookVersionInfo** object | Playbook review details. |

**Table 4-467** PlaybookVersionInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |
| description | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |
| create_time | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| creator_id | String | Creator ID.<br>Minimum: **32**<br>Maximum: **64** |
| modifier_id | String | ID of the user who updated the information.<br>Minimum: **32**<br>Maximum: **64** |
| playbook_id | String | Playbook ID.<br>Minimum: **32**<br>Maximum: **64** |
| version | String | Version No.<br>Minimum: **32**<br>Maximum: **64** |
| enabled | Boolean | Whether to enable the function. - **true** -- Enabled. - **false** -- Disabled |
| status | String | Playbook version status. Options - Editing, APPROVING, UNPASSED, and PUBLISHED<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| action_strategy | String | Execution policy. Currently, only asynchronous concurrent execution is supported. The corresponding value is ASYNC.<br>Minimum: **0**<br>Maximum: **64** |
| actions | Array of **ActionInfo** objects | Workflows associated with the playbook.<br>Array Length: **0 - 99** |
| rule_enable | Boolean | Whether to enable the trigger condition filter. |
| rules | **RuleInfo** object | Playbook triggering specifications information. |
| dataclass_id | String | Data class ID.<br>Minimum: **0**<br>Maximum: **64** |
| trigger_type | String | How the playbook is triggered. The options are as follows - EVENT -- event; TIMER -- scheduled.)<br>Minimum: **0**<br>Maximum: **64** |
| dataobject_create | Boolean | Whether to trigger a playbook when a data object is created. |
| dataobject_update | Boolean | Whether to trigger a playbook when a data object is updated. |
| dataobject_delete | Boolean | Whether to trigger a playbook when a data object is deleted. |
| version_type | Integer | Version type (0 -- draft; 1 -- officially released)<br>Minimum: **0**<br>Maximum: **1** |
| rule_id | String | Filtering rule ID.<br>Minimum: **0**<br>Maximum: **64** |
| dataclass_name | String | Data class name.<br>Minimum: **0**<br>Maximum: **64** |
| approve_name | String | Reviewer.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-468** ActionInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook workflow ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Workflow name.<br>Minimum: **0**<br>Maximum: **1024** |
| description | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |
| action_type | String | Workflow type.<br>Minimum: **0**<br>Maximum: **64** |
| action_id | String | Workflow ID.<br>Minimum: **32**<br>Maximum: **64** |
| playbook_id | String | Playbook ID.<br>Minimum: **0**<br>Maximum: **64** |
| playbook_version_id | String | Playbook version ID.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-469** RuleInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Rule ID.<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| rule | String | Trigger rule.<br>Minimum: **0**<br>Maximum: **128** |

**Status code: 400**

**Table 4-470** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-471** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Clone a playbook and its version. The playbook name is name.

```
{
  "name" : "name"
}
```

## Example Responses

**Status code: 200**

Response parameters when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
```

```
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "description" : "This my XXXX",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "creator_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "modifier_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1",
    "enabled" : true,
    "status" : "editing",
    "action_strategy" : "sync",
    "actions" : [ {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "MyXXX",
      "description" : "This my XXXX",
      "action_type" : "Workflow",
      "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "playbook_id" : "string",
      "playbook_version_id" : "string",
      "project_id" : "string"
    } ],
    "rule_enable" : true,
    "rules" : {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "rule" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "dataclass_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "trigger_type" : "event",
    "dataobject_create" : true,
    "dataobject_update" : true,
    "dataobject_delete" : true,
    "version_type" : 1,
    "rule_id" : "string",
    "dataclass_name" : "string",
    "approve_name" : "string"
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Clone a playbook and its version. The playbook name is name.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class CopyPlaybookVersionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
```

```
this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CopyPlaybookVersionRequest request = new CopyPlaybookVersionRequest();
        CopyPlaybookInfo body = new CopyPlaybookInfo();
        body.withName("name");
        request.withBody(body);
        try {
            CopyPlaybookVersionResponse response = client.copyPlaybookVersion(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Clone a playbook and its version. The playbook name is name.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CopyPlaybookVersionRequest()
        request.body = CopyPlaybookInfo(
            name="name"
        )
        response = client.copy_playbook_version(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
```

```
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Clone a playbook and its version. The playbook name is name.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CopyPlaybookVersionRequest{}
    nameCopyPlaybookInfo:= "name"
    request.Body = &model.CopyPlaybookInfo{
        Name: &nameCopyPlaybookInfo,
    }
    response, err := client.CopyPlaybookVersion(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response parameters when the request is successful. |
| 400 | Response parameters when the request failed. |

## Error Codes

See **Error Codes**.

# 4.6.2 Querying the Playbook Version List

## Function

Querying the Playbook Version List

## Calling Method

For details, see **Calling APIs**.

## URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}/versions

**Table 4-472** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| playbook_id | Yes | String | Playbook ID.<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-473** Query Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| status | No | String | Playbook version status. Options are Editing, APPROVING, UNPASSED, and PUBLISHED<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| enabled | No | Integer | enabled/disabled<br>Minimum: **0**<br>Maximum: **1** |
| version_type | No | Integer | Version type. The options are as follows 0 is draft version; 1 is official version.<br>Minimum: **0**<br>Maximum: **10** |
| offset | No | Integer | Indicates the page number. Start position of the query result. The value starts from 0.<br>Minimum: **0**<br>Maximum: **999999** |
| limit | No | Integer | The maximum number of records can be returned on each page for a pagination query. The value starts from 1.<br>Minimum: **1**<br>Maximum: **999999** |

## Request Parameters

**Table 4-474** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-475** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-476** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Error Message<br>Minimum: **1**<br>Maximum: **32** |
| size | Integer | Records on each page.<br>Minimum: **0**<br>Maximum: **9999** |
| page | Integer | Current page.<br>Minimum: **0**<br>Maximum: **100** |
| total | Integer | Total<br>Minimum: **0**<br>Maximum: **99999** |
| data | Array of **PlaybookVersionListEntity** objects | Playbook version list.<br>Array Length: **0 - 100000000** |

**Table 4-477** PlaybookVersionListEntity

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| description | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |
| create_time | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| creator_id | String | Creator ID.<br>Minimum: **32**<br>Maximum: **64** |
| modifier_id | String | ID of the user who updated the information.<br>Minimum: **32**<br>Maximum: **64** |
| playbook_id | String | Playbook ID.<br>Minimum: **32**<br>Maximum: **64** |
| version | String | Version No.<br>Minimum: **32**<br>Maximum: **64** |
| enabled | Boolean | Activated |
| status | String | Status. (EDITING -- editing, APPROVING -- reviewing, UNPASSED -- not approved, Published -- approved)<br>Minimum: **0**<br>Maximum: **64** |
| action_strategy | String | Execution policy. Currently, only asynchronous concurrent execution is supported. The corresponding value is ASYNC.<br>Minimum: **0**<br>Maximum: **64** |
| rule_enable | Boolean | Whether the filtering rule is enabled. |

| Parameter | Type | Description |
| --- | --- | --- |
| dataclass_id | String | Data class ID.<br>Minimum: **0**<br>Maximum: **64** |
| trigger_type | String | Triggering mode. The options are as follows - EVENT -- event; TIMER -- scheduled.<br>Minimum: **0**<br>Maximum: **64** |
| dataobject_create | Boolean | Whether to trigger a playbook when a data object is created. |
| dataobject_update | Boolean | Whether to trigger a playbook when a data object is updated. |
| dataobject_delete | Boolean | Whether to trigger a playbook when a data object is deleted. |
| version_type | Integer | Edition<br>Minimum: **0**<br>Maximum: **1** |
| rule_id | String | Filtering rule ID.<br>Minimum: **0**<br>Maximum: **64** |
| dataclass_name | String | Data class name.<br>Minimum: **0**<br>Maximum: **64** |
| approve_name | String | Reviewer.<br>Minimum: **0**<br>Maximum: **64** |

**Status code: 400**

**Table 4-478** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-479** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message",
  "size" : 3,
  "page" : 10,
  "total" : 41,
  "data" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "description" : "This my XXXX",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "creator_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "modifier_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1",
    "enabled" : true,
    "status" : "editing",
    "action_strategy" : "sync",
    "rule_enable" : true,
    "dataclass_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "trigger_type" : "event",
    "dataobject_create" : true,
    "dataobject_update" : true,
    "dataobject_delete" : true,
    "version_type" : 1,
    "rule_id" : "string",
    "dataclass_name" : "string",
    "approve_name" : "string"
  } ]
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListPlaybookVersionsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListPlaybookVersionsRequest request = new ListPlaybookVersionsRequest();
        request.withStatus("<status>");
        request.withEnabled(<enabled>);
        request.withVersionType(<version_type>);
        request.withOffset(<offset>);
        request.withLimit(<limit>);
        try {
            ListPlaybookVersionsResponse response = client.listPlaybookVersions(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
```

```
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListPlaybookVersionsRequest()
        request.status = "<status>"
        request.enabled = <enabled>
        request.version_type = <version_type>
        request.offset = <offset>
        request.limit = <limit>
        response = client.list_playbook_versions(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListPlaybookVersionsRequest{}
    statusRequest:= "<status>"
    request.Status = &statusRequest
    enabledRequest:= int32(<enabled>)
    request.Enabled = &enabledRequest
    versionTypeRequest:= int32(<version_type>)
    request.VersionType = &versionTypeRequest
    offsetRequest:= int32(<offset>)
    request.Offset = &offsetRequest
    limitRequest:= int32(<limit>)
```

```
    request.Limit = &limitRequest
    response, err := client.ListPlaybookVersions(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

## Error Codes

See **Error Codes**.

# 4.6.3 Creating a Playbook Version

## Function

Creating a Playbook Version

## Calling Method

For details, see **Calling APIs**.

## URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}/versions

**Table 4-480** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| playbook_id | Yes | String | Playbook ID.<br>Minimum: **32**<br>Maximum: **64** |

## Request Parameters

**Table 4-481** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-482** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| description | No | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |
| workspace_id | No | String | Workspace ID<br>Minimum: **0**<br>Maximum: **2097152** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| playbook_id | No | String | Playbook ID.<br>Minimum: **32**<br>Maximum: **64** |
| actions | No | Array of **ActionInfo** objects | Associated workflows.<br>Array Length: **0 - 99** |
| dataclass_id | No | String | Data class ID.<br>Minimum: **32**<br>Maximum: **64** |
| rule_enable | No | Boolean | Whether the filtering rule is enabled. |
| rule_id | No | String | Filtering rule ID.<br>Minimum: **0**<br>Maximum: **64** |
| trigger_type | No | String | Triggering mode. The options are as follows -- EVENT -- event; TIMER -- scheduled.<br>Minimum: **0**<br>Maximum: **64** |
| dataobject_create | No | Boolean | Whether to trigger a playbook when a data object is created. |
| dataobject_update | No | Boolean | Whether to trigger a playbook when a data object is updated. |
| dataobject_delete | No | Boolean | Whether to trigger a playbook when a data object is deleted. |
| action_strategy | No | String | Execution policy. Currently, only asynchronous concurrent execution is supported. The corresponding value is ASYNC.<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-483** ActionInfo

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| id | No | String | Playbook workflow ID.<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| name | No | String | Workflow name.<br>Minimum: **0**<br>Maximum: **1024** |
| description | No | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |
| action_type | No | String | Workflow type.<br>Minimum: **0**<br>Maximum: **64** |
| action_id | No | String | Workflow ID.<br>Minimum: **32**<br>Maximum: **64** |
| playbook_id | No | String | Playbook ID.<br>Minimum: **0**<br>Maximum: **64** |
| playbook_version_id | No | String | Playbook version ID.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | No | String | Project ID.<br>Minimum: **0**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-484** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-485** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Error message<br>Minimum: **1**<br>Maximum: **32** |
| data | **PlaybookVersionInfo** object | Playbook review details. |

**Table 4-486** PlaybookVersionInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |
| description | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |
| create_time | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| creator_id | String | Creator ID.<br>Minimum: **32**<br>Maximum: **64** |
| modifier_id | String | ID of the user who updated the information.<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| playbook_id | String | Playbook ID.<br>Minimum: **32**<br>Maximum: **64** |
| version | String | Version No.<br>Minimum: **32**<br>Maximum: **64** |
| enabled | Boolean | Whether to enable the function. - **true** -- Enabled. - **false** -- Disabled |
| status | String | Playbook version status. Options - Editing, APPROVING, UNPASSED, and PUBLISHED<br>Minimum: **0**<br>Maximum: **64** |
| action_strategy | String | Execution policy. Currently, only asynchronous concurrent execution is supported. The corresponding value is ASYNC.<br>Minimum: **0**<br>Maximum: **64** |
| actions | Array of **ActionInfo** objects | Workflows associated with the playbook.<br>Array Length: **0 - 99** |
| rule_enable | Boolean | Whether to enable the trigger condition filter. |
| rules | **RuleInfo** object | Playbook triggering specifications information. |
| dataclass_id | String | Data class ID.<br>Minimum: **0**<br>Maximum: **64** |
| trigger_type | String | How the playbook is triggered. The options are as follows - EVENT -- event; TIMER -- scheduled.)<br>Minimum: **0**<br>Maximum: **64** |
| dataobject_create | Boolean | Whether to trigger a playbook when a data object is created. |
| dataobject_update | Boolean | Whether to trigger a playbook when a data object is updated. |
| dataobject_delete | Boolean | Whether to trigger a playbook when a data object is deleted. |

| Parameter | Type | Description |
| --- | --- | --- |
| version_type | Integer | Version type (0 -- draft; 1 -- officially released)<br>Minimum: **0**<br>Maximum: **1** |
| rule_id | String | Filtering rule ID.<br>Minimum: **0**<br>Maximum: **64** |
| dataclass_name | String | Data class name.<br>Minimum: **0**<br>Maximum: **64** |
| approve_name | String | Reviewer.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-487** ActionInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook workflow ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Workflow name.<br>Minimum: **0**<br>Maximum: **1024** |
| description | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |
| action_type | String | Workflow type.<br>Minimum: **0**<br>Maximum: **64** |
| action_id | String | Workflow ID.<br>Minimum: **32**<br>Maximum: **64** |
| playbook_id | String | Playbook ID.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| playbook_version_id | String | Playbook version ID.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-488** RuleInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Rule ID.<br>Minimum: **32**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| rule | String | Trigger rule.<br>Minimum: **0**<br>Maximum: **128** |

**Status code: 400**

**Table 4-489** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-490** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Create a playbook version. Set the workspace ID to string, playbook ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, data class ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, and rule to Enabled.

```
{
  "description" : "This my XXXX",
  "workspace_id" : "string",
  "playbook_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "actions" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "description" : "This my XXXX",
    "action_type" : "Workflow",
    "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook_id" : "string",
    "playbook_version_id" : "string",
    "project_id" : "string"
  } ],
  "dataclass_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "rule_enable" : true,
  "rule_id" : "4185bbd2-9d18-4362-92cb-46df0b24fe4e",
  "trigger_type" : "event",
  "dataobject_create" : true,
  "dataobject_update" : true,
  "dataobject_delete" : true,
  "action_strategy" : "sync"
}
```

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "description" : "This my XXXX",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "creator_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "modifier_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1",
    "enabled" : true,
    "status" : "editing",
    "action_strategy" : "sync",
    "actions" : [ {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "MyXXX",
      "description" : "This my XXXX",
```

```
    "action_type" : "Workflow",
    "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook_id" : "string",
    "playbook_version_id" : "string",
    "project_id" : "string"
  } ],
  "rule_enable" : true,
  "rules" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "rule" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  },
  "dataclass_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "trigger_type" : "event",
  "dataobject_create" : true,
  "dataobject_update" : true,
  "dataobject_delete" : true,
  "version_type" : 1,
  "rule_id" : "string",
  "dataclass_name" : "string",
  "approve_name" : "string"
 }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Create a playbook version. Set the workspace ID to string, playbook ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, data class ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, and rule to Enabled.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class CreatePlaybookVersionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
```

```
        CreatePlaybookVersionRequest request = new CreatePlaybookVersionRequest();
        CreatePlaybookVersionInfo body = new CreatePlaybookVersionInfo();
        List<ActionInfo> listbodyActions = new ArrayList<>();
        listbodyActions.add(
            new ActionInfo()
                .withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withName("MyXXX")
                .withDescription("This my XXXX")
                .withActionType("Workflow")
                .withActionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withPlaybookId("string")
                .withPlaybookVersionId("string")
                .withProjectId("string")
        );
        body.withActionStrategy("sync");
        body.withDataobjectDelete(true);
        body.withDataobjectUpdate(true);
        body.withDataobjectCreate(true);
        body.withTriggerType("event");
        body.withRuleId("4185bbd2-9d18-4362-92cb-46df0b24fe4e");
        body.withRuleEnable(true);
        body.withDataclassId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withActions(listbodyActions);
        body.withPlaybookId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withWorkspaceId("string");
        body.withDescription("This my XXXX");
        request.withBody(body);
        try {
            CreatePlaybookVersionResponse response = client.createPlaybookVersion(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Create a playbook version. Set the workspace ID to string, playbook ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, data class ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, and rule to Enabled.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \
```

```
    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreatePlaybookVersionRequest()
        listActionsbody = [
            ActionInfo(
                id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
                name="MyXXX",
                description="This my XXXX",
                action_type="Workflow",
                action_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
                playbook_id="string",
                playbook_version_id="string",
                project_id="string"
            )
        ]
        request.body = CreatePlaybookVersionInfo(
            action_strategy="sync",
            dataobject_delete=True,
            dataobject_update=True,
            dataobject_create=True,
            trigger_type="event",
            rule_id="4185bbd2-9d18-4362-92cb-46df0b24fe4e",
            rule_enable=True,
            dataclass_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            actions=listActionsbody,
            playbook_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            workspace_id="string",
            description="This my XXXX"
        )
        response = client.create_playbook_version(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Create a playbook version. Set the workspace ID to string, playbook ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, data class ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, and rule to Enabled.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
```

```
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreatePlaybookVersionRequest{}
    idActions:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    nameActions:= "MyXXX"
    descriptionActions:= "This my XXXX"
    actionTypeActions:= "Workflow"
    actionIdActions:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    playbookIdActions:= "string"
    playbookVersionIdActions:= "string"
    projectIdActions:= "string"
    var listActionsbody = []model.ActionInfo{
        {
            Id: &idActions,
            Name: &nameActions,
            Description: &descriptionActions,
            ActionType: &actionTypeActions,
            ActionId: &actionIdActions,
            PlaybookId: &playbookIdActions,
            PlaybookVersionId: &playbookVersionIdActions,
            ProjectId: &projectIdActions,
        },
    }
    actionStrategyCreatePlaybookVersionInfo:= "sync"
    dataobjectDeleteCreatePlaybookVersionInfo:= true
    dataobjectUpdateCreatePlaybookVersionInfo:= true
    dataobjectCreateCreatePlaybookVersionInfo:= true
    triggerTypeCreatePlaybookVersionInfo:= "event"
    ruleIdCreatePlaybookVersionInfo:= "4185bbd2-9d18-4362-92cb-46df0b24fe4e"
    ruleEnableCreatePlaybookVersionInfo:= true
    dataclassIdCreatePlaybookVersionInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    playbookIdCreatePlaybookVersionInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    workspaceIdCreatePlaybookVersionInfo:= "string"
    descriptionCreatePlaybookVersionInfo:= "This my XXXX"
    request.Body = &model.CreatePlaybookVersionInfo{
        ActionStrategy: &actionStrategyCreatePlaybookVersionInfo,
        DataobjectDelete: &dataobjectDeleteCreatePlaybookVersionInfo,
        DataobjectUpdate: &dataobjectUpdateCreatePlaybookVersionInfo,
        DataobjectCreate: &dataobjectCreateCreatePlaybookVersionInfo,
        TriggerType: &triggerTypeCreatePlaybookVersionInfo,
        RuleId: &ruleIdCreatePlaybookVersionInfo,
        RuleEnable: &ruleEnableCreatePlaybookVersionInfo,
        DataclassId: &dataclassIdCreatePlaybookVersionInfo,
        Actions: &listActionsbody,
        PlaybookId: &playbookIdCreatePlaybookVersionInfo,
        WorkspaceId: &workspaceIdCreatePlaybookVersionInfo,
        Description: &descriptionCreatePlaybookVersionInfo,
    }
    response, err := client.CreatePlaybookVersion(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

### Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

### Error Codes

See **Error Codes**.

## 4.6.4 Querying Playbook Version Details

### Function

Show playbook version version

### Calling Method

For details, see **Calling APIs**.

### URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}

**Table 4-491** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| version_id | Yes | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |

## Request Parameters

**Table 4-492** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-493** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-494** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Error message<br>Minimum: **1**<br>Maximum: **32** |
| data | **PlaybookVersionInfo** object | Playbook review details. |

**Table 4-495** PlaybookVersionInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |
| description | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |
| create_time | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| creator_id | String | Creator ID.<br>Minimum: **32**<br>Maximum: **64** |
| modifier_id | String | ID of the user who updated the information.<br>Minimum: **32**<br>Maximum: **64** |
| playbook_id | String | Playbook ID.<br>Minimum: **32**<br>Maximum: **64** |
| version | String | Version No.<br>Minimum: **32**<br>Maximum: **64** |
| enabled | Boolean | Whether to enable the function. - **true** -- Enabled. - **false** -- Disabled |
| status | String | Playbook version status. Options - Editing, APPROVING, UNPASSED, and PUBLISHED<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| action_strategy | String | Execution policy. Currently, only asynchronous concurrent execution is supported. The corresponding value is ASYNC.<br>Minimum: **0**<br>Maximum: **64** |
| actions | Array of **ActionInfo** objects | Workflows associated with the playbook.<br>Array Length: **0 - 99** |
| rule_enable | Boolean | Whether to enable the trigger condition filter. |
| rules | **RuleInfo** object | Playbook triggering specifications information. |
| dataclass_id | String | Data class ID.<br>Minimum: **0**<br>Maximum: **64** |
| trigger_type | String | How the playbook is triggered. The options are as follows - EVENT -- event; TIMER -- scheduled.)<br>Minimum: **0**<br>Maximum: **64** |
| dataobject_create | Boolean | Whether to trigger a playbook when a data object is created. |
| dataobject_update | Boolean | Whether to trigger a playbook when a data object is updated. |
| dataobject_delete | Boolean | Whether to trigger a playbook when a data object is deleted. |
| version_type | Integer | Version type (0 -- draft; 1 -- officially released)<br>Minimum: **0**<br>Maximum: **1** |
| rule_id | String | Filtering rule ID.<br>Minimum: **0**<br>Maximum: **64** |
| dataclass_name | String | Data class name.<br>Minimum: **0**<br>Maximum: **64** |
| approve_name | String | Reviewer.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-496** ActionInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook workflow ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Workflow name.<br>Minimum: **0**<br>Maximum: **1024** |
| description | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |
| action_type | String | Workflow type.<br>Minimum: **0**<br>Maximum: **64** |
| action_id | String | Workflow ID.<br>Minimum: **32**<br>Maximum: **64** |
| playbook_id | String | Playbook ID.<br>Minimum: **0**<br>Maximum: **64** |
| playbook_version_id | String | Playbook version ID.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-497** RuleInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Rule ID.<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| rule | String | Trigger rule.<br>Minimum: **0**<br>Maximum: **128** |

**Status code: 400**

**Table 4-498** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-499** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "description" : "This my XXXX",
    "create_time" : "2021-01-30T23:00:00Z+0800",
```

```
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "creator_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "modifier_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1",
    "enabled" : true,
    "status" : "editing",
    "action_strategy" : "sync",
    "actions" : [ {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "MyXXX",
      "description" : "This my XXXX",
      "action_type" : "Workflow",
      "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "playbook_id" : "string",
      "playbook_version_id" : "string",
      "project_id" : "string"
    } ],
    "rule_enable" : true,
    "rules" : {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "rule" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "dataclass_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "trigger_type" : "event",
    "dataobject_create" : true,
    "dataobject_update" : true,
    "dataobject_delete" : true,
    "version_type" : 1,
    "rule_id" : "string",
    "dataclass_name" : "string",
    "approve_name" : "string"
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowPlaybookVersionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
```

```
            .withSk(sk);

    SecMasterClient client = SecMasterClient.newBuilder()
            .withCredential(auth)
            .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
            .build();
    ShowPlaybookVersionRequest request = new ShowPlaybookVersionRequest();
    try {
        ShowPlaybookVersionResponse response = client.showPlaybookVersion(request);
        System.out.println(response.toString());
    } catch (ConnectionException e) {
        e.printStackTrace();
    } catch (RequestTimeoutException e) {
        e.printStackTrace();
    } catch (ServiceResponseException e) {
        e.printStackTrace();
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
  }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowPlaybookVersionRequest()
        response = client.show_playbook_version(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
```

```
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowPlaybookVersionRequest{}
    response, err := client.ShowPlaybookVersion(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

## Error Codes

See **Error Codes**.

# 4.6.5 Deleting a Playbook Version

## Function

Deleting a Playbook Version

## Calling Method

For details, see **Calling APIs**.

## URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}

**Table 4-500** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| version_id | Yes | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |

## Request Parameters

**Table 4-501** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-502** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-503** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Response message.<br>Minimum: **1**<br>Maximum: **32** |

**Status code: 400**

**Table 4-504** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-505** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message"
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class DeletePlaybookVersionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeletePlaybookVersionRequest request = new DeletePlaybookVersionRequest();
        try {
            DeletePlaybookVersionResponse response = client.deletePlaybookVersion(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeletePlaybookVersionRequest()
        response = client.delete_playbook_version(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeletePlaybookVersionRequest{}
    response, err := client.DeletePlaybookVersion(request)
```

```
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

## Error Codes

See **Error Codes**.

# 4.6.6 Updated the playbook version.

## Function

Updated the playbook version.

## Calling Method

For details, see **Calling APIs**.

## URI

PUT /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}

**Table 4-506** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| version_id | Yes | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |

## Request Parameters

**Table 4-507** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-508** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| description | No | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |
| workspace_id | No | String | Workspace ID<br>Minimum: **0**<br>Maximum: **2097152** |
| playbook_id | No | String | Playbook ID.<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| dataclass_id | No | String | Data class ID.<br>Minimum: **32**<br>Maximum: **64** |
| rule_enable | No | Boolean | Whether to enable the trigger condition filter. |
| enabled | No | Boolean | Whether to activate. - false -- not activated - true -- activated |
| status | No | String | Status (APPROVING -- being reviewed; EDITING -- being edited; UNPASSED -- rejected; Published -- released)<br>Minimum: **0**<br>Maximum: **64** |
| rule_id | No | String | Rule ID.<br>Minimum: **0**<br>Maximum: **64** |
| trigger_type | No | String | Triggering mode. The options are as follows - EVENT -- event; TIMER -- scheduled.<br>Minimum: **0**<br>Maximum: **64** |
| dataobject_create | No | Boolean | Whether to trigger a playbook when a data object is created. |
| dataobject_update | No | Boolean | Whether to trigger a playbook when a data object is updated. |
| dataobject_delete | No | Boolean | Whether to trigger a playbook when a data object is deleted. |
| action_strategy | No | String | Execution policy. Currently, only asynchronous concurrent execution is supported. The corresponding value is ASYNC.<br>Minimum: **0**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-509** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-510** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Error message<br>Minimum: **1**<br>Maximum: **32** |
| data | **PlaybookVersionInfo** object | Playbook review details. |

**Table 4-511** PlaybookVersionInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |
| description | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |
| create_time | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| creator_id | String | Creator ID.<br>Minimum: **32**<br>Maximum: **64** |
| modifier_id | String | ID of the user who updated the information.<br>Minimum: **32**<br>Maximum: **64** |
| playbook_id | String | Playbook ID.<br>Minimum: **32**<br>Maximum: **64** |
| version | String | Version No.<br>Minimum: **32**<br>Maximum: **64** |
| enabled | Boolean | Whether to enable the function. - **true** -- Enabled. - **false** -- Disabled |
| status | String | Playbook version status. Options - Editing, APPROVING, UNPASSED, and PUBLISHED<br>Minimum: **0**<br>Maximum: **64** |
| action_strategy | String | Execution policy. Currently, only asynchronous concurrent execution is supported. The corresponding value is ASYNC.<br>Minimum: **0**<br>Maximum: **64** |
| actions | Array of **ActionInfo** objects | Workflows associated with the playbook.<br>Array Length: **0 - 99** |
| rule_enable | Boolean | Whether to enable the trigger condition filter. |
| rules | **RuleInfo** object | Playbook triggering specifications information. |
| dataclass_id | String | Data class ID.<br>Minimum: **0**<br>Maximum: **64** |
| trigger_type | String | How the playbook is triggered. The options are as follows - EVENT -- event; TIMER -- scheduled.)<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| dataobject_create | Boolean | Whether to trigger a playbook when a data object is created. |
| dataobject_update | Boolean | Whether to trigger a playbook when a data object is updated. |
| dataobject_delete | Boolean | Whether to trigger a playbook when a data object is deleted. |
| version_type | Integer | Version type (0 -- draft; 1 -- officially released)<br>Minimum: **0**<br>Maximum: **1** |
| rule_id | String | Filtering rule ID.<br>Minimum: **0**<br>Maximum: **64** |
| dataclass_name | String | Data class name.<br>Minimum: **0**<br>Maximum: **64** |
| approve_name | String | Reviewer.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-512** ActionInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook workflow ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Workflow name.<br>Minimum: **0**<br>Maximum: **1024** |
| description | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |
| action_type | String | Workflow type.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| action_id | String | Workflow ID.<br>Minimum: **32**<br>Maximum: **64** |
| playbook_id | String | Playbook ID.<br>Minimum: **0**<br>Maximum: **64** |
| playbook_version_id | String | Playbook version ID.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-513** RuleInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Rule ID.<br>Minimum: **32**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| rule | String | Trigger rule.<br>Minimum: **0**<br>Maximum: **128** |

**Status code: 400**

**Table 4-514** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-515** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Update a playbook version. Set the workspace ID to string, playbook ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, data class ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, and playbook rule to Enabled.

```
{
  "description" : "This my XXXX",
  "workspace_id" : "string",
  "playbook_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "dataclass_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "rule_enable" : true,
  "enabled" : true,
  "status" : "UNPASSED",
  "rule_id" : "4185bbd2-9d18-4362-92cb-46df0b24fe4e",
  "trigger_type" : "event",
  "dataobject_create" : true,
  "dataobject_update" : true,
  "dataobject_delete" : true,
  "action_strategy" : "sync"
}
```

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "description" : "This my XXXX",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "creator_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "modifier_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1",
    "enabled" : true,
    "status" : "editing",
    "action_strategy" : "sync",
    "actions" : [ {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "MyXXX",
      "description" : "This my XXXX",
      "action_type" : "Workflow",
```

```
    "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook_id" : "string",
    "playbook_version_id" : "string",
    "project_id" : "string"
  } ],
  "rule_enable" : true,
  "rules" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "rule" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  },
  "dataclass_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "trigger_type" : "event",
  "dataobject_create" : true,
  "dataobject_update" : true,
  "dataobject_delete" : true,
  "version_type" : 1,
  "rule_id" : "string",
  "dataclass_name" : "string",
  "approve_name" : "string"
 }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Update a playbook version. Set the workspace ID to string, playbook ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, data class ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, and playbook rule to Enabled.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class UpdatePlaybookVersionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdatePlaybookVersionRequest request = new UpdatePlaybookVersionRequest();
        ModifyPlaybookVersionInfo body = new ModifyPlaybookVersionInfo();
        body.withActionStrategy("sync");
```

```
        body.withDataobjectDelete(true);
        body.withDataobjectUpdate(true);
        body.withDataobjectCreate(true);
        body.withTriggerType("event");
        body.withRuleId("4185bbd2-9d18-4362-92cb-46df0b24fe4e");
        body.withStatus("UNPASSED");
        body.withEnabled(true);
        body.withRuleEnable(true);
        body.withDataclassId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withPlaybookId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withWorkspaceId("string");
        body.withDescription("This my XXXX");
        request.withBody(body);
        try {
            UpdatePlaybookVersionResponse response = client.updatePlaybookVersion(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Update a playbook version. Set the workspace ID to string, playbook ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, data class ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, and playbook rule to Enabled.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdatePlaybookVersionRequest()
        request.body = ModifyPlaybookVersionInfo(
            action_strategy="sync",
            dataobject_delete=True,
            dataobject_update=True,
            dataobject_create=True,
            trigger_type="event",
            rule_id="4185bbd2-9d18-4362-92cb-46df0b24fe4e",
```

```
        status="UNPASSED",
        enabled=True,
        rule_enable=True,
        dataclass_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        playbook_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        workspace_id="string",
        description="This my XXXX"
    )
    response = client.update_playbook_version(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

Update a playbook version. Set the workspace ID to string, playbook ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, data class ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, and playbook rule to Enabled.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdatePlaybookVersionRequest{}
    actionStrategyModifyPlaybookVersionInfo:= "sync"
    dataobjectDeleteModifyPlaybookVersionInfo:= true
    dataobjectUpdateModifyPlaybookVersionInfo:= true
    dataobjectCreateModifyPlaybookVersionInfo:= true
    triggerTypeModifyPlaybookVersionInfo:= "event"
    ruleIdModifyPlaybookVersionInfo:= "4185bbd2-9d18-4362-92cb-46df0b24fe4e"
    statusModifyPlaybookVersionInfo:= "UNPASSED"
    enabledModifyPlaybookVersionInfo:= true
    ruleEnableModifyPlaybookVersionInfo:= true
    dataclassIdModifyPlaybookVersionInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    playbookIdModifyPlaybookVersionInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    workspaceIdModifyPlaybookVersionInfo:= "string"
    descriptionModifyPlaybookVersionInfo:= "This my XXXX"
    request.Body = &model.ModifyPlaybookVersionInfo{
        ActionStrategy: &actionStrategyModifyPlaybookVersionInfo,
```

```
        DataobjectDelete: &dataobjectDeleteModifyPlaybookVersionInfo,
        DataobjectUpdate: &dataobjectUpdateModifyPlaybookVersionInfo,
        DataobjectCreate: &dataobjectCreateModifyPlaybookVersionInfo,
        TriggerType: &triggerTypeModifyPlaybookVersionInfo,
        RuleId: &ruleIdModifyPlaybookVersionInfo,
        Status: &statusModifyPlaybookVersionInfo,
        Enabled: &enabledModifyPlaybookVersionInfo,
        RuleEnable: &ruleEnableModifyPlaybookVersionInfo,
        DataclassId: &dataclassIdModifyPlaybookVersionInfo,
        PlaybookId: &playbookIdModifyPlaybookVersionInfo,
        WorkspaceId: &workspaceIdModifyPlaybookVersionInfo,
        Description: &descriptionModifyPlaybookVersionInfo,
    }
    response, err := client.UpdatePlaybookVersion(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

### More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

### Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

### Error Codes

See **Error Codes**.

# 4.7 Playbook Rule Management

## 4.7.1 Querying Playbook Rule Details

### Function

Querying Playbook Rule Details

### Calling Method

For details, see **Calling APIs**.

## URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/rules/{rule_id}

**Table 4-516** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| version_id | Yes | String | version Id value<br>Minimum: **32**<br>Maximum: **64** |
| rule_id | Yes | String | version Id value<br>Minimum: **32**<br>Maximum: **64** |

## Request Parameters

**Table 4-517** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-518** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-519** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Error Message<br>Minimum: **1**<br>Maximum: **32** |
| data | **RuleInfo** object | Playbook triggering specifications information. |

**Table 4-520** RuleInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Rule ID.<br>Minimum: **32**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| rule | String | Trigger rule.<br>Minimum: **0**<br>Maximum: **128** |

**Status code: 400**

**Table 4-521** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-522** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "rule" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;
```

```
public class ShowPlaybookRuleSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPlaybookRuleRequest request = new ShowPlaybookRuleRequest();
        try {
            ShowPlaybookRuleResponse response = client.showPlaybookRule(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowPlaybookRuleRequest()
        response = client.show_playbook_rule(request)
        print(response)
    except exceptions.ClientRequestException as e:
```

```
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowPlaybookRuleRequest{}
    response, err := client.ShowPlaybookRule(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

## Error Codes

See **Error Codes**.

# 4.7.2 Deleting a Playbook Rule

## Function

Deleting a Playbook Rule

## Calling Method

For details, see **Calling APIs**.

## URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/rules/{rule_id}

**Table 4-523** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| version_id | Yes | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |
| rule_id | Yes | String | Rule ID.<br>Minimum: **36**<br>Maximum: **36** |

## Request Parameters

**Table 4-524** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-525** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-526** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Response message.<br>Minimum: **1**<br>Maximum: **32** |

**Status code: 400**

**Table 4-527** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-528** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message"
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class DeletePlaybookRuleSolution {

    public static void main(String[] args) {
```

```
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeletePlaybookRuleRequest request = new DeletePlaybookRuleRequest();
        try {
            DeletePlaybookRuleResponse response = client.deletePlaybookRule(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeletePlaybookRuleRequest()
        response = client.delete_playbook_rule(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeletePlaybookRuleRequest{}
    response, err := client.DeletePlaybookRule(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

## Error Codes

See **Error Codes**.

# 4.7.3 Creating a Playbook Rule

## Function

Creating a Playbook Rule

## Calling Method

For details, see **Calling APIs**.

## URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/rules

**Table 4-529** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| version_id | Yes | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |

## Request Parameters

**Table 4-530** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-531** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| rule | Yes | **ConditionInfo** object | Details of playbook triggering rules |

**Table 4-532** ConditionInfo

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| expression_type | No | String | Expression type. This parameter is mandatory for incident-triggered playbooks. The default value is common.<br>Minimum: **0**<br>Maximum: **64** |
| conditions | No | Array of **ConditionItem** objects | Triggering conditions. This parameter is mandatory for incident-triggered playbooks.<br>Array Length: **0 - 99** |
| logics | No | Array of strings | Conditional logic combinations. This parameter is mandatory for incident-triggered playbooks.<br>Minimum: **0**<br>Maximum: **64**<br>Array Length: **0 - 99** |
| cron | No | String | Cron expression (scheduled tasks). This parameter is mandatory for scheduled playbooks.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| schedule_type | No | String | Scheduled task repetition type. The value can be second, hour, day, or week. This parameter is mandatory for scheduled playbooks.<br>Minimum: **0**<br>Maximum: **64** |
| start_type | No | String | Playbook execution type. The value can be IMMEDIATELY or CUSTOM. This parameter is mandatory for scheduled playbooks.<br>Minimum: **0**<br>Maximum: **64** |
| end_type | No | String | Playbook execution termination type. - FOREVER -- The playbook is executed all the time. - CUSTOM -- The playbook stops at a customized time. This parameter is mandatory for scheduled playbooks.<br>Minimum: **0**<br>Maximum: **64** |
| end_time | No | String | End time of a scheduled task. This parameter is mandatory for scheduled playbooks.<br>Minimum: **0**<br>Maximum: **64** |
| repeat_range | No | String | Execution time range, for example, 2021-01-30T23:00:00Z+0800. This parameter is mandatory for scheduled playbooks.<br>Minimum: **0**<br>Maximum: **64** |
| only_once | No | Boolean | Whether the operation is performed only once. This parameter is mandatory for scheduled playbooks. |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| execution_type | No | String | Execution queue type (PARALLEL -- The new task runs in parallel with the previous task). This parameter is mandatory for scheduled playbooks.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-533** ConditionItem

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| name | No | String | Condition name.<br>Minimum: **0**<br>Maximum: **64** |
| detail | No | String | Condition details.<br>Minimum: **0**<br>Maximum: **1028** |
| data | No | Array of strings | Condition expression data.<br>Minimum: **0**<br>Maximum: **2048**<br>Array Length: **0 - 99** |

## Response Parameters

**Status code: 200**

**Table 4-534** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-535** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Error Message<br>Minimum: **1**<br>Maximum: **32** |
| data | **RuleInfo** object | Playbook triggering specifications information. |

**Table 4-536** RuleInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Rule ID.<br>Minimum: **32**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| rule | String | Trigger rule.<br>Minimum: **0**<br>Maximum: **128** |

**Status code: 400**

**Table 4-537** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-538** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Create a playbook rule named logic1 and expression type.

```
{
  "rule" : {
    "expression_type" : "common",
    "conditions" : [ {
      "name" : "condition_0",
      "detail" : "123",
      "data" : [ "waf.alarm.level', '>', '3" ]
    } ],
    "logics" : [ "condition_0" ]
  }
}
```

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "code" : 0,
  "message" : "",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "rule" : "{\"expression_type\":\"common\",\"conditions\":[{\"name\":\"condition_0\",\"data\":
[\"ref_order_id\",\"==\",\"123\"],\"detail\":\"123\"}],\"logics\":[\"condition_0\"]}"
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Create a playbook rule named logic1 and expression type.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
```

```
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class CreatePlaybookRuleSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreatePlaybookRuleRequest request = new CreatePlaybookRuleRequest();
        CreateRuleInfo body = new CreateRuleInfo();
        List<String> listRuleLogics = new ArrayList<>();
        listRuleLogics.add("condition_0");
        List<String> listConditionsData = new ArrayList<>();
        listConditionsData.add("waf.alarm.level', '>', '3");
        List<ConditionItem> listRuleConditions = new ArrayList<>();
        listRuleConditions.add(
            new ConditionItem()
                .withName("condition_0")
                .withDetail("123")
                .withData(listConditionsData)
        );
        ConditionInfo rulebody = new ConditionInfo();
        rulebody.withExpressionType("common")
            .withConditions(listRuleConditions)
            .withLogics(listRuleLogics);
        body.withRule(rulebody);
        request.withBody(body);
        try {
            CreatePlaybookRuleResponse response = client.createPlaybookRule(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Create a playbook rule named logic1 and expression type.

```
# coding: utf-8
```

```
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreatePlaybookRuleRequest()
        listLogicsRule = [
            "condition_0"
        ]
        listDataConditions = [
            "waf.alarm.level", ">", "3"
        ]
        listConditionsRule = [
            ConditionItem(
                name="condition_0",
                detail="123",
                data=listDataConditions
            )
        ]
        rulebody = ConditionInfo(
            expression_type="common",
            conditions=listConditionsRule,
            logics=listLogicsRule
        )
        request.body = CreateRuleInfo(
            rule=rulebody
        )
        response = client.create_playbook_rule(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Create a playbook rule named logic1 and expression type.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
```

```
variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreatePlaybookRuleRequest{}
    var listLogicsRule = []string{
        "condition_0",
    }
    var listDataConditions = []string{
        "waf.alarm.level', '>', '3",
    }
    nameConditions:= "condition_0"
    detailConditions:= "123"
    var listConditionsRule = []model.ConditionItem{
        {
            Name: &nameConditions,
            Detail: &detailConditions,
            Data: &listDataConditions,
        },
    }
    expressionTypeRule:= "common"
    rulebody := &model.ConditionInfo{
        ExpressionType: &expressionTypeRule,
        Conditions: &listConditionsRule,
        Logics: &listLogicsRule,
    }
    request.Body = &model.CreateRuleInfo{
        Rule: rulebody,
    }
    response, err := client.CreatePlaybookRule(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

## Error Codes

See **Error Codes**.

# 4.7.4 Updating a Playbook Rule

## Function

Updating a Playbook Rule

## Calling Method

For details, see **Calling APIs**.

## URI

PUT /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/rules/{rule_id}

**Table 4-539** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| version_id | Yes | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |
| rule_id | Yes | String | Playbook rule ID.<br>Minimum: **36**<br>Maximum: **36** |

## Request Parameters

**Table 4-540** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-541** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| rule | No | **ConditionInfo** object | Details of playbook triggering rules |

**Table 4-542** ConditionInfo

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| expression_type | No | String | Expression type. This parameter is mandatory for incident-triggered playbooks. The default value is common.<br>Minimum: **0**<br>Maximum: **64** |
| conditions | No | Array of **ConditionItem** objects | Triggering conditions. This parameter is mandatory for incident-triggered playbooks.<br>Array Length: **0 - 99** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| logics | No | Array of strings | Conditional logic combinations. This parameter is mandatory for incident-triggered playbooks.<br>Minimum: **0**<br>Maximum: **64**<br>Array Length: **0 - 99** |
| cron | No | String | Cron expression (scheduled tasks). This parameter is mandatory for scheduled playbooks.<br>Minimum: **0**<br>Maximum: **64** |
| schedule_type | No | String | Scheduled task repetition type. The value can be second, hour, day, or week. This parameter is mandatory for scheduled playbooks.<br>Minimum: **0**<br>Maximum: **64** |
| start_type | No | String | Playbook execution type. The value can be IMMEDIATELY or CUSTOM. This parameter is mandatory for scheduled playbooks.<br>Minimum: **0**<br>Maximum: **64** |
| end_type | No | String | Playbook execution termination type. - FOREVER -- The playbook is executed all the time. - CUSTOM -- The playbook stops at a customized time. This parameter is mandatory for scheduled playbooks.<br>Minimum: **0**<br>Maximum: **64** |
| end_time | No | String | End time of a scheduled task. This parameter is mandatory for scheduled playbooks.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| repeat_range | No | String | Execution time range, for example, 2021-01-30T23:00:00Z+0800. This parameter is mandatory for scheduled playbooks.<br>Minimum: **0**<br>Maximum: **64** |
| only_once | No | Boolean | Whether the operation is performed only once. This parameter is mandatory for scheduled playbooks. |
| execution_type | No | String | Execution queue type (PARALLEL -- The new task runs in parallel with the previous task). This parameter is mandatory for scheduled playbooks.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-543** ConditionItem

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| name | No | String | Condition name.<br>Minimum: **0**<br>Maximum: **64** |
| detail | No | String | Condition details.<br>Minimum: **0**<br>Maximum: **1028** |
| data | No | Array of strings | Condition expression data.<br>Minimum: **0**<br>Maximum: **2048**<br>Array Length: **0 - 99** |

## Response Parameters

**Status code: 200**

**Table 4-544** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-545** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Error Message<br>Minimum: **1**<br>Maximum: **32** |
| data | **RuleInfo** object | Playbook triggering specifications information. |

**Table 4-546** RuleInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Rule ID.<br>Minimum: **32**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| rule | String | Trigger rule.<br>Minimum: **0**<br>Maximum: **128** |

**Status code: 400**

**Table 4-547** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-548** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Update a playbook rule named logic1 and supporting all expression types.

```
{
  "rule" : {
    "expression_type" : "common",
    "conditions" : [ {
      "name" : "condition_0",
      "detail" : "123",
      "data" : [ "waf.alarm.level', '>', '3" ]
    } ],
    "logics" : "[\"condition_0\"]"
  }
}
```

## Example Responses

**Status code: 200**

Response parameters when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "rule" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Update a playbook rule named logic1 and supporting all expression types.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
```

```
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class UpdatePlaybookRuleSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdatePlaybookRuleRequest request = new UpdatePlaybookRuleRequest();
        ModifyRuleInfo body = new ModifyRuleInfo();
        List<String> listConditionsData = new ArrayList<>();
        listConditionsData.add("waf.alarm.level', '>', '3");
        List<ConditionItem> listRuleConditions = new ArrayList<>();
        listRuleConditions.add(
            new ConditionItem()
                .withName("condition_0")
                .withDetail("123")
                .withData(listConditionsData)
        );
        ConditionInfo rulebody = new ConditionInfo();
        rulebody.withExpressionType("common")
            .withConditions(listRuleConditions)
            .withLogics();
        body.withRule(rulebody);
        request.withBody(body);
        try {
            UpdatePlaybookRuleResponse response = client.updatePlaybookRule(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Update a playbook rule named logic1 and supporting all expression types.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
```

```
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdatePlaybookRuleRequest()
        listDataConditions = [
            "waf.alarm.level", ">", "3"
        ]
        listConditionsRule = [
            ConditionItem(
                name="condition_0",
                detail="123",
                data=listDataConditions
            )
        ]
        rulebody = ConditionInfo(
            expression_type="common",
            conditions=listConditionsRule,
        )
        request.body = ModifyRuleInfo(
            rule=rulebody
        )
        response = client.update_playbook_rule(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Update a playbook rule named logic1 and supporting all expression types.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
```

```
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdatePlaybookRuleRequest{}
    var listDataConditions = []string{
        "waf.alarm.level', '>', '3",
    }
    nameConditions:= "condition_0"
    detailConditions:= "123"
    var listConditionsRule = []model.ConditionItem{
        {
            Name: &nameConditions,
            Detail: &detailConditions,
            Data: &listDataConditions,
        },
    }
    expressionTypeRule:= "common"
    rulebody := &model.ConditionInfo{
        ExpressionType: &expressionTypeRule,
        Conditions: &listConditionsRule,
    }
    request.Body = &model.ModifyRuleInfo{
        Rule: rulebody,
    }
    response, err := client.UpdatePlaybookRule(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response parameters when the request is successful. |
| 400 | Response parameters when the request failed. |

## Error Codes

See **Error Codes**.

# 4.8 Playbook Instance Management

# 4.8.1 Querying the Playbook Instance List

## Function

Querying the Playbook Instance List

## Calling Method

For details, see **Calling APIs**.

## URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances

**Table 4-549** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

**Table 4-550** Query Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| status | No | String | Playbook instance status. (RUNNING--Running, FINISHED--Successful, Failed--Failed, Retrying--Retrying, Terminated--Terminated)<br>Minimum: **0**<br>Maximum: **64** |
| name | No | String | Instance name.<br>Minimum: **0**<br>Maximum: **64** |
| playbook_name | No | String | Playbook name.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| dataclass_name | No | String | Data class name.<br>Minimum: **0**<br>Maximum: **64** |
| dataobject_name | No | String | Data object name.<br>Minimum: **0**<br>Maximum: **64** |
| trigger_type | No | String | Triggering type. TIMER indicates scheduled triggering, and EVENT indicates event triggering.<br>Minimum: **0**<br>Maximum: **64** |
| from_date | No | String | Start time.<br>Minimum: **32**<br>Maximum: **36** |
| to_date | No | String | Query end time<br>Minimum: **32**<br>Maximum: **36** |
| limit | Yes | Integer | The maximum number of records can be returned on each page for a pagination query. The value starts from 1.<br>Minimum: **1**<br>Maximum: **999999** |
| offset | Yes | Integer | Indicates the page number. Start position of the query result. The value starts from 0.<br>Minimum: **0**<br>Maximum: **999999** |

## Request Parameters

**Table 4-551** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-552** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-553** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| count | Integer | Total<br>Minimum: **0**<br>Maximum: **99999** |
| instances | Array of **PlaybookInstanceInfo** objects | Playbook instance list information.<br>Array Length: **0 - 100** |

**Table 4-554** PlaybookInstanceInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook instance ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Playbook instance name.<br>Minimum: **0**<br>Maximum: **1024** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| playbook | **PlaybookInfoRef** object | Playbook information. |
| dataclass | **DataclassInfoRef** object | Data Information |
| dataobject | **DataobjectInfo** object | Data object details. |
| status | String | Playbook instance status.(RUNNING--Running, FINISHED--Successful, Failed--Failed, Retrying--Retrying, Terminated--Terminated)<br>Minimum: **32**<br>Maximum: **64** |
| trigger_type | String | Triggering type. TIMER indicates scheduled triggering, and EVENT indicates event triggering.<br>Minimum: **0**<br>Maximum: **64** |
| start_time | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |
| end_time | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-555** PlaybookInfoRef

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook ID.<br>Minimum: **32**<br>Maximum: **64** |
| version_id | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Name.<br>Minimum: **32**<br>Maximum: **64** |
| version | String | Version.<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-556** DataclassInfoRef

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Data class ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Data class name.<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-557** DataobjectInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | ID<br>Minimum: **32**<br>Maximum: **64** |
| create_time | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| update_time | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| dataclass_id | String | Data class ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Name.<br>Minimum: **0**<br>Maximum: **1024** |
| content | String | Data content.<br>Minimum: **0**<br>Maximum: **4096** |

**Status code: 400**

**Table 4-558** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-559** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "count" : 41,
  "instances" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook" : {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "version_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "version" : "v1.1.1"
    },
    "dataclass" : {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "dataobject" : {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "status" : "TERMINATED",
    "trigger_type" : "string",
    "start_time" : "2021-01-30T23:00:00Z+0800",
    "end_time" : "2021-01-30T23:00:00Z+0800"
  } ]
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListPlaybookInstancesSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
```

```
        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListPlaybookInstancesRequest request = new ListPlaybookInstancesRequest();
        request.withStatus("<status>");
        request.withName("<name>");
        request.withPlaybookName("<playbook_name>");
        request.withDataclassName("<dataclass_name>");
        request.withDataobjectName("<dataobject_name>");
        request.withTriggerType("<trigger_type>");
        request.withFromDate("<from_date>");
        request.withToDate("<to_date>");
        request.withLimit(<limit>);
        request.withOffset(<offset>);
        try {
            ListPlaybookInstancesResponse response = client.listPlaybookInstances(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListPlaybookInstancesRequest()
        request.status = "<status>"
        request.name = "<name>"
        request.playbook_name = "<playbook_name>"
        request.dataclass_name = "<dataclass_name>"
        request.dataobject_name = "<dataobject_name>"
        request.trigger_type = "<trigger_type>"
```

```
        request.from_date = "<from_date>"
        request.to_date = "<to_date>"
        request.limit = <limit>
        request.offset = <offset>
        response = client.list_playbook_instances(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListPlaybookInstancesRequest{}
    statusRequest:= "<status>"
    request.Status = &statusRequest
    nameRequest:= "<name>"
    request.Name = &nameRequest
    playbookNameRequest:= "<playbook_name>"
    request.PlaybookName = &playbookNameRequest
    dataclassNameRequest:= "<dataclass_name>"
    request.DataclassName = &dataclassNameRequest
    dataobjectNameRequest:= "<dataobject_name>"
    request.DataobjectName = &dataobjectNameRequest
    triggerTypeRequest:= "<trigger_type>"
    request.TriggerType = &triggerTypeRequest
    fromDateRequest:= "<from_date>"
    request.FromDate = &fromDateRequest
    toDateRequest:= "<to_date>"
    request.ToDate = &toDateRequest
    request.Limit = int32(<limit>)
    request.Offset = int32(<offset>)
    response, err := client.ListPlaybookInstances(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
```

```
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

## Error Codes

See **Error Codes**.

# 4.8.2 Querying Playbook Instance Details

## Function

Show playbook instance

## Calling Method

For details, see **Calling APIs**.

## URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/{instance_id}

**Table 4-560** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| instance_id | Yes | String | instance _id<br>Minimum: **36**<br>Maximum: **36** |

## Request Parameters

**Table 4-561** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-562** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-563** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook instance ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Playbook instance name.<br>Minimum: **0**<br>Maximum: **1024** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| playbook | **PlaybookInfoRef** object | Playbook information. |
| dataclass | **DataclassInfoRef** object | Data Information |
| dataobject | **DataobjectInfo** object | Data object details. |
| status | String | Playbook instance status.(RUNNING--Running, FINISHED--Successful, Failed--Failed, Retrying--Retrying, Terminated--Terminated)<br>Minimum: **32**<br>Maximum: **64** |
| trigger_type | String | Triggering type. TIMER indicates scheduled triggering, and EVENT indicates event triggering.<br>Minimum: **0**<br>Maximum: **64** |
| start_time | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |
| end_time | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-564** PlaybookInfoRef

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook ID.<br>Minimum: **32**<br>Maximum: **64** |
| version_id | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Name.<br>Minimum: **32**<br>Maximum: **64** |
| version | String | Version.<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-565** DataclassInfoRef

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Data class ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Data class name.<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-566** DataobjectInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | ID<br>Minimum: **32**<br>Maximum: **64** |
| create_time | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| update_time | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| dataclass_id | String | Data class ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Name.<br>Minimum: **0**<br>Maximum: **1024** |
| content | String | Data content.<br>Minimum: **0**<br>Maximum: **4096** |

**Status code: 400**

**Table 4-567** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-568** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Instance Informations

```
{
  "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "name" : "MyXXX",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "playbook" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1"
  },
  "dataclass" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  },
  "dataobject" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  },
  "status" : "TERMINATED",
  "trigger_type" : "string",
  "start_time" : "2021-01-30T23:00:00Z+0800",
  "end_time" : "2021-01-30T23:00:00Z+0800"
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowPlaybookInstanceSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);
```

```
        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPlaybookInstanceRequest request = new ShowPlaybookInstanceRequest();
        try {
            ShowPlaybookInstanceResponse response = client.showPlaybookInstance(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowPlaybookInstanceRequest()
        response = client.show_playbook_instance(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)
```

```
func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowPlaybookInstanceRequest{}
    response, err := client.ShowPlaybookInstance(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Instance Informations |
| 400 | Error response |

## Error Codes

See **Error Codes**.

# 4.8.3 Operation Playbook Instance

## Function

Operation Playbook Instance

## Calling Method

For details, see **Calling APIs**.

## URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/{instance_id}/operation

**Table 4-569** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| instance_id | Yes | String | Playbook instance ID.<br>Minimum: **36**<br>Maximum: **36** |

## Request Parameters

**Table 4-570** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-571** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| operation | No | String | Operation type Retry Retry termination -- TERMINATE<br>Minimum: **0**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-572** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-573** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook instance ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Playbook instance name.<br>Minimum: **0**<br>Maximum: **1024** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| playbook | **PlaybookInfoRef** object | Playbook information. |
| dataclass | **DataclassInfoRef** object | Data Information |
| dataobject | **DataobjectInfo** object | Data object details. |

| Parameter | Type | Description |
| --- | --- | --- |
| status | String | Playbook instance status.(RUNNING--Running, FINISHED--Successful, Failed--Failed, Retrying--Retrying, Terminated--Terminated)<br>Minimum: **32**<br>Maximum: **64** |
| trigger_type | String | Triggering type. TIMER indicates scheduled triggering, and EVENT indicates event triggering.<br>Minimum: **0**<br>Maximum: **64** |
| start_time | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |
| end_time | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-574** PlaybookInfoRef

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook ID.<br>Minimum: **32**<br>Maximum: **64** |
| version_id | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Name.<br>Minimum: **32**<br>Maximum: **64** |
| version | String | Version.<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-575** DataclassInfoRef

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Data class ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Data class name.<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-576** DataobjectInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | ID<br>Minimum: **32**<br>Maximum: **64** |
| create_time | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **64** |
| dataclass_id | String | Data class ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Name.<br>Minimum: **0**<br>Maximum: **1024** |
| content | String | Data content.<br>Minimum: **0**<br>Maximum: **4096** |

**Status code: 400**

**Table 4-577** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-578** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Retrying All Playbook Instances.

```
{
  "operation" : "RETRY"
}
```

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "name" : "MyXXX",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "playbook" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1"
  },
  "dataclass" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  },
  "dataobject" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  },
  "status" : "TERMINATED",
  "trigger_type" : "string",
  "start_time" : "2021-01-30T23:00:00Z+0800",
  "end_time" : "2021-01-30T23:00:00Z+0800"
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Retrying All Playbook Instances.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ChangePlaybookInstanceSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ChangePlaybookInstanceRequest request = new ChangePlaybookInstanceRequest();
        OperationPlaybookInfo body = new OperationPlaybookInfo();
        body.withOperation("RETRY");
        request.withBody(body);
        try {
            ChangePlaybookInstanceResponse response = client.changePlaybookInstance(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Retrying All Playbook Instances.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
```

```
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ChangePlaybookInstanceRequest()
        request.body = OperationPlaybookInfo(
            operation="RETRY"
        )
        response = client.change_playbook_instance(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Retrying All Playbook Instances.

```
package main

import (
 "fmt"
 "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
 "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ChangePlaybookInstanceRequest{}
    operationOperationPlaybookInfo:= "RETRY"
```

```
    request.Body = &model.OperationPlaybookInfo{
        Operation: &operationOperationPlaybookInfo,
    }
    response, err := client.ChangePlaybookInstance(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

## Error Codes

See **Error Codes**.

# 4.8.4 Querying the Playbook Topology

## Function

Querying the Playbook Topology

## Calling Method

For details, see **Calling APIs**.

## URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/{instance_id}/topology

**Table 4-579** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| instance_id | Yes | String | Playbook instance ID.<br>Minimum: **36**<br>Maximum: **36** |

## Request Parameters

**Table 4-580** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-581** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-582** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| count | Integer | Total<br>Minimum: **0**<br>Maximum: **99999** |
| action_instances | Array of **ActionInstanceInfo** objects | Incident instance list.<br>Array Length: **0 - 100** |

**Table 4-583** ActionInstanceInfo

| Parameter | Type | Description |
| --- | --- | --- |
| action | **ActionInfo** object | Playbook workflows. |
| instance_log | **AuditLogInfo** object | Playbook instance review information. |

**Table 4-584** ActionInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook workflow ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Workflow name.<br>Minimum: **0**<br>Maximum: **1024** |
| description | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |
| action_type | String | Workflow type.<br>Minimum: **0**<br>Maximum: **64** |
| action_id | String | Workflow ID.<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| playbook_id | String | Playbook ID.<br>Minimum: **0**<br>Maximum: **64** |
| playbook_version_id | String | Playbook version ID.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-585** AuditLogInfo

| Parameter | Type | Description |
| --- | --- | --- |
| instance_type | String | Instance type (AOP_WORKFLOW for workflows, SCRIPT for scripts, and PLAYBOOK for playbooks).<br>Minimum: **0**<br>Maximum: **64** |
| action_id | String | Workflow ID.<br>Minimum: **0**<br>Maximum: **1028** |
| action_name | String | Workflow name.<br>Minimum: **0**<br>Maximum: **64** |
| instance_id | String | Instance ID.<br>Minimum: **0**<br>Maximum: **1028** |
| parent_instance_id | String | Instance ID of the parent node.<br>Minimum: **0**<br>Maximum: **64** |
| log_level | String | Log Level<br>Minimum: **0**<br>Maximum: **1028** |
| input | String | Input.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| output | String | Output.<br>Minimum: **0**<br>Maximum: **1028** |
| error_msg | String | Error Message<br>Minimum: **0**<br>Maximum: **64** |
| start_time | String | Start time.<br>Minimum: **0**<br>Maximum: **1028** |
| end_time | String | End time.<br>Minimum: **0**<br>Maximum: **64** |
| status | String | Status. (RUNNING, FINISHED, FAILED, RETRYING, and TERMINATED)<br>Minimum: **0**<br>Maximum: **1028** |
| trigger_type | String | Triggering type. TIMER indicates scheduled triggering, and EVENT indicates event triggering.<br>Minimum: **0**<br>Maximum: **1028** |

**Status code: 400**

**Table 4-586** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-587** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Response when the request is successful.


```
{
  "count" : 41,
  "action_instances" : [ {
    "action" : {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "MyXXX",
      "description" : "This my XXXX",
      "action_type" : "Workflow",
      "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "playbook_id" : "string",
      "playbook_version_id" : "string",
      "project_id" : "string"
    },
    "instance_log" : {
      "instance_type" : "APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG",
      "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "action_name" : "DisabledIp",
      "instance_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "parent_instance_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "log_level" : "DEBUG INFO WARN",
      "input" : "input",
      "output" : "output",
      "error_msg" : "error_msg",
      "start_time" : "2021-01-30T23:00:00Z",
      "end_time" : "2021-01-31T23:00:00Z",
      "status" : "CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED",
      "trigger_type" : "DEBUG, TIMER, EVENT, MANUAL"
    }
  } ]
}
```


## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
```

```
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowPlaybookTopologySolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPlaybookTopologyRequest request = new ShowPlaybookTopologyRequest();
        try {
            ShowPlaybookTopologyResponse response = client.showPlaybookTopology(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowPlaybookTopologyRequest()
```

```
        response = client.show_playbook_topology(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowPlaybookTopologyRequest{}
    response, err := client.ShowPlaybookTopology(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

## Error Codes

See **Error Codes**.

# 4.8.5 Querying Playbook Instance Audit Logs

## Function

Querying Playbook Instance Audit Logs

## Calling Method

For details, see **Calling APIs**.

## URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/auditlogs

**Table 4-588** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

**Table 4-589** Query Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| offset | Yes | Long | offset<br>Minimum: **0**<br>Maximum: **9223372036854775807** |
| limit | Yes | Long | limit<br>Minimum: **10**<br>Maximum: **50** |
| sort_key | No | String | sort_key<br>Minimum: **1**<br>Maximum: **256** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| sort_dir | No | String | sort_dir. asc, desc<br>Enumeration values:<br>• **asc**<br>• **desc** |

## Request Parameters

**Table 4-590** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-591** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| instance_type | No | String | Instance type (AOP_WORKFLOW for workflows, SCRIPT for scripts, and PLAYBOOK for playbooks).<br>Minimum: **0**<br>Maximum: **64** |
| action_id | No | String | Workflow ID.<br>Minimum: **0**<br>Maximum: **1028** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| action_name | No | String | Workflow name.<br>Minimum: **0**<br>Maximum: **64** |
| instance_id | No | String | Instance ID.<br>Minimum: **0**<br>Maximum: **1028** |
| parent_instance_id | No | String | Instance ID of the parent node.<br>Minimum: **0**<br>Maximum: **64** |
| log_level | No | String | Log Level<br>Minimum: **0**<br>Maximum: **1028** |
| input | No | String | Input.<br>Minimum: **0**<br>Maximum: **64** |
| output | No | String | Output.<br>Minimum: **0**<br>Maximum: **1028** |
| error_msg | No | String | Error Message<br>Minimum: **0**<br>Maximum: **64** |
| start_time | No | String | Start time.<br>Minimum: **0**<br>Maximum: **1028** |
| end_time | No | String | End time.<br>Minimum: **0**<br>Maximum: **64** |
| status | No | String | Status. (RUNNING, FINISHED, FAILED, RETRYING, and TERMINATED)<br>Minimum: **0**<br>Maximum: **1028** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| trigger_type | No | String | Triggering type. TIMER indicates scheduled triggering, and EVENT indicates event triggering.<br>Minimum: **0**<br>Maximum: **1028** |

## Response Parameters

**Status code: 200**

**Table 4-592** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-593** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| count | Integer | Total records.<br>Minimum: **0**<br>Maximum: **99999** |
| audit_logs | Array of **AuditLogInfo** objects | Review response list.<br>Array Length: **0 - 100** |

**Table 4-594** AuditLogInfo

| Parameter | Type | Description |
| --- | --- | --- |
| instance_type | String | Instance type (AOP_WORKFLOW for workflows, SCRIPT for scripts, and PLAYBOOK for playbooks).<br>Minimum: **0**<br>Maximum: **64** |
| action_id | String | Workflow ID.<br>Minimum: **0**<br>Maximum: **1028** |

| Parameter | Type | Description |
| --- | --- | --- |
| action_name | String | Workflow name.<br>Minimum: **0**<br>Maximum: **64** |
| instance_id | String | Instance ID.<br>Minimum: **0**<br>Maximum: **1028** |
| parent_instance_id | String | Instance ID of the parent node.<br>Minimum: **0**<br>Maximum: **64** |
| log_level | String | Log Level<br>Minimum: **0**<br>Maximum: **1028** |
| input | String | Input.<br>Minimum: **0**<br>Maximum: **64** |
| output | String | Output.<br>Minimum: **0**<br>Maximum: **1028** |
| error_msg | String | Error Message<br>Minimum: **0**<br>Maximum: **64** |
| start_time | String | Start time.<br>Minimum: **0**<br>Maximum: **1028** |
| end_time | String | End time.<br>Minimum: **0**<br>Maximum: **64** |
| status | String | Status. (RUNNING, FINISHED, FAILED, RETRYING, and TERMINATED)<br>Minimum: **0**<br>Maximum: **1028** |
| trigger_type | String | Triggering type. TIMER indicates scheduled triggering, and EVENT indicates event triggering.<br>Minimum: **0**<br>Maximum: **1028** |

**Status code: 400**

**Table 4-595** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-596** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Query playbook instance review logs. Details - Instance type - APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG; Workflow ID - 909494e3-558e-46b6-a9eb-07a8e18ca62f; Workflow name - DisabledIp; Instance ID - 909494e3-558e-46b6-a9eb-07a8e18ca62f; Parent instance ID - 909494e3-558e-46b6-a9eb-07a8e18ca62f; Log level - DEBUG, INFO WARN; Input - input; Output - output; Error message - error_msg. Start time - 2021-01-30 23:00:00;End time - 2021-01-31 23:00:00; Status - CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED Trigger type - DEBUG, TIMER, EVENT, or MANUAL.

```
{
  "instance_type" : "APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG",
  "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "action_name" : "DisabledIp",
  "instance_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "parent_instance_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "log_level" : "DEBUG INFO WARN",
  "input" : "input",
  "output" : "output",
  "error_msg" : "error_msg",
  "start_time" : "2021-01-30T23:00:00Z",
  "end_time" : "2021-01-31T23:00:00Z",
  "status" : "CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED",
  "trigger_type" : "DEBUG, TIMER, EVENT, MANUAL"
}
```

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "count" : 41,
  "audit_logs" : [ {
    "instance_type" : "APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG",
    "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "action_name" : "DisabledIp",
    "instance_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "parent_instance_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "log_level" : "DEBUG INFO WARN",
    "input" : "input",
    "output" : "output",
    "error_msg" : "error_msg",
    "start_time" : "2021-01-30T23:00:00Z",
    "end_time" : "2021-01-31T23:00:00Z",
    "status" : "CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED",
    "trigger_type" : "DEBUG, TIMER, EVENT, MANUAL"
  } ]
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Query playbook instance review logs. Details - Instance type - APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG; Workflow ID - 909494e3-558e-46b6-a9eb-07a8e18ca62f; Workflow name - DisabledIp; Instance ID - 909494e3-558e-46b6-a9eb-07a8e18ca62f; Parent instance ID - 909494e3-558e-46b6-a9eb-07a8e18ca62f; Log level - DEBUG, INFO WARN; Input - input; Output - output; Error message - error_msg. Start time - 2021-01-30 23:00:00;End time - 2021-01-31 23:00:00; Status - CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED Trigger type - DEBUG, TIMER, EVENT, or MANUAL.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListPlaybookAuditLogsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
```

```
        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListPlaybookAuditLogsRequest request = new ListPlaybookAuditLogsRequest();
        request.withOffset(<offset>L);
        request.withLimit(<limit>L);
        request.withSortKey("<sort_key>");
        request.withSortDir(ListPlaybookAuditLogsRequest.SortDirEnum.fromValue("<sort_dir>"));
        AuditLogInfo body = new AuditLogInfo();
        body.withTriggerType("DEBUG, TIMER, EVENT, MANUAL");
        body.withStatus("CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED");
        body.withEndTime("2021-01-31T23:00:00Z");
        body.withStartTime("2021-01-30T23:00:00Z");
        body.withErrorMsg("error_msg");
        body.withOutput("output");
        body.withInput("input");
        body.withLogLevel("DEBUG INFO WARN");
        body.withParentInstanceId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withInstanceId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withActionName("DisabledIp");
        body.withActionId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withInstanceType("APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG");
        request.withBody(body);
        try {
            ListPlaybookAuditLogsResponse response = client.listPlaybookAuditLogs(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Query playbook instance review logs. Details - Instance type - APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG; Workflow ID - 909494e3-558e-46b6-a9eb-07a8e18ca62f; Workflow name - DisabledIp; Instance ID - 909494e3-558e-46b6-a9eb-07a8e18ca62f; Parent instance ID - 909494e3-558e-46b6-a9eb-07a8e18ca62f; Log level - DEBUG, INFO WARN; Input - input; Output - output; Error message - error_msg. Start time - 2021-01-30 23:00:00;End time - 2021-01-31 23:00:00; Status - CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED Trigger type - DEBUG, TIMER, EVENT, or MANUAL.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
```

```
risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListPlaybookAuditLogsRequest()
        request.offset = <offset>
        request.limit = <limit>
        request.sort_key = "<sort_key>"
        request.sort_dir = "<sort_dir>"
        request.body = AuditLogInfo(
            trigger_type="DEBUG, TIMER, EVENT, MANUAL",
            status="CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED",
            end_time="2021-01-31T23:00:00Z",
            start_time="2021-01-30T23:00:00Z",
            error_msg="error_msg",
            output="output",
            input="input",
            log_level="DEBUG INFO WARN",
            parent_instance_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            instance_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            action_name="DisabledIp",
            action_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            instance_type="APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG"
        )
        response = client.list_playbook_audit_logs(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Query playbook instance review logs. Details - Instance type - APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG; Workflow ID - 909494e3-558e-46b6-a9eb-07a8e18ca62f; Workflow name - DisabledIp; Instance ID - 909494e3-558e-46b6-a9eb-07a8e18ca62f; Parent instance ID - 909494e3-558e-46b6-a9eb-07a8e18ca62f; Log level - DEBUG, INFO WARN; Input - input; Output - output; Error message - error_msg. Start time - 2021-01-30 23:00:00;End time - 2021-01-31 23:00:00; Status - CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED Trigger type - DEBUG, TIMER, EVENT, or MANUAL.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
```

```
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListPlaybookAuditLogsRequest{}
    request.Offset = int64(<offset>)
    request.Limit = int64(<limit>)
    sortKeyRequest:= "<sort_key>"
    request.SortKey = &sortKeyRequest
    sortDirRequest:= model.GetListPlaybookAuditLogsRequestSortDirEnum().<SORT_DIR>
    request.SortDir = &sortDirRequest
    triggerTypeAuditLogInfo:= "DEBUG, TIMER, EVENT, MANUAL"
    statusAuditLogInfo:= "CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED"
    endTimeAuditLogInfo:= "2021-01-31T23:00:00Z"
    startTimeAuditLogInfo:= "2021-01-30T23:00:00Z"
    errorMsgAuditLogInfo:= "error_msg"
    outputAuditLogInfo:= "output"
    inputAuditLogInfo:= "input"
    logLevelAuditLogInfo:= "DEBUG INFO WARN"
    parentInstanceIdAuditLogInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    instanceIdAuditLogInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    actionNameAuditLogInfo:= "DisabledIp"
    actionIdAuditLogInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    instanceTypeAuditLogInfo:= "APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG"
    request.Body = &model.AuditLogInfo{
        TriggerType: &triggerTypeAuditLogInfo,
        Status: &statusAuditLogInfo,
        EndTime: &endTimeAuditLogInfo,
        StartTime: &startTimeAuditLogInfo,
        ErrorMsg: &errorMsgAuditLogInfo,
        Output: &outputAuditLogInfo,
        Input: &inputAuditLogInfo,
        LogLevel: &logLevelAuditLogInfo,
        ParentInstanceId: &parentInstanceIdAuditLogInfo,
        InstanceId: &instanceIdAuditLogInfo,
        ActionName: &actionNameAuditLogInfo,
        ActionId: &actionIdAuditLogInfo,
        InstanceType: &instanceTypeAuditLogInfo,
    }
    response, err := client.ListPlaybookAuditLogs(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

### Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

### Error Codes

See **Error Codes**.

# 4.9 Playbook Approval Management

## 4.9.1 Reviewing a Playbook

### Function

Reviewing a Playbook

### Calling Method

For details, see **Calling APIs**.

### URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/approval

**Table 4-597** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| version_id | Yes | String | Version ID<br>Minimum: **32**<br>Maximum: **64** |

## Request Parameters

**Table 4-598** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/ json;charset=UTF-8<br>Default: **application/ json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-599** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| result | No | String | PASS or UN_PASS<br>Minimum: **32**<br>Maximum: **64** |
| content | No | String | Review Comments<br>Minimum: **32**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-600** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-601** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Response message.<br>Minimum: **1**<br>Maximum: **32** |
| data | **ApproveOpinionDetail** object | Review details. |

**Table 4-602** ApproveOpinionDetail

| Parameter | Type | Description |
| --- | --- | --- |
| result | String | Review result.<br>Minimum: **0**<br>Maximum: **64** |
| content | String | Review content.<br>Minimum: **0**<br>Maximum: **1028** |

**Status code: 400**

**Table 4-603** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-604** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Review a playbook. The review result is PASS and the review comments are xxxxx.

```
{
  "result" : "PASS",
  "content" : "xxxxx"
}
```

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "result" : "PASS",
    "content" : "need modify"
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Review a playbook. The review result is PASS and the review comments are xxxxx.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class CreatePlaybookApproveSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
```

```
        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreatePlaybookApproveRequest request = new CreatePlaybookApproveRequest();
        ApprovePlaybookInfo body = new ApprovePlaybookInfo();
        body.withContent("xxxxx");
        body.withResult("PASS");
        request.withBody(body);
        try {
            CreatePlaybookApproveResponse response = client.createPlaybookApprove(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Review a playbook. The review result is PASS and the review comments are xxxxx.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreatePlaybookApproveRequest()
        request.body = ApprovePlaybookInfo(
            content="xxxxx",
            result="PASS"
        )
        response = client.create_playbook_approve(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
```

```
        print(e.error_code)
        print(e.error_msg)
```

## Go

Review a playbook. The review result is PASS and the review comments are xxxxx.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreatePlaybookApproveRequest{}
    contentApprovePlaybookInfo:= "xxxxx"
    resultApprovePlaybookInfo:= "PASS"
    request.Body = &model.ApprovePlaybookInfo{
        Content: &contentApprovePlaybookInfo,
        Result: &resultApprovePlaybookInfo,
    }
    response, err := client.CreatePlaybookApprove(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |

| Status Code | Description |
| --- | --- |
| 400 | Response when the request failed. |

## Error Codes

See **Error Codes**.

# 4.9.2 Querying Playbook Review Result

## Function

Querying Playbook Review Result

## Calling Method

For details, see **Calling APIs**.

## URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/approval

**Table 4-605** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

**Table 4-606** Query Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| resource_id | No | String | Resource ID.<br>Minimum: **0**<br>Maximum: **64** |
| approve_type | No | String | Review type. (PLAYBOOK or AOP_WORKFLOW)<br>Minimum: **0**<br>Maximum: **64** |

## Request Parameters

**Table 4-607** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-608** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-609** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Response message.<br>Minimum: **1**<br>Maximum: **32** |

| Parameter | Type | Description |
| --- | --- | --- |
| data | Array of **ApproveOpinionDetail** objects | Playbook review details.<br>Array Length: **0 - 99** |

**Table 4-610** ApproveOpinionDetail

| Parameter | Type | Description |
| --- | --- | --- |
| result | String | Review result.<br>Minimum: **0**<br>Maximum: **64** |
| content | String | Review content.<br>Minimum: **0**<br>Maximum: **1028** |

**Status code: 400**

**Table 4-611** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-612** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : [ {
    "result" : "PASS",
    "content" : "need modify"
  } ]
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListPlaybookApprovesSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListPlaybookApprovesRequest request = new ListPlaybookApprovesRequest();
        request.withResourceId("<resource_id>");
        request.withApproveType("<approve_type>");
        try {
            ListPlaybookApprovesResponse response = client.listPlaybookApproves(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
```

```
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListPlaybookApprovesRequest()
        request.resource_id = "<resource_id>"
        request.approve_type = "<approve_type>"
        response = client.list_playbook_approves(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
```

```
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListPlaybookApprovesRequest{}
    resourceIdRequest:= "<resource_id>"
    request.ResourceId = &resourceIdRequest
    approveTypeRequest:= "<approve_type>"
    request.ApproveType = &approveTypeRequest
    response, err := client.ListPlaybookApproves(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

### More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

### Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

### Error Codes

See **Error Codes**.

# 4.10 Playbook Action Management

## 4.10.1 Querying the Playbook Workflow

### Function

Querying the Playbook Workflow List

### Calling Method

For details, see **Calling APIs**.

### URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/actions

**Table 4-613** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| version_id | Yes | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-614** Query Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| limit | Yes | Integer | The maximum number of records can be returned on each page for a pagination query. The value starts from 1.<br>Minimum: **0**<br>Maximum: **999999** |
| offset | Yes | Integer | Indicates the page number. Start position of the query result. The value starts from 0.<br>Minimum: **1**<br>Maximum: **999999** |

## Request Parameters

**Table 4-615** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-616** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-617** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Error Message<br>Minimum: **1**<br>Maximum: **32** |
| total | Integer | Total<br>Minimum: **0**<br>Maximum: **99999** |
| size | Integer | Number of records displayed on each page.<br>Minimum: **0**<br>Maximum: **9999** |
| page | Integer | Current page number.<br>Minimum: **0**<br>Maximum: **100** |

| Parameter | Type | Description |
| --- | --- | --- |
| data | Array of **ActionInfo** objects | Playbook workflow list.<br>Array Length: **0 - 100** |

**Table 4-618** ActionInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook workflow ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Workflow name.<br>Minimum: **0**<br>Maximum: **1024** |
| description | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |
| action_type | String | Workflow type.<br>Minimum: **0**<br>Maximum: **64** |
| action_id | String | Workflow ID.<br>Minimum: **32**<br>Maximum: **64** |
| playbook_id | String | Playbook ID.<br>Minimum: **0**<br>Maximum: **64** |
| playbook_version_id | String | Playbook version ID.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **0**<br>Maximum: **64** |

**Status code: 400**

**Table 4-619** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-620** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Response parameters when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message",
  "total" : 41,
  "size" : 3,
  "page" : 10,
  "data" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "description" : "This my XXXX",
    "action_type" : "Workflow",
    "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook_id" : "string",
    "playbook_version_id" : "string",
    "project_id" : "string"
  } ]
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;
```

```
import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListPlaybookActionsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListPlaybookActionsRequest request = new ListPlaybookActionsRequest();
        request.withLimit(<limit>);
        request.withOffset(<offset>);
        try {
            ListPlaybookActionsResponse response = client.listPlaybookActions(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \
```

```
    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListPlaybookActionsRequest()
        request.limit = <limit>
        request.offset = <offset>
        response = client.list_playbook_actions(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListPlaybookActionsRequest{}
    request.Limit = int32(<limit>)
    request.Offset = int32(<offset>)
    response, err := client.ListPlaybookActions(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

### Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response parameters when the request is successful. |
| 400 | Response parameters when the request failed. |

### Error Codes

See **Error Codes**.

## 4.10.2 Creating a Playbook Action

### Function

Creating a Playbook Action

### Calling Method

For details, see **Calling APIs**.

### URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/actions

**Table 4-621** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| version_id | Yes | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |

## Request Parameters

**Table 4-622** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-623** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| [items] | Yes | Array of **CreateAction** objects | Creating a Playbook Version |

**Table 4-624** CreateAction

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| name | No | String | Name.<br>Minimum: **0**<br>Maximum: **1024** |
| description | No | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |
| action_type | Yes | String | Type. The default value is AOP_WORKFLOW.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| action_id | Yes | String | Playbook workflow ID.<br>Minimum: **32**<br>Maximum: **64** |
| sort_order | No | String | Sort By<br>Minimum: **0**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-625** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-626** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Error message<br>Minimum: **1**<br>Maximum: **32** |
| data | Array of **ActionInfo** objects | list of informations of playbook action<br>Array Length: **0 - 100** |

**Table 4-627** ActionInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook workflow ID.<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| name | String | Workflow name.<br>Minimum: **0**<br>Maximum: **1024** |
| description | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |
| action_type | String | Workflow type.<br>Minimum: **0**<br>Maximum: **64** |
| action_id | String | Workflow ID.<br>Minimum: **32**<br>Maximum: **64** |
| playbook_id | String | Playbook ID.<br>Minimum: **0**<br>Maximum: **64** |
| playbook_version_id | String | Playbook version ID.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **0**<br>Maximum: **64** |

**Status code: 400**

**Table 4-628** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-629** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Create a playbook workflow. Workflow name is MyXXX; Description is This my XXXX; Workflow type is aopworkflow; Workflow ID is 909494e3-558e-46b6-a9eb-07a8e18ca62f; Sorted by string.

```
[ {
  "name" : "MyXXX",
  "description" : "This my XXXX",
  "action_type" : "aopworkflow",
  "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "sort_order" : "string"
} ]
```

## Example Responses

**Status code: 200**

Response when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "description" : "This my XXXX",
    "action_type" : "Workflow",
    "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook_id" : "string",
    "playbook_version_id" : "string",
    "project_id" : "string"
  } ]
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Create a playbook workflow. Workflow name is MyXXX; Description is This my XXXX; Workflow type is aopworkflow; Workflow ID is 909494e3-558e-46b6-a9eb-07a8e18ca62f; Sorted by string.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
```

```
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class CreatePlaybookActionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreatePlaybookActionRequest request = new CreatePlaybookActionRequest();
        List<CreateAction> listbodyCreateActionInfo = new ArrayList<>();
        listbodyCreateActionInfo.add(
            new CreateAction()
                .withName("MyXXX")
                .withDescription("This my XXXX")
                .withActionType("aopworkflow")
                .withActionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withSortOrder("string")
        );
        request.withBody(listbodyCreateActionInfo);
        try {
            CreatePlaybookActionResponse response = client.createPlaybookAction(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Create a playbook workflow. Workflow name is MyXXX; Description is This my XXXX; Workflow type is aopworkflow; Workflow ID is 909494e3-558e-46b6-a9eb-07a8e18ca62f; Sorted by string.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
```

```
risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreatePlaybookActionRequest()
        listCreateActionInfobody = [
            CreateAction(
                name="MyXXX",
                description="This my XXXX",
                action_type="aopworkflow",
                action_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
                sort_order="string"
            )
        ]
        request.body = listCreateActionInfobody
        response = client.create_playbook_action(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Create a playbook workflow. Workflow name is MyXXX; Description is This my XXXX; Workflow type is aopworkflow; Workflow ID is 909494e3-558e-46b6-a9eb-07a8e18ca62f; Sorted by string.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
```

```
        Build())

    request := &model.CreatePlaybookActionRequest{}
    nameCreateActionInfo:= "MyXXX"
    descriptionCreateActionInfo:= "This my XXXX"
    sortOrderCreateActionInfo:= "string"
    var listCreateActionInfobody = []model.CreateAction{
        {
            Name: &nameCreateActionInfo,
            Description: &descriptionCreateActionInfo,
            ActionType: "aopworkflow",
            ActionId: "909494e3-558e-46b6-a9eb-07a8e18ca62f",
            SortOrder: &sortOrderCreateActionInfo,
        },
    }
    request.Body = &listCreateActionInfobody
    response, err := client.CreatePlaybookAction(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response when the request is successful. |
| 400 | Response when the request failed. |

## Error Codes

See **Error Codes**.

# 4.10.3 Delete Playbook Action

## Function

Delete Playbook Action

## Calling Method

For details, see **Calling APIs**.

## URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/actions/{action_id}

**Table 4-630** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| version_id | Yes | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |
| action_id | Yes | String | Playbook workflow ID.<br>Minimum: **32**<br>Maximum: **64** |

## Request Parameters

**Table 4-631** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-632** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-633** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Response message.<br>Minimum: **1**<br>Maximum: **32** |

**Status code: 400**

**Table 4-634** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-635** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Response parameters when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message"
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class DeletePlaybookActionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeletePlaybookActionRequest request = new DeletePlaybookActionRequest();
        try {
            DeletePlaybookActionResponse response = client.deletePlaybookAction(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeletePlaybookActionRequest()
        response = client.delete_playbook_action(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeletePlaybookActionRequest{}
    response, err := client.DeletePlaybookAction(request)
```

```
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response parameters when the request is successful. |
| 400 | Response parameters when the request failed. |

## Error Codes

See **Error Codes**.

# 4.10.4 Updating a Playbook Workflow

## Function

Updating a Playbook Workflow

## Calling Method

For details, see **Calling APIs**.

## URI

PUT /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/actions/{action_id}

**Table 4-636** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| version_id | Yes | String | Playbook version ID.<br>Minimum: **32**<br>Maximum: **64** |
| action_id | Yes | String | Playbook workflow ID.<br>Minimum: **32**<br>Maximum: **64** |

## Request Parameters

**Table 4-637** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **1**<br>Maximum: **2097152** |
| content-type | Yes | String | application/json;charset=UTF-8<br>Default: **application/json;charset=UTF-8**<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-638** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| name | No | String | Name.<br>Minimum: **0**<br>Maximum: **1024** |
| description | No | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| action_type | No | String | Type. The default value is AOP_WORKFLOW.<br>Minimum: **0**<br>Maximum: **64** |
| action_id | No | String | Playbook workflow ID.<br>Minimum: **32**<br>Maximum: **64** |
| sort_order | No | String | Sort By<br>Minimum: **0**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-639** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-640** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **1**<br>Maximum: **32** |
| message | String | Error message<br>Minimum: **1**<br>Maximum: **32** |
| data | **ActionInfo** object | Playbook workflows. |

**Table 4-641** ActionInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Playbook workflow ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Workflow name.<br>Minimum: **0**<br>Maximum: **1024** |
| description | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |
| action_type | String | Workflow type.<br>Minimum: **0**<br>Maximum: **64** |
| action_id | String | Workflow ID.<br>Minimum: **32**<br>Maximum: **64** |
| playbook_id | String | Playbook ID.<br>Minimum: **0**<br>Maximum: **64** |
| playbook_version_id | String | Playbook version ID.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID.<br>Minimum: **0**<br>Maximum: **64** |

**Status code: 400**

**Table 4-642** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-643** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Update a playbook workflow. Workflow name is MyXXX; Description is This my XXXX; Workflow type is aopworkflow; Workflow ID is 909494e3-558e-46b6-a9eb-07a8e18ca62f; Sorted by string.

```
{
  "name" : "MyXXX",
  "description" : "This my XXXX",
  "action_type" : "aopworkflow",
  "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "sort_order" : "string"
}
```

## Example Responses

**Status code: 200**

Response parameters when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "description" : "This my XXXX",
    "action_type" : "Workflow",
    "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook_id" : "string",
    "playbook_version_id" : "string",
    "project_id" : "string"
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Update a playbook workflow. Workflow name is MyXXX; Description is This my XXXX; Workflow type is aopworkflow; Workflow ID is 909494e3-558e-46b6-a9eb-07a8e18ca62f; Sorted by string.

```
package com.huaweicloud.sdk.test;
```

```
import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class UpdatePlaybookActionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdatePlaybookActionRequest request = new UpdatePlaybookActionRequest();
        ModifyActionInfo body = new ModifyActionInfo();
        body.withSortOrder("string");
        body.withActionId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withActionType("aopworkflow");
        body.withDescription("This my XXXX");
        body.withName("MyXXX");
        request.withBody(body);
        try {
            UpdatePlaybookActionResponse response = client.updatePlaybookAction(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Update a playbook workflow. Workflow name is MyXXX; Description is This my XXXX; Workflow type is aopworkflow; Workflow ID is 909494e3-558e-46b6-a9eb-07a8e18ca62f; Sorted by string.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
```

```
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdatePlaybookActionRequest()
        request.body = ModifyActionInfo(
            sort_order="string",
            action_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            action_type="aopworkflow",
            description="This my XXXX",
            name="MyXXX"
        )
        response = client.update_playbook_action(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Update a playbook workflow. Workflow name is MyXXX; Description is This my XXXX; Workflow type is aopworkflow; Workflow ID is 909494e3-558e-46b6-a9eb-07a8e18ca62f; Sorted by string.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())
```

```
    request := &model.UpdatePlaybookActionRequest{}
    sortOrderModifyActionInfo:= "string"
    actionIdModifyActionInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    actionTypeModifyActionInfo:= "aopworkflow"
    descriptionModifyActionInfo:= "This my XXXX"
    nameModifyActionInfo:= "MyXXX"
    request.Body = &model.ModifyActionInfo{
        SortOrder: &sortOrderModifyActionInfo,
        ActionId: &actionIdModifyActionInfo,
        ActionType: &actionTypeModifyActionInfo,
        Description: &descriptionModifyActionInfo,
        Name: &nameModifyActionInfo,
    }
    response, err := client.UpdatePlaybookAction(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

### More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

### Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response parameters when the request is successful. |
| 400 | Response parameters when the request failed. |

### Error Codes

See **Error Codes**.

# 4.11 Incident Relationship Management

## 4.11.1 Querying the Associated Data Object List

### Function

Querying the Associated Data Object List

### Calling Method

For details, see **Calling APIs**.

## URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/{dataclass_type}/{data_object_id}/{related_dataclass_type}/search

**Table 4-644** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| dataclass_type | Yes | String | Data class to which the associated subject data object belongs. The value is plural in lowercase, for example, "alerts" and "incidents".<br>Minimum: **1**<br>Maximum: **64** |
| data_object_id | Yes | String | ID of the associated data object.<br>Minimum: **32**<br>Maximum: **36** |
| related_dataclass_type | Yes | String | Data class to which the associated subject data object belongs. The value is plural in lowercase, for example, "alerts" and "incidents".<br>Minimum: **1**<br>Maximum: **64** |

## Request Parameters

**Table 4-645** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **0**<br>Maximum: **2097152** |
| content-type | Yes | String | Content type.<br>Default: **application/json;charset=UTF-8**<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-646** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| limit | No | Integer | Number of records displayed on each page.<br>Minimum: **0**<br>Maximum: **1000** |
| offset | No | Integer | Offset<br>Minimum: **0**<br>Maximum: **1000** |
| sort_by | No | String | Sorting field -- create_time \| update_time<br>Minimum: **0**<br>Maximum: **1000** |
| order | No | String | Sort by -- DESC \| ASC<br>Minimum: **0**<br>Maximum: **1000**<br>Enumeration values:<br>• **DESC**<br>• **ASC** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| from_date | No | String | Search start time, for example, 2023-02-20T00:00:00.000Z<br>Minimum: **0**<br>Maximum: **64** |
| to_date | No | String | Search end time, for example, 2023-02-27T23:59:59.999Z<br>Minimum: **0**<br>Maximum: **64** |
| condition | No | **condition** object | Search condition expression. |

**Table 4-647** condition

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| conditions | No | Array of **conditions** objects | Expression list.<br>Array Length: **0 - 999** |
| logics | No | Array of strings | Expression logic.<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 999** |

**Table 4-648** conditions

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| name | No | String | Expression name.<br>Minimum: **0**<br>Maximum: **64** |
| data | No | Array of strings | Expression content list.<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 999** |

## Response Parameters

**Status code: 200**

**Table 4-649** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-650** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Message<br>Minimum: **0**<br>Maximum: **1024** |
| total | Integer | Total number of alerts.<br>Minimum: **0**<br>Maximum: **10000** |
| limit | Integer | Number of records displayed on each page.<br>Minimum: **0**<br>Maximum: **10000** |
| offset | Integer | Offset<br>Minimum: **0**<br>Maximum: **10000** |
| success | Boolean | Successful or not. |
| data | Array of **DataObjectDetail** objects | Alert list.<br>Array Length: **0 - 10000** |

**Table 4-651** DataObjectDetail

| Parameter | Type | Description |
| --- | --- | --- |
| create_time | String | Recording time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |

| Parameter | Type | Description |
| --- | --- | --- |
| data_object | **DataObject** object | Alert entity information. |
| dataclass_ref | **dataclass_ref** object | Data class object. |
| format_version | Integer | Format version.<br>Minimum: **0**<br>Maximum: **999** |
| id | String | Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | String | ID of the current project.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Update time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| version | Integer | Version.<br>Minimum: **0**<br>Maximum: **999** |
| workspace_id | String | ID of the current workspace.<br>Minimum: **0**<br>Maximum: **36** |

**Table 4-652** DataObject

| Parameter | Type | Description |
| --- | --- | --- |
| version | String | Version of the data source of the alert. The value must be one officially released by the Huawei Cloud SSA service.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | String | ID of the account (domain_id) to whom the data is delivered and hosted.<br>Minimum: **0**<br>Maximum: **36** |
| region_id | String | ID of the region where the account to whom the data is delivered and hosted belongs to.<br>Minimum: **0**<br>Maximum: **36** |
| workspace_id | String | ID of the current workspace.<br>Minimum: **0**<br>Maximum: **36** |
| environment | **environment** object | Coordinates of the environment where the alert was generated. |
| datasource | **datasource** object | Source the data is first reported. |
| first_observed_time | String | First discovery time. The format is ISO 8601-YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| last_observed_time | String | First discovery time. The format is ISO 8601-YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

| Parameter | Type | Description |
| --- | --- | --- |
| create_time | String | Recording time. The format is ISO 8601- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| arrive_time | String | Data receiving time. The format is ISO 8601-YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| title | String | Alert title.<br>Minimum: **0**<br>Maximum: **255** |
| description | String | Alert description.<br>Minimum: **0**<br>Maximum: **1024** |
| source_url | String | Alert URL, which points to the page of the current incident description in the data source product.<br>Minimum: **0**<br>Maximum: **1024** |
| count | Integer | Incident occurrences<br>Minimum: **0**<br>Maximum: **999** |
| confidence | Integer | Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or incident. Value range -- 0-100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.<br>Minimum: **0**<br>Maximum: **100** |

| Parameter | Type | Description |
| --- | --- | --- |
| severity | String | Severity level. Value range: Tips \| Low \| Medium \| High \| Fatal Description:<br>• **0**: TIPS: No threats are found.<br>• **1**: LOW: No actions are required for the threat.<br>• **2**: MEDIUM: The threat needs to be handled but is not urgent.<br>• **3**: HIGH: The threat must be handled preferentially.<br>• **4**: FATAL: The threat must be handled immediately to prevent further damage.<br>Minimum: **3**<br>Maximum: **6**<br>Enumeration values:<br>• **Tips**<br>• **Low**<br>• **Medium**<br>• **High**<br>• **Fatal** |
| criticality | Integer | Criticality, which specifies the importance level of the resources involved in an incident. Value range -- 0 to 100. The value 0 indicates that the resource is not critical, and 100 indicates that the resource is critical.<br>Minimum: **0**<br>Maximum: **100** |
| alert_type | **alert_type** object | Alert classification. For details, see the Alert Type Definition. |
| network_list | Array of **network_list** objects | Network Information<br>Array Length: **0 - 999** |
| resource_list | Array of **resource_list** objects | Affected resources.<br>Array Length: **0 - 999** |
| remediation | **remediation** object | Remedy measure. |

| Parameter | Type | Description |
| --- | --- | --- |
| verification_state | String | Verification status, which identifies the accuracy of an incident. The options are as follows: – Unknown – True_Positive – False_Positive Enter Unknown by default.<br>Minimum: **32**<br>Maximum: **64**<br>Enumeration values:<br>• **Unknown**<br>• **True_Positive**<br>• **False_Positive** |
| handle_status | String | Incident handling status. The options are as follows:<br>• Open: enabled.<br>• Block: blocked.<br>• Closed: closed. The default value is Open.<br>Minimum: **4**<br>Maximum: **5**<br>Enumeration values:<br>• **Open**<br>• **Block**<br>• **Closed** |
| sla | Integer | Risk close time -- Set the acceptable risk duration. Unit -- Hour<br>Minimum: **0**<br>Maximum: **999** |
| update_time | String | Update time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the alert occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| close_time | String | Closing time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Timezone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT +8 is used.<br>Minimum: **0**<br>Maximum: **30** |

| Parameter | Type | Description |
| --- | --- | --- |
| ipdrr_phase | String | Period/Handling phase No. Prepartion\| Detection and Analysis\|Containm, Eradication& Recovery\|Post-Incident-Activity<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **Prepartion**<br>• **Detection and Analysis**<br>• **Containm, Eradication& Recovery**<br>• **Post-Incident-Activity** |
| simulation | String | Debugging field.<br>Minimum: **0**<br>Maximum: **64** |
| actor | String | Alert investigator.<br>Minimum: **0**<br>Maximum: **64** |
| owner | String | Owner and service owner.<br>Minimum: **0**<br>Maximum: **64** |
| creator | String | Creator<br>Minimum: **0**<br>Maximum: **64** |
| close_reason | String | Close reason.<br>• False positive.<br>• Resolved<br>• Repeated<br>• Other<br>Minimum: **0**<br>Maximum: **64**<br>Enumeration values:<br>• **False detection**<br>• **Resolved**<br>• **Repeated**<br>• **Other** |
| close_comment | String | Whether to close comment.<br>Minimum: **0**<br>Maximum: **1024** |

| Parameter | Type | Description |
| --- | --- | --- |
| malware | **malware** object | Malware |
| system_info | Object | System information. |
| process | Array of **process** objects | Process information.<br>Array Length: **0 - 999** |
| user_info | Array of **user_info** objects | User Details<br>Array Length: **0 - 999** |
| file_info | Array of **file_info** objects | File Information<br>Array Length: **0 - 999** |

**Table 4-653** environment

| Parameter | Type | Description |
| --- | --- | --- |
| vendor_type | String | Environment provider. The value can be **HWCP**, **HWC**, **AWS**, **Azure**, or **GCP**.<br>Minimum: **0**<br>Maximum: **64** |
| domain_id | String | Tenant ID.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region ID. **global** is returned for global services.<br>Minimum: **0**<br>Maximum: **64** |
| cross_workspace_id | String | ID of the source workspace for the data delivery. If the source workspace ID is null, then the destination workspace account ID is used.<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Project ID. The default value is null for global services.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-654** datasource

| Parameter | Type | Description |
| --- | --- | --- |
| source_type | Integer | Data source type. The options are as follows--1- Huawei product 2- Third-party product 3-Tenant product<br>Minimum: **1**<br>Maximum: **3**<br>Enumeration values:<br>• **1**<br>• **2**<br>• **3** |
| domain_id | String | Account ID to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | String | ID of the project to which the data source product belongs.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region where the data source is located, for example, cn-north1. For details about the value range, see *Regions and Endpoints*.<br>Minimum: **0**<br>Maximum: **64** |
| company_name | String | Name of the company to which a data source belongs.<br>Minimum: **0**<br>Maximum: **16** |
| product_name | String | Name of the data source.<br>Minimum: **0**<br>Maximum: **24** |
| product_feature | String | Name of the feature of the product that detects the incident.<br>Minimum: **0**<br>Maximum: **24** |
| product_module | String | Threat detection module list.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-655** alert_type

| Parameter | Type | Description |
| --- | --- | --- |
| category | String | Type<br>Minimum: **0**<br>Maximum: **1024** |
| alert_type | String | Alert type.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-656** network_list

| Parameter | Type | Description |
| --- | --- | --- |
| direction | String | Direction. The value can be IN or OUT.<br>Minimum: **0**<br>Maximum: **3**<br>Enumeration values:<br>• **IN**<br>• **OUT** |
| protocol | String | Protocol, including Layer 7 and Layer 4 protocols. For details, see IANA registered name. https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.<br>Minimum: **0**<br>Maximum: **64** |
| src_ip | String | Source IP address<br>Minimum: **0**<br>Maximum: **64** |
| src_port | Integer | Source port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| src_domain | String | Source domain name.<br>Minimum: **0**<br>Maximum: **128** |
| src_geo | **src_geo** object | Geographical location of the source IP address. |
| dest_ip | String | Destination IP address<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| dest_port | String | Destination port. The value ranges from 0 to 65535.<br>Minimum: **0**<br>Maximum: **65535** |
| dest_domain | String | Destination domain name<br>Minimum: **0**<br>Maximum: **128** |
| dest_geo | **dest_geo** object | Geographical location of the destination IP address. |

**Table 4-657** src_geo

| Parameter | Type | Description |
| --- | --- | --- |
| latitude | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |
| city_code | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-658** dest_geo

| Parameter | Type | Description |
| --- | --- | --- |
| latitude | Number | Latitude<br>Minimum: **0**<br>Maximum: **90** |
| longitude | Number | Longitude<br>Minimum: **0**<br>Maximum: **180** |

| Parameter | Type | Description |
| --- | --- | --- |
| city_code | String | City code. For example, Beijing or Shanghai.<br>Minimum: **0**<br>Maximum: **64** |
| country_code | String | Country code. For details, see ISO 3166-1 alpha-2. For example, CN \| US \| DE \| IT \| SG.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-659** resource_list

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Cloud service resource ID.<br>Minimum: **0**<br>Maximum: **36** |
| name | String | Resource name.<br>Minimum: **0**<br>Maximum: **255** |
| type | String | Resource type. This parameter references the value of RMS type on Huawei Cloud.<br>Minimum: **0**<br>Maximum: **64** |
| provider | String | Cloud service name, which is the same as the provider field in the RMS service.<br>Minimum: **0**<br>Maximum: **64** |
| region_id | String | Region ID in Huawei Cloud, for example, cn-north-1.<br>Minimum: **0**<br>Maximum: **36** |
| domain_id | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |
| project_id | String | ID of the account to which the resource belongs, in UUID format.<br>Minimum: **0**<br>Maximum: **36** |

| Parameter | Type | Description |
| --- | --- | --- |
| ep_id | String | Specifies the enterprise project ID.<br>Minimum: **0**<br>Maximum: **128** |
| ep_name | String | Enterprise Project Name<br>Minimum: **0**<br>Maximum: **128** |
| tags | String | Resource tag.<br>1. A maximum of 50 key/value pairs are supported.<br>2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _, :, /,@<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-660** remediation

| Parameter | Type | Description |
| --- | --- | --- |
| recommendation | String | Recommended solution.<br>Minimum: **0**<br>Maximum: **128** |
| url | String | Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.<br>Minimum: **0**<br>Maximum: **2048** |

**Table 4-661** malware

| Parameter | Type | Description |
| --- | --- | --- |
| malware_family | String | Malicious family.<br>Minimum: **0**<br>Maximum: **64** |
| malware_class | String | Malware category.<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-662** process

| Parameter | Type | Description |
| --- | --- | --- |
| process_name | String | Process name.<br>Minimum: **0**<br>Maximum: **64** |
| process_path | String | Process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_pid | Integer | Process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_uid | Integer | Process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_cmdline | String | Process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_parent_name | String | Parent process name.<br>Minimum: **0**<br>Maximum: **64** |
| process_parent_path | String | Parent process execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_parent_pid | Integer | Parent process ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_parent_uid | Integer | Parent process user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_parent_cmdline | String | Parent process command line.<br>Minimum: **0**<br>Maximum: **128** |
| process_child_name | String | Subprocess name.<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| process_child_path | String | Subprocess execution file path.<br>Minimum: **0**<br>Maximum: **512** |
| process_child_pid | Integer | Subprocess ID.<br>Minimum: **0**<br>Maximum: **65535** |
| process_child_uid | Integer | Subprocess user ID.<br>Minimum: **0**<br>Maximum: **655350** |
| process_child_cmdline | String | Subprocess command line<br>Minimum: **0**<br>Maximum: **128** |
| process_launche_time | String | Incident start time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |
| process_terminate_time | String | Process end time. The format is ISO 8601 -- YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.<br>Minimum: **0**<br>Maximum: **30** |

**Table 4-663** user_info

| Parameter | Type | Description |
| --- | --- | --- |
| user_id | String | User UID<br>Minimum: **0**<br>Maximum: **36** |
| user_name | String | Username<br>Minimum: **32**<br>Maximum: **64** |

**Table 4-664** file_info

| Parameter | Type | Description |
| --- | --- | --- |
| file_path | String | File path/name.<br>Minimum: **0**<br>Maximum: **128** |
| file_content | String | File path/name.<br>Minimum: **0**<br>Maximum: **1024** |
| file_new_path | String | New file path/name.<br>Minimum: **32**<br>Maximum: **64** |
| file_hash | String | File Hash<br>Minimum: **0**<br>Maximum: **128** |
| file_md5 | String | File MD5<br>Minimum: **0**<br>Maximum: **128** |
| file_sha256 | String | File SHA256<br>Minimum: **0**<br>Maximum: **128** |
| file_attr | String | File attribute.<br>Minimum: **0**<br>Maximum: **1024** |

**Table 4-665** dataclass_ref

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Unique identifier of a data class. The value is in UUID format and can contain a maximum of 36 characters.<br>Minimum: **0**<br>Maximum: **36** |
| name | String | Data class name.<br>Minimum: **0**<br>Maximum: **36** |

**Status code: 400**

**Table 4-666** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-667** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Query the data object relationship list. The offset is 10, and three alerts are queried.

```
{
  "limit" : 3,
  "offset" : 10
}
```

## Example Responses

**Status code: 200**

Response body for querying associating data objects.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "total" : 41,
  "limit" : 3,
  "offset" : 10,
  "data" : null
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Query the data object relationship list. The offset is 10, and three alerts are queried.

```
package com.huaweicloud.sdk.test;
```

```
import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListDataobjectRelationsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListDataobjectRelationsRequest request = new ListDataobjectRelationsRequest();
        DataobjectSearch body = new DataobjectSearch();
        body.withOffset(10);
        body.withLimit(3);
        request.withBody(body);
        try {
            ListDataobjectRelationsResponse response = client.listDataobjectRelations(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Query the data object relationship list. The offset is 10, and three alerts are queried.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
```

```
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListDataobjectRelationsRequest()
        request.body = DataobjectSearch(
            offset=10,
            limit=3
        )
        response = client.list_dataobject_relations(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Query the data object relationship list. The offset is 10, and three alerts are queried.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListDataobjectRelationsRequest{}
    offsetDataobjectSearch:= int32(10)
    limitDataobjectSearch:= int32(3)
    request.Body = &model.DataobjectSearch{
        Offset: &offsetDataobjectSearch,
        Limit: &limitDataobjectSearch,
    }
    response, err := client.ListDataobjectRelations(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
```

```
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response body for querying associating data objects. |
| 400 | Response body for failed requests for querying associating data objects. |

## Error Codes

See **Error Codes**.

# 4.11.2 Associating a Data Object

## Function

Associating a Data Object

## Calling Method

For details, see **Calling APIs**.

## URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/{dataclass_type}/{data_object_id}/{related_dataclass_type}

**Table 4-668** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| dataclass_type | Yes | String | Data class to which the associated subject data object belongs. The value is plural in lowercase, for example, "alerts" and "incidents".<br>Minimum: **1**<br>Maximum: **64** |
| data_object_id | Yes | String | ID of the associated data object.<br>Minimum: **32**<br>Maximum: **36** |
| related_dataclass_type | Yes | String | Data class to which the associated subject data object belongs. The value is plural in lowercase, for example, "alerts" and "incidents".<br>Minimum: **1**<br>Maximum: **64** |

## Request Parameters

**Table 4-669** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **0**<br>Maximum: **2097152** |
| content-type | Yes | String | Content type.<br>Default: **application/json;charset=UTF-8**<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-670** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| ids | No | Array of strings | ID list of associated data objects.<br>Minimum: **32**<br>Maximum: **64**<br>Array Length: **0 - 100** |

## Response Parameters

**Status code: 200**

**Table 4-671** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-672** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Id value<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error message<br>Minimum: **0**<br>Maximum: **32** |
| request_id | String | Error message<br>Minimum: **0**<br>Maximum: **32** |
| success | Boolean | Error message<br>Minimum: **1**<br>Maximum: **32** |
| total | Integer | tatal count<br>Minimum: **0**<br>Maximum: **99999** |

| Parameter | Type | Description |
| --- | --- | --- |
| limit | Integer | current page count<br>Minimum: **0**<br>Maximum: **9999** |
| offset | Integer | current page size<br>Minimum: **0**<br>Maximum: **100** |
| data | **DataResponse** object | indicator batch operation response |

**Table 4-673** DataResponse

| Parameter | Type | Description |
| --- | --- | --- |
| success_ids | Array of strings | id list<br>Minimum: **32**<br>Maximum: **64**<br>Array Length: **0 - 999** |
| error_ids | Array of strings | id list<br>Minimum: **32**<br>Maximum: **64**<br>Array Length: **0 - 999** |

**Status code: 400**

**Table 4-674** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-675** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Create an incident relationship. Incident ID is f60bf0e7-73b8-4832-8fc4-8c2a12830552.

```
{
  "ids" : [ "f60bf0e7-73b8-4832-8fc4-8c2a12830552" ]
}
```

## Example Responses

**Status code: 200**

Response body for the request for associating a data object.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "request_id" : "Error message",
  "success" : false,
  "total" : 41,
  "limit" : 3,
  "offset" : 10,
  "data" : {
    "success_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ],
    "error_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ]
  }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Create an incident relationship. Incident ID is f60bf0e7-73b8-4832-8fc4-8c2a12830552.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class CreateDataobjectRelationsSolution {
```

```
    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateDataobjectRelationsRequest request = new CreateDataobjectRelationsRequest();
        CreateDataobjectRelationsRequestBody body = new CreateDataobjectRelationsRequestBody();
        List<String> listbodyIds = new ArrayList<>();
        listbodyIds.add("f60bf0e7-73b8-4832-8fc4-8c2a12830552");
        body.withIds(listbodyIds);
        request.withBody(body);
        try {
            CreateDataobjectRelationsResponse response = client.createDataobjectRelations(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Create an incident relationship. Incident ID is f60bf0e7-73b8-4832-8fc4-8c2a12830552.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()
```

```
    try:
        request = CreateDataobjectRelationsRequest()
        listIdsbody = [
            "f60bf0e7-73b8-4832-8fc4-8c2a12830552"
        ]
        request.body = CreateDataobjectRelationsRequestBody(
            ids=listIdsbody
        )
        response = client.create_dataobject_relations(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Create an incident relationship. Incident ID is f60bf0e7-73b8-4832-8fc4-8c2a12830552.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateDataobjectRelationsRequest{}
    var listIdsbody = []string{
        "f60bf0e7-73b8-4832-8fc4-8c2a12830552",
    }
    request.Body = &model.CreateDataobjectRelationsRequestBody{
        Ids: &listIdsbody,
    }
    response, err := client.CreateDataobjectRelations(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response body for the request for associating a data object. |
| 400 | Response body for failed requests for associating a data object. |

## Error Codes

See **Error Codes**.

# 4.11.3 Canceling Association with a Data Object

## Function

Canceling Association with a Data Object

## Calling Method

For details, see **Calling APIs**.

## URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/{dataclass_type}/{data_object_id}/{related_dataclass_type}

**Table 4-676** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| dataclass_type | Yes | String | Data class to which the associated subject data object belongs. The value is plural in lowercase, for example, "alerts" and "incidents".<br>Minimum: **1**<br>Maximum: **64** |
| data_object_id | Yes | String | ID of the associated data object.<br>Minimum: **32**<br>Maximum: **36** |
| related_dataclass_type | Yes | String | Data class to which the associated subject data object belongs. The value is plural in lowercase, for example, "alerts" and "incidents".<br>Minimum: **1**<br>Maximum: **64** |

## Request Parameters

**Table 4-677** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **0**<br>Maximum: **2097152** |
| content-type | Yes | String | Content type.<br>Default: **application/json;charset=UTF-8**<br>Minimum: **0**<br>Maximum: **64** |

**Table 4-678** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| ids | No | Array of strings | ID list of associated data objects.<br>Minimum: **32**<br>Maximum: **64**<br>Array Length: **0 - 100** |

## Response Parameters

**Status code: 200**

**Table 4-679** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-680** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Message<br>Minimum: **0**<br>Maximum: **1024** |
| data | **BatchOperateDataobjectResult** object | Returned object for batch operation on alerts. |

**Table 4-681** BatchOperateDataobjectResult

| Parameter | Type | Description |
| --- | --- | --- |
| error_ids | Array of strings | IDs of alerts not transferred to incidents<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 100** |

| Parameter | Type | Description |
| --- | --- | --- |
| success_ids | Array of strings | IDs of alerts transferred to incidents.<br>Minimum: **0**<br>Maximum: **100**<br>Array Length: **0 - 100** |

**Status code: 400**

**Table 4-682** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-683** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Delete an incident relationship. Incident ID is f60bf0e7-73b8-4832-8fc4-8c2a12830552.

```
{
  "ids" : [ "f60bf0e7-73b8-4832-8fc4-8c2a12830552" ]
}
```

## Example Responses

**Status code: 200**

Response body for the request for canceling associating a data object.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "request_id" : "Error message",
  "success" : false,
  "total" : 41,
```

```
 "limit" : 3,
 "offset" : 10,
 "data" : {
  "success_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ],
  "error_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ]
 }
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Delete an incident relationship. Incident ID is f60bf0e7-73b8-4832-8fc4-8c2a12830552.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class DeleteDataobjectRelationsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteDataobjectRelationsRequest request = new DeleteDataobjectRelationsRequest();
        CreateDataobjectRelationsRequestBody body = new CreateDataobjectRelationsRequestBody();
        List<String> listbodyIds = new ArrayList<>();
        listbodyIds.add("f60bf0e7-73b8-4832-8fc4-8c2a12830552");
        body.withIds(listbodyIds);
        request.withBody(body);
        try {
            DeleteDataobjectRelationsResponse response = client.deleteDataobjectRelations(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
```

```
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Delete an incident relationship. Incident ID is f60bf0e7-73b8-4832-8fc4-8c2a12830552.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteDataobjectRelationsRequest()
        listIdsbody = [
            "f60bf0e7-73b8-4832-8fc4-8c2a12830552"
        ]
        request.body = CreateDataobjectRelationsRequestBody(
            ids=listIdsbody
        )
        response = client.delete_dataobject_relations(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Delete an incident relationship. Incident ID is f60bf0e7-73b8-4832-8fc4-8c2a12830552.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
```

```
risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteDataobjectRelationsRequest{}
    var listIdsbody = []string{
        "f60bf0e7-73b8-4832-8fc4-8c2a12830552",
    }
    request.Body = &model.CreateDataobjectRelationsRequestBody{
        Ids: &listIdsbody,
    }
    response, err := client.DeleteDataobjectRelations(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Response body for the request for canceling associating a data object. |
| 400 | Response body for failed requests for canceling associating a data object. |

## Error Codes

See **Error Codes**.

# 4.12 Data Class Management

# 4.12.1 Querying the Data Class List

## Function

Querying the Data Class List

## Calling Method

For details, see **Calling APIs**.

## URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses

**Table 4-684** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

**Table 4-685** Query Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| offset | No | Number | Offset<br>Minimum: **0**<br>Maximum: **999999999**<br>Default: **0** |
| limit | No | Number | Data volume<br>Minimum: **1**<br>Maximum: **100**<br>Default: **10** |
| name | No | String | Name<br>Minimum: **0**<br>Maximum: **64** |
| business_code | No | String | Code<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| description | No | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |
| is_built_in | No | Boolean | Built-in or Not |

## Request Parameters

**Table 4-686** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **0**<br>Maximum: **2097152** |
| content-type | Yes | String | Content type.<br>Default: **application/json;charset=UTF-8**<br>Minimum: **0**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-687** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-688** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| dataclass_details | Array of **DataClassResponseBody** objects | Data class details.<br>Array Length: **0 - 100** |
| total | Number | Total data volume<br>Minimum: **2**<br>Maximum: **999999999** |

**Table 4-689** DataClassResponseBody

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Data class ID.<br>Minimum: **32**<br>Maximum: **64** |
| create_time | String | Creation time.<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Update time.<br>Minimum: **0**<br>Maximum: **64** |
| creator_id | String | Creator ID.<br>Minimum: **32**<br>Maximum: **64** |
| creator_name | String | Creator username<br>Minimum: **32**<br>Maximum: **64** |
| modifier_id | String | ID of the user who updated the information.<br>Minimum: **32**<br>Maximum: **64** |
| modifier_name | String | Creator username<br>Minimum: **32**<br>Maximum: **64** |
| cloud_pack_version | String | Subscribed version.<br>Minimum: **2**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| region_id | String | Region ID<br>Minimum: **0**<br>Maximum: **64** |
| project_id | String | Tenant ID.<br>Minimum: **0**<br>Maximum: **64** |
| workspace_id | String | Workspace ID<br>Minimum: **0**<br>Maximum: **64** |
| domain_id | String | domain id<br>Minimum: **0**<br>Maximum: **64** |
| name | String | Data class name.<br>Minimum: **2**<br>Maximum: **64** |
| business_code | String | Service code for the data class.<br>Minimum: **2**<br>Maximum: **64** |
| description | String | Description of the data class.<br>Minimum: **2**<br>Maximum: **1024** |
| is_built_in | Boolean | Whether the data class is built in SecMaster. The options are - **true** for built-in and **false** for outsourced. |
| parent_id | String | Parent data class ID.<br>Minimum: **32**<br>Maximum: **64** |
| type_num | Number | Quantity of sub-type data classes.<br>Minimum: **0**<br>Maximum: **99999** |

**Status code: 400**

**Table 4-690** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-691** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Query the data object relationship list. The offset is 10, and three alerts are queried.

```
{
  "limit" : 3,
  "offset" : 10
}
```

## Example Responses

**Status code: 200**

Request succeeded.

```
{
  "total" : 41,
  "dataclass_details" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "creator_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "creator_name" : "Tom",
    "modifier_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "modifier_name" : "Jerry",
    "cloud_pack_version" : "Subscribed version.",
    "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "Evidence",
    "business_code" : "Evidence",
    "description" : "Description of custom data classes.",
    "is_built_in" : false,
    "parent_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "type_num" : 9
```

```
 } ]
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Query the data object relationship list. The offset is 10, and three alerts are queried.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListDataclassSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListDataclassRequest request = new ListDataclassRequest();
        request.withOffset(<offset>);
        request.withLimit(<limit>);
        request.withName("<name>");
        request.withBusinessCode("<business_code>");
        request.withDescription("<description>");
        request.withIsBuiltIn(<is_built_in>);
        try {
            ListDataclassResponse response = client.listDataclass(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Query the data object relationship list. The offset is 10, and three alerts are queried.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListDataclassRequest()
        request.offset = <offset>
        request.limit = <limit>
        request.name = "<name>"
        request.business_code = "<business_code>"
        request.description = "<description>"
        request.is_built_in = <IsBuiltIn>
        response = client.list_dataclass(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Query the data object relationship list. The offset is 10, and three alerts are queried.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
```

```
    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListDataclassRequest{}
    offsetRequest:= float32(<offset>)
    request.Offset = &offsetRequest
    limitRequest:= float32(<limit>)
    request.Limit = &limitRequest
    nameRequest:= "<name>"
    request.Name = &nameRequest
    businessCodeRequest:= "<business_code>"
    request.BusinessCode = &businessCodeRequest
    descriptionRequest:= "<description>"
    request.Description = &descriptionRequest
    isBuiltInRequest:= <is_built_in>
    request.IsBuiltIn = &isBuiltInRequest
    response, err := client.ListDataclass(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Request succeeded. |
| 400 | Response body of the failed requests for querying the data class list. |

## Error Codes

See **Error Codes**.

# 4.12.2 Querying the Data Class List

## Function

This API is used to query the data class list.

## Calling Method

For details, see **Calling APIs**.

## URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/fields

**Table 4-692** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |
| dataclass_id | Yes | String | Data class ID.<br>Minimum: **32**<br>Maximum: **36** |

**Table 4-693** Query Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| offset | No | Number | Offset<br>Minimum: **0**<br>Maximum: **999999999**<br>Default: **0** |
| limit | No | Number | Data volume<br>Minimum: **1**<br>Maximum: **100**<br>Default: **10** |
| name | No | String | Name<br>Minimum: **0**<br>Maximum: **64** |
| is_built_in | No | Boolean | Built-in or Not |
| field_category | No | String | Field types.<br>Minimum: **0**<br>Maximum: **1024** |
| mapping | No | Boolean | Whether to display in other places other the classification and mapping module. |

## Request Parameters

**Table 4-694** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **0**<br>Maximum: **2097152** |
| content-type | Yes | String | Content type.<br>Default: **application/json;charset=UTF-8**<br>Minimum: **0**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-695** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-696** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| field_details | Array of **FieldResponseBody** objects | list of informations of field<br>Array Length: **0 - 100** |
| total | Number | Total data volume<br>Minimum: **2**<br>Maximum: **999999999** |

**Table 4-697** FieldResponseBody

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Id value<br>Minimum: **32**<br>Maximum: **64** |
| cloud_pack_version | String | Subscribed version.<br>Minimum: **2**<br>Maximum: **64** |
| business_id | String | ID of associated service.<br>Minimum: **32**<br>Maximum: **64** |
| business_type | String | Associated service.<br>Minimum: **2**<br>Maximum: **64** |
| dataclass_name | String | Data class name.<br>Minimum: **2**<br>Maximum: **64** |
| business_code | String | Service code for the field.<br>Minimum: **2**<br>Maximum: **64** |
| field_key | String | Key<br>Minimum: **2**<br>Maximum: **64** |
| name | String | Field name.<br>Minimum: **2**<br>Maximum: **64** |
| description | String | Field description.<br>Minimum: **2**<br>Maximum: **1024** |
| default_value | String | Default value.<br>Minimum: **2**<br>Maximum: **1024** |
| display_type | String | Display type.<br>Minimum: **2**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| field_type | String | Field type, such as short text, radio, and grid.<br>Minimum: **2**<br>Maximum: **64** |
| extra_json | String | Additional JSON.<br>Minimum: **2**<br>Maximum: **64** |
| field_tooltip | String | Tool tip.<br>Minimum: **2**<br>Maximum: **64** |
| iu_type | String | Input and output types.<br>Minimum: **2**<br>Maximum: **64** |
| used_by | String | Services.<br>Minimum: **2**<br>Maximum: **64** |
| json_schema | String | JSON mode.<br>Minimum: **2**<br>Maximum: **64** |
| is_built_in | Boolean | Whether it is built in SecMaster. The options are - **true** for built-in and **false** for outsourced. |
| case_sensitive | Boolean | Case-sensitive mode. - **true** Enabled. **False** Disabled. |
| read_only | Boolean | Read-only mode. **True** Enabled. **False** Disabled. |
| required | Boolean | Mandatory mode. **True** Enabled. **False** Disabled. |
| searchable | Boolean | Search mode. **True** Enabled. **False** Disabled. |
| visible | Boolean | Visible mode. **True** Enabled. **False** Disabled. |
| maintainable | Boolean | Maintenance mode. **True** Enabled. **False** Disabled. |
| editable | Boolean | Edit mode. **True** Enabled. **False** Disabled. |
| creatable | Boolean | Creation mode. **True** Enabled. **False** Disabled. |
| mapping | Boolean | Whether to display in other places other the classification and mapping module. |

| Parameter | Type | Description |
| --- | --- | --- |
| target_api | String | Target API.<br>Minimum: **0**<br>Maximum: **1024** |
| creator_id | String | Creator id value<br>Minimum: **32**<br>Maximum: **64** |
| creator_name | String | Creator name value<br>Minimum: **32**<br>Maximum: **64** |
| modifier_id | String | Modifier id value<br>Minimum: **32**<br>Maximum: **64** |
| modifier_name | String | Modifier name value<br>Minimum: **32**<br>Maximum: **64** |
| create_time | String | Create time<br>Minimum: **0**<br>Maximum: **64** |
| update_time | String | Update time<br>Minimum: **0**<br>Maximum: **64** |

**Status code: 400**

**Table 4-698** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-699** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Query the data object relationship list. The offset is 10, and three alerts are queried.

```
{
  "limit" : 3,
  "offset" : 10
}
```

## Example Responses

**Status code: 200**

Request succeeded.

```
{
  "total" : 41,
  "field_details" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "cloud_pack_version" : "Subscribed version.",
    "business_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "business_type" : "Service type",
    "dataclass_name" : "Business ID",
    "business_code" : "My Field",
    "field_key" : "Key",
    "name" : "Field name.",
    "description" : "Field description.",
    "default_value" : "Default value.",
    "display_type" : "Display type.",
    "field_type" : "shorttext",
    "extra_json" : "{}",
    "field_tooltip" : "Tool tip.",
    "iu_type" : "Input and output types.",
    "used_by" : "Services.",
    "json_schema" : "{}",
    "is_built_in" : false,
    "case_sensitive" : false,
    "read_only" : false,
    "required" : false,
    "searchable" : false,
    "visible" : false,
    "maintainable" : false,
    "editable" : false,
    "creatable" : false,
    "mapping" : true,
    "target_api" : "Target API.",
    "creator_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "creator_name" : "Tom",
    "modifier_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "modifier_name" : "Jerry",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800"
  } ]
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Query the data object relationship list. The offset is 10, and three alerts are queried.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListDataclassFieldsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListDataclassFieldsRequest request = new ListDataclassFieldsRequest();
        request.withOffset(<offset>);
        request.withLimit(<limit>);
        request.withName("<name>");
        request.withIsBuiltIn(<is_built_in>);
        request.withFieldCategory("<field_category>");
        request.withMapping(<mapping>);
        try {
            ListDataclassFieldsResponse response = client.listDataclassFields(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Query the data object relationship list. The offset is 10, and three alerts are queried.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListDataclassFieldsRequest()
        request.offset = <offset>
        request.limit = <limit>
        request.name = "<name>"
        request.is_built_in = <IsBuiltIn>
        request.field_category = "<field_category>"
        request.mapping = <Mapping>
        response = client.list_dataclass_fields(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Query the data object relationship list. The offset is 10, and three alerts are queried.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
```

```
    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListDataclassFieldsRequest{}
    offsetRequest:= float32(<offset>)
    request.Offset = &offsetRequest
    limitRequest:= float32(<limit>)
    request.Limit = &limitRequest
    nameRequest:= "<name>"
    request.Name = &nameRequest
    isBuiltInRequest:= <is_built_in>
    request.IsBuiltIn = &isBuiltInRequest
    fieldCategoryRequest:= "<field_category>"
    request.FieldCategory = &fieldCategoryRequest
    mappingRequest:= <mapping>
    request.Mapping = &mappingRequest
    response, err := client.ListDataclassFields(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

### More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

### Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Request succeeded. |
| 400 | Response body of the failed requests for querying the data class list. |

### Error Codes

See **Error Codes**.

# 4.13 Workflow Management

## 4.13.1 Querying the Workflow List

### Function

This API is used to query the workflow list.

## Calling Method

For details, see **Calling APIs**.

## URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/workflows

**Table 4-700** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

**Table 4-701** Query Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| offset | No | Number | Offset<br>Minimum: **0**<br>Maximum: **999999999**<br>Default: **0** |
| limit | No | Number | Data volume<br>Minimum: **1**<br>Maximum: **100**<br>Default: **10** |
| order | No | String | Sorting sequence, including **asc** for ascending order and **desc** for descending order.<br>Minimum: **0**<br>Maximum: **4**<br>Enumeration values:<br>• **asc**<br>• **desc** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| sortby | No | String | Sorting fields, including **create_time** for creation time and **category** for classification name.<br>Minimum: **2**<br>Maximum: **32**<br>Enumeration values:<br>• **category**<br>• **create_time** |
| enabled | No | Boolean | Whether to enable. |
| last_version | No | Boolean | Latest version. |
| name | No | String | Workflow name.<br>Minimum: **1**<br>Maximum: **64** |
| description | No | String | Description<br>Minimum: **1**<br>Maximum: **512** |
| dataclass_id | No | String | Data class ID.<br>Minimum: **1**<br>Maximum: **64** |
| dataclass_name | No | String | Data class name.<br>Minimum: **1**<br>Maximum: **64** |
| aop_type | No | String | Process Type<br>Minimum: **1**<br>Maximum: **64** |

## Request Parameters

**Table 4-702** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **0**<br>Maximum: **2097152** |
| content-type | Yes | String | Content type.<br>Default: **application/json;charset=UTF-8**<br>Minimum: **0**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-703** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-704** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Return code.<br>Minimum: **0**<br>Maximum: **1000** |
| total | Integer | Total records.<br>Minimum: **0**<br>Maximum: **1000** |
| offset | Integer | Current page size.<br>Minimum: **0**<br>Maximum: **1000** |

| Parameter | Type | Description |
| --- | --- | --- |
| limit | Integer | Current page.<br>Minimum: **0**<br>Maximum: **1000** |
| message | String | Request ID<br>Minimum: **32**<br>Maximum: **36** |
| success | Boolean | Successful or not. |
| data | Array of **AopWorkflowInfo** objects | Workflow list.<br>Array Length: **0 - 100** |

**Table 4-705** AopWorkflowInfo

| Parameter | Type | Description |
| --- | --- | --- |
| id | String | Workflow ID.<br>Minimum: **32**<br>Maximum: **64** |
| name | String | Workflow name.<br>Minimum: **0**<br>Maximum: **1024** |
| description | String | Description.<br>Minimum: **0**<br>Maximum: **1024** |
| project_id | String | Tenant ID.<br>Minimum: **32**<br>Maximum: **64** |
| owner_id | String | Owner ID.<br>Minimum: **32**<br>Maximum: **64** |
| creator_id | String | Creator ID.<br>Minimum: **32**<br>Maximum: **64** |
| edit_role | String | Edit<br>Minimum: **32**<br>Maximum: **64** |

| Parameter | Type | Description |
| --- | --- | --- |
| use_role | String | User role.<br>Minimum: **32**<br>Maximum: **64** |
| approve_role | String | Reviewer.<br>Minimum: **32**<br>Maximum: **64** |
| enabled | Boolean | Enabled or not |
| workspace_id | String | Workspace ID<br>Minimum: **32**<br>Maximum: **64** |
| version_id | String | Workflow version ID.<br>Minimum: **32**<br>Maximum: **64** |
| current_approval_version_id | String | Version to be viewed currently.<br>Minimum: **1**<br>Maximum: **64** |
| current_rejected_versoin_id | String | Version that has been rejected currently.<br>Minimum: **1**<br>Maximum: **64** |
| aop_type | String | AOP types. - **NORMAL**: General - **SURVEY**: Investigation - **HEMOSTASIS**: Prevention - **EASE**: Mitigation<br>Minimum: **1**<br>Maximum: **64** |
| engine_type | String | There are two types of engine, shared and dedicated.<br>Minimum: **1**<br>Maximum: **64** |
| dataclass_id | String | ID of the data class.<br>Minimum: **1**<br>Maximum: **64** |

**Status code: 400**

**Table 4-706** Response header parameters

| Parameter | Type | Description |
| --- | --- | --- |
| X-request-id | String | Request ID, in the format request_uuid-timestamp-hostname. |

**Table 4-707** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| code | String | Error Code<br>Minimum: **0**<br>Maximum: **64** |
| message | String | Error Description<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

Query the workflow list. The offset is 10, and three alerts are queried.

```
{
  "limit" : 3,
  "offset" : 10
}
```

## Example Responses

**Status code: 200**

Request succeeded.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "total" : 41,
  "limit" : 2,
  "offset" : 1,
  "success" : true,
  "data" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "Workflow name.",
    "description" : "Description.",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "owner_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "creator_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "edit_role" : "Editor.",
    "use_role" : "User.",
    "approve_role" : "Approver.",
    "enabled" : true,
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "current_approval_version_id" : "v2",
    "current_rejected_versoin_id" : "v1",
    "aop_type" : "Mitigation (ease).",
```

```
    "engine_type" : "public_engine",
    "dataclass_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  } ]
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

Query the workflow list. The offset is 10, and three alerts are queried.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListWorkflowsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListWorkflowsRequest request = new ListWorkflowsRequest();
        request.withEnabled(<enabled>);
        request.withLastVersion(<last_version>);
        request.withName("<name>");
        request.withDescription("<description>");
        request.withDataclassId("<dataclass_id>");
        request.withDataclassName("<dataclass_name>");
        request.withAopType("<aop_type>");
        request.withOffset(<offset>);
        request.withLimit(<limit>);
        request.withOrder(ListWorkflowsRequest.OrderEnum.fromValue("<order>"));
        request.withSortby(ListWorkflowsRequest.SortbyEnum.fromValue("<sortby>"));
        try {
            ListWorkflowsResponse response = client.listWorkflows(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
```

```
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Query the workflow list. The offset is 10, and three alerts are queried.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListWorkflowsRequest()
        request.enabled = <Enabled>
        request.last_version = <LastVersion>
        request.name = "<name>"
        request.description = "<description>"
        request.dataclass_id = "<dataclass_id>"
        request.dataclass_name = "<dataclass_name>"
        request.aop_type = "<aop_type>"
        request.offset = <offset>
        request.limit = <limit>
        request.order = "<order>"
        request.sortby = "<sortby>"
        response = client.list_workflows(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Query the workflow list. The offset is 10, and three alerts are queried.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)
```

```
func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListWorkflowsRequest{}
    enabledRequest:= <enabled>
    request.Enabled = &enabledRequest
    lastVersionRequest:= <last_version>
    request.LastVersion = &lastVersionRequest
    nameRequest:= "<name>"
    request.Name = &nameRequest
    descriptionRequest:= "<description>"
    request.Description = &descriptionRequest
    dataclassIdRequest:= "<dataclass_id>"
    request.DataclassId = &dataclassIdRequest
    dataclassNameRequest:= "<dataclass_name>"
    request.DataclassName = &dataclassNameRequest
    aopTypeRequest:= "<aop_type>"
    request.AopType = &aopTypeRequest
    offsetRequest:= float32(<offset>)
    request.Offset = &offsetRequest
    limitRequest:= float32(<limit>)
    request.Limit = &limitRequest
    orderRequest:= model.GetListWorkflowsRequestOrderEnum().<ORDER>
    request.Order = &orderRequest
    sortbyRequest:= model.GetListWorkflowsRequestSortbyEnum().<SORTBY>
    request.Sortby = &sortbyRequest
    response, err := client.ListWorkflows(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 200 | Request succeeded. |
| 400 | Response body of the failed requests for querying the data class list. |

### Error Codes

See **Error Codes**.

# 4.14 Data Space Management

## 4.14.1 Creating a Data Space

### Function

create dataspace

### Calling Method

For details, see **Calling APIs**.

### URI

POST /v1/{project_id}/workspaces/{workspace_id}/siem/dataspaces

**Table 4-708** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

### Request Parameters

**Table 4-709** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| dataspace_name | Yes | String | Data space name<br>Minimum: **5**<br>Maximum: **63** |
| description | Yes | String | Description.<br>Minimum: **1**<br>Maximum: **255** |

## Response Parameters

None

## Example Requests

```
{
  "dataspace_name" : "dataspace-01",
  "description" : "test dataspace"
}
```

## Example Responses

**Status code: 200**

```
{
  "domain_id" : "0531ed520xxxxxxebedb6e57xxxxxxxx",
  "region_id" : "cn-north-1",
  "project_id" : "2b31ed520xxxxxxebedb6e57xxxxxxxx",
  "dataspace_id" : "a00106ba-bede-453c-8488-b60c70bd6aed",
  "dataspace_name" : "dataspace-01",
  "dataspace_type" : "system-defined",
  "description" : "test dataspace",
  "create_by" : "0642ed520xxxxxxebedb6e57xxxxxxxx",
  "create_time" : 1584883694354,
  "update_by" : "0642ed520xxxxxxebedb6e57xxxxxxxx",
  "update_time" : 1584883694354
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class CreateDataspaceSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
```

```
        CreateDataspaceRequest request = new CreateDataspaceRequest();
        CreateDataspaceRequestBody body = new CreateDataspaceRequestBody();
        request.withBody(body);
        try {
            CreateDataspaceResponse response = client.createDataspace(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateDataspaceRequest()
        request.body = CreateDataspaceRequestBody(
        )
        response = client.create_dataspace(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)
```

```
func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateDataspaceRequest{}
    request.Body = &model.CreateDataspaceRequestBody{
    }
    response, err := client.CreateDataspace(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

### More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

### Status Codes

| Status Code | Description |
| --- | --- |
| 200 | |

### Error Codes

See **Error Codes**.

# 4.15 Pipelines

## 4.15.1 Creating a Data Pipeline

### Function

create pipe

## Calling Method

For details, see **Calling APIs**.

## URI

POST /v1/{project_id}/workspaces/{workspace_id}/siem/pipes

**Table 4-710** Path Parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| project_id | Yes | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| workspace_id | Yes | String | Workspace ID<br>Minimum: **32**<br>Maximum: **36** |

## Request Parameters

**Table 4-711** Request header parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| X-Auth-Token | Yes | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.<br>Minimum: **0**<br>Maximum: **2097152** |

**Table 4-712** Request body parameters

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| dataspace_id | Yes | String | Workspace ID<br>Minimum: **36**<br>Maximum: **36** |
| pipe_name | Yes | String | Data pipeline name.<br>Minimum: **5**<br>Maximum: **63** |

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| description | No | String | Description.<br>Minimum: **1**<br>Maximum: **255** |
| storage_period | Yes | Integer | Data storage duration, in days. The default value is 30. The value ranges from 1 to 3600.<br>Minimum: **1**<br>Maximum: **3600** |
| shards | Yes | Integer | Number of pipeline partitions. One partition is created by default. A maximum of 64 partitions can be created.<br>Minimum: **1**<br>Maximum: **64** |
| timestamp_field | No | String | Timestamp field.<br>Default: **__time**<br>Minimum: **1**<br>Maximum: **256** |
| mapping | No | Map<String,**KeyIndex**> | Index field mapping. Each key object carries information about a field. There are multiple key objects. The key is variable and indicates the field name. Nesting is supported. |

**Table 4-713** KeyIndex

| Parameter | Mandatory | Type | Description |
| --- | --- | --- | --- |
| type | No | String | Field type. The options are text (full-text index field), keyword (structured field), Long, Integer, Double, Float (time field), and Date (time field).<br>Enumeration values:<br>• **text**<br>• **keyword**<br>• **long**<br>• **integer**<br>• **double**<br>• **float**<br>• **date** |
| is_chinese_exist | No | Boolean | Whether Chinese characters are contained. |
| properties | No | Map<String,**KeyIndex**> | Nested structure. |

## Response Parameters

**Status code: 201**

**Table 4-714** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| domain_id | String | Account ID.<br>Minimum: **32**<br>Maximum: **36** |
| project_id | String | Project ID.<br>Minimum: **32**<br>Maximum: **36** |
| dataspace_id | String | Data space ID<br>Minimum: **32**<br>Maximum: **36** |
| dataspace_name | String | Data space name<br>Minimum: **32**<br>Maximum: **36** |

| Parameter | Type | Description |
| --- | --- | --- |
| pipe_id | String | Indicates the pipe ID.<br>Minimum: **32**<br>Maximum: **36** |
| pipe_name | String | Pipeline Name<br>Minimum: **32**<br>Maximum: **36** |
| pipe_type | String | Pipeline type. **System-defined** Preset types. **User-defined** Custom types.<br>Minimum: **5**<br>Maximum: **128** |
| description | String | Description.<br>Minimum: **5**<br>Maximum: **128** |
| storage_period | Integer | Index storage period by the day.<br>Minimum: **1**<br>Maximum: **100000** |
| shards | Integer | Index shard quantity.<br>Minimum: **1**<br>Maximum: **128** |
| create_by | String | Created By<br>Minimum: **5**<br>Maximum: **128** |
| create_time | Integer | Creation time<br>Minimum: **0**<br>Maximum: **1010000000** |
| update_by | String | Updated by<br>Minimum: **5**<br>Maximum: **128** |
| update_time | Integer | Update time.<br>Minimum: **0**<br>Maximum: **10000000000** |

**Status code: 400**

**Table 4-715** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| error_msg | String | Invalid request message.<br>Minimum: **1**<br>Maximum: **128** |
| error_code | String | Error code<br>Minimum: **1**<br>Maximum: **128** |

**Status code: 401**

**Table 4-716** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| error_msg | String | Permissions error.<br>Minimum: **1**<br>Maximum: **128** |
| error_code | String | Error code<br>Minimum: **1**<br>Maximum: **128** |

**Status code: 500**

**Table 4-717** Response body parameters

| Parameter | Type | Description |
| --- | --- | --- |
| error_msg | String | Internal system error.<br>Minimum: **1**<br>Maximum: **128** |
| error_code | String | Error code<br>Minimum: **1**<br>Maximum: **128** |

## Example Requests

```
{
  "dataspace_id" : "a00106ba-bede-453c-8488-b60c70bd6aed",
  "pipe_name" : "pipe-01",
  "description" : "test pipe",
  "storage_period" : 30,
```

```
  "shards" : 3,
  "mapping" : {
    "name" : {
      "type" : "text"
    },
    "id" : {
      "type" : "text"
    },
    "publish_time" : {
      "type" : "data",
      "format" : "yyyy-MM-dd HH:mm:ss"
    }
  }
}
```

## Example Responses

**Status code: 201**

Created pipeline returned.

```
{
  "domain_id" : "0531ed520xxxxxxebedb6e57xxxxxxxx",
  "project_id" : "2b31ed520xxxxxxebedb6e57xxxxxxxx",
  "dataspace_id" : "a00106ba-bede-453c-8488-b60c70bd6aed",
  "dataspace_name" : "dataspace-01",
  "pipe_id" : "b22106ba-bede-453c-8488-b60c70bd6aed",
  "pipe_name" : "pipe-01",
  "pipe_type" : "system-defined",
  "description" : "test pipe",
  "storage_period" : 30,
  "shards" : 3,
  "create_by" : "0642ed520xxxxxxebedb6e57xxxxxxxx",
  "create_time" : 1584883694354,
  "update_by" : "0642ed520xxxxxxebedb6e57xxxxxxxx",
  "update_time" : 1584883694354
}
```

## SDK Sample Code

The SDK sample code is as follows.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class CreatePipeSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
```

```
        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreatePipeRequest request = new CreatePipeRequest();
        CreatePipeRequestBody body = new CreatePipeRequestBody();
        request.withBody(body);
        try {
            CreatePipeResponse response = client.createPipe(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreatePipeRequest()
        request.body = CreatePipeRequestBody(
        )
        response = client.create_pipe(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main
```

```
import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreatePipeRequest{}
    request.Body = &model.CreatePipeRequestBody{
    }
    response, err := client.CreatePipe(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description |
| --- | --- |
| 201 | Created pipeline returned. |
| 400 | Request error. |
| 401 | Authentication failed. |
| 403 | Access denied. |
| 500 | Internal system error. |

## Error Codes

See **Error Codes**.

# A Appendix

## A.1 Status Codes

- Normal

| Status Code | Description |
| --- | --- |
| 201 | Success |

- Abnormal

| Status Code | Status | Description |
| --- | --- | --- |
| 400 | Bad Request | Parameter error. |
| 401 | Unauthorized | Authentication failed. |
| 403 | Forbidden | Access denied. |
| 500 | Internal Server Error | Internal server error. |

## A.2 Error Codes

If an error code starting with APIGW is returned after you call an API, rectify the fault by referring to the instructions provided in **API Gateway Error Codes**.

| Status Code | Error Codes | Error Message | Description | Solution |
| --- | --- | --- | --- | --- |
| 400 | SecMaster.11061001 | alert process status error. | -- | -- |

| Status Code | Error Codes | Error Message | Description | Solution |
| --- | --- | --- | --- | --- |
| 400 | SecMaster.11061002 | alert rule count out of range. | -- | -- |
| 400 | SecMaster.11061003 | alert rule schedule out of range. | -- | -- |
| 400 | SecMaster.11061004 | alert rule name already exist. | -- | -- |
| 400 | SecMaster.20010001 | Invalid workspace ID. | -- | -- |
| 400 | SecMaster.20030001 | Invalid parameters. | -- | -- |
| 400 | SecMaster.20030002 | Invalid project ID. | -- | -- |
| 400 | SecMaster.20030003 | Invalid name. | -- | -- |
| 400 | SecMaster.20030004 | Failed to create the data object. | -- | -- |
| 400 | SecMaster.20030005 | Failed to obtain the data object. | -- | -- |
| 400 | SecMaster.20030009 | Invalid sorting field. | -- | -- |
| 400 | SecMaster.20030010 | Invalid sorting. | -- | -- |
| 400 | SecMaster.20030011 | Data object update error. | -- | -- |
| 400 | SecMaster.20030012 | Data object deletion error. | -- | -- |
| 400 | SecMaster.20030013 | Data object search error. | -- | -- |
| 400 | SecMaster.20030022 | Failed to find one dataclass. | -- | -- |
| 400 | SecMaster.20030025 | Failed to valid data object. | -- | -- |

| Status Code | Error Codes | Error Message | Description | Solution |
|---|---|---|---|---|
| 400 | SecMaster.20039999 | Unknown errors | -- | -- |
| 400 | SecMaster.20040000 | Unknown Error. | -- | -- |
| 400 | SecMaster.20040402 | Failed to query the data class. | -- | -- |
| 400 | SecMaster.20040516 | The number of fields exceeds the maximum. | -- | -- |
| 400 | SecMaster.20041001 | Invalid workspace ID. | -- | -- |
| 400 | SecMaster.20041002 | Invalid parameters. | -- | -- |
| 400 | SecMaster.20041003 | Invalid project ID. | -- | -- |
| 400 | SecMaster.20041031 | Fail to get data object. | -- | -- |
| 400 | SecMaster.20041033 | No associated data object is selected. | -- | -- |
| 400 | SecMaster.20041504 | Failed to create the incident. | -- | -- |
| 400 | SecMaster.20041507 | Failed to update the incident. | -- | -- |
| 400 | SecMaster.20041508 | Failed to delete the incident. | -- | -- |
| 400 | SecMaster.20041509 | The number of incidents created per day exceeds the upper limit. | -- | -- |

| Status Code | Error Codes | Error Message | Description | Solution |
| --- | --- | --- | --- | --- |
| 400 | SecMaster.20041804 | Incorrect content included in the request for converting an alert to an incident. | -- | -- |
| 400 | SecMaster.20041805 | Failed to create the alert. | -- | -- |
| 400 | SecMaster.20041808 | Failed to update alert. | -- | -- |
| 400 | SecMaster.20041809 | Failed to delete the alert. | -- | -- |
| 400 | SecMaster.20041810 | The number of alerts created per day exceeds the upper limit. | -- | -- |
| 400 | SecMaster.20041811 | The number of incidents transferred by alerts per day exceeds the upper limit. | -- | -- |
| 400 | SecMaster.20041903 | Failed to find dataclass. | -- | -- |
| 400 | SecMaster.20041904 | The indicator is not exist. | -- | -- |
| 400 | SecMaster.20041905 | Failed to create indicator. | -- | -- |
| 400 | SecMaster.20041906 | Failed to update indicator. | -- | -- |
| 400 | SecMaster.20041907 | Failed to delete indicator. | -- | -- |

| Status Code | Error Codes | Error Message | Description | Solution |
| --- | --- | --- | --- | --- |
| 400 | SecMaster.20042501 | The number of indicators created per day exceeds the upper limit. | -- | -- |
| 400 | SecMaster.20048001 | The playbook cannot be deleted because it has a running instance or an activated version. | -- | -- |
| 400 | SecMaster.20048002 | The playbook cannot be enabled because it does not have an activated version. | -- | -- |
| 400 | SecMaster.20048003 | The playbook cannot be reviewed because it is in an incorrect state. | -- | -- |
| 400 | SecMaster.20048004 | The resource does not exist. | -- | -- |
| 400 | SecMaster.20048005 | The draft cannot be activated before it passes the review. | -- | -- |
| 400 | SecMaster.20048006 | Incorrect playbook ID. | -- | -- |
| 400 | SecMaster.20048007 | Incorrect playbook version ID. | -- | -- |

| Status Code | Error Codes | Error Message | Description | Solution |
|---|---|---|---|---|
| 400 | SecMaster.20048008 | Incorrect playbook action ID. | -- | -- |
| 400 | SecMaster.20048009 | Incorrect playbook rule ID. | -- | -- |
| 400 | SecMaster.20048013 | The playbook is being enabled. You cannot deactivate the version. | -- | -- |
| 400 | SecMaster.20048014 | The playbook has been released and cannot be edited. | -- | -- |
| 400 | SecMaster.20048015 | The playbook name must be unique. | -- | -- |
| 400 | SecMaster.20048016 | Incorrect time range of the scheduled task. | -- | -- |
| 400 | SecMaster.20048017 | Incorrect Corn expression of the scheduled task. | -- | -- |
| 400 | SecMaster.20048018 | The number of versions has reached the upper limit. | -- | -- |
| 400 | SecMaster.20048019 | A new version cannot be created because there is a version being reviewed. | -- | -- |
| 400 | SecMaster.20048020 | Incorrect data object ID. | -- | -- |

| Status Code | Error Codes | Error Message | Description | Solution |
|---|---|---|---|---|
| 400 | SecMaster.20048021 | Invalid playbook search text. | -- | -- |
| 400 | SecMaster.20048022 | The end time must be later than the start time. | -- | -- |
| 400 | SecMaster.20048023 | Failed to register schedule job of playbook. | -- | -- |
| 400 | SecMaster.20048024 | Failed to disable schedule job of playbook. | -- | -- |
| 400 | SecMaster.20048025 | End time of the schedule playbook must be larger than start time. | -- | -- |
| 400 | SecMaster.20048026 | End time of the schedule playbook is invalid. | -- | -- |
| 400 | SecMaster.20048027 | The data class id of playbook is empty. | -- | -- |
| 400 | SecMaster.20048028 | The matching process of playbook is not enabled. You cannot submit the version | -- | -- |
| 400 | SecMaster.20048029 | Failed to convert data of playbook | -- | -- |
| 400 | SecMaster.20048030 | The number of playbooks exceeds the limit. | -- | -- |

| Status Code | Error Codes | Error Message | Description | Solution |
| --- | --- | --- | --- | --- |
| 400 | SecMaster.20048031 | The number of matching process exceeds the limit. | -- | -- |
| 400 | SecMaster.20048032 | The scheduled interval of playbook is invalid. | -- | -- |
| 400 | SecMaster.20048033 | The matching process of playbook can not be empty. | -- | -- |
| 400 | SecMaster.20048034 | The dataclass of matching process is inconsistent with the dataclass of playbook. | -- | -- |
| 400 | SecMaster.20048035 | The built-in playbook cannot be modified. | -- | -- |
| 400 | SecMaster.20048036 | The built-in playbook cannot be deleted. | -- | -- |

# A.3 Obtaining a Project ID

## Obtaining a Project ID by Calling an API

You can obtain the project ID by calling the API used to **query project information based on the specified criteria**.

The API used to obtain a project ID is GET https://{Endpoint}/v3/projects. **{Endpoint}** is the IAM endpoint and can be obtained from **Regions and Endpoints**. For details about API authentication, see **Authentication**.

In the following example, **id** indicates the project ID.

```
{
    "projects": [
        {
            "domain_id": "65382450e8f64ac0870cd180d14e684b",
```

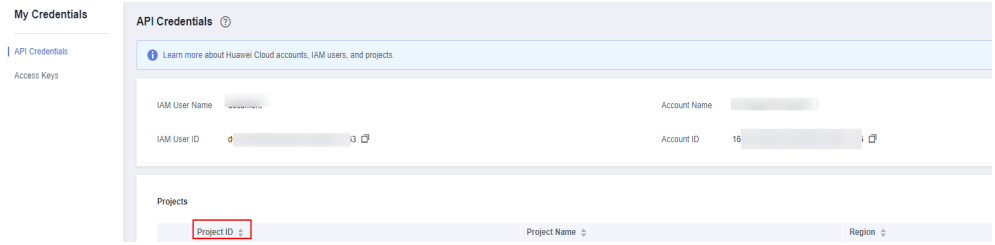
```
            "is_domain": false,
            "parent_id": "65382450e8f64ac0870cd180d14e684b",
            "name": "xxxxxxxx",
            "description": "",
            "links": {
                "next": null,
                "previous": null,
                "self": "https://www.example.com/v3/projects/a4a5d4098fb4474fa22cd05f897d6b99"
            },
            "id": "a4a5d4098fb4474fa22cd05f897d6b99",
            "enabled": true
        }
    ],
    "links": {
        "next": null,
        "previous": null,
        "self": "https://www.example.com/v3/projects"
    }
}
```


## Obtaining a Project ID from the Console

A project ID is required for some URLs when an API is called. To obtain a project ID, perform the following operations:

1. Log in to the management console.
2. Click the username and choose **My Credentials** from the drop-down list.
3. On the page, view the project ID in the project list.

**Figure A-1** Viewing project IDs



# B Change History

| Released On | Description |
| --- | --- |
| 2024-03-20 | This issue is the sixth official release.<br>• Updated parameter descriptions and examples of some APIs. |
| 2024-01-31 | This issue is the fifth official release.<br>• Updated parameter descriptions and examples of some APIs. |
| 2023-12-11 | This issue is the fourth official release.<br>• Added online API debugging, CLI examples, and SDK code examples.<br>• Added the description of APIs related to data space and pipeline management. |
| 2023-11-03 | This issue is the third official release.<br>• Updated the description of API parameters.<br>• Updated error codes. |
| 2023-08-10 | This issue is the second official release.<br>• Updated the description of API parameters.<br>• Updated error codes. |
| 2023-05-26 | This issue is the first official release. |