

SecMaster

API Reference

Issue 01
Date 2024-12-23



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI 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
2 API Overview	3
3 Calling APIs	5
3.1 Making an API Request	5
3.2 Authentication	7
3.3 Response	9
4 API	11
4.1 Alert Management	11
4.1.1 Searching for an Alert List	11
4.1.2 Creating an Alert Rule	27
4.1.3 Deleting an Alert	52
4.1.4 This API is used to convert alerts to incidents	54
4.1.5 Querying Alert Detail	57
4.1.6 Updating an Alert	71
4.2 Incident Management	96
4.2.1 This API is used to search for the incident list	96
4.2.2 Creating an Incident	111
4.2.3 Deleting an Incident	136
4.2.4 Obtaining Details of an Incident	138
4.2.5 Updating an Incident	151
4.3 Indicator Management	177
4.3.1 Query the intelligence indicator list	177
4.3.2 Creating an Indicator	183
4.3.3 This API is used to delete an indicator	190
4.3.4 Querying Indicator Details	193
4.3.5 Updating Indicators	198
4.4 Playbook Management	205
4.4.1 Playbook Running Monitoring	205
4.4.2 Querying Playbook Statistic Data	209
4.4.3 Querying the Playbook List	212
4.4.4 Creating a Playbook	216
4.4.5 Querying Playbook Details	219

4.4.6 Deleting a Playbook.....	222
4.4.7 Modifying a Playbook.....	226
4.5 Alert Rule Management.....	229
4.5.1 Listing Alert Rules.....	229
4.5.2 Creating an Alert Rule.....	234
4.5.3 Deleting an Alert Rule.....	240
4.5.4 Querying an Alert Rule.....	244
4.5.5 Updating an Alert Rule.....	248
4.5.6 Simulating an Alert Rule.....	254
4.5.7 Total number of alert rules.....	257
4.5.8 Enabling an Alert Rule.....	259
4.5.9 Disabling an Alert Rule.....	263
4.5.10 Listing Alert Rule Templates.....	267
4.5.11 Viewing Alert Rule Templates.....	271
4.6 Playbook Version Management.....	275
4.6.1 Cloning a Playbook and Its Version.....	275
4.6.2 Querying the Playbook Version List.....	280
4.6.3 Creating a Playbook Version.....	284
4.6.4 Querying Playbook Version Details.....	290
4.6.5 Deleting a Playbook Version.....	295
4.6.6 Updated the playbook version.....	297
4.7 Playbook Rule Management.....	303
4.7.1 Querying Playbook Rule Details.....	303
4.7.2 Deleting a Playbook Rule.....	306
4.7.3 Creating a Playbook Rule.....	308
4.7.4 Updating a Playbook Rule.....	313
4.8 Playbook Instance Management.....	317
4.8.1 Querying the Playbook Instance List.....	317
4.8.2 Querying Playbook Instance Details.....	322
4.8.3 Operation Playbook Instance.....	326
4.8.4 Querying the Playbook Topology.....	330
4.8.5 Querying Playbook Instance Audit Logs.....	333
4.9 Playbook Approval Management.....	338
4.9.1 Reviewing a Playbook.....	338
4.9.2 Querying Playbook Review Result.....	341
4.10 Playbook Action Management.....	343
4.10.1 Querying the Playbook Workflow.....	344
4.10.2 Creating a Playbook Action.....	347
4.10.3 Delete Playbook Action.....	350
4.10.4 Updating a Playbook Workflow.....	353
4.11 Incident Relationship Management.....	356
4.11.1 Querying the Associated Data Object List.....	356

4.11.2 Associating a Data Object.....	369
4.11.3 Canceling Association with a Data Object.....	373
4.12 Data Class Management.....	376
4.12.1 Querying the Data Class List.....	376
4.12.2 Querying the Data Class List.....	379
4.13 Workflow Management.....	384
4.13.1 Querying the Workflow List.....	384
4.14 Data Space Management.....	388
4.14.1 Creating a Data Space.....	388
4.15 Pipelines.....	390
4.15.1 Creating a Data Pipeline.....	390
4.16 Workspace Management.....	394
4.16.1 Creating a Workspace.....	394
4.16.2 Querying the Workspace List.....	399
4.17 Metering and Billing.....	404
4.17.1 On-Demand Subscription of SecMaster.....	404
4.18 Metric Query.....	408
4.18.1 Querying Metrics in Batches.....	408
4.19 Baseline Inspection.....	412
4.19.1 Search Baseline Check Results.....	412
A Appendix.....	419
A.1 Status Codes.....	419
A.2 Error Codes.....	419
A.3 Obtaining a Project ID.....	423
A.4 About Metrics.....	424

1 Before You Start

SecMaster is a next-gen cloud-native security operations center that helps with cloud asset management, security posture management, security information and incident management, security orchestration, and automatic response. It helps prevent risks, detect threats, and automatically handle security incidents.

Before calling SecMaster APIs, ensure that you have understood the concepts related to SecMaster. For more details, see [Service Overview](#).

Endpoints

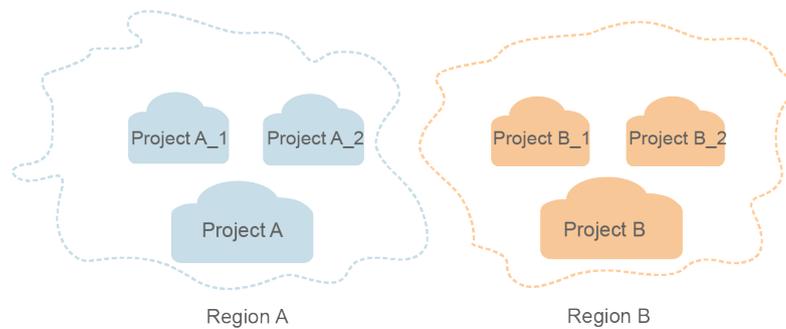
An endpoint is the **request address** for calling an API. Endpoints vary depending on services and regions. For the endpoints of all services, see regions and endpoints.

Basic 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 isolating 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 API Overview

You can use all SecMaster functions through APIs.

Type	Description
Alert APIs	APIs for creating, deleting, and converting alerts to incidents.
Incident APIs	APIs for creating, updating, and obtaining incidents.
Indicator APIs	APIs for managing indicators, including APIs for creating, updating, and obtaining indicators.
Playbook APIs	APIs for querying, creating, and modifying playbooks.
Alert rule API	APIs for creating, deleting, viewing, and enabling alert rules.
Playbook version APIs	APIs for querying, creating, and updating playbook versions.
Playbook rule API	APIs for creating, querying, and deleting playbook rules.
Playbook instance API	APIs for querying and operating playbook instances.
Playbook review API	Playbook review APIs, including the APIs for reviewing playbooks and querying playbook review results.
Incident associations APIs	APIs for querying, creating, and cancelling incident associations.
Data class APIs	APIs for querying the data class list and field list.
Workflow APIs	Workflow APIs, including the API for querying the workflow list.
Data space APIs	Data space APIs, including the API for creating data spaces.
Pipeline APIs	Pipeline APIs, including the API for creating a pipeline.

Type	Description
Workspace APIs	Workspace APIs, including the APIs for adding and querying workspaces.
Metering and billing APIs	Metering and billing APIs
Metric APIs	APIs for querying metrics, including the API for batch queries.
Baseline inspection APIs	Baseline inspection APIs, including the API for searching check results.

3 Calling APIs

3.1 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 the administrator.
- **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.

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 **xxxxxxxxxxxxxxxxxxxx** to the project name. You can learn more information about projects from the administrator.

 **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": "xxxxxxxxxxxxxxxxxxxx"
      }
    }
  }
}
```

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.

3.2 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": "xxxxxxx"
      }
    }
  }
}
```

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.

NOTICE

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

3.3 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 3-1](#) 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 3-1 Header of the response to the request for obtaining a user token

```

connection → keep-alive
content-type → application/json
date → Tue, 12 Feb 2019 06:52:13 GMT
server → Web Server
strict-transport-security → max-age=31536000; includeSubdomains;
transfer-encoding → chunked
via → proxy A
x-content-type-options → nosniff
x-download-options → noopen
x-frame-options → SAMEORIGIN
x-iam-trace-id → 218d45ab-d674-4995-af3a-2d0255ba41b5
x-subject-token → MIIVXQVJKoZIhvcNAQcCoIIYJCCEoCAQExDTALBglghkgBZQMEAgEwgharBgkqhkiG9w0BBwGgghacBIIWmHsidG9rZW4iOnsiZXhwaXJlc19hdCI6ijlwMTktMDItMTNUMC
fj3KJ56YgKnpVNRbW2eZ5eb78SZOkqjACgkqO1wi4JlGzrpd18LGXK5tdffq4lqHCYb8P4NaYONYeicAgzIVeFYtLWT1GSO0zxKZmlQHqJ82HBqHdglZO9fuEbL5dMhdavj+33wEI
xHRCe9I87o+k9-
j+CMZSEB7bUGd5Uj6eRASXI1jipPEGA270g1FruooL6jggIFkNPQuFSOU8+uSsttVwRtNfsC+qTp22Rkd5MCqFGQ8LcuXc3a+9CMBnOintWW7oeRUVhVpxk8pxiX1wTEboX-
RzT6MUbvpGw-oPNFYxJECKnoH3HRozv0wN--n5d6Nbxg==
x-xss-protection → 1; mode=block;

```

(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": "xxxxxxx",
            .....

```

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.

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.
workspace_id	Yes	String	Workspace ID

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.
content-type	Yes	String	Content type.

Table 4-3 Request body parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page.
offset	No	Integer	Offset
sort_by	No	String	Sorting field -- create_time update_time
order	No	String	Sort by -- DESC ASC
from_date	No	String	Search start time, for example, 2023-02-20T00:00:00.000Z
to_date	No	String	Search end time, for example, 2023-02-27T23:59:59.999Z
condition	No	condition object	Search condition expression.

Table 4-4 condition

Parameter	Mandatory	Type	Description
conditions	No	Array of conditions objects	Expression list.
logics	No	Array of strings	Expression logic.

Table 4-5 conditions

Parameter	Mandatory	Type	Description
name	No	String	Expression name.
data	No	Array of strings	Expression content list.

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
message	String	Error Message
total	Integer	Total number of alerts.
limit	Integer	Number of records displayed on each page.
offset	Integer	Offset
success	Boolean	Successful or not.
data	Array of ListAlertDetail objects	Alert list.

Table 4-8 ListAlertDetail

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.
data_object	ListAlertRsp object	Alert entity information.
dataclass_ref	dataclass_ref object	Data class object.
format_version	Integer	Format version.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
type	String	Data Types.
project_id	String	ID of the current project.
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.
version	Integer	Version.
workspace_id	String	ID of the current workspace.

Table 4-9 ListAlertRsp

Parameter	Type	Description
version	String	Version of the data source of the alert. The value must be one officially released by the Cloud SSA service.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	String	ID of the account (domain_id) to whom the data is delivered and hosted.

Parameter	Type	Description
region_id	String	ID of the region where the account to whom the data is delivered and hosted belongs to.
workspace_id	String	ID of the current workspace.
labels	String	Tag (display only)
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.
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.
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.
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.
title	String	Alert title.
description	String	Alert description.
source_url	String	Alert URL, which points to the page of the current incident description in the data source product.
count	Integer	Incident occurrences

Parameter	Type	Description
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%.
severity	String	Severity level. Value range: Tips Low Medium High Fatal Description: <ul style="list-style-type: none"> • 0: TIPS: No threats are found. • 1: LOW: No actions are required for the threat. • 2: MEDIUM: The threat needs to be handled but is not urgent. • 3: HIGH: The threat must be handled preferentially. • 4: FATAL: The threat must be handled immediately to prevent further damage.
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.
alert_type	alert_type object	Alert classification. For details, see the Alert Type Definition.
network_list	Array of network_list objects	Network Information
resource_list	Array of resource_list objects	Affected resources.
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: <ul style="list-style-type: none"> - Unknown - True_Positive - False_Positive Enter Unknown by default.
handle_status	String	Incident handling status. The options are as follows: <ul style="list-style-type: none"> • Open: enabled. • Block: blocked. • Closed: closed. The default value is Open.
sla	String	Risk close 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.
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.
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.
ipdrr_phase	String	Period/Handling phase No. Preparation Detection and Analysis Containment,Eradiation& Recovery Post-Incident-Activity
chop_phase	String	Period/Handling phase No. Preparation Detection and Analysis Containment,Eradiation& Recovery Post-Incident-Activity

Parameter	Type	Description
ppdr_phase	String	Period/Handling phase No. Preparation Detection and Analysis Containm,Eradiation& Recovery Post-Incident-Activity
simulation	String	Debugging field.
actor	String	Alert investigator.
owner	String	Owner and service owner.
creator	String	Creator
close_reason	String	Close reason. <ul style="list-style-type: none"> • False detection. • Resolved • Repeated • Other
close_comment	String	Whether to close comment.
malware	malware object	Malware
system_info	Object	System information.
process	Array of process objects	Process information.
user_info	Array of user_info objects	User Details
file_info	Array of file_info objects	Document information.
system_alert_table	Object	Layout fields in the alerts list.

Table 4-10 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Tenant ID.
region_id	String	Region ID. global is returned for global services.
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.

Parameter	Type	Description
project_id	String	Project ID. The default value is null for global services.

Table 4-11 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows-- 1- cloud product 2- Third-party product 3- Tenant product
domain_id	String	Account ID to which the data source product belongs.
project_id	String	ID of the project to which the data source product belongs.
region_id	String	Region where the data source is located, for example, cn-north1. For details about the value range, see <i>Regions and Endpoints</i> .
company_name	String	Name of the company to which a data source belongs.
product_name	String	Name of the data source.
product_feature	String	Name of the feature of the product that detects the incident.
product_module	String	Threat detection module list.

Table 4-12 alert_type

Parameter	Type	Description
category	String	Type
alert_type	String	Alert type.

Table 4-13 network_list

Parameter	Type	Description
direction	String	Direction. The value can be IN or OUT.

Parameter	Type	Description
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 .
src_ip	String	Source IP address
src_port	Integer	Source port. The value ranges from 0 to 65535.
src_domain	String	Source domain name.
src_geo	src_geo object	Geographical location of the source IP address.
dest_ip	String	Destination IP address
dest_port	String	Destination port. The value ranges from 0 to 65535.
dest_domain	String	Destination domain name
dest_geo	dest_geo object	Geographical location of the destination IP address.

Table 4-14 src_geo

Parameter	Type	Description
latitude	Number	Latitude
longitude	Number	Longitude
city_code	String	City code. For example, Beijing or Shanghai.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-15 dest_geo

Parameter	Type	Description
latitude	Number	Latitude
longitude	Number	Longitude

Parameter	Type	Description
city_code	String	City code. For example, Beijing or Shanghai.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-16 resource_list

Parameter	Type	Description
id	String	Cloud service resource ID.
name	String	Resource name.
type	String	Resource type. This parameter references the value of RMS type on Cloud.
provider	String	Cloud service name, which is the same as the provider field in the RMS service.
region_id	String	Region ID in Cloud, for example, cn-north-1.
domain_id	String	ID of the account to which the resource belongs, in UUID format.
project_id	String	ID of the account to which the resource belongs, in UUID format.
ep_id	String	Specifies the enterprise project ID.
ep_name	String	Enterprise Project Name
tags	String	Resource tag. 1. A maximum of 50 key/value pairs are supported. 2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _ , ; , / , @

Table 4-17 remediation

Parameter	Type	Description
recommendation	String	Recommended solution.

Parameter	Type	Description
url	String	Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-18 malware

Parameter	Type	Description
malware_family	String	Malicious family.
malware_class	String	Malware category.

Table 4-19 process

Parameter	Type	Description
process_name	String	Process name.
process_path	String	Process execution file path.
process_pid	Integer	Process ID.
process_uid	Integer	Process user ID.
process_cmdline	String	Process command line.
process_parent_name	String	Parent process name.
process_parent_path	String	Parent process execution file path.
process_parent_pid	Integer	Parent process ID.
process_parent_uid	Integer	Parent process user ID.
process_parent_cmdline	String	Parent process command line.
process_child_name	String	Subprocess name.
process_child_path	String	Subprocess execution file path.
process_child_pid	Integer	Subprocess ID.
process_child_uid	Integer	Subprocess user ID.

Parameter	Type	Description
process_child_command_line	String	Subprocess command line
process_launch_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.
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.

Table 4-20 user_info

Parameter	Type	Description
user_id	String	User UID
user_name	String	Username

Table 4-21 file_info

Parameter	Type	Description
file_path	String	File path/name.
file_content	String	File path/name.
file_new_path	String	New file path/name.
file_hash	String	File Hash
file_md5	String	File MD5
file_sha256	String	File SHA256
file_attr	String	File attribute.

Table 4-22 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.
name	String	Data class name.

Status code: 400

Table 4-23 Response header parameters

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

Table 4-24 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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" : "2021-01-30T23:00:00Z+0800",
  "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"
}
}
}
}

```

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 4-25 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID

Request Parameters

Table 4-26 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.
content-type	Yes	String	Content type.

Table 4-27 Request body parameters

Parameter	Mandatory	Type	Description
data_object	Yes	Alert object	Alert entity information.

Table 4-28 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 Cloud SSA service.
id	No	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	No	String	ID of the account (domain_id) to whom the data is delivered and hosted.
region_id	No	String	ID of the region where the account to whom the data is delivered and hosted belongs to.
workspace_id	No	String	ID of the current workspace.
labels	No	String	Tag (display only)
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.

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.
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.
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.
title	No	String	Alert title.
description	No	String	Alert description.
source_url	No	String	Alert URL, which points to the page of the current incident description in the data source product.
count	No	Integer	Incident occurrences
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%.

Parameter	Mandatory	Type	Description
severity	No	String	Severity level. Value range: Tips Low Medium High Fatal Description: <ul style="list-style-type: none"> • 0: TIPS: No threats are found. • 1: LOW: No actions are required for the threat. • 2: MEDIUM: The threat needs to be handled but is not urgent. • 3: HIGH: The threat must be handled preferentially. • 4: FATAL: The threat must be handled immediately to prevent further damage.
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.
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
resource_list	No	Array of resource_list objects	Affected resources.
remediation	No	remediation object	Remedy measure.
verification_state	No	String	Verification status, which identifies the accuracy of an incident. The options are as follows: <ul style="list-style-type: none"> - Unknown - True_Positive - False_Positive Enter Unknown by default.

Parameter	Mandatory	Type	Description
handle_status	No	String	Incident handling status. The options are as follows: <ul style="list-style-type: none"> • Open: enabled. • Block: blocked. • Closed: closed. The default value is Open.
sla	No	Integer	Risk close time -- Set the acceptable risk duration. Unit -- Hour
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.
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.
ipdrr_phase	No	String	Period/Handling phase No. Preparation Detection and Analysis Containm,Eradication& Recovery Post-Incident-Activity
simulation	No	String	Debugging field.
actor	No	String	Alert investigator.
owner	No	String	Owner and service owner.
creator	No	String	Creator
close_reason	No	String	Close reason. <ul style="list-style-type: none"> • False detection. • Resolved • Repeated • Other
close_comment	No	String	Whether to close comment.

Parameter	Mandatory	Type	Description
malware	No	malware object	Malware
system_info	No	Object	System information.
process	No	Array of process objects	Process information.
user_info	No	Array of user_info objects	User Details
file_info	No	Array of file_info objects	Document information.
system_alert_table	No	Object	Layout fields in the alerts list.

Table 4-29 environment

Parameter	Mandatory	Type	Description
vendor_type	No	String	Environment provider.
domain_id	No	String	Tenant ID.
region_id	No	String	Region ID. global is returned for global services.
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.
project_id	No	String	Project ID. The default value is null for global services.

Table 4-30 data_source

Parameter	Mandatory	Type	Description
source_type	No	Integer	Data source type. The options are as follows-- 1- cloud product 2- Third-party product 3- Tenant product

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

Table 4-31 alert_type

Parameter	Mandatory	Type	Description
category	No	String	Type
alert_type	No	String	Alert type.

Table 4-32 network_list

Parameter	Mandatory	Type	Description
direction	No	String	Direction. The value can be IN or 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 .
src_ip	No	String	Source IP address

Parameter	Mandatory	Type	Description
src_port	No	Integer	Source port. The value ranges from 0 to 65535.
src_domain	No	String	Source domain name.
src_geo	No	src_geo object	Geographical location of the source IP address.
dest_ip	No	String	Destination IP address
dest_port	No	String	Destination port. The value ranges from 0 to 65535.
dest_domain	No	String	Destination domain name
dest_geo	No	dest_geo object	Geographical location of the destination IP address.

Table 4-33 src_geo

Parameter	Mandatory	Type	Description
latitude	No	Number	Latitude
longitude	No	Number	Longitude
city_code	No	String	City code. For example, Beijing or Shanghai.
country_code	No	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-34 dest_geo

Parameter	Mandatory	Type	Description
latitude	No	Number	Latitude
longitude	No	Number	Longitude
city_code	No	String	City code. For example, Beijing or Shanghai.
country_code	No	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-35 resource_list

Parameter	Mandatory	Type	Description
id	No	String	Cloud service resource ID.
name	No	String	Resource name.
type	No	String	Resource type. This parameter references the value of RMS type on Cloud.
provider	No	String	Cloud service name, which is the same as the provider field in the RMS service.
region_id	No	String	Region ID in Cloud, for example, cn-north-1.
domain_id	No	String	ID of the account to which the resource belongs, in UUID format.
project_id	No	String	ID of the account to which the resource belongs, in UUID format.
ep_id	No	String	Specifies the enterprise project ID.
ep_name	No	String	Enterprise Project Name
tags	No	String	Resource tag. 1. A maximum of 50 key/value pairs are supported. 2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _ ; , /, @

Table 4-36 remediation

Parameter	Mandatory	Type	Description
recommendation	No	String	Recommended solution.
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.

Table 4-37 malware

Parameter	Mandatory	Type	Description
malware_family	No	String	Malicious family.
malware_class	No	String	Malware category.

Table 4-38 process

Parameter	Mandatory	Type	Description
process_name	No	String	Process name.
process_path	No	String	Process execution file path.
process_pid	No	Integer	Process ID.
process_uid	No	Integer	Process user ID.
process_cmdline	No	String	Process command line.
process_parent_name	No	String	Parent process name.
process_parent_path	No	String	Parent process execution file path.
process_parent_pid	No	Integer	Parent process ID.
process_parent_uid	No	Integer	Parent process user ID.
process_parent_cmdline	No	String	Parent process command line.
process_child_name	No	String	Subprocess name.
process_child_path	No	String	Subprocess execution file path.
process_child_pid	No	Integer	Subprocess ID.
process_child_uid	No	Integer	Subprocess user ID.
process_child_cmdline	No	String	Subprocess command line

Parameter	Mandatory	Type	Description
process_launched_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.
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.

Table 4-39 user_info

Parameter	Mandatory	Type	Description
user_id	No	String	User UID
user_name	No	String	Username

Table 4-40 file_info

Parameter	Mandatory	Type	Description
file_path	No	String	File path/name.
file_content	No	String	File path/name.
file_new_path	No	String	New file path/name.
file_hash	No	String	File Hash
file_md5	No	String	File MD5
file_sha256	No	String	File SHA256
file_attr	No	String	File attribute.

Response Parameters

Status code: 200

Table 4-41 Response header parameters

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

Table 4-42 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
data	AlertDetail object	Alert Detail

Table 4-43 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.
data_object	Alert object	Alert entity information.
dataclass_ref	dataclass_ref object	Data class object.
format_version	Integer	Format version.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
type	String	Data Types.
project_id	String	ID of the current project.
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.
version	Integer	Version.
workspace_id	String	ID of the current workspace.

Table 4-44 Alert

Parameter	Type	Description
version	String	Version of the data source of the alert. The value must be one officially released by the Cloud SSA service.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	String	ID of the account (domain_id) to whom the data is delivered and hosted.
region_id	String	ID of the region where the account to whom the data is delivered and hosted belongs to.
workspace_id	String	ID of the current workspace.
labels	String	Tag (display only)
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.
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.
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.

Parameter	Type	Description
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.
title	String	Alert title.
description	String	Alert description.
source_url	String	Alert URL, which points to the page of the current incident description in the data source product.
count	Integer	Incident occurrences
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%.
severity	String	Severity level. Value range: Tips Low Medium High Fatal Description: <ul style="list-style-type: none"> ● 0: TIPS: No threats are found. ● 1: LOW: No actions are required for the threat. ● 2: MEDIUM: The threat needs to be handled but is not urgent. ● 3: HIGH: The threat must be handled preferentially. ● 4: FATAL: The threat must be handled immediately to prevent further damage.
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.
alert_type	alert_type object	Alert classification. For details, see the Alert Type Definition.

Parameter	Type	Description
network_list	Array of network_list objects	Network Information
resource_list	Array of resource_list objects	Affected resources.
remediation	remediation object	Remedy measure.
verification_state	String	Verification status, which identifies the accuracy of an incident. The options are as follows: <ul style="list-style-type: none"> - Unknown - True_Positive - False_Positive Enter Unknown by default.
handle_status	String	Incident handling status. The options are as follows: <ul style="list-style-type: none"> • Open: enabled. • Block: blocked. • Closed: closed. The default value is Open.
sla	Integer	Risk close time -- Set the acceptable risk duration. Unit -- Hour
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.
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.
ipdr_phase	String	Period/Handling phase No. Preparation Detection and Analysis Containm,Eradication& Recovery Post-Incident-Activity
simulation	String	Debugging field.
actor	String	Alert investigator.

Parameter	Type	Description
owner	String	Owner and service owner.
creator	String	Creator
close_reason	String	Close reason. <ul style="list-style-type: none"> • False detection. • Resolved • Repeated • Other
close_comment	String	Whether to close comment.
malware	malware object	Malware
system_info	Object	System information.
process	Array of process objects	Process information.
user_info	Array of user_info objects	User Details
file_info	Array of file_info objects	Document information.
system_alert_table	Object	Layout fields in the alerts list.

Table 4-45 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Tenant ID.
region_id	String	Region ID. global is returned for global services.
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.
project_id	String	Project ID. The default value is null for global services.

Table 4-46 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows-- 1- cloud product 2- Third-party product 3- Tenant product
domain_id	String	Account ID to which the data source product belongs.
project_id	String	ID of the project to which the data source product belongs.
region_id	String	Region where the data source is located, for example, cn-north1. For details about the value range, see <i>Regions and Endpoints</i> .
company_name	String	Name of the company to which a data source belongs.
product_name	String	Name of the data source.
product_feature	String	Name of the feature of the product that detects the incident.
product_module	String	Threat detection module list.

Table 4-47 alert_type

Parameter	Type	Description
category	String	Type
alert_type	String	Alert type.

Table 4-48 network_list

Parameter	Type	Description
direction	String	Direction. The value can be IN or 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 .
src_ip	String	Source IP address

Parameter	Type	Description
src_port	Integer	Source port. The value ranges from 0 to 65535.
src_domain	String	Source domain name.
src_geo	src_geo object	Geographical location of the source IP address.
dest_ip	String	Destination IP address
dest_port	String	Destination port. The value ranges from 0 to 65535.
dest_domain	String	Destination domain name
dest_geo	dest_geo object	Geographical location of the destination IP address.

Table 4-49 src_geo

Parameter	Type	Description
latitude	Number	Latitude
longitude	Number	Longitude
city_code	String	City code. For example, Beijing or Shanghai.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-50 dest_geo

Parameter	Type	Description
latitude	Number	Latitude
longitude	Number	Longitude
city_code	String	City code. For example, Beijing or Shanghai.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-51 resource_list

Parameter	Type	Description
id	String	Cloud service resource ID.
name	String	Resource name.
type	String	Resource type. This parameter references the value of RMS type on Cloud.
provider	String	Cloud service name, which is the same as the provider field in the RMS service.
region_id	String	Region ID in Cloud, for example, cn-north-1.
domain_id	String	ID of the account to which the resource belongs, in UUID format.
project_id	String	ID of the account to which the resource belongs, in UUID format.
ep_id	String	Specifies the enterprise project ID.
ep_name	String	Enterprise Project Name
tags	String	Resource tag. 1. A maximum of 50 key/value pairs are supported. 2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _ , ; , /, @

Table 4-52 remediation

Parameter	Type	Description
recommendation	String	Recommended solution.
url	String	Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-53 malware

Parameter	Type	Description
malware_family	String	Malicious family.

Parameter	Type	Description
malware_class	String	Malware category.

Table 4-54 process

Parameter	Type	Description
process_name	String	Process name.
process_path	String	Process execution file path.
process_pid	Integer	Process ID.
process_uid	Integer	Process user ID.
process_cmdline	String	Process command line.
process_parent_name	String	Parent process name.
process_parent_path	String	Parent process execution file path.
process_parent_pid	Integer	Parent process ID.
process_parent_uid	Integer	Parent process user ID.
process_parent_cmdline	String	Parent process command line.
process_child_name	String	Subprocess name.
process_child_path	String	Subprocess execution file path.
process_child_pid	Integer	Subprocess ID.
process_child_uid	Integer	Subprocess user ID.
process_child_cmdline	String	Subprocess command line
process_launched_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.

Parameter	Type	Description
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.

Table 4-55 user_info

Parameter	Type	Description
user_id	String	User UID
user_name	String	Username

Table 4-56 file_info

Parameter	Type	Description
file_path	String	File path/name.
file_content	String	File path/name.
file_new_path	String	New file path/name.
file_hash	String	File Hash
file_md5	String	File MD5
file_sha256	String	File SHA256
file_attr	String	File attribute.

Table 4-57 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.
name	String	Data class name.

Status code: 400

Table 4-58 Response header parameters

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

Table 4-59 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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",
"ipdr_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"
}
}
}
}

```

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 4-60 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID

Request Parameters

Table 4-61 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.
content-type	Yes	String	Content type.

Table 4-62 Request body parameters

Parameter	Mandatory	Type	Description
batch_ids	No	Array of strings	IDs of deleted alerts

Response Parameters

Status code: 200

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
message	String	Error Message
data	BatchOperateAlertResult object	Returned object for batch operation on alerts.

Table 4-65 BatchOperateAlertResult

Parameter	Type	Description
error_ids	Array of strings	IDs of alerts not transferred to incidents
success_ids	Array of strings	IDs of alerts transferred to incidents.

Status code: 400

Table 4-66 Response header parameters

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

Table 4-67 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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" ]
  }
}
```

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 4-68 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Parameter	Mandatory	Type	Description
workspace_id	Yes	String	Workspace ID

Request Parameters

Table 4-69 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.
content-type	Yes	String	Content type.

Table 4-70 Request body parameters

Parameter	Mandatory	Type	Description
ids	No	Array of strings	IDs of the alerts to be converted into incidents.
incident_content	No	incident_content object	Incident details.

Table 4-71 incident_content

Parameter	Mandatory	Type	Description
title	No	String	Trace
incident_type	No	incident_type object	Incident type.

Table 4-72 incident_type

Parameter	Mandatory	Type	Description
id	No	String	Incident type ID
category	No	String	Parent incident type.
incident_type	No	String	Child incident type.

Response Parameters

Status code: 200

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
message	String	Error Message
data	BatchOperateAlertResult object	Returned object for batch operation on alerts.

Table 4-75 BatchOperateAlertResult

Parameter	Type	Description
error_ids	Array of strings	IDs of alerts not transferred to incidents
success_ids	Array of strings	IDs of alerts transferred to incidents.

Status code: 400

Table 4-76 Response header parameters

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

Table 4-77 Response body parameters

Parameter	Type	Description
code	String	Error Code

Parameter	Type	Description
message	String	Error Description

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" ]
  }
}
```

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 4-78 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
alert_id	Yes	String	Alert ID.

Request Parameters

Table 4-79 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.
content-type	Yes	String	Content type.

Response Parameters

Status code: 200

Table 4-80 Response header parameters

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

Table 4-81 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
data	AlertDetail object	Alert Detail

Table 4-82 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.
data_object	Alert object	Alert entity information.
dataclass_ref	dataclass_ref object	Data class object.
format_version	Integer	Format version.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
type	String	Data Types.
project_id	String	ID of the current project.
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.
version	Integer	Version.
workspace_id	String	ID of the current workspace.

Table 4-83 Alert

Parameter	Type	Description
version	String	Version of the data source of the alert. The value must be one officially released by the Cloud SSA service.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	String	ID of the account (domain_id) to whom the data is delivered and hosted.
region_id	String	ID of the region where the account to whom the data is delivered and hosted belongs to.
workspace_id	String	ID of the current workspace.
labels	String	Tag (display only)
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.
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.
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.

Parameter	Type	Description
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.
title	String	Alert title.
description	String	Alert description.
source_url	String	Alert URL, which points to the page of the current incident description in the data source product.
count	Integer	Incident occurrences
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%.
severity	String	Severity level. Value range: Tips Low Medium High Fatal Description: <ul style="list-style-type: none"> ● 0: TIPS: No threats are found. ● 1: LOW: No actions are required for the threat. ● 2: MEDIUM: The threat needs to be handled but is not urgent. ● 3: HIGH: The threat must be handled preferentially. ● 4: FATAL: The threat must be handled immediately to prevent further damage.
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.
alert_type	alert_type object	Alert classification. For details, see the Alert Type Definition.

Parameter	Type	Description
network_list	Array of network_list objects	Network Information
resource_list	Array of resource_list objects	Affected resources.
remediation	remediation object	Remedy measure.
verification_state	String	Verification status, which identifies the accuracy of an incident. The options are as follows: <ul style="list-style-type: none"> - Unknown - True_Positive - False_Positive Enter Unknown by default.
handle_status	String	Incident handling status. The options are as follows: <ul style="list-style-type: none"> • Open: enabled. • Block: blocked. • Closed: closed. The default value is Open.
sla	Integer	Risk close time -- Set the acceptable risk duration. Unit -- Hour
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.
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.
ipdr_phase	String	Period/Handling phase No. Preparation Detection and Analysis Containm,Eradication& Recovery Post-Incident-Activity
simulation	String	Debugging field.
actor	String	Alert investigator.

Parameter	Type	Description
owner	String	Owner and service owner.
creator	String	Creator
close_reason	String	Close reason. <ul style="list-style-type: none"> • False detection. • Resolved • Repeated • Other
close_comment	String	Whether to close comment.
malware	malware object	Malware
system_info	Object	System information.
process	Array of process objects	Process information.
user_info	Array of user_info objects	User Details
file_info	Array of file_info objects	Document information.
system_alert_table	Object	Layout fields in the alerts list.

Table 4-84 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Tenant ID.
region_id	String	Region ID. global is returned for global services.
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.
project_id	String	Project ID. The default value is null for global services.

Table 4-85 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows-- 1- cloud product 2- Third-party product 3- Tenant product
domain_id	String	Account ID to which the data source product belongs.
project_id	String	ID of the project to which the data source product belongs.
region_id	String	Region where the data source is located, for example, cn-north1. For details about the value range, see <i>Regions and Endpoints</i> .
company_name	String	Name of the company to which a data source belongs.
product_name	String	Name of the data source.
product_feature	String	Name of the feature of the product that detects the incident.
product_module	String	Threat detection module list.

Table 4-86 alert_type

Parameter	Type	Description
category	String	Type
alert_type	String	Alert type.

Table 4-87 network_list

Parameter	Type	Description
direction	String	Direction. The value can be IN or 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 .
src_ip	String	Source IP address

Parameter	Type	Description
src_port	Integer	Source port. The value ranges from 0 to 65535.
src_domain	String	Source domain name.
src_geo	src_geo object	Geographical location of the source IP address.
dest_ip	String	Destination IP address
dest_port	String	Destination port. The value ranges from 0 to 65535.
dest_domain	String	Destination domain name
dest_geo	dest_geo object	Geographical location of the destination IP address.

Table 4-88 src_geo

Parameter	Type	Description
latitude	Number	Latitude
longitude	Number	Longitude
city_code	String	City code. For example, Beijing or Shanghai.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-89 dest_geo

Parameter	Type	Description
latitude	Number	Latitude
longitude	Number	Longitude
city_code	String	City code. For example, Beijing or Shanghai.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-90 resource_list

Parameter	Type	Description
id	String	Cloud service resource ID.
name	String	Resource name.
type	String	Resource type. This parameter references the value of RMS type on Cloud.
provider	String	Cloud service name, which is the same as the provider field in the RMS service.
region_id	String	Region ID in Cloud, for example, cn-north-1.
domain_id	String	ID of the account to which the resource belongs, in UUID format.
project_id	String	ID of the account to which the resource belongs, in UUID format.
ep_id	String	Specifies the enterprise project ID.
ep_name	String	Enterprise Project Name
tags	String	Resource tag. 1. A maximum of 50 key/value pairs are supported. 2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _ ;, /, @

Table 4-91 remediation

Parameter	Type	Description
recommendation	String	Recommended solution.
url	String	Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-92 malware

Parameter	Type	Description
malware_family	String	Malicious family.

Parameter	Type	Description
malware_class	String	Malware category.

Table 4-93 process

Parameter	Type	Description
process_name	String	Process name.
process_path	String	Process execution file path.
process_pid	Integer	Process ID.
process_uid	Integer	Process user ID.
process_cmdline	String	Process command line.
process_parent_name	String	Parent process name.
process_parent_path	String	Parent process execution file path.
process_parent_pid	Integer	Parent process ID.
process_parent_uid	Integer	Parent process user ID.
process_parent_cmdline	String	Parent process command line.
process_child_name	String	Subprocess name.
process_child_path	String	Subprocess execution file path.
process_child_pid	Integer	Subprocess ID.
process_child_uid	Integer	Subprocess user ID.
process_child_cmdline	String	Subprocess command line
process_launched_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.

Parameter	Type	Description
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.

Table 4-94 user_info

Parameter	Type	Description
user_id	String	User UID
user_name	String	Username

Table 4-95 file_info

Parameter	Type	Description
file_path	String	File path/name.
file_content	String	File path/name.
file_new_path	String	New file path/name.
file_hash	String	File Hash
file_md5	String	File MD5
file_sha256	String	File SHA256
file_attr	String	File attribute.

Table 4-96 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.
name	String	Data class name.

Status code: 400

Table 4-97 Response header parameters

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

Table 4-98 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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",
"ipdr_phase" : "Preparation|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"
  }
}
}
}

```

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 4-99 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
alert_id	Yes	String	Alert ID.

Request Parameters

Table 4-100 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.
content-type	Yes	String	Content type.

Table 4-101 Request body parameters

Parameter	Mandatory	Type	Description
batch_ids	No	Array of strings	IDs of updated alerts.
data_object	No	Alert object	Alert entity information.

Table 4-102 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 Cloud SSA service.
id	No	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	No	String	ID of the account (domain_id) to whom the data is delivered and hosted.
region_id	No	String	ID of the region where the account to whom the data is delivered and hosted belongs to.
workspace_id	No	String	ID of the current workspace.
labels	No	String	Tag (display only)

Parameter	Mandatory	Type	Description
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.
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.
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.
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.
title	No	String	Alert title.
description	No	String	Alert description.
source_url	No	String	Alert URL, which points to the page of the current incident description in the data source product.
count	No	Integer	Incident occurrences

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%.
severity	No	String	Severity level. Value range: Tips Low Medium High Fatal Description: <ul style="list-style-type: none"> ● 0: TIPS: No threats are found. ● 1: LOW: No actions are required for the threat. ● 2: MEDIUM: The threat needs to be handled but is not urgent. ● 3: HIGH: The threat must be handled preferentially. ● 4: FATAL: The threat must be handled immediately to prevent further damage.
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.
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
resource_list	No	Array of resource_list objects	Affected resources.
remediation	No	remediation object	Remedy measure.

Parameter	Mandatory	Type	Description
verification_status	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.
handle_status	No	String	Incident handling status. The options are as follows: <ul style="list-style-type: none"> • Open: enabled. • Block: blocked. • Closed: closed. The default value is Open.
sla	No	Integer	Risk close time -- Set the acceptable risk duration. Unit -- Hour
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.
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.
ipdrr_phase	No	String	Period/Handling phase No. Preparation Detection and Analysis Containm,Eradiation& Recovery Post-Incident-Activity
simulation	No	String	Debugging field.
actor	No	String	Alert investigator.
owner	No	String	Owner and service owner.
creator	No	String	Creator

Parameter	Mandatory	Type	Description
close_reason	No	String	Close reason. <ul style="list-style-type: none"> • False detection. • Resolved • Repeated • Other
close_comment	No	String	Whether to close comment.
malware	No	malware object	Malware
system_info	No	Object	System information.
process	No	Array of process objects	Process information.
user_info	No	Array of user_info objects	User Details
file_info	No	Array of file_info objects	Document information.
system_alert_table	No	Object	Layout fields in the alerts list.

Table 4-103 environment

Parameter	Mandatory	Type	Description
vendor_type	No	String	Environment provider.
domain_id	No	String	Tenant ID.
region_id	No	String	Region ID. global is returned for global services.
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.
project_id	No	String	Project ID. The default value is null for global services.

Table 4-104 data_source

Parameter	Mandatory	Type	Description
source_type	No	Integer	Data source type. The options are as follows-- 1- cloud product 2- Third-party product 3- Tenant product
domain_id	No	String	Account ID to which the data source product belongs.
project_id	No	String	ID of the project to which the data source product belongs.
region_id	No	String	Region where the data source is located, for example, cn-north1. For details about the value range, see <i>Regions and Endpoints</i> .
company_name	No	String	Name of the company to which a data source belongs.
product_name	No	String	Name of the data source.
product_feature	No	String	Name of the feature of the product that detects the incident.
product_module	No	String	Threat detection module list.

Table 4-105 alert_type

Parameter	Mandatory	Type	Description
category	No	String	Type
alert_type	No	String	Alert type.

Table 4-106 network_list

Parameter	Mandatory	Type	Description
direction	No	String	Direction. The value can be IN or 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 .
src_ip	No	String	Source IP address
src_port	No	Integer	Source port. The value ranges from 0 to 65535.
src_domain	No	String	Source domain name.
src_geo	No	src_geo object	Geographical location of the source IP address.
dest_ip	No	String	Destination IP address
dest_port	No	String	Destination port. The value ranges from 0 to 65535.
dest_domain	No	String	Destination domain name
dest_geo	No	dest_geo object	Geographical location of the destination IP address.

Table 4-107 src_geo

Parameter	Mandatory	Type	Description
latitude	No	Number	Latitude
longitude	No	Number	Longitude
city_code	No	String	City code. For example, Beijing or Shanghai.
country_code	No	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-108 dest_geo

Parameter	Mandatory	Type	Description
latitude	No	Number	Latitude

Parameter	Mandatory	Type	Description
longitude	No	Number	Longitude
city_code	No	String	City code. For example, Beijing or Shanghai.
country_code	No	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-109 resource_list

Parameter	Mandatory	Type	Description
id	No	String	Cloud service resource ID.
name	No	String	Resource name.
type	No	String	Resource type. This parameter references the value of RMS type on Cloud.
provider	No	String	Cloud service name, which is the same as the provider field in the RMS service.
region_id	No	String	Region ID in Cloud, for example, cn-north-1.
domain_id	No	String	ID of the account to which the resource belongs, in UUID format.
project_id	No	String	ID of the account to which the resource belongs, in UUID format.
ep_id	No	String	Specifies the enterprise project ID.
ep_name	No	String	Enterprise Project Name
tags	No	String	Resource tag. <ol style="list-style-type: none"> 1. A maximum of 50 key/value pairs are supported. 2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _ ; , /, @

Table 4-110 remediation

Parameter	Mandatory	Type	Description
recommendation	No	String	Recommended solution.
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.

Table 4-111 malware

Parameter	Mandatory	Type	Description
malware_family	No	String	Malicious family.
malware_class	No	String	Malware category.

Table 4-112 process

Parameter	Mandatory	Type	Description
process_name	No	String	Process name.
process_path	No	String	Process execution file path.
process_pid	No	Integer	Process ID.
process_uid	No	Integer	Process user ID.
process_cmdline	No	String	Process command line.
process_parent_name	No	String	Parent process name.
process_parent_path	No	String	Parent process execution file path.
process_parent_pid	No	Integer	Parent process ID.
process_parent_uid	No	Integer	Parent process user ID.
process_parent_cmdline	No	String	Parent process command line.
process_child_name	No	String	Subprocess name.

Parameter	Mandatory	Type	Description
process_child_path	No	String	Subprocess execution file path.
process_child_pid	No	Integer	Subprocess ID.
process_child_uid	No	Integer	Subprocess user ID.
process_child_cmdline	No	String	Subprocess command line
process_launch_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.
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.

Table 4-113 user_info

Parameter	Mandatory	Type	Description
user_id	No	String	User UID
user_name	No	String	Username

Table 4-114 file_info

Parameter	Mandatory	Type	Description
file_path	No	String	File path/name.
file_content	No	String	File path/name.
file_new_path	No	String	New file path/name.
file_hash	No	String	File Hash
file_md5	No	String	File MD5
file_sha256	No	String	File SHA256

Parameter	Mandatory	Type	Description
file_attr	No	String	File attribute.

Response Parameters

Status code: 200

Table 4-115 Response header parameters

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

Table 4-116 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
data	AlertDetail object	Alert Detail

Table 4-117 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.
data_object	Alert object	Alert entity information.
dataclass_ref	dataclass_ref object	Data class object.
format_version	Integer	Format version.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
type	String	Data Types.
project_id	String	ID of the current project.

Parameter	Type	Description
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.
version	Integer	Version.
workspace_id	String	ID of the current workspace.

Table 4-118 Alert

Parameter	Type	Description
version	String	Version of the data source of the alert. The value must be one officially released by the Cloud SSA service.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	String	ID of the account (domain_id) to whom the data is delivered and hosted.
region_id	String	ID of the region where the account to whom the data is delivered and hosted belongs to.
workspace_id	String	ID of the current workspace.
labels	String	Tag (display only)
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.

Parameter	Type	Description
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.
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.
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.
title	String	Alert title.
description	String	Alert description.
source_url	String	Alert URL, which points to the page of the current incident description in the data source product.
count	Integer	Incident occurrences
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%.
severity	String	Severity level. Value range: Tips Low Medium High Fatal Description: <ul style="list-style-type: none"> ● 0: TIPS: No threats are found. ● 1: LOW: No actions are required for the threat. ● 2: MEDIUM: The threat needs to be handled but is not urgent. ● 3: HIGH: The threat must be handled preferentially. ● 4: FATAL: The threat must be handled immediately to prevent further damage.

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.
alert_type	alert_type object	Alert classification. For details, see the Alert Type Definition.
network_list	Array of network_list objects	Network Information
resource_list	Array of resource_list objects	Affected resources.
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.
handle_status	String	Incident handling status. The options are as follows: <ul style="list-style-type: none"> • Open: enabled. • Block: blocked. • Closed: closed. The default value is Open.
sla	Integer	Risk close time -- Set the acceptable risk duration. Unit -- Hour
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.

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.
ipdrr_phase	String	Period/Handling phase No. Preparation Detection and Analysis Containm,Eradiation& Recovery Post-Incident-Activity
simulation	String	Debugging field.
actor	String	Alert investigator.
owner	String	Owner and service owner.
creator	String	Creator
close_reason	String	Close reason. <ul style="list-style-type: none"> • False detection. • Resolved • Repeated • Other
close_comment	String	Whether to close comment.
malware	malware object	Malware
system_info	Object	System information.
process	Array of process objects	Process information.
user_info	Array of user_info objects	User Details
file_info	Array of file_info objects	Document information.
system_alert_table	Object	Layout fields in the alerts list.

Table 4-119 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Tenant ID.

Parameter	Type	Description
region_id	String	Region ID. global is returned for global services.
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.
project_id	String	Project ID. The default value is null for global services.

Table 4-120 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows-- 1- cloud product 2- Third-party product 3- Tenant product
domain_id	String	Account ID to which the data source product belongs.
project_id	String	ID of the project to which the data source product belongs.
region_id	String	Region where the data source is located, for example, cn-north1. For details about the value range, see <i>Regions and Endpoints</i> .
company_name	String	Name of the company to which a data source belongs.
product_name	String	Name of the data source.
product_feature	String	Name of the feature of the product that detects the incident.
product_module	String	Threat detection module list.

Table 4-121 alert_type

Parameter	Type	Description
category	String	Type
alert_type	String	Alert type.

Table 4-122 network_list

Parameter	Type	Description
direction	String	Direction. The value can be IN or 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 .
src_ip	String	Source IP address
src_port	Integer	Source port. The value ranges from 0 to 65535.
src_domain	String	Source domain name.
src_geo	src_geo object	Geographical location of the source IP address.
dest_ip	String	Destination IP address
dest_port	String	Destination port. The value ranges from 0 to 65535.
dest_domain	String	Destination domain name
dest_geo	dest_geo object	Geographical location of the destination IP address.

Table 4-123 src_geo

Parameter	Type	Description
latitude	Number	Latitude
longitude	Number	Longitude
city_code	String	City code. For example, Beijing or Shanghai.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-124 dest_geo

Parameter	Type	Description
latitude	Number	Latitude

Parameter	Type	Description
longitude	Number	Longitude
city_code	String	City code. For example, Beijing or Shanghai.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-125 resource_list

Parameter	Type	Description
id	String	Cloud service resource ID.
name	String	Resource name.
type	String	Resource type. This parameter references the value of RMS type on Cloud.
provider	String	Cloud service name, which is the same as the provider field in the RMS service.
region_id	String	Region ID in Cloud, for example, cn-north-1.
domain_id	String	ID of the account to which the resource belongs, in UUID format.
project_id	String	ID of the account to which the resource belongs, in UUID format.
ep_id	String	Specifies the enterprise project ID.
ep_name	String	Enterprise Project Name
tags	String	Resource tag. <ol style="list-style-type: none"> 1. A maximum of 50 key/value pairs are supported. 2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _ , ; , /, @

Table 4-126 remediation

Parameter	Type	Description
recommendation	String	Recommended solution.

Parameter	Type	Description
url	String	Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-127 malware

Parameter	Type	Description
malware_family	String	Malicious family.
malware_class	String	Malware category.

Table 4-128 process

Parameter	Type	Description
process_name	String	Process name.
process_path	String	Process execution file path.
process_pid	Integer	Process ID.
process_uid	Integer	Process user ID.
process_cmdline	String	Process command line.
process_parent_name	String	Parent process name.
process_parent_path	String	Parent process execution file path.
process_parent_pid	Integer	Parent process ID.
process_parent_uid	Integer	Parent process user ID.
process_parent_cmdline	String	Parent process command line.
process_child_name	String	Subprocess name.
process_child_path	String	Subprocess execution file path.
process_child_pid	Integer	Subprocess ID.
process_child_uid	Integer	Subprocess user ID.

Parameter	Type	Description
process_child_command_line	String	Subprocess command line
process_launch_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.
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.

Table 4-129 user_info

Parameter	Type	Description
user_id	String	User UID
user_name	String	Username

Table 4-130 file_info

Parameter	Type	Description
file_path	String	File path/name.
file_content	String	File path/name.
file_new_path	String	New file path/name.
file_hash	String	File Hash
file_md5	String	File MD5
file_sha256	String	File SHA256
file_attr	String	File attribute.

Table 4-131 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.
name	String	Data class name.

Status code: 400

Table 4-132 Response header parameters

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

Table 4-133 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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",
"ipdr_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",
    "ipdr_phase": "Preparation|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"
  }
}

```

```
}  
}
```

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 4-134 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID

Request Parameters

Table 4-135 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.
content-type	Yes	String	Content type.

Table 4-136 Request body parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page.
offset	No	Integer	Offset
sort_by	No	String	Sorting field -- create_time update_time
order	No	String	Sort by -- DESC ASC
from_date	No	String	Search start time, for example, 2023-02-20T00:00:00.000Z
to_date	No	String	Search end time, for example, 2023-02-27T23:59:59.999Z
condition	No	condition object	Search condition expression.

Table 4-137 condition

Parameter	Mandatory	Type	Description
conditions	No	Array of conditions objects	Expression list.
logics	No	Array of strings	Expression logic.

Table 4-138 conditions

Parameter	Mandatory	Type	Description
name	No	String	Expression name.
data	No	Array of strings	Expression content list.

Response Parameters

Status code: 200

Table 4-139 Response header parameters

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

Table 4-140 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
total	Integer	Total number of incidents.
limit	Integer	Number of records displayed on each page.
offset	Integer	Offset
success	Boolean	Successful or not.
data	Array of IncidentDetail objects	Event List

Table 4-141 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.
data_object	Incident object	Incident entity information.
dataclass_ref	dataclass_ref object	Data class object.
format_version	Integer	Format version.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
project_id	String	ID of the current project.
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.
version	Integer	Version.
workspace_id	String	ID of the current workspace.

Table 4-142 Incident

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

Parameter	Type	Description
workspace_id	String	ID of the current workspace.
labels	String	Tag (display only)
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.
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.
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.
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.
title	String	Incident title.
description	String	Event Description
source_url	String	Incident URL, which points to the page of the current incident description in the data source product.
count	Integer	Incident occurrences
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%.

Parameter	Type	Description
severity	String	Severity level. Value range: Tips Low Medium High Fatal Description: <ul style="list-style-type: none"> • 0: TIPS: No threats are found. • 1: LOW: No actions are required for the threat. • 2: MEDIUM: The threat needs to be handled but is not urgent. • 3: HIGH: The threat must be handled preferentially. • 4: FATAL: The threat must be handled immediately to prevent further damage.
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.
incident_type	incident_type object	Incident categories. For details, see the Alert Incident Type Definition.
network_list	Array of network_list objects	Network Information
resource_list	Array of resource_list objects	Affected resources.
remediation	remediation object	Remedy measure.
verification_state	String	Verification status, which identifies the accuracy of an incident. The options are as follows: <ul style="list-style-type: none"> - Unknown - True_Positive - False_Positive Enter Unknown by default.

Parameter	Type	Description
handle_status	String	Incident handling status. The options are as follows: <ul style="list-style-type: none"> • Open: enabled. • Block: blocked. • Closed: closed. The default value is Open.
sla	Integer	Risk close time -- Set the acceptable risk duration. Unit -- Hour
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.
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.
ipdr_phase	String	Period/Handling phase No. Preparation Detection and Analysis Containment,Eradication& Recovery Post-Incident-Activity
simulation	String	Debugging field.
actor	String	Incident investigator.
owner	String	Owner and service owner.
creator	String	Creator
close_reason	String	Close reason. <ul style="list-style-type: none"> • False detection. • Resolved • Repeated • Other
close_comment	String	Whether to close comment.
malware	malware object	Malware
system_info	Object	System information.
process	Array of process objects	Process information.

Parameter	Type	Description
user_info	Array of user_info objects	User Details
file_info	Array of file_info objects	Document Information
system_alert_table	Object	Layout fields in the incident list.

Table 4-143 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Tenant ID.
region_id	String	Region ID. global is returned for global services.
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.
project_id	String	Project ID. The default value is null for global services.

Table 4-144 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows-- 1- cloud product 2- Third-party product 3- Tenant product
domain_id	String	Account ID to which the data source product belongs.
project_id	String	ID of the project to which the data source product belongs.
region_id	String	Region where the data source is located, for example, cn-north1. For details about the value range, see <i>Regions and Endpoints</i> .
company_name	String	Name of the company to which a data source belongs.
product_name	String	Name of the data source.

Parameter	Type	Description
product_feature	String	Name of the feature of the product that detects the incident.
product_module	String	Threat detection module list.

Table 4-145 incident_type

Parameter	Type	Description
category	String	Type
incident_type	String	Incident type.

Table 4-146 network_list

Parameter	Type	Description
direction	String	Direction. The value can be IN or 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 .
src_ip	String	Source IP address
src_port	Integer	Source port. The value ranges from 0 to 65535.
src_domain	String	Source domain name.
src_geo	src_geo object	Geographical location of the source IP address.
dest_ip	String	Destination IP address
dest_port	String	Destination port. The value ranges from 0 to 65535.
dest_domain	String	Destination domain name
dest_geo	dest_geo object	Geographical location of the destination IP address.

Table 4-147 src_geo

Parameter	Type	Description
latitude	Number	Latitude
longitude	Number	Longitude
city_code	String	City code. For example, Beijing or Shanghai.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-148 dest_geo

Parameter	Type	Description
latitude	Number	Latitude
longitude	Number	Longitude
city_code	String	City code. For example, Beijing or Shanghai.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-149 resource_list

Parameter	Type	Description
id	String	Cloud service resource ID.
name	String	Resource name.
type	String	Resource type. This parameter references the value of RMS type on Cloud.
provider	String	Cloud service name, which is the same as the provider field in the RMS service.
region_id	String	Region ID in Cloud, for example, cn-north-1.
domain_id	String	ID of the account to which the resource belongs, in UUID format.
project_id	String	ID of the account to which the resource belongs, in UUID format.

Parameter	Type	Description
ep_id	String	Specifies the enterprise project ID.
ep_name	String	Enterprise Project Name
tags	String	Resource tag. 1. A maximum of 50 key/value pairs are supported. 2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _ ;, /, @

Table 4-150 remediation

Parameter	Type	Description
recommendation	String	Recommended solution.
url	String	Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-151 malware

Parameter	Type	Description
malware_family	String	Malicious family.
malware_class	String	Malware category.

Table 4-152 process

Parameter	Type	Description
process_name	String	Process name.
process_path	String	Process execution file path.
process_pid	Integer	Process ID.
process_uid	Integer	Process user ID.
process_cmdline	String	Process command line.
process_parent_name	String	Parent process name.

Parameter	Type	Description
process_parent_path	String	Parent process execution file path.
process_parent_pid	Integer	Parent process ID.
process_parent_uid	Integer	Parent process user ID.
process_parent_cmdline	String	Parent process command line.
process_child_name	String	Subprocess name.
process_child_path	String	Subprocess execution file path.
process_child_pid	Integer	Subprocess ID.
process_child_uid	Integer	Subprocess user ID.
process_child_cmdline	String	Subprocess command line
process_launched_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.
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.

Table 4-153 user_info

Parameter	Type	Description
user_id	String	User UID
user_name	String	Username

Table 4-154 file_info

Parameter	Type	Description
file_path	String	File path/name.
file_content	String	File path/name.
file_new_path	String	New file path/name.
file_hash	String	File Hash
file_md5	String	File MD5
file_sha256	String	File SHA256
file_attr	String	File attribute.

Table 4-155 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.
name	String	Data class name.

Status code: 400

Table 4-156 Response header parameters

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

Table 4-157 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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",
"ipdr_phase" : "Preparation|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"
  }
}

```

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 4-158 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID

Request Parameters

Table 4-159 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.
content-type	Yes	String	Content type.

Table 4-160 Request body parameters

Parameter	Mandatory	Type	Description
data_object	No	Incident object	Incident entity information.

Table 4-161 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 Cloud SSA service.
id	No	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	No	String	ID of the account (domain_id) to whom the data is delivered and hosted.
region_id	No	String	ID of the region where the account to whom the data is delivered and hosted belongs to.
workspace_id	No	String	ID of the current workspace.
labels	No	String	Tag (display only)

Parameter	Mandatory	Type	Description
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.
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.
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.
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.
title	No	String	Incident title.
description	No	String	Event Description
source_url	No	String	Incident URL, which points to the page of the current incident description in the data source product.
count	No	Integer	Incident occurrences

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%.
severity	No	String	Severity level. Value range: Tips Low Medium High Fatal Description: <ul style="list-style-type: none"> ● 0: TIPS: No threats are found. ● 1: LOW: No actions are required for the threat. ● 2: MEDIUM: The threat needs to be handled but is not urgent. ● 3: HIGH: The threat must be handled preferentially. ● 4: FATAL: The threat must be handled immediately to prevent further damage.
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.
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
resource_list	No	Array of resource_list objects	Affected resources.
remediation	No	remediation object	Remedy measure.

Parameter	Mandatory	Type	Description
verification_status	No	String	Verification status, which identifies the accuracy of an incident. The options are as follows: <ul style="list-style-type: none"> - Unknown - True_Positive - False_Positive Enter Unknown by default.
handle_status	No	String	Incident handling status. The options are as follows: <ul style="list-style-type: none"> • Open: enabled. • Block: blocked. • Closed: closed. The default value is Open.
sla	No	Integer	Risk close time -- Set the acceptable risk duration. Unit -- Hour
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.
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.
ipdrr_phase	No	String	Period/Handling phase No. Preparation Detection and Analysis Containm,Eradiation& Recovery Post-Incident-Activity
simulation	No	String	Debugging field.
actor	No	String	Incident investigator.
owner	No	String	Owner and service owner.
creator	No	String	Creator

Parameter	Mandatory	Type	Description
close_reason	No	String	Close reason. <ul style="list-style-type: none"> • False detection. • Resolved • Repeated • Other
close_comment	No	String	Whether to close comment.
malware	No	malware object	Malware
system_info	No	Object	System information.
process	No	Array of process objects	Process information.
user_info	No	Array of user_info objects	User Details
file_info	No	Array of file_info objects	Document Information
system_alert_table	No	Object	Layout fields in the incident list.

Table 4-162 environment

Parameter	Mandatory	Type	Description
vendor_type	No	String	Environment provider.
domain_id	No	String	Tenant ID.
region_id	No	String	Region ID. global is returned for global services.
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.
project_id	No	String	Project ID. The default value is null for global services.

Table 4-163 data_source

Parameter	Mandatory	Type	Description
source_type	No	Integer	Data source type. The options are as follows-- 1- cloud product 2- Third-party product 3- Tenant product
domain_id	No	String	Account ID to which the data source product belongs.
project_id	No	String	ID of the project to which the data source product belongs.
region_id	No	String	Region where the data source is located, for example, cn-north1. For details about the value range, see <i>Regions and Endpoints</i> .
company_name	No	String	Name of the company to which a data source belongs.
product_name	No	String	Name of the data source.
product_feature	No	String	Name of the feature of the product that detects the incident.
product_module	No	String	Threat detection module list.

Table 4-164 incident_type

Parameter	Mandatory	Type	Description
category	No	String	Type
incident_type	No	String	Incident type.

Table 4-165 network_list

Parameter	Mandatory	Type	Description
direction	No	String	Direction. The value can be IN or 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 .
src_ip	No	String	Source IP address
src_port	No	Integer	Source port. The value ranges from 0 to 65535.
src_domain	No	String	Source domain name.
src_geo	No	src_geo object	Geographical location of the source IP address.
dest_ip	No	String	Destination IP address
dest_port	No	String	Destination port. The value ranges from 0 to 65535.
dest_domain	No	String	Destination domain name
dest_geo	No	dest_geo object	Geographical location of the destination IP address.

Table 4-166 src_geo

Parameter	Mandatory	Type	Description
latitude	No	Number	Latitude
longitude	No	Number	Longitude
city_code	No	String	City code. For example, Beijing or Shanghai.
country_code	No	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-167 dest_geo

Parameter	Mandatory	Type	Description
latitude	No	Number	Latitude

Parameter	Mandatory	Type	Description
longitude	No	Number	Longitude
city_code	No	String	City code. For example, Beijing or Shanghai.
country_code	No	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-168 resource_list

Parameter	Mandatory	Type	Description
id	No	String	Cloud service resource ID.
name	No	String	Resource name.
type	No	String	Resource type. This parameter references the value of RMS type on Cloud.
provider	No	String	Cloud service name, which is the same as the provider field in the RMS service.
region_id	No	String	Region ID in Cloud, for example, cn-north-1.
domain_id	No	String	ID of the account to which the resource belongs, in UUID format.
project_id	No	String	ID of the account to which the resource belongs, in UUID format.
ep_id	No	String	Specifies the enterprise project ID.
ep_name	No	String	Enterprise Project Name
tags	No	String	Resource tag. <ol style="list-style-type: none"> 1. A maximum of 50 key/value pairs are supported. 2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _ ; , /, @

Table 4-169 remediation

Parameter	Mandatory	Type	Description
recommendation	No	String	Recommended solution.
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.

Table 4-170 malware

Parameter	Mandatory	Type	Description
malware_family	No	String	Malicious family.
malware_class	No	String	Malware category.

Table 4-171 process

Parameter	Mandatory	Type	Description
process_name	No	String	Process name.
process_path	No	String	Process execution file path.
process_pid	No	Integer	Process ID.
process_uid	No	Integer	Process user ID.
process_cmdline	No	String	Process command line.
process_parent_name	No	String	Parent process name.
process_parent_path	No	String	Parent process execution file path.
process_parent_pid	No	Integer	Parent process ID.
process_parent_uid	No	Integer	Parent process user ID.
process_parent_cmdline	No	String	Parent process command line.
process_child_name	No	String	Subprocess name.

Parameter	Mandatory	Type	Description
process_child_path	No	String	Subprocess execution file path.
process_child_pid	No	Integer	Subprocess ID.
process_child_uid	No	Integer	Subprocess user ID.
process_child_cmdline	No	String	Subprocess command line
process_launch_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.
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.

Table 4-172 user_info

Parameter	Mandatory	Type	Description
user_id	No	String	User UID
user_name	No	String	Username

Table 4-173 file_info

Parameter	Mandatory	Type	Description
file_path	No	String	File path/name.
file_content	No	String	File path/name.
file_new_path	No	String	New file path/name.
file_hash	No	String	File Hash
file_md5	No	String	File MD5
file_sha256	No	String	File SHA256

Parameter	Mandatory	Type	Description
file_attr	No	String	File attribute.

Response Parameters

Status code: 200

Table 4-174 Response header parameters

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

Table 4-175 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
data	IncidentDetail object	Incident Detail

Table 4-176 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.
data_object	Incident object	Incident entity information.
dataclass_ref	dataclass_ref object	Data class object.
format_version	Integer	Format version.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
project_id	String	ID of the current project.

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.
version	Integer	Version.
workspace_id	String	ID of the current workspace.

Table 4-177 Incident

Parameter	Type	Description
version	String	Version of the data source of an incident. The version must be one officially released by the Cloud SSA service.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	String	ID of the account (domain_id) to whom the data is delivered and hosted.
region_id	String	ID of the region where the account to whom the data is delivered and hosted belongs to.
workspace_id	String	ID of the current workspace.
labels	String	Tag (display only)
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.

Parameter	Type	Description
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.
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.
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.
title	String	Incident title.
description	String	Event Description
source_url	String	Incident URL, which points to the page of the current incident description in the data source product.
count	Integer	Incident occurrences
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%.
severity	String	Severity level. Value range: Tips Low Medium High Fatal Description: <ul style="list-style-type: none"> ● 0: TIPS: No threats are found. ● 1: LOW: No actions are required for the threat. ● 2: MEDIUM: The threat needs to be handled but is not urgent. ● 3: HIGH: The threat must be handled preferentially. ● 4: FATAL: The threat must be handled immediately to prevent further damage.

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.
incident_type	incident_type object	Incident categories. For details, see the Alert Incident Type Definition.
network_list	Array of network_list objects	Network Information
resource_list	Array of resource_list objects	Affected resources.
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.
handle_status	String	Incident handling status. The options are as follows: <ul style="list-style-type: none"> • Open: enabled. • Block: blocked. • Closed: closed. The default value is Open.
sla	Integer	Risk close time -- Set the acceptable risk duration. Unit -- Hour
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.

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.
ipdrr_phase	String	Period/Handling phase No. Preparation Detection and Analysis Containment, Eradication & Recovery Post-Incident-Activity
simulation	String	Debugging field.
actor	String	Incident investigator.
owner	String	Owner and service owner.
creator	String	Creator
close_reason	String	Close reason. <ul style="list-style-type: none"> • False detection. • Resolved • Repeated • Other
close_comment	String	Whether to close comment.
malware	malware object	Malware
system_info	Object	System information.
process	Array of process objects	Process information.
user_info	Array of user_info objects	User Details
file_info	Array of file_info objects	Document Information
system_alert_table	Object	Layout fields in the incident list.

Table 4-178 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Tenant ID.

Parameter	Type	Description
region_id	String	Region ID. global is returned for global services.
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.
project_id	String	Project ID. The default value is null for global services.

Table 4-179 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows-- 1- cloud product 2- Third-party product 3- Tenant product
domain_id	String	Account ID to which the data source product belongs.
project_id	String	ID of the project to which the data source product belongs.
region_id	String	Region where the data source is located, for example, cn-north1. For details about the value range, see <i>Regions and Endpoints</i> .
company_name	String	Name of the company to which a data source belongs.
product_name	String	Name of the data source.
product_feature	String	Name of the feature of the product that detects the incident.
product_module	String	Threat detection module list.

Table 4-180 incident_type

Parameter	Type	Description
category	String	Type
incident_type	String	Incident type.

Table 4-181 network_list

Parameter	Type	Description
direction	String	Direction. The value can be IN or 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 .
src_ip	String	Source IP address
src_port	Integer	Source port. The value ranges from 0 to 65535.
src_domain	String	Source domain name.
src_geo	src_geo object	Geographical location of the source IP address.
dest_ip	String	Destination IP address
dest_port	String	Destination port. The value ranges from 0 to 65535.
dest_domain	String	Destination domain name
dest_geo	dest_geo object	Geographical location of the destination IP address.

Table 4-182 src_geo

Parameter	Type	Description
latitude	Number	Latitude
longitude	Number	Longitude
city_code	String	City code. For example, Beijing or Shanghai.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-183 dest_geo

Parameter	Type	Description
latitude	Number	Latitude

Parameter	Type	Description
longitude	Number	Longitude
city_code	String	City code. For example, Beijing or Shanghai.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-184 resource_list

Parameter	Type	Description
id	String	Cloud service resource ID.
name	String	Resource name.
type	String	Resource type. This parameter references the value of RMS type on Cloud.
provider	String	Cloud service name, which is the same as the provider field in the RMS service.
region_id	String	Region ID in Cloud, for example, cn-north-1.
domain_id	String	ID of the account to which the resource belongs, in UUID format.
project_id	String	ID of the account to which the resource belongs, in UUID format.
ep_id	String	Specifies the enterprise project ID.
ep_name	String	Enterprise Project Name
tags	String	Resource tag. <ol style="list-style-type: none"> 1. A maximum of 50 key/value pairs are supported. 2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _ , ; , /, @

Table 4-185 remediation

Parameter	Type	Description
recommendation	String	Recommended solution.

Parameter	Type	Description
url	String	Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-186 malware

Parameter	Type	Description
malware_family	String	Malicious family.
malware_class	String	Malware category.

Table 4-187 process

Parameter	Type	Description
process_name	String	Process name.
process_path	String	Process execution file path.
process_pid	Integer	Process ID.
process_uid	Integer	Process user ID.
process_cmdline	String	Process command line.
process_parent_name	String	Parent process name.
process_parent_path	String	Parent process execution file path.
process_parent_pid	Integer	Parent process ID.
process_parent_uid	Integer	Parent process user ID.
process_parent_cmdline	String	Parent process command line.
process_child_name	String	Subprocess name.
process_child_path	String	Subprocess execution file path.
process_child_pid	Integer	Subprocess ID.
process_child_uid	Integer	Subprocess user ID.

Parameter	Type	Description
process_child_cmd_line	String	Subprocess command line
process_launched_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.
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.

Table 4-188 user_info

Parameter	Type	Description
user_id	String	User UID
user_name	String	Username

Table 4-189 file_info

Parameter	Type	Description
file_path	String	File path/name.
file_content	String	File path/name.
file_new_path	String	New file path/name.
file_hash	String	File Hash
file_md5	String	File MD5
file_sha256	String	File SHA256
file_attr	String	File attribute.

Table 4-190 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.
name	String	Data class name.

Status code: 400

Table 4-191 Response header parameters

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

Table 4-192 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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",
  "ipdr_phase": "Preparation|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"
}
}

```

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 4-193 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID

Request Parameters

Table 4-194 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.
content-type	Yes	String	Content type.

Table 4-195 Request body parameters

Parameter	Mandatory	Type	Description
batch_ids	No	Array of strings	IDs of deleted alerts.

Response Parameters

Status code: 200

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
message	String	Error Message
data	data object	Returned object for batch deleting incidents.

Table 4-198 data

Parameter	Type	Description
error_ids	Array of strings	IDs of alerts not transferred to incidents
success_ids	Array of strings	IDs of alerts transferred to incidents.

Status code: 400

Table 4-199 Response header parameters

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

Table 4-200 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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" ]
  }
}
```

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 4-201 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
incident_id	Yes	String	Incident ID.

Request Parameters

Table 4-202 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.
content-type	Yes	String	Content type.

Response Parameters

Status code: 200

Table 4-203 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
data	IncidentDetail object	Incident Detail

Table 4-204 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.
data_object	Incident object	Incident entity information.
dataclass_ref	dataclass_ref object	Data class object.
format_version	Integer	Format version.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
project_id	String	ID of the current project.
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.
version	Integer	Version.
workspace_id	String	ID of the current workspace.

Table 4-205 Incident

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

Parameter	Type	Description
workspace_id	String	ID of the current workspace.
labels	String	Tag (display only)
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.
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.
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.
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.
title	String	Incident title.
description	String	Event Description
source_url	String	Incident URL, which points to the page of the current incident description in the data source product.
count	Integer	Incident occurrences
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%.

Parameter	Type	Description
severity	String	Severity level. Value range: Tips Low Medium High Fatal Description: <ul style="list-style-type: none"> • 0: TIPS: No threats are found. • 1: LOW: No actions are required for the threat. • 2: MEDIUM: The threat needs to be handled but is not urgent. • 3: HIGH: The threat must be handled preferentially. • 4: FATAL: The threat must be handled immediately to prevent further damage.
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.
incident_type	incident_type object	Incident categories. For details, see the Alert Incident Type Definition.
network_list	Array of network_list objects	Network Information
resource_list	Array of resource_list objects	Affected resources.
remediation	remediation object	Remedy measure.
verification_state	String	Verification status, which identifies the accuracy of an incident. The options are as follows: <ul style="list-style-type: none"> - Unknown - True_Positive - False_Positive Enter Unknown by default.

Parameter	Type	Description
handle_status	String	Incident handling status. The options are as follows: <ul style="list-style-type: none"> • Open: enabled. • Block: blocked. • Closed: closed. The default value is Open.
sla	Integer	Risk close time -- Set the acceptable risk duration. Unit -- Hour
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.
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.
ipdr_phase	String	Period/Handling phase No. Preparation Detection and Analysis Containment,Eradication& Recovery Post-Incident-Activity
simulation	String	Debugging field.
actor	String	Incident investigator.
owner	String	Owner and service owner.
creator	String	Creator
close_reason	String	Close reason. <ul style="list-style-type: none"> • False detection. • Resolved • Repeated • Other
close_comment	String	Whether to close comment.
malware	malware object	Malware
system_info	Object	System information.
process	Array of process objects	Process information.

Parameter	Type	Description
user_info	Array of user_info objects	User Details
file_info	Array of file_info objects	Document Information
system_alert_table	Object	Layout fields in the incident list.

Table 4-206 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Tenant ID.
region_id	String	Region ID. global is returned for global services.
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.
project_id	String	Project ID. The default value is null for global services.

Table 4-207 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows-- 1- cloud product 2- Third-party product 3- Tenant product
domain_id	String	Account ID to which the data source product belongs.
project_id	String	ID of the project to which the data source product belongs.
region_id	String	Region where the data source is located, for example, cn-north1. For details about the value range, see <i>Regions and Endpoints</i> .
company_name	String	Name of the company to which a data source belongs.
product_name	String	Name of the data source.

Parameter	Type	Description
product_feature	String	Name of the feature of the product that detects the incident.
product_module	String	Threat detection module list.

Table 4-208 incident_type

Parameter	Type	Description
category	String	Type
incident_type	String	Incident type.

Table 4-209 network_list

Parameter	Type	Description
direction	String	Direction. The value can be IN or 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 .
src_ip	String	Source IP address
src_port	Integer	Source port. The value ranges from 0 to 65535.
src_domain	String	Source domain name.
src_geo	src_geo object	Geographical location of the source IP address.
dest_ip	String	Destination IP address
dest_port	String	Destination port. The value ranges from 0 to 65535.
dest_domain	String	Destination domain name
dest_geo	dest_geo object	Geographical location of the destination IP address.

Table 4-210 src_geo

Parameter	Type	Description
latitude	Number	Latitude
longitude	Number	Longitude
city_code	String	City code. For example, Beijing or Shanghai.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-211 dest_geo

Parameter	Type	Description
latitude	Number	Latitude
longitude	Number	Longitude
city_code	String	City code. For example, Beijing or Shanghai.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-212 resource_list

Parameter	Type	Description
id	String	Cloud service resource ID.
name	String	Resource name.
type	String	Resource type. This parameter references the value of RMS type on Cloud.
provider	String	Cloud service name, which is the same as the provider field in the RMS service.
region_id	String	Region ID in Cloud, for example, cn-north-1.
domain_id	String	ID of the account to which the resource belongs, in UUID format.
project_id	String	ID of the account to which the resource belongs, in UUID format.

Parameter	Type	Description
ep_id	String	Specifies the enterprise project ID.
ep_name	String	Enterprise Project Name
tags	String	Resource tag. 1. A maximum of 50 key/value pairs are supported. 2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _ ;, /, @

Table 4-213 remediation

Parameter	Type	Description
recommendation	String	Recommended solution.
url	String	Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-214 malware

Parameter	Type	Description
malware_family	String	Malicious family.
malware_class	String	Malware category.

Table 4-215 process

Parameter	Type	Description
process_name	String	Process name.
process_path	String	Process execution file path.
process_pid	Integer	Process ID.
process_uid	Integer	Process user ID.
process_cmdline	String	Process command line.
process_parent_name	String	Parent process name.

Parameter	Type	Description
process_parent_path	String	Parent process execution file path.
process_parent_pid	Integer	Parent process ID.
process_parent_uid	Integer	Parent process user ID.
process_parent_cmdline	String	Parent process command line.
process_child_name	String	Subprocess name.
process_child_path	String	Subprocess execution file path.
process_child_pid	Integer	Subprocess ID.
process_child_uid	Integer	Subprocess user ID.
process_child_cmdline	String	Subprocess command line
process_launched_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.
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.

Table 4-216 user_info

Parameter	Type	Description
user_id	String	User UID
user_name	String	Username

Table 4-217 file_info

Parameter	Type	Description
file_path	String	File path/name.
file_content	String	File path/name.
file_new_path	String	New file path/name.
file_hash	String	File Hash
file_md5	String	File MD5
file_sha256	String	File SHA256
file_attr	String	File attribute.

Table 4-218 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.
name	String	Data class name.

Status code: 400

Table 4-219 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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",
"ipdr_phase": "Prepartion|Detection and Analysis|Containm,Eradiation& 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"
}
}

```

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 4-220 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
incident_id	Yes	String	Incident ID.

Request Parameters

Table 4-221 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.
content-type	Yes	String	Content type.

Table 4-222 Request body parameters

Parameter	Mandatory	Type	Description
batch_ids	No	Array of strings	IDs of updated alerts.
data_object	No	Incident object	Incident entity information.

Table 4-223 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 Cloud SSA service.
id	No	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	No	String	ID of the account (domain_id) to whom the data is delivered and hosted.
region_id	No	String	ID of the region where the account to whom the data is delivered and hosted belongs to.
workspace_id	No	String	ID of the current workspace.
labels	No	String	Tag (display only)
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.
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.

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.
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.
title	No	String	Incident title.
description	No	String	Event Description
source_url	No	String	Incident URL, which points to the page of the current incident description in the data source product.
count	No	Integer	Incident occurrences
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%.

Parameter	Mandatory	Type	Description
severity	No	String	Severity level. Value range: Tips Low Medium High Fatal Description: <ul style="list-style-type: none"> • 0: TIPS: No threats are found. • 1: LOW: No actions are required for the threat. • 2: MEDIUM: The threat needs to be handled but is not urgent. • 3: HIGH: The threat must be handled preferentially. • 4: FATAL: The threat must be handled immediately to prevent further damage.
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.
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
resource_list	No	Array of resource_list objects	Affected resources.
remediation	No	remediation object	Remedy measure.

Parameter	Mandatory	Type	Description
verification_status	No	String	Verification status, which identifies the accuracy of an incident. The options are as follows: <ul style="list-style-type: none"> - Unknown - True_Positive - False_Positive Enter Unknown by default.
handle_status	No	String	Incident handling status. The options are as follows: <ul style="list-style-type: none"> • Open: enabled. • Block: blocked. • Closed: closed. The default value is Open.
sla	No	Integer	Risk close time -- Set the acceptable risk duration. Unit -- Hour
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.
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.
ipdrr_phase	No	String	Period/Handling phase No. Preparation Detection and Analysis Containm,Eradiation& Recovery Post-Incident-Activity
simulation	No	String	Debugging field.
actor	No	String	Incident investigator.
owner	No	String	Owner and service owner.
creator	No	String	Creator

Parameter	Mandatory	Type	Description
close_reason	No	String	Close reason. <ul style="list-style-type: none"> • False detection. • Resolved • Repeated • Other
close_comment	No	String	Whether to close comment.
malware	No	malware object	Malware
system_info	No	Object	System information.
process	No	Array of process objects	Process information.
user_info	No	Array of user_info objects	User Details
file_info	No	Array of file_info objects	Document Information
system_alert_table	No	Object	Layout fields in the incident list.

Table 4-224 environment

Parameter	Mandatory	Type	Description
vendor_type	No	String	Environment provider.
domain_id	No	String	Tenant ID.
region_id	No	String	Region ID. global is returned for global services.
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.
project_id	No	String	Project ID. The default value is null for global services.

Table 4-225 data_source

Parameter	Mandatory	Type	Description
source_type	No	Integer	Data source type. The options are as follows-- 1- cloud product 2- Third-party product 3- Tenant product
domain_id	No	String	Account ID to which the data source product belongs.
project_id	No	String	ID of the project to which the data source product belongs.
region_id	No	String	Region where the data source is located, for example, cn-north1. For details about the value range, see <i>Regions and Endpoints</i> .
company_name	No	String	Name of the company to which a data source belongs.
product_name	No	String	Name of the data source.
product_feature	No	String	Name of the feature of the product that detects the incident.
product_module	No	String	Threat detection module list.

Table 4-226 incident_type

Parameter	Mandatory	Type	Description
category	No	String	Type
incident_type	No	String	Incident type.

Table 4-227 network_list

Parameter	Mandatory	Type	Description
direction	No	String	Direction. The value can be IN or 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 .
src_ip	No	String	Source IP address
src_port	No	Integer	Source port. The value ranges from 0 to 65535.
src_domain	No	String	Source domain name.
src_geo	No	src_geo object	Geographical location of the source IP address.
dest_ip	No	String	Destination IP address
dest_port	No	String	Destination port. The value ranges from 0 to 65535.
dest_domain	No	String	Destination domain name
dest_geo	No	dest_geo object	Geographical location of the destination IP address.

Table 4-228 src_geo

Parameter	Mandatory	Type	Description
latitude	No	Number	Latitude
longitude	No	Number	Longitude
city_code	No	String	City code. For example, Beijing or Shanghai.
country_code	No	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-229 dest_geo

Parameter	Mandatory	Type	Description
latitude	No	Number	Latitude

Parameter	Mandatory	Type	Description
longitude	No	Number	Longitude
city_code	No	String	City code. For example, Beijing or Shanghai.
country_code	No	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-230 resource_list

Parameter	Mandatory	Type	Description
id	No	String	Cloud service resource ID.
name	No	String	Resource name.
type	No	String	Resource type. This parameter references the value of RMS type on Cloud.
provider	No	String	Cloud service name, which is the same as the provider field in the RMS service.
region_id	No	String	Region ID in Cloud, for example, cn-north-1.
domain_id	No	String	ID of the account to which the resource belongs, in UUID format.
project_id	No	String	ID of the account to which the resource belongs, in UUID format.
ep_id	No	String	Specifies the enterprise project ID.
ep_name	No	String	Enterprise Project Name
tags	No	String	Resource tag. <ol style="list-style-type: none"> 1. A maximum of 50 key/value pairs are supported. 2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _ ; , /, @

Table 4-231 remediation

Parameter	Mandatory	Type	Description
recommendation	No	String	Recommended solution.
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.

Table 4-232 malware

Parameter	Mandatory	Type	Description
malware_family	No	String	Malicious family.
malware_class	No	String	Malware category.

Table 4-233 process

Parameter	Mandatory	Type	Description
process_name	No	String	Process name.
process_path	No	String	Process execution file path.
process_pid	No	Integer	Process ID.
process_uid	No	Integer	Process user ID.
process_cmdline	No	String	Process command line.
process_parent_name	No	String	Parent process name.
process_parent_path	No	String	Parent process execution file path.
process_parent_pid	No	Integer	Parent process ID.
process_parent_uid	No	Integer	Parent process user ID.
process_parent_cmdline	No	String	Parent process command line.
process_child_name	No	String	Subprocess name.

Parameter	Mandatory	Type	Description
process_child_path	No	String	Subprocess execution file path.
process_child_pid	No	Integer	Subprocess ID.
process_child_uid	No	Integer	Subprocess user ID.
process_child_cmdline	No	String	Subprocess command line
process_launch_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.
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.

Table 4-234 user_info

Parameter	Mandatory	Type	Description
user_id	No	String	User UID
user_name	No	String	Username

Table 4-235 file_info

Parameter	Mandatory	Type	Description
file_path	No	String	File path/name.
file_content	No	String	File path/name.
file_new_path	No	String	New file path/name.
file_hash	No	String	File Hash
file_md5	No	String	File MD5
file_sha256	No	String	File SHA256

Parameter	Mandatory	Type	Description
file_attr	No	String	File attribute.

Response Parameters

Status code: 200

Table 4-236 Response header parameters

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

Table 4-237 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
data	IncidentDetail object	Incident Detail

Table 4-238 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.
data_object	Incident object	Incident entity information.
dataclass_ref	dataclass_ref object	Data class object.
format_version	Integer	Format version.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
project_id	String	ID of the current project.

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.
version	Integer	Version.
workspace_id	String	ID of the current workspace.

Table 4-239 Incident

Parameter	Type	Description
version	String	Version of the data source of an incident. The version must be one officially released by the Cloud SSA service.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	String	ID of the account (domain_id) to whom the data is delivered and hosted.
region_id	String	ID of the region where the account to whom the data is delivered and hosted belongs to.
workspace_id	String	ID of the current workspace.
labels	String	Tag (display only)
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.

Parameter	Type	Description
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.
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.
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.
title	String	Incident title.
description	String	Event Description
source_url	String	Incident URL, which points to the page of the current incident description in the data source product.
count	Integer	Incident occurrences
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%.
severity	String	Severity level. Value range: Tips Low Medium High Fatal Description: <ul style="list-style-type: none"> • 0: TIPS: No threats are found. • 1: LOW: No actions are required for the threat. • 2: MEDIUM: The threat needs to be handled but is not urgent. • 3: HIGH: The threat must be handled preferentially. • 4: FATAL: The threat must be handled immediately to prevent further damage.

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.
incident_type	incident_type object	Incident categories. For details, see the Alert Incident Type Definition.
network_list	Array of network_list objects	Network Information
resource_list	Array of resource_list objects	Affected resources.
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.
handle_status	String	Incident handling status. The options are as follows: • Open: enabled. • Block: blocked. • Closed: closed. The default value is Open.
sla	Integer	Risk close time -- Set the acceptable risk duration. Unit -- Hour
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.

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.
ipdrr_phase	String	Period/Handling phase No. Preparation Detection and Analysis Containment, Eradication & Recovery Post-Incident-Activity
simulation	String	Debugging field.
actor	String	Incident investigator.
owner	String	Owner and service owner.
creator	String	Creator
close_reason	String	Close reason. <ul style="list-style-type: none"> • False detection. • Resolved • Repeated • Other
close_comment	String	Whether to close comment.
malware	malware object	Malware
system_info	Object	System information.
process	Array of process objects	Process information.
user_info	Array of user_info objects	User Details
file_info	Array of file_info objects	Document Information
system_alert_table	Object	Layout fields in the incident list.

Table 4-240 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Tenant ID.

Parameter	Type	Description
region_id	String	Region ID. global is returned for global services.
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.
project_id	String	Project ID. The default value is null for global services.

Table 4-241 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows-- 1- cloud product 2- Third-party product 3- Tenant product
domain_id	String	Account ID to which the data source product belongs.
project_id	String	ID of the project to which the data source product belongs.
region_id	String	Region where the data source is located, for example, cn-north1. For details about the value range, see <i>Regions and Endpoints</i> .
company_name	String	Name of the company to which a data source belongs.
product_name	String	Name of the data source.
product_feature	String	Name of the feature of the product that detects the incident.
product_module	String	Threat detection module list.

Table 4-242 incident_type

Parameter	Type	Description
category	String	Type
incident_type	String	Incident type.

Table 4-243 network_list

Parameter	Type	Description
direction	String	Direction. The value can be IN or 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 .
src_ip	String	Source IP address
src_port	Integer	Source port. The value ranges from 0 to 65535.
src_domain	String	Source domain name.
src_geo	src_geo object	Geographical location of the source IP address.
dest_ip	String	Destination IP address
dest_port	String	Destination port. The value ranges from 0 to 65535.
dest_domain	String	Destination domain name
dest_geo	dest_geo object	Geographical location of the destination IP address.

Table 4-244 src_geo

Parameter	Type	Description
latitude	Number	Latitude
longitude	Number	Longitude
city_code	String	City code. For example, Beijing or Shanghai.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-245 dest_geo

Parameter	Type	Description
latitude	Number	Latitude

Parameter	Type	Description
longitude	Number	Longitude
city_code	String	City code. For example, Beijing or Shanghai.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-246 resource_list

Parameter	Type	Description
id	String	Cloud service resource ID.
name	String	Resource name.
type	String	Resource type. This parameter references the value of RMS type on Cloud.
provider	String	Cloud service name, which is the same as the provider field in the RMS service.
region_id	String	Region ID in Cloud, for example, cn-north-1.
domain_id	String	ID of the account to which the resource belongs, in UUID format.
project_id	String	ID of the account to which the resource belongs, in UUID format.
ep_id	String	Specifies the enterprise project ID.
ep_name	String	Enterprise Project Name
tags	String	Resource tag. <ol style="list-style-type: none"> 1. A maximum of 50 key/value pairs are supported. 2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _ , ; , /, @

Table 4-247 remediation

Parameter	Type	Description
recommendation	String	Recommended solution.

Parameter	Type	Description
url	String	Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-248 malware

Parameter	Type	Description
malware_family	String	Malicious family.
malware_class	String	Malware category.

Table 4-249 process

Parameter	Type	Description
process_name	String	Process name.
process_path	String	Process execution file path.
process_pid	Integer	Process ID.
process_uid	Integer	Process user ID.
process_cmdline	String	Process command line.
process_parent_name	String	Parent process name.
process_parent_path	String	Parent process execution file path.
process_parent_pid	Integer	Parent process ID.
process_parent_uid	Integer	Parent process user ID.
process_parent_cmdline	String	Parent process command line.
process_child_name	String	Subprocess name.
process_child_path	String	Subprocess execution file path.
process_child_pid	Integer	Subprocess ID.
process_child_uid	Integer	Subprocess user ID.

Parameter	Type	Description
process_child_command_line	String	Subprocess command line
process_launch_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.
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.

Table 4-250 user_info

Parameter	Type	Description
user_id	String	User UID
user_name	String	Username

Table 4-251 file_info

Parameter	Type	Description
file_path	String	File path/name.
file_content	String	File path/name.
file_new_path	String	New file path/name.
file_hash	String	File Hash
file_md5	String	File MD5
file_sha256	String	File SHA256
file_attr	String	File attribute.

Table 4-252 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.
name	String	Data class name.

Status code: 400

Table 4-253 Response header parameters

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

Table 4-254 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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",
"ipdr_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",
"ipdr_phase" : "Preparation|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"
}
}

```

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 Query the intelligence indicator list

Function

Query the intelligence indicator list.

Calling Method

For details, see [Calling APIs](#).

URI

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

Table 4-255 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID

Request Parameters

Table 4-256 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Token of the tenant.
content-type	Yes	String	application/ json;charset=UTF-8

Table 4-257 Request body parameters

Parameter	Mandatory	Type	Description
ids	No	Array of strings	List of indicator IDs.
dataclass_id	No	String	Data class ID.
condition	Yes	condition object	Search condition expression.
offset	Yes	Integer	request offset, from 0
limit	Yes	Integer	request limit size
sort_by	No	String	sort by property, create_time.
from_date	No	String	Query start time, for example, 2024-01-20T00:00:00.000Z +0800
to_date	No	String	Query end time, for example, 2024-01-26T23:59:59.999Z +0800

Table 4-258 condition

Parameter	Mandatory	Type	Description
conditions	No	Array of conditions objects	Expression list.
logics	No	Array of strings	Expression logic.

Table 4-259 conditions

Parameter	Mandatory	Type	Description
name	No	String	Expression name.
data	No	Array of strings	Expression content list.

Response Parameters

Status code: 200

Table 4-260 Response header parameters

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

Table 4-261 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
total	Integer	Total
data	Array of IndicatorDetail objects	List of indicators.

Table 4-262 IndicatorDetail

Parameter	Type	Description
id	String	Indicator ID.
name	String	Indicator name.
data_object	IndicatorDataObjectDetail object	Indicator details
workspace_id	String	Workspace ID
project_id	String	Project ID.
dataclass_ref	DataClassRefPojo object	Data class object information.
create_time	String	Creation time.
update_time	String	Update time.

Table 4-263 IndicatorDataObjectDetail

Parameter	Type	Description
indicator_type	indicator_type object	Indicator type object.
value	String	Value, for example, ip url domain.

Parameter	Type	Description
update_time	String	Update time.
create_time	String	Creation time.
environment	environment object	Environment Info
data_source	data_source object	Data source.
first_report_time	String	First Occurred At
is_deleted	Boolean	Delete
last_report_time	String	Last occurred.
granular_marking	Integer	Confidentiality level. 1 -- First discovery; 2 -- Self-produced data; 3 -- Purchase required; and 4 -- Direct query from the external network.
name	String	Name.
id	String	Indicator ID.
project_id	String	Project ID.
revoked	Boolean	Whether to discard.
status	String	Status. The options are Open, Closed, and Revoked.
verdict	String	Threat degree. The options are Black, White, and Gray.
workspace_id	String	Workspace ID
confidence	Integer	Confidence. The value range is 80 to 100.

Table 4-264 indicator_type

Parameter	Type	Description
indicator_type	String	Indicator type.
id	String	Indicator type ID.

Table 4-265 environment

Parameter	Type	Description
vendor_type	String	Environment suppliers
domain_id	String	Tenant ID.
region_id	String	Region ID
project_id	String	Project ID.

Table 4-266 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows-- 1- cloud product 2- Third-party product 3- Tenant product
domain_id	String	Tenant ID.
project_id	String	Project ID.
region_id	String	Region ID

Table 4-267 DataClassRefPojo

Parameter	Type	Description
id	String	Data class ID.
name	String	Data class name.

Status code: 400

Table 4-268 Response header parameters

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

Table 4-269 Response body parameters

Parameter	Type	Description
code	String	Error Code

Parameter	Type	Description
message	String	Error Description

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" ],
  "dataclass_id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
  "condition" : {
    "conditions" : [ {
      "name" : "name",
      "data" : [ "name", "=", "Indicator name" ]
    } ],
    "logics" : [ "name" ]
  },
  "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" : {
        "indicator_type" : "ipv6",
        "id" : "ac794b2dfab9fe8c0676587301a636d3"
      },
      "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
}

```

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 4-270 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID

Request Parameters

Table 4-271 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Token of the tenant.
content-type	Yes	String	application/ json;charset=UTF-8

Table 4-272 Request body parameters

Parameter	Mandatory	Type	Description
data_object	Yes	CreateIndicatorDetail object	Indicator details.

Table 4-273 CreateIndicatorDetail

Parameter	Mandatory	Type	Description
data_source	Yes	data_source object	Data source.
verdict	Yes	String	Threat Rating
confidence	No	Integer	Confidence level
status	No	String	Status
labels	No	String	Tag.
value	Yes	String	Value.
granular_marking	Yes	String	Confidentiality level. 1 -- First discovery; 2 -- Self-produced data; 3 -- Purchase required; and 4 -- Direct query from the external network.
environment	Yes	environment object	Environment Info
defanged	Yes	Boolean	Still valid?
first_report_time	Yes	String	First Occurred At
last_report_time	No	String	Last occurred.

Parameter	Mandatory	Type	Description
id	No	String	Indicator ID.
indicator_type	Yes	indicator_type object	Indicator type statistics.
name	Yes	String	Indicator name.
dataclass_id	No	String	Data class ID.
workspace_id	Yes	String	workspace id
project_id	No	String	Project id value
dataclass	No	DataClassRefPojo object	Data class object information.
create_time	No	String	Create time
update_time	No	String	Update time

Table 4-274 data_source

Parameter	Mandatory	Type	Description
source_type	Yes	Integer	current page count
domain_id	Yes	String	Id value
project_id	Yes	String	Id value
region_id	Yes	String	Id value
product_name	Yes	String	Id value
product_feature	Yes	String	Id value

Table 4-275 environment

Parameter	Mandatory	Type	Description
vendor_type	Yes	String	Environment suppliers
domain_id	Yes	String	Tenant ID.
region_id	Yes	String	Region ID
project_id	Yes	String	Project ID.

Table 4-276 indicator_type

Parameter	Mandatory	Type	Description
indicator_type	Yes	String	Metric Type
id	Yes	String	Indicator type ID.

Table 4-277 DataClassRefPojo

Parameter	Mandatory	Type	Description
id	Yes	String	Data class ID.
name	No	String	Data class name.

Response Parameters

Status code: 200

Table 4-278 Response header parameters

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

Table 4-279 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
data	IndicatorDetail object	Indicator details.

Table 4-280 IndicatorDetail

Parameter	Type	Description
id	String	Indicator ID.
name	String	Indicator name.
data_object	IndicatorDataObjectDetail object	Indicator details

Parameter	Type	Description
workspace_id	String	Workspace ID
project_id	String	Project ID.
dataclass_ref	DataClassRefPojo object	Data class object information.
create_time	String	Creation time.
update_time	String	Update time.

Table 4-281 IndicatorDataObjectDetail

Parameter	Type	Description
indicator_type	indicator_type object	Indicator type object.
value	String	Value, for example, ip url domain.
update_time	String	Update time.
create_time	String	Creation time.
environment	environment object	Environment Info
data_source	data_source object	Data source.
first_report_time	String	First Occurred At
is_deleted	Boolean	Delete
last_report_time	String	Last occurred.
granular_marking	Integer	Confidentiality level. 1 -- First discovery; 2 -- Self-produced data; 3 -- Purchase required; and 4 -- Direct query from the external network.
name	String	Name.
id	String	Indicator ID.
project_id	String	Project ID.
revoked	Boolean	Whether to discard.
status	String	Status. The options are Open, Closed, and Revoked.
verdict	String	Threat degree. The options are Black, White, and Gray.

Parameter	Type	Description
workspace_id	String	Workspace ID
confidence	Integer	Confidence. The value range is 80 to 100.

Table 4-282 indicator_type

Parameter	Type	Description
indicator_type	String	Indicator type.
id	String	Indicator type ID.

Table 4-283 environment

Parameter	Type	Description
vendor_type	String	Environment suppliers
domain_id	String	Tenant ID.
region_id	String	Region ID
project_id	String	Project ID.

Table 4-284 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows-- 1- cloud product 2- Third-party product 3- Tenant product
domain_id	String	Tenant ID.
project_id	String	Project ID.
region_id	String	Region ID

Table 4-285 DataClassRefPojo

Parameter	Type	Description
id	String	Data class ID.
name	String	Data class name.

Status code: 400

Table 4-286 Response header parameters

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

Table 4-287 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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",
    "workspace_id": "909494e3-558e-46b6-a9eb-07a8e18ca620",
    "project_id": "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "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" : {  
        "indicator_type" : "ipv6",  
        "id" : "ac794b2dfab9fe8c0676587301a636d3"  
      },  
      "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"  
  }  
}
```

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 4-288 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID

Request Parameters

Table 4-289 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Token of the tenant.
content-type	Yes	String	application/ json;charset=UTF-8

Table 4-290 Request body parameters

Parameter	Mandatory	Type	Description
batch_ids	No	Array of strings	List of indicator IDs.

Response Parameters

Status code: 200

Table 4-291 Response header parameters

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

Table 4-292 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
data	IndicatorBatchOperateResponse object	Intelligence response parameters

Table 4-293 IndicatorBatchOperateResponse

Parameter	Type	Description
success_ids	Array of strings	Succeeded IDs.
error_ids	Array of strings	Failed IDs.

Status code: 400

Table 4-294 Response header parameters

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

Table 4-295 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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" ]
  }
}
```

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 4-296 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
indicator_id	Yes	String	Intelligence indicator ID.

Request Parameters

Table 4-297 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Token of the tenant.
content-type	Yes	String	application/ json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-298 Response header parameters

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

Table 4-299 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
data	IndicatorDetail object	Indicator details.

Table 4-300 IndicatorDetail

Parameter	Type	Description
id	String	Indicator ID.
name	String	Indicator name.
data_object	IndicatorDataObjectDetail object	Indicator details
workspace_id	String	Workspace ID
project_id	String	Project ID.
dataclass_ref	DataClassRefPojo object	Data class object information.

Parameter	Type	Description
create_time	String	Creation time.
update_time	String	Update time.

Table 4-301 IndicatorDataObjectDetail

Parameter	Type	Description
indicator_type	indicator_type object	Indicator type object.
value	String	Value, for example, ip url domain.
update_time	String	Update time.
create_time	String	Creation time.
environment	environment object	Environment Info
data_source	data_source object	Data source.
first_report_time	String	First Occurred At
is_deleted	Boolean	Delete
last_report_time	String	Last occurred.
granular_marking	Integer	Confidentiality level. 1 -- First discovery; 2 -- Self-produced data; 3 -- Purchase required; and 4 -- Direct query from the external network.
name	String	Name.
id	String	Indicator ID.
project_id	String	Project ID.
revoked	Boolean	Whether to discard.
status	String	Status. The options are Open, Closed, and Revoked.
verdict	String	Threat degree. The options are Black, White, and Gray.
workspace_id	String	Workspace ID
confidence	Integer	Confidence. The value range is 80 to 100.

Table 4-302 indicator_type

Parameter	Type	Description
indicator_type	String	Indicator type.
id	String	Indicator type ID.

Table 4-303 environment

Parameter	Type	Description
vendor_type	String	Environment suppliers
domain_id	String	Tenant ID.
region_id	String	Region ID
project_id	String	Project ID.

Table 4-304 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows-- 1- cloud product 2- Third-party product 3- Tenant product
domain_id	String	Tenant ID.
project_id	String	Project ID.
region_id	String	Region ID

Table 4-305 DataClassRefPojo

Parameter	Type	Description
id	String	Data class ID.
name	String	Data class name.

Status code: 400

Table 4-306 Response header parameters

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

Table 4-307 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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": {
        "indicator_type": "ipv6",
        "id": "ac794b2dfab9fe8c0676587301a636d3"
      },
      "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"
  }
}
```

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 4-308 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
indicator_id	Yes	String	Indicator ID.

Request Parameters

Table 4-309 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Token of the tenant.
content-type	Yes	String	application/ json;charset=UTF-8

Table 4-310 Request body parameters

Parameter	Mandatory	Type	Description
data_object	No	IndicatorDataObjectDetail object	Indicator details

Table 4-311 IndicatorDataObjectDetail

Parameter	Mandatory	Type	Description
indicator_type	No	indicator_type object	Indicator type object.
value	No	String	Value, for example, ip url domain.
update_time	No	String	Update time.
create_time	No	String	Creation time.
environment	No	environment object	Environment Info
data_source	No	data_source object	Data source.
first_report_time	No	String	First Occurred At
is_deleted	No	Boolean	Delete
last_report_time	No	String	Last occurred.
granular_marking	No	Integer	Confidentiality level. 1 -- First discovery; 2 -- Self-produced data; 3 -- Purchase required; and 4 -- Direct query from the external network.
name	No	String	Name.
id	No	String	Indicator ID.
project_id	No	String	Project ID.
revoked	No	Boolean	Whether to discard.
status	No	String	Status. The options are Open, Closed, and Revoked.
verdict	No	String	Threat degree. The options are Black, White, and Gray.

Parameter	Mandatory	Type	Description
workspace_id	No	String	Workspace ID
confidence	No	Integer	Confidence. The value range is 80 to 100.

Table 4-312 indicator_type

Parameter	Mandatory	Type	Description
indicator_type	No	String	Indicator type.
id	No	String	Indicator type ID.

Table 4-313 environment

Parameter	Mandatory	Type	Description
vendor_type	No	String	Environment suppliers
domain_id	No	String	Tenant ID.
region_id	No	String	Region ID
project_id	No	String	Project ID.

Table 4-314 data_source

Parameter	Mandatory	Type	Description
source_type	No	Integer	Data source type. The options are as follows-- 1- cloud product 2- Third-party product 3- Tenant product
domain_id	No	String	Tenant ID.
project_id	No	String	Project ID.
region_id	No	String	Region ID

Response Parameters

Status code: 200

Table 4-315 Response header parameters

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

Table 4-316 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
data	IndicatorDetail object	Indicator details.

Table 4-317 IndicatorDetail

Parameter	Type	Description
id	String	Indicator ID.
name	String	Indicator name.
data_object	IndicatorDataObjectDetail object	Indicator details
workspace_id	String	Workspace ID
project_id	String	Project ID.
dataclass_ref	DataClassRefPojo object	Data class object information.
create_time	String	Creation time.
update_time	String	Update time.

Table 4-318 IndicatorDataObjectDetail

Parameter	Type	Description
indicator_type	indicator_type object	Indicator type object.
value	String	Value, for example, ip url domain.
update_time	String	Update time.
create_time	String	Creation time.

Parameter	Type	Description
environment	environment object	Environment Info
data_source	data_source object	Data source.
first_report_time	String	First Occurred At
is_deleted	Boolean	Delete
last_report_time	String	Last occurred.
granular_marking	Integer	Confidentiality level. 1 -- First discovery; 2 -- Self-produced data; 3 -- Purchase required; and 4 -- Direct query from the external network.
name	String	Name.
id	String	Indicator ID.
project_id	String	Project ID.
revoked	Boolean	Whether to discard.
status	String	Status. The options are Open, Closed, and Revoked.
verdict	String	Threat degree. The options are Black, White, and Gray.
workspace_id	String	Workspace ID
confidence	Integer	Confidence. The value range is 80 to 100.

Table 4-319 indicator_type

Parameter	Type	Description
indicator_type	String	Indicator type.
id	String	Indicator type ID.

Table 4-320 environment

Parameter	Type	Description
vendor_type	String	Environment suppliers
domain_id	String	Tenant ID.

Parameter	Type	Description
region_id	String	Region ID
project_id	String	Project ID.

Table 4-321 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows-- 1- cloud product 2- Third-party product 3- Tenant product
domain_id	String	Tenant ID.
project_id	String	Project ID.
region_id	String	Region ID

Table 4-322 DataClassRefPojo

Parameter	Type	Description
id	String	Data class ID.
name	String	Data class name.

Status code: 400

Table 4-323 Response header parameters

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

Table 4-324 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

Example Requests

Update an indicator. Set the trigger flag to No and value to IP.

```
{
  "data_object": {
    "indicator_type": {
      "indicator_type": "ipv6",
      "id": "ac794b2dfab9fe8c0676587301a636d3"
    },
    "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": {
        "indicator_type": "ipv6",
        "id": "ac794b2dfab9fe8c0676587301a636d3"
      },
      "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"
  }
}
```

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 4-325 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
playbook_id	Yes	String	Playbook ID.

Table 4-326 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 occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
version_query_type	Yes	String	Playbook version type. The options are 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 occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Request Parameters

Table 4-327 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.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-328 Response header parameters

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

Table 4-329 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
data	PlaybookInstanceMonitorDetail object	Playbook monitoring details.

Table 4-330 PlaybookInstanceMonitorDetail

Parameter	Type	Description
total_instance_run_num	Integer	Total running times.
schedule_instance_run_num	Integer	Scheduled executions.
event_instance_run_num	Integer	Time-triggered executions.
average_run_time	Number	Average duration.
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.
success_instance_num	Integer	Number of successful instances.
fail_instance_num	Integer	Failed instances.
terminate_instance_num	Integer	Number of terminated instances.

Parameter	Type	Description
running_instance_num	Integer	Number of running instances.

Table 4-331 PlaybookInstanceRunStatistics

Parameter	Type	Description
playbook_instance_id	String	Playbook instance ID.
playbook_instance_name	String	Playbook instance name.
playbook_instance_run_time	Number	Playbook instance running time.

Status code: 400

Table 4-332 Response header parameters

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

Table 4-333 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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
}
}

```

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 4-334 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID

Request Parameters

Table 4-335 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.
content-type	Yes	String	application/ json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-336 Response header parameters

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

Table 4-337 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
data	PlaybookStatisticDetail object	Playbook statistic information.

Table 4-338 PlaybookStatisticDetail

Parameter	Type	Description
unapproved_num	Integer	Number of unapproved playbooks.
disabled_num	Integer	Number of playbooks that are not enabled.
enabled_num	Integer	Number of enabled playbooks.

Status code: 400

Table 4-339 Response header parameters

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

Table 4-340 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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
  }
}
```

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 4-341 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID

Table 4-342 Query Parameters

Parameter	Mandatory	Type	Description
search_txt	No	String	Keyword
enabled	No	Boolean	Whether to enable.
offset	Yes	Integer	Indicates the page number. Start position of the query result. The value starts from 0.
limit	Yes	Integer	The maximum number of records can be returned on each page for a pagination query. The value starts from 1.
description	No	String	Playbook description.
dataclass_name	No	String	Data class name.
name	No	String	Playbook name.

Request Parameters

Table 4-343 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.
content-type	Yes	String	application/ json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-344 Response header parameters

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

Table 4-345 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Response message information
total	Integer	Total records.
size	Integer	Records on each page.
page	Integer	Current page.
data	Array of PlaybookInfo objects	Playbook list information.

Table 4-346 PlaybookInfo

Parameter	Type	Description
id	String	Playbook ID.
name	String	Playbook name.
description	String	Provides supplementary information about the resource.
create_time	String	Playbook creation time.
update_time	String	Playbook update time.
project_id	String	Project ID.
version_id	String	Playbook version ID.
enabled	Boolean	Whether to enable.
workspace_id	String	Workspace ID
approve_role	String	Reviewer role.
user_role	String	Role
edit_role	String	Edit Role for Account
owner_id	String	ID
version	String	Version No.
dataclass_name	String	Data class name.
dataclass_id	String	Data class ID.
unaudited_version_id	String	ID of the playbook version to be reviewed.
reject_version_id	String	ID of the rejected playbook version.

Status code: 400

Table 4-347 Response header parameters

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

Table 4-348 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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"
  } ]
}
```

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 4-349 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID

Request Parameters

Table 4-350 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.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-351 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Playbook name.
description	No	String	Description.
workspace_id	Yes	String	Workspace ID

Response Parameters

Status code: 200

Table 4-352 Response header parameters

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

Table 4-353 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
data	PlaybookInfo object	Playbook details.

Table 4-354 PlaybookInfo

Parameter	Type	Description
id	String	Playbook ID.
name	String	Playbook name.
description	String	Provides supplementary information about the resource.
create_time	String	Playbook creation time.
update_time	String	Playbook update time.
project_id	String	Project ID.
version_id	String	Playbook version ID.
enabled	Boolean	Whether to enable.
workspace_id	String	Workspace ID
approve_role	String	Reviewer role.
user_role	String	Role
edit_role	String	Edit Role for Account
owner_id	String	ID
version	String	Version No.

Parameter	Type	Description
dataclass_name	String	Data class name.
dataclass_id	String	Data class ID.
unaudited_version_id	String	ID of the playbook version to be reviewed.
reject_version_id	String	ID of the rejected playbook version.

Status code: 400

Table 4-355 Response header parameters

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

Table 4-356 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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"
}
```

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"
}
}

```

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 4-357 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
playbook_id	Yes	String	ID of playbook

Request Parameters

Table 4-358 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.
content-type	Yes	String	application/ json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-359 Response header parameters

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

Table 4-360 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
data	PlaybookInfo object	Playbook details.

Table 4-361 PlaybookInfo

Parameter	Type	Description
id	String	Playbook ID.
name	String	Playbook name.
description	String	Provides supplementary information about the resource.

Parameter	Type	Description
create_time	String	Playbook creation time.
update_time	String	Playbook update time.
project_id	String	Project ID.
version_id	String	Playbook version ID.
enabled	Boolean	Whether to enable.
workspace_id	String	Workspace ID
approve_role	String	Reviewer role.
user_role	String	Role
edit_role	String	Edit Role for Account
owner_id	String	ID
version	String	Version No.
dataclass_name	String	Data class name.
dataclass_id	String	Data class ID.
unaudited_version_id	String	ID of the playbook version to be reviewed.
reject_version_id	String	ID of the rejected playbook version.

Status code: 400

Table 4-362 Response header parameters

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

Table 4-363 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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"
  }
}
```

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 4-364 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
playbook_id	Yes	String	ID of playbook

Request Parameters

Table 4-365 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.
content-type	Yes	String	application/ json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-366 Response header parameters

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

Table 4-367 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
data	PlaybookInfo object	Playbook details.

Table 4-368 PlaybookInfo

Parameter	Type	Description
id	String	Playbook ID.
name	String	Playbook name.
description	String	Provides supplementary information about the resource.
create_time	String	Playbook creation time.
update_time	String	Playbook update time.
project_id	String	Project ID.
version_id	String	Playbook version ID.
enabled	Boolean	Whether to enable.
workspace_id	String	Workspace ID
approve_role	String	Reviewer role.
user_role	String	Role
edit_role	String	Edit Role for Account
owner_id	String	ID
version	String	Version No.
dataclass_name	String	Data class name.
dataclass_id	String	Data class ID.
unaudited_version_id	String	ID of the playbook version to be reviewed.
reject_version_id	String	ID of the rejected playbook version.

Status code: 400

Table 4-369 Response header parameters

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

Table 4-370 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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"
  }
}
```

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 4-371 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
playbook_id	Yes	String	Playbook ID.

Request Parameters

Table 4-372 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.
content-type	Yes	String	application/ json;charset=UTF-8

Table 4-373 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	Playbook name.
description	No	String	Description.
enabled	No	Boolean	Whether to enable.

Parameter	Mandatory	Type	Description
active_version_id	No	String	ID of the enabled playbook version.

Response Parameters

Status code: 200

Table 4-374 Response header parameters

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

Table 4-375 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
data	PlaybookInfo object	Playbook details.

Table 4-376 PlaybookInfo

Parameter	Type	Description
id	String	Playbook ID.
name	String	Playbook name.
description	String	Provides supplementary information about the resource.
create_time	String	Playbook creation time.
update_time	String	Playbook update time.
project_id	String	Project ID.
version_id	String	Playbook version ID.
enabled	Boolean	Whether to enable.
workspace_id	String	Workspace ID
approve_role	String	Reviewer role.

Parameter	Type	Description
user_role	String	Role
edit_role	String	Edit Role for Account
owner_id	String	ID
version	String	Version No.
dataclass_name	String	Data class name.
dataclass_id	String	Data class ID.
unaudited_version_id	String	ID of the playbook version to be reviewed.
reject_version_id	String	ID of the rejected playbook version.

Status code: 400

Table 4-377 Response header parameters

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

Table 4-378 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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"
  }
}
```

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 4-379 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. Project ID.
workspace_id	Yes	String	Workspace ID. Workspace ID.

Table 4-380 Query Parameters

Parameter	Mandatory	Type	Description
offset	Yes	Long	The query offset. Offset.
limit	Yes	Long	Number of bucket groups Limit.
sort_key	No	String	Sorting field. Sort key
sort_dir	No	String	Sort direction, asc or desc.
pipe_id	No	String	Pipeline ID.Pipe ID.
rule_name	No	String	Alert rule name.
rule_id	No	String	Alert rule ID.
status	No	Array of strings	Status. The options are as follows - Enabled - Disabled
severity	No	Array of strings	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.

Request Parameters

Table 4-381 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.

Response Parameters

Status code: 200

Table 4-382 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 4-383 Response body parameters

Parameter	Type	Description
count	Long	Total number. Total count.
records	Array of AlertRule objects	Alert models. Alert rules.

Table 4-384 AlertRule

Parameter	Type	Description
rule_id	String	Alert rule ID.
pipe_id	String	Pipeline ID.Pipe ID.
pipe_name	String	Data pipeline name.Pipe name.
create_by	String	Created by. Created by.
create_time	Long	Creation time. Create time.
update_by	String	Updated by. Update by.
update_time	Long	Update time. Update time.
delete_time	Long	The deletion time. Delete time.
rule_name	String	Alert rule name.
query	String	Query.
query_type	String	SQL query syntax. Query type. SQL.
status	String	Status. The options are as follows - Enabled - Disabled
severity	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.
custom_properties	Map<String,String >	Custom extension information. Custom properties.
event_grouping	Boolean	Alert group. Alert group.
schedule	Schedule object	Schedule Rule.

Parameter	Type	Description
triggers	Array of AlertRuleTrigger objects	Alert triggering rules. Alert triggers.

Table 4-385 Schedule

Parameter	Type	Description
frequency_interval	Integer	Scheduling interval. Frequency interval.
frequency_unit	String	The unit of the scheduling interval. The value can be minute, hour, or day. Frequency unit. MINUTE, HOUR, DAY.
period_interval	Integer	Time window interval. Period interval.
period_unit	String	Time Window unit. The value can be minute, hour, or day. Period unit. MINUTE, HOUR, DAY.
delay_interval	Integer	The delay interval. Delay interval
overtime_interval	Integer	Timeout interval. Overtime interval

Table 4-386 AlertRuleTrigger

Parameter	Type	Description
mode	String	Number of modes. Mode. 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.
expression	String	expression
severity	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.
accumulated_time s	Integer	accumulated_times

Status code: 400

Table 4-387 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"
  } ]
} ] ] }
```

Status Codes

Status Code	Description
200	Success
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 4-388 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. Project ID.
workspace_id	Yes	String	Workspace ID. Workspace ID.

Request Parameters

Table 4-389 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.

Table 4-390 Request body parameters

Parameter	Mandatory	Type	Description
pipe_id	Yes	String	Pipeline ID.Pipe ID.
rule_name	Yes	String	Alert rule name. Alert rule name.
description	No	String	Link description.Description.
query	Yes	String	Query statement. Query.
query_type	No	String	SQL query syntax. Query type. SQL.
status	No	String	Status. The options are as follows - Enabled - Disabled
severity	No	String	Severity. The options are as follows - Tips - Low - Medium - High - 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.
suppression	No	Boolean	Alert containment. Suppression.
simulation	No	Boolean	Simulated alerts. Simulation.
schedule	Yes	Schedule object	
triggers	Yes	Array of AlertRuleTrigger objects	Alert triggering rules. Alert triggers.
pipe_name	Yes	String	pipe name
alert_name	Yes	String	alert name
alert_description	No	String	alert description
alert_remediation	No	String	alert remediation
accumulated_times	No	Integer	accumulated times

Table 4-391 Schedule

Parameter	Mandatory	Type	Description
frequency_interval	Yes	Integer	Scheduling interval. Frequency interval.
frequency_unit	Yes	String	The unit of the scheduling interval. The value can be minute, hour, or day. Frequency unit. MINUTE, HOUR, DAY.
period_interval	Yes	Integer	Time window interval. Period interval.
period_unit	Yes	String	Time Window unit. The value can be minute, hour, or day. Period unit. MINUTE, HOUR, DAY.
delay_interval	No	Integer	The delay interval. Delay interval
overtime_interval	No	Integer	Timeout interval. Overtime interval

Table 4-392 AlertRuleTrigger

Parameter	Mandatory	Type	Description
mode	No	String	Number of modes. Mode. 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.
expression	Yes	String	expression
severity	No	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.
accumulated_times	No	Integer	accumulated_times

Response Parameters

Status code: 200

Table 4-393 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 4-394 Response body parameters

Parameter	Type	Description
rule_id	String	Alert rule ID.
pipe_id	String	Pipeline ID.Pipe ID.
pipe_name	String	Data pipeline name.Pipe name.
create_by	String	Created by. Created by.
create_time	Long	Creation time. Create time.
update_by	String	Updated by. Update by.
update_time	Long	Update time. Update time.
delete_time	Long	The deletion time. Delete time.
rule_name	String	Alert rule name.
query	String	Query.
query_type	String	SQL query syntax. Query type. SQL.
status	String	Status. The options are as follows - Enabled - Disabled
severity	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.
custom_properties	Map<String,String >	Custom extension information. Custom properties.
event_grouping	Boolean	Alert group. Alert group.
schedule	Schedule object	Schedule Rule.
triggers	Array of AlertRuleTrigger objects	Alert triggering rules. Alert triggers.

Table 4-395 Schedule

Parameter	Type	Description
frequency_interval	Integer	Scheduling interval. Frequency interval.
frequency_unit	String	The unit of the scheduling interval. The value can be minute, hour, or day. Frequency unit. MINUTE, HOUR, DAY.
period_interval	Integer	Time window interval. Period interval.
period_unit	String	Time Window unit. The value can be minute, hour, or day. Period unit. MINUTE, HOUR, DAY.
delay_interval	Integer	The delay interval. Delay interval
overtime_interval	Integer	Timeout interval. Overtime interval

Table 4-396 AlertRuleTrigger

Parameter	Type	Description
mode	String	Number of modes. Mode. 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.
expression	String	expression
severity	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.
accumulated_time s	Integer	accumulated_times

Status code: 400

Table 4-397 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",
  "pipe_name" : "sec-hss-alarm",
  "rule_name" : "Alert rule",
  "description" : "An alert rule",
  "query" : "* | select status, count(*) as count group by status",
  "query_type" : "SQL",
  "status" : "ENABLED",
  "severity" : "TIPS",
  "alert_name" : "test",
  "custom_properties" : {
    "references" : "https://localhost/references",
    "maintainer" : "isap"
  },
  "event_grouping" : false,
  "suppression" : false,
  "simulation" : false,
  "accumulated_times" : 1,
  "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",
    "accumulated_times" : 1
  } ]
}
```

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"
  } ]
}

```

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 4-398 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. Project ID.
workspace_id	Yes	String	Workspace ID. Workspace ID.

Request Parameters

Table 4-399 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.

Table 4-400 Request body parameters

Parameter	Mandatory	Type	Description
[items]	Yes	Array of strings	Array of Alert rule ID

Response Parameters

Status code: 200

Table 4-401 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 4-402 Response body parameters

Parameter	Type	Description
deleted	Boolean	Deleted.
fail_list	Array of AlertRule objects	Alert rule ID.
success_list	Array of AlertRule objects	Alert rule ID.

Table 4-403 AlertRule

Parameter	Type	Description
rule_id	String	Alert rule ID.
pipe_id	String	Pipeline ID.Pipe ID.
pipe_name	String	Data pipeline name.Pipe name.
create_by	String	Created by. Created by.
create_time	Long	Creation time. Create time.
update_by	String	Updated by. Update by.
update_time	Long	Update time. Update time.
delete_time	Long	The deletion time. Delete time.
rule_name	String	Alert rule name.
query	String	Query.
query_type	String	SQL query syntax. Query type. SQL.
status	String	Status. The options are as follows - Enabled - Disabled
severity	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.
custom_properties	Map<String,String >	Custom extension information. Custom properties.
event_grouping	Boolean	Alert group. Alert group.
schedule	Schedule object	Schedule Rule.
triggers	Array of AlertRuleTrigger objects	Alert triggering rules. Alert triggers.

Table 4-404 Schedule

Parameter	Type	Description
frequency_interval	Integer	Scheduling interval. Frequency interval.
frequency_unit	String	The unit of the scheduling interval. The value can be minute, hour, or day. Frequency unit. MINUTE, HOUR, DAY.
period_interval	Integer	Time window interval. Period interval.

Parameter	Type	Description
period_unit	String	Time Window unit. The value can be minute, hour, or day. Period unit. MINUTE, HOUR, DAY.
delay_interval	Integer	The delay interval. Delay interval
overtime_interval	Integer	Timeout interval. Overtime interval

Table 4-405 AlertRuleTrigger

Parameter	Type	Description
mode	String	Number of modes. Mode. 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.
expression	String	expression
severity	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.
accumulated_time s	Integer	accumulated_times

Status code: 400

Table 4-406 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

```
{
  "deleted" : true,
  "fail_list" : [],
  "success_list" : []
}
```

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 4-407 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. Project ID.
workspace_id	Yes	String	Workspace ID. Workspace ID.
rule_id	Yes	String	Alert rule ID.

Request Parameters

Table 4-408 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.

Response Parameters

Status code: 200

Table 4-409 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 4-410 Response body parameters

Parameter	Type	Description
rule_id	String	Alert rule ID.
pipe_id	String	Pipeline ID.Pipe ID.
pipe_name	String	Data pipeline name.Pipe name.
create_by	String	Created by. Created by.
create_time	Long	Creation time. Create time.
update_by	String	Updated by. Update by.
update_time	Long	Update time. Update time.
delete_time	Long	The deletion time. Delete time.
rule_name	String	Alert rule name.
query	String	Query.
query_type	String	SQL query syntax. Query type. SQL.
status	String	Status. The options are as follows - Enabled - Disabled

Parameter	Type	Description
severity	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.
custom_properties	Map<String,String >	Custom extension information. Custom properties.
event_grouping	Boolean	Alert group. Alert group.
schedule	Schedule object	Schedule Rule.
triggers	Array of AlertRuleTrigger objects	Alert triggering rules. Alert triggers.

Table 4-411 Schedule

Parameter	Type	Description
frequency_interval	Integer	Scheduling interval. Frequency interval.
frequency_unit	String	The unit of the scheduling interval. The value can be minute, hour, or day. Frequency unit. MINUTE, HOUR, DAY.
period_interval	Integer	Time window interval. Period interval.
period_unit	String	Time Window unit. The value can be minute, hour, or day. Period unit. MINUTE, HOUR, DAY.
delay_interval	Integer	The delay interval. Delay interval
overtime_interval	Integer	Timeout interval. Overtime interval

Table 4-412 AlertRuleTrigger

Parameter	Type	Description
mode	String	Number of modes. Mode. 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.
expression	String	expression
severity	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.

Parameter	Type	Description
accumulated_times	Integer	accumulated_times

Status code: 400

Table 4-413 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"
  } ]
}
```

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 4-414 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. Project ID.
workspace_id	Yes	String	Workspace ID. Workspace ID.
rule_id	Yes	String	Alert rule ID.

Request Parameters

Table 4-415 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.

Table 4-416 Request body parameters

Parameter	Mandatory	Type	Description
rule_name	No	String	Alert rule name.
description	No	String	Description.Description.
query	No	String	Query.
query_type	No	String	SQL query syntax. Query type. SQL.
status	No	String	Status. The options are as follows - Enabled - Disabled
severity	No	String	Severity. The options are as follows - Tips - Low - Medium - High - 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.
suppression	No	Boolean	Alert containment. Suppression
simulation	No	Boolean	Simulated alerts. Simulation.
schedule	No	Schedule object	Schedule Rule.
triggers	No	Array of AlertRuleTrigger objects	Alert triggering rules. Alert triggers.

Table 4-417 Schedule

Parameter	Mandatory	Type	Description
frequency_interval	Yes	Integer	Scheduling interval. Frequency interval.
frequency_unit	Yes	String	The unit of the scheduling interval. The value can be minute, hour, or day. Frequency unit. MINUTE, HOUR, DAY.
period_interval	Yes	Integer	Time window interval. Period interval.

Parameter	Mandatory	Type	Description
period_unit	Yes	String	Time Window unit. The value can be minute, hour, or day. Period unit. MINUTE, HOUR, DAY.
delay_interval	No	Integer	The delay interval. Delay interval
overtime_interval	No	Integer	Timeout interval. Overtime interval

Table 4-418 AlertRuleTrigger

Parameter	Mandatory	Type	Description
mode	No	String	Number of modes. Mode. 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.
expression	Yes	String	expression
severity	No	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.
accumulated_times	No	Integer	accumulated_times

Response Parameters

Status code: 200

Table 4-419 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 4-420 Response body parameters

Parameter	Type	Description
rule_id	String	Alert rule ID.
pipe_id	String	Pipeline ID.Pipe ID.
pipe_name	String	Data pipeline name.Pipe name.
create_by	String	Created by. Created by.
create_time	Long	Creation time. Create time.
update_by	String	Updated by. Update by.
update_time	Long	Update time. Update time.
delete_time	Long	The deletion time. Delete time.
rule_name	String	Alert rule name.
query	String	Query.
query_type	String	SQL query syntax. Query type. SQL.
status	String	Status. The options are as follows - Enabled - Disabled
severity	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.
custom_properties	Map<String,String >	Custom extension information. Custom properties.
event_grouping	Boolean	Alert group. Alert group.
schedule	Schedule object	Schedule Rule.
triggers	Array of AlertRuleTrigger objects	Alert triggering rules. Alert triggers.

Table 4-421 Schedule

Parameter	Type	Description
frequency_interval	Integer	Scheduling interval. Frequency interval.
frequency_unit	String	The unit of the scheduling interval. The value can be minute, hour, or day. Frequency unit. MINUTE, HOUR, DAY.
period_interval	Integer	Time window interval. Period interval.

Parameter	Type	Description
period_unit	String	Time Window unit. The value can be minute, hour, or day. Period unit. MINUTE, HOUR, DAY.
delay_interval	Integer	The delay interval. Delay interval
overtime_interval	Integer	Timeout interval. Overtime interval

Table 4-422 AlertRuleTrigger

Parameter	Type	Description
mode	String	Number of modes. Mode. 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.
expression	String	expression
severity	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.
accumulated_time_s	Integer	accumulated_times

Status code: 400

Table 4-423 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"  
  } ]  
}
```

Status Codes

Status Code	Description
200	Success

Status Code	Description
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 4-424 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. Project ID.
workspace_id	Yes	String	Workspace ID. Workspace ID.

Request Parameters

Table 4-425 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.

Table 4-426 Request body parameters

Parameter	Mandatory	Type	Description
pipe_id	Yes	String	Pipeline ID.Pipe ID.
query	Yes	String	Query.
query_type	No	String	SQL query syntax. Query type. SQL.
from	Yes	Long	Start time.Start time.
to	Yes	Long	End time.End time.
event_grouping	No	Boolean	Alert group. Incident group.
triggers	Yes	Array of AlertRuleTrigger objects	Alert triggering rules. Alert triggers.

Table 4-427 AlertRuleTrigger

Parameter	Mandatory	Type	Description
mode	No	String	Number of modes. Mode. 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.
expression	Yes	String	expression
severity	No	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.
accumulated_times	No	Integer	accumulated_times

Response Parameters

Status code: 200

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.

Table 4-429 Response body parameters

Parameter	Type	Description
alert_count	Integer	Number of alarms. Alert count.
severity	String	Severity. The options are as follows - Tips - Low - Medium - High - Critical Severity.

Status code: 400

Table 4-430 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"
}
```

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 4-431 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. Project ID.
workspace_id	Yes	String	Workspace ID. Workspace ID.

Request Parameters

Table 4-432 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.

Response Parameters

Status code: 200

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.

Table 4-434 Response body parameters

Parameter	Type	Description
category	String	Indicator type and number of groups. Metric category. GROUP_COUNT.
metric	Map<String,Number>	Indicator value. Metric value.

Status code: 400

Table 4-435 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
  }
}
```

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 4-436 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. Project ID.
workspace_id	Yes	String	Workspace ID. Workspace ID.

Request Parameters

Table 4-437 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.

Table 4-438 Request body parameters

Parameter	Mandatory	Type	Description
[items]	Yes	Array of strings	EnableAlertRuleRequestBody

Response Parameters

Status code: 200

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.

Table 4-440 Response body parameters

Parameter	Type	Description
fail_list	Array of AlertRule objects	Alert rule ID.

Parameter	Type	Description
success_list	Array of AlertRule objects	Alert rule ID.

Table 4-441 AlertRule

Parameter	Type	Description
rule_id	String	Alert rule ID.
pipe_id	String	Pipeline ID.Pipe ID.
pipe_name	String	Data pipeline name.Pipe name.
create_by	String	Created by. Created by.
create_time	Long	Creation time. Create time.
update_by	String	Updated by. Update by.
update_time	Long	Update time. Update time.
delete_time	Long	The deletion time. Delete time.
rule_name	String	Alert rule name.
query	String	Query.
query_type	String	SQL query syntax. Query type. SQL.
status	String	Status. The options are as follows - Enabled - Disabled
severity	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.
custom_properties	Map<String,String >	Custom extension information. Custom properties.
event_grouping	Boolean	Alert group. Alert group.
schedule	Schedule object	Schedule Rule.
triggers	Array of AlertRuleTrigger objects	Alert triggering rules. Alert triggers.

Table 4-442 Schedule

Parameter	Type	Description
frequency_interval	Integer	Scheduling interval. Frequency interval.

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.
period_interval	Integer	Time window interval. Period interval.
period_unit	String	Time Window unit. The value can be minute, hour, or day. Period unit. MINUTE, HOUR, DAY.
delay_interval	Integer	The delay interval. Delay interval
overtime_interval	Integer	Timeout interval. Overtime interval

Table 4-443 AlertRuleTrigger

Parameter	Type	Description
mode	String	Number of modes. Mode. 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.
expression	String	expression
severity	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.
accumulated_time s	Integer	accumulated_times

Status code: 400

Table 4-444 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

```
{  
  "fail_list" : [],  
  "success_list" : []  
}
```

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 4-445 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. Project ID.
workspace_id	Yes	String	Workspace ID. Workspace ID.

Request Parameters

Table 4-446 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.

Table 4-447 Request body parameters

Parameter	Mandatory	Type	Description
[items]	Yes	Array of strings	DisableAlertRuleRequestBody

Response Parameters

Status code: 200

Table 4-448 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 4-449 Response body parameters

Parameter	Type	Description
fail_list	Array of AlertRule objects	Alert rule ID.
success_list	Array of AlertRule objects	Alert rule ID.

Table 4-450 AlertRule

Parameter	Type	Description
rule_id	String	Alert rule ID.
pipe_id	String	Pipeline ID.Pipe ID.
pipe_name	String	Data pipeline name.Pipe name.
create_by	String	Created by. Created by.
create_time	Long	Creation time. Create time.
update_by	String	Updated by. Update by.
update_time	Long	Update time. Update time.
delete_time	Long	The deletion time. Delete time.
rule_name	String	Alert rule name.
query	String	Query.
query_type	String	SQL query syntax. Query type. SQL.
status	String	Status. The options are as follows - Enabled - Disabled
severity	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.
custom_properties	Map<String,String >	Custom extension information. Custom properties.
event_grouping	Boolean	Alert group. Alert group.
schedule	Schedule object	Schedule Rule.
triggers	Array of AlertRuleTrigger objects	Alert triggering rules. Alert triggers.

Table 4-451 Schedule

Parameter	Type	Description
frequency_interval	Integer	Scheduling interval. Frequency interval.
frequency_unit	String	The unit of the scheduling interval. The value can be minute, hour, or day. Frequency unit. MINUTE, HOUR, DAY.
period_interval	Integer	Time window interval. Period interval.

Parameter	Type	Description
period_unit	String	Time Window unit. The value can be minute, hour, or day. Period unit. MINUTE, HOUR, DAY.
delay_interval	Integer	The delay interval. Delay interval
overtime_interval	Integer	Timeout interval. Overtime interval

Table 4-452 AlertRuleTrigger

Parameter	Type	Description
mode	String	Number of modes. Mode. 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.
expression	String	expression
severity	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.
accumulated_time s	Integer	accumulated_times

Status code: 400

Table 4-453 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

```
{
  "fail_list" : [ ],
  "success_list" : [ ]
}
```

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 4-454 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. Project ID.
workspace_id	Yes	String	Workspace ID. Workspace ID.

Table 4-455 Query Parameters

Parameter	Mandatory	Type	Description
offset	Yes	Long	The query offset. Offset.
limit	Yes	Long	Number of bucket groups Limit.
sort_key	No	String	Sorting field. Sort key

Parameter	Mandatory	Type	Description
sort_dir	No	String	Sort direction, asc or desc.
severity	No	Array of strings	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.

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.

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
count	Long	Total number. Total count.
records	Array of AlertRuleTemplate objects	Alert rule template. Alert rule templates.

Table 4-459 AlertRuleTemplate

Parameter	Type	Description
template_id	String	Alert rule template ID. Alert rule template ID.
update_time	Long	Update time.Update time.
template_name	String	Alert rule template ID. Alert rule template ID.
data_source	String	Data source. Data source.
version	String	Version. Version
query	String	Query.
query_type	String	SQL query syntax, SQL. Query type. SQL.
severity	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.
custom_properties	Map<String,String >	Custom extension information. Custom properties.
event_grouping	Boolean	Alert group. Alert group.
schedule	Schedule object	Schedule Rule.
triggers	Array of AlertRuleTrigger objects	Alert triggering rules. Alert triggers.

Table 4-460 Schedule

Parameter	Type	Description
frequency_interval	Integer	Scheduling interval. Frequency interval.
frequency_unit	String	The unit of the scheduling interval. The value can be minute, hour, or day. Frequency unit. MINUTE, HOUR, DAY.
period_interval	Integer	Time window interval. Period interval.
period_unit	String	Time Window unit. The value can be minute, hour, or day. Period unit. MINUTE, HOUR, DAY.
delay_interval	Integer	The delay interval. Delay interval
overtime_interval	Integer	Timeout interval. Overtime interval

Table 4-461 AlertRuleTrigger

Parameter	Type	Description
mode	String	Number of modes. Mode. 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.
expression	String	expression
severity	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.
accumulated_time s	Integer	accumulated_time s

Status code: 400

Table 4-462 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"
} ]
} ]
}

```

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 4-463 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. Project ID.
workspace_id	Yes	String	Workspace ID. Workspace ID.
template_id	Yes	String	Alert rule template ID. Alert rule template ID.

Request Parameters

Table 4-464 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.

Response Parameters

Status code: 200

Table 4-465 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 4-466 Response body parameters

Parameter	Type	Description
template_id	String	Alert rule template ID. Alert rule template ID.
update_time	Long	Update time.Update time.
template_name	String	Alert rule template ID. Alert rule template ID.
data_source	String	Data source. Data source.
version	String	Version. Version
query	String	Query.
query_type	String	SQL query syntax, SQL. Query type. SQL.
severity	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.
custom_properties	Map<String,String >	Custom extension information. Custom properties.

Parameter	Type	Description
event_grouping	Boolean	Alert group. Alert group.
schedule	Schedule object	Schedule Rule.
triggers	Array of AlertRuleTrigger objects	Alert triggering rules. Alert triggers.

Table 4-467 Schedule

Parameter	Type	Description
frequency_interval	Integer	Scheduling interval. Frequency interval.
frequency_unit	String	The unit of the scheduling interval. The value can be minute, hour, or day. Frequency unit. MINUTE, HOUR, DAY.
period_interval	Integer	Time window interval. Period interval.
period_unit	String	Time Window unit. The value can be minute, hour, or day. Period unit. MINUTE, HOUR, DAY.
delay_interval	Integer	The delay interval. Delay interval
overtime_interval	Integer	Timeout interval. Overtime interval

Table 4-468 AlertRuleTrigger

Parameter	Type	Description
mode	String	Number of modes. Mode. 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.
expression	String	expression
severity	String	Severity. The options are as follows - Tips - Low - Medium - High - FATAL.
accumulated_times	Integer	accumulated_times

Status code: 400

Table 4-469 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"
  } ]
}
```

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 4-470 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
version_id	Yes	String	Playbook version ID.

Request Parameters

Table 4-471 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.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-472 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	Name.

Response Parameters

Status code: 200

Table 4-473 Response header parameters

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

Table 4-474 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error message
data	PlaybookVersionInfo object	Playbook review details.

Table 4-475 PlaybookVersionInfo

Parameter	Type	Description
id	String	Playbook version ID.
description	String	Description.
create_time	String	Creation time.
update_time	String	Update time.
project_id	String	Project ID.
creator_id	String	Creator ID.
modifier_id	String	ID of the user who updated the information.
playbook_id	String	Playbook ID.
version	String	Version No.

Parameter	Type	Description
enabled	Boolean	Whether to enable the function. - true -- Enabled. - false -- Disabled
status	String	Playbook version status. Options - Editing, APPROVING, UNPASSED, and PUBLISHED
action_strategy	String	Execution policy. Currently, only asynchronous concurrent execution is supported. The corresponding value is ASYNC.
actions	Array of ActionInfo objects	Workflows associated with the playbook.
rule_enable	Boolean	Whether to enable the trigger condition filter.
rules	RuleInfo object	Playbook triggering specifications information.
dataclass_id	String	Data class ID.
trigger_type	String	How the playbook is triggered. The options are as follows - EVENT -- event; TIMER -- scheduled.)
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)
rule_id	String	Filtering rule ID.
dataclass_name	String	Data class name.
approve_name	String	Reviewer.

Table 4-476 ActionInfo

Parameter	Type	Description
id	String	Playbook workflow ID.
name	String	Workflow name.

Parameter	Type	Description
description	String	Description.
action_type	String	Workflow type.
action_id	String	Workflow ID.
playbook_id	String	Playbook ID.
playbook_version_id	String	Playbook version ID.
project_id	String	Project ID.

Table 4-477 RuleInfo

Parameter	Type	Description
id	String	Rule ID.
project_id	String	Project ID.
rule	String	Trigger rule.

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
message	String	Error Description

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"
  }
}
```

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 4-480 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
playbook_id	Yes	String	Playbook ID.

Table 4-481 Query Parameters

Parameter	Mandatory	Type	Description
status	No	String	Playbook version status. Options are Editing, APPROVING, UNPASSED, and PUBLISHED
enabled	No	Integer	enabled/disabled
version_type	No	Integer	Version type. The options are as follows 0 is draft version; 1 is official version.
offset	No	Integer	Indicates the page number. Start position of the query result. The value starts from 0.
limit	No	Integer	The maximum number of records can be returned on each page for a pagination query. The value starts from 1.

Request Parameters

Table 4-482 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.
content-type	Yes	String	application/ json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-483 Response header parameters

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

Table 4-484 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
size	Integer	Records on each page.
page	Integer	Current page.
total	Integer	Total
data	Array of PlaybookVersion-ListEntity objects	Playbook version list.

Table 4-485 PlaybookVersionListEntity

Parameter	Type	Description
id	String	Playbook version ID.
description	String	Description.
create_time	String	Creation time.
update_time	String	Update time.
project_id	String	Project ID.
creator_id	String	Creator ID.
modifier_id	String	ID of the user who updated the information.
playbook_id	String	Playbook ID.
version	String	Version No.
enabled	Boolean	Activated
status	String	Status. (EDITING -- editing, APPROVING -- reviewing, UNPASSED -- not approved, Published -- approved)
action_strategy	String	Execution policy. Currently, only asynchronous concurrent execution is supported. The corresponding value is ASYNC.
rule_enable	Boolean	Whether the filtering rule is enabled.
dataclass_id	String	Data class ID.
trigger_type	String	Triggering mode. The options are as follows - EVENT -- event; TIMER -- scheduled.
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
rule_id	String	Filtering rule ID.
dataclass_name	String	Data class name.
approve_name	String	Reviewer.

Status code: 400

Table 4-486 Response header parameters

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

Table 4-487 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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"  
  } ]  
}
```

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 4-488 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
playbook_id	Yes	String	Playbook ID.

Request Parameters

Table 4-489 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.
content-type	Yes	String	application/ json;charset=UTF-8

Table 4-490 Request body parameters

Parameter	Mandatory	Type	Description
description	No	String	Description.
workspace_id	No	String	Workspace ID
playbook_id	No	String	Playbook ID.
actions	No	Array of ActionInfo objects	Associated workflows.
dataclass_id	No	String	Data class ID.
rule_enable	No	Boolean	Whether the filtering rule is enabled.
rule_id	No	String	Filtering rule ID.
trigger_type	No	String	Triggering mode. The options are as follows -- EVENT -- event; TIMER -- scheduled.
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.

Table 4-491 ActionInfo

Parameter	Mandatory	Type	Description
id	No	String	Playbook workflow ID.
name	No	String	Workflow name.
description	No	String	Description.
action_type	No	String	Workflow type.
action_id	No	String	Workflow ID.
playbook_id	No	String	Playbook ID.
playbook_version_id	No	String	Playbook version ID.
project_id	No	String	Project ID.

Response Parameters

Status code: 200

Table 4-492 Response header parameters

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

Table 4-493 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error message
data	PlaybookVersionInfo object	Playbook review details.

Table 4-494 PlaybookVersionInfo

Parameter	Type	Description
id	String	Playbook version ID.
description	String	Description.

Parameter	Type	Description
create_time	String	Creation time.
update_time	String	Update time.
project_id	String	Project ID.
creator_id	String	Creator ID.
modifier_id	String	ID of the user who updated the information.
playbook_id	String	Playbook ID.
version	String	Version No.
enabled	Boolean	Whether to enable the function. - true -- Enabled. - false -- Disabled
status	String	Playbook version status. Options - Editing, APPROVING, UNPASSED, and PUBLISHED
action_strategy	String	Execution policy. Currently, only asynchronous concurrent execution is supported. The corresponding value is ASYNC.
actions	Array of ActionInfo objects	Workflows associated with the playbook.
rule_enable	Boolean	Whether to enable the trigger condition filter.
rules	RuleInfo object	Playbook triggering specifications information.
dataclass_id	String	Data class ID.
trigger_type	String	How the playbook is triggered. The options are as follows - EVENT -- event; TIMER -- scheduled.)
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)
rule_id	String	Filtering rule ID.

Parameter	Type	Description
dataclass_name	String	Data class name.
approve_name	String	Reviewer.

Table 4-495 ActionInfo

Parameter	Type	Description
id	String	Playbook workflow ID.
name	String	Workflow name.
description	String	Description.
action_type	String	Workflow type.
action_id	String	Workflow ID.
playbook_id	String	Playbook ID.
playbook_version_id	String	Playbook version ID.
project_id	String	Project ID.

Table 4-496 RuleInfo

Parameter	Type	Description
id	String	Rule ID.
project_id	String	Project ID.
rule	String	Trigger rule.

Status code: 400

Table 4-497 Response header parameters

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

Table 4-498 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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"
}
}

```

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 4-499 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
version_id	Yes	String	Playbook version ID.

Request Parameters

Table 4-500 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.
content-type	Yes	String	application/ json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-501 Response header parameters

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

Table 4-502 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error message
data	PlaybookVersionInfo object	Playbook review details.

Table 4-503 PlaybookVersionInfo

Parameter	Type	Description
id	String	Playbook version ID.
description	String	Description.
create_time	String	Creation time.
update_time	String	Update time.
project_id	String	Project ID.
creator_id	String	Creator ID.
modifier_id	String	ID of the user who updated the information.
playbook_id	String	Playbook ID.
version	String	Version No.
enabled	Boolean	Whether to enable the function. - true -- Enabled. - false -- Disabled
status	String	Playbook version status. Options - Editing, APPROVING, UNPASSED, and PUBLISHED
action_strategy	String	Execution policy. Currently, only asynchronous concurrent execution is supported. The corresponding value is ASYNC.
actions	Array of ActionInfo objects	Workflows associated with the playbook.
rule_enable	Boolean	Whether to enable the trigger condition filter.
rules	RuleInfo object	Playbook triggering specifications information.
dataclass_id	String	Data class ID.
trigger_type	String	How the playbook is triggered. The options are as follows - EVENT -- event; TIMER -- scheduled.)
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)
rule_id	String	Filtering rule ID.
dataclass_name	String	Data class name.
approve_name	String	Reviewer.

Table 4-504 ActionInfo

Parameter	Type	Description
id	String	Playbook workflow ID.
name	String	Workflow name.
description	String	Description.
action_type	String	Workflow type.
action_id	String	Workflow ID.
playbook_id	String	Playbook ID.
playbook_version_id	String	Playbook version ID.
project_id	String	Project ID.

Table 4-505 RuleInfo

Parameter	Type	Description
id	String	Rule ID.
project_id	String	Project ID.
rule	String	Trigger rule.

Status code: 400

Table 4-506 Response header parameters

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

Table 4-507 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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"
  }
}
```

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 4-508 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
version_id	Yes	String	Playbook version ID.

Request Parameters

Table 4-509 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.
content-type	Yes	String	application/ json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-510 Response header parameters

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

Table 4-511 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Response message.

Status code: 400

Table 4-512 Response header parameters

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

Table 4-513 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

Example Requests

None

Example Responses

Status code: 200

Response when the request is successful.

```
{  
  "code" : 0,  
  "message" : "Error message"  
}
```

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 4-514 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
version_id	Yes	String	Playbook version ID.

Request Parameters

Table 4-515 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.
content-type	Yes	String	application/ json;charset=UTF-8

Table 4-516 Request body parameters

Parameter	Mandatory	Type	Description
description	No	String	Description.
workspace_id	No	String	Workspace ID
playbook_id	No	String	Playbook ID.
dataclass_id	No	String	Data class ID.
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)
rule_id	No	String	Rule ID.

Parameter	Mandatory	Type	Description
trigger_type	No	String	Triggering mode. The options are as follows - EVENT -- event; TIMER -- scheduled.
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.

Response Parameters

Status code: 200

Table 4-517 Response header parameters

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

Table 4-518 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error message
data	PlaybookVersionInfo object	Playbook review details.

Table 4-519 PlaybookVersionInfo

Parameter	Type	Description
id	String	Playbook version ID.
description	String	Description.

Parameter	Type	Description
create_time	String	Creation time.
update_time	String	Update time.
project_id	String	Project ID.
creator_id	String	Creator ID.
modifier_id	String	ID of the user who updated the information.
playbook_id	String	Playbook ID.
version	String	Version No.
enabled	Boolean	Whether to enable the function. - true -- Enabled. - false -- Disabled
status	String	Playbook version status. Options - Editing, APPROVING, UNPASSED, and PUBLISHED
action_strategy	String	Execution policy. Currently, only asynchronous concurrent execution is supported. The corresponding value is ASYNC.
actions	Array of ActionInfo objects	Workflows associated with the playbook.
rule_enable	Boolean	Whether to enable the trigger condition filter.
rules	RuleInfo object	Playbook triggering specifications information.
dataclass_id	String	Data class ID.
trigger_type	String	How the playbook is triggered. The options are as follows - EVENT -- event; TIMER -- scheduled.)
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)
rule_id	String	Filtering rule ID.

Parameter	Type	Description
dataclass_name	String	Data class name.
approve_name	String	Reviewer.

Table 4-520 ActionInfo

Parameter	Type	Description
id	String	Playbook workflow ID.
name	String	Workflow name.
description	String	Description.
action_type	String	Workflow type.
action_id	String	Workflow ID.
playbook_id	String	Playbook ID.
playbook_version_id	String	Playbook version ID.
project_id	String	Project ID.

Table 4-521 RuleInfo

Parameter	Type	Description
id	String	Rule ID.
project_id	String	Project ID.
rule	String	Trigger rule.

Status code: 400

Table 4-522 Response header parameters

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

Table 4-523 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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"
}

```

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 4-524 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Parameter	Mandatory	Type	Description
workspace_id	Yes	String	Workspace ID
version_id	Yes	String	version Id value
rule_id	Yes	String	version Id value

Request Parameters

Table 4-525 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.
content-type	Yes	String	application/ json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-526 Response header parameters

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

Table 4-527 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
data	RuleInfo object	Playbook triggering specifications information.

Table 4-528 RuleInfo

Parameter	Type	Description
id	String	Rule ID.
project_id	String	Project ID.
rule	String	Trigger rule.

Status code: 400

Table 4-529 Response header parameters

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

Table 4-530 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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"
  }
}
```

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 4-531 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
version_id	Yes	String	Playbook version ID.
rule_id	Yes	String	Rule ID.

Request Parameters

Table 4-532 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.
content-type	Yes	String	application/ json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-533 Response header parameters

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

Table 4-534 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Response message.

Status code: 400

Table 4-535 Response header parameters

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

Table 4-536 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

Example Requests

None

Example Responses

Status code: 200

Response when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message"
}
```

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 4-537 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
version_id	Yes	String	Playbook version ID.

Request Parameters

Table 4-538 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.
content-type	Yes	String	application/ json;charset=UTF-8

Table 4-539 Request body parameters

Parameter	Mandatory	Type	Description
rule	Yes	ConditionInfo object	Details of playbook triggering rules

Table 4-540 ConditionInfo

Parameter	Mandatory	Type	Description
expression_type	No	String	Expression type. This parameter is mandatory for incident-triggered playbooks. The default value is common.
conditions	No	Array of ConditionInfo objects	Triggering conditions. This parameter is mandatory for incident-triggered playbooks.

Parameter	Mandatory	Type	Description
logics	No	Array of strings	Conditional logic combinations. This parameter is mandatory for incident-triggered playbooks.
cron	No	String	Cron expression (scheduled tasks). This parameter is mandatory for scheduled playbooks.
schedule_type	No	String	Scheduled task repetition type. The value can be second, hour, day, or week. This parameter is mandatory for scheduled playbooks.
start_type	No	String	Playbook execution type. The value can be IMMEDIATELY or CUSTOM. This parameter is mandatory for scheduled playbooks.
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.
end_time	No	String	End time of a scheduled task. This parameter is mandatory for scheduled playbooks.
repeat_range	No	String	Execution time range, for example, 2021-01-30T23:00:00Z+0800. This parameter is mandatory for scheduled playbooks.
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.

Table 4-541 ConditionItem

Parameter	Mandatory	Type	Description
name	No	String	Condition name.
detail	No	String	Condition details.
data	No	Array of strings	Condition expression data.

Response Parameters

Status code: 200

Table 4-542 Response header parameters

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

Table 4-543 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
data	RuleInfo object	Playbook triggering specifications information.

Table 4-544 RuleInfo

Parameter	Type	Description
id	String	Rule ID.
project_id	String	Project ID.
rule	String	Trigger rule.

Status code: 400

Table 4-545 Response header parameters

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

Table 4-546 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

Example Requests

create a playbook rule named condition_0 and supporting all expression types.

```
{
  "rule" : {
    "expression_type" : "common",
    "conditions" : [ {
      "name" : "condition_0",
      "detail" : "Open",
      "data" : [ "handle_status, ==, Open" ]
    } ],
    "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\"]}"
  }
}
```

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 4-547 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
version_id	Yes	String	Playbook version ID.
rule_id	Yes	String	Playbook rule ID.

Request Parameters

Table 4-548 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.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-549 Request body parameters

Parameter	Mandatory	Type	Description
rule	No	ConditionInfo object	Details of playbook triggering rules

Table 4-550 ConditionInfo

Parameter	Mandatory	Type	Description
expression_type	No	String	Expression type. This parameter is mandatory for incident-triggered playbooks. The default value is common.
conditions	No	Array of ConditionItem objects	Triggering conditions. This parameter is mandatory for incident-triggered playbooks.
logics	No	Array of strings	Conditional logic combinations. This parameter is mandatory for incident-triggered playbooks.
cron	No	String	Cron expression (scheduled tasks). This parameter is mandatory for scheduled playbooks.
schedule_type	No	String	Scheduled task repetition type. The value can be second, hour, day, or week. This parameter is mandatory for scheduled playbooks.
start_type	No	String	Playbook execution type. The value can be IMMEDIATELY or CUSTOM. This parameter is mandatory for scheduled playbooks.
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.
end_time	No	String	End time of a scheduled task. This parameter is mandatory for scheduled playbooks.

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.
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.

Table 4-551 ConditionItem

Parameter	Mandatory	Type	Description
name	No	String	Condition name.
detail	No	String	Condition details.
data	No	Array of strings	Condition expression data.

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
code	String	Error code
message	String	Error Message

Parameter	Type	Description
data	RuleInfo object	Playbook triggering specifications information.

Table 4-554 RuleInfo

Parameter	Type	Description
id	String	Rule ID.
project_id	String	Project ID.
rule	String	Trigger rule.

Status code: 400

Table 4-555 Response header parameters

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

Table 4-556 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

Example Requests

Update a playbook rule named condition_0 and supporting all expression types.

```
{
  "rule": {
    "expression_type": "common",
    "conditions": [ {
      "name": "condition_0",
      "detail": "Open",
      "data": [ "handle_status, ==, Open" ]
    } ],
    "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"
  }
}
```

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 4-557 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID

Table 4-558 Query Parameters

Parameter	Mandatory	Type	Description
status	No	String	Playbook instance status. (RUNNING--Running, FINISHED--Successful, Failed--Failed, Retrying--Retrying, Terminated--Terminated)
name	No	String	Instance name.
playbook_name	No	String	Playbook name.
dataclass_name	No	String	Data class name.
dataobject_name	No	String	Data object name.
trigger_type	No	String	Triggering type. TIMER indicates scheduled triggering, and EVENT indicates event triggering.
from_date	No	String	Start time.
to_date	No	String	Query end time
limit	Yes	Integer	The maximum number of records can be returned on each page for a pagination query. The value starts from 1.
offset	Yes	Integer	Indicates the page number. Start position of the query result. The value starts from 0.

Request Parameters

Table 4-559 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.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-560 Response header parameters

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

Table 4-561 Response body parameters

Parameter	Type	Description
count	Integer	Total
instances	Array of PlaybookInstanceInfo objects	Playbook instance list information.

Table 4-562 PlaybookInstanceInfo

Parameter	Type	Description
id	String	Playbook instance ID.
name	String	Playbook instance name.
project_id	String	Project ID.
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)
trigger_type	String	Triggering type. TIMER indicates scheduled triggering, and EVENT indicates event triggering.
start_time	String	Creation time.

Parameter	Type	Description
end_time	String	Update time.

Table 4-563 PlaybookInfoRef

Parameter	Type	Description
id	String	Playbook ID.
version_id	String	Playbook version ID.
name	String	Name.
version	String	Version.

Table 4-564 DataclassInfoRef

Parameter	Type	Description
id	String	Data class ID.
name	String	Data class name.

Table 4-565 DataobjectInfo

Parameter	Type	Description
id	String	ID
create_time	String	Creation time.
update_time	String	Update time.
project_id	String	Project ID.
dataclass_id	String	Data class ID.
name	String	Name.
content	String	Data content.

Status code: 400

Table 4-566 Response header parameters

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

Table 4-567 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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"
  } ]
}
```

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 4-568 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
instance_id	Yes	String	instance_id

Request Parameters

Table 4-569 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.
content-type	Yes	String	application/ json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-570 Response header parameters

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

Table 4-571 Response body parameters

Parameter	Type	Description
id	String	Playbook instance ID.
name	String	Playbook instance name.
project_id	String	Project ID.
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)

Parameter	Type	Description
trigger_type	String	Triggering type. TIMER indicates scheduled triggering, and EVENT indicates event triggering.
start_time	String	Creation time.
end_time	String	Update time.

Table 4-572 PlaybookInfoRef

Parameter	Type	Description
id	String	Playbook ID.
version_id	String	Playbook version ID.
name	String	Name.
version	String	Version.

Table 4-573 DataclassInfoRef

Parameter	Type	Description
id	String	Data class ID.
name	String	Data class name.

Table 4-574 DataobjectInfo

Parameter	Type	Description
id	String	ID
create_time	String	Creation time.
update_time	String	Update time.
project_id	String	Project ID.
dataclass_id	String	Data class ID.
name	String	Name.
content	String	Data content.

Status code: 400

Table 4-575 Response header parameters

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

Table 4-576 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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"
}
```

Status Codes

Status Code	Description
200	Instance Informations

Status Code	Description
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 4-577 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
instance_id	Yes	String	Playbook instance ID.

Request Parameters

Table 4-578 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.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-579 Request body parameters

Parameter	Mandatory	Type	Description
operation	No	String	Operation type Retry Retry termination -- TERMINATE

Response Parameters

Status code: 200

Table 4-580 Response header parameters

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

Table 4-581 Response body parameters

Parameter	Type	Description
id	String	Playbook instance ID.
name	String	Playbook instance name.
project_id	String	Project ID.
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)
trigger_type	String	Triggering type. TIMER indicates scheduled triggering, and EVENT indicates event triggering.
start_time	String	Creation time.
end_time	String	Update time.

Table 4-582 PlaybookInfoRef

Parameter	Type	Description
id	String	Playbook ID.
version_id	String	Playbook version ID.
name	String	Name.
version	String	Version.

Table 4-583 DataclassInfoRef

Parameter	Type	Description
id	String	Data class ID.
name	String	Data class name.

Table 4-584 DataobjectInfo

Parameter	Type	Description
id	String	ID
create_time	String	Creation time.
update_time	String	Update time.
project_id	String	Project ID.
dataclass_id	String	Data class ID.
name	String	Name.
content	String	Data content.

Status code: 400

Table 4-585 Response header parameters

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

Table 4-586 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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"
}
```

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 4-587 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
instance_id	Yes	String	Playbook instance ID.

Request Parameters

Table 4-588 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.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-589 Response header parameters

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

Table 4-590 Response body parameters

Parameter	Type	Description
count	Integer	Total
action_instances	Array of ActionInstanceInfo objects	Incident instance list.

Table 4-591 ActionInstanceInfo

Parameter	Type	Description
action	ActionInfo object	Playbook workflows.
instance_log	AuditLogInfo object	Playbook instance review information.

Table 4-592 ActionInfo

Parameter	Type	Description
id	String	Playbook workflow ID.
name	String	Workflow name.
description	String	Description.
action_type	String	Workflow type.
action_id	String	Workflow ID.
playbook_id	String	Playbook ID.
playbook_version_id	String	Playbook version ID.
project_id	String	Project ID.

Table 4-593 AuditLogInfo

Parameter	Type	Description
instance_type	String	Instance type (AOP_WORKFLOW for workflows, SCRIPT for scripts, and PLAYBOOK for playbooks).
action_id	String	Workflow ID.
action_name	String	Workflow name.
instance_id	String	Instance ID.
parent_instance_id	String	Instance ID of the parent node.
log_level	String	Log Level
input	String	Input.
output	String	Output.
error_msg	String	Error Message
start_time	String	Start time.
end_time	String	End time.
status	String	Status. (RUNNING, FINISHED, FAILED, RETRYING, and TERMINATED)
trigger_type	String	Triggering type. TIMER indicates scheduled triggering, and EVENT indicates event triggering.

Status code: 400

Table 4-594 Response header parameters

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

Table 4-595 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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"
    }
  }
} ] }
```

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 4-596 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID

Table 4-597 Query Parameters

Parameter	Mandatory	Type	Description
offset	Yes	Long	offset
limit	Yes	Long	limit
sort_key	No	String	sort_key
sort_dir	No	String	sort_dir. asc, desc

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.
content-type	Yes	String	application/ json;charset=UTF-8

Table 4-599 Request body parameters

Parameter	Mandatory	Type	Description
instance_type	No	String	Instance type (AOP_WORKFLOW for workflows, SCRIPT for scripts, and PLAYBOOK for playbooks).
action_id	No	String	Workflow ID.
action_name	No	String	Workflow name.
instance_id	No	String	Instance ID.
parent_instance_id	No	String	Instance ID of the parent node.
log_level	No	String	Log Level
input	No	String	Input.
output	No	String	Output.
error_msg	No	String	Error Message
start_time	No	String	Start time.
end_time	No	String	End time.
status	No	String	Status. (RUNNING, FINISHED, FAILED, RETRYING, and TERMINATED)
trigger_type	No	String	Triggering type. TIMER indicates scheduled triggering, and EVENT indicates event triggering.

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
count	Integer	Total records.
audit_logs	Array of AuditLogInfo objects	Review response list.

Table 4-602 AuditLogInfo

Parameter	Type	Description
instance_type	String	Instance type (AOP_WORKFLOW for workflows, SCRIPT for scripts, and PLAYBOOK for playbooks).
action_id	String	Workflow ID.
action_name	String	Workflow name.
instance_id	String	Instance ID.
parent_instance_id	String	Instance ID of the parent node.
log_level	String	Log Level
input	String	Input.
output	String	Output.
error_msg	String	Error Message
start_time	String	Start time.
end_time	String	End time.
status	String	Status. (RUNNING, FINISHED, FAILED, RETRYING, and TERMINATED)
trigger_type	String	Triggering type. TIMER indicates scheduled triggering, and EVENT indicates event triggering.

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
message	String	Error Description

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"
  }
]
```

```
}]
}
```

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 4-605 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
version_id	Yes	String	Version ID

Request Parameters

Table 4-606 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.
content-type	Yes	String	application/ json;charset=UTF-8

Table 4-607 Request body parameters

Parameter	Mandatory	Type	Description
result	No	String	PASS or UN_PASS
content	No	String	Review Comments

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
message	String	Response message.
data	ApproveOpinionDetail object	Review details.

Table 4-610 ApproveOpinionDetail

Parameter	Type	Description
result	String	Review result.
content	String	Review content.

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
message	String	Error Description

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"
  }
}
```

Status Codes

Status Code	Description
200	Response when the request is successful.
400	Response when the request failed.

Error Codes

See [Error Codes](#).

4.9.2 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 4-613 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID

Table 4-614 Query Parameters

Parameter	Mandatory	Type	Description
resource_id	No	String	Resource ID.
approve_type	No	String	Review type. (PLAYBOOK or AOP_WORKFLOW)

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.
content-type	Yes	String	application/ json;charset=UTF-8

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
message	String	Response message.
data	Array of ApproveOpinionDetail objects	Playbook review details.

Table 4-618 ApproveOpinionDetail

Parameter	Type	Description
result	String	Review result.
content	String	Review content.

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
message	String	Error Description

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"
  } ]
}
```

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 4-621 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
version_id	Yes	String	Playbook version ID.

Table 4-622 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.
offset	Yes	Integer	Indicates the page number. Start position of the query result. The value starts from 0.

Request Parameters

Table 4-623 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.
content-type	Yes	String	application/ json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-624 Response header parameters

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

Table 4-625 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
total	Integer	Total
size	Integer	Number of records displayed on each page.
page	Integer	Current page number.
data	Array of ActionInfo objects	Playbook workflow list.

Table 4-626 ActionInfo

Parameter	Type	Description
id	String	Playbook workflow ID.
name	String	Workflow name.
description	String	Description.
action_type	String	Workflow type.
action_id	String	Workflow ID.
playbook_id	String	Playbook ID.
playbook_version_id	String	Playbook version ID.
project_id	String	Project ID.

Status code: 400

Table 4-627 Response header parameters

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

Table 4-628 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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"
} ]
}
```

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 4-629 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
version_id	Yes	String	Playbook version ID.

Request Parameters

Table 4-630 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.
content-type	Yes	String	application/ json;charset=UTF-8

Table 4-631 Request body parameters

Parameter	Mandatory	Type	Description
[items]	Yes	Array of CreateAction objects	Create actions

Table 4-632 CreateAction

Parameter	Mandatory	Type	Description
name	No	String	Name.
description	No	String	Description.
action_type	Yes	String	Type. The default value is AOP_WORKFLOW.
action_id	Yes	String	Playbook workflow ID.
sort_order	No	String	Sort By

Response Parameters

Status code: 200

Table 4-633 Response header parameters

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

Table 4-634 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error message
data	Array of ActionInfo objects	list of informations of playbook action

Table 4-635 ActionInfo

Parameter	Type	Description
id	String	Playbook workflow ID.
name	String	Workflow name.
description	String	Description.
action_type	String	Workflow type.
action_id	String	Workflow ID.
playbook_id	String	Playbook ID.
playbook_version_id	String	Playbook version ID.
project_id	String	Project ID.

Status code: 400

Table 4-636 Response header parameters

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

Table 4-637 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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"  
  } ]  
}
```

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 4-638 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
version_id	Yes	String	Playbook version ID.
action_id	Yes	String	Playbook workflow ID.

Request Parameters

Table 4-639 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.
content-type	Yes	String	application/ json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-640 Response header parameters

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

Table 4-641 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Response message.

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
message	String	Error Description

Example Requests

None

Example Responses

Status code: 200

Response parameters when the request is successful.

```
{
  "code" : 0,
  "message" : "Error message"
}
```

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 4-644 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
version_id	Yes	String	Playbook version ID.
action_id	Yes	String	Playbook workflow ID.

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.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-646 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	Name.
description	No	String	Description.
action_type	No	String	Type. The default value is AOP_WORKFLOW.
action_id	No	String	Playbook workflow ID.
sort_order	No	String	Sort By

Response Parameters

Status code: 200

Table 4-647 Response header parameters

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

Table 4-648 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error message
data	ActionInfo object	Playbook workflows.

Table 4-649 ActionInfo

Parameter	Type	Description
id	String	Playbook workflow ID.
name	String	Workflow name.
description	String	Description.
action_type	String	Workflow type.
action_id	String	Workflow ID.
playbook_id	String	Playbook ID.

Parameter	Type	Description
playbook_version_id	String	Playbook version ID.
project_id	String	Project ID.

Status code: 400

Table 4-650 Response header parameters

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

Table 4-651 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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"
}
}
```

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 4-652 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
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".

Parameter	Mandatory	Type	Description
data_object_id	Yes	String	ID of the associated data object.
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".

Request Parameters

Table 4-653 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.
content-type	Yes	String	Content type.

Table 4-654 Request body parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page.
offset	No	Integer	Offset
sort_by	No	String	Sorting field -- create_time update_time
order	No	String	Sort by -- DESC ASC
from_date	No	String	Search start time, for example, 2023-02-20T00:00:00.000Z
to_date	No	String	Search end time, for example, 2023-02-27T23:59:59.999Z
condition	No	condition object	Search condition expression.

Table 4-655 condition

Parameter	Mandatory	Type	Description
conditions	No	Array of conditions objects	Expression list.
logics	No	Array of strings	Expression logic.

Table 4-656 conditions

Parameter	Mandatory	Type	Description
name	No	String	Expression name.
data	No	Array of strings	Expression content list.

Response Parameters

Status code: 200

Table 4-657 Response header parameters

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

Table 4-658 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error Message
total	Integer	Total number of alerts.
limit	Integer	Number of records displayed on each page.
offset	Integer	Offset
success	Boolean	Successful or not.
data	Array of DataObjectDetail objects	Alert list.

Table 4-659 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.
data_object	DataObject object	Alert entity information.
dataclass_ref	dataclass_ref object	Data class object.
format_version	Integer	Format version.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
project_id	String	ID of the current project.
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.
version	Integer	Version.
workspace_id	String	ID of the current workspace.

Table 4-660 DataObject

Parameter	Type	Description
version	String	Version of the data source of the alert. The value must be one officially released by the Cloud SSA service.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	String	ID of the account (domain_id) to whom the data is delivered and hosted.

Parameter	Type	Description
region_id	String	ID of the region where the account to whom the data is delivered and hosted belongs to.
workspace_id	String	ID of the current workspace.
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.
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.
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.
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.
title	String	Alert title.
description	String	Alert description.
source_url	String	Alert URL, which points to the page of the current incident description in the data source product.
count	Integer	Incident occurrences

Parameter	Type	Description
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%.
severity	String	Severity level. Value range: Tips Low Medium High Fatal Description: <ul style="list-style-type: none"> • 0: TIPS: No threats are found. • 1: LOW: No actions are required for the threat. • 2: MEDIUM: The threat needs to be handled but is not urgent. • 3: HIGH: The threat must be handled preferentially. • 4: FATAL: The threat must be handled immediately to prevent further damage.
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.
alert_type	alert_type object	Alert classification. For details, see the Alert Type Definition.
network_list	Array of network_list objects	Network Information
resource_list	Array of resource_list objects	Affected resources.
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: <ul style="list-style-type: none"> - Unknown - True_Positive - False_Positive Enter Unknown by default.
handle_status	String	Incident handling status. The options are as follows: <ul style="list-style-type: none"> • Open: enabled. • Block: blocked. • Closed: closed. The default value is Open.
sla	Integer	Risk close time -- Set the acceptable risk duration. Unit -- Hour
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.
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.
ipdrr_phase	String	Period/Handling phase No. Preparation Detection and Analysis Containment, Eradication & Recovery Post-Incident-Activity
simulation	String	Debugging field.
actor	String	Alert investigator.
owner	String	Owner and service owner.
creator	String	Creator

Parameter	Type	Description
close_reason	String	Close reason. <ul style="list-style-type: none"> • False detection. • Resolved • Repeated • Other
close_comment	String	Whether to close comment.
malware	malware object	Malware
system_info	Object	System information.
process	Array of process objects	Process information.
user_info	Array of user_info objects	User Details
file_info	Array of file_info objects	File Information

Table 4-661 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Tenant ID.
region_id	String	Region ID. global is returned for global services.
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.
project_id	String	Project ID. The default value is null for global services.

Table 4-662 datasource

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows-- 1- cloud product 2- Third-party product 3- Tenant product

Parameter	Type	Description
domain_id	String	Account ID to which the data source product belongs.
project_id	String	ID of the project to which the data source product belongs.
region_id	String	Region where the data source is located, for example, cn-north1. For details about the value range, see <i>Regions and Endpoints</i> .
company_name	String	Name of the company to which a data source belongs.
product_name	String	Name of the data source.
product_feature	String	Name of the feature of the product that detects the incident.
product_module	String	Threat detection module list.

Table 4-663 alert_type

Parameter	Type	Description
category	String	Type
alert_type	String	Alert type.

Table 4-664 network_list

Parameter	Type	Description
direction	String	Direction. The value can be IN or 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 .
src_ip	String	Source IP address
src_port	Integer	Source port. The value ranges from 0 to 65535.
src_domain	String	Source domain name.

Parameter	Type	Description
src_geo	src_geo object	Geographical location of the source IP address.
dest_ip	String	Destination IP address
dest_port	String	Destination port. The value ranges from 0 to 65535.
dest_domain	String	Destination domain name
dest_geo	dest_geo object	Geographical location of the destination IP address.

Table 4-665 src_geo

Parameter	Type	Description
latitude	Number	Latitude
longitude	Number	Longitude
city_code	String	City code. For example, Beijing or Shanghai.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-666 dest_geo

Parameter	Type	Description
latitude	Number	Latitude
longitude	Number	Longitude
city_code	String	City code. For example, Beijing or Shanghai.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN US DE IT SG.

Table 4-667 resource_list

Parameter	Type	Description
id	String	Cloud service resource ID.

Parameter	Type	Description
name	String	Resource name.
type	String	Resource type. This parameter references the value of RMS type on Cloud.
provider	String	Cloud service name, which is the same as the provider field in the RMS service.
region_id	String	Region ID in Cloud, for example, cn-north-1.
domain_id	String	ID of the account to which the resource belongs, in UUID format.
project_id	String	ID of the account to which the resource belongs, in UUID format.
ep_id	String	Specifies the enterprise project ID.
ep_name	String	Enterprise Project Name
tags	String	Resource tag. <ol style="list-style-type: none"> 1. A maximum of 50 key/value pairs are supported. 2. Value: a maximum of 255 characters, including letters, digits, spaces, and +, -, =, ., _ ;, /, @

Table 4-668 remediation

Parameter	Type	Description
recommendation	String	Recommended solution.
url	String	Link to the general fix information for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-669 malware

Parameter	Type	Description
malware_family	String	Malicious family.
malware_class	String	Malware category.

Table 4-670 process

Parameter	Type	Description
process_name	String	Process name.
process_path	String	Process execution file path.
process_pid	Integer	Process ID.
process_uid	Integer	Process user ID.
process_cmdline	String	Process command line.
process_parent_name	String	Parent process name.
process_parent_path	String	Parent process execution file path.
process_parent_pid	Integer	Parent process ID.
process_parent_uid	Integer	Parent process user ID.
process_parent_cmdline	String	Parent process command line.
process_child_name	String	Subprocess name.
process_child_path	String	Subprocess execution file path.
process_child_pid	Integer	Subprocess ID.
process_child_uid	Integer	Subprocess user ID.
process_child_cmdline	String	Subprocess command line
process_launched_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.
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.

Table 4-671 user_info

Parameter	Type	Description
user_id	String	User UID
user_name	String	Username

Table 4-672 file_info

Parameter	Type	Description
file_path	String	File path/name.
file_content	String	File path/name.
file_new_path	String	New file path/name.
file_hash	String	File Hash
file_md5	String	File MD5
file_sha256	String	File SHA256
file_attr	String	File attribute.

Table 4-673 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.
name	String	Data class name.

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
message	String	Error Description

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
}
```

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 4-676 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
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".
data_object_id	Yes	String	ID of the associated data object.
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".

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.
content-type	Yes	String	Content type.

Table 4-678 Request body parameters

Parameter	Mandatory	Type	Description
ids	No	Array of strings	ID list of associated data objects.

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
message	String	Error Message
request_id	String	Request ID.
total	Integer	Total number of alerts.
limit	Integer	Number of records displayed on each page.
offset	Integer	Offset
success	Boolean	Successful or not.
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
success_ids	Array of strings	IDs of alerts transferred to incidents.

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
message	String	Error Description

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

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 4-684 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
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".
data_object_id	Yes	String	ID of the associated data object.
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".

Request Parameters

Table 4-685 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.

Parameter	Mandatory	Type	Description
content-type	Yes	String	Content type.

Table 4-686 Request body parameters

Parameter	Mandatory	Type	Description
ids	No	Array of strings	ID list of associated data objects.

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
code	String	Error code
message	String	Error Message
data	BatchOperateDataobjectResult object	Returned object for batch operation on alerts.

Table 4-689 BatchOperateDataobjectResult

Parameter	Type	Description
error_ids	Array of strings	IDs of alerts not transferred to incidents
success_ids	Array of strings	IDs of alerts transferred to incidents.

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
message	String	Error Description

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" ]
  }
}
```

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 4-692 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID

Table 4-693 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Offset
limit	No	Integer	Data volume
name	No	String	Name
business_code	No	String	Code
description	No	String	Description.
is_built_in	No	Boolean	Built-in or Not

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.
content-type	Yes	String	Content type.

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
dataclass_details	Array of DataClassResponseBody objects	Data class details.
total	Number	Total data volume

Table 4-697 DataClassResponseBody

Parameter	Type	Description
id	String	Data class ID.
create_time	String	Creation time.
update_time	String	Update time.
creator_id	String	Creator ID.
creator_name	String	Creator username

Parameter	Type	Description
modifier_id	String	ID of the user who updated the information.
modifier_name	String	Creator username
cloud_pack_version	String	Subscribed version.
region_id	String	Region ID
project_id	String	Tenant ID.
workspace_id	String	Workspace ID
domain_id	String	domain id
name	String	Data class name.
business_code	String	Service code for the data class.
description	String	Description of the data class.
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.
type_num	Number	Quantity of sub-type data classes.

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
message	String	Error Description

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
  } ]
}
```

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 4-700 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID
dataclass_id	Yes	String	Data class ID.

Table 4-701 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Offset
limit	No	Integer	Data volume
name	No	String	Name
is_built_in	No	Boolean	Built-in or Not
field_category	No	String	Field types.
mapping	No	Boolean	Whether to display in other places other the classification and mapping module.

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.
content-type	Yes	String	Content type.

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
field_details	Array of FieldResponseBody objects	list of informations of field
total	Number	Total data volume

Table 4-705 FieldResponseBody

Parameter	Type	Description
id	String	Id value
cloud_pack_version	String	Subscribed version.
business_id	String	ID of associated service.
business_type	String	Associated service.
dataclass_name	String	Data class name.
business_code	String	Service code for the field.
field_key	String	Key
name	String	Field name.
description	String	Field description.
default_value	String	Default value.
display_type	String	Display type.
field_type	String	Field type, such as short text, radio, and grid.
extra_json	String	Additional JSON.
field_tooltip	String	Tool tip.

Parameter	Type	Description
iu_type	String	Input and output types.
used_by	String	Services.
json_schema	String	JSON mode.
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.
target_api	String	Target API.
creator_id	String	Creator id value
creator_name	String	Creator name value
modifier_id	String	Modifier id value
modifier_name	String	Modifier name value
create_time	String	Create time
update_time	String	Update time

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
message	String	Error Description

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"
} ]
}

```

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 4-708 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID

Table 4-709 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Offset
limit	No	Integer	Data volume
order	No	String	Sorting sequence, including asc for ascending order and desc for descending order.
sortby	No	String	Sorting fields, including create_time for creation time and category for classification name.
enabled	No	Boolean	Whether to enable.
last_version	No	Boolean	Latest version.
name	No	String	Workflow name.
description	No	String	Description
dataclass_id	No	String	Data class ID.
dataclass_name	No	String	Data class name.
aop_type	No	String	Process Type

Request Parameters

Table 4-710 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.
content-type	Yes	String	Content type.

Response Parameters

Status code: 200

Table 4-711 Response header parameters

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

Table 4-712 Response body parameters

Parameter	Type	Description
code	String	Return code.
total	Integer	Total records.
offset	Integer	Current page size.
limit	Integer	Current page.
message	String	Request ID
success	Boolean	Successful or not.
data	Array of AopWorkflowInfo objects	Workflow list.

Table 4-713 AopWorkflowInfo

Parameter	Type	Description
id	String	Workflow ID.
name	String	Workflow name.
description	String	Description.
project_id	String	Tenant ID.
owner_id	String	Owner ID.
creator_id	String	Creator ID.
edit_role	String	Edit
use_role	String	User role.
approve_role	String	Reviewer.
enabled	Boolean	Enabled or not
workspace_id	String	Workspace ID
version_id	String	Workflow version ID.

Parameter	Type	Description
current_approval_version_id	String	Version to be viewed currently.
current_rejected_versions_id	String	Version that has been rejected currently.
aop_type	String	AOP types. - NORMAL : General - SURVEY : Investigation - HEMOSTASIS : Prevention - EASE : Mitigation
engine_type	String	There are two types of engine, shared and dedicated.
dataclass_id	String	ID of the data class.

Status code: 400

Table 4-714 Response header parameters

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

Table 4-715 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

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_version_id": "v1",
    "aop_type": "Mitigation (ease).",
    "engine_type": "public_engine",
    "dataclass_id": "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  } ]
}
```

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 4-716 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID

Request Parameters

Table 4-717 Request body parameters

Parameter	Mandatory	Type	Description
dataspace_name	Yes	String	Data space name
description	Yes	String	Description.

Response Parameters

Status code: 200

Table 4-718 Response body parameters

Parameter	Type	Description
domain_id	String	Account ID.
region_id	String	region ID
project_id	String	Project ID.
dataspace_id	String	Workspace ID
dataspace_name	String	Workspace Name
dataspace_type	String	Data space type. The value can be system-defined or user-defined.
description	String	Description.
create_by	String	Created By
create_time	Long	Created
update_by	String	Updated by
update_time	Long	Update time.

Example Requests

```
{  
  "dataspace_name": "dataspace-01",  
  "description": "test dataspace"  
}
```

Example Responses

Status code: 200

Request successful.

```
{  
  "domain_id": "0531ed520xxxxxxebdb6e57xxxxxxx",  
  "region_id": "cn-north-1",  
  "project_id": "2b31ed520xxxxxxebdb6e57xxxxxxx",  
  "dataspace_id": "a00106ba-bede-453c-8488-b60c70bd6aed",  
  "dataspace_name": "dataspace-01",  
  "dataspace_type": "system-defined",  
  "description": "test dataspace",  
  "create_by": "0642ed520xxxxxxebdb6e57xxxxxxx",  
  "create_time": 1584883694354,  
  "update_by": "0642ed520xxxxxxebdb6e57xxxxxxx",  
  "update_time": 1584883694354  
}
```

Status Codes

Status Code	Description
200	Request successful.

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 4-719 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID

Request Parameters

Table 4-720 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.

Table 4-721 Request body parameters

Parameter	Mandatory	Type	Description
dataspace_id	Yes	String	Workspace ID
pipe_name	Yes	String	Data pipeline name.
description	No	String	Description.
storage_period	Yes	Integer	Data storage duration, in days. The default value is 30. The value ranges from 1 to 3600.
shards	Yes	Integer	Number of pipeline partitions. One partition is created by default. A maximum of 64 partitions can be created.
timestamp_field	No	String	Timestamp field.
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 4-722 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).
is_chinese_exist	No	Boolean	Whether Chinese characters are contained.
properties	No	Map<String,KeyIndex>	Nested structure.

Response Parameters

Status code: 200

Table 4-723 Response body parameters

Parameter	Type	Description
domain_id	String	Account ID.
project_id	String	Project ID.
dataspace_id	String	Data space ID
dataspace_name	String	Data space name
pipe_id	String	Indicates the pipe ID.
pipe_name	String	Pipeline Name
pipe_type	String	Pipeline type. System-defined Preset types. User-defined Custom types.
description	String	Description.
storage_period	Integer	Index storage period by the day.
shards	Integer	Index shard quantity.
create_by	String	Created By
create_time	Integer	Creation time
update_by	String	Updated by
update_time	Integer	Update time.

Status code: 400

Table 4-724 Response body parameters

Parameter	Type	Description
error_msg	String	Invalid request message.
error_code	String	Error code

Status code: 401

Table 4-725 Response body parameters

Parameter	Type	Description
error_msg	String	Permissions error.
error_code	String	Error code

Status code: 403

Table 4-726 Response body parameters

Parameter	Type	Description
-	String	

Status code: 500

Table 4-727 Response body parameters

Parameter	Type	Description
error_msg	String	Internal system error.
error_code	String	Error code

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"
}
}
```

Example Responses

Status code: 200

Created pipeline returned.

```
{
  "domain_id" : "0531ed520xxxxxebedb6e57xxxxxxx",
  "project_id" : "2b31ed520xxxxxebedb6e57xxxxxxx",
  "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" : "0642ed520xxxxxebedb6e57xxxxxxx",
  "create_time" : 1584883694354,
  "update_by" : "0642ed520xxxxxebedb6e57xxxxxxx",
  "update_time" : 1584883694354
}
```

Status Codes

Status Code	Description
200	Created pipeline returned.
400	Request error.
401	Authentication failed.
403	Access denied.
500	Internal system error.

Error Codes

See [Error Codes](#).

4.16 Workspace Management

4.16.1 Creating a Workspace

Function

Before using the baseline check, alarm management, security analysis, and security orchestration functions of the SecMaster, you need to create a workspace.

The workspace can divide resources into different working scenarios to avoid inconvenience in searching for resources.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v1/{project_id}/workspaces

Table 4-728 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-729 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 the user token.
content-type	Yes	String	application/ json;charset=UTF-8

Table 4-730 Request body parameters

Parameter	Mandatory	Type	Description
region_id	Yes	String	Region ID.
enterprise_project_id	No	String	Enterprise project ID.
enterprise_project_name	No	String	Enterprise project name.
view_bind_id	No	String	Space ID bound to the view.
is_view	No	Boolean	Indicates whether the view is used.
name	Yes	String	Workspace name.

Parameter	Mandatory	Type	Description
description	No	String	Workspace description
project_name	Yes	String	Project name.
tags	No	Array of TagsPojo objects	You can tag resources under your account for classification. TMS provides you with a visualized table to manage resource tags, including editing tags in batches.

Table 4-731 TagsPojo

Parameter	Mandatory	Type	Description
key	No	String	Tag key.
value	No	String	Tag value.

Response Parameters

Status code: 200

Table 4-732 Response body parameters

Parameter	Type	Description
id	String	Workspace ID.
create_time	String	Creation time.
update_time	String	Update time.
name	String	Workspace name.
description	String	Workspace description.
creator_id	String	Creator ID.
creator_name	String	Creator name.
modifier_id	String	Modifier ID.
modifier_name	String	Modifier name.
project_id	String	Project ID.
project_name	String	Project name.
domain_id	String	Tenant ID.
domain_name	String	Tenant name.

Parameter	Type	Description
enterprise_project_id	String	Enterprise project ID.
enterprise_project_name	String	Enterprise project name.
is_view	Boolean	Indicates whether the view is used.
region_id	String	Region ID.
view_bind_id	String	Space ID bound to the view.
view_bind_name	String	Space name bound to the view.
workspace_agency_list	Array of workspace_agency_list objects	This parameter is used only in the view scenario. The spaces managed by the view are listed.

Table 4-733 workspace_agency_list

Parameter	Type	Description
project_id	String	ID of the project to which the agency space belongs.
id	String	Space agency ID.
name	String	Space agency name.
region_id	String	ID of the region to which the agency space belongs
workspace_attribution	String	THIS_ACCOUNT: current account space; CROSS_ACCOUNT: cross-account space
agency_version	String	IAM agency version used when a user creates a hosting space. The value can be V3 or V5.
domain_id	String	ID of the tenant agency.
domain_name	String	Name of the tenant agency.
iam_agency_id	String	IAM agency ID.
iam_agency_name	String	IAM agency name.
resource_spec_code	Array of strings	The purchased version of agency space
selected	Boolean	Indicates whether a view is selected.

Status code: 400

Table 4-734 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Status code: 500

Table 4-735 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Request body for creating a workspace

```
{
  "name": "My Workspace",
  "region_id": "cn-north-4",
  "project_name": "cn-north-4",
  "enterprise_project_id": "",
  "enterprise_project_name": "",
  "tags": [ {
    "key": "tag1",
    "value": "value1"
  } ],
  "description": "My workspace"
}
```

Example Responses

Status code: 200

Request successful.

```
{
  "create_time": "2024-07-02T09:25:17Z+0800",
  "creator_id": "b4*****46a",
  "creator_name": "l00644738",
  "description": "My workspace",
  "domain_id": "ac*****bf4",
  "domain_name": "scc****09",
  "enterprise_project_id": "",
  "enterprise_project_name": "",
  "id": "39*****bf",
  "is_view": false,
  "modifier_id": "",
  "modifier_name": "",
  "name": "My Workspace",
  "project_id": "15*****da6",
}
```

```

"project_name" : "cn-north-4",
"region_id" : "cn-north-4",
"update_time" : "2024-07-02T09:25:17Z+0800",
"view_bind_id" : "",
"view_bind_name" : "",
"workspace_agency_list" : [ ]
}

```

Status Codes

Status Code	Description
200	Request successful.
400	Invalid request parameter.
500	Request failed.

Error Codes

See [Error Codes](#).

4.16.2 Querying the Workspace List

Function

This API is used to query workspace list. You can filter tenants' workspaces by workspace name, workspace description, and creation time.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v1/{project_id}/workspaces

Table 4-736 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 4-737 Query Parameters

Parameter	Mandatory	Type	Description
offset	Yes	Number	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.
limit	Yes	Number	Number of records displayed on each page
region_id	No	String	Region ID
name	No	String	This API is used to query the name.
description	No	String	Search by description
view_bind_id	No	String	Space ID bound to the view
view_bind_name	No	String	Space name bound to the view
create_time_start	No	String	Creation start time, for example, 2024-04-26T16:08:09Z+0800.
create_time_end	No	String	Creation end time, for example, 2024-04-2T16:08:09Z+0800.
is_view	No	Boolean	Indicates whether to query the view. The value can be true or false.
ids	No	String	Workspace ID array, which is separated by commas (,).
normal_project_id	No	String	General project ID.
enterprise_project_id	No	String	Enterprise project ID.

Request Parameters

Table 4-738 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 the user token.
content-type	Yes	String	application/ json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-739 Response body parameters

Parameter	Type	Description
workspaces	Array of CreateWorkspaceResponseBody objects	list of informations of workspaces
count	Number	Total data volume

Table 4-740 CreateWorkspaceResponseBody

Parameter	Type	Description
id	String	Workspace ID.
create_time	String	Creation time.
update_time	String	Update time.
name	String	Workspace name.
description	String	Workspace description.
creator_id	String	Creator ID.
creator_name	String	Creator name.
modifier_id	String	Modifier ID.
modifier_name	String	Modifier name.

Parameter	Type	Description
project_id	String	Project ID.
project_name	String	Project name.
domain_id	String	Tenant ID.
domain_name	String	Tenant name.
enterprise_project_id	String	Enterprise project ID.
enterprise_project_name	String	Enterprise project name.
is_view	Boolean	Indicates whether the view is used.
region_id	String	Region ID.
view_bind_id	String	Space ID bound to the view.
view_bind_name	String	Space name bound to the view.
workspace_agency_list	Array of workspace_agency_list objects	This parameter is used only in the view scenario. The spaces managed by the view are listed.

Table 4-741 workspace_agency_list

Parameter	Type	Description
project_id	String	ID of the project to which the agency space belongs.
id	String	Space agency ID.
name	String	Space agency name.
region_id	String	ID of the region to which the agency space belongs
workspace_attribution	String	THIS_ACCOUNT: current account space; CROSS_ACCOUNT: cross-account space
agency_version	String	IAM agency version used when a user creates a hosting space. The value can be V3 or V5.
domain_id	String	ID of the tenant agency.
domain_name	String	Name of the tenant agency.
iam_agency_id	String	IAM agency ID.
iam_agency_name	String	IAM agency name.

Parameter	Type	Description
resource_spec_code	Array of strings	The purchased version of agency space
selected	Boolean	Indicates whether a view is selected.

Status code: 400

Table 4-742 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Status code: 500

Table 4-743 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Request successful.

```
{
  "count" : 1,
  "workspaces" : [ {
    "create_time" : "2024-07-02T09:25:17Z+0800",
    "creator_id" : "b4*****46a",
    "creator_name" : "l00644738",
    "description" : "My workspace",
    "domain_id" : "ac*****bf4",
    "domain_name" : "scc****09",
    "enterprise_project_id" : "",
    "enterprise_project_name" : "",
    "id" : "39*****bf",
    "is_view" : false,
    "modifier_id" : "",
    "modifier_name" : "",
    "name" : "My Workspace",
```

```
"project_id" : "15*****da6",  
"project_name" : "cn-north-4",  
"region_id" : "cn-north-4",  
"update_time" : "2024-07-02T09:25:17Z+0800",  
"view_bind_id" : "",  
"view_bind_name" : "",  
"workspace_agency_list" : [ ]  
}]  
}
```

Status Codes

Status Code	Description
200	Request successful.
400	Invalid request parameter.
500	Request failed.

Error Codes

See [Error Codes](#).

4.17 Metering and Billing

4.17.1 On-Demand Subscription of SecMaster

Function

Enable the on-demand SecMaster.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v1/{project_id}/subscriptions/orders

Table 4-744 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant project ID.

Request Parameters

Table 4-745 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 the user token.
X-Language	Yes	String	Current language environment zh-cn or en-us.

Table 4-746 Request body parameters

Parameter	Mandatory	Type	Description
region_id	Yes	String	Region ID, for example, cn-north-4.
domain_id	Yes	String	domainId
tag_list	No	Array of TagInfo objects	Charging tag.
product_list	No	Array of ProductPostPaid objects	Product list.
operate_type	No	String	Specifies the operation type. The value can be create or addition.

Table 4-747 TagInfo

Parameter	Mandatory	Type	Description
key	Yes	String	Identifier. The value is a string of 2 to 36 characters consisting of only letters, digits, underscores (_), and hyphens (-).

Parameter	Mandatory	Type	Description
value	Yes	String	Content. The value is a string of 2 to 36 characters consisting of only letters, digits, underscores (_), and hyphens (-).

Table 4-748 ProductPostPaid

Parameter	Mandatory	Type	Description
id	Yes	String	Specifies the identifier, which must be unique in each price query and is used for identifying the mappings between requests and responses.
product_id	Yes	String	Offering ID, which is obtained from the CBC price inquiry.
cloud_service_type	Yes	String	Cloud service type. The fixed value is hws.service.type.sa.
resource_type	Yes	String	Specifies the resource type of the purchased product. For example, the resource type for typical scenarios in SecMaster is hws.resource.type.secmaster.typical.
resource_spec_code	Yes	String	Specifies the resource specifications of the purchased product. For example, the resource specification for the basic edition in SecMaster is secmaster.basic.

Parameter	Mandatory	Type	Description
usage_measurement_id	Yes	Integer	Specifies the usage measurement unit. This parameter is mandatory for a pay-per-use task. For example, the resources are billed by hour, the usage value is 1, and the usage measurement unit is hour. The options are: 4: Hours 10: GB. The bandwidth usage is measured by traffic (GB). 11: MB. The bandwidth usage is measured by traffic (MB).
usage_value	Yes	Number	Specifies the usage value. This parameter is mandatory for a pay-per-use task. For example, the resources are billed by hour, the usage value is 1, and the usage measurement unit is hour.
resource_size	Yes	Integer	Specifies the number of quotas.
usage_factor	Yes	String	Specifies the usage factor. This parameter is mandatory for a pay-per-use task. The value is the same as the usage factor of SDRs. The mappings between cloud services and usage factors are as follows: Typical configuration: Duration Situation management: duration Security orchestration: count Intelligent analysis: flow
resource_id	No	String	Resource ID, which is transferred only when the quota is added.

Response Parameters

None

Example Requests

```
https://{endpoint}/v1/{projectId}/subscriptions/orders
```

```
{
  "domain_id" : "abcdef8a41164a2280ec65f1f4c4mlnyz",
  "region_id" : "cn-north-4",
  "product_list" : [ {
    "product_id" : "OFFI908269345109094402",
    "cloud_service_type" : "hws.service.type.sa",
    "id" : "E52E1A22-9408-459A-9F67-7B5C11B1E71A",
    "resource_spec_code" : "secmaster.professional",
    "resource_type" : "hws.resource.type.secmaster.typical",
    "usage_factor" : "duration",
    "usage_value" : 1,
    "usage_measure_id" : 4,
    "resource_size" : 1
  } ]
}
```

Example Responses

Status code: 400

Parameter error.

```
{
  "error_msg" : "You already have [standard edition] package. To use more, upgrade the SecMaster edition you are using or increase the quota.",
  "error_code" : "SecMaster.00010201"
}
```

Status Codes

Status Code	Description
200	Request successful.
400	Parameter error.
403	Insufficient permissions.

Error Codes

See [Error Codes](#).

4.18 Metric Query

4.18.1 Querying Metrics in Batches

Function

This API is used to query metrics in batches.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v1/{project_id}/workspaces/{workspace_id}/sa/metrics/hits

Table 4-749 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Table 4-750 Query Parameters

Parameter	Mandatory	Type	Description
timespan	No	String	The time range for querying metrics. The format is ISO8601, for example, 2007-03-01T13:00:00Z/2008-05-11T15:30:00Z, 2007-03-01T13:00:00Z/P1Y2M10DT2H30M, or P1Y2M10DT2H30M/2008-05-11T15:30:00Z.
cache	No	Boolean	Indicates whether to enable the cache. The default value is true. The value false indicates that the cache is disabled.

Request Parameters

Table 4-751 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.

Table 4-752 Request body parameters

Parameter	Mandatory	Type	Description
metric_ids	Yes	Array of strings	Specifies the metric ID list to be queried. For details about how to obtain the existing metrics, see the related information in the appendix.
workspace_ids	No	Array of strings	Workspace list. This API is mandatory when the metric supports obtaining data of multiple workspaces.
params	No	Array of Map<String,String> objects	Indicates the parameter list of the metric to be queried. Each element in the list is in K-V format of <String, String>. The number of elements must be the same as that of the metric_ids list. For details, see the appendix.
interactive_params	No	Array of Map<String,String> objects	For query the interactive parameters, if the metric supports interactive parameters, enter a parameter list in the K-V format of <String, String>. For details, see the appendix.
field_ids	No	Array of strings	Metric card ID list

Response Parameters

Status code: 200

Table 4-753 Response body parameters

Parameter	Type	Description
[items]	Array of ShowMetricResultResponseBody objects	

Table 4-754 ShowMetricResultResponseBody

Parameter	Type	Description
metric_id	String	Metric ID
result	result object	Metric query result.
metric_format	Array of MetricFormat objects	Metric format. The value is fixed based on different metrics.
log_msg	String	Result log information
status	String	Query result status. The options are as follows: SUCCESS: The query is successful. FAILED: The query fails. FALLBACK: The default value is used.

Table 4-755 result

Parameter	Type	Description
labels	Array of strings	Title of the metric query result table
datarows	Array<Array<Object>>	Metric query result table.
effective_column	String	Effective columns. If this parameter exists, the specified column is used as the metric data result.

Table 4-756 MetricFormat

Parameter	Type	Description
data	String	Data format
display	String	Display format
display_param	Map<String,String>	Display parameter
data_param	Map<String,String>	Data parameters

Example Requests

Query the alarm severity distribution from June 25 to the current time through the metric API.

```
https://{endpoint}/v1/{project_id}/workspaces/{workspace_id}/sa/metrics/hits
```

```
{  
  "metric_ids": [ "1f0f5e29-5a92-17a5-2c16-5f37c6dc109c" ],  
  "params": [ {  
    "start_date": "2024-06-25T00:00:00.000+08:00"  
  } ]  
}
```

Example Responses

Status code: 200

Request successful.

```
[ {  
  "metric_id": "1f0f5e29-5a92-17a5-2c16-5f37c6dc109c",  
  "result": {  
    "labels": [ "label1" ],  
    "datarows": [ [ { } ] ],  
    "effective_column": "0:1"  
  },  
  "status": "SUCCESS"  
} ]
```

Status Codes

Status Code	Description
200	Request successful.

Error Codes

See [Error Codes](#).

4.19 Baseline Inspection

4.19.1 Search Baseline Check Results

Function

This API is used to search baseline check results.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/workspaces/{workspace_id}/sa/baseline/search

Table 4-757 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-758 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token.
X-Language	Yes	String	Language. The values are zh-CN and en-US.
content-type	Yes	String	Content type.

Table 4-759 Request body parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Page size.
offset	No	Integer	Offset. The records after this offset will be queried.
sort_by	No	String	Sorting keyword.
order	No	String	Descending or ascending order, the value is DESC or ESC.
from_date	No	String	Start time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Parameter	Mandatory	Type	Description
to_date	No	String	End time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
condition	No	Object	Search condition expression.

Response Parameters

Status code: 200

Table 4-760 Response body parameters

Parameter	Type	Description
code	String	Error code
total	Integer	Total number of queried records.
size	Integer	Page size.
page	Integer	Offset.
success	Boolean	Successful or not.
data	Array of strings	List of searching result.

Status code: 400

Table 4-761 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

Status code: 401

Table 4-762 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

Status code: 500

Table 4-763 Response body parameters

Parameter	Type	Description
code	String	Error Code
message	String	Error Description

Example Requests

Query the request example of baseline check results. The time ranges from June 20, 2024 to June 27, 2024. The compliance package ID is 6add7d71-2261-4195-bab7-8ada0f0ed4d2. The directory ID is 0b78937f-4d9b-4223-9a46-2361e5090be0. The resource type is iam_user. The results are sorted in descending order of the update time. Each page contains 10 records.

```
{
  "limit" : 10,
  "offset" : 0,
  "sort_by" : "last_observed_time",
  "order" : "DESC",
  "from_date" : "2024-06-20T00:00:00.000Z",
  "to_date" : "2024-06-27T23:59:59.999Z",
  "condition" : {
    "conditions" : [ {
      "name" : "compliance_package_id",
      "data" : [ "compliance_package_id", "=", "6add7d71-2261-4195-bab7-8ada0f0ed4d2" ]
    }, {
      "name" : "catalog_id",
      "data" : [ "catalog_id", "=", "0b78937f-4d9b-4223-9a46-2361e5090be0" ]
    }, {
      "name" : "resource.type",
      "data" : [ "resource.type", "=", "iam_user" ]
    } ],
    "logics" : [ "compliance_package_id", "AND", "catalog_id", "AND", "resource.type" ]
  }
}
```

Example Responses

Status code: 200

Request successful.

```
{
  "code" : "00000000",
  "data" : [ {
    "create_time" : "2024-01-03T01:16:21.666+08:00",
```

```

"data_object" : {
  "arrive_time" : "2024-01-03T11:28:03.993Z+0800",
  "baseline_type" : {
    "baseline_type" : "Compliance Check",
    "baseline_type_en" : "Compliance Check",
    "baseline_type_zh" : "Compliance Check",
    "category" : "",
    "category_en" : "",
    "category_zh" : "",
    "id" : "23f48a58cXXX162846076cd0"
  },
  "catalog_id" : "9378d1e8-XXX-4aae-XXX-c41cf6829ede",
  "checkitem_id" : "13fcc967-cb49-XXX-811a-9f72ce6ce8ac",
  "compliance_package_id" : "39488f96-XXX-4cc6-XXX-ad3c29b3a6c2",
  "create_time" : "2024-01-02T17:16:21.666Z+0800",
  "data_source" : {
    "company_name" : "XXX",
    "domain_id" : "ac7438b990efXXXb45e8bf4",
    "product_feature" : "SA",
    "product_module" : "Base-line",
    "product_name" : "SecMaster",
    "project_id" : "15645222e8XXX93dab6341da6",
    "region_id" : "cn-north-7",
    "source_type" : 1
  },
  "dataclass_id" : "f846c8e0-XXX-XXX-bcbf-f77190847f08",
  "domain_id" : "ac7438b990eXXX1004eb45e8bf4",
  "domain_name" : "ac7438b99XXX1004eb45e8bf4",
  "end_time" : "2024-01-03T11:28:51.564Z+0800",
  "execitem_id" : "ca2a1361-5738-479c-8c40-d078e775a23a",
  "execitem_version" : 1,
  "first_observed_time" : "2024-01-03T11:28:50.955Z+0800",
  "handle_status" : "qualified",
  "id" : "39c56d70a9c2492XXXd91934cb5cb_13fcc967-XXX-494b-XXX-9f72ce6ce8ac",
  "is_deleted" : false,
  "last_observed_time" : "2024-01-03T11:28:51.564Z+0800",
  "method" : 1,
  "origin_id" : "",
  "project_id" : "15645222e874XXX93dab6341da6",
  "region_id" : "cn-north-7",
  "region_name" : "cn-north-7",
  "resource" : {
    "domain_id" : "ac7438b990eXXX04eb45e8bf4",
    "id" : "39c56d70a9cXXX1934cb5cb",
    "name" : "adfasd",
    "project_id" : "15645222XXXc93dab6341da6",
    "provider" : "XXX",
    "region_id" : "cn-north-7",
    "type" : "agency"
  },
  "severity" : "informational",
  "start_time" : "2024-01-03T11:28:50.955Z+0800",
  "task_id" : "10da8403-XXX-442d-XXX-fa2fdf42a3a1",
  "title" : "Agency Permissions for Project Services",
  "trigger_flag" : false,
  "update_time" : "2024-01-03T11:28:51.887Z+0800",
  "workspace_id" : "1350a050-XXX-45e2-XXX-9cbfef116de7"
},
"dataclass_ref" : {
  "id" : "f846c8e0-XXX-3767-XXX-f77190847f08"
},
"format_version" : 0,
"id" : "39c56d7XXX278fXXX934cb5cb_13fcc967-cb49-XXX-811a-9f72ce6ce8ac",
"update_time" : "2024-01-03T19:28:51.887+08:00",
"version" : 0
}, {
  "create_time" : "2024-01-03T01:16:21.821+08:00",
  "data_object" : {
    "arrive_time" : "2024-01-03T11:28:03.993Z+0800",

```

```

"baseline_type": {
  "baseline_type": "Compliance check",
  "baseline_type_en": "Compliance Check",
  "baseline_type_zh": "Compliance check",
  "category": "",
  "category_en": "",
  "category_zh": "",
  "id": "23f48a58c5b2fXXX162846076cd0"
},
"catalog_id": "9378d1e8-XXX-4aae-XXX-c41cf6829ede",
"checkitem_id": "13fcc967-cb49-XXX-811a-9f72ce6ce8ac",
"compliance_package_id": "39488f96-XXX-4cc6-XXX-ad3c29b3a6c2",
"create_time": "2024-01-02T17:16:21.821Z+0800",
"data_source": {
  "company_name": "XXX",
  "domain_id": "ac7438b990efXXX004eb45e8bf4",
  "product_feature": "SA",
  "product_module": "Base-line",
  "product_name": "SecMaster",
  "project_id": "15645222XXX5c93dab6341da6",
  "region_id": "cn-north-7",
  "source_type": 1
},
"dataclass_id": "f846c8e0-XXX-3767-bcbf-f77190847f08",
"domain_id": "ac7438b990eXXXb741004eb45e8bf4",
"domain_name": "ac7438bXXX37b741004eb45e8bf4",
"end_time": "2024-01-03T11:28:51.701Z+0800",
"execitem_id": "ca2a1361-XXX-479c-XXX-d078e775a23a",
"execitem_version": 1,
"first_observed_time": "2024-01-03T11:28:51.565Z+0800",
"handle_status": "qualified",
"id": "f295575ab57XXX977d9be93ca9fe_13fcc967-XXX-494b-XXX-9f72ce6ce8ac",
"is_deleted": false,
"last_observed_time": "2024-01-03T11:28:51.701Z+0800",
"method": 1,
"origin_id": "",
"project_id": "15645222e8XXXa985c93dab6341da6",
"region_id": "cn-north-7",
"region_name": "cn-north-7",
"resource": {
  "domain_id": "ac7438b99XXX1004eb45e8bf4",
  "id": "f295575ab57bXXXd9be93ca9fe",
  "name": "apigw_admin_trust_secmaster",
  "project_id": "15645222e8XXX93dab6341da6",
  "provider": "XXX",
  "region_id": "cn-north-7",
  "type": "agency"
},
"severity": "informational",
"start_time": "2024-01-03T11:28:51.565Z+0800",
"task_id": "10da8403-4955XXXd-a974-faXXX2a3a1",
"title": "Agency Permissions for Project Services",
"trigger_flag": false,
"update_time": "2024-01-03T11:28:52.023Z+0800",
"workspace_id": "1350a050-d09a-4XXX-9503-9cbfef116de7"
},
"dataclass_ref": {
  "id": "f846c8e0-cf0e-XXX-bcbf-XXX7f08"
},
"format_version": 0,
"id": "f295575ab57b49XXXe93ca9fe_13fcc967-XXX-494b-XXX-9f72ce6ce8ac",
"update_time": "2024-01-03T19:28:52.023+08:00",
"version": 0
}],
"page": 0,
"size": 10,
"success": true,
"total": 2
}

```

Status code: 400

Request failed.

```
{  
  "error_code" : "SecMaster.00040006",  
  "error_msg" : "Invalid request parameters"  
}
```

Status code: 401

Insufficient permissions.

```
{  
  "error_code" : "SecMaster.90010015",  
  "error_msg" : "Unauthorized request"  
}
```

Status code: 500

Request failed.

```
{  
  "error_code" : "SecMaster.00040011",  
  "error_msg" : "Internal system error."  
}
```

Status Codes

Status Code	Description
200	Request successful.
400	Request failed.
401	Insufficient permissions.
500	Request failed.

Error Codes

See [Error Codes](#).

A Appendix

A.1 Status Codes

- Normal

Status Code	Description
200	Request succeeded.
201	Request succeeded.

- 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

Status Code	Error Codes	Error Message
400	SecMaster.11061001	alert process status error.
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.

Status Code	Error Codes	Error Message
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.
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.
400	SecMaster.20041804	Incorrect content included in the request for converting an alert to an incident.
400	SecMaster.20041805	Failed to create the alert.

Status Code	Error Codes	Error Message
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.
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.
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.

Status Code	Error Codes	Error Message
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.
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.
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.

Status Code	Error Codes	Error Message
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 IAM 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 the administrator. For details about API authentication, see [Authentication](#).

In the following example, **id** indicates the project ID.

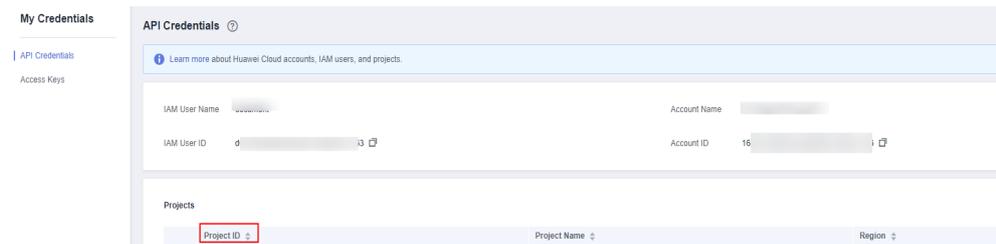
```
{
  "projects": [
    {
      "domain_id": "65382450e8f64ac0870cd180d14e684b",
      "is_domain": false,
      "parent_id": "65382450e8f64ac0870cd180d14e684b",
      "name": "xxxxxxx",
      "description": "",
      "links": {
        "next": null,
        "previous": null,
        "self": "https://www.example.com/v3/projects/a4a5d4098fb4474fa22cd05f897d6b99"
      },
      "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



A.4 About Metrics

Table A-1 Metric description

Metric	ID	Metric Description	Metric Parameter
Total assets	6f8d4892-713c-4d12-8584-dc04f7847b32	Total number of assets in the workspace	None
High-Risk Resources	a5597747-8cef-4342-9855-3fdaf00ad460	Total number of high-risk assets in the workspace	None
Number of assets at other risk levels	09ca4eb8-a4ca-4ef4-b75f-e9172f39393b	Total number of assets except high-risk assets in the workspace	None
Distribution of alerts by severity	1f0f5e29-5a92-17a5-2c16-5f37c6dc109c	Alert distribution by severity in the workspace from the specified start time to the current time	Set params to start_date , which indicates the start time of statistics collection. For example: "start_date": "2024-06-21T00:00:00.000+08:00"
Distribution of vulnerabilities by severity	815c8a73-c855-fd29-63e2-b093d05a7ef0	Distribution of vulnerabilities at different severity levels in the workspace	None

Metric	ID	Metric Description	Metric Parameter
Distribution of failed baseline check results	fee4d416-25b4-46c6-aa1b-851c7251e04b	Distribution of baseline check results at different levels for the past 30 days in the workspace	None
Security score trend	39d386dc-5868-adb6-a8e9-d5e92bb75663	Daily security scores for the last seven days in the workspace	None
Top 5 threat events	aaa6e851-601b-53c5-61ef-ffc95889ebf3	Top 5 threat alarm events in the workspace from the specified start time to the current time	Set params to start_date , which indicates the start time of statistics collection. For example: "start_date": "2024-06-21T00:00:00.000+08:00"
Workspace security score	cf6cce38-bc32-fd89-c0b5-3ba2cdf98eda	Latest security score in the workspace	None