



Hik IP Receiver Pro API

Developer Guide

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use this Document with the guidance and assistance of professionals trained in supporting the Product.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW.

ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Contents

Chapter 1 Overview	1
1.1 Introduction	1
1.2 Release Notes	1
Chapter 2 Security Authentication	5
Chapter 3 API Description	6
3.1 Operation Method	6
3.2 URL Format	6
3.3 Message Format	7
3.4 Others	8
Chapter 4 Typical Application Based on Hik IP Receiver Pro	10
Chapter 5 Alarm and Event	11
5.1 Subscribe to Alarm and Event in Arming Mode	11
Chapter 6 Security Control	14
Chapter 7 API Reference	15
7.1 http://<ipAddress>:<port>/<videoUrl>	15
7.2 /ISAPI/ContentMgmt/DeviceMgmt/deviceList?format=json	15
7.3 /ISAPI/Event/notification/subscribeDeviceMgmt?format=json	16
7.4 /ISAPI/Event/notification/unSubscribeDeviceMgmt/<ID>?format=json	16
7.5 /ISAPI/SecurityCP/control/arm/<ID>?ways=<string>&format=json&devIndex=<uuid>	17
7.6 /ISAPI/SecurityCP/control/bypass?format=json&devIndex=<uuid>	18
7.7 /ISAPI/SecurityCP/control/bypassRecover?format=json&devIndex=<uuid>	18
7.8 /ISAPI/SecurityCP/control/deactivation?format=json&devIndex=<uuid>	19
7.9 /ISAPI/SecurityCP/control/clearAlarm/<ID>?format=json&devIndex=<uuid>	19
7.10 /ISAPI/SecurityCP/control/disarm/<ID>?format=json&devIndex=<uuid>	20
7.11 /ISAPI/SecurityCP/control/outputs?format=json&devIndex=<uuid>	20
7.12 /ISAPI/SecurityCP/status/exDevStatus?format=json&devIndex=<uuid>	21

7.13 /ISAPI/SecurityCP/status/subSystems?format=json&devIndex=<uuid>	22
7.14 /ISAPI/SecurityCP/status/zones?format=json&devIndex=<uuid>	22
Appendix A. Request and Response Messages	24
A.1 JSON_ErrorList	24
A.2 JSON_ExDevStatus	24
A.3 JSON_EventNotificationAlert_AlarmEventInfo	28
A.4 JSON_EventNotificationAlert_cancelVoiceTalkEvent	29
A.5 JSON_EventNotificationAlert_CIDAlarmMsg	31
A.6 JSON_EventNotificationAlert_CidAlarmMsg	33
A.7 JSON_EventNotificationAlert_DeviceDeleted	36
A.8 JSON_EventNotificationAlert_DevStatusChangedAlarmMsg	37
A.9 JSON_EventNotificationAlert_DiskRecoverAlarmMsg	39
A.10 JSON_EventNotificationAlert_diskerror	40
A.11 JSON_EventNotificationAlert_diskfull	42
A.12 JSON_EventNotificationAlert_HeartbeatInfo	44
A.13 JSON_EventNotificationAlert_FallingDownAlarmMsg	45
A.14 JSON_EventNotificationAlert_fielddetection	46
A.15 JSON_EventNotificationAlert_fireDetection	49
A.16 JSON_EventNotificationAlert_IO	53
A.17 JSON_EventNotificationAlert_linedetection	54
A.18 JSON_EventNotificationAlert_VMD	57
A.19 JSON_EventNotificationAlert_RecordExceptionAlarmMsg	60
A.20 JSON_EventNotificationAlert_RegionEntranceAlarmMsg	62
A.21 JSON_EventNotificationAlert_RegionExitingAlarmMsg	65
A.22 JSON_EventNotificationAlert_requestVoiceTalkEvent	68
A.23 JSON_EventNotificationAlert_TDA	70
A.24 JSON_EventNotificationAlert_TMA	74
A.25 JSON_EventNotificationAlert_TMPA	79

A.26 JSON_EventNotificationAlert_PIR	83
A.27 JSON_EventNotificationAlert_VideoLossAlarmMsg	85
A.28 JSON_EventNotificationAlert_VideoTamperingAlarmMsg	87
A.29 JSON_EventNotificationAlert_VideoVerificationAlarmMsg	88
A.30 JSON_EventNotificationAlert_hppConnectionStatusChanged	93
A.31 JSON_EventNotificationAlert_deviceKeyStateChanged	94
A.32 JSON_EventNotificationAlert_longTimeLeave	95
A.33 JSON_EventNotificationAlert_heartBeatAbnormal	96
A.34 JSON_EevntNotificationAlert_respireAbnormal	97
A.35 JSON_EventNotificationAlert_deviceHPPNetworkChanged	98
A.36 JSON_BypassList	99
A.37 JSON_DeactivationList	100
A.38 JSON_OutputsCtrl	100
A.39 JSON_ResponseStatus	100
A.40 JSON_SearchDescription	101
A.41 JSON_SearchResult	102
A.42 JSON_SubscribeDeviceMgmt	104
A.43 JSON_SubscribeDeviceMgmtRsp	104
A.44 JSON_SubSysList	104
A.45 JSON_ZoneCond	105
A.46 JSON_ZoneSearch	105
A.47 JSON_ZoneList	108
Appendix B. Event Types	112
Appendix C. Status Codes	115
Appendix D. Event Code List	119
D.1 Event Codes of Security Control Device	119
D.2 Event Codes of Encoding Device	134
D.3 Event Codes of Radar Device	135

D.4 Event Codes of Access Control Device	135
D.5 Event Codes of Device/Platform Status	135

Chapter 1 Overview

1.1 Introduction

The Hik IP Receiver Pro SDK based on a text protocol in RESTful style provides a uniform integration scheme for Hikvision products. It solves the integration difficulties of multiple open protocols, increases integration efficiency, and improves the compatibility of Hikvision security control devices and the third-party platform. This manual mainly introduces the communication and security mechanism, Hik IP Receiver Pro operations, management (e.g., configuration, maintenance) of devices that are added to Hik IP Receiver Pro, alarm/event subscription, security control panel applications, and so on.



Note

REST (REpresentational State Transfer) is a protocol design method (named as RESTful) which abstracts all information as the resources. The abstracted resources are marked by the uniform identifies, i.e., URI (Uniform Resource Identifiers), for simple and extendable management.

1.2 Release Notes

Summary of Changes in Version 2.3.0_April., 2025

1. Add a device source and device type **IP Speaker**. See [*JSON_SearchDescription*](#) and [*JSON_SearchResult*](#) for details.
2. For [*JSON_SearchResult*](#) :
 - Add three fields **numOfDevice**, **numOfUnauthorized**, and **numOfNotActivated** to count the number of all devices, unauthorized devices, and unactivated devices.
 - Add two fields **pluginEnable** and **pluginType** for enabling verification for video plugin, video intercom plugin, security control panel plugin, and IP speaker plugin.
 - Add a device offline reason: HPP link exception.
 - Add a field **deviceIDPriority** to set the priority of device ID (zone ID or device number).
3. Add two fields **oneTimeDeactivationMode** (one-time deactivation mode) and **deactivationMode** (permanent deactivation mode) to control zone deactivation. See [*JSON_ZoneSearch*](#) for details.
4. Add a protocol of deactivation of zones. See [*/ISAPI/SecurityCP/control/deactivation?format=json&devIndex=<uuid>*](#) and [*JSON_DeactivationList*](#) .
5. In the section **Request and Response Messages**, change the title of Json_List to Json_BypassList. See [*JSON_BypassList*](#) for details.
6. Add an event of Hik-Partner Pro network changes. See [*JSON_EventNotificationAlert_deviceHPPNetworkChanged*](#) for details.
7. Add two events codes **deviceHppAbnormal** and **deviceHppNormal**. See [*Event Codes of Device/Platform Status*](#) for details.

Summary of Changes in Version 2.2.0_August., 2024

1. Add a field **seq** (serial No.) to the request message about the peripherals status. You can set this field to control a peripheral if the device No. is not available. See [***JSON_ExDevStatus***](#) for details.
2. Add a field **seq** to the request message about relay control parameters. You can set this field to control a relay if the relay No. is not available. See [***JSON_OutputsCtrl***](#) for details.
3. Add the following three auxiliary care radar events:

Table 1-1 Event Details

Event	Related Document
Abnormal Respiratory Rate Alarm	<i>JSON_EevntNotificationAlert_respireAbnormal</i>
Irregular Heartbeat Alarm	<i>JSON_EventNotificationAlert_heartBeatAbnormal</i>
Prolonged Bed Exit Alarm	<i>JSON_EventNotificationAlert_longTimeLeave</i>

4. Add 17 event codes for security control panels: 1313, 1314, 1349, 1571, 1572, 1573, 1753, 1754, 1926, 1991, 3313, 3314, 3349, 3571, 3572, 3753, and 3754. See [***Event Codes of Security Control Device***](#) for details.
5. Add three event codes for auxiliary care radars: **longTimeLeave**, **heartBeatAbnormal**, and **respireAbnormal**. See [***Event Codes of Radar Device***](#) for details.

Summary of Changes in Version 2.1.0_May., 2024

1. Add one device key status event: **deviceKeyStateChanged** (Device key status changed event). See [***JSON_EventNotificationAlert_deviceKeyStateChanged***](#) for details.
2. Extend the message about search results [***JSON_SearchResult***](#) :
added one field **offlineHint** (offline reason of direct connection).

Summary of Changes in Version 2.0.0_Dec., 2023

1. Extend the message about search conditions of channel list [***JSON_SearchDescription***](#) :
added one value to the field **connectionMode**: "OTAP";
added one value to the field **devSource**: 7 (OTAP alarm device);
2. Extend the message about search results [***JSON_SearchResult***](#) :
added one field **OTAP** (ID and key of OTAP device);
added one value to the field **connectionMode**: "OTAP";
added one value to the field **devSource**: 7 (OTAP alarm device);
added one value to the field **onlineType**: 2 (OTAP).
3. Add remarks to [***/ISAPI/SecurityCP/control/outputs?format=json&devIndex=<uuid>***](#) and [***/ISAPI/SecurityCP/status/exDevStatus?format=json&devIndex=<uuid>***](#) :

This API does not support alarm devices accessed via OTAP.

4. Add one device connection status event: **hppConnectionStatusChanged** (Hik-Partner Pro connection status changed event). See **JSON_EventNotificationAlert_hppConnectionStatusChanged** for details.

Summary of Changes in Version 1.8.0_Jul., 2023

1. Add one medical radar device event: **FallingDownAlarmMsg** (people falling down detection event). See **JSON_EventNotificationAlert_FallingDownAlarmMsg** for details.
2. Extend the message about video verification alarm details **JSON_EventNotificationAlert_VideoVerificationAlarmMsg** :
added one field **deviceSerial** (device serial No.).
3. Extended the message about CID (Contact ID) alarm details **JSON_EventNotificationAlert_CidAlarmMsg** :
added one field **deviceSerial** (device serial No.).
4. Extend the message about search results **JSON_SearchResult** :
added one field **isNeedUpgrade** (whether the device needs upgrade);
added one field **remark** (remarks of the device);
added one value to the field **devStatus**: "unknown".
5. Extend the message about search conditions of channel list **JSON_SearchDescription** :
added one field **isNeedUpgrade** (whether the device needs upgrade);
added one value to the field **devStatus**: "unknown";
added one value to the field **devSource**: "radar device".

Summary of Changes in Version 1.7.0_Apr., 2023

1. Extend the message about search conditions of channel list **JSON_SearchDescription** :
added three fields: **activeStatus** (device status), **connectionMode** (connection mode), and **devSource** (device source);
added one value to the field **orderByColumn**: 4 (device serial No.).
2. Extend the message about search results **JSON_SearchResult** :
added one field **existUnauth** (whether unauthorized devices exist);
added one value to the field **activeStatus**: "unauth" (unauthorized);
added one value to the field **devSource**: 4 (ISUP5.0 video devices);
edited the description of the value in the field **onlineType**: 0 (HPP).
3. Add 8 events codes to **Event Codes of Security Control Device** :

HikCode	CIDCode	SIACode	Description
1310	E311	YT	Battery Fault
1330	E330	ET	Expander Fault
1750	E750	IA	Drilling alarm
1786	E153	KT	Temperature Alarm

HikCode	CIDCode	SIACode	Description
3310	R311	YR	Battery Fault Restored
3330	R330	ER	Expander Fault Restored
3750	R750	IR	Drilling Alarm Restored
3786	R3153	KJ	Temperature Alarm Restored

Summary of Changes in Version 1.6.0_Oct., 2022

1. Extend the message about video verification alarm details
JSON_EventNotificationAlert_VideoVerificationAlarmMsg :
added two fields **videoInfoList** (video information list) and **isTalk** (whether it supports two-way audio verification).
2. Extend the message about CID (Contact ID) alarm details
JSON_EventNotificationAlert_CidAlarmMsg :
added one field **isTalk** (whether it supports two-way audio verification).
3. Add the two access control events: **requestVoiceTalkEvent** (two-way audio request alarm) and **cancelVoiceTalkEvent** (two-way audio canceling alarm). See **JSON_EventNotificationAlert_requestVoiceTalkEvent** and **JSON_EventNotificationAlert_cancelVoiceTalkEvent** for details.

Summary of Changes in Version 1.2.0_March, 2021

New document.

Chapter 2 Security Authentication

When communicating via Hik IP Receiver Pro SDK, the digest of the session must be authenticated.

Note

- The authentication must be based on *HTTP Authentication: Basic and Digest Access Authentication*, see <https://tools.ietf.org/html/rfc2617> for details.
- The request session must contain authentication information, otherwise, device will return 401 error code.
- For login authentication, the available URL is GET .

The message digest, which contains user name, password, specific nonce value, HTTP or RTSP operation methods, and request URL, is generated by the MD5 algorithm, see the calculation rules below.

qop=Undefined

Digest=MD5(MD5(A1):<nonce>:MD5(A2))

qop="auth:"

Digest=MD5(MD5(A1):<nonce>:<nc>:<cnonce>:<qop>:MD5(A2))

qop="auth-int:"

Digest=MD5(MD5(A1):<nonce>:<nc>:<cnonce>:<qop>:MD5(A2))

Note

- The **qop** is a value for determining whether the authentication is required.
- A1 and A2 are two data blocks required for digest calculation.
A1: Data block about security, which contains user name, password, security domain, random number, and so on. If the digest calculation algorithm is MD5, A1=<user>:<realm>:<password>; if the algorithm is MD5-sess, A1=MD5(<user>:<realm>:<password>):<nonce>:<cnonce>.
A2: Data block about message, such as URL, repeated requests, message body, and so on, it helps to prevent repeated, and realize the resource/message tamper-proof. If the **qop** is not defined or it is "auth:", A2=<request-method>:<uri-directive-value>; if the **qop** is "auth-int:", A2=<request-method>:<uri-directive-value>:MD5(<request-entity-body>).
- The **nonce** is the random number generated by service, the following generation formula is suggested: nonce = BASE64(time-stamp MD5(time-stamp ":" ETag ":" private-key)). The **time-stamp** in the formula is the time stamp generated by service or the unique serial No.; the **ETag** is the value of HTTP ETag header in the request message; the **private-key** is the data that only known by service.

If authentication fail, the device will return the message, and the remaining authentication attempts will also be returned. If the remaining attempts is 0, the user will be locked at the next authentication attempt.

Chapter 3 API Description

3.1 Operation Method

The resource operation methods of the SDK are same as those of HTTP (Hyper Text Transport Protocol), see details in the following table.

**Note**

For details about HTTP and HTTPS, please refer to <https://tools.ietf.org/html/rfc2612> and <https://tools.ietf.org/html/rfc2818>.

Table 3-1 HTTP Operation Method

Method	Description
POST	Create resources.
GET	Retrieve resources. This method cannot change the system status, only return data as the response to the requester.
PUT	Update resources.
DELETE	Delete resources.

3.2 URL Format

URL (Uniform Resource Locator) is a further class of URIs, it can identify a resource and locate the resource by describing its primary access mechanism.

The format of URL is defined as the follows: {protocol}://{ipAddress}:{port}{abs_path}?{query}.

protocol

Protocol types, i.e., HTTP (version 1.1), HTTPS, RTSP (version 1.0).

host

Host name, IP address, or the FQDN (Fully Qualified Domain Name) of network devices.

port

Port number of host service for listening the connection status of TCP (Transmission Control Protocol, see <https://tools.ietf.org/html/rfc793>) or UDP (User Datagram Protocol, see <https://tools.ietf.org/html/rfc768>). If this field is not configured, the default port number will be adopted. For HTTP, the default port number is 80, for HTTPS, the default port number is 443, and for RTSP, the default port number is 554.

abs_path

Resource URI: /ServiceName/ResourceType/resource. Here, the **ServiceName** is ISAPI; the **ResourceType** is predefined with upper camel case according to different functions , see details in the following table; the **resource** is defined with lower camel case and can be extended in actual applications. E.g., /ISAPI/System/deviceInfo/deviceName.

Predefined URI Model	Description
/ISAPI/System/...	System related resources
/ISAPI/Security/...	Security related resources
/ISAPI/Streaming/...	Video streaming and management related resources
/ISAPI/Event...	Event/alarm related resources
/ISAPI/PTZCtrl/...	PTZ control related resources
/ISAPI/Image/...	Video encoding and image related resources
/ISAPI/ContentMgmt/...	Storage management related resources

query

Strings for describing resources information, including related parameters. The parameter names and values must be listed as the following format in this field: ?p1=v1&p2=v2&...&pn=vn.



Note

- To locate the connected device, when operating lower-level device via the URL, the **query** field should be filled as ?devIndex=uuid&p1=v1&p2=v2&...&pn=vn. The uuid (or guid) is a 32-byte (128 bits) random number, which is unique and generated by operating system when adding device, and its format is "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx".
- For message in JSON format, the **query** field should be filled as ?format=json&p1=v1&p2=v2&...&pn=vn. For details about message format, refer to the next section below. E.g., http://10.17.132.22/ISAPI/System/time?format=json&devIndex=550e8400e29b41d4a716446655440000.

3.3 Message Format

The request and response messages generated among the interaction of device gateway, devices, and system are data in JSON format.



Note

The message format here is only available for URLs based on HTTP.

- The leaf node (without any sub node) in the message is named by lower camel case, while the non-leaf node in the message is named by upper camel case.
- To communicate by the messages in JSON format, the devices must support the public specifications in <http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-404.pdf> and HTTP with version 1.1.



Note

JSON is a lightweight data format which is a subset of JavaScript language and is small, fast, and easy to be parsed.

- Generally, for configuration information, the **Content-Type** of message is "application/json", see the example below:

```
//Request message
GET /ISAPI/System/deviceInfo?format=json HTTP/1.1
...

//Response message
HTTP/1.1 200 OK
...
Content-Type: application/json
...
"DeviceStatus":""
...
```

For data (e.g., firmware, configuration files), the **Content-Type** of message is "application/octet-stream", see the example below:

```
//Request message
POST /ISAPI/System/streamMedia?format=json&devIndex=550e8400e29b41d4a716446655440000 HTTP/1.1
...
Content-Type: application/octet-stream
...
[proprietary configuration file data content]

//Response message
HTTP/1.1 200 OK
...
Content-Type: application/json
...
"ResponseStatus":""
...
```

3.4 Others

Time Format

The time format in the device gateway SDK adopts ISO8601 standard (see details in <http://www.w3.org/TR/NOTE-datetime-970915>), that is, YYYY-MM-DDThh:mm:ss.sTZD (e.g., 2017-08-16T20:17:06+08:00, 2017-08-16T20:09:06Z).

Error Processing

During the integration applications of device gateway SDK, when the error of URL based on HTTP occurs, the ***JSON_ResponseStatus*** message which contains error code will be returned. If the error of URL based on RTSP occurs, the corresponding status code will directly be returned, for details, refer to <https://tools.ietf.org/html/rfc2326> .



Note

For batch operations, if some operations fail, both the ***JSON_ResponseStatus*** message and failure details message (see details in actual batch operations, such as adding devices or deleting devices in a batch) will be returned.

Chapter 4 Typical Application Based on Hik IP Receiver Pro

The Hik IP Receiver Pro provides service including protocol conversion, linking channels to zone, event receiving, transmitting event to ARC (alarm receiving center), video/image verification via Hik VideoPlugin, etc.

The Hik IP Receiver Pro can add devices (e.g. AX Pro security control panel, network camera, NVR, and DVR) on Hik-ProConnect, add security control panels by ISUP5.0, and add third-party devices with device name and account ID, and connect to ARC. And then the communication and interaction between added devices and ARC will be built on the protocol conversion function of Hik IP Receiver Pro, refer to the application framework below.

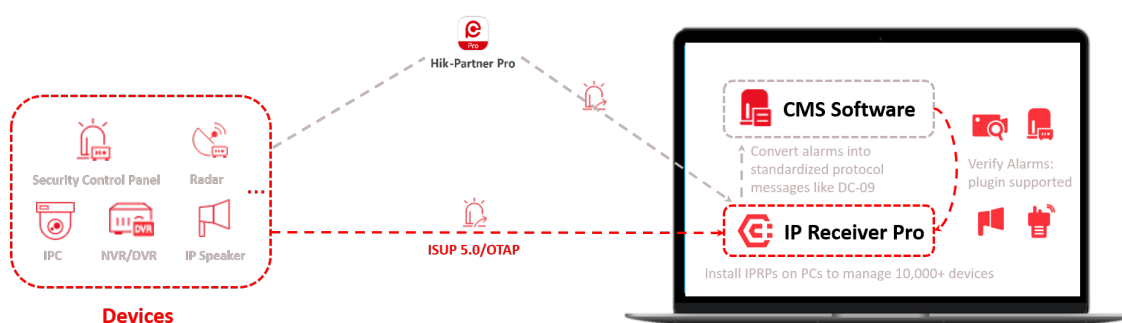


Figure 4-1 Typical Application Based on Hik IP Receiver Pro

Chapter 5 Alarm and Event

You can arm the devices via the Hik IP Receiver Pro, and the devices will upload the alarm or event information to Hik IP Receiver Pro if the alarm is triggered or the event occurs. And the third-party system can send the subscription conditions to multiple devices for subscribing to all alarms or events via Hik IP Receiver Pro by setting up only one connection.

5.1 Subscribe to Alarm and Event in Arming Mode

For arming mode, the system will connect to the devices automatically and send commands to the devices for uploading alarm/event information when the alarm is triggered or event occurred. In this case, multiple connections are built among the third-party system, device gateway, and devices, so the arming parameters (including alarm/event types to be subscribed, linkage actions, arming schedule, and so on) or alarm/event information will be sent or uploaded via the device gateway.

Before You Start

- Make sure you have configured the protocol type as Private and enabled it on Hik IP Receiver Pro
- Make sure you have configured the alarm parameters, such as arming schedule, linkage actions (set to "center"), and so on, to arm the device.

Steps

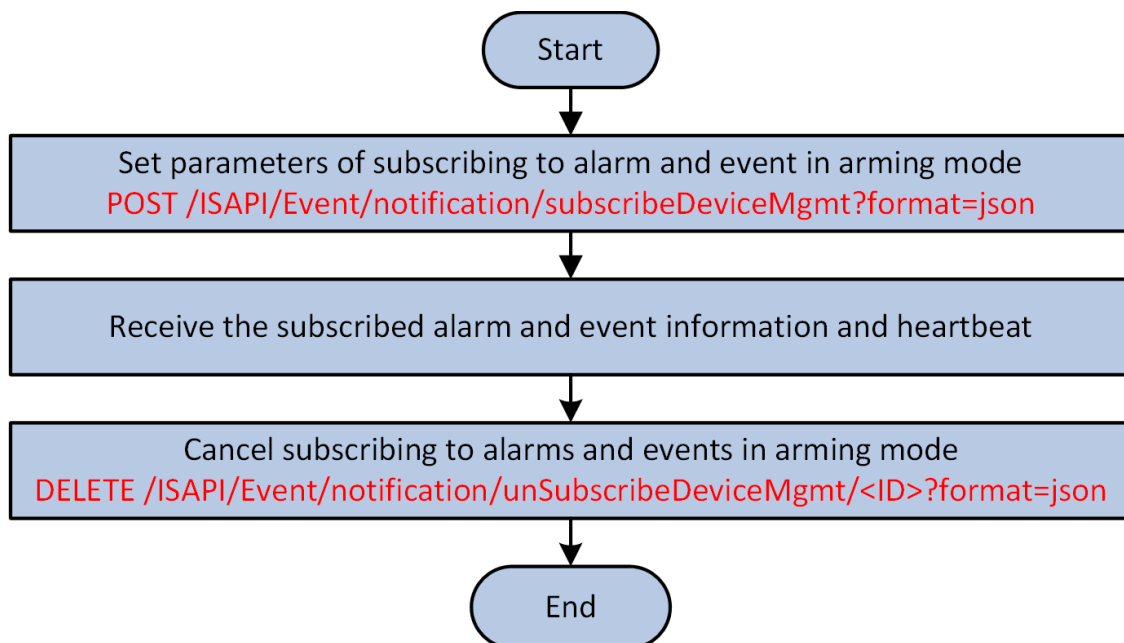


Figure 5-1 API Calling Flow of Subscribing to Alarm and Event in Arming Mode

1. Call **/ISAPI/Event/notification/subscribeDeviceMgmt?format=json** by POST method to set parameters of subscribing to all alarms and events in arming mode.



Note

Refer to **Event Types** for the supported alarm or event types.

2. When the alarm is triggered or event occurred, receive the alarm or event information and heartbeat from the messages **JSON_EventNotificationAlert_AlarmEventInfo** and **JSON_EventNotificationAlert_HeartbeatInfo** uploaded by device.



Note

- If receiving alarm/event information exception or receiving heartbeat timed out (the default heartbeat interval is 10 seconds, and the suggested timeout is 30 seconds), you should call **/ISAPI/Event/notification/subscribeDeviceMgmt?format=json** by POST to rebuild the link.
- The alarm or event information messages vary with different alarm or event types, refer to common alarm or event information message in **JSON_EventNotificationAlert_AlarmEventInfo**.

3. Call **/ISAPI/Event/notification/unSubscribeDeviceMgmt/<ID>?format=json** by DELETE to cancel subscribing to alarms and events in arming mode.

Example

Message Example of Subscribing to Alarm or Event in Arming Mode

Request Message

```
POST /ISAPI/Event/notification/subscribeDeviceMgmt?format=json HTTP/1.1
Host: 127.0.0.1:80
X-Forwarded-For: 127.0.0.1
X-Real-Port: 57946
Connection: Keep-Alive
Content-Length: 63
Content-Type: application/x-www-form-urlencoded
Authorization: Digest username="admin",
realm="DS-GWAS0101(6419)",
nonce="4e546c6c596a55355a5749364e5752684f4445344d57593d",
uri="/ISAPI/Event/notification/subscribeDeviceMgmt",
cnonce="7e867c78d9874aa904b489a6791aaef",
nc=00000001,
qop="auth",
response="fa7d3d95762b6e10c8a18f09f1f61e81"
```

```
{
  "SubscribeDeviceMgmt":{
    "eventMode":"all",
    "defenceMode":"all"
  }
}
```

Response Message

```
HTTP/1.1 200 OK
Server: nginx
```

```
Date: Wed, 26 Dec 2018 11:38:38 GMT
Content-Type: multipart/mixed; boundary=boundary
Connection: close
MIME-Version: 1.0

--boundary
Content-Type: application/json; charset="UTF-8"
Content-Length: 39

{"SubscribeDeviceMgmtRsp":{"id":5939}}
--boundary
Content-Type: application/json; charset="UTF-8"
Content-Length: 415

{
  "EventNotificationAlert":{
    "channelID": "1",
    "dateTime": "2018-01-21T12:50:39+08:00",
    "activePostCount": 1,
    "eventType": "devStatusChanged",
    "eventState": "active",
    "eventDescription": "device status about online or offline changed",
    "devIndex": "2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName": "Device1",
    "status": "online",
  }
}
--boundary
Content-Type: application/json; charset="UTF-8"
Content-Length: 183

{
  "EventNotificationAlert":{
    "dateTime": "2018-12-26T19:39:21+08:00",
    "activePostCount": 1,
    "eventType": "heartBeat",
    "eventState": "active",
    "eventDescription": "Heart Beat"
  }
}
```

Chapter 6 Security Control

A security control device detects people, vehicles, etc., entering a predefined region, triggers events and alarms, and reports events/alarms information (such as location) to security personnel. The region can be classified as zone and partition: for zone, it refers to a protection area and is regarded as the maximum recognizable unit to distinguish the alarm event; for partition, it is an independent control system of a security control device, allows you to batch arm or disarm all zones in it.

Control Alarm Device

Function	URI
Arm partition	<u>PUT /ISAPI/SecurityCP/control/arm/<ID>?ways=<string>&format=json&devIndex=<uuid></u>
Disarm partition	<u>PUT /ISAPI/SecurityCP/control/disarm/<ID>?format=json&devIndex=<uuid></u>
Clear partition's alarms	<u>PUT /ISAPI/SecurityCP/control/clearAlarm/<ID>?format=json&devIndex=<uuid></u>
Bypass zone in a batch	<u>PUT /ISAPI/SecurityCP/control/bypass?format=json&devIndex=<uuid></u>
Recover zone bypass in a batch	<u>PUT /ISAPI/SecurityCP/control/bypassRecover?format=json&devIndex=<uuid></u>
Deactivate zone in a batch	<u>PUT /ISAPI/SecurityCP/control/deactivation?format=json&devIndex=<uuid></u>
Control relay	<u>POST /ISAPI/SecurityCP/control/outputs?format=json&devIndex=<uuid></u>

Get Real-Time Status of Alarm Device

Function	URI
Get all partitions' statuses	<u>GET /ISAPI/SecurityCP/status/subSystems?format=json&devIndex=<uuid></u>
Get zones' statuses by conditions	<u>GET /ISAPI/SecurityCP/status/zones?format=json&devIndex=<uuid></u>
Get all peripherals' statuses	<u>GET /ISAPI/SecurityCP/status/exDevStatus?format=json&devIndex=<uuid></u>

Chapter 7 API Reference

7.1 http://<ipAddress>:<port>/<videoUrl>

Download the video or picture files from alarm via the permission of admin user.

Request URI Definition

Table 7-1 GET http://<ipAddress>:<port>/<videoUrl>

Method	GET
Description	Download the video or picture files from alarm via the permission of admin user.
Query	None
Request	None
Response	Video Data

Remarks

- The <ipAddress> and <port> in the URL refer to the IP address and port No. of Hik IP Receiver Pro; the <videoUrl> in the URL is the video or picture file URL uploaded in the alarm message.
- For access control events, the uploaded event and alarm message only contains picture file URL.

7.2 /ISAPI/ContentMgmt/DeviceMgmt/deviceList?format=json

Search for the added device list.

Request URI Definition

Table 7-2 POST /ISAPI/ContentMgmt/DeviceMgmt/deviceList?format=json

Method	POST
Description	Search for the added device list.
Query	format : determine the format of request or response message. security : the version No. of encryption scheme. When security does not exist, it indicates that the data is not encrypted; when security is 1, it indicates that the nodes of sensitive information in the message are encrypted in AES128 CBC mode; when security is 2, it indicates

	that the nodes of sensitive information in the message are encrypted in AES256 CBC mode. iv : the initialization vector, and it is required when security is 1 or 2.
Request	<u><i>JSON_SearchDescription</i></u>
Response	<u><i>JSON_SearchResult</i></u>

7.3 /ISAPI/Event/notification/subscribeDeviceMgmt?format=json

Enable subscribing alarm/event in arming mode.

Request URI Definition

Table 7-3 POST /ISAPI/Event/notification/subscribeDeviceMgmt?format=json

Method	POST
Description	Enable subscribing alarm/event in arming mode.
Query	format : determine the format of request or response message.
Request	<u><i>JSON_SubscribeDeviceMgmt</i></u>
Response	Succeeded: <u><i>JSON_SubscribeDeviceMgmtRsp</i></u> + <u><i>JSON_EventNotificationAlert_AlarmEventInfo</i></u> or <u><i>JSON_EventNotificationAlert_HeartbeatInfo</i></u> Failed: <u><i>JSON_ResponseStatus</i></u>

Remarks

- The *JSON_EventNotificationAlert_AlarmEventInfo* and *JSON_EventNotificationAlert_HeartbeatInfo* are uploaded repeatedly.
- Arming/disarming all devices is supported, while arming/disarming a single device is no longer supported.
- The value of **eventMode** in *JSON_SubscribeDeviceMgmt* should be "all" to arm all added devices. For the devices added later, Hik IP Receiver Pro will arm them automatically without further operation.

7.4 /ISAPI/Event/notification/unSubscribeDeviceMgmt/<ID>?format=json

Disable alarm/event subscription in arming mode.

Request URI Definition

Table 7-4 DELETE /ISAPI/Event/notification/unSubscribeDeviceMgmt/<ID>?format=json

Method	DELETE
Description	Disable alarm/event subscription in arming mode.
Query	format: determine the format of request or response message.
Request	None.
Response	<u><i>JSON ResponseStatus</i></u>

Remarks

The **ID** in the URI is the subscription ID, which is returned by the device gateway.

7.5 /ISAPI/SecurityCP/control/arm/<ID>? ways=<string>&format=json&devIndex=<uuid>

Arm the partition.

Request URI Definition

**Table 7-5 PUT /ISAPI/SecurityCP/control/arm/<ID>?
ways=<string>&format=json&devIndex=<uuid>**

Method	PUT
Description	Arm the partition.
Query	ways: arming mode, "stay"-stay arming and "away"-away arming are available. format: determine the format of request or response message. devIndex: a uuid or guid (a 32-byte or 128-bit random number) for locating the connected or lower-level devices, which is unique and generated by operating system when adding device, and its format is "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx".
Request	None
Response	<u><i>JSON ResponseStatus</i></u>

Remarks

The **<ID>** in the request URI refers to the partition No., which starts from 1. If ID equals to 0xffffffff, all partitions are selected.

7.6 /ISAPI/SecurityCP/control/bypass?format=json&devIndex=<uuid>

Bypass zones in a batch.

Request URI Definition

Table 7-6 PUT /ISAPI/SecurityCP/control/bypass?format=json&devIndex=<uuid>

Method	PUT
Description	Bypass zones in a batch.
Query	format: determine the format of request or response message. devIndex: a uuid or guid (a 32-byte or 128-bit random number) for locating the connected or lower-level devices, which is unique and generated by operating system when adding device, and its format is "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx".
Request	<i><u>JSON BypassList</u></i>
Response	<i><u>JSON ResponseStatus</u></i>

7.7 /ISAPI/SecurityCP/control/bypassRecover?format=json&devIndex=<uuid>

Recover bypass of zones in a batch.

Request URI Definition

Table 7-7 PUT /ISAPI/SecurityCP/control/bypassRecover?format=json&devIndex=<uuid>

Method	PUT
Description	Recover bypass of zones in a batch.
Query	format: determine the format of request or response message. devIndex: a uuid or guid (a 32-byte or 128-bit random number) for locating the connected or lower-level devices, which is unique and generated by operating system when adding device, and its format is "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx".
Request	<i><u>JSON BypassList</u></i>
Response	<i><u>JSON ResponseStatus</u></i>

7.8 /ISAPI/SecurityCP/control/deactivation? format=json&devIndex=<uuid>

Deactivation of zones.

Request URI Definition

Table 7-8 PUT /ISAPI/SecurityCP/control/deactivation?format=json&devIndex=<uuid>

Method	PUT
Description	Deactivation of zones in a batch.
Query	None
Request	<u><i>JSON_DeactivationList</i></u>
Response	<u><i>JSON_ResponseStatus</i></u>

Remarks

Applicable to security control panels that support the OTAP protocol, which does not support zone bypass.

7.9 /ISAPI/SecurityCP/control/clearAlarm/<ID>? format=json&devIndex=<uuid>

Clear the alarms.

Request URI Definition

Table 7-9 PUT /ISAPI/SecurityCP/control/clearAlarm/<ID>?format=json&devIndex=<uuid>

Method	PUT
Description	Clear the alarms.
Query	format: determine the format of request or response message. devIndex: a uuid or guid (a 32-byte or 128-bit random number) for locating the connected or lower-level devices, which is unique and generated by operating system when adding device, and its format is "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx".
Request	None
Response	<u><i>JSON_ResponseStatus</i></u>

Remarks

The <ID> in the request URI refers to the partition No., if the value of ID is 0xffffffff, it indicates all partitions.

7.10 /ISAPI/SecurityCP/control/disarm/<ID>?format=json&devIndex=<uuid>

Disarm the partition.

Request URI Definition

Table 7-10 PUT /ISAPI/SecurityCP/control/disarm/<ID>?format=json&devIndex=<uuid>

Method	PUT
Description	Disarm the partition.
Query	format: determine the format of request or response message. devIndex: a uuid or guid (a 32-byte or 128-bit random number) for locating the connected or lower-level devices, which is unique and generated by operating system when adding device, and its format is "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx".
Request	None.
Response	<i><u>JSON_ResponseStatus</u></i>

Remarks

The <ID> in the request URI refers to the partition No., which starts from 1. If ID equals to 0xffffffff, all partitions are selected.

7.11 /ISAPI/SecurityCP/control/outputs?format=json&devIndex=<uuid>

Control relays in batch.

Request URI Definition

Table 7-11 POST /ISAPI/SecurityCP/control/outputs?format=json&devIndex=<uuid>

Method	POST
Description	Control relays in batch.
Query	format: determine the format of request or response message.

	devIndex: a uuid or guid (a 32-byte or 128-bit random number) for locating the connected or lower-level devices, which is unique and generated by operating system when adding device, and its format is "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx".
Request	<u><i>JSON_OutputsCtrl</i></u>
Response	Succeeded: <u><i>JSON_ResponseStatus</i></u> Failed: <u><i>JSON_ErrorList</i></u>

Remarks

Alarm devices accessed via OTAP does not support this API.

7.12 /ISAPI/SecurityCP/status/exDevStatus? format=json&devIndex=<uuid>

Get statuses of all peripherals.

Request URI Definition

Table 7-12 GET /ISAPI/SecurityCP/status/exDevStatus?format=json&devIndex=<uuid>

Method	GET
Description	Get statuses of all peripherals.
Query	format: determine the format of request or response message. devIndex: a uuid or guid (a 32-byte or 128-bit random number) for locating the connected or lower-level devices, which is unique and generated by operating system when adding device, and its format is "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx".
Request	None.
Response	Succeeded: <u><i>JSON_ExDevStatus</i></u> Failed: <u><i>JSON_ResponseStatus</i></u>

Remarks

Alarm devices accessed via OTAP does not support this API.

7.13 /ISAPI/SecurityCP/status/subSystems? format=json&devIndex=<uuid>

Get statuses of all partitions.

Request URI Definition

Table 7-13 GET /ISAPI/SecurityCP/status/subSystems?format=json&devIndex=<uuid>

Method	GET
Description	Get statuses of all partitions.
Query	format: determine the format of request or response message. devIndex: a uuid or guid (a 32-byte or 128-bit random number) for locating the connected or lower-level devices, which is unique and generated by operating system when adding device, and its format is "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx".
Request	None
Response	Succeeded: <u><i>JSON_SubSysList</i></u> Failed: <u><i>JSON_ResponseStatus</i></u>

Remarks

Devices accessed via OTAP does not support this API.

7.14 /ISAPI/SecurityCP/status/zones?format=json&devIndex=<uuid>

Search for zone statuses by conditions. The search result is displayed in pages.

Request URI Definition

Table 7-14 POST /ISAPI/SecurityCP/status/zones?format=json&devIndex=<uuid>

Method	POST
Description	Search for statuses of all zones.
Query	format: determine the format of request or response message. devIndex: a uuid or guid (a 32-byte or 128-bit random number) for locating the connected or lower-level devices, which is unique and generated by operating system when adding device, and its format is "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx".

Request	<i><u>JSON_ZoneCond</u></i>
Response	Succeeded: <i><u>JSON_ZoneSearch</u></i> Failed: <i><u>JSON_ResponseStatus</u></i>

Appendix A. Request and Response Messages

A.1 JSON_ErrorList

JSON message about error list

```
{
  "requestURL": "",
  /*optional, request URL*/
  "ErrorList":[{
    "id": "",
    /*required, string type, error object ID*/
    "statusCode": ,
    /*status code, it will not be returned when succeeded or no exception*/
    "statusString": "",
    /*status description, it will not be returned when succeeded or no exception*/
    "subStatusCode": "",
    /*sub status code, it will not be returned when succeeded or no exception*/
    "errorCode": ,
    /*error code, it is optional when succeeded, and it corresponds to subStatusCode*/
    "errorMsg": "ok"
  }]
}
```

A.2 JSON_ExDevStatus

JSON message about peripherals status.

```
{
  "ExDevStatus":{
    "OutputModList":[{
      /*optional, wireless output module list/
      "OutputMod":{
        "id": ,
        /*optional, int, wireless output module No.*/
        "seq": "",
        /*optional, string, serial No. of wireless output module*/
        "status": "",
        /*optional, string, wireless output module status: "notRelated"-unlinked, "online", "offline", "heartbeatAbnormal"-
        heartbeat exception*/
        "tamperEvident": ,
        /*optional, boolean, tampering status: "true"-tampered, "false"-not tampered*/
        "charge": ""
        /*optional, string, power status: "normal", "lowPower"*/
        "chargeValue": 0,
        /*optional, int, power value; range: [0,100]*/
```

```
    "signal":255,
    /*optional, int, signal strength; range: [0,255]*/
    "model":"","
    /*optional, string, model: "DS-PM1-O8-WE" (wireless output module with 8 channels), "DS-PM1-O2-WE" (wireless
    output module with 2 channels)*/
    "temperature":1,
    /*optional, int, read-only, temperature*/
    }
  }],
  "OutputList":[{"
    /*optional, relay list*/
    "Output":{"
      "id": ,
      /*optional, integer, relay No.*/
      "seq": ,
      /*optional, string, relay Serial No.*/
      "name":"","
      /*optional, string, relay name*/
      "status":"","
      /*optional, string, relay status: "notRelated"-unlinked, "on"-open, "off"-closed, "offline"*/
      "tamperEvident": ,
      /*optional, boolean, tampering status: "true"-tampered, "false"-not tampered*/
      "charge":"","
      /*optional, string, power status: "normal", "lowPower"*/
      "chargeValue":0,
      /*optional, int, power value; range: [0,100]*/
      "linkage":"","
      /*optional, string, event linkage type of relay: "alarm", "arming", "disarming", "manualCtrl"-manual control*/
      "signal":255,
      /*optional, int, signal strength; range: [0,255]*/
      "temperature":1,
      /*optional, int, read-only, temperature*/
    }
  }],
  "SirenList":[{"
    /*optional, siren list*/
    "Siren":{"
      "id": ,
      /*optional, integer, siren No.*/
      "seq":"","
      /*optional, string, siren serial No.*/
      "name":"","
      /*optional, string, siren name*/
      "status":"","
      /*optional, string, siren status: "notRelated"-unlinked, "on"-enabled, "off"-disabledd, "offline"*/
      "tamperEvident": ,
      /*optional, boolean, tampering status: "true"-tampered, "false"-not tampered*/
      "sirenAttrib": "",
      /*string, siren attributes: "wired", "wireless"*/
      "charge":"","
      /*optional, string, power status: "normal", "lowPower"*/
      "chargeValue":0,
```



```
/*optional, int, power value; range: [0,100]*/
    "signal":255,
/*optional, int, signal strength; range: [0,255]*/
    "model": "",
/*optional, string, model: "DS-PS1-I-WE" (wireless indoor siren), "DS-PS1-E-WE" (wireless outdoor siren)*/
    "temperature":1,
/*optional, int, read-only, temperature*/
    "subSystemList":[1,2,3],
/*optional, list, list of linked partitions*/
    "powerSupplyStatus":""
/*optional, string, power supply status: "battery", "DC12V" (12V direct current)*/
    }
  }],
  "RepeaterList":[{"
/*optional, repeater list*/
    "Repeater":{
      "id": ,
/*optional, integer type, repeater No.*/
      "seq": "",
/*optional, string, repeater serial No.*/
      "name": "",
/*optional, string, rrepeater name*/
      "status": "",
/*optional, string, repeater status: "notRelated"-unlinked, "online", "offline"*/
      "tamperEvident": ,
/*optional, boolean, tampering status: "true"-tampered, "false"-not tampered*/
      "charge": "",
/*optional, string, power status: "normal", "lowPower"*/
      "chargeValue":0,
/*optional, int, power value; range: [0,100]*/
      "signal":255,
/*optional, int, signal strength; range: [0,255]*/
      "model": "",
/*optional, string, model: "DS-PR1-WE" (wireless repeater)*/
      "temperature":0,
/*optional, int, read-only, temperature*/
    }
  ]
  "CardReaderList":[{"
/*optional, card reader list*/
    "CardReader":{
      "id": ,
/*optional, int, card reader No.*/
      "seq": "",
/*optional, string, card reader serial No.*/
      "name": "",
/*optional, string, card reader name*/
      "status": "",
/*optional, string, card reader status: "notRelated"-not linked, "online", "offline", "heartbeatAbnormal"-heartbeat
exception*/
      "tamperEvident": ,
/*optional, boolean, tampering status: "true"-tampered, "false"-not tampered*/
```

```
"charge": "",
/*optional, string, state of charge: "normal", "lowPower"-low battery*/
"chargeValue": 0,
/*optional, int, power value; range: [0,100]*/
"signal": 255,
/*optional, int, signal strength; range: [0,255]*/
"model": "",
/*optional, string, model: "DS-PR1-WE" (wireless repeater)*/
"temperature": 0,
/*optional, int, read-only, temperature*/
"subSystemList": [1,2,3],
/*optional, list, list of linked partitions*/
}
}],
"ExtensionList": [{
/*optional, extension module list*/
"ExtensionModule": {
"Id": ,
/*optional, int, extension module No.*/
"seq": ,
/*optional, string, extension module serial No.*/
"name": "",
/*optional, string, extension module name*/
"address": 1,
/*optional, int, module address, this node is returned by wired modules*/
"linkageAddress": 1,
/*optional, int, linked module address, this node is returned by wireless modules*/
"type": "",
/*optional, string, module type: "wiredZone"-wired zone module, "wiredOutput"-wired output module,
"wirelessOutput"-wireless output module, "wirelessRecv"-wireless receiver module (wired module)*/
"status": "",
/*optional, string, keypad status: "online", "offline", "heartbeatAbnormal"-heartbeat exception*/
"tamperEvident": ,
/*optional, boolean, tampering status: "true"-tampered, "false"-not tampered*/
"moduleAttrib": "",
/*string, module attribute: "wired", "wireless"*/
"charge": "",
/*optional, string, state of charge: "normal", "lowPower"-low battery*/
"chargeValue": 0,
/*optional, int, power value; range: [0,100]*/
"temperature": 0,
/*optional, int, read-only, temperature*/
}
}],
"KeypadList": [{
/*optional, keypad list*/
"Keypad": {
"Id": 1,
/*optional, int, keypad No.*/
"seq": "",
/*optional, string, keypad serial No.*/
"name": "",
```

```
/*optional, string, keypad name*/
  "status":"","
/*optional, string, keypad status: "notRelated"-not linked, "online", "offline", "heartbeatAbnormal"-heartbeat
exception*/
  "tamperEvident": ,
/*optional, boolean, tampering status: "true"-tampered, "false"-not tampered*/
  "keypadAttrib":"","
/*string, keypad attribute: "wired", "wireless"*/
  "charge":"","
/*optional, string, state of charge: "normal", "lowPower"-low battery*/
  "signal": ,
/*optional, int, signal strength, it is between 0 and 255*/
  "address":
/*optional, int, keypad address, this node is only returned by wired keypads*/
  "model": "DS-PK1-E-WE",
/*optional, string, model: "DS-PK1-E-WE" (wireless LED keypad)*/
  }
}]
  "RemoteList":[{
/*optional*/
    "Remote":{
      "id": ,
/*optional, int, remote control No.*/
      "seq":"","
/*optional, string, remote control serial No.*/
      "name":"","
/*optional, string, remote control name*/
      "status":"","
/*optional, string, remote control status: "notRelated"-not linked, "online", "offline", "heartbeatAbnormal"-heartbeat
exception*/
      "charge":"","
/*optional, string, state of charge: "normal", "lowPower"-low battery*/
      "chargeValue":0,
/*optional, int, power value; range: [0,100]*/
      "model": "",
/*optional, string, model*/
    }
  }]
}
```

A.3 JSON_EventNotificationAlert_AlarmEventInfo

JSON message about alarm or event information to be uploaded

```
{
  "EventNotificationAlert": {
    "channelID":"","
/*optional, dep, string, device channel No.*/
    "dateTime":"","
```

```

/*required, alarm/event triggered or occurred time, it must contain time zone information, e.g.,
"2017-04-22T15:39:01+08:00"*/
"activePostCount": ,
/*required, integer, alarm/event frequency*/
"eventType": "",
/*required, string, alarm/event types, see details in the Event Types*/
"eventState": "",
/*required, string, durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is
detected, the alarm/event information will be uploaded continuously unit the status is set to "inactive"*/
"eventDescription": "",
/*required, string, description*/
"devIndex": "",
/*optional, string, device ID (uuid/guid)*/
"...": "",
/*for different alarm/event types, the nodes are different, see the message examples below for details*/
"channelName": ""
/*required, string, camera name*/
}
}

```

See Also

Event Types

A.4 JSON_EventNotificationAlert_cancelVoiceTalkEvent

JSON message about details of two-way audio canceling alarm

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Event type, here it should be "cancelVoiceTalkEvent".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously unit the status is set to "inactive".

Field Name	Req. or Opt.	Date Type	Description
eventDescription	Req.	string	Event description, here it is "Two-way Audio Canceling Alarm".
devIndex	Opt.	string	Device ID (uuid/guid).
channelName	Req.	string	Camera name.
VoiceTalkEvent	Opt.	object	Details of the two-way audio canceling alarm.

Table A-1 VoiceTalkEvent

Field Name	Req. or Opt.	Date Type	Description
deviceName	Opt.	string	Device name.
target	Opt.	object	Target information.

Table A-2 target

Field Name	Req. or Opt.	Date Type	Description
buildingNumber	Opt.	int	Building No.
communityNumber	Opt.	string	Community No.
floorNumber	Opt.	int	Floor No.
periodNumber	Opt.	int	Phase No.
roomNumber	Opt.	int	Room No.
unitNumber	Opt.	int	Unit No.

Message Example

```
{
  "EventNotificationAlert": {
    "channelID": "1",
    "dateTime": "2018-03-13T19:42:27+08:00",
    "activePostCount": 1,
    "eventType": "cancelVoiceTalkEvent",
    "eventState": "active",
    "eventDescription": "Two-way Audio Canceling Alarm",
    "devIndex": "2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName": "Camera 01"
  },
  "VoiceTalkEvent": {
    "target": {
      "buildingNumber": 1,

```

```

    "communityNumber": "0",
    "floorNumber":22,
    ...
  }
  "deviceName ": ""
}
}
}


```

A.5 JSON_EventNotificationAlert_CIDAlarmMsg

JSON message about device heartbeat information (for encoding devices)

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
eventType	Req.	string	Event type, here it should be "CIDAlarm".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously until the status is set to "inactive".
eventDescription	Req.	string	Event description, here it is "CID alarm".
devIndex	Opt.	string	Device ID (uuid/guid).
CIDAlarm	Opt.	object	CID alarm information.
CIDCode	Opt.	string	CID alarm code is a 4-digit string, the last three digits indicate the event/ alarm code, and the first digit indicates the alarm status (1-triggered, 3-restored), e.g., "1103"-zone alarm triggered, "3103"-zone alarm restored, refer to <i>CID Code</i> for details.

Field Name	Req. or Opt.	Date Type	Description
			 Note For encoding devices, the CIDCode should be "1602" only.
CIDDescribe	Opt.	string	Description of CID code, the maximum description length is 127 bytes.
CIDParam	Opt.	string	CID parameter, which contains 8 sub parameters, i.e., userType, userNo, zoneNo, keyboardNo, videoChanNo, dskNo, moduleAddr, and userName; each sub parameter should be separated by commas.

Remarks

The descriptions of 8 sub parameters of CID parameter (**CIDParam**) are shown as below:

userType

User type, a 4-byte integer, values: 1-keyboard user, 2-network user, others-invalid

userNo

User No., a 4-byte integer, the value -1 is invalid.

zoneNo

Zone No., a 4-byte integer, the value -1 is invalid.

keyboardNo

Keyboard No., a 4-byte integer, the value -1 is invalid.

videoChanNo

Video channel No., a 4-byte integer, the value -1 is invalid.

dskNo

HDD No., a 4-byte integer, the value -1 is invalid.

moduleAddr

Module address, a 4-byte integer, the value -1 is invalid.

userName

User name, the maximum name length is 31 bytes, it can be set to "NONE".

Message Example

```
{
  "EventNotificationAlert":{
    "dateTime":"2018-01-21T12:50:39+08:00",
    "devIndex":"C5F2860E-8946-45FA-AC51-BD2429A82804",
    "eventType":"CIDAlarm",
    "eventState":"active",
    "eventDescription":"CID Alarm",
    "CIDAlarm":{
      "CIDCode":"1602",
      "CIDDescribe":"HeartBeat",
      "CIDParam":"-1,-1,-1,-1,-1,-1,NONE"
    }
  }
}
```

A.6 JSON_EventNotificationAlert_CidAlarmMsg

JSON message about CID (Contact ID) alarm details

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered alarm.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Event type, here it should be "CIDAlarm".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously unit the status is set to "inactive".
eventDescription	Req.	string	Event description, here it is "CID alarm".

Field Name	Req. or Opt.	Date Type	Description
devIndex	Opt.	string	Device ID (uuid/guid).
channelName	Req.	string	Camera name.
deviceID	Opt.	string	accountID
deviceSerial	Opt.	string	Device serial No.
CIDAlarm	Opt.	object	CID alarm information.

Table A-3 CIDAlarm

Field Name	Req. or Opt.	Date Type	Description
subSys	Opt.	int	Partition number, which generated the alarm reports: 0 (all reports). Value range: [0,32].
zoneNo	Opt.	int	Zone No.
CIDCode	Opt.	string	CID alarm code is a 4-digit string, the last three digits indicate the event/ alarm code, and the first digit indicates the alarm status (1-triggered, 3-restored), e.g., "1103"-zone alarm triggered, "3103"-zone alarm restored, refer to <i>CID Code</i> for details.
CIDType	Opt.	int	CID alarm type: 1 (zone alarm), 2 (video alarm), 3 (virtual zone alarm), 4 (duress alarm), 5 (exception alarm), 6 (operation alarm).
CIDDescribe	Opt.	string	Description of CID code, the maximum description length is 127 bytes.
timeZoneIdx	Opt.	int	Time zone index No.: 1 (GMT-12:00), 2 (GMT-11:00), 3 (GMT-10:00), ..., 14 (GMT-01:00), 15 (GMT), 16 (GMT +01:00), ..., 34 (GMT-13:00), 35 (GMT +14:00).
triggerTime	Opt.	string	CID alarm time, e.g., 2009-02-24 16:59:00.

Field Name	Req. or Opt.	Date Type	Description
uploadTime	Opt.	string	CID alarm uploaded time, e.g., 2009-02-24 16:59:00.
CIDParam	Opt.	string	CID parameter, which contains 8 sub parameters, i.e., userType, userNo, zoneNo, keyboardNo, videoChanNo, dskNo, moduleAddr, and userName; each sub parameter should be separated by comma.
UUID	Opt.	string	Alarm ID.
isVideo	Opt.	int	The file type: 0 (no video file, while picture may exist), 1 (AVI file), 2 (MP4 file).
isTalk	Opt.	int	Whether it supports two-way audio verification: 0 (not support), 1 (support).

Remarks

The descriptions of 8 sub parameters of CID parameter (**CIDParam**) are shown as below:

userType

User type, a 4-byte integer, values: 1-keyboard user, 2-network user, others-invalid

userNo

User No., a 4-byte integer, the value -1 is invalid.

zoneNo

Zone No., a 4-byte integer, the value -1 is invalid.

keyboardNo

Keyboard No., a 4-byte integer, the value -1 is invalid.

videoChanNo

Video channel No., a 4-byte integer, the value -1 is invalid.

dskNo

HDD No., a 4-byte integer, the value -1 is invalid.

moduleAddr

Module address, a 4-byte integer, the value -1 is invalid.

userName

User name, the maximum name length is 31 bytes, it can be set to "NONE".

See Also

Event Code List

Message Example

```
{
  "EventNotificationAlert":{
    "channelID":"1",
    "dateTime":"2018-01-21T12:50:39+08:00",
    "activePostCount":1,
    "eventType":"CIDAlarm",
    "eventState":"active",
    "eventDescription":"CID Alarm",
    "devIndex":"2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName":"Ipdome",
    "deviceID":"123456",
    "deviceSerial":"123456",
    "CIDAlarm":{
      "subSys":0,
      "zoneNo":1,
      "CIDCode":"1103",
      "CIDType":1,
      "CIDDescribe":"alarm",
      "timeZoneIdx":0,
      "triggerTime":"2009-02-24 16:59:00",
      "uploadTime":"2009-02-24 16:59:00",
      "CIDParam":"1,2,1,1,1,0,admin",
      "isVideo":1,
      "isTalk":0,
      "UUID":"be1ad122-2a53-11eb-aabf-4576d7843e50"
    }
  }
}
```

A.7 JSON_EventNotificationAlert_DeviceDeleted

JSON message about device deleted alarm information

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Device serial No.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format with time zone (i.e.,

Field Name	Req. or Opt.	Date Type	Description
			"yyyy-MM-ddThh:mm:ssZ"). The maximum length is 32 bytes.
eventType	Req.	string	Event type, here it should be "devicedeleted".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously unit the status is set to "inactive"
eventDescription	Req.	string	Event description, here it is "device deleted".
devIndex	Opt.	string	Device ID (uuid/guid)
channelName	Req.	string	Camera name

Message Example

```
{
  "EventNotificationAlert":{
    "channelID":"1",
    "dateTime":"2018-01-21T12:50:39+08:00",
    "activePostCount":1,
    "eventType":"devicedeleted",
    "eventState":"active",
    "eventDescription": "",
    "devIndex":"2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName":"lpdome"
  }
}
```

A.8 JSON_EventNotificationAlert_DevStatusChangedAlarmMsg

JSON message about details of device status changed alarm

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered alarm
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Event type, here it should be "devStatusChanged".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously unit the status is set to "inactive"
eventDescription	Req.	string	Event description, here it is "device status (online/offline) changed".
devIndex	Opt.	string	Device ID (uuid/guid)
channelName	Req.	string	Camera name
status	Req.	string	Device status: "online", "offline".

Message Example

```
{
  "EventNotificationAlert":{
    "channelID":"1",
    "dateTime":"2018-01-21T12:50:39+08:00",
    "activePostCount":1,
    "eventType":"devStatusChanged",
    "eventState":"active",
    "eventDescription":"device status about online or offline changed",
    "devIndex":"2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName":"Ipdome",
    "status":"online"
  }
}
```

A.9 JSON_EventNotificationAlert_DiskRecoverAlarmMsg

JSON message about disk recover alarm details

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered alarm
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Type of event that triggers alarm, here it should be "diskrecover".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously unit the status is set to "inactive"
eventDescription	Req.	string	Event description, here it is "diskrecover alarm".
devIndex	Opt.	string	Device ID (uuid/guid)
channelName	Req.	string	Camera name
zoneName	Opt.	string	Zone name
visualState	Opt.	string	Download status of the video for verification
VideoReview	Opt.	object	Video verification information
protocolType	Req.	string	Protocol type: "HikCIDProtocol"
HikCIDParams	Opt.	object	HikCIDProtocol parameters. It is valid when the value of protocolType is "HikCIDProtocol".

Field Name	Req. or Opt.	Date Type	Description
subSys	Opt.	int	Partition number, which generated the alarm reports: 0 (all reports). Value range: [0,32].
ZoneNo	Opt.	int	Zone number
videoURL	Opt.	string	Video URL

Message Example

```
{
  "EventNotificationAlert":{
    "channelID":"1",
    "dateTime":"2018-01-21T12:50:39+08:00",
    "activePostCount":1,
    "eventType":"diskrecover",
    "eventState":"active",
    "eventDescription":"diskrecover alarm",
    "devIndex":"2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName":"lpdome"
  },
  "VideoReview":{
    "protocolType":"HikCIDProtocol"
  },
  "HikCIDParams":{
    "subSys":0,
    "ZoneNo":1,
    "videoURL":"..."
  }
}
```

A.10 JSON_EventNotificationAlert_diskerror

JSON message about HDD error alarm details

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered alarm.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").

Field Name	Req. or Opt.	Date Type	Description
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Event type, here it should be "diskerror".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously until the status is set to "inactive".
eventDescription	Req.	string	Event description, here it is "diskerror alarm".
devIndex	Opt.	string	Device ID (uuid/guid).
channelName	Req.	string	Camera name.
zoneName	Opt.	string	Zone name
visualState	Opt.	string	Download status of the video for verification
VideoReview	Opt.	object	Video verification information.
protocolType	Req.	string	Protocol type: "HikCIDProtocol".
HikCIDParams	Opt.	object	HikCIDProtocol parameters. It is valid when the value of protocolType is "HikCIDProtocol".
subSys	Opt.	int	Partition number, which generated the alarm reports: 0 (all reports). Value range: [0,32].
ZoneNo	Opt.	int	Zone number.
videoURL	Opt.	string	Video URL.

Message Example

```
{
  "EventNotificationAlert":{
    "channelID":"1",
    "dateTime":"2018-01-21T12:50:39+08:00",
    "activePostCount":1,
    "eventType":"diskerror",
```



```

"eventState":"active",
"eventDescription":"diskerror alarm",
"devIndex":"2cd6716d-767f-4756-ac55-50276a5e3b4a",
"channelName":"Ipdome",
"VideoReview":{
  "protocolType":"HikCIDProtocol"
  "HikCIDParams":{
    "subSys":0,
    "ZoneNo":1,
    "videoURL":"..."
  }
}
}
}
}

```

A.11 JSON_EventNotificationAlert_diskfull

JSON message about HDD full alarm details

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
ipAddress	Opt.	string	IPv4 address.
ipv6Address	Opt.	string	IPv6 address.
portNo	Opt.	string	Port number.
protocolType	Opt.	string	Protocol type: "HTTP", "HTTPS".
macAddress	Opt.	string	Device Mac address.
channelID	Req.	string	Channel No. of the device that triggered alarm.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Event type, here it should be "diskfull".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/

Field Name	Req. or Opt.	Date Type	Description
			event information will be uploaded continuously unit the status is set to "inactive".
eventDescription	Req.	string	Event description, here it is "diskfull alarm".
devIndex	Opt.	string	Device ID (uuid/guid).
channelName	Req.	string	Camera name.
zoneName	Opt.	string	Zone name
visualState	Opt.	string	Download status of the video for verification
VideoReview	Opt.	object	Video verification information.
protocolType	Req.	string	Protocol type: "HikCIDProtocol".
HikCIDParams	Opt.	object	HikCIDProtocol parameters. It is valid when the value of protocolType is "HikCIDProtocol".
subSys	Opt.	int	Partition number, which generated the alarm reports: 0 (all reports). Value range: [0,32].
ZoneNo	Opt.	int	Zone number.
videoURL	Opt.	string	Video URL.

Message Example

```
{
  "EventNotificationAlert":{
    "channelID":"1",
    "dateTime":"2018-01-21T12:50:39+08:00",
    "activePostCount":1,
    "eventType":"diskfull",
    "eventState":"active",
    "eventDescription":"diskfull alarm",
    "devIndex":"2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName":"lpdome",
    "VideoReview":{
      "protocolType":"HikCIDProtocol"
    },
    "HikCIDParams":{
      "subSys":0,
      "ZoneNo":1,
      "videoURL":"..."
    }
  }
}
```

```
}  
}  
}  
}
```

A.12 JSON_EventNotificationAlert_HeartbeatInfo

JSON message about heartbeat information to be uploaded

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Opt.	string	Channel No. of the device that triggered alarm.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Event type, here it should be "heartBeat".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously unit the status is set to "inactive".
eventDescription	Req.	string	Event description, here it is "Heartbeat".

Remarks

You can calculate the arming duration according to the value of node **activePostCount** and the heartbeat interval.

Example

Message Example of Uploading Heartbeat Information

```
{  
  "EventNotificationAlert":{  
    "channelID":"1",  
    "dateTime":"2017-04-22T15:39:01+08:00",  
    "activePostCount":2,  
  }  
}
```

```
"eventType":"heartBeat",
"eventState":"active",
"eventDescription":"Heartbeat"
}
}
```

A.13 JSON_EventNotificationAlert_FallingDownAlarmMsg

JSON message about falling down alarm details

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered alarm.
dateTime	Req.	ISO 8601	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Type of event that triggers alarm, here it should be "fallingDown".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously until the status is set to "inactive".
eventDescription	Req.	string	Event description, here it is "People Falling Down Detection Event".
devIndex	Opt.	string	Device ID (uuid/guid).
channelName	Req.	string	Camera name.

Message Example

```
{
  "EventNotificationAlert":{
    "channelID":"0",
    "dateTime":"2018-03-13T19:42:27+08:00",
    "activePostCount":1,
    "eventType":"fallingDown",
    "eventState":"active",
```

```
"eventDescription":"People Falling Down Detection Event",
"devIndex":"2cd6716d-767f-4756-ac55-50276a5e3b4a",
"channelName":""
}
}
```

A.14 JSON_EventNotificationAlert_fieldddetection

JSON message about intrusion alarm details

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered alarm.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Type of event that triggers alarm, here it should be "fieldddetection".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously unit the status is set to "inactive".
eventDescription	Req.	string	Event description, here it is "fieldddetection alarm".
devIndex	Opt.	string	Device ID (uuid/guid).
channelName	Req.	string	Camera name.
zoneName	Opt.	string	Zone name
visualState	Opt.	string	Download status of the video for verification
DetectionRegionList	Opt.	object	Detection region, this node is valid in expert mode.

Field Name	Req. or Opt.	Date Type	Description
DetectionRegionEntry	Req.	list	Detection region information.
regionID	Req.	string	Detection region ID.
sensitivityLevel	Opt.	int	Sensitivity. Value range: [0,100].
RegionCoordinatesList	Opt.	list	Detection region coordinates.
RegionCoordinates			
positionX	Req.	int	X-coordinate of a vertex on the rule frame, which is between 0 and 1000.
positionY	Req.	int	Y-coordinate of a vertex on the rule frame, which is between 0 and 1000.
detectionTarget	Opt.	string	Target type: "human", "vehicle", "others".
TargetRect	Opt.		Coordinates of target.
X	Req.	float	X-coordinate.
Y	Req.	float	Y-coordinate.
width	Req.	float	Width of target.
height	Req.	float	Height of target.
VideoReview	Opt.	object	Video verification information.
protocolType	Req.	string	Protocol type: "HikCIDProtocol".
HikCIDParams	Opt.	object	HikCIDProtocol parameters. It is valid when the value of protocolType is "HikCIDProtocol".
subSys	Opt.	int	Partition number, which generated the alarm reports: 0 (all reports). Value range: [0,32].
ZoneNo	Opt.	int	Zone number.
videoURL	Opt.	string	Video URL.

Sample Message of Intrusion Alarm Details

```
{
  "EventNotificationAlert":{
    "channelID":"1",
    "dateTime":"2018-01-21T12:50:39+08:00",
    "activePostCount":1,
    "eventType":"fielddetection",
    "eventState":"active",
    "eventDescription":"",
    "devIndex":"2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName":"Ipdome",
    "DetectionRegionList":[{
      "DetectionRegionEntry":{
        "regionID":"1",
        "sensitivityLevel":50,
        "RegionCoordinatesList":[{
          "RegionCoordinates":{
            "positionX":0,
            "positionY":0
          },
          "RegionCoordinates":{
            "positionX":0,
            "positionY":100
          },
          "RegionCoordinates":{
            "positionX":100,
            "positionY":100
          },
          "RegionCoordinates":{
            "positionX":100,
            "positionY":0
          }
        ]
      },
      "detectionTarget":"human",
      "TargetRect":{
        "X":0,
        "Y":1,
        "width":0.5,
        "height":0.5
      }
    }
  ]
}
"VideoReview":{
  "protocolType":"HikCIDProtocol"
  "HikCIDParams":{
    "subSys":0,
    "ZoneNo":1,
    "videoURL":"..."
  }
}
```

```
}  
}
```

A.15 JSON_EventNotificationAlert_fireDetection

JSON message about fire detection alarm details

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered alarm.
dateTime	Req.	ISO 8601	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Type of event that triggers alarm, here it should be "fireDetection".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously until the status is set to "inactive".
eventDescription	Req.	string	Event description.
devIndex	Opt.	string	Device ID (uuid/guid).
channelName	Req.	string	Camera name.
zoneName	Opt.	string	Zone name
visualState	Opt.	string	Download status of the video for verification
subSys	Opt.	int	Partition number, which generated the alarm reports: 0 (all reports). Value range: [0,32].
ZoneNo	Opt.	int	Zone number
DetectionRegionList	Opt.	object	Detection region.

Field Name	Req. or Opt.	Date Type	Description
detectionPicturesNumber	Opt.	int	Number of detected pictures. Value of range: [1, 2]
visibleLightURL	Opt.	string	Visible light picture URL.
thermalURL	Opt.	string	Thermal imaging picture URL.
URLCertificationType	Opt.	string	Picture URL authentication method: "no" (no authentication), "digest" (digest authentication).
VideoReview	Opt.	object	Video verification information.

Table A-4 DetectionRegionEntry

Field Name	Req. or Opt.	Date Type	Description
regionID	Req.	string	Area ID.
RegionCoordinatesList	Opt.	object	Rule area
FireDetection	Opt.	object	Fire detection information.

Table A-5 FireDetection

Field Name	Req. or Opt.	Date Type	Description
FireRegion	Opt.	object	Fire detection frame.
HighestPoint	Opt.	object	Coordinates of highest temperature point in the fire detection frame.
temperatureUnit	Opt.	string	Temperature unit.
fireMaxTemperature	Opt.	int	The highest temperature; value range: [300, 4000]; unit: °C.
targetDistance	Opt.	int	Target distance; value range: [100, 10000]; unit: m.
AbsoluteHigh	Opt.	object	PTZ position information.
lookDownUpAngle	Opt.	float	Device tilting angle with high accuracy.
PTZAbsoluteEx	Opt.	object	Extension of PTZ position information. It is accurate to three decimal places.

Table A-6 FireRegion

Field Name	Req. or Opt.	Date Type	Description
X	Req.	int	Target x-coordinates. Value range: [0, 1000].
Y	Req.	int	Target y-coordinates. Value range: [0, 1000].
width	Req.	int	Target width. Value range: [0, 1000].
height	Req.	int	Target height. Value range: [0, 1000].

Table A-7 HighestPoint

Field Name	Req. or Opt.	Date Type	Description
X	Req.	int	Target x-coordinates. Value range: [0, 1000].
Y	Req.	int	Target y-coordinate. Value range: [0, 1000].

Table A-8 AbsoluteHigh

Field Name	Req. or Opt.	Date Type	Description
elevation	Opt.	int	Panning value, range: [-900, 2700].
azimuth	Opt.	int	Tilting value, range: [0, 3600].
absoluteZoom	Opt.	int	Zooming in/out value: [0, 1000].

Table A-9 PTZAbsoluteEx

Field Name	Req. or Opt.	Date Type	Description
elevation	Opt.	int	Panning value, range: [-90.000, 270.000].
azimuth	Opt.	int	Tilting value, range: [0, 360.000].
absoluteZoom	Opt.	int	Zooming in/out value: [0, 10000.00].

Message Example

```
{
  "EventNotificationAlert": {
    "channelID": "1",
    "dateTime": "2021-11-22T11:38:41+08:00",
    "activePostCount": "2",
    "eventType": "fireDetection",
    "eventState": "active",
    "eventDescription": "fireDetection alarm",
    "DetectionRegionList": {
      "DetectionRegionEntry": {
```

```
"regionID": "1",
"RegionCoordinatesList": {
  "RegionCoordinates": [{
    "positionX": "388",
    "positionY": "694"
  },
  {
    "positionX": "523",
    "positionY": "694"
  },
  {
    "positionX": "523",
    "positionY": "999"
  },
  {
    "positionX": "388",
    "positionY": "829"
  }
]
},
"FireDetection": {
  "FireRegion": {
    "x": "388",
    "y": "694",
    "width": "135",
    "height": "305"
  },
  "HighestPoint": {
    "x": "486",
    "y": "937"
  },
  "temperatureUnit": "celsius",
  "fireMaxTemperature": "115",
  "targetDistance": "-1",
  "AbsoluteHigh": {
    "elevation": "0",
    "azimuth": "0",
    "absoluteZoom": "0"
  }
}
},
"VideoReview": {
  "HikCIDParams": {
    "subSys": 0,
    "ZoneNo": 1,
    "videoURL": "..."
  },
  "protocolType": "HikCIDProtocol"
},
"devIndex": "C5F2860E-8946-45FA-AC51-BD2429A82804",
"channelName": "Camera 01",
```

```
"detectionPicturesNumber": "1",
"thermalURL": "...",
"deviceSerial": "E60250720"
}
}
```

A.16 JSON_EventNotificationAlert_IO

JSON message about IO alarm details

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered alarm
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Event type, here it should be "IO".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously unit the status is set to "inactive"
eventDescription	Req.	string	Event description, here it is "IO alarm".
devIndex	Opt.	string	Device ID (uuid/guid)
inputIOPortID	Opt.	int	IO input port ID
channelName	Req.	string	Camera name
zoneName	Opt.	string	Zone name
visualState	Opt.	string	Download status of the video for verification
VideoReview	Opt.	object	Video verification information

Field Name	Req. or Opt.	Date Type	Description
protocolType	Req.	string	Protocol type: "HikCIDProtocol"
HikCIDParams	Opt.	object	HikCIDProtocol parameters. It is valid when the value of protocolType is "HikCIDProtocol".
subSys	Opt.	int	Partition number, which generated the alarm reports: 0 (all reports). Value range: [0,32].
ZoneNo	Opt.	int	Zone number
videoURL	Opt.	string	Video URL

Message Example

```
{
  "EventNotificationAlert":{
    "channelID":"1",
    "dateTime":"2018-03-13T19:42:27+08:00",
    "activePostCount":1,
    "eventType":"IO",
    "eventState":"active",
    "eventDescription":"IO alarm",
    "devIndex":"2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "inputIOPortID":1,
    "channelName":"Camera 01",
    "VideoReview":{
      "protocolType":"HikCIDProtocol"
      "HikCIDParams":{
        "subSys":0,
        "ZoneNo":1,
        "videoURL":"..."
      }
    }
  }
}
```

A.17 JSON_EventNotificationAlert_linedetection

JSON message about line crossing alarm details

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered alarm.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Type of event that triggers alarm, here it should be "linedetection".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously unit the status is set to "inactive".
eventDescription	Req.	string	Event description, here it is "linedetection alarm".
devIndex	Opt.	string	Device ID (uuid/guid).
channelName	Req.	string	Camera name.
zoneName	Opt.	string	Zone name
visualState	Opt.	string	Download status of the video for verification
DetectionRegionList	Opt.	object	Detection region, this node is valid in expert mode.
DetectionRegionEntry	Req.	list	Detection region information.
regionID	Req.	string	Detection region ID.
sensitivityLevel	Opt.	int	Sensitivity. Value range: [0,100].
RegionCoordinatesList	Opt.	list	Detection region coordinates.
RegionCoordinates			

Field Name	Req. or Opt.	Date Type	Description
positionX	Req.	int	X-coordinate of a vertex on the rule frame, which is between 0 and 1000.
positionY	Req.	int	Y-coordinate of a vertex on the rule frame, which is between 0 and 1000.
detectionTarget	Opt.	string	Target type: "human", "vehicle", "others".
TargetRect	Opt.		Coordinates of target.
X	Req.	float	X-coordinate.
Y	Req.	float	Y-coordinate.
width	Req.	float	Width of target.
height	Req.	float	Height of target.
VideoReview	Opt.	object	Video verification information.
protocolType	Req.	string	Protocol type: "HikCIDProtocol".
HikCIDParams	Opt.	object	HikCIDProtocol parameters. It is valid when the value of protocolType is "HikCIDProtocol".
subSys	Opt.	int	Partition number, which generated the alarm reports: 0 (all reports). Value range: [0,32].
ZoneNo	Opt.	int	Zone number.
videoURL	Opt.	string	Video URL.

Example

Sample Message of Line Crossing Alarm Details

```
{
  "EventNotificationAlert":{
    "channelID":"1",
    "dateTime":"2018-01-21T12:50:39+08:00",
    "activePostCount":1,
    "eventType":"linedetection",
    "eventState":"active",
    "eventDescription":"",
    "devIndex":"2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName":"Ipdome",
    "DetectionRegionList":[{
      "DetectionRegionEntry":{
        "regionID":"1",
```

```
"sensitivityLevel":50,
"RegionCoordinatesList":[{"
  "RegionCoordinates":{
    "positionX":0,
    "positionY":0
  },
  "RegionCoordinates":{
    "positionX":0,
    "positionY":100
  },
  "RegionCoordinates":{
    "positionX":100,
    "positionY":100
  },
  "RegionCoordinates":{
    "positionX":100,
    "positionY":0
  }
}],
"detectionTarget":"human",
"TargetRect":{
  "X":0,
  "Y":1,
  "width":0.5,
  "height":0.5
}
}
}
}
}
"VideoReview":{
  "protocolType":"HikCIDProtocol"
  "HikCIDParams":{
    "subSys":0,
    "ZoneNo":1,
    "videoURL":"..."
  }
}
}
```

A.18 JSON_EventNotificationAlert_VMD

JSON message about motion detection alarm details

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered alarm.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Type of event that triggers alarm, here it should be "VMD".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously unit the status is set to "inactive".
eventDescription	Req.	string	Event description, here it is "VMD alarm".
devIndex	Opt.	string	Device ID (uuid/guid).
channelName	Req.	string	Camera name.
zoneName	Opt.	string	Zone name
visualState	Opt.	string	Download status of the video for verification
DetectionRegionList	Opt.	object	Detection region, this node is valid in expert mode.
DetectionRegionEntry	Req.	list	Detection region information.
regionID	Req.	string	Detection region ID.
sensitivityLevel	Req.	int	Sensitivity. Value range: [0,100].
RegionCoordinatesList	Req.	list	Detection region coordinates.
RegionCoordinates	Req.		

Field Name	Req. or Opt.	Date Type	Description
positionX	Req.	int	X-coordinate of a vertex on the rule frame, which is between 0 and 1000.
positionY	Req.	int	Y-coordinate of a vertex on the rule frame, which is between 0 and 1000.
VideoReview	Opt.	object	Video verification information.
protocolType	Req.	string	Protocol type: "HikCIDProtocol".
HikCIDParams	Opt.	object	HikCIDProtocol parameters. It is valid when the value of protocolType is "HikCIDProtocol".
subSys	Opt.	int	Partition number, which generated the alarm reports: 0 (all reports). Value range: [0,32].
ZoneNo	Opt.	int	Zone number.
videoURL	Opt.	string	Video URL.

Message Example (Normal Mode)

```
{
  "EventNotificationAlert":{
    "channelID": "1",
    "dateTime": "2018-03-13T19:42:27+08:00",
    "activePostCount": 1,
    "eventType": "VMD",
    "eventState": "active",
    "eventDescription": "VMD alarm",
    "devIndex": "2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName": "Camera 01",
    "VideoReview":{
      "HikCIDParams":{
        "subSys": 0,
        "ZoneNo": 1,
        "videoURL": "..."
      }
    }
  }
}
```

Message Example (Expert Mode)

```
{
  "EventNotificationAlert":{
    "channelID": "1",
```

```
"dateTime":"2018-03-13T20:36:34+08:00",
"activePostCount":1,
"eventType":"VMD",
"eventState":"active",
"eventDescription":"VMD alarm",
"detectionRegionList":{
  "detectionRegionEntry":{
    "regionID":"1",
    "sensitivityLevel":50,
    "regionCoordinatesList":{
      "regionCoordinates":{
        "positionX":216,
        "positionY":216
      },
      {
        "positionX":756,
        "positionY":756
      },
      {
        "positionX":756,
        "positionY":756
      },
      {
        "positionX":216,
        "positionY":216
      }
    ]
  }
},
"devIndex":"2cd6716d-767f-4756-ac55-50276a5e3b4a",
"channelName":"Camera 01",
"videoReview":{
  "protocolType":"HikCIDProtocol",
  "hikCIDParams":{
    "subSys": 0,
    "zoneNo": 1,
    "videoURL":"..."
  }
}
}
```

A.19 JSON_EventNotificationAlert_RecordExceptionAlarmMsg

JSON message about record exception alarm details

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered alarm
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Event type, here it should be "recordException".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously unit the status is set to "inactive"
eventDescription	Req.	string	Event description, here it is "recordException alarm".
devIndex	Opt.	string	Device ID (uuid/guid)
channelName	Req.	string	Camera name
zoneName	Opt.	string	Zone name
visualState	Opt.	string	Download status of the video for verification
VideoReview	Opt.	object	Video verification information
protocolType	Req.	string	Protocol type: "HikCIDProtocol"
HikCIDParams	Opt.	object	HikCIDProtocol parameters. It is valid when the value of protocolType is "HikCIDProtocol".
subSys	Opt.	int	Partition number, which generated the alarm reports: 0 (all reports). Value range: [0,32].
ZoneNo	Opt.	int	Zone number
videoURL	Opt.	string	Video URL

Message Example

```
{
  "EventNotificationAlert":{
    "channelID":"1",
    "dateTime":"2018-01-21T12:50:39+08:00",
    "activePostCount":1,
    "eventType":"recordException",
    "eventState":"active",
    "eventDescription":"recordException alarm",
    "devIndex":"2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName":"Ipdome"
    "VideoReview":{
      "protocolType":"HikCIDProtocol"
      "HikCIDParams":{
        "subSys":0,
        "ZoneNo":1,
        "videoURL":"..."
      }
    }
  }
}
```

A.20 JSON_EventNotificationAlert_RegionEntranceAlarmMsg

JSON message about region entrance alarm details

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered alarm.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Type of event that triggers alarm, here it should be "regionEntrance".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/

Field Name	Req. or Opt.	Data Type	Description
			event information will be uploaded continuously until the status is set to "inactive".
eventDescription	Req.	string	Event description, here it is "regionEntrance alarm".
devIndex	Opt.	string	Device ID (uuid/guid).
channelName	Req.	string	Camera name.
zoneName	Opt.	string	Zone name
visualState	Opt.	string	Download status of the video for verification
DetectionRegionList	Opt.	object	Detection region, this node is valid in expert mode.
DetectionRegionEntry	Req.	list	Detection region information.
regionID	Req.	string	Detection region ID.
sensitivityLevel	Opt.	int	Sensitivity. Value range: [0,100].
RegionCoordinatesList	Opt.	list	Detection region coordinates.
RegionCoordinates			
positionX	Req.	int	X-coordinate of a vertex on the rule frame, which is between 0 and 1000.
positionY	Req.	int	Y-coordinate of a vertex on the rule frame, which is between 0 and 1000.
detectionTarget	Opt.	string	Target type: "human", "vehicle", "others".
TargetRect	Opt.		Coordinates of target.
X	Req.	float	X-coordinate.
Y	Req.	float	Y-coordinate.
width	Req.	float	Width of target.
height	Req.	float	Height of target.

Field Name	Req. or Opt.	Date Type	Description
VideoReview	Opt.	object	Video verification information.
protocolType	Req.	string	Protocol type: "HikCIDProtocol".
HikCIDParams	Opt.	object	HikCIDProtocol parameters. It is valid when the value of protocolType is "HikCIDProtocol".
subSys	Opt.	int	Partition number, which generated the alarm reports: 0 (all reports). Value range: [0,32].
ZoneNo	Opt.	int	Zone number.
videoURL	Opt.	string	Video URL.

Example

Sample Message of Region Entrance Alarm Details

```
{
  "EventNotificationAlert":{
    "channelID":"1",
    "dateTime":"2018-01-21T12:50:39+08:00",
    "activePostCount":1,
    "eventType":"regionEntrance",
    "eventState":"active",
    "eventDescription": "",
    "devIndex":"2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName":"Ipdome",
    "DetectionRegionList":{
      "DetectionRegionEntry":{
        "regionID":"1",
        "sensitivityLevel":50,
        "RegionCoordinatesList":{
          "RegionCoordinates":{
            "positionX":0,
            "positionY":0
          },
          "RegionCoordinates":{
            "positionX":0,
            "positionY":100
          },
          "RegionCoordinates":{
            "positionX":100,
            "positionY":100
          },
          "RegionCoordinates":{
            "positionX":100,
            "positionY":0
          }
        }
      }
    }
  }
}
```

```
}  
},  
"detectionTarget":"human",  
"TargetRect":{  
  "X":0,  
  "Y":1,  
  "width":0.5,  
  "height":0.5  
}  
}  
}}  
"VideoReview":{  
  "protocolType":"HikCIDProtocol"  
  "HikCIDParams":{  
    "subSys":0,  
    "ZoneNo":1,  
    "videoURL":"..."  
  }  
}  
}  
}
```

A.21 JSON_EventNotificationAlert_RegionExitingAlarmMsg

JSON message about region exiting alarm details

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered alarm.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Type of event that triggers alarm, here it should be "regionExiting".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded

Field Name	Req. or Opt.	Date Type	Description
			continuously unit the status is set to "inactive".
eventDescription	Req.	string	Event description, here it is "regionExiting alarm".
devIndex	Opt.	string	Device ID (uuid/guid).
channelName	Req.	string	Camera name.
zoneName	Opt.	string	Zone name
visualState	Opt.	string	Download status of the video for verification
DetectionRegionList	Opt.	object	Detection region, this node is valid in expert mode.
DetectionRegionEntry	Req.	list	Detection region information.
regionID	Req.	string	Detection region ID.
sensitivityLevel	Opt.	int	Sensitivity. Value range: [0,100].
RegionCoordinatesList	Opt.	list	Detection region coordinates.
RegionCoordinates			
positionX	Req.	int	X-coordinate of a vertex on the rule frame, which is between 0 and 1000.
positionY	Req.	int	Y-coordinate of a vertex on the rule frame, which is between 0 and 1000.
detectionTarget	Opt.	string	Target type: "human", "vehicle", "others".
TargetRect	Opt.		Coordinates of target.
X	Req.	float	X-coordinate.
Y	Req.	float	Y-coordinate.
width	Req.	float	Width of target.
height	Req.	float	Height of target.
VideoReview	Opt.	object	Video verification information.

Field Name	Req. or Opt.	Date Type	Description
protocolType	Req.	string	Protocol type: "HikCIDProtocol".
HikCIDParams	Opt.	object	HikCIDProtocol parameters. It is valid when the value of protocolType is "HikCIDProtocol".
subSys	Opt.	int	Partition number, which generated the alarm reports: 0 (all reports). Value range: [0,32].
ZoneNo	Opt.	int	Zone number.
videoURL	Opt.	string	Video URL.

Example

Sample Message of Region Exiting Alarm Details

```
{
  "EventNotificationAlert":{
    "channelID":"1",
    "dateTime":"2018-01-21T12:50:39+08:00",
    "activePostCount":1,
    "eventType":"regionExiting",
    "eventState":"active",
    "eventDescription": "",
    "devIndex":"2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName":"!pdome",
    "DetectionRegionList":[{
      "DetectionRegionEntry":{
        "regionID":"1",
        "sensitivityLevel":50,
        "RegionCoordinatesList":[{
          "RegionCoordinates":{
            "positionX":0,
            "positionY":0
          },
          "RegionCoordinates":{
            "positionX":0,
            "positionY":100
          },
          "RegionCoordinates":{
            "positionX":100,
            "positionY":100
          },
          "RegionCoordinates":{
            "positionX":100,
            "positionY":0
          }
        }
      }
    }],
  },
}
```

```
"detectionTarget":"human",
  "TargetRect":{
    "X":0,
    "Y":1,
    "width":0.5,
    "height":0.5
  }
}
}}
"VideoReview":{
  "protocolType":"HikCIDProtocol"
  "HikCIDParams":{
    "subSys":0,
    "ZoneNo":1,
    "videoURL":"..."
  }
}
}
```

A.22 JSON_EventNotificationAlert_requestVoiceTalkEvent

JSON message about details of two-way audio request alarm

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered alarm.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Event type, here it should be "requestVoiceTalkEvent".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously until the status is set to "inactive".

Field Name	Req. or Opt.	Date Type	Description
eventDescription	Req.	string	Event description, here it is "Two-way Audio Request Alarm".
devIndex	Opt.	string	Device ID (uuid/guid).
channelName	Req.	string	Camera name.
VoiceTalkEvent	Opt.	object	Details of the two-way audio request alarm.

Table A-10 VoiceTalkEvent

Field Name	Req. or Opt.	Date Type	Description
deviceName	Opt.	string	Device name.
target	Opt.	object	Target information.

Table A-11 target

Field Name	Req. or Opt.	Date Type	Description
buildingNumber	Opt.	int	Building No.
communityNumber	Opt.	string	Community No.
floorNumber	Opt.	int	Floor No.
periodNumber	Opt.	int	Phase No.
roomNumber	Opt.	int	Room No.
unitNumber	Opt.	int	Unit No.

Message Example

```
{
  "EventNotificationAlert": {
    "channelID": "1",
    "dateTime": "2018-03-13T19:42:27+08:00",
    "activePostCount": 1,
    "eventType": "requestVoiceTalkEvent",
    "eventState": "active",
    "eventDescription": "Two-way Audio Request Alarm",
    "devIndex": "2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName": "Camera 01"
  },
  "VoiceTalkEvent": {
    "target": {
      "buildingNumber": 1,

```

```

    "communityNumber": "0",
    "floorNumber": 22,
    ...
  }
  "deviceName ": ""
}
}
}

```

A.23 JSON_EventNotificationAlert_TDA

JSON message about temperature difference alarm details

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered alarm.
dateTime	Req.	ISO 8601	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Type of event that triggers alarm, here it should be "TDA".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously until the status is set to "inactive".
eventDescription	Req.	string	Event description.
devIndex	Opt.	string	Device ID (uuid/guid).
channelName	Req.	string	Camera name.
zoneName	Opt.	string	Zone name
visualState	Opt.	string	Download status of the video for verification

Field Name	Req. or Opt.	Date Type	Description
subSys	Opt.	int	Partition number, which generated the alarm reports: 0 (all reports). Value range: [0,32].
ZoneNo	Opt.	int	Zone number
DetectionRegionList	Opt.	object	Detection region.
detectionPicturesNumber	Opt.	int	Number of detected pictures. Value of range: [1, 2]
visibleLightURL	Opt.	string	Visible light picture URL.
thermalURL	Opt.	string	Thermal imaging picture URL.
thermalInfoURL	Opt.	string	Additional information data of the thermal imaging picture.
URLCertificationType	Opt.	string	Picture URL authentication method: "no" (no authentication), "digest" (digest authentication).
VideoReview	Opt.	object	Video verification information.

Table A-12 DetectionRegionEntry

Field Name	Req. or Opt.	Date Type	Description
AlarmRuleList	Opt.	array	Alarm rule list.
TDA	Opt.	object	Temperature difference alarm information.

Table A-13 AlarmRuleList

Field Name	Req. or Opt.	Date Type	Description
alarmID	Req.	int	Rule ID of temperature difference alarm.
RegionCoordinatesList	Opt.	object	Rule area.

Table A-14 TDA

Field Name	Req. or Opt.	Date Type	Description
thermometryUnit	Req.	string	Temperature unit: "celsius, fahrenheit, kelvin".
ruleTemperatureDiff	Opt.	float	Configured temperature difference threshold, which is accurate to one decimal place.
currTemperatureDiff	Opt.	float	Current temperature difference, which is accurate to one decimal place.
alarmType	Opt.	string	Alarm type: "MaxTemperature" (highest temperature), "MinTemperature" (lowest temperature), "AverageTemperature" (average temperature).
alarmRule	Opt.	string	Alarm rule: "greater" (higher than), "less" (lower than).
toleranceTemperature	Opt.	float	Temperature tolerance, which is accurate to one decimal place.
AbsoluteHigh	Opt.	object	PTZ coordinates.
presetNo	Opt.	int	Preset No.
alarmFilteringTime	Opt.	int	Temperature measurement alarm dwell time.
alertFilteringTime	Opt.	int	Temperature pre-alarm dwell time.
sensorInfo	Opt.	object	Sensor alarm information.

Message Example

```
{
  "DetectionRegionList": [{
    "DetectionRegionEntry": {
      "AlarmRuleList": [{
        "RegionCoordinatesList": [{
          "RegionCoordinates": {
            "positionX": 128.0,
            "positionY": 263.0
          }
        }
      ],
      {
        "RegionCoordinates": {
          "positionX": 120.0,
          "positionY": 563.0
        }
      }
    }
  ]
}
```

```
    }
  },
  {
    "RegionCoordinates": {
      "positionX": 899.0,
      "positionY": 589.0
    }
  },
  {
    "RegionCoordinates": {
      "positionX": 935.0,
      "positionY": 263.0
    }
  },
  {
    "RegionCoordinates": {
      "positionX": 935.0,
      "positionY": 269.0
    }
  }
],
"alarmID": 1
},
{
  "RegionCoordinatesList": [{
    "RegionCoordinates": {
      "positionX": 631.0,
      "positionY": 656.0
    }
  },
  {
    "RegionCoordinates": {
      "positionX": 121.0,
      "positionY": 654.0
    }
  },
  {
    "RegionCoordinates": {
      "positionX": 116.0,
      "positionY": 963.0
    }
  },
  {
    "RegionCoordinates": {
      "positionX": 641.0,
      "positionY": 957.0
    }
  }
],
"alarmID": 2
}
```



```
"TDA": {
  "AbsoluteHigh": {
    "absoluteZoom": 0.1,
    "azimuth": 0.0,
    "elevation": 0.0
  },
  "alarmRule": "less",
  "alarmType": "MinTemperature",
  "currTemperatureDiff": -0.1,
  "presetNo": 1,
  "ruleTemperatureDiff": 2.0,
  "thermometryUnit": "celsius",
  "toleranceTemperature": 0.0
}
}},
"VideoReview": {
  "HikCIDParams": {
    "subSys": 0,
    "ZoneNo": 1,
    "videoURL": "..."
  },
  "protocolType": "HikCIDProtocol"
},
"activePostCount": 101,
"channelID": 1,
"channelName": "Camera 01",
"dateTime": "2021-11-19T17:23:08+08:00",
"detectionPicturesNumber": 1,
"eventDescription": "Temperature Diff Alarm",
"eventState": "active",
"eventType": "TDA",
"thermalURL": "..."
}
```

A.24 JSON_EventNotificationAlert_TMA

JSON message about temperature measurement alarm

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered alarm.
dateTime	Req.	ISO 8601	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Type of event that triggers alarm, here it should be "TMA".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously until the status is set to "inactive".
eventDescription	Req.	string	Event description.
devIndex	Opt.	string	Device ID (uuid/guid).
channelName	Req.	string	Camera name.
visualState	Opt.	string	Download status of the video for verification
subSys	Opt.	int	Partition number, which generated the alarm reports: 0 (all reports). Value range: [0,32].
zoneName	Opt.	string	Zone name
ZoneNo	Opt.	int	Zone number
DetectionRegionList	Opt.	object	Detection region.
detectionPicturesNumber	Opt.	int	Number of detected pictures. Value of range: [1, 2]
visibleLightURL	Opt.	string	Visible light picture URL.
thermalURL	Opt.	string	Thermal imaging picture URL.
thermalInfoURL	Opt.	string	Additional information data of the thermal imaging picture.

Field Name	Req. or Opt.	Date Type	Description
URLCertificationType	Opt.	string	Picture URL authentication method: "no" (no authentication), "digest" (digest authentication).
VideoReview	Opt.	object	Video verification information.

Table A-15 DetectionRegionEntry

Field Name	Req. or Opt.	Date Type	Description
regionID	Opt.	string	Area ID.
RegionCoordinatesList	Opt.	object	Rule area.
TMA	Opt.	object	Temperature measurement alarm information.

Table A-16 TMA

Field Name	Req. or Opt.	Date Type	Description
thermometryUnit	Req.	string	Temperature unit: "celsius, fahrenheit, kelvin".
ruleTemperature	Req.	float	Configured rule temperature.
currTemperature	Req.	float	Current temperature.
ruleCalibType	Req.	string	Rule calibration type: "region", "line", "point".
ruleType	Req.	string	Alarm type: "highest temp is higher than" (the highest temperature is higher than), "lowest temp is higher than" (the lowest temperature is higher than), "average temp is higher than" (the average temperature is higher than), "temp diff is higher than" (the temperature difference is higher than), "highest temp is lower than" (the highest temperature is lower than),

Field Name	Req. or Opt.	Date Type	Description
			"lowest temp is lower than" (the lowest temperature is lower than), "average temp is lower than" (the average temperature is lower than), "temp diff is lower than" (the temperature difference is lower than), "temperatureSuddenIncrease" (temperature sudden increase), "temperatureSuddenDecrease" (temperature sudden decrease).
MaximumTemperaturePoint	Opt.	object	Coordinates of highest temperature point for line/frame temperature measurement.
AbsoluteHigh	Opt.	object	PTZ coordinates.
presetNo	Opt.	int	Preset No.
temperatureSuddenChangeCycle	Opt.	int	Cycle of temperature sudden change.
temperatureSuddenChangeValue	Opt.	float	Value of temperature sudden change. It is accurate to one decimal place.
alarmFilteringTime	Opt.	int	Temperature measurement alarm dwell time.
sensorInfo	Opt.	object	Sensor alarm information.

Message Example

```
{
  "EventNotificationAlert": {
    "channelID": "1",
    "dateTime": "2021-11-19T17:22:24+08:00",
    "activePostCount": "101",
    "eventType": "TMA",
    "eventState": "active",
    "eventDescription": "Temperature Measurement Alarm",
    "DetectionRegionList": {
      "DetectionRegionEntry": [{
        "regionID": "1",
        "RegionCoordinatesList": {
          "RegionCoordinates": [{
            "positionX": "128",
            "positionY": "261"
          }],
        }
      }],
    }
  }
}
```

```
{
  "positionX": "120",
  "positionY": "564"
},
{
  "positionX": "898",
  "positionY": "589"
},
{
  "positionX": "935",
  "positionY": "261"
},
{
  "positionX": "935",
  "positionY": "268"
}
],
},
"TMA": {
  "thermometryUnit": "celsius",
  "ruleTemperature": "35.0",
  "currTemperature": "39.8",
  "ruleCalibType": "region",
  "ruleType": "highest temp is higher than",
  "MaximumTemperaturePoint": {
    "RegionCoordinates": {
      "positionX": "762",
      "positionY": "321"
    }
  },
},
"AbsoluteHigh": {
  "elevation": "0.000",
  "azimuth": "0.000",
  "absoluteZoom": "0.10"
},
"presetNo": "1"
},
},
{
  "regionID": "3",
  "RegionCoordinatesList": {
    "RegionCoordinates": {
      "positionX": "120",
      "positionY": "369"
    }
  },
},
"TMA": {
  "thermometryUnit": "celsius",
  "ruleTemperature": "20.0",
  "currTemperature": "28.5",
  "ruleCalibType": "point",
  "ruleType": "average temp is higher than",
```

```

    "AbsoluteHigh": {
      "elevation": "0.000",
      "azimuth": "0.000",
      "absoluteZoom": "0.10"
    },
    "presetNo": "1"
  }
}
],
{
  "VideoReview": {
    "HikCIDParams": {
      "subSys": 0,
      "ZoneNo": 1,
      "videoURL": "..."
    },
    "protocolType": "HikCIDProtocol"
  },
  "channelName": "Camera 01",
  "detectionPicturesNumber": "1",
  "URLCertificationType": "no"
}
}

```

A.25 JSON_EventNotificationAlert_TMPA

JSON message about temperature measurement pre-alarm details

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered alarm.
dateTime	Req.	ISO 8601	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Type of event that triggers alarm, here it should be "TMPA".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event

Field Name	Req. or Opt.	Date Type	Description
			information will be uploaded continuously until the status is set to "inactive".
eventDescription	Req.	string	Event description.
devIndex	Opt.	string	Device ID (uuid/guid).
channelName	Req.	string	Camera name.
zoneName	Opt.	string	Zone name
visualState	Opt.	string	Download status of the video for verification
subSys	Opt.	int	Partition number, which generated the alarm reports: 0 (all reports). Value range: [0,32].
ZoneNo	Opt.	int	Zone number
DetectionRegionList	Opt.	object	Detection region.
detectionPicturesNumber	Opt.	int	Number of detected pictures. Value of range: [1, 2]
visibleLightURL	Opt.	string	Visible light picture URL.
thermalURL	Opt.	string	Thermal imaging picture URL.
thermalInfoURL	Opt.	string	Additional information data of the thermal imaging picture.
URLCertificationType	Opt.	string	Picture URL authentication method: "no" (no authentication), "digest" (digest authentication).
VideoReview	Opt.	object	Video verification information.

Table A-17 DetectionRegionEntry

Field Name	Req. or Opt.	Date Type	Description
regionID	Opt.	string	Area ID.
RegionCoordinatesList	Opt.	object	Rule area.
TPMA	Opt.	object	Temperature measurement pre-alarm information.

Table A-18 TMPA

Field Name	Req. or Opt.	Date Type	Description
thermometryUnit	Req.	string	Temperature unit: "celsius, fahrenheit, kelvin".
ruleTemperature	Req.	float	Configured rule temperature.
currTemperature	Req.	float	Current temperature.
ruleCalibType	Req.	string	Rule calibration type: "region", "line", "point".
ruleType	Req.	string	Alarm type: "highest temp is higher than" (the highest temperature is higher than), "lowest temp is higher than" (the lowest temperature is higher than), "average temp is higher than" (the average temperature is higher than), "temp diff is higher than" (the temperature difference is higher than), "highest temp is lower than" (the highest temperature is lower than), "lowest temp is lower than" (the lowest temperature is lower than), "average temp is lower than" (the average temperature is lower than), "temp diff is lower than" (the temperature difference is lower than), "temperatureSuddenIncrease" (temperature sudden increase), "temperatureSuddenDecrease" (temperature sudden decrease).
MaximumTemperaturePoint	Opt.	object	Coordinates of highest temperature point for line/frame temperature measurement.
AbsoluteHigh	Opt.	object	PTZ coordinates.
presetNo	Opt.	int	Preset No.
temperatureSuddenChangeCycle	Opt.	int	Cycle of temperature sudden change.

Field Name	Req. or Opt.	Date Type	Description
temperatureSuddenChangeValue	Opt.	float	Value of temperature sudden change. It is accurate to one decimal place.
alertFilteringTime	Opt.	int	Temperature measurement pre-alarm dwell time.
sensorInfo	Opt.	object	Sensor alarm information.

Table A-19 sensorInfo

Field Name	Req. or Opt.	Date Type	Description
id	Req.	int	Sensor ID.
sensorName	Opt.	string	Sensor name.
sensorType	Req.	string	Sensor type: "temperatureSensor" (temperature sensor).
identificationCode	Req.	string	Sensor identification code, value range: [1, 64].

Message Example

```
{
  "EventNotificationAlert": {
    "channelID": "1",
    "dateTime": "2021-11-19T17:22:23+08:00",
    "activePostCount": "101",
    "eventType": "TMPA",
    "eventState": "active",
    "eventDescription": "Temperature Measurement Precautionary Alarm",
    "DetectionRegionList": {
      "DetectionRegionEntry": {
        "regionID": "2",
        "RegionCoordinatesList": {
          "RegionCoordinates": [{
            "positionX": "632",
            "positionY": "655"
          },
          {
            "positionX": "120",
            "positionY": "655"
          },
          {
            "positionX": "115",
            "positionY": "962"
          },
          {

```

```
        "positionX": "642",
        "positionY": "958"
      }
    ]
  },
  "TMPA": {
    "thermometryUnit": "celsius",
    "ruleTemperature": "30.0",
    "currTemperature": "27.8",
    "ruleCalibType": "region",
    "ruleType": "highest temp is higher than",
    "MaximumTemperaturePoint": {
      "RegionCoordinates": {
        "positionX": "300",
        "positionY": "721"
      }
    },
    "AbsoluteHigh": {
      "elevation": "0.000",
      "azimuth": "0.000",
      "absoluteZoom": "0.10"
    },
    "presetNo": "1",
    "alarmRuleTemperature": "35.0"
  }
},
"VideoReview": {
  "HikCIDParams": {
    "subSys": 0,
    "ZoneNo": 1,
    "videoURL": "..."
  },
  "protocolType": "HikCIDProtocol"
},
"channelName": "Camera 01",
"detectionPicturesNumber": "1",
"thermalURL": "..."
}
```

A.26 JSON_EventNotificationAlert_PIR

JSON message about PIR alarm details.

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered an alarm.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss plus the UTC suffix").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Event type, namely PIR.
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously until the status is set to "inactive"
eventDescription	Req.	string	Event description, namely "PIR alarm".
devIndex	Opt.	string	Device ID (uuid/guid)
CaptureList	Opt.	array	The list of captured pictures
channelName	Req.	string	Camera name
ZoneNo	Opt.	int	Zone No.
zoneName	Opt.	string	Zone name
visualState	Opt.	string	Download status of the video for verification
VideoReview	Opt.	object	Video verification information
subSys	Opt.	int	Partition number, which generated the alarm reports: 0 (all reports). Value range: [0,32].
videoURL	Opt.	string	Video URL
resourcesContent Type	Req.	string	Alarm transmission method: url.

Field Name	Req. or Opt.	Date Type	Description
resourcesContent	Opt.	string	The URL string.
protocolType	Req.	string	Protocol type: "HikCIDProtocol"

Message Example

```
{
  "EventNotificationAlert": {
    "channelID": "1",
    "dateTime": "2024-01-21T12:50:39+08:00",
    "activePostCount": 1,
    "eventType": "PIR",
    "eventState": "active",
    "eventDescription": "PIR alarm",
    "devIndex": "2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName": "Ipdome"
  },
  "CaptureList" : [{
    "resourcesContentType": "url",
    "resourcesContent": "xxxxx"}],
  "VideoReview" : {
    "HikCIDParams" : {
      "subSys": 0,
      "ZoneNo": 1,
      "videoURL": "..."
    }
  },
  "protocolType": "HikCIDProtocol" } }
```

A.27 JSON_EventNotificationAlert_VideoLossAlarmMsg

JSON message about video loss alarm details

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered alarm.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.

Field Name	Req. or Opt.	Date Type	Description
eventType	Req.	string	Event type, here it should be "videoloss".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously until the status is set to "inactive".
eventDescription	Req.	string	Event description, here it is "videoloss alarm".
devIndex	Opt.	string	Device ID (uuid/guid).
channelName	Req.	string	Camera name.
zoneName	Opt.	string	Zone name
visualState	Opt.	string	Download status of the video for verification
VideoReview	Opt.	object	Video verification information.
protocolType	Req.	string	Protocol type: "HikCIDProtocol".
HikCIDParams	Opt.	object	HikCIDProtocol parameters. It is valid when the value of protocolType is "HikCIDProtocol".
subSys	Opt.	int	Partition number, which generated the alarm reports: 0 (all reports). Value range: [0,32].
ZoneNo	Opt.	int	Zone number.
videoURL	Opt.	string	Video URL.

Message Example

```
{
  "EventNotificationAlert":{
    "channelID":"1",
    "dateTime":"2018-01-21T12:50:39+08:00",
    "activePostCount":1,
    "eventType":"videoloss",
    "eventState":"active",
    "eventDescription":"videoloss alarm",
    "devIndex":"2cd6716d-767f-4756-ac55-50276a5e3b4a",
```

```

"channelName": "Ipdome"
"VideoReview": {
  "protocolType": "HikCIDProtocol"
  "HikCIDParams": {
    "subSys": 0,
    "ZoneNo": 1,
    "videoURL": "..."
  }
}
}
}
}

```

A.28 JSON_EventNotificationAlert_VideoTamperingAlarmMsg

JSON message about video tampering alarm details

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered alarm.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Event type, here it should be "shelteralarm".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously until the status is set to "inactive".
eventDescription	Req.	string	Event description, here it is "shelteralarm alarm".
devIndex	Opt.	string	Device ID (uuid/guid).
channelName	Req.	string	Camera name.
zoneName	Opt.	string	Zone name

Field Name	Req. or Opt.	Date Type	Description
visualState	Opt.	string	Download status of the video for verification
VideoReview	Opt.	object	Video verification information.
protocolType	Req.	string	Protocol type: "HikCIDProtocol".
HikCIDParams	Opt.	object	HikCIDProtocol parameters. It is valid when the value of protocolType is "HikCIDProtocol".
subSys	Opt.	int	Partition number, which generated the alarm reports: 0 (all reports). Value range: [0,32].
ZoneNo	Opt.	int	Zone number.
videoURL	Opt.	string	Video URL.

Message Example

```
{
  "EventNotificationAlert":{
    "channelID":"1",
    "dateTime":"2018-03-13T19:42:27+08:00",
    "activePostCount":1,
    "eventType":"shelteralarm",
    "eventState":"active",
    "eventDescription":"shelteralarm alarm",
    "devIndex":"2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName":"Camera 01",
    "VideoReview":{
      "protocolType": "HikCIDProtocol"
      "HikCIDParams":{
        "subSys":0,
        "ZoneNo":1,
        "videoURL":"..."
      }
    }
  }
}
```

A.29 JSON_EventNotificationAlert_VideoVerificationAlarmMsg

JSON message about video verification alarm details

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered alarm.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Event type, here it should be "videoReview".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously unit the status is set to "inactive".
eventDescription	Req.	string	Event description, here it is "video review".
devIndex	Opt.	string	Device ID (uuid/guid).
channelName	Req.	string	Camera name.
deviceId	Opt.	string	accountID
deviceSerial	Opt.	string	Device serial No.
VideoReview	Opt.	object	Video verification information.

Table A-20 VideoReview

Field Name	Req. or Opt.	Date Type	Description
protocolType	Req.	string	Protocol type: "HikCIDProtocol".
HikCIDParams	Opt.	object	HikCIDProtocol parameters. It is valid when the value of protocolType is "HikCIDProtocol".

Table A-21 HikCIDParams

Field Name	Req. or Opt.	Date Type	Description
subSys	Opt.	int	Partition number, which generated the alarm reports: 0 (all reports). Value range: [0,32].
ZoneNo	Opt.	int	Zone number.
CIDCode	Opt.	string	CID alarm code is a 4-digit string, the last three digits indicate the event/ alarm code, and the first digit indicates the alarm status (1-triggered, 3-restored), e.g., "1103"-zone alarm triggered, "3103"-zone alarm restored, refer to <i>CID Code</i> for details.
CIDType	Opt.	int	CID alarm type: 1 (zone alarm), 2 (video alarm), 3 (virtual zone alarm), 4 (duress alarm), 5 (exception alarm), 6 (operation alarm).
CIDDescribe	Opt.	string	Description of CID code, the maximum description length is 127 bytes.
timeZoneldx	Opt.	int	Time zone index No.: 1 (GMT-12:00), 2 (GMT-11:00), 3 (GMT-10:00), ..., 14 (GMT-01:00), 15 (GMT), 16 (GMT +01:00), ..., 34 (GMT-13:00), 35 (GMT +14:00).
triggerTime	Opt.	string	CID alarm time, e.g., 2009-10-09 16:59:00.
uploadTime	Opt.	string	CID alarm uploaded time, e.g., 2019-10-09 17:55:46.
CIDParam	Opt.	string	CID parameter, which contains 8 sub parameters, i.e., userType, userNo, zoneNo, keyboardNo, videoChanNo, dskNo, moduleAddr, and userName; each sub parameter should be separated by comma. See the remarks below for details.

Field Name	Req. or Opt.	Date Type	Description
UUID	Opt.	string	Alarm ID.
isVideo	Opt.	int	The file type: 0 (no video file, while picture may exist), 1 (AVI file), 2 (MP4 file).
videoURL	Opt.	string	Video URL.
videoInfoList	Opt.	array	Video information list. This field will be returned only when the device has dual lens.
isTalk	Opt.	int	Whether it supports two-way audio verification: 0 (not support), 1 (support).

Table A-22 videoInfoList

Field Name	Req. or Opt.	Date Type	Description
videoURL	Opt.	string	Video URL.
cameraPosition	Opt.	enum	Camera position, subType: string, "left" (left camera), "right" (right camera). 180° PIRCAM has dual lens, of which one is on the left, and the other one is on the right. It supports two lens to capture at the same time.

Remarks

The descriptions of 8 sub parameters of CID parameter (**CIDParam**) are shown as below:

userType

User type, a 4-byte integer, values: 1-keyboard user, 2-network user, others-invalid.

userNo

User No., a 4-byte integer, the value -1 is invalid.

zoneNo

Zone No., a 4-byte integer, the value -1 is invalid.

keyboardNo

Keyboard No., a 4-byte integer, the value -1 is invalid.

videoChanNo

Video channel No., a 4-byte integer, the value -1 is invalid.

dskNo

HDD No., a 4-byte integer, the value -1 is invalid.

moduleAddr

Module address, a 4-byte integer, the value -1 is invalid.

userName

User name, the maximum name length is 31 bytes, it can be set to "NONE".

See Also

Event Code List

Message Example

```
{
  "EventNotificationAlert":{
    "channelID":"1",
    "dateTime":"2018-01-21T12:50:39+08:00",
    "activePostCount":1,
    "eventType":"videoReview",
    "eventState":"active",
    "eventDescription":"video review",
    "devIndex":"2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName":"Ipdome",
    "deviceId":"123456",
    "deviceSerial":"123456",
    "VideoReview": {
      "protocolType":"HikCIDProtocol"
      "HikCIDParams":{
        "subSys":0,
        "ZoneNo":1,
        "CIDCode":"1103",
        "CIDType":1,
        "CIDDescribe":"alarm",
        "timeZoneIdx":0,
        "triggerTime":"2009-02-24 16:59:00",
        "uploadTime":"2009-02-24 16:59:00",
        "CIDParam":"1,2,1,1,1,0,admin",
        "UUID":"0",
        "isVideo":1,
        "videoURL":"..."
        "videoInfoList":[
          {
            "videoURL":"...",
            "cameraPosition":"left"
          },
          {
            "videoURL":"...",
            "cameraPosition":"right"
          }
        ]
      }
    }
  }
}
```

```
    },  
    "isTalk":0  
  ]  
}  
}  
}  
}
```

A.30 JSON_EventNotificationAlert_hppConnectionStatusChanged

JSON message about details of Hik-Partner Pro connection status

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	int	Channel No. of the device that triggered alarm.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MMddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Type of event that triggers alarm, here it should be "hppConnectStateChanged".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously until the status is set to "inactive".
eventDescription	Req.	string	Event description, here it is "IP Receiver Pro and Hik-Partner Pro connection state changed".
status	Req.	string	Connection status: "normal", "abnormal".

Message Example

```
{  
  "EventNotificationAlert": {
```

```

"channelID": "0",
"dateTime": "2018-01-21T12:50:39+08:00",
"activePostCount": 1,
"eventType": "hppConnectionStatusChanged",
"eventState": "active",
"eventDescription": "IP Receiver Pro and Hik-Partner Pro connection state changed",
"status": "abnormal"
}
}

```

A.31 JSON_EventNotificationAlert_deviceKeyStateChanged

JSON message about details of device key status

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	int	Channel No. of the device that triggered alarm.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MMddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Type of event that triggers alarm, here it should be "deviceKeyStateChanged".
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously until the status is set to "inactive".
eventDescription	Req.	string	Event description, here it is "Device key status changed".
status	Req.	string	Connection status: "normal", "abnormal".
devIndex	Opt.	string	Unique ID of alarm device.
channelName	Req.	string	Channel name (camera name).

Message Example

```
{
  "EventNotificationAlert":{
    "channelID":"0",
    "dateTime":"2018-01-21T12:50:39+08:00",
    "activePostCount":1,
    "eventType":"deviceKeyStateChanged",
    "eventState":"active",
    "eventDescription":"Device key status changed",
    "devIndex": "A52FB43E-7B75-4671-B8BF-B5AB9B2A4D61",
    "channelName": "",
    "status":" abnormal"
  }
}
```

A.32 JSON_EventNotificationAlert_longTimeLeave

JSON message about details on prolonged bed exit alarms triggered by auxiliary care radars.

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered an alarm.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss plus the UTC suffix").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Event type, namely longTimeLeave.
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously unit the status is set to "inactive"
eventDescription	Req.	string	Event description, namely "Prolonged Bed Exit Alarm".

Field Name	Req. or Opt.	Date Type	Description
devIndex	Opt.	string	Device ID (uuid/guid)
channelName	Req.	string	Camera name

Message Example

```
{
  "EventNotificationAlert": {
    "channelID": "0",
    "dateTime": "2024-03-13T19:42:27+08:00",
    "activePostCount": 1,
    "eventType": "longTimeLeave",
    "eventState": "active",
    "eventDescription": "Prolonged Bed Exit Alarm",
    "devIndex": "2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName": ""
  }
}
```

A.33 JSON_EventNotificationAlert_heartBeatAbnormal

JSON message about details on irregular heartbeat alarms triggered by auxiliary care radars.

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered an alarm.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss plus the UTC suffix").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Event type, namely heartBeatAbnormal.
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously until the status is set to "inactive"

Field Name	Req. or Opt.	Date Type	Description
eventDescription	Req.	string	Event description, namely "Irregular Heartbeat Alarm".
devIndex	Opt.	string	Device ID (uuid/guid)
channelName	Req.	string	Camera name

Message Example

```
{
  "EventNotificationAlert": {
    "channelID": "0",
    "dateTime": "2024-03-13T19:42:27+08:00",
    "activePostCount": 1,
    "eventType": "heartBeatAbnormal",
    "eventState": "active",
    "eventDescription": "Irregular Heartbeat Alarm",
    "devIndex": "2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName": ""}}

```

A.34 JSON_EevntNotificationAlert_respireAbnormal

JSON message about details on abnormal respiratory rate alarms triggered by auxiliary care radars.

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	string	Channel No. of the device that triggered an alarm.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss plus the UTC suffix").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Event type, namely respireAbnormal.
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded

Field Name	Req. or Opt.	Date Type	Description
			continuously unit the status is set to "inactive"
eventDescription	Req.	string	Event description, namely "Abnormal Respiratory Rate Alarm".
devIndex	Opt.	string	Device ID (uuid/guid)
channelName	Req.	string	Camera name

Message Example

```
{
  "EventNotificationAlert": {
    "channelID": "0",
    "dateTime": "2024-03-13T19:42:27+08:00",
    "activePostCount": 1,
    "eventType": "respireAbnormal",
    "eventState": "active",
    "eventDescription": "Abnormal Respiratory Rate Alarm",
    "devIndex": "2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName": ""}}

```

A.35 JSON_EventNotificationAlert_deviceHPPNetworkChanged

JSON message about details of Hik-Partner Pro network changes

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
channelID	Req.	int	Channel No. of the device that triggered alarm.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MMddThh:mm:ss").
activePostCount	Req.	int	Number of times that the same alarm has been triggered.
eventType	Req.	string	Type of event that triggers alarm, here it should be "deviceHPPNetworkChanged".

Field Name	Req. or Opt.	Date Type	Description
eventState	Req.	string	Durative alarm/event status: "active"-valid, "inactive"-invalid, e.g., when a moving target is detected, the alarm/event information will be uploaded continuously unit the status is set to "inactive".
eventDescription	Req.	string	Event description, here it is "Device Network changed on Hik-Partner Pro".
status	Req.	string	Connection status: "normal", "abnormal".
devIndex	Opt.	string	Unique ID of security control panels.
channelName	Opt.	string	Channel name (camera name)

Message Example

```
{
  "EventNotificationAlert": {
    "channelID": "0",
    "dateTime": "2018-01-21T12:50:39+08:00",
    "activePostCount": 1,
    "eventType": "deviceHPPNetworkChanged",
    "eventState": "active",
    "eventDescription": "Device Network changed on Hik-Partner Pro",
    "status": "abnormal",
    "devIndex": "2cd6716d-767f-4756-ac55-50276a5e3b4a",
    "channelName": "Ipdome"
  }
}
```

A.36 JSON_BypassList

JSON message about list parameters

```
{
  "List": [{
    "id":
/*int, zone No., which starts from 0. It is required when controlling multiple zones*/
  ]}
}
```

A.37 JSON_DeactivationList

JSON message about list parameters

```
{
  "List": [{
    "id":
      /*int, zone No., which starts from 0. It is required when controlling multiple zones*/
      "oneTimeDeactivationMode": "off",
      /*optional, string, one-time deactivation mode, enum: [off#disable deactivation (all alarms are reported), lidOnly#
      tamper deactivation (tamper alarms are not reported during armed mode), entirely# complete deactivation (no
      alarms are reported)], desc: effective during armed mode, disabled upon disarming*/
      "deactivationMode": "off",
      /*optional, string, permanent deactivation mode, enum: [off#disable deactivation (all alarms are reported), lidOnly#
      tamper deactivation (tamper alarms are not reported, entirely# complete deactivation (no alarms are reported))*/
    }
  ]
}
```

A.38 JSON_OutputsCtrl

JSON message about relay control parameters

```
{
  "OutputsCtrl": {
    "switch": ""
    /*required, string, whether to open relay: "open"-yes, "close"-no*/
    "List": [{
      /*this node is required for multiple relays control*/
      "id": ,
      /*optional, int, relay number, which starts from 0*/
      "seq": ,
      /*optional, string, relay serial No.,you can set this node to control a relay if the relay No. is not available.*/
    }
  ]
}
```

A.39 JSON_ResponseStatus

JSON message about response information and status

```
{
  "requestURL": "",
  /*optional, string, request URL*/
  "statusCode": ,
  /*required, int, status code*/
  "statusString": "",
  /*required, string, status description*/
}
```

```
"subStatusCode": "",
/*required, string, sub status code*/
"errorCode": ,
/*optional, int, error code, which correspond to subStatusCode; this field is required when statusCode does not equal to 1*/
"errorMsg": ""
/*optional, string, error code; this field is required when statusCode does not equal to 1*/
"rebootRequired":
/*optional, int, whether the reboot is required: 1=yes (reboot to take effect), other values-no; if reboot is not required, this field may be not returned*/
}
```



Note

See **Status Codes** for details about the status codes and sub status codes.

A.40 JSON_SearchDescription

JSON message about search conditions of channel list

```
{
  "SearchDescription": {
    "position": ,
    /*required, int, index, which starts from 0*/
    "maxResult": ,
    /*required, int, the maximum number of searched results in a single search*/
    "Filter":{
      "key": "",
      /*optional, search by keywords (fuzzy search: device serial number/device name/account ID/deviceID/remark); the maximum length is 128 bytes*/
      "devStatus": ["online", "offline", "unknown"],
      /*optional, string, device status: "online", "offline", "unknown"*/
      "activeStatus": ["active", "inactive", "unauth"],
      /*optional, string, alarm activation status: "active", "inactive", "unauth" (unauthorized)*/
      "connectionMode": ["HPP", "OTAP", "ISUP", "Dual-Connection"],
      /*optional, string, connection mode, "HPP", "OTAP", "ISUP", "Dual-Connection"*/
      "notAddedByUserId": 2,
      /*optional, int, user index, range of value: [2, 150]. It indicates to search for devices that cannot be operated by the user*/
      "devSource": [0,1,2,3,4,5,6,7],
      /*optional, int, device source: 0 (Hikvision security control panel), 1 (Hikvision video devices), 2 (third-party devices), 3 (ISUP5.0 security control panel), 4 (ISUP5.0 video devices), 5 (Hikvision access control devices), 6 (radar devices), 7 (OTAP alarm devices), 8 (IP speaker devices)*/
      "devType": [0,1,2,3],
      /*optional, int, device source: 0 (security control panel), 1 (video devices), 2 (access control devices), 3 (radar devices), 4 (IP speaker devices), 100 (other devices)*/
      "isNeedUpgrade": [0,1],
      /*optional, int, whether the device needs upgrade: 0 (no), 1 (yes)*/
      "orderByColumn": ,
      /*optional, int, sorting mode: 1 (device name), 2 (firmware version), 3 (account ID), 4 (device serial No.)*/
      "order": 0
    }
  }
}
```

```
/*dependent, int, depends on orderByColumn: 0 (ascending order), 1 (descending order)*/  
}  
}  
}
```

A.41 JSON_SearchResult

JSON message about search results

```
{  
  "SearchResult": {  
    "numOfDevice": 10,  
    /*optional, int, total number of devices*/  
    "numOfUnauthorized": 10,  
    /*optional, int, number of unauthorized devices*/  
    "numOfNotActivated": 10,  
    /*optional, int, number of unactivated devices*/  
    "numOfMatches": 10,  
    /*optional, int, number of returned records*/  
    "totalMatches": 100,  
    /*optional, int, total number of matched records*/  
    "existUnauth": false,  
    /*optional, boolean, whether unauthorized device exists*/  
    "MatchList": [{  
      /*MatchList is returned when totalMatches is larger than 0*/  
      "Device": {  
        "devIndex": "2cd6716d-767f-4756-ac55-50276a5e3b4a",  
        /*required, device ID (uuid/guid), string*/  
        "accountID": "",  
        /*required, string; up to 512 characters are allowed*/  
        "devName": "",  
        /*required, device name, string, up to 512 characters are allowed*/  
        "devSerial": "",  
        /*optional, string, device serial number; up to 48 characters are allowed*/  
        "devMode": "",  
        /*optional, device model, string*/  
        "devVersion": "",  
        /*optional, string, device version*/  
        "activeStatus": "active",  
        /*activation status: "inactive", "active", "unauth" (unauthorized); it is returned when devStatus is set to  
        "online"*/  
        "siteInfo": {  
          /*optional, string, device site information*/  
          "siteID": "",  
          /*optional, string, device site ID*/  
          "siteName": "",  
          /*optional, string, device site name*/  
        },  
        "ISUP": {  
          /*optional, ISUP device ID and key, it is valid when the value of connectionMode is 2*/
```

```
"deviceId":"111",
/*optional, string, device ID*/
"deviceKey":"111"
/*optional, string, device key, it is not returned by default. If the device key is not modified, you do not need to set this
filed; if modified, this filed should be encrypted*/
},
"OTAP":
/*optional, device ID and key of OTAP device*/
{
"deviceId":"111",
/*optional, string, up to 31 characters are allowed, including letters and digits*/
"deviceKey":"111"
/*optional, string, device key, up to 32 characters are allowed, it is not returned by default. If the device key is not
modified, you do not need to set this filed; if modified, this filed should be encrypted*/
},
"streamKey":"sdk123456"
/*optional, string, stream key, it is not returned by default. If the device key is not modified, you do not need to set
this filed; if modified, this filed should be encrypted*/
"devSource":0,
/*required, int, device source: 0 (Hikvision security control panel), 1 (Hikvision video devices), 2 (third-party devices),
3 (ISUP5.0 security control panel), 4 (ISUP5.0 video devices), 5 (Hikvision access control devices), 6 (radar device), 7
(OTAP alarm device), 8 (IP speaker devices)*/
"devType":0,
/*optional, int, device source: 0 (security control panel), 1 (video devices), 2 (access control devices), 3 (radar devices),
4 (IP speaker devices), 100 (other devices)*/
"connectionMode":0
/*required, int, connection mode: 0 (unknown), 1 (HPP), 2 (dual-connection), 3 (ISUP), 4 (OTAP)*/
"devStatus": "online"
/*optional, string, device status: "online", "offline", "unknown"*/
"onlineType":0
/*optional, int, online type: 0 (HPP), 1 (ISUP), 2 (OTAP). It is valid when devStatus is "online" and connectionMod is 2
(dual-connection)*/
"offlineHint":0,
/*optional, int, offline reason of direct connection, it is returned when direct connection is offline: 0 (wait for the
device to register), 1 (incorrect key), 2 (network exception), 3 (protocol mismatch), returned when HPP link is offline in
a dual-link direct connection
mode, 4 (HPP link exception)*/
"isNeedUpgrade":0,
/*optional, int, whether the device needs upgrade: 0 (no), 1 (yes), only valid for devices added via HPP*/
"remark":""
/*optional, string, remarks of the device, up to 512 characters are allowed*/
"pluginEnable": "true"
/*optional, boolean, whether to enable plugin verification. It corresponds to the plugin verification button on the web
page*/
"pluginType": "0"
/*optional, int, plugin verification type, effective when pluginEnable is true. 0 (video plugin verification), 1 (video
intercom plugin verification), 2 (security panel plugin verification), 3 (IP speaker plugin verification)*/
"deviceIDPriority": "deviceNo"
/*optional, boolean, device ID priority, enum: [zoneID# zone number priority, deviceNo# device number priority], for
security control panel devices*/
}
},
```

```
{...}
]
}
}
```

A.42 JSON_SubscribeDeviceMgmt

JSON message about subscription conditions

```
{
  "SubscribeDeviceMgmt":{
    "eventMode": "",
    /*required, string, arming mode: "all"-arm all added devices*/
    "defenceMode": "",
    /*required, string type, subscription mode: "all"-subscribe to all events*/
  }
}
```

A.43 JSON_SubscribeDeviceMgmtRsp

JSON message about subscription results

```
{
  "SubscribeDeviceMgmtRsp":{
    "id": "",
    /*optional, integer, subscription ID*/
  }
}
```

A.44 JSON_SubSysList

JSON message about partition list

```
{
  "SubSysList":[{
    "SubSys":{
      "id":,
      /*required, int, partition No.*/
      "arming": "",
      /*optional, string, partition arming status: "stay"-stay armed, "away"-away armed, "disarm"-disarmed, "arming"-arming*/
      "alarm": "",
      /*optional, boolean, whether the alarm triggered in the partition: true=yes, false=no*/
      "enabled": true
    }
  }
  /*optional, boolean, whether to enable the partition: true, false*/
}
```

```
}}  
}
```

A.45 JSON_ZoneCond

JSON message about zone status search condition

```
{  
  "ZoneCond": {  
    /*req, object, zone status search condition*/  
    "searchID": "test",  
    /*required, string, search ID. It is used to confirm the upper-level platform or system. If the platform or the system is  
    the same one during two searching, the search history will be saved in the memory to speed up next searching*/  
    "searchResultPosition": 0,  
    /*required, int, the start position of the search result in the result list. In a single search, if you cannot get all the  
    records in the result list, you can mark the end position and get the following records after the marked position in the  
    next search*/  
    "maxResults": 30  
    /*required, int, the maximum number of search results this time by calling this URI*/  
  }  
}
```

A.46 JSON_ZoneSearch

JSON message about zone status search result

```
{  
  "ZoneSearch": {  
    /*read-only, required, object, zone status search result*/  
    "searchID": "test",  
    /*read-only, required, string, search ID. It is used to confirm the upper-level platform or system. If the platform or the  
    system is the same one during two searching, the search history will be saved in the memory to speed up next  
    searching*/  
    "responseStatusStrg": "OK",  
    /*read-only, required, enum, subType:string, searching status description: "OK" (searching completed), "NO MATCH"  
    (no matched results), "MORE" (searching for more results)*/  
    "numOfMatches": 1,  
    /*read-only, required, int, number of results returned this time*/  
    "totalMatches": 1,  
    /*read-only, required, int, total number of matched results*/  
    "ZoneList": [  
    /*read-only, optional, array, zone status list*/  
    {  
      "Zone": {  
        /*read-only, optional, object, zone status*/  
        "id": 1,  
        /*read-only, required, int, zone number*/  
        "name": "test",  
        /*read-only, optional, string, zone name*/
```



```
"status": "notRelated",
/*read-only, optional, enum, subType:string, zone status: "notRelated" (unlinked), "online", "offline", "trigger"
(triggered), "breakDown" (malfunctioning), "heartbeatAbnormal" (abnormal heartbeat)*/
"reason": "short",
/*read-only, optional, enum, subType:string, cause of failure: "short" (short circuit), "break" (open circuit). This field is
valid when the value of status is "breakDown" and only for the zones or relays of multichannel transmitters*/
"tamperEvident": true,
/*read-only, optional, boolean, zone tampering status: true (tamper-proof), false (not tamper-proof)*/
"shielded": true,
/*read-only, optional, boolean, zone shielding status: true (shielded), false (not shielded)*/
"bypassed": true,
/*read-only, optional, boolean, whether the zone is bypassed: true (bypassed), false (not bypassed)*/
"oneTimeDeactivationMode": "off",
/*optional, string, one-time deactivation mode, enum: [off#disable deactivation (all alarms are reported), lidOnly#
tamper deactivation (tamper alarms are not reported during armed mode), entirely# complete deactivation (no
alarms are reported)], desc: effective during armed mode, disabled upon disarming*/
"deactivationMode": "off",
/*optional, string, permanent deactivation mode, enum: [off#disable deactivation (all alarms are reported), lidOnly#
tamper deactivation (tamper alarms are not reported, entirely# complete deactivation (no alarms are reported))*/
"armed": true,
/*read-only, optional, boolean, whether the zone is armed: true (yes), false (no)*/
"isArming": true,
/*read-only, optional, boolean, whether the zone is in arming. The value of this field can be true only*/
"alarm": true,
/*read-only, optional, boolean, whether the alarm is triggered in the zone: true (alarm is triggered), false (no alarm
triggered)*/
"charge": "normal",
/*read-only, optional, enum, subType:string, battery power status of the zone: "normal", "lowPower" (low battery)*/
"chargeValue": 0,
/*read-only, optional, int, remaining battery percentage; range:[0, 100]*/
"signal": 0,
/*read-only, optional, int, signal strength; range:[0, 255]*/
"temperature": 1,
/*read-only, optional, int, temperature*/
"alwaysActiveEnabled": true,
/*read-only, optional, boolean, whether to enable always active function*/
"waterDetectorAlarm": "yes",
/*read-only, optional, enum, subType:string, water detector alarm: "yes", "no", "fault"*/
"smokeDetectedExceed": "yes",
/*read-only, optional, enum, subType:string, smoke detection alarm: "yes", "no", "fault"*/
"temperatureExceed": "yes",
/*read-only, optional, enum, subType:string, temperature detection alarm: "yes", "no", "fault"*/
"subSystemNo": 1,
/*read-only, optional, int, partition number*/
"linkageSubSystem": [1, 2, 3],
/*read-only, optional, array, subType:int, linked partitions*/
"pollingOptionEnable": true,
/*read-only, optional, boolean*/
"zoneAttrib": "wired",
/*read-only, optional, enum, subType:string, zone attribute: "wired", "wireless" (default)*/
"RelatedChanList": [
/*read-only, optional, array, subType:object, list of linked channel No.*/
```

```
{
  "RelatedChan": {
    /*read-only, optional, object, linked channel*/
    "relator": "test",
    /*read-only, required, string, device linked to the channel when the alarm is triggered*/
    "cameraSeq": "test",
    /*read-only, optional, string, camera serial number*/
    "relatedChan": 1
  },
  /*read-only, optional, int, linked channel number*/
  },
  "detectorType": "test",
  /*read-only, optional, string, subType:string, type of the detector linked to the zone*/
  "model": "DS-PM1-O8-WE",
  /*read-only, optional, enum, subType:string, model: "DS-PM1-O8-WE", "DS-PM1-O2-WE"*/
  "stayAway": true,
  /*read-only, optional, boolean, whether the stay arming bypass is enabled for the zone*/
  "zoneType": "Instant",
  /*read-only, optional, enum, subType:string, zone type: "Instant" (instant zone), "Delay" (delay zone), "Follow" (follow zone), "Perimeter" (perimeter zone), "24hNoSound" (24-hour silent zone), "Emergency" (panic zone), "Fire" (fire zone), "Gas" (gas zone), "Medical" (medical zone), "Timeout" (timeout zone), "Non-Alarm" (disabled zone), "Key" (key zone), "24hSound" (24-hour sound zone)*/
  "InputList": [
    /*read-only, optional, array, subType:object, input status list*/
    {
      "id": 1,
      /*read-only, required, int, input ID*/
      "enabled": true,
      /*read-only, required, boolean, whether the input is enabled*/
      "mode": "NO"
    },
    /*read-only, optional, enum, subType:string, input type: "rolling shutter", "NC" (always closed), "NO" (always open)*/
    {
      "id": 2,
      /*read-only, required, int, input ID*/
      "enabled": true,
      /*read-only, required, boolean, whether the input is enabled*/
      "mode": "NC"
    }
  ],
  "humidity": 10,
  /*read-only, optional, int, humidity; range:[10, 90]; unit: percentage (the detection range of humidity detector is from 10% to 90%)*/
  "healthStatus": "normal",
  /*read-only, optional, enum, subType:string, health status: "normal", "fault" (abnormal)*/
  "antiMaskingEnabled": true,
  /*read-only, optional, boolean, whether to enable anti-masking: true (enable), false (disable)*/
  "mountingType": "wall",
  /*read-only, optional, enum, subType:string, mounting type: "wall" (wall-mounted), "ceiling" (ceiling-mounted)*/
  "MagnetShockCurrentStatus": {
    /*read-only, optional, object, current status of door contact detector. It is supported by the MC Shock only*/
    "magnetOpenStatus": true,
    /*read-only, optional, boolean, whether the door contact is open: true (open), false (close)*/
    "magnetShockStatus": true,
    /*read-only, optional, boolean, door contact vibration status: true (vibrate), false (not vibrate)*/
    "magnetTiltStatus": true
  },
  /*read-only, optional, boolean, whether the door contact is tilted: true (tilted), false (not tilted)*/
  "tiltStatus": false
}
```

```
    "magnetOpenStatus": true,
    /*read-only, optional, boolean, whether the door contact is open: true (open), false (close). It is valid for the door
    contact detector only, and supported by both wireless zone and wired zone*/
    "devIndex": "test",
    /*read-only, optional, string, device index, range:[1, 64]*/
    "devName": "test",
    /*read-only, optional, string, device name, range:[1,64]*/
    "isAvailable": true,
    /*read-only, optional, boolean, whether the partition is available: true (default), false*/
    "isBypassedAvailable": true,
    /*read-only, optional, boolean, whether the zone bypass is configurable: true (yes, default value), false (no)*/
    "version": "test",
    /*read-only, optional, string, detector version number; range:[1, 32]*/
    "pirCamConnected": true,
    /*read-only, optional, boolean, whether the outdoor triple technology detector and PIR camera are connected: true
    (connected), false (disconnected)*/
    "accessModuleType": "transmitter",
    /*read-only, optional, enum, subType:string, access module type: "transmitter" (external single channel transmitter),
    "localTransmitter" (onboard transmitter), "multiTransmitter" (external multichannel transmitter), "localRelay"
    (onboard Arming Region module), "keypad" (external wired keypad)*/
    "relatedAccessModuleID": 1,
    /*read-only, optional, int, linked access module ID. It is invalid for the onboard access module*/
    "address": 254,
    /*read-only, optional, int, wired (extended) module address. This field works with accessModuleType, which defines
    the access module type*/
    "deviceNo": 1
    /*read-only, optional, int, device number, range:[1, 1000]. After installation, the installer will upload the device ID and
    the corresponding peripheral/detector information to the ARC for device type recognition*/
  }
}
]
```

A.47 JSON_ZoneList

JSON message about zone list

```
{
  "ZoneList":[{
    "Zone":{
      "id": ,
      /*required, int, zone No.*/
      "name": "",
      /*optional, string, zone name*/
      "status": "",
      /*optional, string, zone status: "notRelated"-unlinked, "online", "offline", "trigger"-alarm triggered, "breakDown"-
      fault, "heartbeatAbnormal"-heartbeat exception*/
      "tamperEvident": ,
      /*optional, boolean, zone tampering status: true-tampered, false-not tampered*/
    }
  }
}
```

```
"shielded": ,
/*optional, boolean, whether the zone is shielded: true=yes, false-no*/
"bypassed": "",
/*optional, boolean, whether to bypass zone: true=yes, false-no*/
"armed": "",
/*optional, boolean, whether to arm zone: true=yes, false-no*/
"isArming": true,
/*optional, boolean, whether the zone is armed. The value of node is true*/
"alarm": "",
/*optional, boolean, whether the alarm triggered in the zone: true=yes, false-no*/
"charge": "",
/*optional, string, power status: "normal", "lowPower"*/
"chargeValue": 0,
/*optional, int, battery power value; value range: [0,100]*/
"signal": 0,
/*optional, int, signal strength; value range: [0,255]*/
"alwaysActiveEnabled": true,
/*optional, boolean, whether to enable alwaysActive function*/
"waterDetectorEnabled": true,
/*optional, boolean, whether to enable water leak detection*/
"smokeDetectedEnabled": true,
/*optional, boolean, whether to enable smoke detection*/
"temperatureExceed": "",
/*optional, string, whether the temperature exceeded threshold: "yes", "no", "fault"*/
"temperature": 1,
/*optional, read-only, int, temperature*/
"detectorType": "",
/*optional, string, type of the detector linked to the zone, see details about the supported detector types in remarks*/
"model": "",
/*optional, string, model: "DS-PM1-O8-WE" (8-channel wireless output module), "DS-PM1-O2-WE" (2-channel
wireless output module)*/
"subSystemNo": 1,
/*optional, int, partition number; this node is not returned if device supports linking multiple partitions to the zone*/
"linkageSubSystem": [1, 2, 3],
/*optional, array, partitions linked to the zone; this node is valid for multiple partitions linked to the zone*/
"pollingOptionEnable": true,
/*optional, boolean, whether to enable heartbeat detection: true (the security control panel will detect the heartbeat
of the peripheral)*/
"stayAway": true,
/*optional, boolean, whether the zone is stay armed*/
"zoneType": "",
/*optional, string, zone type: "Instant"-instant zone, "Delay"-delay zone, "Follow"-follow zone, "Perimeter"-perimeter
zone, "24hNoSound"-24-hour silent zone, "Emergency"-panic zone, "Fire"-fire zone, "Gas"-gas zone, "Medical"-
medical zone, "Timeout"-timeout zone, "Non-Alarm"-disabled zone, "Key"-key zone, "24hSound"-24 annunciating
zone*/
"InputList": [{
/*optional, list of input status*/
"id": 1,
/*required, int, input ID*/
"enabled": true,
/*required, boolean, whether to enable the input port*/
"mode": ""
```

```

/*optional, mode: "rolling shutter", "NC" (remain open), "NO"(remain closed)*/
    }}
  }
}}
}

```

Remarks

Table A-23 Detector Type

detectorType	Description
panicButton	Panic button
magneticContact	Door magnetic contact detector
smokeDetector	Smoke detector
activeInfraredDetector	Active IR detector
passiveInfraredDetector	PIR detector
glassBreakDetector	Glass-break detector
vibrationDetector	Shock detector
dualTechnologyPirDetector	Dual-technology motion detector
tripleTechnologyPirDetector	Triple-technology detector
humidityDetector	Humidity detector
temperatureDetector	Temperature detector
combustibleGasDetector	Gas detector
dynamicSwitch	Dynamic switch
controlSwitch	Control switch
smartLock	Smart lock
waterDetector	Water detector
displacementDetector	Displacement detector
singleInfraredDetector	Door contact
singleZoneModule	Wireless single input expander
curtainInfraredDetector	IR curtain detector
pircam	Pircam detector (detector equipped with camera)
slimMagneticContact	Slim magnetic contact

detectorType	Description
indoorDualTechnologyDetector	Indoor dual technology detector
magnetShockDetector	Magnet shock detector
waterLeakDetector	Water leak detector
wirelessSmokeDetector	Wireless smoke detector
wirelessGlassBreakDetector	Wireless glass break detector
wirelessTemperatureHumidityDetector	Wireless temperature humidity detector
wirelessHeatDetector	Wireless heat detector
wirelessCODetector	Wireless CO detector
wirelessPIRCeilingDetector	Wireless PIR ceiling detector
wirelessExternalMagnetDetector	Wireless external magnet detector
wirelessPIRCurtainDetector	Wireless PIR curtain detector
wirelessDTAMCurtainDetector	Wireless DTAM curtain detector
other	Others

Appendix B. Event Types

General Event

eventType	Event Type Name and Details
devStatusChanged	Device Status Changed Alarm, see details in <i><u>JSON_EventNotificationAlert_DevStatusChangedAlarmMsg</u></i> .
devicedeleted	Device Deleted Alarm, see details in <i><u>JSON_EventNotificationAlert_DeviceDeleted</u></i> .
CIDAlarm	Device Heartbeat Information, see details in <i><u>JSON_EventNotificationAlert_CIDAlarmMsg</u></i> .
IO	Alarm Input Alarm, see details in <i><u>JSON_EventNotificationAlert_IO</u></i> .
VMD	Motion Detection Alarm, see details in <i><u>JSON_EventNotificationAlert_VMD</u></i> .
diskfull	HDD Full Alarm, see details in <i><u>JSON_EventNotificationAlert_diskfull</u></i> .
diskerror	HDD Error Alarm, see details in <i><u>JSON_EventNotificationAlert_diskerror</u></i> .
diskrecover	HDD Recover Alarm, see details in <i><u>JSON_EventNotificationAlert_DiskRecoverAlarmMsg</u></i> .
videoloss	Video Loss Alarm, see details in <i><u>JSON_EventNotificationAlert_VideoLossAlarmMsg</u></i> .
shelteralarm	Video Tampering Alarm, see details in <i><u>JSON_EventNotificationAlert_VideoTamperingAlarmMsg</u></i> .
recordException	Recording Exception Alarm, see details in <i><u>JSON_EventNotificationAlert_RecordExceptionAlarmMsg</u></i> .
fireDetection	Fire Detection Alarm, see details in <i><u>JSON_EventNotificationAlert_fireDetection</u></i> .
TMPA	Temperature Measurement Pre-alarm, see details in <i><u>JSON_EventNotificationAlert_TMPA</u></i> .
TMA	Temperature Measurement Alarm, see details in <i><u>JSON_EventNotificationAlert_TMA</u></i> .

eventType	Event Type Name and Details
TDA	Temperature Difference Alarm, see details in <i>JSON_EventNotificationAlert_TDA</i> .
hppConnectionStatusChanged	Hik-Partner Pro Connection Status Changed Alarm, see details in <i>JSON_EventNotificationAlert_hppConnectionStatusChanged</i> .

Smart Event

eventType	Event Type Name and Details
fielddetection	Intrusion Alarm, see details in <i>JSON_EventNotificationAlert_fielddetection</i> .
linedetection	Line Crossing Alarm, see details in <i>JSON_EventNotificationAlert_linedetection</i> .
regionEntrance	Region Entrance Alarm, see details in <i>JSON_EventNotificationAlert_RegionEntranceAlarmMsg</i> .
regionExiting	Region Exiting Alarm, see details in <i>JSON_EventNotificationAlert_RegionExitingAlarmMsg</i> .

Security Control Event

eventType	Event Type Name and Details
videoReview	Video Verification Alarm, see details in <i>JSON_EventNotificationAlert_VideoVerificationAlarmMsg</i> .
CIDAlarm	CID (Contact ID) Alarm, see details in <i>JSON_EventNotificationAlert_CidAlarmMsg</i> .
PIR	PIR Alarm. See details in <i>JSON_EventNotificationAlert_PIR</i> .

Access Control Event

eventType	Event Type Name and Details
requestVoiceTalkEvent	Two-way Audio Request Alarm, see details in <i>JSON_EventNotificationAlert_requestVoiceTalkEvent</i>
cancelVoiceTalkEvent	Two-way Audio Canceling Alarm, see details in <i>JSON_EventNotificationAlert_cancelVoiceTalkEvent</i> .

Radar Event

eventType	Event Type Name and Details
fallingDown	Falling Down Alarm. See details in <u><i>JSON_EventNotificationAlert_FallingDownAlarmMsg</i></u> .
longTimeLeave	Prolonged Bed Exit Alarm. See details in <u><i>JSON_EventNotificationAlert_longTimeLeave</i></u> .
heartBeatAbnormal	Irregular Heartbeat Alarm. See details in <u><i>JSON_EventNotificationAlert_heartBeatAbnormal</i></u> .
respireAbnormal	Abnormal Respiratory Rate Alarm. See details in <u><i>JSON_EevntNotificationAlert_respireAbnormal</i></u> .

Appendix C. Status Codes

The status classification of this SDK is based on the status codes of HTTP. 7 kinds of status codes are predefined, including 1 (OK), 2 (Device Busy), 3 (Device Error), 4 (Invalid Operation), 5 (Invalid Message Format), 6 (Invalid Message Content), and 7 (Reboot Required). Each kind of status code contains multiple sub status codes.

StatusCode=1

SubStatusCode	Error Code	Description
ok	0x1	Operation completed.
riskPassword	0x10000002	Risky password.

StatusCode=2

SubStatusCode	Error Code	Description
noMemory	0x20000001	Insufficient memory.
upgrading	0x20000003	Upgrading.
networkError	0x20000009	Network error.

StatusCode=3

SubStatusCode	Error Code	Description
deviceError	0x30000001	Device hardware error.
createSocketError	0x30000004	Creating socket failed.
sendRequestError	0x30000006	Sending request failed.
passwordDecodeError	0x30000008	Decrypting password failed.
passwordEncryptError	0x30000009	Encrypting password failed.
pictureUploadFailed	0x3000000B	Uploading picture failed.
connecteDatabaseError	0x3000000E	Connecting to database failed.
internalError	0x30000014	Internal error.
uninitialized	0x3000000C	Uninitialized.

Status Code=4

SubStatusCode	Error Code	Description
notSupport	0x40000001	Not supported.
lowPrivilege	0x40000002	No permission.
badAuthorization	0x40000003	Authentication failed.
methodNotAllowed	0x40000004	Invalid HTTP method.
notActivated	0x40000007	Inactivated.
hasActivated	0x40000008	Activated.
invalidContent	0x4000000A	Invalid message content.
maxSessionUserLink	0x4000000B	No more user can log in.
loginPasswordError	0x4000000C	Incorrect password.
MgmtLokedError	0x4000000D	Logging in management platform failed. IP is locked.
interfaceOperationError	0x40001002	Operation failed.
openFileError	0x40001014	Opening file failed.
taskPacking	0x40001034	The resource is already occupied.
taskNoRecFile	0x40001039	The video file does not exist.
updateLangUnmatched	0x40001042	Upgrade packet language mismatches.
userMaxNum	0x40001047	No more user can be added.
monitorNodeOverLimit	0x4000104D	No more camera can be added.
deviceExist	0x40001054	The device is already added.
pwdErrorLoginFailed	0x40001055	Login failed. Check the user name and password.
setArmingError	0x40001083	Setting arming information failed.
taskModifyFailed	0x400010B1	Editing task failed.
getDeviceInfoFailed	0x400010BC	Getting device information failed.
noDiskSpace	0x400010E6	Insufficient HDD space.
cannotSameAsOldPassword	0x400010E8	The new password and old password must be different.
originalPassError	0x400010E9	Incorrect old password.

SubStatusCode	Error Code	Description
writeFileError	0x400010EA	Writing file failed.
accessFileDirectoryFailed	0x40001104	Accessing file path failed.
unKnownErrorCode	0x4000111D	Unknown error code.
deviceVervisionNotMatch	0x40001128	Device version mismatches.
theSessionIdDoesNotExist	0x40001135	The session ID does not exist.
theCameraIdDoesNotExist	0x40001137	The camera ID does not exist.
theDeviceIdDoesNotExist	0x4000113B	The device ID does not exist.
gettingResourceNodeInformationFailed	0x40001176	Getting resource node information failed.
noMoreTasksCanBeAdded	0x4000118A	No more task can be added.
theZoneAlreadyExists	0x40001388	The zone already exist.
thePartitionAlreadyExists	0x40001389	The partition(area) already exists.
thePartitionRelatedZone	0x4000138A	The partition(area) has been linked to zone(s). Cancel the linkage to delete the partition(area).

StatusCode=5

SubStatusCode	Error Code	Description
badJsonFormat	0x50000002	Invalid JSON format.
badURLFormat	0x50000003	Invalid URL format.

StatusCode=6

SubStatusCode	Error Code	Description
badParameters	0x60000001	Incorrect parameter.
badXmlContent	0x60000003	Incorrect XML message content.
badPort	0x6000000B	Port number conflicted.
portError	0x6000000C	Invalid port number.
badVersion	0x6000000F	Version mismatches.
requestMemoryNULL	0x6000003F	No memory is requested.

SubStatusCode	Error Code	Description
tokenTimeout	0x600000040	The token timed out.
passwordLenNoMoreThan16	0x60000005F	Up to 16 characters are allowed in the password.
eventCodeExist	0x600000060	The event code already exists.
diskError	0x60001009	HDD error.

StatusCode=7

SubStatusCode	Error Code	Description
rebootRequired	0x700000001	Reboot device to take effect.

Appendix D. Event Code List

This event code list includes the CID code and SIA code of security control device, encoding device, access control and device online/offline event.

- For event codes of security control device, see [***Event Codes of Security Control Device***](#) .
- For event codes of encoding device, see [***Event Codes of Encoding Device***](#) .
- For event codes of access control device, see [***Event Codes of Access Control Device***](#) .
- For event codes of radars, see [***Event Codes of Radar Device***](#) .
- For event codes of device and platform status, see [***Event Codes of Device/Platform Status***](#) .

D.1 Event Codes of Security Control Device

The following table displays the event codes of security control devices.

HikCode	CIDCode	SIACode	Description
1100	E100	MA	Medical Alarm
1103	E130	BA	Burglary Alarm
1110	E111	FA	Fire Alarm
1114	E114	KA	Fire Alarm
1121	E121	HA	Duress
1122	E122	HA	Silent Panic Alarm
1123	E123	AA	Audible Panic Alarm
1124	E133	AB	24H Alarm
1125	E133	BA	24H Vibration Alarm
1126	E130	BA	Timeout Alarm
1127	E120	BA	Silent Panic Alarm
1129	E120	PA	Panic Alarm
1130	E130	BA	Burglary Alarm
1131	E131	BA	Perimeter Alarm
1132	E132	AD	Interior Burglary Alarm
1133	E130	BA	24H Alarm
1134	E134	BA	Entry/Exit Alarm

HikCode	CIDCode	SIACode	Description
1137	E316	TA	Device Tampered
1139	E139	BV	Confirmed Alarm
1141	E141	AE	BUS Open-circuit Alarm
1142	E142	AF	BUS Short-circuit Alarm
1144	E144	TA	External Probe Disconnected
1148	E145	AG	Device Motion Alarm
1149	E137	BA	Masking Alarm
1151	E162	GA	Gas Leakage Alarm
1154	E154	WA	Water Leakage Alarm
1207	E207	AH	Zone Early-Warning
1301	E301	AT	AC Power Loss
1302	E302	YT	Low System Battery
1305	E305	ZY	Control Panel Reset
1310	E311	YT	Battery Fault
1311	E311	YM	Battery Disconnected
1312	E312	YI	Overcurrent Protection Triggered
1313	E313	YT	Battery Fault
1314	E314	YM	Battery Missing
1318	E311	YM	Power Depletion
1319	E319	YP	Overvoltage Protection Triggered
1328	E328	AI	Power Output Short Circuit
1330	E330	ET	Expander Fault
1333	E333	AI	Expander Exception
1336	E336	AJ	Printer Disconnected

HikCode	CIDCode	SIACode	Description
1337	E338	XT	Repeater Battery Low
1338	E338	AL	Expander Low Voltage
1339	E301	YP	Mains Power Lost
1340	E311	YM	Repeater Battery Disconnected
1341	E144	TA	Lid Opened
1342	E301	YP	Expander AC Power Loss
1343	E144	TA	Wireless Repeater Tampered
1344	E144	TA	Wireless Siren Tampered
1345	E381	XL	Wireless Siren Disconnected
1346	E144	TA	Wireless Device Tampered
1347	E384	XT	Low Wireless Device Battery
1348	E381	XL	Wireless Device Disconnected
1349	E337	YP	External Power Failure
1351	E351	LT	Main Channel ATP Fault
1352	E352	LT	Backup Channel ATP Fault
1354	E354	AM	Telephone Line Disconnected
1359	E354	YC	Uploading Report Failed
1380	E380	FT	Detector Sensor Fault
1382	E382	AN	BUS Supervision Fault
1383	E144	TA	Detector Tampered

HikCode	CIDCode	SIACode	Description
1386	E386	AO	Zone Open-circuit Alarm
1387	E387	AP	Zone Short-circuit Alarm
1401	E401	OP	Disarming
1403	E403	OA	Auto Disarming
1406	E406	BC	Alarm Clearing
1409	E409	CS	Keyswitch Zone Disarming
1443	E443	AQ	Turn On Output by Schedulet
1452	E452	CT	Late to Disarm
1455	E455	CD	Auto Arming Failed
1460	E460	AR	Turning On Output Failed
1461	E461	AS	Turning Off Output Failed
1462	E462	AT	Auto Disarming Failed
1467	E461	JA	Incorrect Password
1556	E556	AT	Network Change
1570	E570	QB	Zone Bypassed
1571	E570	QB	Deactivated Temporarily
1572	E383	TU	Lid Deactivated / Lid Was Temporarily Disabled
1573	E573	QB	Deactivated
1574	E574	AU	Group Bypass
1601	E601	AV	Manual Report Test
1602	E602	RP	Periodic Report Test
1607	E607	TS	Test Mode Entered

HikCode	CIDCode	SIACode	Description
1617	E617	AW	Telephone Connection Test
1627	E627	LB	Enter Programming
1628	E628	LX	Exit Programming
1750	E750	IA	Drilling alarm
1753	E158	KS	High Temperature Alarm
1754	E159	ZA	Low Temperature Alarm
1755	E755	UB	Permanent Deactivation-Alarm Only
1756	E756	UB	One-Time Deactivation-Alarm Only
1757	E757	UA	Technical Zone Alarm
1759	E131	BA	Intrusion Alarm
1761	E761	TS	Enter Soak Test
1762	E762	NC	Bus Loop Disconnected
1766	E766	UX	Link Wireless Detector/Peripheral to Receiver
1767	E767	OT	Delay Auto-Arming
1770	E770	RS	Replace Detector/Peripheral
1773	E131	BA	Cross-Zone Alarm
1774	E774	AX	PIR Alarm
1775	E775	AY	Sudden Increase of Sound Intensity Alarm
1776	E776	AZ	Sudden Decrease of Sound Intensity Alarm
1777	E777	BA	Audio Input Fault

HikCode	CIDCode	SIACode	Description
1778	E131	BA	Line Crossing Alarm
1779	E134	BA	Region Entrance Detection
1780	E112	FA	Fire Source Alarm
1781	E158	KS	High Temperature Pre-Alarm
1782	E159	ZS	Low Temperature Pre-Alarm
1783	E158	KA	High Temperature Alarm
1784	E159	ZA	Low Temperature Alarm
1785	E134	EA	Region Exiting Detection
1786	E153	KT	Temperature Alarm
1810	E120	PA	Keypad/Keyfob Panic Alarm
1811	E110	FA	Keypad/Keyfob Fire Alarm
1812	E812	BB	Keypad/Keyfob Burglary Alarm
1822	E454	CI	Arming Failed
1847	E100	MA	Keypad/Keyfob Medical Alarm
1862	E501	DK	Keypad Locked
1863	E863	BC	Absence Alarm
1864	E501	DK	Tag Reader Locked
1865	E421	BD	Unregistered Tag
1910	E910	BE	Keypad Disconnected
1911	E911	BF	KBUS Relay Disconnected

HikCode	CIDCode	SIACode	Description
1912	E912	BG	KBUS GP/K Disconnected
1913	E913	BH	KBUS MN/K Disconnected
1914	E381	XL	Wireless Detector Disconnected
1915	E384	XT	Wireless Detector Low Battery
1916	E381	XL	Expander Disconnected
1917	E381	XL	Wireless Repeater Disconnected
1918	E918	BI	Radar Transmitter Fault
1919	E384	XT	Wireless Siren Low Battery
1920	E920	NT	Cellular Data Network Disconnected
1921	E921	NT	SIM Card Exception
1922	E922	NT	Wi-Fi Communication Fault
1923	E344	XQ	RF Signal Exception
1924	E924	NT	Network Flow Exceeded
1925	E384	XT	Low Keyfob Battery
1926	E926	NT	SIM Card Phone Number Conflicted
1930	E930	NT	IP Address Conflicted
1931	E931	NT	Wired Network Exception
1940	E131	BA	Motion Detection Alarm Started
1941	E941	BA	Masking Alarm

HikCode	CIDCode	SIACode	Description
1942	E942	BK	Video Signal Loss
1943	E943	BL	Input/Output Format Unmatched
1944	E944	BM	Video Input Exception
1945	E945	BN	Full HDD
1946	E946	BO	HDD Exception
1947	E947	BP	Upload Picture Failed
1948	E948	BQ	Sending Email Failed
1949	E949	BR	Network Camera Disconnected
1960	E960	BS	Duty Checking
1961	E961	BT	Post Response
1962	E962	BU	Fire Alarm Consulting
1963	E963	BV	Duress Alarm Consulting
1964	E964	BW	Emergency Medical Alarm Consulting
1970	E970	BX	BUS Query
1971	E971	BY	BUS Registration
1973	E973	BZ	Single-Zone Disarming
1974	E974	CA	Single-Zone Alarm Cleared
1975	E306	CB	Detector Deleted
1976	E976	CC	Business Consulting
1977	E306	CD	Expander Deleted
1978	E306	CE	Wireless Repeater Deleted
1979	E306	CF	Wireless Siren Deleted
1980	E306	CG	Wireless Device Deleted

HikCode	CIDCode	SIACode	Description
1982	E306	XI	Panel Reset to Factory Settings
1983	E983	RB	Upgrading Firmware
1984	E984	RS	Upgrading Firmware Failed
1985	E985	UR	User has been removed
1986	E986	UR	User has been removed
1987	E383	TB	Notifications about the state of the lid are disabled
1988	E570	QB	Device deactivated
1989	E100	MA	Silent Medical Alarm
1991	E991	YI	Bus Overload
3100	R100	MH	Medical Alarm Restored
3103	R130	BH	Burglary Alarm Restored
3110	R111	FH	Fire Alarm Restored
3114	R114	KH	Fire Alarm Restored
3122	R122	HH	Silent Panic Alarm Restored
3123	R123	CH	Audible Panic Alarm Restored
3124	R133	CI	24H Alarm Restored
3125	R133	BH	24H Vibration Alarm Restored
3126	R130	BH	Timeout Alarm Restored
3129	R120	PH	Panic Alarm Restored

HikCode	CIDCode	SIACode	Description
3130	R130	BH	Burglary Alarm Restored
3131	R131	BH	Perimeter Alarm Restored
3132	R132	CK	Interior Burglary Alarm Restored
3133	R130	BH	24H Alarm Restored
3134	R134	BH	Entry/Exit Alarm Restored
3137	R316	TR	Device Tamper Restored
3139	R139	BW	Confirmed Alarm Restore
3141	R141	CL	BUS Open-circuit Restored
3142	R142	CN	BUS Short-circuit Restored
3144	R144	TR	External Probe Connected
3148	R145	CO	Device Motion Alarm Restored
3149	R137	BH	Masking Alarm Restored
3151	R162	GH	Gas Leakage Alarm Restored
3154	R154	WH	Water Leakage Alarm Restored
3207	R207	CP	Zone Early-Warning Dismissed
3301	R301	AR	AC Power Restored
3302	R302	YR	Low System Battery Restored
3310	R311	YR	Battery Fault Restored

HikCode	CIDCode	SIACode	Description
3311	R311	YR	Battery Reconnected
3312	R312	YJ	Overcurrent Protection Restored
3313	R311	YR	Battery is OK
3314	R311	YR	Battery Reconnected
3319	R319	YQ	Overvoltage Protection Restored
3328	R328	CQ	Power Output Short Circuit Restored
3330	R330	ER	Expander Fault Restored
3333	R333	CQ	Expander Restored
3336	R336	CR	Printer Connected
3337	R338	XR	Repeater Battery Voltage Restored
3338	R338	CS	Normal Expander Voltage
3339	R301	YQ	Mains Power Restored
3340	R311	YR	Repeater Battery Reconnected
3341	R144	TR	Lid Restored
3342	R301	YQ	Expander AC Power Loss Restored
3343	R144	TR	Wireless Repeater Tamper Restored
3344	R144	TR	Wireless Siren Tamper Restored
3345	R381	XC	Wireless Siren Connected
3346	R144	TR	Wireless Device Tamper Restored

HikCode	CIDCode	SIACode	Description
3347	R384	XR	Low Wireless Device Battery Restored
3348	R381	XC	Wireless Device Connected
3349	R337	YQ	External Power Restored
3351	R351	LR	Main Channel ATP Restored
3352	R352	LR	Backup Channel ATP Restored
3354	R354	CU	Telephone Line Connected
3359	R354	YK	Report Uploading Restored
3380	R380	FJ	Detector Sensor Fault Restored
3382	R382	CV	BUS Supervision Restored
3383	R144	TR	Detector Tamper Restored
3400	R400	CL	Arming
3401	R401	CL	Away Arming
3403	R403	CA	Auto Arming
3408	R408	CW	Instant Arming
3409	R409	OS	Keyswitch Zone Arming
3441	R441	NL	Stay Arming
3442	R442	CX	Forced Arming
3443	R443	CX	Turn Off Output by Schedule
3570	R570	QU	Zone Bypass Restored
3571	R570	QU	Active Again

HikCode	CIDCode	SIACode	Description
3572	R383	QU	Active Again
3573	R573	BU	Restored after auto deactivation
3574	R574	CZ	Group Bypass Restored
3607	R607	TE	Test Mode Exited
3750	R750	IR	Drilling Alarm Restored
3753	R158	KA	High Temperature Alarm Restored
3754	R159	ZH	Low Temperature Alarm Restored
3757	R757	UH	Technical Zone Alarm Restored
3759	R131	BH	Intrusion Detection Restored
3761	R761	TE	Exit Soak Test
3762	R762	NR	Bus Loop Restored
3770	R770	RU	Replacing Detector/Peripheral Failed
3773	R131	BH	Cross-Zone Alarm Restored
3774	R774	CZ	PIR Alarm Restored
3775	R775	DE	Sudden Increase of Sound Intensity Alarm Restored
3776	R776	DF	Sudden Decrease of Sound Intensity Alarm Restored
3777	R777	DC	Audio Input Restored
3778	R131	BH	Line Crossing Alarm Restored
3780	R112	FH	Fire Source Alarm Restored

HikCode	CIDCode	SIACode	Description
3781	R158	KR	High Temperature Pre-Alarm Restored
3782	R159	ZR	Low Temperature Pre-Alarm Restored
3783	R158	KH	High Temperature Alarm Restored
3784	R159	ZH	Low Temperature Alarm Restored
3786	R153	KJ	Temperature Alarm Restored
3862	R501	DO	Keypad Unlocked
3864	R501	DO	Tag Reader Unlocked
3900	R400	CF	The area has been armed with faults
3910	R910	DH	Keypad Connected
3911	R911	DI	KBUS Relay Connected
3912	R912	DF	KBUS GP/K Connected
3913	R913	DG	KBUS MN/K Connected
3914	R381	XC	Wireless Detector Connected
3915	R384	XR	Normal Wireless Detector Battery
3916	R381	XC	Expander Connected
3917	R381	XC	Wireless Repeater Connected
3918	R918	DL	Radar Transmitter Restored
3919	R384	XR	Normal Wireless Siren Battery
3920	R920	NR	Cellular Data Network Connected
3921	R921	NR	SIM Card Restored

HikCode	CIDCode	SIACode	Description
3922	R922	NR	Wi-Fi Connected
3923	R344	XH	Normal RF Signal
3925	R384	XR	Low Keyfob Battery Restored
3930	R930	NR	Normal IP address
3931	R931	NR	Normal Wired Network
3940	R131	BH	Motion Detection Alarm Stopped
3941	R941	BH	Masking Alarm Restored
3942	R942	DK	Video Signal Restored
3943	R943	DL	Input/Output Format Restored
3944	R944	DM	Video Input Restored
3945	R945	DN	Free HDD
3946	R946	DO	HDD Restored
3949	R949	DS	Network Camera Connected
3962	R962	DQ	Fire Alarm Consulting Over
3963	R963	DU	Duress Alarm Consulting Over
3964	R964	DV	Emergency Medical Alarm Consulting Over
3965	R965	DW	Patrol
3973	R973	DX	Single-Zone Arming
3975	R306	DY	Detector Added
3976	R976	DZ	Business Consulting Over
3977	R306	EA	Expander Added

HikCode	CIDCode	SIACode	Description
3978	R306	EB	Wireless Repeater Added
3979	R306	EC	Wireless Siren Added
3980	R306	ED	Wireless Device Added
3984	R984	RS	The firmware has updated
3985	R985	UA	New user has been added
3987	R383	TU	Notifications about the state of the lid are enabled
3988	R570	QU	The device is active again

D.2 Event Codes of Encoding Device

The following table displays the event codes of encoding device.

Original Code	CID Code	SIA Code	Event Name
IO	E900	VA	IO Alarm
VMD	E901	VB	Motion Detection Alarm
diskerror	E902	VC	Disk Error Alarm
diskfull	E903	VD	Disk Full Alarm
diskrecover	E904	VE	Disk Restored Alarm
fielddetection	E905	VF	Intrusion Detection Alarm
linedetection	E906	VG	Line Crossing Detection Alarm
rapidMove	E907	VH	Fast Moving Alarm
recordException	E908	VI	Recording Exception Alarm
regionEntrance	E909	VJ	Region Entrance Detection Alarm
regionExiting	E910	VK	Region Exiting Detection Alarm
shelteralarm	E911	VL	Video Tampering Alarm

Original Code	CID Code	SIA Code	Event Name
videoloss	E912	VM	Video Loss Alarm
fireDetection	E913	VN	Fire Detection Alarm
TMPA	E914	VO	Temperature Measurement Precautionary Alarm
TMA	E915	VP	Temperature Measurement Alarm
TDA	E916	VQ	Temperature Diff Alarm

D.3 Event Codes of Radar Device

The following is the event codes of radar devices.

HikCode	CIDCode	SIACode	Description
fallingDown	E700	RA	Person Fall Alarm
longTimeLeave	E701	RB	Prolonged Bed Exit Alarm
heartBeatAbnormal	E702	RC	Irregular Heartbeat Alarm
respireAbnormal	E703	RD	Abnormal Respiratory Rate Alarm

D.4 Event Codes of Access Control Device

The following table displays the event codes of access control devices.

HikCode	CIDCode	SIACode	Description
requestVoiceTalkEvent	E800	DA	Request Voice Talk Interactive Event
cancelVoiceTalkEvent	R800	NA	Cancel Voice Talk Interactive Event

D.5 Event Codes of Device/Platform Status

The following is the event codes of Device/Platform Status.

Original Code	CID Code	SIA Code	Event Name
deviceoffline	E350	OF	Device Offline Alarm
deviceonline	R350	ON	Device Online Alarm
devicedeleted	E349	OD	Device Deleted from HPP Alarm
deviceKeyAbnormal	E500	KA	Device Key Exception
deviceKeyNormal	R500	KR	Device Key Exception Restored
hppConnectAbnormal	E600	HA	Communication Exception Between IP Receiver Pro and Hik-Partner Pro
hppConnectNormal	R600	RA	Communication Restored Between IP Receiver Pro and Hik-Partner Pro
deviceHppAbnormal	E400	DA	Device Network Exception on Hik-Partner Pro
deviceHppNormal	R400	DN	Device Network Exception Restored on Hik-Partner Pro



See Far, Go Further