Hik-Partner Pro OpenAPI V2.14.0

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.

Contents

Chapter 1 Overview

1.1 Introduction

This document introduces the open capabilities and APIs provided by Hik-Partner Pro for the third-party manufacturers or developers to fast integrate related applications, including managing sites, managing devices, subscribing to and receiving alarms, ARC services, etc.

1.2 Update History

Summary of Changes in Version 2.14.0_October, 2025

1. Added a typical application: ***Webhook Message Push*** .
   - Added an API to get the message push configuration: ***POST /api/hpcgw/webhook/v1/config/query*** .
   - Added an API to save message push configurations: ***POST /api/hpcgw/webhook/v1/config/save*** .
   - Added an API to delete message push configurations: ***POST /api/hpcgw/webhook/v1/config/delete*** .
2. Deleted the field **picUrl** from response parameters of API ***POST /api/hpcgw/v1/device/camera/list*** .
3. Deleted the field **X-Username** from request parameters of API ***PUT /api/hpcgw/v2/device/transparent/otap/multi/prop/get*** .
4. Extended the request header of API ***PUT /api/hpcgw/v2/device/transparent/otap/multi/prop/put*** : added a field **X-UserType** (user type of AX Pro devices) .
5. Extended the CID event information ***JSON_EventNotificationAlert_cidEvent*** : added a field **standardCode** (CID event standard code).

Summary of Changes in Version 2.13.0_May, 2025

1. Added one API for uploading an audio file: ***POST /api/hpcgw/v1/audio/file/upload*** .
2. Added one API for applying the audio file to a device: ***POST /api/hpcgw/v1/audio/file/add*** .
3. Added one API for getting the device's audio files: ***POST /api/hpcgw/v1/audio/file/list/get*** .
4. Added one API for deleting audio files: ***POST/ api/hpcgw/v1/audio/file/del*** .
5. Added one API for the audio file cut-in: ***POST /api/hpcgw/v1/audio/inter/cut*** .
6. Added two error codes: VMS022554 (physical resources do not exist) and VMS050034 (linked device not found). See details in ***Status or Error Code*** .

Summary of Changes in Version 2.11.800_Feb, 2025

1. Extended the response parameters of ***POST /api/hpcgw/v1/device/list*** .
2. Added 11 APIs transmitted via OTAP protocol: ***GET/PUT/POST/DELETE /api/hpcgw/v2/device/transparent/{otap uri}*** .

- Get property: ***GET /api/hpcgw/v2/device/transparent/otap/prop*** ;
- Set property: ***PUT /api/hpcgw/v2/device/transparent/otap/prop*** ;
- Get property directly from device: ***GET /api/hpcgw/v2/device/transparent/otap/direct*** ;
- Set property directly for device: ***PUT /api/hpcgw/v2/device/transparent/otap/direct*** ;
- Perform operations on device: ***PUT /api/hpcgw/v2/device/transparent/otap/action*** ;
- Search for object model definition: ***POST /api/hpcgw/v2/device/transparent/otap/product/profile*** ;
- Batch get properties: ***POST /api/hpcgw/v2/device/transparent/otap/multi/prop/get/by/shadow*** ;
- Batch set properties: ***PUT /api/hpcgw/v2/device/transparent/otap/multi/prop/put/by/shadow*** ;
- Batch get properties directly from device: ***PUT /api/hpcgw/v2/device/transparent/otap/multi/prop/get*** ;
- Batch set properties directly for device: ***PUT /api/hpcgw/v2/device/transparent/otap/multi/prop/put*** ;
- Get OTAP list data: ***GET /api/hpcgw/v2/device/transparent/api/service/device/otap/table/list?pageIndex=%s&pageSize=%s*** .

3. Added 6 device related APIs:
    - Search for device PIN code: ***POST /api/hpcgw/v1/device/pincode/query*** ;
    - Upgrade device: ***POST /api/hpcgw/v1/device/upgrade*** ;
    - Get the upgrade progress of device: ***POST /api/hpcgw/v1/device/upgrade/progress*** ;
    - Check whether the object model device adding capability is supported: ***POST /api/hpcgw/v1/device/iot/ability/query*** ;
    - Search for adding status of the object model device: ***POST /api/hpcgw/v1/device/iot/add/result*** ;
    - Wake up solar camera: ***POST /api/hpcgw/v1/device/camera/wakeUp*** .
4. For ARC service related APIs:
    - Extended the request parameters in ***POST /api/hpcgw/v1/arcservice/device/list*** ;
    - Added the API of editing the ARC event list of device: ***POST /api/hpcgw/v1/arcservice/event/type/update*** ;
    - Added the API of editing device account No.: ***POST /api/hpcgw/v1/arcservice/account/number/update*** .
5. Added the API of activating device maintenance package: ***POST /api/hpcgw/v1/vas/opspack/active*** .
6. Extended ***Status or Error Code*** , ***Event Details*** , etc.

Summary of Changes in Version 2.0.0_Mar, 2024

1. Added typical applications for hot spare devices: ***Hot Spare*** .
    - added the API calling flow for host device related functions ***API Calling Flow for Hot Spare (Host)*** ;
    - added the API calling flow for spare device related functions ***API Calling Flow for Hot Spare (Spare)*** .
2. Added APIs for operations on hot spare devices:

  - added an API of adding and configuring hot spare device ***POST /api/hpcgw/v1/hotspare/add*** ;
  - added an API of searching for hot spare device information ***POST /api/hpcgw/v1/hotspare/get*** ;
  - added an API of deleting hot spare device(s) ***POST /api/hpcgw/v1/hotspare/delete*** ;
  - added an API of checking if the host device is offline via heartbeat ***POST /api/hpcgw/v1/hotspare/heartbeat*** ;
  - added an API of uploading hot spare file: ***POST /api/hpcgw/v1/hotspare/file/upload*** ;
  - added an API of getting hot spare file download URL ***POST /api/hpcgw/v1/hotspare/file/downloadurl*** ;
  - added an API of searching for uploaded hot spare files ***POST api/hpcgw/v1/hotspare/file/get*** ;
  - added an API of deleting hot spare file ***POST /api/hpcgw/v1/hotspare/file/delete*** .

3. Added status/error codes for hot spare device (LAP026338, LAP026339, LAP026341, LAP026342, and LAP068001): ***Status or Error Code*** .

Summary of Changes in Version 1.9_Sep, 2023

1. Added an API for getting the list of site managers: ***POST /api/hpcgw/v1/site/sitemanagers*** .
2. Added an API for handing over sites by sharing: ***POST /api/hpcgw/v2/site/handover/share*** .
3. Added an API for searching for list of end users of handover by sharing: ***POST /api/hpcgw/v2/site/customer/list*** .
4. Added an API for searching for end user information of handover by sharing: ***POST /api/hpcgw/v1/site/customer/detail*** .
5. Added an API for modifying end user's account information: ***POST /api/hpcgw/v1/site/customer/account/update*** .
6. Added an API for modifying device permission information for end users: ***POST /api/hpcgw/v1/site/customer/devices/update*** .
7. Added an API for canceling the sharing for the end user: ***POST /api/hpcgw/v1/site/customer/cancle*** .
8. Added an API for getting the site health monitoring report: ***POST /api/hpcgw/v1/site/health/report*** .
9. Added an API for getting storage file information by time: ***POST /api/hpcgw/v1/video/by/time*** .
10. Added values for the response parameter **deviceSubCategory**: ***POST /api/hpcgw/v1/device/list*** and ***POST /api/hpcgw/v1/arcservice/device/list*** .
11. Added 4 error codes LAP008127, LAP064001, LAP064003, and LAP064007: ***Status or Error Code*** .

Summary of Changes in Version 1.8.2_Jul, 2023

Upgraded the API of assigning a single site manager to assigning multiple site managers ***POST /api/hpcgw/v2/site/assign*** :
Added two request parameters **installerPermissionTimes** and **expiredDurationTime**, and extended the request message.

Summary of Changes in Version 1.8.1_Jun, 2023

Extended the response message of the API ***POST /api/hpcgw/v1/site/search*** :
Added two nodes **siteDeliveryStatus** and **cloudEnable**.

Summary of Changes in Version 1.8.0_May, 2023

1. Added an API for searching for employee list: ***POST /api/hpcgw/v1/installers/search*** .
2. Added an API for assigning site admin: ***POST /api/hpcgw/v2/site/assign*** .
3. Extended the request message of the API ***GET/PUT/POST/DELETE /api/hpcgw/v1/device/transparent/{isapi uri}*** :
   Added a node **X-Userlevel** to the messages.
4. Added an API for enabling/disabling the device operation permission of end users: ***POST /api/hpcgw/v1/device/cloud/enable*** .
5. Added 2 error codes **LAP008044** and **LAP008077**: ***Status or Error Code*** .
6. Added a message about device added alarm information:
   JSON_EventNotificationAlert_deviceadded .

Summary of Changes in Version 1.7.0_Apr., 2023

1. Added an API for getting the upgrade status of device: ***POST /api/hpcgw/v1/device/upgrade/state*** .
2. Added fingerprint information option to the response parameter **subStatus** for ***POST /api/hpcgw/v1/acs/privilege/status*** .
3. Added an API for synchronizing person information from device to the platform: ***POST /api/hpcgw/v1/person/synchronize*** ;
   Added an API for searching for person information synchronization progress: ***POST /api/hpcgw/v1/person/synchronize/progress*** ;
   Added an API for searching for person synchronization details: ***POST /api/hpcgw/v1/person/synchronize/details*** .
4. Added 2 error codes **LAP020047** and **LAP030069**: ***Status or Error Code*** .

Summary of Changes in Version 1.6.0_Nov., 2022

1. Updated notes about the typical application of events and alarms, see details in ***Events and Alarms*** .
2. Added two flow charts about applying person information to device and deleting person information from device, see details in ***Cloud Attendance System*** . Also, updated notes about deleting persons, see details in ***Cloud Attendance System*** .
3. Extended the response messages of the API ***POST /api/hpcgw/v1/site/search*** and ***GET /api/hpcgw/v1/arcservice/site/{id}/info*** :
   Added some site-sharing-related nodes.
4. Added two APIs about sharing and canceling sharing a site: ***POST /api/hpcgw/v1/site/share*** and ***POST /api/hpcgw/v1/site/share/cancel/{id}*** .
5. Added notes about applying person information in the following APIs: ***POST /api/hpcgw/v1/person/add*** and ***POST /api/hpcgw/v1/person/update*** .

6. Extended the response message of the API ***POST /api/hpcgw/v1/acs/privilege/status*** :
   Added two nodes **subStatus** and **error** to the node **deviceLists** of **personAuthorities** of **data**.
7. Added eight error codes LAP008081, LAP008082, LAP008087, LAP008092, LAP008093, LAP008099, LAP008103, and LAP008104. See details in ***Status or Error Code*** .

Summary of Changes in Version 1.5.0_Sep., 2022

1. Changed the product name from Hik-ProConnect to Hik-Partner Pro.
2. Extended the response message of the API ***POST /api/hpcgw/v1/mq/messages*** :
   Added a sub node **deviceSerial** (device serial No.) to the node **list** of the node **data**.
3. Extended the request message of the API ***POST /api/hpcgw/v1/person/add*** and ***POST /api/hpcgw/v1/person/update*** :
   Added a node **cardNo** (card number) to the messages.
4. Added one error code LAP500007 (the number of calling times exceeds limit). See details in ***Status or Error Code*** .
5. Added an event type voiceTalkEvent (intercom event). See details in ***Event Details*** .
6. Extended the message about CID event details ***JSON_EventNotificationAlert_cidEvent*** :
   Added three sub nodes **evttype** (event type), **isTalk** (whether in two-way audio mode or not), and **media** (double video verification) to **CIDEvent**.
7. Extended the message about video review alarm information ***JSON_EventNotificationAlert_Linkage*** :
   Added a node **media** (right/left camera);
   Added two sub nodes **id** (picture ID) and **url** (URL for downloading picture) to the node **pictureList**.

Summary of Changes in Version 1.4.0_June, 2022

1. Added a node **<channelID>** to the node **<EventNotificationAlert version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">** of the message ***XML_EventNotificationAlert_regionEntrance*** and ***XML_EventNotificationAlert_regionExiting*** .

Summary of Changes in Version 1.3.0_May, 2022

1. Added a node **temp** to the node **CIDEvent**. See details in ***JSON_EventNotificationAlert_cidEvent*** .
2. Add a node **deviceSerial** to ***JSON_EventNotificationAlert_ACSEvent*** .

Summary of Changes in Version 1.2.0_Jan., 2022

1. Added an API for getting the URL for downloading an alarm-related picture. See details in ***POST /api/hpcgw/v1/alarm/pictureurl*** .
2. Added 46 error codes. See details in ***Status or Error Code*** .

Summary of Changes in Version 1.1.0_Dec., 2021

1. Added APIs for cloud attendance system. See details in ***Cloud Attendance System*** .
2. Added an alarm message for access control events. See details in ***JSON_EventNotificationAlert_ACSEvent*** .
3. Added URIs that are transmitted via ***GET/PUT/POST/DELETE /api/hpcgw/v1/device/transparent/{isapi uri}*** :
   Search for person information: POST ***/ISAPI/AccessControl/UserInfo/Search?format=json*** ;
   Search for access control events: POST ***/ISAPI/AccessControl/AcsEvent?format=json*** .
   Edit device information: PUT /ISAPI/System/deviceInfo.
   Manage all configured presets: POST /ISAPI/PTZCtrl/channels/<ID>/presets.
   Delete all presets: DELETE /ISAPI/PTZCtrl/channels/<ID>/presets.
   Get a preset: GET /ISAPI/PTZCtrl/channels/<ID>/presets/<ID>.
   Search partition status according to conditions: POST /ISAPI/SecurityCP/status/zones?format=json.
   Get or set device time parameters: PUT /ISAPI/System/time.
   Get or set all digital channels: PUT /ISAPI/ContentMgmt/InputProxy/channels.
   Create digital channels: POST /ISAPI/ContentMgmt/InputProxy/channels.

Summary of Changes in Version 1.0.0_Aug., 2021

New Document.

Chapter 2 Typical Applications

2.1 API Key

API Key is an account forHik-Partner Pro developers, which consists of API Key and API Secret. The API Key has one-to-one correspondence with the Hik-Partner Pro account. To apply for an API Key, you need to register an account first (domain name: https://hik-partner.com.). After that, you can contact the Hikvision support team to obtained the API Key. The operations conducted on the site, device, etc. by calling OpenAPI with API Key are matched with those via Hik-Partner Pro Portal/APP with Hik-Partner Pro account.

2.2 Get Token Information

The accessToken is a call credential of Open APIs, and it is obtained by API Key in the following way.

- Request URI: ***POST /api/hpcgw/v1/token/get***
- Request Parameters:

```
POST /api/hpcgw/v1/token/get HTTP/1.1
Host: api.hik-partner.com
Content-Type: application/json

{
  "appKey": "8yedmtihdf5awj4o2pf4h9fy5z0a7gr3",
  "secretKey": "b23910pv2i1myvdtn6qlr54ra2jpcp1k"
}
```

- Response Parameters:

```
{
  "data": {
    "accessToken": "hpc.6grytwlw2z1li7k0nk2v0ti2h6kipfb8",
    "expireTime": 1640416102626,
    "areaDomain": "https://isgpapi.hik-partner.com"
  },
  "errorCode": "0"
}
```

The "expireTime" in response parameters represents the expiration time of the token, which is accurate to millisecond. The obtained token is valid within 7 days. If the token expires, the error code LAP500004 will be returned, and you need to get a new token by the API key.

2.3 Site Management

The APIs related with site management are listed as below.

Function	API
Add the information of a site	***POST /api/hpcgw/v1/site/add***
Delete the information of a site	***POST /api/hpcgw/v1/site/{id}/delete***
Edit the information of a site	***POST /api/hpcgw/v1/site/{id}/update***
Search for the site information	***POST /api/hpcgw/v1/site/search***
Sharing a site	***POST /api/hpcgw/v1/site/share***
Cancel sharing a site	***POST /api/hpcgw/v1/site/share/cancel/{id}***

2.4 Device Management

Through the APIs of site management and device management, you can add, delete, edit and search devices, as well as configuring and operating devices. The integration process is as follows.

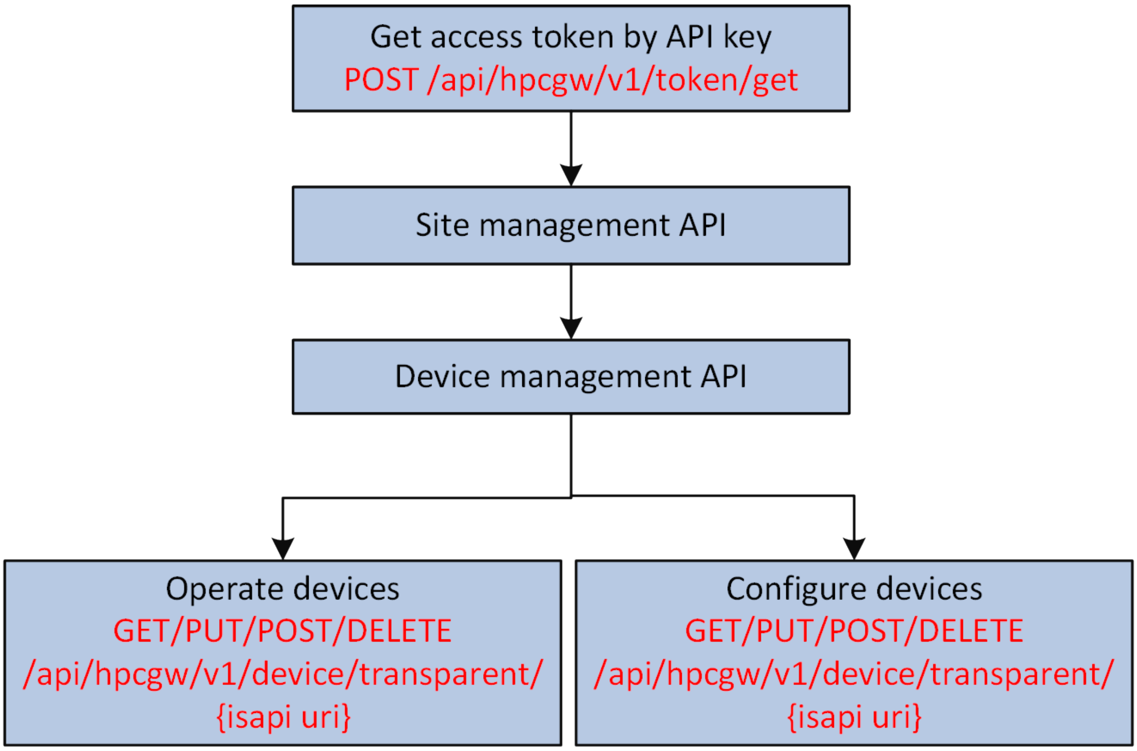

Get access token by API key
POST /api/hpcgw/v1/token/get
Site management API
Device management API
Operate devices
GET/PUT/POST/DELETE
/api/hpcgw/v1/device/transparent/{isapi uri}
Configure devices
GET/PUT/POST/DELETE
/api/hpcgw/v1/device/transparent/{isapi uri}

Figure 2-1 Device Management Integration Flow

The APIs related with device management are listed as below.

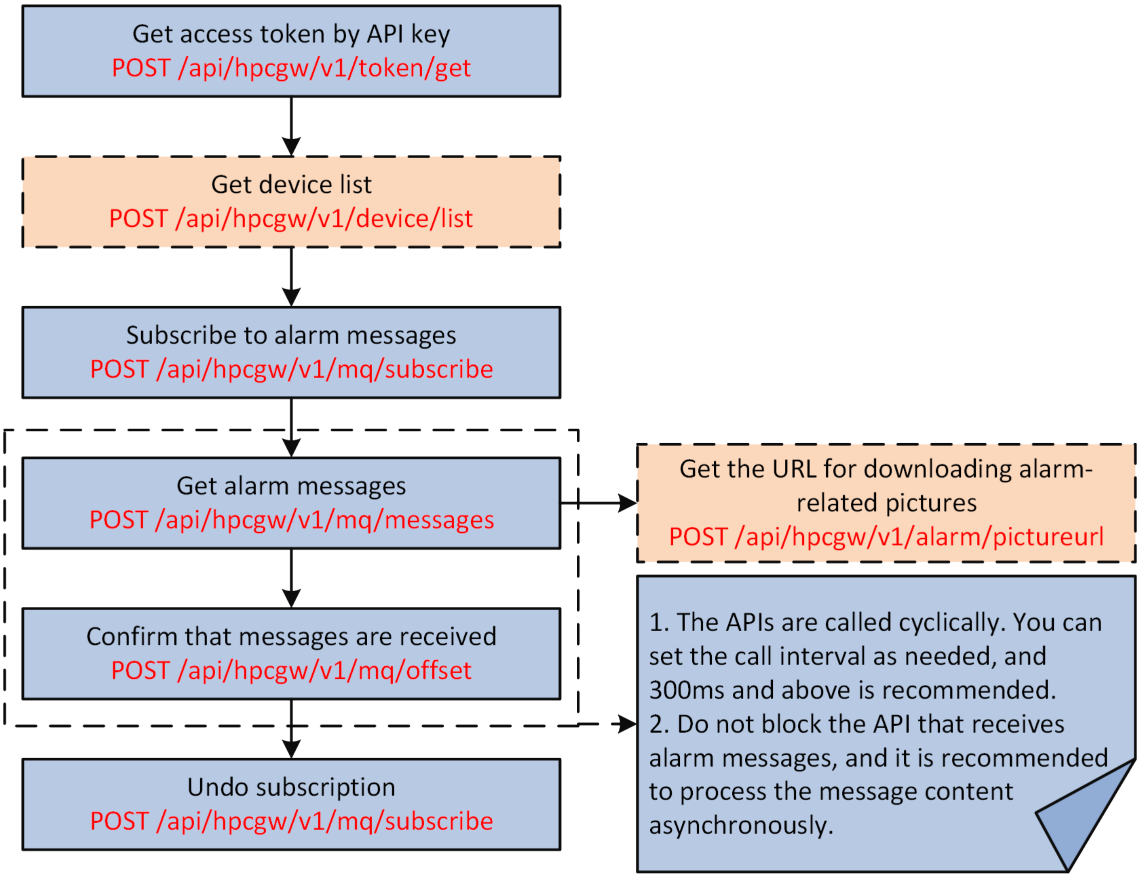
Function	API
Add the information of devices	***POST /api/hpcgw/v2/device/add***
Delete the information of a device	***POST /api/hpcgw/v1/device/delete***
Edit the information of a device	***POST /api/hpcgw/v1/device/update***
Get the device list	***POST /api/hpcgw/v1/device/list***
Get the list of channels linked with a device	***POST /api/hpcgw/v1/device/camera/list***
Transmit ISAPI protocols	***GET/PUT/POST/DELETE /api/hpcgw/v1/device/transparent/{isapi uri}***

Note

For site management APIs, refer to ***Site Management*** .

2.5 Events and Alarms

Events refer to device online/offline events, reported events and alarms by devices, and inspected events from Hik-Partner Pro. A third party platform can subscribe on-demand through the API of subscribing to alarm messages from the devices. The flow is as follows.


Get access token by API key
POST /api/hpcgw/v1/token/get
Get device list
POST /api/hpcgw/v1/device/list
Subscribe to alarm messages
POST /api/hpcgw/v1/mq/subscribe
Get alarm messages
POST /api/hpcgw/v1/mq/messages
Confirm that messages are received
POST /api/hpcgw/v1/mq/offset
Undo subscription
POST /api/hpcgw/v1/mq/subscribe
Get the URL for downloading alarm-related pictures
POST /api/hpcgw/v1/alarm/pictureurl

1. The APIs are called cyclically. You can set the call interval as needed, and 300ms and above is recommended.
2. Do not block the API that receives alarm messages, and it is recommended to process the message content asynchronously.

Figure 2-2 Integration Flow of Subscribing to Events/Alarms

The APIs related with event and alarms are listed as below.

Function	API
Subscribe to alarm messages from the devices	***POST /api/hpcgw/v1/mq/subscribe***
Get alarm messages	***POST /api/hpcgw/v1/mq/messages***
Confirm that messages are received	***POST /api/hpcgw/v1/mq/offset***
Get the URL for downloading an alarm-related picture	***POST /api/hpcgw/v1/alarm/pictureurl***

Note

The API " ***POST /api/hpcgw/v1/mq/messages*** " uses the long polling method. If there are no alarms, the API will be blocked for 20s.

Here are some notes for calling the API "Get the URL for downloading an alarm-related picture".

1. There are two types of URL format:
   a. URLs begin with "ISAPI_FILES" cannot be downloaded via the URL that is included in the alarm information. For example, ISAPI_FILES/E44034229_2/20220107064543310-E44034229-2-10000-5$encrypt=2,2022-01-07T08:58:43,107be007f872b61a720d4c1b075c968e.
      In this situation, alarm pictures cannot be downloaded via the URL that is included in the alarm information. You need to first get the URL via the API "Get the URL for downloading an alarm-related picture", and then download the alarm-related picture.
   b. The other format is "https://xxx&isEncrypted=xx&xxx&isDevVideo=xx". For example, https://ieu.ezvizlife.com/v3/alarms/pic/get?fileId=20211231074837-E61958062-1-40002-2-1&deviceSerialNo=E61958062&cn=1&isEncrypted=0&isCloudStored=0&ct=5&lc=7&bn=5_alarm.eu&isDevVideo=0.
      In this situation, alarm pictures can be downloaded via the URL that is included in the alarm information.
2. The alarm picture might be encrypted, and the decryption steps are as follows.
   a. Distinguish the encryption type by the value of **isEncrypted** or **encrypt** in the picture URL. 0 means the picture is not encrypted, 1 means it is encrypted by device, and 2 means it is encrypted by platform.
   b. Use different ways to decrypt pictures.
      i. For pictures encrypted by platform, the decryption steps are as follows.
         1. a. For the first URL type, get the values of **checksum** and **timestamp** in the URL. Perform standard SHA256 (checksum+timestampt), sort them by big endian, and get the first 16 characters which is decryption key.
            b. For the second URL type, get the values of **checksum** and **alarmTime** in the event message. Perform standard SHA256 (checksum+alarmTime), sort them by big endian, and get the first 16 characters which is decryption key.
         2. Standard AES decryption: The key is from the 48th character to the last character in the encryption file. Other parameters are: Alignment method: PKCS5Padding; Encryption and decryption mode: cbc128; Offset: 48, 49, 50, 51, 52, 53, 54, 55, 0, 0, 0, 0, 0, 0, 0, 0.
         3. You are recommended to verify the header: use the 0 to 16 characters to tell whether the fixed value **hikencodepicture** is correct or not.
      ii. For pictures encrypted by device, the stream encryption key configured by its user on the Device Configuration page is required. The decryption steps are as follows.
         1. After the device key is subjected to two md5 operations, compare it with the 16-32 bytes of the encrypted file. If they are the same, the file is correct.
         2. Get the decryption key, encode the device key in byte sequence and take the first 16 bytes, which is the decryption key.
         3. Standard AES decryption: the secret key is the 48th byte to the end of the encrypted file, use it to get the decrypted picture. Decryption parameters are as follows. Alignment mode: PKCS5; Padding Encryption mode: cbc128; Offset: 48, 49, 50, 51, 52, 53, 54, 55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0.
      iii. The pictures are distinguished between single-picture and multi-picture modes by the **isDevVideo**: 0 for single picture, 1 for multi-picture. If **isDevVideo** does not exist, it means

single picture. The method of decrypting multiple pictures is based on that of decrypting one picture. The steps are as follows.

1. Take the first 4 bytes of the encrypted file and get the value of **Len**, which is the length of the picture data bytes.
2. Take the byte stream from 0 to **Len**, which is the complete data of the first picture.
3. Decrypt the single picture data according to different encryption methods, and get the decrypted picture.
4. From the end of the previous picture, get the next picture data according to the above method, and then decrypt the data until the end of the data.

2.5.1 Event Types and Details

See ***Event Details*** for details.

2.6 ARC Service

For ARC integration, in addition to the basic APIs, special ARC Service-related APIs are provided. For ARC integration, Open APIs can be called using the ARC ID/Key applied for in the Hik-Partner Pro Portal. ARC ID and Key are equivalent to API Key and API Secret. The ARC integration flow is as follows.

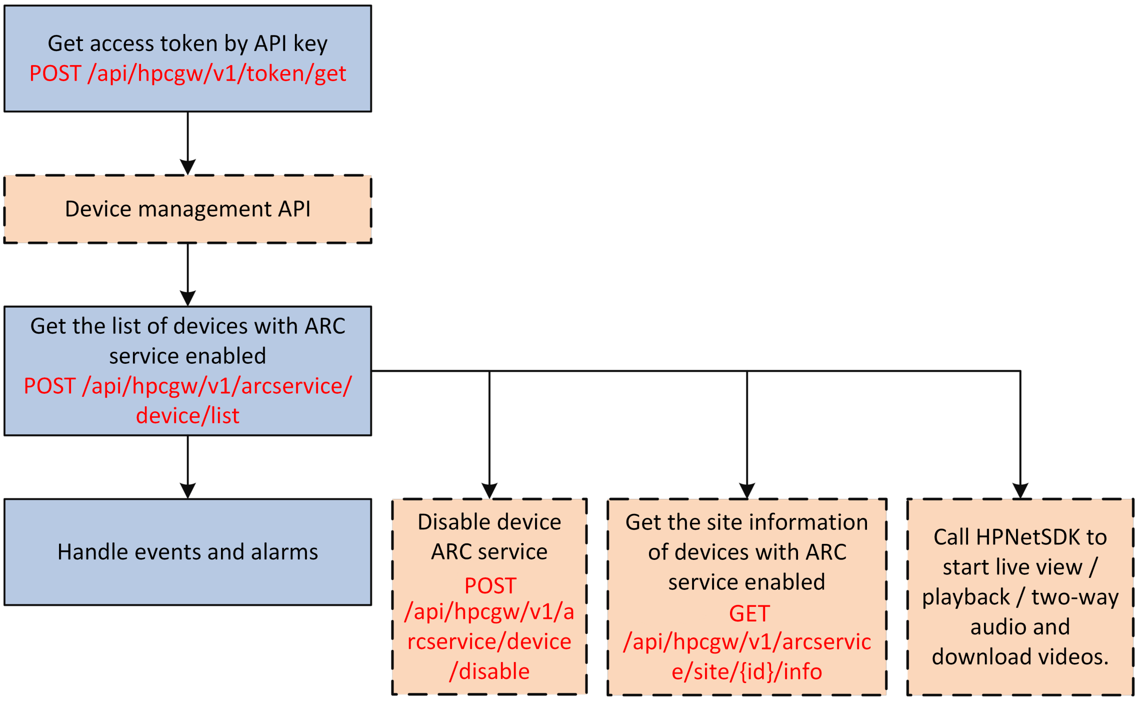

Get access token by API key
POST /api/hpcgw/v1/token/get
Device management API
Get the list of devices with ARC service enabled
POST /api/hpcgw/v1/arcservice/device/list
Handle events and alarms
Disable device ARC service
POST /api/hpcgw/v1/arcservice/device/disable
Get the site information of devices with ARC service enabled
GET /api/hpcgw/v1/arcservice/site/{id}/info
Call HPNetSDK to start live view / playback / two-way audio and download videos.

Figure 2-3 ARC Services Integration Flow

The APIs related with ARC service are listed as below.

Function	API
Get the list of devices with ARC service enabled	***POST /api/hpcgw/v1/arcservice/device/list***
Disable the ARC service of devices	***POST /api/hpcgw/v1/arcservice/device/disable***
Get the site information of devices with ARC service enabled	***GET /api/hpcgw/v1/arcservice/site/{id}/info***

Note

- For device management APIs, refer to ***Device Management*** .
- For APIs about events and alarms, refer to ***Events and Alarms*** .
- You can apply for an API key online via Hik-Partner Pro Portal.

2.7 VSaaS Service

In addition to basic device management, VSaaS integration is mainly video-related functions, including live view, playback, video download, and two-way audio, which need to be implemented using Hik-Partner Pro HPNetSDK (see HPNetSDK development Guide for details). The integration process is as follows.

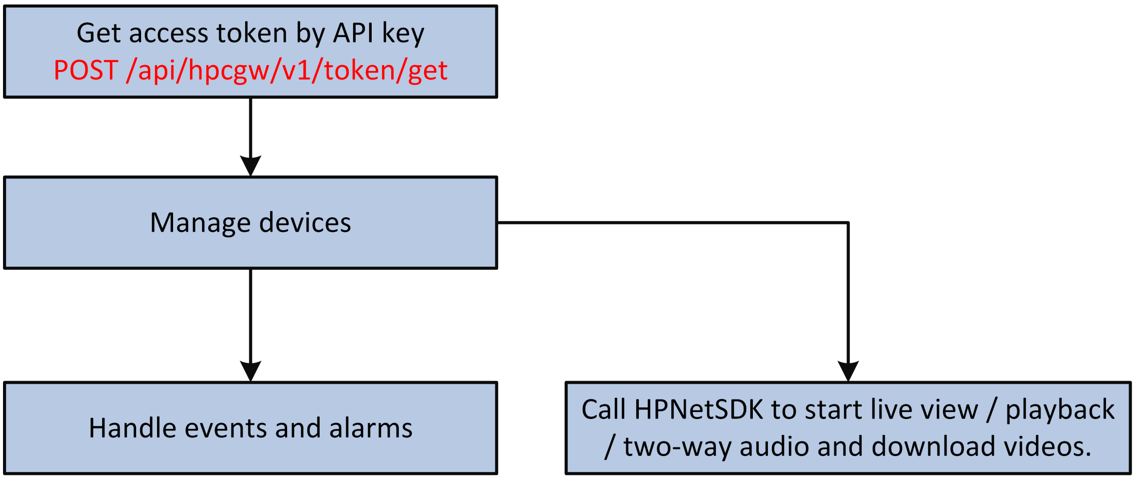

Get access token by API key
POST /api/hpcgw/v1/token/get
Manage devices
Handle events and alarms
Call HPNetSDK to start live view / playback / two-way audio and download videos.

Figure 2-4 VSaaS Service Integration Flow

Note

- For device management APIs, refer to ***Device Management*** .
- For APIs about events and alarms, refer to ***Events and Alarms*** .
- Applying for an API key for integrating VSaaS service can only be done offline via emails or other methods.

2.8 Cloud Attendance System

For cloud attendance integration, in addition to the basic APIs, special APIs related to cloud attendance integration are also provided. The integration process is as follows.

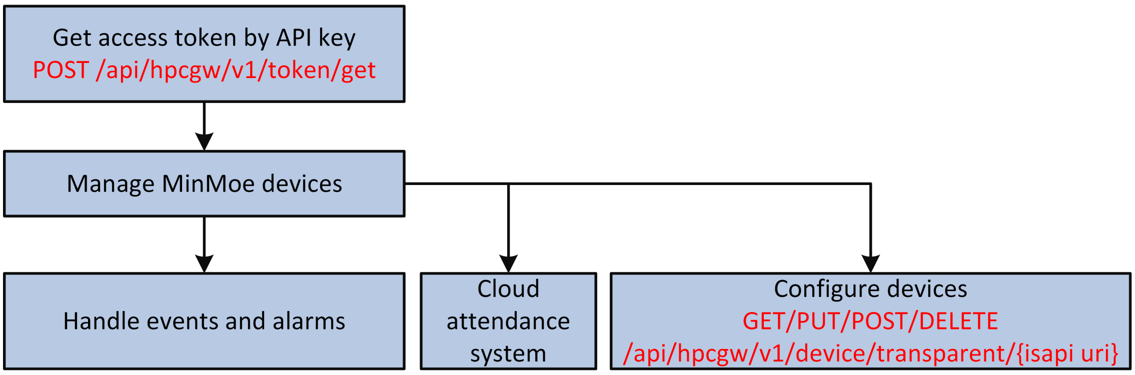


Figure 2-5 Cloud Attendance System Integration Flow

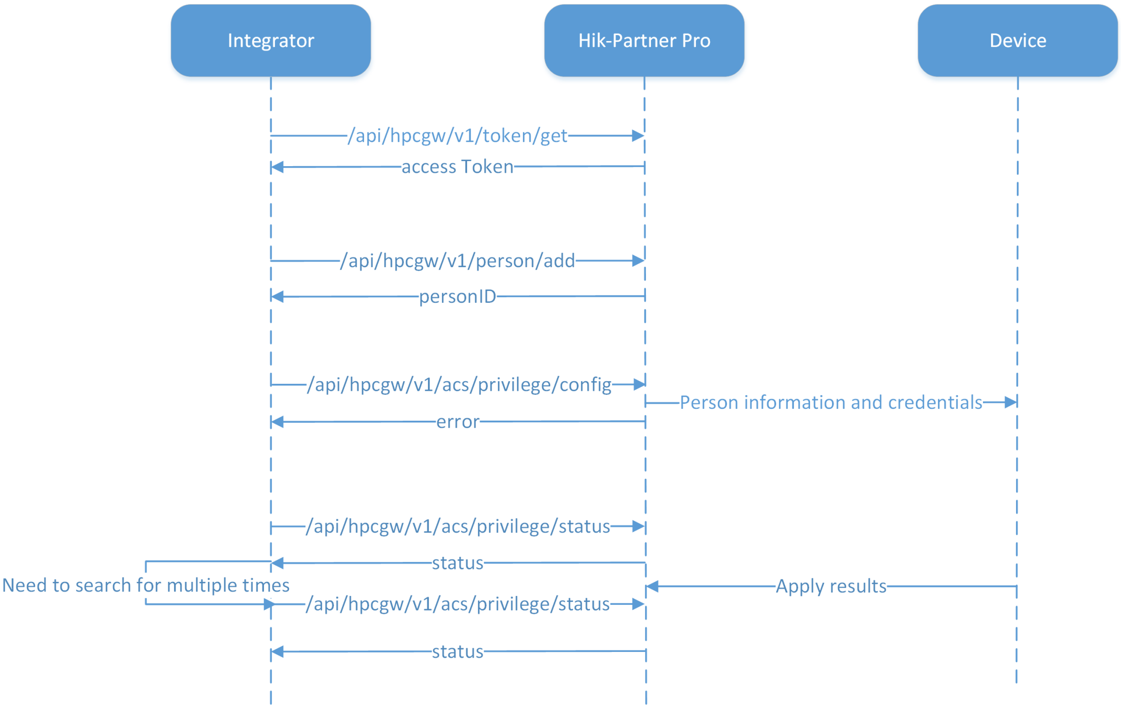

Integrator
Hik-Partner Pro
Device
/api/hpcgw/v1/token/get
access Token
/api/hpcgw/v1/person/add
personID
/api/hpcgw/v1/acs/privilege/config
Person information and credentials
error
/api/hpcgw/v1/acs/privilege/status
status
Need to search for multiple times
Apply results
/api/hpcgw/v1/acs/privilege/status
status

Figure 2-6 Apply Person Information to Device

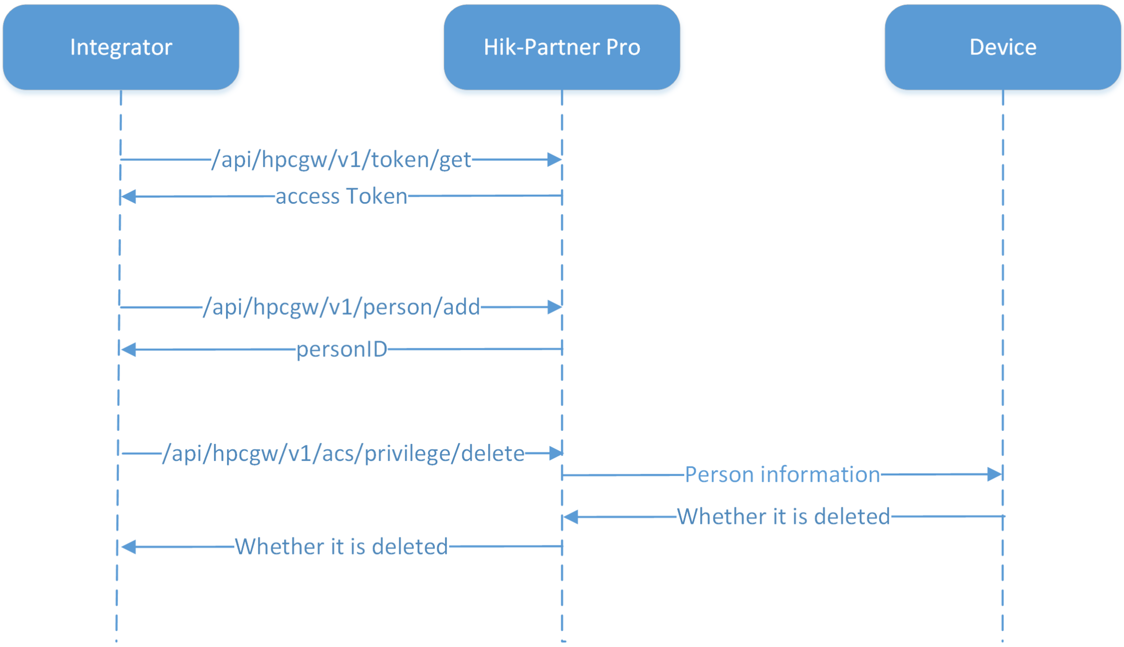


Figure 2-7 Delete Person Information from Device

The APIs related with cloud attendance system are listed as below.

Function	API
Add a person	***POST /api/hpcgw/v1/person/add***
Edit person information	***POST /api/hpcgw/v1/person/update***
Delete a person	***POST /api/hpcgw/v1/person/delete***
Apply person information and permission to an access control device	***POST /api/hpcgw/v1/acs/privilege/config***
Get the applying status of person information and permission	***POST /api/hpcgw/v1/acs/privilege/status***
Delete the applied person information and permission from an access control device	***POST /api/hpcgw/v1/acs/privilege/delete***

Note

- For device management APIs, refer to ***Device Management*** .
- For APIs about events and alarms, refer to ***Events and Alarms*** .
- Applying for an API key for integrating cloud attendance service can only be done offline via emails or other methods.
- Deleting person information and permissions can not be completed if you only call ***POST /api/hpcgw/v1/person/delete*** . You also need to call ***POST /api/hpcgw/v1/acs/privilege/delete*** .

2.9 Hot Spare

The API calling flows for hot spare (host) and hot spare (spare) are as follows.

2.9.1 API Calling Flow for Hot Spare (Host)

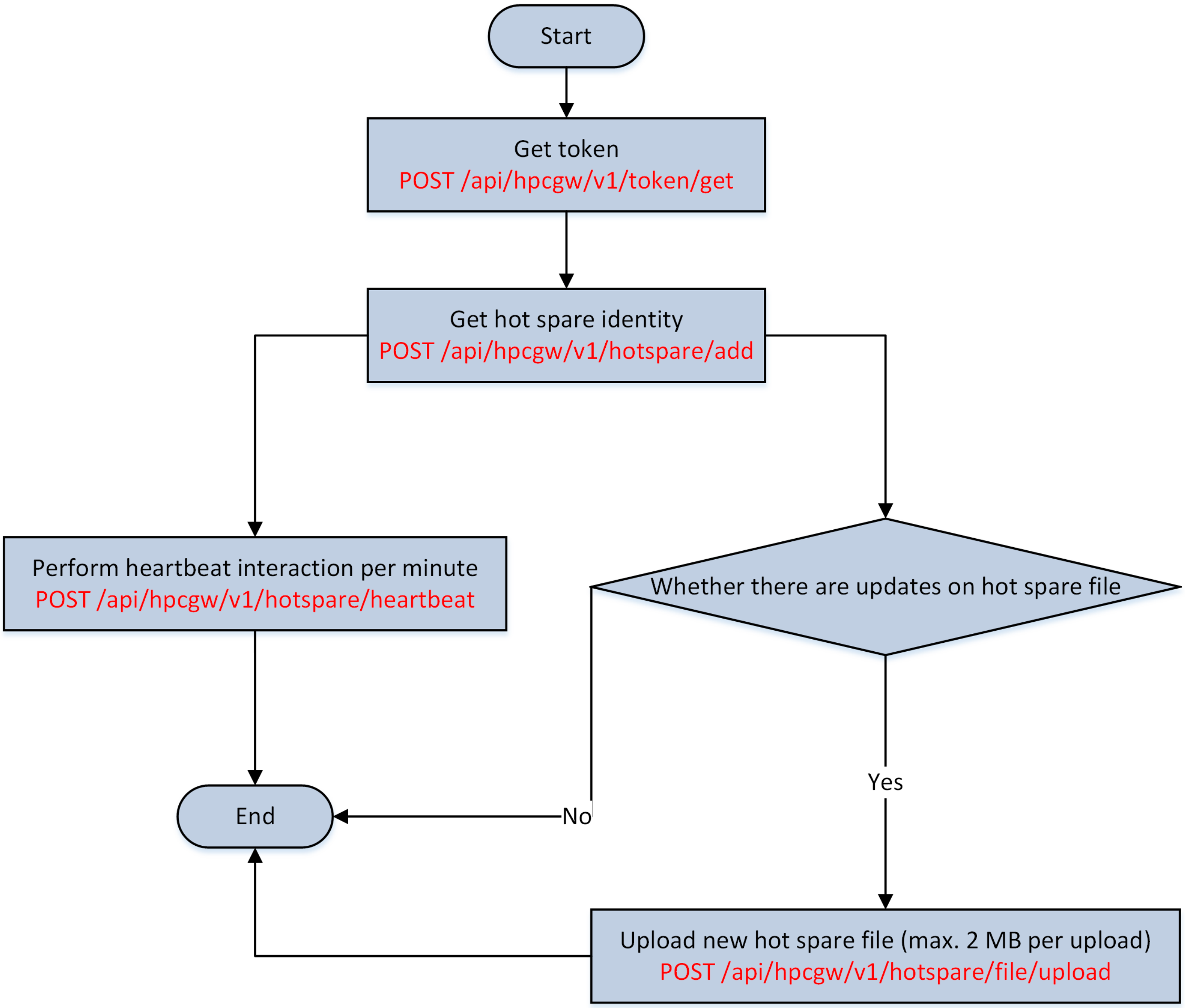

Start
Get token
POST /api/hpcgw/v1/token/get
Get hot spare identity
POST /api/hpcgw/v1/hotspare/add
Perform heartbeat interaction per minute
POST /api/hpcgw/v1/hotspare/heartbeat
Whether there are updates on hot spare file
Yes
No
End
Upload new hot spare file (max. 2 MB per upload)
POST /api/hpcgw/v1/hotspare/file/upload

Figure 2-8 API Calling Flow for Hot Spare (Host)

1. Call ***POST /api/hpcgw/v1/token/get*** and enter the ARC ID and ARC key, to get the token.

Note

This API is the base API and the token returned can be called by other APIs.

2. Call ***POST /api/hpcgw/v1/hotspare/add*** to set the hot spare identity for host device.

3. The host device calls the API of heartbeat interaction ***POST /api/hpcgw/v1/hotspare/heartbeat*** per minute, to make sure the host device activity status can be detected.
4. Call ***POST /api/hpcgw/v1/hotspare/file/upload*** to upload a hot spare file that is no larger than 2 MB.

Note

- For uploading larger files, please contact the technical support.
- When there are updates on the host device configuration, which requires an updated hot spare file, you can upload a new file for replacement.

2.9.2 API Calling Flow for Hot Spare (Spare)

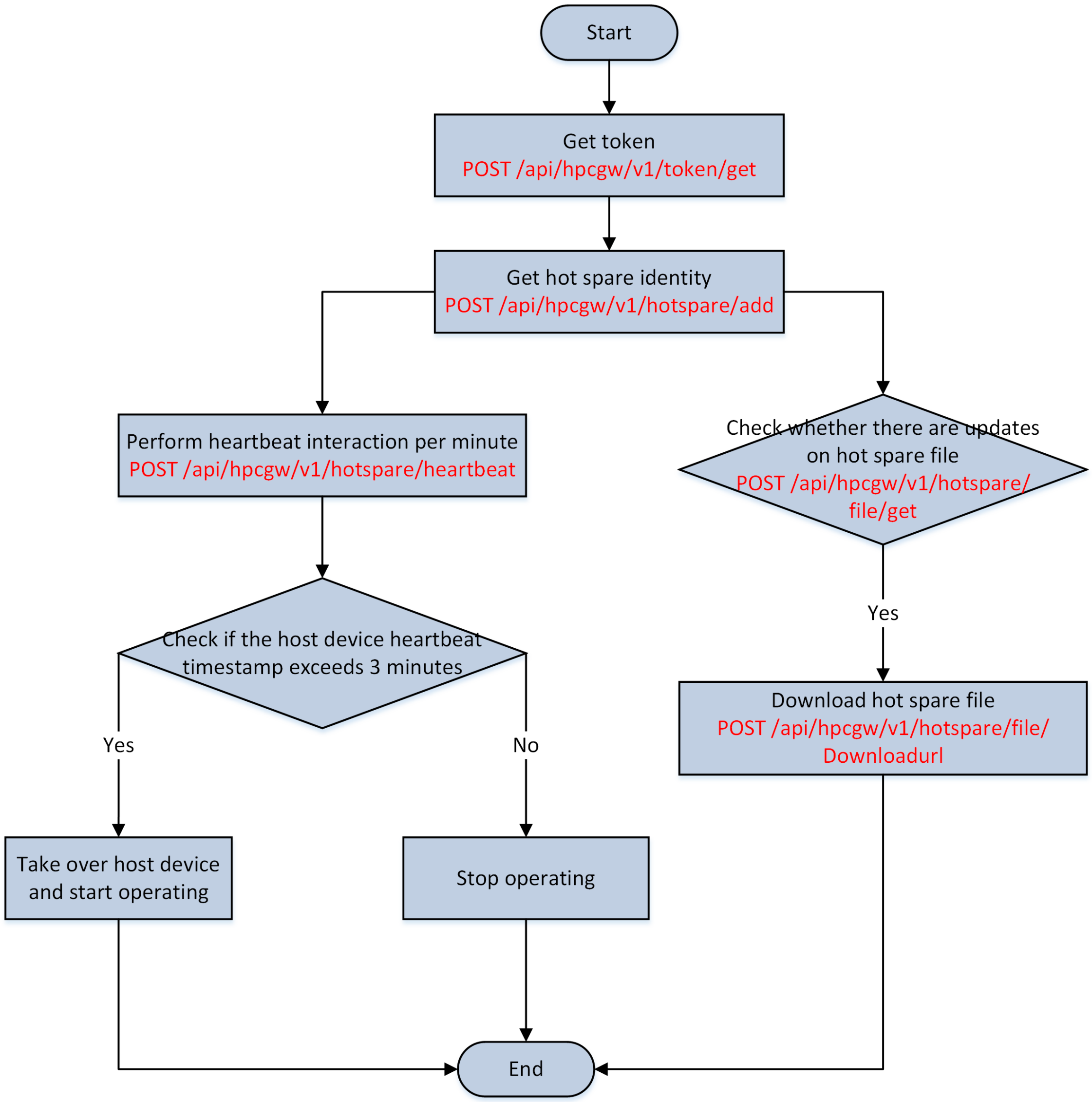

Start
Get token
POST /api/hpcgw/v1/token/get
Get hot spare identity
POST /api/hpcgw/v1/hotspare/add
Perform heartbeat interaction per minute
POST /api/hpcgw/v1/hotspare/heartbeat
Check whether there are updates on hot spare file
POST /api/hpcgw/v1/hotspare/file/get
Check if the host device heartbeat timestamp exceeds 3 minutes
Yes
No
Yes
Download hot spare file
POST /api/hpcgw/v1/hotspare/file/Downloadurl
Take over host device and start operating
Stop operating
End

Figure 2-9 API calling flow of Hot Spare (Spare)

1. Call ***POST /api/hpcgw/v1/token/get*** and enter the ARC ID and ARC key, to get the token.

Note

This API is the base API and the token returned can be called by other APIs.

2. Call ***POST /api/hpcgw/v1/hotspare/add*** to set the hot spare identity for host device.

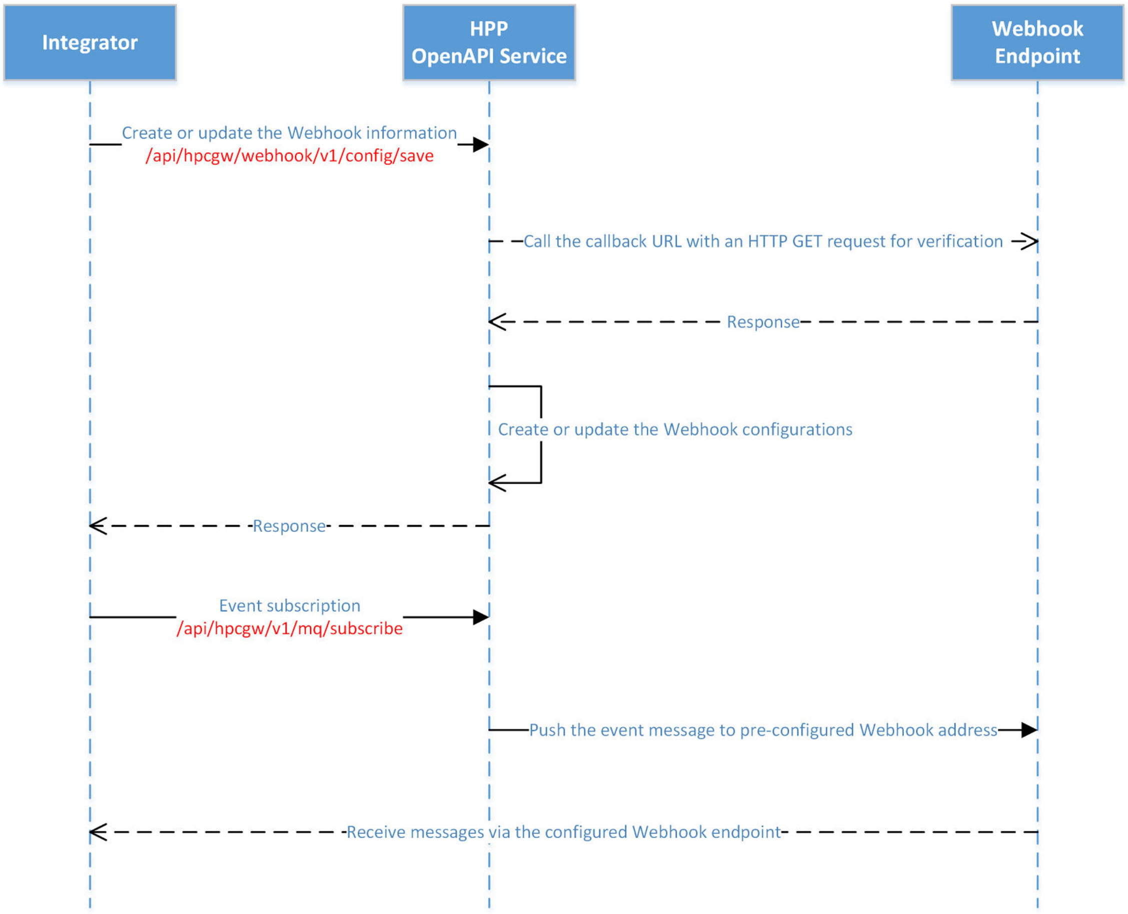
3. The host device calls the API of heartbeat interaction ***POST /api/hpcgw/v1/hotspare/heartbeat*** per minute, to make sure the host device activity status can be detected in case of any breakdown.
4. Call ***POST api/hpcgw/v1/hotspare/file/get*** as scheduled, and compare the time with the last updating time of the downloaded local file to check if there are updates. If there are, call ***POST /api/hpcgw/v1/hotspare/file/downloadurl*** to get the download URL for downloading the latest hot spare file from the cloud.

2.10 Webhook Message Push

Note

After the Webhook configuration, event notifications are pushed via Webhook. The original polling may no longer acquire messages. If integrators have implemented the event notification via polling (/api/hpcgw/v1/mq/messages), they need to contact the technical support to switch from polling to Webhook.

Webhook Integration Flow


Integrator
HPP OpenAPI Service
Webhook Endpoint
Create or update the Webhook information
/api/hpcgw/webhook/v1/config/save
Call the callback URL with an HTTP GET request for verification
Response
Create or update the Webhook configurations
Response
Event subscription
/api/hpcgw/v1/mq/subscribe
Push the event message to pre-configured Webhook address
Receive messages via the configured Webhook endpoint

1. Call the API ***POST /api/hpcgw/webhook/v1/config/save*** to create the Webhook configuration.
2. Call the API ***POST /api/hpcgw/v1/mq/subscribe*** to subscribe to events.
3. Receive event notifications via the configured Webhook endpoint.
   Return an HTTP status code 2XX for success, and return non-2XX for failure. The timeout is 5 seconds.

Security Control

Note

For security, callback URLs must use HTTPS during Webhook operations.

1. **Callback URL Signature Verification**
   When an integrator creates a Webhook configuration via the API, the OpenAPI service firstly verifies the callback URL by sending an HTTPS GET request, including the following headers: **X-Hook-Batch-Id** (random string) and **X-Hook-Timestamp** (request initiation timestamp).
   Verification criteria: The response must contain an X-Hook-Signature (see X-Hook-Signature and Signature Algorithm Demo below) in the header, and the signature must pass validation. Only after successful validation is the Webhook created. Similarly, when updating the Webhook, the same verification process will be performed to confirm the URL validity.
2. **Push Message Signature Verification**
   To ensure the message security (tamper-proof and anti-replay), receivers must verify the sender. When the system service sends an HTTP POST request to the callback URL, the Webhook related request headers are as follows:

Table 2-1 Webhook Related Request Header

HTTP Header	Description
X-Hook-Batch-Id	Matches the **batchId** in the request body.
X-Hook-Signature	Digital signature (format: algorithm + signature). For example: `sha256=ede4cd6ad2e2b76b81d5c403234629a36a9d75793b12c7b9e382c8f061d1bf61` It is used by receivers to verify senders.
X-Hook-Timestamp	Request initiation timestamp. (Receivers must validate this timestamp to enhance the signature freshness and improve security, e.g., the timestamp deviation should be no longer than 1 minute.)

Note

During the Webhook registration, integrators must specify a Webhook secret key (**signSecret**) of API ***POST /api/hpcgw/webhook/v1/config/save***). It defaults to the integrator's SecretKey (SK) when the field is absent.

X-Hook-Signature

1. Prefix: Hash function identifier (currently fixed as sha256).
2. Delimiter: Equals sign (=).
3. Digital Signature: Hex-encoded hash value generated as follows:
    - Concatenate the following elements to form the message: request timestamp (matches X-Hook-Timestamp), period (.), batchId.
    - Determine the hash function via prefix (e.g., SHA-256), then generate MAC using HMAC algorithm with the secret key (**signSecret** during Webhook registration).
    - Hex-encode the MAC to generate the final signature.

Example Code of Signature Algorithm Demo (Java)

~~~
```java
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import java.nio.charset.StandardCharsets;

    public class SignatureDemo {
        private static final String HASH_ALGORITHM = "HmacSHA256";
        public static String generateSignature(String secret, String timestamp, String batchId) throws Exception {
            // Step 1: Concatenate `Message`
            String message = timestamp + "." + batchId;
            // Step 2: Generate `MAC` using `secret` as a key with `HmacSHA256`
            Mac mac = Mac.getInstance(HASH_ALGORITHM);
            SecretKeySpec secretKey = new SecretKeySpec(secret.getBytes(StandardCharsets.UTF_8), HASH_ALGORITHM);
            mac.init(secretKey);
            byte[] rawMac = mac.doFinal(message.getBytes(StandardCharsets.UTF_8));

            // Step 3: Convert `MAC` to a hexadecimal string
            StringBuilder hexString = new StringBuilder();
            for (byte b : rawMac) {
                hexString.append(String.format("%02x", b));
            }
            // The final signature format: `sha256=<signature>`
            return "sha256=" + hexString.toString();
        }

        public static void main(String[] args) {
            try {
                String secret = "your_secret_key";
                Long timestamp = System.currentTimeMillis();
                String batchId = "ebd5a32a518c423f91d4f889a9d5e841";
                String signature = generateSignature(secret, timestamp + "", batchId);
                System.out.println("Generated Signature: " + signature);
            } catch (Exception e) {
                e.printStackTrace();
            }
        }
    }
~~~

Message Example

```
{
    "batchId": "9dce56d70exxxx202d3d56691fc7",
    "list": [
        {
            "messageId": "e21a5d62fxxxxxxx82d29a2e55952",
            "accountNumber": "12XX",
            "deviceSerial": "Q01XXXXXX",
            "formatType": "JSON",
            "alarmData": "{\"CIDEvent\":{\"code\":1401,\"description\":\"DisarmOperation\",\"evttype\":\"13\",\"system
\":1,\"systemName\":\"Area 1\",\"userName\":\"user@xxx.net\",\"userNo\":502},\"deviceSerial\":\"Q01XXXXXX\",
\"eventDescription\":\"CID event\",\"eventType\":\"cidEvent\",\"relationId\":\"053f29d4-4d51-xxxx-439e502209e7\",
\"triggerTime\":\"2025-06-19T21:04:41\",\"version\":\"v30\"}"
        },
        {
            "messageId": "e21a5d62f8xxxxxxx29a2e55953",
            "accountNumber": "12XX",
            "deviceSerial": "Q01XXXXXX",
            "formatType": "JSON",
            "alarmData": "{\"CIDEvent\":{\"code\":1401,\"description\":\"DisarmOperation\",\"evttype\":\"13\",\"system
\":1,\"systemName\":\"Area 1\",\"userName\":\"user@xxx.net\",\"userNo\":502},\"deviceSerial\":\"Q01XXXXXX\",
\"eventDescription\":\"CID event\",\"eventType\":\"cidEvent\",\"relationId\":\"053f29d4-4d51-xxxx-439e502209e7\",
\"triggerTime\":\"2025-06-19T21:04:41\",\"version\":\"v30\"}"
        }
    ]
}
```

Chapter 3 API Reference

3.1 POST /api/hpcgw/v1/token/get

Get the token information.

Note

- The obtained token is valid within 7 days, and it is accurate to millisecond. If the token expires, the error code LAP500004 error code will be returned, and you need to get a new token with the API key.
- Request URL: [Domain Name]/api/hpcgw/v1/token/get, and the available domain names are as follows:

Area	Domain Name
General	https://api.hik-partner.com
Russia	https://api.hik-partnerru.com

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
appKey	Req.	String	Body	Access Key ID (API Key or ARC ID).
secretKey	Req.	String	Body	Secret Access Key (API Secret or ARC Key).

Response Parameters

Parameter	Data Type	Description
accessToken	String	Access token, which is used as the authentication information in the request

Parameter	Data Type	Description
		header when you call the other APIs in this developer guide.
expireTime	Long	The expiration time of the access token displayed in milliseconds. It is valid within 7 days, and you can get it again if it is expired.
areaDomain	String	The area's domain name. You should use the returned domain name when calling the other APIs in this developer guide. • Europe: https://ieuapi.hik-partner.com • Northern America: https://iusapi.hik-partner.com • South America: https://isaapi.hik-partner.com • Singapore: https://isgpapi.hik-partner.com • Russia: https://api.hik-partnerru.com

Note

You can use the original domain names until the end of 2023.

- Russia: https://api.hik-proconnectru.com
- Others: https://api.hik-proconnect.com

Response Example

```
{
  "accessToken ": "jmna8qnqg8d3dgnzs87m4v2dme3l",
  "expireTime ": 1585747008592,
  "areaDomain": "https://ieuapi.hik-partner.com"
}
```

3.2 POST /api/hpcgw/v1/installers/search

Search for the employee list.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
page	Opt.	Integer	Body	Current page No. By default, it is the first page.
pageSize	Opt.	Integer	Body	Number of items per page. By default, it is 20.
search	Opt.	String	Body	Search condition, including user name, e-mail address, and phone number. Fuzzy search is supported. When this field is not configured, all results will be displayed.

Request Example

```
{
  "search": "name"
}
```

Response Parameters

Parameter	Data Type	Description
id	String	Employee ID (InstallerId).
firstName	String	Employee's first name.
lastName	String	Employee's last name.
email	String	Email address.
phone	String	Phone number.
invitedStatus	Boolean	Registration status of the invited employee: true (registered), false (unregistered).

Parameter	Data Type	Description
isAdmin	Boolean	Whether the employee is the admin.
enableStatus	Boolean	Whether the employee's identity is enabled: true (yes), false (no).

Response Example

```
{
 "data":{
  "page": 1,
  "pageSize": 20,
  "rows": [{
   "email": "string",
   "enableStatus": true,
   "firstName": "string",
   "id": "string",
   "invitedStatus": true,
   "isAdmin": true,
   "lastName": "string",
   "phone": "string"
  }],
  "total": 0,
  "totalPage": 0
 },
 "errorCode": "0"
}
```

3.3 POST /api/hpcgw/v1/site/add

Add the information of a site.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
name	Req.	String	Body	Site name. The maximum length is 128 characters.

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
timeZone	Req.	Integer	Body	Time zone. See details in ***Time Zone List*** .
timeSync	Opt.	Boolean	Body	Whether to synchronize the time zone. By default it is False.
siteState	Opt.	String	Body	State where the site is located. The maximum length is 128 characters.
siteCity	Opt.	String	Body	City where the site is located. The maximum length is 128 characters.
siteStreet	Opt.	String	Body	Street where the site is located. The maximum length is 128 characters.
location	Opt.	String	Body	Detailed address of the site. The maximum length is 128 characters.

Request Example

```
{
  "name": "",
  "siteCity": "",
  "siteState": "",
  "siteStreet": "",
  "location": "",
  "timeSync": true,
  "timeZone": 222
}
```

Response Example

```
{
  "errorCode": "0"
}
```

3.4 POST /api/hpcgw/v1/site/{id}/delete

Delete the information of a site.

Request Parameters

Note

If you delete a site, all devices of the site will be deleted.

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
id	Req.	String	Path	Site ID.

Response Example

```
{
  "errorCode": "0"
}
```

3.5 POST /api/hpcgw/v1/site/{id}/update

Edit the information of a site.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
id	Req.	String	Path	Site ID.
name	Req.	String	Body	Site name. The maximum length is 128 characters.
siteState	Opt.	String	Body	State where the site is located. The maximum length is 128 characters.

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
siteCity	Opt.	String	Body	City where the site is located. The maximum length is 128 characters.
siteStreet	Opt.	String	Body	Street where the site is located. The maximum length is 128 characters.
location	Opt.	String	Body	Detailed address of the site. The maximum length is 128 characters.

Request Example

```
{
  "name": "",
  "siteCity": "",
  "siteState": "",
  "siteStreet": "",
  "location": ""
}
```

Response Example

```
{
  "errorCode": "0"
}
```

3.6 POST /api/hpcgw/v1/site/search

Search for the site information.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
page	Opt.	Integer	Body	Current page No. By default, it is the first page.
pageSize	Opt.	Integer	Body	Number of items per page. By default, it is 20.
search	Opt.	String	Body	Search condition, including site name, site address, site installer, etc. Fuzzy search is supported.

Request Example

```
{
  "page": 0,
  "pageSize": 0,
  "search": ""
}
```

Response Parameters

Parameter	Data Type	Description
id	String	Site ID.
siteName	String	Site name.
timeZone	String	Time zone. See details in ***Time Zone List*** .
timeSync	Boolean	Whether to synchronize the time zone. By default it is False.
installerId	String	Installer ID. The first installer ID will be returned if there are multiple installers.
installerFirstName	String	Installer's first name.
installerLastName	String	Installer's last name.
siteState	String	State where the site is located.
siteCity	String	City where the site is located.
siteStreet	String	Street where the site is located.
location	String	Detailed address of the site.
sharedInfo	Object	Information about site sharing.

Parameter	Data Type	Description
shareType	Integer	0: the site belongs to the current company, and has not been shared. 1: the site belongs to the current company, but it is shared with a maintenance service partner. 2: the site is shared with you by other companies, and you have provided maintenance services. 3: the site belongs to the current company, and it is shared with installers to provide you with device installation and configuration services. After you hand over the site to customers, the sharing with the installation service partner will be revoked automatically. 4: the site is shared by other companies, and you have provided device installation and configuration services.
shareState	Integer	0: Waiting to be authenticated by end user. 1: Waiting for other companies to accept. 2: It is currently shared with others. 3: Sharing request denied by end user. 4: Sharing request denied by other companies.
shareToCompany	Object	It is returned when you sharing your sites with other companies. Only one node can exist between this node and **shareFromCompany**.
shareFromCompany	Object	It is returned when the site is shared with you by other companies. Only one node can exist between this node and **shareToCompany**.
address	String	Sharer/Sharee company address.
companyName	String	Sharer/Sharee company name.
email	String	Sharer/Sharee email address.
firstName	String	Sharer/Sharee person first name.
lastName	String	Sharer/Sharee person last name.
phone	String	Sharer/Sharee company phone number.

Parameter	Data Type	Description
street	String	Street where the sharer/sharee company is located.
siteDeliveryStatus	Integer	0-site not handed over, 1-site handover in progress, 2-site handed over.
cloudEnable	Boolean	As long as permission for a device is enabled, true will be returned; only when permission for all devices are disabled will false be returned.

Response Example

```
{
 "data": {
   "page": 1,
   "pageSize": 20,
   "rows": [
    {
     "id": "",
     "installerFirstName": "",
     "installerId": "",
     "installerLastName": "",
     "location": "",
     "siteCity": "",
     "siteName": "",
     "siteState": "",
     "siteStreet": "",
     "timeSync": true,
     "timeZone": "182",
     "siteDeliveryStatus": 2,
     "cloudEnable": true,
     "sharedInfo":
      {
       "shareState": 4,
       "shareType": 3,
       "shareToCompany":
        {
         "address": "",
         "companyName": "",
         "email": "",
         "firstName": "",
         "lastName": "",
         "phone": "",
         "street": ""
        }
      }
     },
     {
      "id": "",
    "installerFirstName": "",
    "installerId": "",
    "installerLastName": "",
    "location": "",
    "siteCity": "",
    "siteName": "",
    "siteState": "",
    "siteStreet": "",
    "timeSync": true,
    "timeZone": "182",
    "siteDeliveryStatus": 2,
    "cloudEnable": true,
    "sharedInfo":
       {
        "shareState": 4,
        "shareType": 4,
        "shareFromCompany":
        {
         "address": "",
         "companyName": "",
         "email": "",
         "firstName": "",
         "lastName": "",
         "phone": "",
         "street": ""
        }
       }
     }
   ],
   "total": 0,
   "totalPage": 0
 },
 "errorCode": "0"
}
```

3.7 POST /api/hpcgw/v1/site/share

Share a site.

Request Parameters

Note

1. There are two scenarios of sharing a site, and this API is only applicable to the first scenario.

   - A site is not handed over but shared with an installation service provider to get device installation services.
   - Installers are authorized by end users to manage a site, and the site is shared with a maintenance service partner to cooperatively provide services for end users.

2. Only sites that are not transferred can be shared.

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
email	Req.	String	Body	Employee email of the company which the site is shared with. Also, the site sharing feature should be enabled.
siteId	Req.	String	Body	The ID of the site to be shared.
applyTimeType	Opt.	Integer	Body	Authorized duration of the site: -1 or empty: permanent. 0: 1 hour. 1: 2 hours. 2: 4 hours. 3: 8 hours. 4: 24 hours.
describe	Opt.	String	Body	Additional information which will be displayed to employees.

Request Example

```
{
   "email": "xxx@xx.com",
   "describe": "additional information",
   "siteId": "xxxxx",
   "applyTimeType ": 0
}
```

Response Example

```
{
"errorCode": "0"
}
```

3.8 POST /api/hpcgw/v1/site/share/cancel/{id}

Cancel sharing a site.

Request Parameters

Parameter	Req./Opt./Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
id	Req.	String	Path	Site ID, which is contained in URL directory.

Response Example

```
{
"errorCode": "0"
}
```

3.9 POST /api/hpcgw/v2/site/assign

Assign site manager(s).

Note

After the caller assign new manager(s), the previous manager(s) will be removed. However, the manager(s) with Manage All Sites permission will not be removed.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
siteIds	Req.	Array	Body	ID list of the sites to assign the manager to.
installerPermissionTimes	Req.	Object	Body	ID of the employee to be assigned and validity of site management permission. Up to 100 pairs of the two nodes are supported.
expiredDurationTime	Req.	Long	Body	Validity of site management permission (unit: ms): -1 (permanent).
installerId	Req.	String	Body	ID of the employee to be assigned. 1 to 48 characters allowed. Not allowed to be empty. The employee ID can be obtained via ***POST /api/hpcgw/v1/installers/search*** . The employee to be assigned should have the permission for site management. To delete an employee from the site manager list, assign the site to the company's admin.

Request Example

```
{
   "siteIds": [
      "aaaa",
      "bbbb"
   ],
   "installerPermissionTimes":[
       {
          "installerId":"xxxx",
            "expiredDurationTime":-1
        }
  ]
}
```

Response Example

```
{
"errorCode": "0"
}
```

3.10 POST /api/hpcgw/v1/site/sitemanagers

Get the list of site managers.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
siteId	Req.	String	Body	Site ID.

Request Example

```
{
   "siteId": "aaaaa"
}
```

Response Parameters

Parameter	Data Type	Description
installerMangers	Object	Site manager information.
installerId	String	Site manager ID.
installerFirstName	String	Site manager's first name.
installerLastName	String	Site manager's last name.
installerEmail	String	Site manager's email.

Parameter	Data Type	Description
installerPhone	String	Site manager's phone No.
expireDurationTime	Long	Site manager permission expiring time, accurate to millisecond: -1 (permanently valid).

Response Example

```
{
  "data":{
    "installerMangers":[
      {
        "installerId":"aaa",
        "installerFirstName":"aa",
        "installerLastName":"bb",
        "installerEmail":"aa@outlook.net",
        "installerPhone":"6523123",
        "expireDurationTime":"1873727183782"
      }
    ]
  },
  "errorCode":"0"
}
```

3.11 POST /api/hpcgw/v2/site/handover/share

Hand over sites by sharing.

Note

After the installation and configurations of devices are completed, you can hand over devices to your customer (end user) by sharing. After your customer accepts the handover:

- You still take the ownership of the devices, and your customer only has the permission to use them.
- You can set the device permissions shared with your customer.
- For sites that have been handed over by sharing, you can call this API to share them with more users.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
siteId	Req.	String	Body	Site ID.
batchHcAccount	Req.	Object	Body	End user's account information.
hcAcccount	Req.	String	Body	End user's account.
type	Req.	Integer	Body	Account type: 0-email, 1-phone No.
userSharePermission	Req.	Object	Body	Device permission details shared with end users.
deviceSerial	Req.	String	Body	Device serial No. 1 to 9 characters allowed.
ax2PermissionDetails	Opt.	Object	Body	Security control panel permission information shared with users, valid for security control panels of AX Pro series.
ax2Permission	Opt.	Array	Body	Security control panel permission shared with users: • Permission for sharing devices with other users: 20-device sharing permission. • Operation permissions (AX Pro V1.2.7 and above): 0-arm, 1-disarm / silence alarm, 6-view logs/status, 7-zone bypass, 8-automation control. • Notification permission(AX Pro V1.2.9 and above):

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
				10-PircamGif, 11-VideoClips, 12-keypad/keyfob/app panic alarm, 13-keypad/keyfob medical alarm, 14-keypad fire alarm, 15-smart alarm event, 16-panel lid opened, 17-peripherals lid opened, 18-zone alarm, 19-panel operation, 21-panel status (power and battery), 22-panel status (communications), 23-zone status, 24-peripheral status.
areaPermission	Opt.	Array	Body	Security control panel partition (area) permissions to be shared with users (supported by AX Pro V1.2.9 and above). You can set the list of partition (area) No.s to share the corresponding permissions: -1 (all included).
otherPermissionDetails	Opt.	Object	Body	Other device permission information that can be shared to users. This node is valid for non AX Pro security control panels.
permission	Opt.	Integer	Body	Permission items that can be shared include: 0-live view, 1-playback, 2-two-way audio, 3-alarm, 4-call / open door, 5-PTZ, 6-sharing permission, not supported by channel-level permissions.

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
				Permissions that can be shared for different device types: • Encoding device channel permission: live view, playback, two-way audio, alarm, and PTZ. • Access control device channel permission: live view, playback, two-way audio, alarm, and call / open door. • Video intercom device channel permission: live view, playback, two-way audio, alarm, and call / open door. • Doorbell channel permission: live view, playback, two-way audio, alarm, and call. • Hik-ProConnect Box channel permission: live view, playback, alarm, and PTZ. • Radar device permission: alarm. • Switch and router: no permission can be shared.
channelNo	Opt.	Array	Body	Channel No. list shared with the user: -1 (all channels). This node is only valid for channel-level permissions.
remark	Opt.	String	Body	Remarks.

Request Example

```
{
   "siteId": "aaaaa",
      "batchHcAccount":[
      {
       "hcAccount":"ccccc@yopamail.com",
       "type":0
```

```
    }],
    "userSharePermission":[
    {
      "deviceSerial":"ABC",
      "otherPermissionDetails":[{
          "permission":1,
          "channelNo":["1","2"]
          },
          {
          "permission":3,
          "channelNo":["-1"]
          }
    ]
   },
   {
        "deviceSerial":"DEF",
        "ax2PermissionDetails":{
           "ax2Permission":[1,2],
           "areaPermission":["-1"]
        }
    }]
}
```

Response Example

```
{
"errorCode": "0"
}
```

3.12 POST /api/hpcgw/v2/site/customer/list

Search for list of end users of handover by sharing.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
siteId	Req.	String	Body	Site ID.

Request Example

```
{
   "siteId": "aaaaa"
}
```

Response Parameters

Parameter	Data Type	Description
customers	Object	End user information.
hcAccount	String	Site manager ID.
type	Integer	Account type: 0-email, 1-phone No.
status	String	Sharing status: "0"-rejected, "1"-approved, "2"-pending, "3"-expired, "4"-not registered.

Response Example

```
{
  "data":{
    "customers":[
      {
        "hcAccount":"abc@yopmail.com",
        "type":0,
        "status":"0"
      }
    ]
  },
  "errorCode":"0"
}
```

3.13 POST /api/hpcgw/v1/site/customer/detail

Search for end user information of handover by sharing.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
siteId	Req.	String	Body	Site ID.
hcAccount	Req.	String	Body	End user account.

Request Example

```
{
   "siteId": "aaaaa",
   "hcAccount": "abc@163.com"
}
```

Response Parameters

Parameter	Data Type	Description
shareDevices	Object	Shared device information.
deviceSerial	String	Device serial No.
ax2PermissionDetails	Object	Security control panel permission information shared with users, valid for security control panels of AxPro series.
ax2Permission	Array	Security control panel permission shared with the user. See specific values in ***POST /api/hpcgw/v2/site/handover/share*** .
areaPermission	Array	Security control panel partition (area) permissions to be shared with the user, supported by AX Pro V1.2.9 and above. You can set the list of partition (area) No.s to share the corresponding permissions: -1 (all included).
otherPermissionDetails	Object	Other device permission information that is shared with the user. This node is valid for non AxPro security control panels.

Parameter	Data Type	Description
permission	Integer	Permission items that can be shared. See specific values in ***POST /api/hpcgw/v2/site/handover/share*** .
channelNo	Array	Channel No. list shared with the user: -1 (all channels). This node is only valid for channel-level permissions.

Response Example

```
{
 "data":{
  "shareDevices":[
   {
    "deviceSerial":"ABC",
    "otherPermissionDetails":[
     {
      "permission":1,
      "channelNo":["1","2"]
     }]
   },
   {
    "deviceSerial":"DEF",
    "ax2PermissionDetails":{
      "ax2Permission":[1,2],
      "areaPermission":["1","2"]
    }
   }
  ]
 },
 "errorCode":"0"
}
```

3.14 POST /api/hpcgw/v1/site/customer/account/update

Modify end user's account information.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
siteId	Req.	String	Body	Site ID.
oldShareHc	Req.	Object	Body	Account information before modification.
newShareHc	Req.	Object	Body	Account information after modification.
hcAcccount	Req.	String	Body	Account.
type	Req.	Integer	Body	Account type: 0-email, 1-phone No.

Request Example

```
{
  "siteId": "aaaaa",
    "oldShareHc": {
      "hcAccount":"abc@yopmail.com",
      "type":0
    },
    "newShareHc": {
      "hcAccount":"def@yopmail.com",
      "type":0
    }
}
```

Response Example

```
{
"errorCode": "0"
}
```

3.15 POST /api/hpcgw/v1/site/customer/devices/update

Modify device permission information for end users.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
siteId	Req.	Array	Body	Site ID
sharedHc	Req.	Object	Body	Information of user with permission information to be edited.
hcAcccount	Req.	Long	Body	Account.
type	Req.	String	Body	Account type: 0-email, 1-phone No.
shareDevices	Req.	Object	Body	Shared device information.
deviceSerial	Req.	String	Body	Device serial No. Not allowed to be empty. 1 to 9 characters allowed.
ax2PermissionDetails	Opt.	Object	Body	Security control panel permission information shared with users, valid for security control panels of AxPro series.
ax2Permission	Opt.	Array	Body	Security control panel permission shared with users. See specific values in ***POST /api/hpcgw/v2/site/handover/share*** .
areaPermission	Opt.	Array	Body	Security control panel partition (area) permissions to be shared with the user, supported by AX Pro V1.2.9 and above. You can set the list of partition (area) No.s to share the corresponding permissions: -1 (all included).

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
otherPermissionDetails	Opt.	Object	Body	Other device permission information that can be shared to users. This node is valid for non AxPro security control panels.
permission	Opt.	Integer	Body	Permission items that can be shared. See specific values in ***POST /api/hpcgw/v2/site/handover/share*** .
channelNo	Opt.	Array	Body	Channel No. list shared with the user: -1 (all channels). This node is only valid or channel-level permissions.

Request Example

```
{
   "siteId": "aaaaa",
      "sharedHc": {
         "hcAccount":"ccccc@yopamail.com",
         "type":0,
         "shareDevices":[
          {
               "deviceSerial":"ABC",
               "otherPermissionDetails":[
                {
                     "permission":1,
                     "channelNo":["1","2"]
                 }]
          },
          {
                "deviceSerial":"DEF",
                "ax2PermissionDetails":{
                     "ax2Permission":[1,2],
                     "areaPermission":["1","2"]
                }
           }]
      }
}
```

Response Example

```
{
"errorCode": "0"
}
```

3.16 POST /api/hpcgw/v1/site/customer/cancle

Cancel the sharing for the end user.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
siteId	Req.	String	Body	Site ID.
hcAcccounts	Req.	Array	Body	User account list.

Request Example

```
{
  "siteId": "aaaaa",
    "hcAccounts": [
    "aaa",
    "bbb"
    ]
}
```

Response Example

```
{
"errorCode": "0"
}
```

3.17 POST /api/hpcgw/v1/site/health/report

Get the site health monitoring report.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
siteId	Req.	Array	Body	Site ID.

Request Example

```
{
   "siteId": "aaaaa"
}
```

Response Parameters

Parameter	Data Type	Description
siteId	String	Site ID.
reportDetail	Array	Report details.
deviceSerial	String	Device serial No.
deviceName	String	Device name.
category	String	Device type: "1"-encoding device, "2"-alarm device.
deviceSubCategory	Integer	Device sub-category: 0-unknown, 1-NVR, 2-DVR, 3-Ax2, 4-Ax Hub, 5- Ax Hybrid, 6-panic alarm station, 7-box panic alarm station, 8-pole panic alarm station, 9-MinMoe, 10-Ax Hybrid Pro, 11-solar camera, 12-door station, 13-fall detection radar.
deviceIp	String	Device IP.
deviceModel	String	Device model.
deviceId	String	Device ID.
onlineStatus	Integer	Device network status: 0-offline, 1-online.

Parameter	Data Type	Description
lastOfflineTime	String	Last time offline, in ISO 8601 format, which is represented by "yyyy- MM-ddTHH:mm:ss", e.g., "2021-03-25T06:26:01".
alarmDeviceStatus	Array	Alarm device status information.
operRes	String	Alarm device diagnosis result: "pass", "not pass".
cloudStatus	String	Alarm device cloud connection status: "online", "offline".
workStatus	String	Alarm device working status: "alarm", "partArm", "allDisArm".
cellConnectStatus	String	Mobile network connection status for alarm device: "connected", "not connected", "not Enabled", "unknown".
cellSignalStrength	String	Mobile network signal strength for alarm device: "strong", "middle", "weak", "noSignal".
dataUsed	String	Consumed mobile network data by alarm device, unit: MB.
networkCable	String	Wired network connection status for alarm device: "ok", "disconnect".
wifiSignalStrength	String	Wi-Fi signal strength for alarm device: "strong", "middle", "weak", "noSignal".
batteryStatus	String	Alarm device battery status: "ok", "low".
arcConnectStatus	String	ARC connection status for different alarm devices. E.g., the ARC1 connection status: "notEnabled[1]", "not connected[1]", "connected[1]", Multiple items are separated by comma.
lastInspected	String	Last inspection time, according to the local time of device, e.g., "20,May,2023 16:56:12".
IPCStatusList	Array	Network camera channel status of alarm device.
id	String	Channel ID.

Parameter	Data Type	Description
status	String	Online status of network camera: "normal"-connected, "break"-disconnected", "notRegister"-not registered.
lastTriggerTime	String	Last triggering time, according to the local time of device, e.g., "20,May,2023 16:56:12".
zones	Array	Zone status information of alarm device.
name	String	Zone name.
zoneId	Integer	Zone ID.
deviceId	String	Device ID.
tamperStatus	String	Tempering status: "true"-enabled, "false"-disabled.
diagnosticsResult	String	Diagnosis result: "PASS", "NOT PASS".
networkStatus	String	Network status: "ok", "offline".
batteryStatus	String	Battery status: "ok", "low", "unknown".
signalStrength	String	Signal strength: "strong", "middle", "weak", "noSignal".
peripheralType	String	Zone type: "Wired Zone", "Wireless Zone".
byPassStatus	String	Bypass status: "No"-disabled, "Yes"-enabled".
externalPower	String	External power connection status: "Connected", "not connected".
lastTriggerTime	String	Last triggering time, according to the local time of device, e.g., "20,May,2023 16:56:12".
lastCaptureTime	String	Last capture time, according to the local time of device, e.g., "20,May,2023 16:56:12".
keyPadList	Array	Alarm device keyboard status information.
remoteList	Array	Alarm device remote control status information.
cardReaderList	Array	Alarm device card reader status information.
outPutList	Array	Alarm device output module status information.
repeaterList	Array	Alarm device repeater status information.
sirenList	Array	Alarm device sounder status information.

Parameter	Data Type	Description
transmitterList	Array	Alarm device transmitter status information.
relayList	Array	Alarm device relay status information.
remoteList	Array	Alarm device remote control status information.
id	Array	ID.
name	Integer	Name.
seq	String	Serial No.
lastOperationTime	String	Last operation time, according to the local time of device, e.g., "20,May,2023 16:56:12".
LastSoundTime	String	Last whistling time, according to the local time of device, e.g., "20,May,2023 16:56:12".
enCodingDeviceStatus	Array	Encoding device status information.
loopEnable	Integer	Overwritten recording status for encoding device: 0-disabled, 1-enabled.
diskUsage	Double	Encoding device disk usage.
diskStatus	Integer	Encoding device disk status (all disks included): 0-unknown, 1-network camera disk not found, 2-network camera disk normal, 3-network camera disk error, 5-NVR disk full, 6-NVR disk exception, 7-NVR disk error, 8-NVR normal, 9-speed dome disk full, 10-speed dome disk error, 11-speed dome disk not found, 12-speed dome disk normal, 13-thermal imaging device disk not found, 14-thermal imaging device disk normal, 15-thermal imaging device disk full, 16-thermal imaging device disk error.
videoSingle	Integer	Video loss status: 0-not relevant, 1-normal, 2-lost.
channels	Array	Encoding device channel status information.
name	String	Channel name.
status	Integer	Channel network status: 0-offline, 1-online.
deviceId	String	Device ID.
channelNo	Integer	Channel No.

Parameter	Data Type	Description
channelIpaddr	String	Channel IP.
hdds	Array	Encoding device disk status information.
deviceId	String	Device ID.
hddNo	Integer	HDD No.
temperature	Integer	Temperature.
poweronday	Integer	Running time, unit: day.
selfevaluatingstatus	Integer	Self-evaluation status: 0-ok, 1-error.
allevaluatingstatus	Integer	Overall evaluation status: 0-functional, 1-bad sectors, 2-fault.
hddAttributeDtoList	Array	HDD Smart status.
hddNo	Integer	HDD No.
status	Integer	Status: 0-normal, 1-exceptional.
attributed	Integer	Smart value: 0-Unknown Attribute, 1-Raw Read Error Rate, 2-Throughput Performance, 3-Spin Up Time, 4-Start/Stop Count, 5-Reallocated Sector Count, 6-Read Channel Margin, 7-Seek Error Rate, 8-Seek Time Performance, 9-Power-on Hours Count, 10-Spin Up Retry Count, 11-Spin Up Retry Count, 12-Power Cycle Count, 13-Soft Read Error Rate, 183-SATA Downshift Error Count, 184-End-to-End Error, 185-Head Stability, 186-Induced Op-Vibration Detection, 187-Reported Uncorrectable Errors, 188-Command Timeout, 189-High Fly Writes, 190-Temperature Difference from 100, 191-G-Sense Error Rate, 192-Power Off Retract Count, 193-Load/Unload Cycle Count, 194-HDD Temperature, 195-Hardware ECC Recovered, 196-Reallocation Count, 197-Current Pending Sector Count, 198-Offline Scan Uncorrectable Count, 199-Ultra ATA CRC Error Rate, 200-Write Error Count, 201-Soft Read Error Rate, 202-Data Address Mark Errors, 203-Run Out Cancel, 204-Soft ECC Correction, 205-Thermal Asperity Rate, 206-Flying Height Measurement, 207-Spin High

Parameter	Data Type	Description
		Current, 208-Spin Buzz, 209-Offline Seek Performance, 211-Vibration During Write, 212-Shock During Write, 220-Disk Shift, 221-G-Sense Error Rate, 222-Loaded Hours, 223-Load/Unlock Retry Count, 224-Load Friction, 225-Load/Unload Cycle Count, 226-Load-in Time, 227-Torque Amplification Count, 228-Power Off Retract Count, 230-Head Amplitude, 231-Temperature Celsius, 240-Head Flying Hours, 250-Read Error Retry Rate.

Response Example

```
{
 "data":{
  "siteId": "8a748c538837c238018837d715ec0045",
  "reportDetail": [
    {
      "deviceSerial": "Q11111111",
      "deviceVersion": "V1.2.7",
      "deviceModel":"DS-PWA96-M-WE",
      "deviceIp":"127.0.0.1",
      "category": "1",
      "deviceSubCategory": "1",
      "deviceId": "HQ11111111",
      "onlineStatus": 0,
      "lastOfflineTime": "2021-03-25T06:26:01",
      "enCodingDeviceStatus": {
        "loopEnable": 1,
        "diskUsage": 90.0,
        "diskStatus": 0,
        "videoSingle": 0,
        "channels": [
          {
            "name": "xxx",
            "deviceId": "xxx",
            "status": 0,
            "channelNo": 35,
            "channelIpaddr": "xxx"
          }
        ],
        "hdds": [
          {
            "deviceId": "1",
            "temperature": 60,
            "poweronday": 5,
            "hddNo": 0,
             "selfevaluatingstatus": 1,
             "allevaluatingstatus": 0
          }
       ],
       "hddAttributeDtoList": [
          {
             "hddNo": 1,
             "status": 0,
             "attributed ": "0"
          }
       ]
    },
    "alarmDeviceStatus": {
       "operRes": "pass",
       "cloudStatus": "online",
       "workStatus": "alarm",
       "cellConnectStatus": "connected",
       "cellSignalStrength": "strong",
       "dataUsed": "70M",
       "networkCable": "ok",
       "wifiSignalStrength": "strong",
       "batteryStatus": "ok",
       "arcConnectStatus": "not connected[1],notEnabled[2]",
       "lastInspected": "20,May,2023 16:56:12",
       "IPCStatusList": [
          {
             "id": "1",
             "status": "normal ",
             "type": "Network Camera ",
             "lastTriggerTime": "5,Sep,2023 18:14:59"
          }
       ],
       "zones": [
          {
             "name": "Wireless Zone 1",
             "zoneId": 0,
             "deviceId": "HQ11111111",
             "tamperStatus": "true",
             "diagnosticsResult": "PASS",
             "networkStatus": "ok",
             "batteryStatus": "ok",
             "signalStrength": "strong",
             "peripheralType": "Wired Zone",
             "byPassStatus": "No",
             "externalPower": "Connected",
             "lastTriggerTime": "5,Sep,2023 18:14:59",
             "lastCaptureTime": "5,Sep,2023 18:14:59"
          }
       ],
    "keyPadList ": [
          {
     "id": 0,
            "name": "Wireless Zone 1",
            "seq": "Q132344",
            "tamperStatus": "true",
            "diagnosticsResult": "PASS",
            "networkStatus": "ok",
            "batteryStatus": "ok",
            "signalStrength": "strong",
            "peripheralType": "Wired Zone",
            "byPassStatus": "No",
            "lastOperationTime": "5,Sep,2023 18:14:59"
          }
        ],
        "cardReaderList": [
          {
            "id": 0,
            "name": "Wireless Zone 1",
            "seq": "Q13232",
            "tamperStatus": "true",
            "diagnosticsResult": "PASS",
            "networkStatus": "ok",
            "batteryStatus": "ok",
            "signalStrength": "strong",
            "peripheralType": "Wired Zone",
            "byPassStatus": "No",
            "lastOperationTime": "5,Sep,2023 18:14:59"
          }
        ],
      "outPutList": [
          {
           "id": 0,
            "name": "Wireless Zone 1",
            "seq": "Q1323456",
            "tamperStatus": "true",
            "diagnosticsResult": "PASS",
            "networkStatus": "ok",
            "batteryStatus": "ok",
            "signalStrength": "strong",
            "peripheralType": "Wired Zone",
            "byPassStatus": "No",
            "externalPower": "Connected"
          }
        ],
        "repeaterList": [
          {
           "id": 0,
            "name": "Wireless Zone 1",
            "seq": "Q132349",
            "tamperStatus": "true",
            "diagnosticsResult": "PASS",
            "networkStatus": "ok",
            "batteryStatus": "ok",
            "signalStrength": "strong",
        "peripheralType": "Wired Zone",
        "byPassStatus": "No",
        "externalPower": "Connected"
      }
    ],
    "sirenList": [
      {
         "id": 0,
        "name": "Wireless Zone 1",
        "seq": "Q1852",
        "tamperStatus": "true",
        "diagnosticsResult": "PASS",
        "networkStatus": "ok",
        "batteryStatus": "ok",
        "signalStrength": "strong",
        "peripheralType": "Wired Zone",
        "byPassStatus": "No",
        "externalPower": "Connected",
        "lastSoundTime": "5,Sep,2023 18:14:59"
      }
    ],
    "TransmitterList": [
      {
        "id": 0,
        "name": "Wireless Zone 1",
        "seq": "Q1323446",
        "tamperStatus": "true",
        "diagnosticsResult": "PASS",
        "networkStatus": "ok",
        "batteryStatus": "ok",
        "signalStrength": "strong",
        "peripheralType": "Wired Zone",
        "byPassStatus": "No",
        "externalPower": "Connected",
        "lastTriggerTime": "5,Sep,2023 18:14:59"
      }
    ],
    "relayList": [
      {
        "id": 0,
        "name": "Wireless Zone 1",
        "tamperStatus": "true",
        "diagnosticsResult": "PASS",
        "networkStatus": "ok",
        "batteryStatus": "ok",
        "signalStrength": "strong",
        "peripheralType": "Wired Zone",
        "byPassStatus": "No"
      }
    ],
    "remoteList": [
      {
              "id": 0,
              "name": "Wireless Zone 1",
              "diagnosticsResult": "PASS",
              "seq": "Q1323441",
              "peripheralType": "Wired Zone",
              "lastOperationTime": "5,Sep,2023 18:14:59"
            }
          ]
        }
      }
    ]
  },
  "errorCode":"0"
}
```

3.18 POST /api/hpcgw/v2/device/add

Add the information of devices.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceList	Req.	array	Body	Device list, which is not allowed to be empty.
deviceSerial	Req.	String	Body	Device serial No. Not allowed to be empty.1 to 9 characters allowed.
validateCode	Req.	String	Body	Device verification code. Not allowed to be empty. 1 to 18 characters allowed.
siteId	Req.	String	Body	ID of the site that the devices will be added to. Not allowed

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
				to be empty.1 to 48 characters allowed.
extendInfo	Opt.	String	Body	Extended information. Customized information allowed. 1 to 256 characters allowed.

Request Example

```
{
   "deviceList": [
      {
         "deviceSerial": "abc",
         "validateCode": "def",
         "extendInfo": "xxx"
      }
   ],
   "siteId": "aaaaa"
}
```

Response Parameters

Parameter	Data Type	Description
addSuccessList	Array	The list of successfully added device. Empty list allowed.
addFailedList	Array	The list of devices failed to be added. Empty list allowed.
deviceName	String	Device name.
deviceSerial	String	Device serial No.
deviceCategory	String	Device type.
failReason	String	Cause of failure.

Response Example

```
{
  "data":{
    "addFailedList":[{
      "deviceSerial":"abc",
      "failReason":"add Exception{LAP006001}"
    },
    {
      "deviceSerial":"def",
      "failReason":"add Exception{LAP006001}"
    }],
    "addSuccessList":[{
      "deviceCategory":"0",
      "deviceName":"string",
      "deviceSerial":"abc"
    }]
  },
  "errorCode":"0"
}
```

3.19 POST /api/hpcgw/v1/device/delete

Delete the information of a device.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
id	Req.	String	Body	Device ID. Not allowed to be empty. The maximum length is 48 characters.

Request Example

```
{
    "id": ""
}
```

Response Example

```
{
    "errorCode": "0"
}
```

3.20 POST /api/hpcgw/v1/device/update

Edit the information of a device.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceId	Req.	String	Body	Device ID.
deviceName	Req.	String	Body	Device name. The maximum length is 128 characters.
extendInfo	Opt.	String	Body	Extended information. Customized information allowed. 1 to 256 characters allowed.

Request Example

```
{
   "deviceId": "",
   "deviceName": "",
   “extendInfo”: “xxx”
}
```

Response Example

```
{
   "errorCode": "0"
}
```

3.21 POST /api/hpcgw/v1/device/list

Get the device list.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
page	Opt.	Integer	Body	Page No. The value is page 1 by default.
pageSize	Opt.	Integer	Body	Number of items on each page. The value is 20 by default.
siteId	Opt.	String	Body	Site ID.
deviceSerial	Opt.	String	Body	Device serial No.

Request Example

```
{
  "page": 1,
  "pageSize": 20
}
```

Response Parameters

Parameter	Data Type	Description
id	String	Device ID.
deviceName	String	Device name.
deviceOnlineStatus	Integer	Device status: 0 (offline), 1 (online), 2 (unknown).
deviceSerial	String	Device serial No.
deviceVersion	String	Device version No.
deviceType	String	Device model type.
deviceCategory	Integer	Device type: 1 (IPC), 2 (NVR), 3 (AlarmHost), 4 (Intercom), 5 (AccessControl), 7 (IPDome), 8 (Doorbell), 9 (StorageBox), 10 (thermalCamera), 11 (Switch), 99 (all devices).

Parameter	Data Type	Description
deviceSubCategory	Integer	Device sub type: 0 (unknown), 1 (NVR), 2 (DVR), 3 (AX2), 4 (AX Hub), 5 (AX Hybrid), 6 (panic alarm station), 7 (box panic alarm station), 8 (pole panic alarm station), 9 (MinMoe), 10 (AX Hybrid Pro), 11 (solar camera), 12 (door station), 13 (fall detection radar).
isSubscribed	Boolean	Whether to subscribe to event information.
deviceAddTime	String	Time (in ISO 8601 format) when the device is added, e.g., "2021-03-25T06:26:01.927Z".
timeZone	String	Time zone. See details in ***Time Zone List*** .
extInfo	String	Extended information added for the device.
siteID	String	Site ID.
siteName	String	Site name.
deviceShareFlag	Boolean	Whether it is a shared device.
arcId	String	Linked ARC ID.
arcCompanyName	String	Linked ARC company name.

Response Example

```
{
  "data":{
    "page": 1,
    "pageSize": 20,
    "rows": [{
      "deviceCategory": 3,
      "deviceName": "xxx",
      "deviceOnlineStatus": 0,
      "deviceSerial": " Q01728482",
      "deviceVersion": " V2.0.0 build 200224",
      "id": "xxxxxxxxxx",
      "deviceSubCategory":0,
      "deviceType": "DS-PWA96-M-WE",
      "isSubscribed": 1,
      "deviceAddTime":”2014-03-25T06:26:01.927Z”,
      "timeZone":"182",
      "extInfo":"xxxx",
      "siteID":"xxxxxxxx",
      "siteName":"xxx",
      "deviceShareFlag":false,
      "arcId":"xxx",
      "arcCompanyName":"xxx"
    }],
    "total": 0,
    "totalPage": 0
  },
  "errorCode": "0"
}
```

3.22 POST /api/hpcgw/v1/device/camera/list

Get the list of channels linked with a device.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceSerial	Req.	String	Body	Device serial No.

Request Example

```
{
  "deviceSerial": "abc"
}
```

Response Parameters

Parameter	Data Type	Description
deviceSerial	String	Device Serial No.
ipcSerial	String	Serial No, of the network camera.
channelNo	int	Channel No.
deviceName	String	Device name.
channelName	String	Channel name.
status	int	Channel status: 0 (offline), 1 (online), -1(unknown).
isShared	String	Channel sharing status: 0 (not shared), 1 (shared with others), 2 (shared by others).

Parameter	Data Type	Description
isEncrypt	int	Whether to encrypt stream: 0 (not encrypted), 1 (encrypted).
videoLevel	int	Video resolution: 0 (fluent), 1 (balanced), (2 (HD), 3 (ultra HD).
relatedIpc	boolean	Whether the current channel is linked with the network camera: true (yes), false (no).

Response Example

```
{
  "data":[{
    "deviceSerial":"427734222",
    "ipcSerial":"427734222",
    "channelNo":1,
    "deviceName":"My(427734222)427734222",
    "channelName":"My(427734222)427734222",
    "status":1,
    "isShared":"0",
    "isEncrypt":0,
    "videoLevel":2,
    "relatedIpc":false
  }],
  "errorCode":"0"
}
```

3.23 GET/PUT/POST/DELETE /api/hpcgw/v1/device/transparent/{isapi uri}

Transmit ISAPI protocols.

Note

- Refer to ***Request URIs*** for details about the supported URIs. Contact technical support or log into tpp.hikvision.com if you need the complete list of supported URIs.
- This API can be called by ARC to control devices of other installers.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json or application/xml.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
X-Devserial	Req.	String	Header	Device serial No.
X-Username	Opt.	String	Header	User name. This node is required when a user is specified to operate AX Pro devices.
X-Password	Opt.	String	Header	Password. This node is required when a user is specified to operate the devices.
X-Userlevel	Opt.	Integer	Header	Specify the user type on AX Pro devices: 0-installer (default), 1-admin/operator.

Request Example

XML Message:

```
<?xml version="1.0" encoding="UTF-8"?>
<NTPServer version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
   <id>1</id>
   <addressingFormatType>ipaddress</addressingFormatType>
   <ipAddress>10.10.10.10</ipAddress>
   <portNo>123</portNo>
   <synchronizeInterval>1</synchronizeInterval>
</NTPServer>
```

JSON Message:

```
{
"Zone":{
   "id":1,
   "zoneName":"test",
   "zoneType":"Instant",
   "delayTime":1,
   "stayAwayEnabled":true,
   "chimeEnabled":true,
   "silentEnabled":true,
   "timeOut":true,
   "detectorSeqCfg":"mod",
   "detectorSeq":"123456789"
 }
}
```

HTTP Request Message

```
PUT /api/hpcgw/v1/device/transparent/ISAPI/System/time/ntpServers/1 HTTP/1.1
Host: api.hik-partner.com
Authorization: Bearer at.2eafygyuabvmptnbak3ctbiq03eotm8x-6pkihc3byk-1w21rv5-dhjflmofu
X-Devserial: 519928976
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<NTPServer version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <id>1</id>
    <addressingFormatType>ipaddress</addressingFormatType>
    <ipAddress>10.10.10.10</ipAddress>
    <portNo>123</portNo>
    <synchronizeInterval>1</synchronizeInterval>
</NTPServer>
```

Response Parameters

Parameter	Data Type	Parameter Type	Description
X-EZO-Code	String	Header	Returned code.
X-ErrorCode	String	Header	Error code.
X-DeviceCode	String	Header	Error code returned from the device.

Response Example

XML Message

```
<?xml version="1.0" encoding="UTF-8"?>
  <NTPServer version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
      <id>1</id>
      <addressingFormatType>ipaddress</addressingFormatType>
      <ipAddress>10.10.10.10</ipAddress>
      <portNo>123</portNo>
      <synchronizeInterval>1</synchronizeInterval>
  </NTPServer>
```

JSON Message

```
{
  "Zone": {
        "id": 1,
        "zoneName": "test",
        "zoneType": "Instant",
        "delayTime": 1,
        "stayAwayEnabled": true,
        "chimeEnabled": true,
        "silentEnabled": true,
        "timeOut": true,
        "detectorSeqCfg": "mod",
        "detectorSeq": "123456789"
  }
}
```

3.24 GET/PUT/POST/DELETE /api/hpcgw/v2/device/transparent/{otap uri}

APIs transmited via OTAP protocols.

Note

Those APIs can be called by ARC to control devices of other installers.

Supported OTAP URIs

Description	URI	Method
Get Property	/otap/prop	GET
Set Property	/otap/prop	PUT
Get Property Directly from Device	/otap/prop/direct	GET
Set Property Directly for Device	/otap/prop/direct	PUT
Perform Operations on Device	/otap/action	PUT
Get Object Model Definition	/otap/product/profile	POST
Batch Get Properties	/otap/multi/prop/get/by/shadow	POST
Batch Set Properties	/otap/multi/prop/put/by/shadow	PUT
Batch Get Properties Directly from Device	/otap/multi/prop/get	PUT
Batch Set Properties Directly for Device	/otap/multi/prop/put	PUT
Get OTAP List Data	/api/service/device/otap/table/list?pageIndex=%s&pageSize=%s	GET

3.24.1 GET /api/hpcgw/v2/device/transparent/otap/prop

Get property.

Request URL

https://{areaDomain}/api/hpcgw/v2/device/transparent/otap/prop

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/x-www-form-urlencoded.
Authorization	Req.	String	Header	User access token, which is in the format of "Bearer <accessToken>".
x-devserial	Req.	String	Header	Device serial No.
X-LocalIndex	Req.	String	Header	Resource No.
X-ResourceCategory	Req.	String	Header	Resource category.
X-DomainIdentifier	Req.	String	Header	Function field.
X-PropIdentifier	Req.	String	Header	Function property identifier.

Request Example

```
curl --location --request GET 'https://isgpapi.hik-partner.com/api/hpcgw/v2/device/transparent/otap/prop' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer hpc.mgjxfwu0wexwxw2021lmz3oocnt8uf4b' \
--header 'x-devserial: Q04054748' \
--header 'X-LocalIndex: 0' \
--header 'X-ResourceCategory: global' \
--header 'X-DomainIdentifier: InfoMgr' \
--header 'X-PropIdentifier: DeviceVersion
```

Response Parameters

Parameter	Data Type	Description
data	JSON	Property value. See details of its format in the relevant OTAP protocol document.
errorCode	String	Service response status code.
message	String	Service response status description.

Response Example

```
{
   "data": {
      "firmwareReleasedDate": "build 240205",
      "firmwareVersion": "V1.0.0"
   },
   "errorCode": "0",
   "message": "Ok"
}
```

3.24.2 PUT /api/hpcgw/v2/device/transparent/otap/prop

Set property.

Request URL

https://{areaDomain}/api/hpcgw/v2/device/transparent/otap/prop

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	User access token, which is in the format of "Bearer <accessToken>".
x-devserial	Req.	String	Header	Device serial No.
X-LocalIndex	Req.	String	Header	Resource No.

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
X-ResourceCategory	Req.	String	Header	Resource category.
X-DomainIdentifier	Req.	String	Header	Function field.
X-PropIdentifier	Req.	String	Header	Function property identifier.

Request Example

```
curl --location --request PUT 'https://isgpapi.hik-partner.com/api/hpcgw/v2/device/transparent/otap/prop' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer hpc.1uqrvv3n3e6dfxem17atusunm295wk7t' \
--header 'x-devserial: Q31153369' \
--header 'X-LocalIndex: 0' \
--header 'X-ResourceCategory: global' \
--header 'X-DomainIdentifier: TimeMgr' \
--header 'X-PropIdentifier: LocalDateTime' \
--data '{
   "localDateTime": "2024-04-22T15:39:01+08:00"
}'
```

Response Parameters

Parameter	Data Type	Description
errorCode	String	Service response status code.
message	String	Service response status description.

Response Example

```
{
   "errorCode": "0",
   "message": "Ok"
}
```

3.24.3 GET /api/hpcgw/v2/device/transparent/otap/direct

Get property directly from device.

Request URL

https://{areaDomain}/api/hpcgw/v2/device/transparent/otap/direct

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/x-www-form-urlencoded.
Authorization	Req.	String	Header	User access token, which is in the format of "Bearer <accessToken>".
x-devserial	Req.	String	Header	Device serial No.
X-LocalIndex	Req.	String	Header	Resource No.
X-ResourceCategory	Req.	String	Header	Resource category.
X-DomainIdentifier	Req.	String	Header	Function field.
X-PropIdentifier	Req.	String	Header	Function property identifier.
X-Username	Opt.	String	Header	User name to be specified for operating on AX Pro device.
X-UserType	Opt.	String	Header	User type of the specified **X-Username** on on AX Pro device: "installer" (default), "administrator", "operator".

Request Example

```
curl --location --request GET 'https://isgpapi.hik-partner.com/api/hpcgw/v2/device/transparent/otap/direct' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer hpc.mgjxfwu0wexwxw2021lmz3oocnt8uf4b' \
--header 'x-devserial: Q04054748' \
--header 'X-LocalIndex: 0' \
--header 'X-ResourceCategory: global' \
--header 'X-DomainIdentifier: InfoMgr' \
--header 'X-PropIdentifier: DeviceDescription'
```

Response Parameters

Parameter	Data Type	Description
data	JSON	Property value. See details of its format in the relevant OTAP protocol document.
errorCode	String	Service response status code.
message	String	Service response status description.

Response Example

```
{
   "data": {
      "deviceName": "AX HOME",
      "deviceType": "PWAEco",
      "macAddress": "08:54:11:20:08:ff",
      "model": "DS-PA101-32P-WB",
      "serialNumber": "Q29598581"
   },
   "errorCode": "0",
   "message": "Ok"
}
```

3.24.4 PUT /api/hpcgw/v2/device/transparent/otap/direct

Set property directly for device.

Request URL

https://{areaDomain}/api/hpcgw/v2/device/transparent/otap/direct

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	User access token, which is in the format of "Bearer <accessToken>".
x-devserial	Req.	String	Header	Device serial No.
X-LocalIndex	Req.	String	Header	Resource No.

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
X-ResourceCategory	Req.	String	Header	Resource category.
X-DomainIdentifier	Req.	String	Header	Function field.
X-PropIdentifier	Req.	String	Header	Function property identifier.
X-Username	Opt.	String	Header	User name to be specified for operating on AX Pro device.
X-UserType	Opt.	String	Header	User type of the specified **X-Username** on on AX Pro device: "installer" (default), "administrator", "operator".

Request Example

```
curl --location --request PUT 'https://isgpapi.hik-partner.com/api/hpcgw/v2/device/transparent/otap/direct' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer hpc.1uqrvv3n3e6dfxem17atusunm295wk7t' \
--header 'x-devserial: Q31153369' \
--header 'X-LocalIndex: 0' \
--header 'X-ResourceCategory: global' \
--header 'X-DomainIdentifier: InfoMgr' \
--header 'X-PropIdentifier: DeviceDescription' \
--data '{
   "deviceName": "test1234"
}'
```

Response Parameters

Parameter	Data Type	Description
errorCode	String	Service response status code.
message	String	Service response status description.

Response Example

```
{
   "errorCode": "0",
    "message": "Ok"
}
```

3.24.5 PUT /api/hpcgw/v2/device/transparent/otap/action

Perform operations on device.

Request URL

https://{areaDomain}/api/hpcgw/v2/device/transparent/otap/action

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	User access token, which is in the format of "Bearer <accessToken>".
x-devserial	Req.	String	Header	Device serial No.
X-LocalIndex	Req.	String	Header	Resource No.
X-ResourceCategory	Req.	String	Header	Resource category.
X-DomainIdentifier	Req.	String	Header	Function field.
X-Actionidentifier	Req.	String	Header	Function operation identifier.
X-Username	Opt.	String	Header	User name to be specified for operating on AX Pro device.
X-UserType	Opt.	String	Header	User type of the specified **X-Username** on on AX Pro device: "installer" (default), "administrator", "operator".

Request Example

```
curl --location --request PUT 'https://isgpapi.hik-partner.com/api/hpcgw/v2/device/transparent/otap/action' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer hpc.c3qmm09ogn7krggg16p5r7muja3yscn5' \
--header 'x-devserial: Q31153341' \
--header 'X-LocalIndex: 0' \
--header 'X-ResourceCategory: global' \
--header 'X-DomainIdentifier: ZoneMgr' \
--header 'X-Actionidentifier: SearchZoneStatus' \
--data '{
   "searchID":"test101",
   "searchResultPosition":1,
   "maxResults":32
}'
```

Response Parameters

Parameter	Data Type	Description
errorCode	String	Service response status code.
message	String	Service response status description.

Response Example

```
{
   "data": [
      {
         "armStatus": "armed",
         "exitDelayTime": 0,
         "name": "Area 1",
         "subSystemID": 1
      }
   ],
   "errorCode": "0",
   "message": "Ok"
}
```

3.24.6 POST /api/hpcgw/v2/device/transparent/otap/product/profile

Search for object model definition.

Request URL

https://{areaDomain}/api/hpcgw/v2/device/transparent/otap/product/profile

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	User access token, which is in the format of "Bearer <accessToken>".
x-devserial	Req.	String	Header	Device serial No.
needSchema	Opt.	Boolean	Body	Whether schema is needed: true, false (default).
checkMD5	Opt.	Boolean	Body	Whether MD5 verification is needed: true, false (default).
needGzip	Opt.	Boolean	Body	Whether to compress returned object model protocol via gzip: true, false (default).
md5	Opt.	String	Body	MD5 saved by the caller to local PC.
identifier	Opt.	String	Body	Function identifier.

Request Example

```
curl --location --request POST 'https://isgpapi.hik-partner.com/api/hpcgw/v2/device/transparent/otap/product/
profile' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer hpc.3ebcwoaaybdmlue33uqhw7xag57j6bcv' \
--header 'x-devserial: Q31153341'
```

Response Parameters

Parameter	Data Type	Description
data	Object	In JSON format.
-gzipProfile	Byte[]	gzip package of **-profile** content.
-productId	String	Object model No.
-version	String	Object model protocol version No.
-md5	String	MD5 value, the digest value of **-profile** content.

Parameter	Data Type	Description
-changed	Boolean	true (**-profile** content updates exist), false (no updates on **-profile** content).
-profile	Object	**-profile** object information.
--version	String	**-profile** version.
--capacities	Map	Capability set.
--resources	Array	Resource list.
---identifier	String	Function identifier.
---title	String	Resource name.
---sid	Integer	Short identifier.
---resourceCategory	String	Resource category.
---localIndex	Array	Resource No.
---localIndexRule	Object	Rule object information.
----ruleType	String	Rule type.
----ruleRange	Object	Rule range object information.
-----minimum	Integer	Minimum value.
-----maximum	Integer	Maximum value.
-----step	Integer	Step.
---dynamic	Boolean	Whether it is dynamic resource.
---global	Boolean	Whether it is global resource.
---domains	Array	Domains.
----identifier	String	Function identifier.
----sid	Integer	Short ID.
----title	String	Domain name.
----props	Array	Property.
-----identifier	String	Function identifier.
-----version	String	Protocol version No.
-----access	String	Access permission.
-----title	String	Function name.

Parameter	Data Type	Description
-----sid	Integer	Short identifier.
-----schema	Map<String,Object>	Identifier schema.
----actions	Array	Operation.
-----identifier	String	Function identifier.
-----version	String	Protocol version No.
-----direction	String	Access permission.
-----title	String	Function name.
-----sid	Integer	Short identifier.
-----schema	Map<String,Object>	Identifier schema.
-----input	Object	Request schema.
-----output	Object	Output schema information.
------schema	Map<String,Object>	Output schema.
----events	Array	Event
-----identifier	String	Function identifier.
-----version	String	Protocol version No.
-----eventType	Array	Event type.
-----title	String	Function name.
-----sid	Integer	Short identifier.
-----input	Object	Request schema information.
------schema	Map<String,Object>	Request schema.

Response Example

```
{
   "errorCode": "0",
   "message": "Ok",
   "data": {
      "profile": {
         "version": "V1.0.0 build 210102",
         "capacities": null,
         "resources": [
            {
               "identifier": "global",
               "title": null,
"sid": null,
"resourceCategory": "global",
"localIndex": [
  "0"
],
"localIndexRule": {
  "ruleType": null,
  "ruleRange": null
},
"dynamic": false,
"global": true,
"domains": [
  {
    "identifier": "DoorMagnetic",
    "sid": 746,
    "title": null,
    "props": [
      {
        "identifier": "OpenSound",
        "version": "v3.0",
        "access": "rw",
        "title": null,
        "sid": null,
        "schema": null
      }
    ],
    "actions": [
      {
        "identifier": "Erasure",
        "sid": null,
        "version": "v3.0",
        "direction": "Plt2Dev",
        "title": null,
        "input": null,
        "output": null
      }
    ],
    "events": [
      {
        "identifier": "MagneticAlarm",
        "sid": null,
        "version": "v3.0",
        "title": null,
        "eventType": [
          "notification"
        ],
        "input": null
      },
      {
        "identifier": "DoorRestored",
        "sid": null,
        "version": "v3.0",
              "title": null,
              "eventType": [
                "notification"
              ],
              "input": null
            }
          ]
        },
        {
          "identifier": "AppRemind",
          "sid": 457,
          "title": null,
          "props": [

            {
              "identifier": "AppMsgSwitch",
              "version": "v3.0",
              "access": "rw",
              "title": null,
              "sid": null,
              "schema": null
            }
          ],
          "actions": [],
          "events": []
        },
        {
          "identifier": "BatteryInfo",
          "sid": null,
          "title": null,
          "props": [
            {
              "identifier": "SurplusPower",
              "version": "v3.0",
              "access": "rw",
              "title": null,
              "sid": null,
              "schema": null
            }
          ],
          "actions": [],
          "events": []
        }
      ]
    }
  ]
},
"gzipProfile": null,
"productId": "CS-T2C-BG",
"version": "V1.0.0 build 211203",
"md5": "c9898669dabc3e4429ab86eee49b3ae1",
"changed": true
```

```
  }
}
```

3.24.7 POST /api/hpcgw/v2/device/transparent/otap/multi/prop/get/by/shadow

Batch get properties.

Request URL

https://{areaDomain}/api/hpcgw/v2/device/transparent/otap/multi/prop/get/by/shadow

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	User access token, which is in the format of "Bearer <accessToken>".
propRequests	Req.	JSON Array	Body	Device property list.
-deviceSerial	Req.	String	Body	Device serial No.
-resourceCategory	Req.	String	Body	Resource category.
-localIndex	Req.	String	Body	Resource No.
-domainId	Req.	String	Body	Function field.
-propId	Opt.	String	Body	Function identifier.

Request Example

```
curl --location --request POST 'https://isgpapi.hik-partner.com/api/hpcgw/v2/device/transparent/otap/multi/
prop/get/by/shadow' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer hpc.3ebcwoaaybdmlue33uqhw7xag57j6bcv' \
--data '[
  {
    "deviceSerial": "Q29598581",
    "resourceCategory": "Zone",
    "localIndex": "1",
    "domainId": "ZoneMgr",
    "propId": "SingleZoneBasicInfo"
  },
  {
    "deviceSerial": "Q29598581",
    "resourceCategory": "global",
    "localIndex": "0",
    "domainId": "InfoMgr",
    "propId": "DeviceVersion"
  }
]'
```

Response Parameters

Parameter	Data Type	Description
data	JSON Array	Property value. See details of its format in the relevant OTAP protocol document.
errorCode	String	Service response status code.
message	String	Service response status description.

Response Example

```
{
  "data": [
    {
      "deviceSerial": "Q29598581",
      "propResps": [
        {
          "deviceSerial": "Q29598581",
          "domainId": "InfoMgr",
          "localIndex": "0",
          "propId": "DeviceVersion",
          "resourceCategory": "global",
          "timestamp": 1711616019401,
          "value": {
            "firmwareReleasedDate": "build 240130",
            "firmwareVersion": "V1.0.0"
          }
        },
        {
          "deviceSerial": "Q29598581",
          "domainId": "ZoneMgr",
          "localIndex": "1",
          "propId": "SingleZoneBasicInfo",
          "resourceCategory": "Zone",
          "timestamp": 1711616018757,
          "value": {
            "childDevID": "Q27811987",
            "deactivationMode": "off",
            "delayParam": {
              "entryDelay": 30,
              "exitDelay": 30
            },
            "detectorType": "magneticContact",
            "deviceNo": 1,
            "linkageSubSystems": [
              1
            ],
            "model": "DS-PD121-WB",
            "serialNumber": "Q27811987",
            "version": "V1.0.0 build 231219",
            "zoneName": "Magnetic Contact 1",
            "zoneType": "instant"
          }
        }
      ]
    }
  ],
  "errorCode": "0",
  "message": "Ok"
}
```

3.24.8 PUT /api/hpcgw/v2/device/transparent/otap/multi/prop/put/by/shadow

Batch set properties.

Request URL

https://{areaDomain}/api/hpcgw/v2/device/transparent/otap/multi/prop/put/by/shadow

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	User access token, which is in the format of "Bearer <accessToken>".
propRequests	Req.	JSON Array	Body	List of information to be set.
-deviceSerial	Req.	String	Body	Device serial No.
-propReqs	Req.	JSON Array	Body	Device property information.
-resourceCategory	Req.	String	Body	Resource category.

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
-localIndex	Req.	String	Body	Resource No.
-domainId	Req.	String	Body	Function field.
-propId	Req.	String	Body	Function identifier.
-value	Req.	JSON	Body	Edited content. See details of its format in the relevant OTAP protocol document.

Request Example

```
curl --location --request PUT 'https://isgpapi.hik-partner.com/api/hpcgw/v2/device/transparent/otap/multi/
prop/put/by/shadow' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer hpc.l68ptk43b0hfijoko3vxfhx5oegqo6mz' \
--data '[
  {
    "deviceSerial": "Q31153369",
    "propReqs": [
      {
        "resourceCategory": "SubSystem",
        "localIndex": "1",
        "domainId": "AlarmSubSystemMgr",
        "propId": "SingleSubSystemBasicInfo3224",
        "value": {
          "linkageZoneInfo": {
            "supportLinkageZones": [
              1
            ]
          },
          "linkageChildDevInfo": [
            {}
          ],
          "name": "Area 2",
          "enabled": true
        }
      },
      {
        "resourceCategory": "SubSystem",
        "localIndex": "2",
        "domainId": "AlarmSubSystemMgr",
        "propId": "SingleSubSystemBasicInfo",
        "value": {
          "name": "area 8",
          "enabled": false
        }
      }
      ]
   }
]'
```

Response Parameters

Parameter	Data Type	Description
data	JSON Array	Result of batch setting properties.
deviceSerial	String	Device serial No.
errorCode	String	Device response status code.
message	String	Device response status description.

Response Example

```
{
   "data": [
      {
         "code": "200",
         "deviceSerial": "Q29598581",
         "message": "Operation succeeded"
      }
   ],
   "errorCode": "0",
   "message": "Ok"
}
```

3.24.9 PUT /api/hpcgw/v2/device/transparent/otap/multi/prop/get

Batch get properties directly from device.

Request URL

https://{areaDomain}/api/hpcgw/v2/device/transparent/otap/multi/prop/get

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	User access token, which is in the format of "Bearer <accessToken>".
x-devserial	Req.	String	Header	Device serial No.

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
propRequests	Req.	JSON Array	Body	Device property list.
-resourceCategory	Req.	String	Body	Resource category.
-localIndex	Req.	String	Body	Resource No.
-domainId	Req.	String	Body	Function field.
-propId	Req.	String	Body	Function identifier.

Request Example

```
curl --location --request PUT https://isgpapi.hik-partner.com/api/hpcgw/v2/device/transparent/otap/multi/prop/get
--header Content-Type: application/json
--header Authorization: Bearer hpc.l68ptk43b0hfijoko3vxfhx5oegqo6mz
--header x-devserial: Q31153341
--data [
  {
    "localIndex": "0",
    "resourceCategory": "global",
    "domainId": "InfoMgr",
    "propId": "DeviceDescription"
  },
  {
    "localIndex": "0",
    "resourceCategory": "global",
    "domainId": "InfoMgr",
    "propId": "DeviceVersion"
  }
]
```

Response Parameters

Parameter	Data Type	Description
data	Object	Result of batch getting properties from device.
errorCode	String	Device response status code.
message	String	Device response status description.

Response Example

```
{
  "data": [
    {
      "propResps": [
        {
          "deviceSerial": "F65153704",
          "resourceCategory": "SubSystem",
          "localIndex": "1",
          "domainId": "AlarmSubSystemMgr",
          "propId": "SingleSubSystemBasicInfo",
          "value": {
            "linkageZoneInfo": {
              "supportLinkageZones": [
                2
              ]
            },
            "linkageChildDevInfo": [
              {}
            ],
            "name": "Area 2",
            "enabled": true
          },
          "timestamp": 1690251526886
        },
        {
          "deviceSerial": "F65153704",
          "resourceCategory": "SubSystem",
          "localIndex": "2",
          "domainId": "AlarmSubSystemMgr",
          "propId": "SingleSubSystemBasicInfo",
          "value": {
            "linkageZoneInfo": {
              "supportLinkageZones": [
                2
              ]
            },
            "linkageChildDevInfo": [
              {}
            ],
            "name": "area 8",
            "enabled": false
          },
          "timestamp": 1690251527410
        }
      ]
    }
  ],
  "errorCode": "0",
  "message": "Ok"
}
```

3.24.10 PUT /api/hpcgw/v2/device/transparent/otap/multi/prop/put

Batch set properties directly for device.

Request URL

https://{areaDomain}/api/hpcgw/v2/device/transparent/otap/multi/prop/put

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	User access token, which is in the format of "Bearer <accessToken>".
x-devserial	Req.	String	Header	Device serial No.
X-Username	Opt.	String	Header	User email to be specified for operating on the alarm device.
X-UserType	Opt.	String	Header	The user type of AX Pro devices: "installer", "administrator", "operator".
propRequests	Req.	JSON Array	Body	Device property list.
-resourceCategory	Req.	String	Body	Resource category.
-localIndex	Req.	String	Body	Resource No.
-domainId	Req.	String	Body	Function field.
-propId	Req.	String	Body	Function identifier.
-value	Req.	JSON	Body	Edited content. See details of its format in the relevant OTAP protocol document.

Request Example

```
curl --location --request PUT https://isgpapi.hik-partner.com/api/hpcgw/v2/device/transparent/otap/multi/prop/put
--header Content-Type: application/json
--header Authorization: Bearer hpc.l68ptk43b0hfijoko3vxfhx5oegqo6mz
--header x-devserial: Q31153341
--data [
  {
    "resourceCategory": "SubSystem",
    "localIndex": "1",
    "domainId": "AlarmSubSystemMgr",
    "propId": "SingleSubSystemBasicInfo3224",
    "value": {
      "linkageZoneInfo": {
        "supportLinkageZones": [
          1
        ]
      },
      "linkageChildDevInfo": [
        {}
      ],
      "name": "Area 2",
      "enabled": true
    }
  },
  {
    "resourceCategory": "SubSystem",
    "localIndex": "2",
    "domainId": "AlarmSubSystemMgr",
    "propId": "SingleSubSystemBasicInfo",
    "value": {
      "name": "area 8",
      "enabled": false
    }
  }
]
```

Response Parameters

Parameter	Data Type	Description
data	Object	Result of batch setting properties for device.
errorCode	String	Device response status code.
message	String	Device response status description.

Response Example

```
{
  "data": [
    {
      "propResps": [
        {
          "deviceSerial": "F65153704",
          "resourceCategory": "SubSystem",
          "localIndex": "1",
          "domainId": "AlarmSubSystemMgr",
          "propId": "SingleSubSystemBasicInfo",
          "value": {
            "linkageZoneInfo": {
              "supportLinkageZones": [
                2
              ]
            },
            "linkageChildDevInfo": [
              {}
            ],
            "name": "Area 2",
            "enabled": true
          },
          "timestamp": 1690251526886
        },
        {
          "deviceSerial": "F65153704",
          "resourceCategory": "SubSystem",
          "localIndex": "2",
          "domainId": "AlarmSubSystemMgr",
          "propId": "SingleSubSystemBasicInfo",
          "value": {
            "linkageZoneInfo": {
              "supportLinkageZones": [
                2
              ]
            },
            "linkageChildDevInfo": [
              {}
            ],
            "name": "area 8",
            "enabled": false
          },
          "timestamp": 1690251527410
        }
      ]
    }
  ],
  "errorCode": "0",
  "message": "Ok"
}
```

3.24.11 GET /api/hpcgw/v2/device/transparent/api/service/device/otap/table/list?pageIndex=%s&pageSize=%s

Get OTAP list data.

Request URL

https://{areaDomain}/api/hpcgw/v2/device/transparent/api/service/device/otap/table/list?pageIndex=%s&pageSize=%s

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	User access token, which is in the format of "Bearer <accessToken>".
x-devserial	Req.	String	Header	Device serial No.
X-LocalIndex	Req.	String	Header	Resource No.
X-ResourceCategory	Req.	String	Header	Resource category.
X-DomainIdentifier	Req.	String	Header	Function field.
X-PropIdentifier	Req.	String	Header	Function property identifier.
x-listIdentifier	Req.	String	Header	Function identifier.
pageIndex	Req.	Integer	Body	Page No., 1 by default. If the configured value is less than or equal to 0, page No. 1 will be returned; if the configured value is larger than the last page No., the last page No. will be returned.
pageSize	Req.	Integer	Body	Number of records on each page, 10 by default, maximum 150.

Request Example

```
curl --location --request GET https://ieuapi.hik-partner.com/api/hpcgw/v2/device/transparent/api/service/device/
otap/table/list?pageIndex=1&pageSize=150 ' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer hpc.l68ptk43b0hfijoko3vxfhx5oegqo6mz' \
--header 'x-devserial: Q04553078' \
--header 'X-DomainIdentifier: UserMgr' \
--header 'X-PropIdentifier: UserInfoCfgList' \
--header 'X-LocalIndex: 0' \
--header 'X-ResourceCategory: global' \
--header 'x-listIdentifier: UserInfoCfgChangeSync'
```

Response Parameters

Parameter	Data Type	Description
data	Object	Returned OTAP list data.
pageIndex	Integer	Page No.
pageSize	Integer	Number of records on each page.
records	Array< String >	Property value, in JSON format.
totalPages	Integer	Total pages.
totalElements	Integer	Total number of records.

Response Example

```
{
   "data": {
          " pageIndex": 1,
          " pageSize":150,
          " records ": ["xxx","xxx"],
" totalPages":1,
" totalElements":20
      },
   "errorCode": "0",
   "message": "Ok"
}
```

3.25 POST /api/hpcgw/v1/device/upgrade/state

Get the upgrade status of device, i.e., whether there is a later version for device upgrade.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceSerial	Req.	String	Body	Device serial No.

Request Example

```
{
  "deviceSerial": "abc"
}
```

Response Parameters

Parameter	Data Type	Description
isNeedUpgrade	Integer	Whether a later version is available for device upgrade: 0-no, 1-yes.

Response Example

```
{
"data": {
    "isNeedUpgrade": 1
},
"errorCode": "0"
}
```

3.26 POST /api/hpcgw/v1/device/cloud/enable

Enable/disable the device operation permission of end users.

Note

After handing over the site by sharing it to the end user, you can disable the Hik-Connect Mobile Client for the devices. Once it is disabled, the end user cannot perform device operations (such as live view, playback, arming and disarming, etc.) on Hik-Connect Mobile Client.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
siteId	Req.	String	Body	Site ID.
cloudEnable	Req.	Boolean	Body	Enable/disable device permission: true (enable), false (disable).

Request Example

```
{
  "siteId": "abcdcedfhg",
  "cloudEnable": false
}
```

Response Example

```
{
"errorCode": "0"
}
```

3.27 POST /api/hpcgw/v1/device/pincode/query

Search for device PIN code. Up to 100 requests can be made for each device within 24 hours.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceSerial	Req.	String	Body	Device serial No.

Request Example

```
{
  "deviceSerial": "abc"
}
```

Response Parameters

Parameter	Data Type	Description
pin	String	PIN code.
deviceSerial	String	Device serial No.

Response Example

```
{
"data": {
"pin": "xxxx",
"deviceSerial":"xxxx"
},
"errorCode": "0"
}
```

3.28 POST /api/hpcgw/v1/device/upgrade

Upgrade device. For security control panel of the first generation (AlarmHost(3)), the request parameters **username** and **password** are required; for other security control panels, **pinCode** is required and **username** is optional.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceSerial	Req.	String	Body	Device serial No.
password	Opt.	String	Body	EN certificated device password.

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
username	Opt.	String	Body	EN certificated device user name.
pinCode	Opt.	String	Body	Pin code, obtained from ***Request Parameters*** .

Request Example

```
{
"deviceSerial": "abc",
"password":"xxx",
"username":"xxx",
"pinCdode":"xxx"
}
```

Response Parameters

Parameter	Data Type	Description
deviceSerial	String	Device serial No.
error	String	Error code for upgrading failed.
errorDesc	String	Error description for upgrading failed.

Response Example

```
{
"data": {
"deviceSerial":"xxxx",
"error":"xxxx",
"errorDesc":"xxxx"
},
"errorCode": "0"
}
```

3.29 POST /api/hpcgw/v1/device/upgrade/progress

Get the upgrade progress of device.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceSerial	Req.	String	Body	Device serial No.

Request Example

```
{
  "deviceSerial": "abc"
}
```

Response Parameters

Parameter	Data Type	Description
deviceSerial	String	Device serial No.
progress	Integer	Upgrading progress (%).
statue	Integer	0-to be upgraded, 1-start upgrading, 2-download in progress, 3-download finished, 4-burning in progress, 5-burning finished, 6-rebooting, 7-upgrade finished, 8-device returns error code.
error	String	Error code for upgrading failed.
errorDesc	String	Error description for upgrading failed.

Response Example

```
{
"data": {
    "progress": 1,
 "statue": 1,
"error":"xxxx",
"errorDesc":"xxxx"
},
"errorCode": "0"
}
```

3.30 POST /api/hpcgw/v1/device/iot/ability/query

Check whether the object model device adding capability is supported. If it is, call the API of adding object model device.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceSerial	Req.	String	Body	Device serial No.
siteId	Req.	String	Body	Site ID, 1 to 48 digits, which cannot be null. Specify the site which the device is added to.

Request Example

```
{
  "deviceSerial": "abc",
  "siteId": "aaaaa"
}
```

Response Parameters

Parameter	Data Type	Description
supportForceCheckAuth	Integer	Whether adding via physical button is supported: 0-no, 1-yes.

Response Example

```
{
  "data": {
    "supportForceCheckAuth":1
  },
  "errorCode": "0"
}
```

3.31 POST /api/hpcgw/v1/device/iot/add/result

Search for adding status of the object model device.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceSerial	Req.	String	Body	Device serial No.

Request Example

```
{
  "deviceSerial": "abc"
}
```

Response Parameters

Parameter	Data Type	Description
deviceName	String	Device name.
deviceSerial	String	Device serial No.
deviceCategory	Integer	Device type.
subType	Integer	Device subtype.

Response Example

```
{
    "data": {
"deviceSerial":"xxxx",
"deviceName":"xxxx",
"deviceCategory":"xxxx",
"subType":"xxxx"
    },
    "errorCode": "0"
}
```

3.32 POST /api/hpcgw/v1/device/camera/wakeUp

Wake up solar camera.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceSerial	Req.	String	Body	Device serial No.

Request Example

```
{
  "deviceSerial": "xxxx"
}
```

Response Parameters

Parameter	Data Type	Description
wakeUp	Integer	1 (awake), 0 (sleeping).

Response Example

```
{
"data":{
  "wakeUp":1
},
"errorCode": "0"
}
```

3.33 POST /api/hpcgw/v1/mq/subscribe

Subscribe to alarm messages from the devices.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
subType	Req.	Integer	Body	Status: 1 (subscribe), 0 (unsubscribe)
subMode	Req.	String	Body	Subscription mode: "all" (all devices, including newly-added devices), "list" (devices in the list).
deviceSerialList	Opt.	Array	Body	Device serial No. list. This node is not valid when **subMode** is "all", while it is required when **subMode** is "list".

Request Example

```
{
  "subType": 1,
  "subMode": "list",
  "deviceSerialList": ["abc", "def"]
}
```

Response Example

```
{
  "errorCode": "0"
}
```

3.34 POST /api/hpcgw/v1/mq/messages

Get alarm messages.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".

Response Parameters

Parameter	Data Type	Description
formatType	String	Message format: XML and JSON
accountNumber	String	User No.
deviceSerial	String	Device serial No.
alarmData	String	The alarm data type is string when the message format is JSON and XML. If you need the complete ISAPI protocols, contact technical support or visit tpp.hikvision.com.
batchId	String	The ID of batch operation, which is used to manually confirm that the messages are received, or the message will be re-sent after a while.

Note

It is recommended to call the API continuously to get event information. After getting event information, it is recommended to call the offset API to confirm that the messages are received as soon as possible. By default, the platform only caches two hours of event information.

Response Example

```
{
  "data":{
    "batchId":"xxxxx",
    "list":[{
      "formatType":"XML",
      "accountNumber":"xxx",
      "deviceSerial": "DS2323", //device serial number,
      "alarmData":"xxx"
    },
    {
      "formatType":"JSON",
      "accountNumber":"xxx",
      "deviceSerial": "DS2323", //device serial number,
      "alarmData":{
        "deviceSerial":"xxx",
        "eventType":"VMD"
      }
    }]
  },
  "errorCode":"0"
}
```

3.35 POST /api/hpcgw/v1/mq/offset

Confirm that messages are received.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
batchId	Req.	String	Body	The ID of the Batch operation, which is returned by the API ***POST /api/hpcgw/v1/mq/ messages*** .

Request Example

```
{
  "batchId": "xxxx"
}
```

Response Example

```
{
  "errorCode": "0"
}
```

3.36 POST /api/hpcgw/v1/alarm/pictureurl

Get the URL for downloading an alarm-related picture.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
filePath	Req.	String	Body	The directory of the file attached in the alarm message. The file name starts with ISAPI_ FILES.

Request Example

```
{
  "filePath":“ISAPI_FILES/C94115305_6/20210809105618274-
C94115305-6-10000-2$encrypt=2,2021-08-09T12:54:25,fd9b7f16393203046d40be71da380128”
}
```

Response Parameters

Parameter	Data Type	Description
pictureUrl	String	The URL for downloading the picture. Valid for two hours.
encrypt	Boolean	Whether the picture is encrypted.

Response Example

```
{
  "data":{
    "pictureUrl": "",
    "encrypt": true
  },
  "errorCode": "0"
}
```

3.37 POST /api/hpcgw/v1/arcservice/device/list

Get the list of devices with ARC service enabled. This API is available to ARC users only.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
page	Opt.	Integer	Body	Page No. The value is page 1.
pageSize	Opt.	Integer	Body	The number of items on each page. The value is 20 by default.
siteId	Opt.	Integer	Body	Site ID.
deviceSerialList	Opt.	List<String>	Body	Device serial No. set. Maximum 200 items are allowed.

Request Example

```
{
  "page": 1,
  "pageSize": 20,
  "deviceSerialList": ["xxxx","xxxx"]
}
```

Response Parameters

Parameter	Data Type	Description
id	String	Device ID.
deviceName	String	Device name.
deviceOnlineStatus	Integer	Device status: 0 (offline), 1 (online), 2 (unknown).
deviceSerial	String	Device serial No.
deviceVersion	String	Device version No.

Parameter	Data Type	Description
deviceType	String	Device model type.
deviceCategory	Integer	Device type: 1 (IPC), 2 (NVR), 3 (AlarmHost), 4 (Intercom), 5 (AccessControl), 7 (IPDome), 8 (Doorbell), 9 (StorageBox) 10 (thermalCamera), 11 (Switch), 99 (all devices).
deviceSubCategory	Integer	Device sub type: 0 (Unknown), 1 (NVR), 2 (DVR), 3 (AX2), 4 (AX Hub), 5 (AX Hybrid), 6 (panic alarm station), 7 (box panic alarm station), 8 (pole panic alarm station), 9 (MinMoe), 10 (AX Hybrid Pro), 11 (solar camera), 12 (door station), 13 (fall detection radar).
isSubscribed	Boolean	Whether to subscribe to event/alarm information.
deviceAddTime	String	Time (in ISO 8601 format) when the device is added, e.g., "2021-03-25T06:26:01.927Z".
timeZone	String	Time zone. See details in ***Time Zone List*** .
extInfo	String	Extended information added for the device.
siteID	String	Site ID.
siteName	String	Site name.

Response Example

```
{
 "data":{
  "page": 1,
  "pageSize": 20,
  "rows": [{
   "deviceCategory": 3,
   "deviceName": "xxx",
   "deviceOnlineStatus": 0,
   "deviceSerial": " Q01728482",
   "deviceVersion": " V2.0.0 build 200224",
   "id": "xxxxxxxxxx",
   "deviceSubCategory":0,
   "deviceType": "DS-PWA96-M-WE",
   "isSubscribed": 1,
   "deviceAddTime":”2014-03-25T06:26:01.927Z”,
   "timeZone":"182",
   "extInfo":"xxxx",
   "siteID":"xxxxxxxx",
   "siteName":"xxx"
```

```
    }],
    "total": 0,
    "totalPage": 0
  },
  "errorCode": "0"
}
```

3.38 POST /api/hpcgw/v1/arcservice/device/enable

Enable the ARC service of devices. All event types will be subscribed by default. This API is available to both ARC users and installers.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceSerial	Req.	String	Body	Device serial No.
arcId	Req.	String	Body	ARC ID.

Request Example

```
{
   "deviceSerial": "xxx",
   "arcId": "xxx"
}
```

Response Parameters

Parameter	Data Type	Description
permission	Integer	ARC permission status: 0 (to be approved by end user), 1 (approved and applied), null (editing failed).

Response Example

```
{
“data”:{
   “permission”: 1
   },
"errorCode": "0"
}
```

3.39 POST /api/hpcgw/v1/arcservice/device/disable

Disable the ARC service of devices. This API is available to both ARC users and installers.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceSerial	Req.	String	Body	Device serial No.

Request Example

```
{
  "deviceSerial": "xxx"
}
```

Response Example

```
{
  "errorCode": "0"
}
```

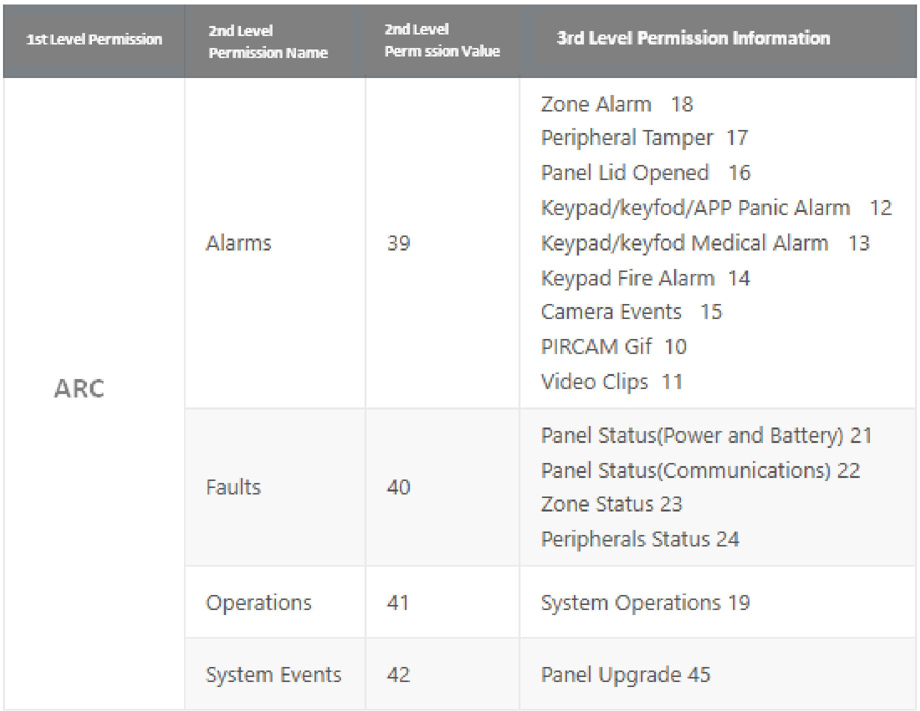
3.40 POST /api/hpcgw/v1/arcservice/event/type/update

Edit the ARC event list of device. This API is available to both ARC users and installers. Either **ax2PermissionList** or **CCTVEventList** should be configured: **ax2PermissionList** is the specific permission to devices of AX Pro series; **CCTVEventList** is the event list of encoding device.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceSerial	Req.	String	Body	Device serial No.
ax2PermissionList	Opt.	List<Integer>	Body	Supported event list of security control panel (completely overwritten once edited, e.g., first set to <10, 11, 12, 13> and the second time set to <10>, <10> shall prevail): • Permission items of **AX Pro and AX Hybrid Pro series**: 10-PIRCAM Gif, 11-Video Clips, 12-Panic Alar, 13-Medical Alarm, 14-Fire Alarm, 15-Smart Alarm, 16-Panel Lid Opened, 17-Peripheral Tamper, 18-Zone Alarm, 19-System Operation, 21-Panel Status(Power&Battery), 22-Panel Status(Communications), 23-Zone Status, 24-Peripherals Status, 45-Panel Upgrade. **Note** For AX Pro series, 10 to 18 belongs to 39, therefore should be entered along with 39; same with 21 to 24 that belongs to 40, 19 that belongs to 41, and 45

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
				belong to 42. See the ARC Permission table below. • Permission items of **AX Home series**: 5-Alarms, 6-Faults, 7-Operations, 8-System Events.
CCTVEventList	Opt.	List<Integer>	Body	Supported event list of security control panel (completely overwritten once edited, e.g., first set to <1, 2, 3> and the second time set to <4>, <4> shall prevail); if set to <0>, all values previously set will be canceled): 1-IO, 2-VMD, 3-diskerror, 4-diskfull, 5-diskrecover, 6-fielddetection, 7-linedetection, 9-recordException, 10-regionEntrance, 11-regionExiting, 12-shelteralarm, 13-videoloss, 14-fireDetection, 15-TMPA, 16-TMA, 17-TDA.



1st Level Permission	2nd Level Permission Name	2nd Level Perm ssion Value	3rd Level Permission Information
ARC	Alarms	39	Zone Alarm 18 Peripheral Tamper 17 Panel Lid Opened 16 Keypad/keyfod/APP Panic Alarm 12 Keypad/keyfod Medical Alarm 13 Keypad Fire Alarm 14 Camera Events 15 PIRCAM Gif 10 Video Clips 11
	Faults	40	Panel Status(Power and Battery) 21 Panel Status(Communications) 22 Zone Status 23 Peripherals Status 24
	Operations	41	System Operations 19
	System Events	42	Panel Upgrade 45

Figure 3-1 ARC Permission

Request Example

```
{
 "deviceSerial": "xxx",
 "ax2PermissionLists": [
  22
 ],
 "eventFilterLists": [
  1
 ]
}
```

Response Parameters

Parameter	Data Type	Description
permission	Integer	ARC permission status: 0 (request in progress), 1 (editing applied), null (editing failed).

Response Example

```
{
“data”:{
    “permission”: 1
    },
"errorCode": "0"
}
```

3.41 POST /api/hpcgw/v1/arcservice/account/number/update

Edit device account No. This API is available to both ARC users and installers.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceSerial	Req.	String	Body	Device serial No.
accountNumber	Req.	String	Body	Account No.

Request Example

```
{
    "deviceSerial": "xxx",
    "accountNumber": "xxx"
}
```

Response Example

None.

3.42 GET /api/hpcgw/v1/arcservice/site/{id}/info

Get site information of devices with ARC service enabled. This API is available to ARC users only.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
id	Req.	String	Body	Site ID.

Response Parameters

Parameter	Data Type	Description
id	String	The site ID.
siteName	String	Site name.
timeZone	String	Site time zone.
timeSync	boolean	Whether to sync time zone.
installerId	String	Site manager (installer) ID. The first installer ID will be returned if there are multiple installers.
installerFirstName	String	Site manager (installer) first name.
installerLastName	String	Site manager (installer) last name.
installerEmail	String	Site manager (installer) email.
installerPhone	String	Site manager (installer) phone number.
siteState	String	The state where the site locates.
siteCity	String	The city where the site locates.
siteStreet	String	The street where the site locates.
location	String	The detailed address where the site locates.
siteOwnerName	String	Site owner (end user) name.
siteOwnerEmail	String	Site owner (end user) email.
siteOwnerPhone	String	Site owner (end user) phone number.
sharedInfo	Object	Information about site sharing.

Parameter	Data Type	Description
shareType	Integer	0: the site belongs to the current company, and has not been shared. 1: the site belongs to the current company, but it is shared with a maintenance service partner. 2: the site is shared by other companies, and you have provided maintenance services. 3: the site belongs to the current company, and it is shared with installers to provide you with device installation and configuration services. After you hand over the site to customers, the sharing with the installation service partner will be revoked automatically. 4: the site is shared by other companies, and you have provided device installation and configuration services.
shareState	Integer	0: Waiting to be authenticated by end user. 1: Waiting for other companies to accept. 2: It is currently shared with others. 3: Sharing request denied by end user. 4: Sharing request denied by other companies.
shareToCompany	Object	It is returned when you sharing your sites with other companies. Only one node can exist between this node and **shareFromCompany**.
shareFromCompany	Object	It is returned when the site is shared with you by other companies. Only one node can exist between this node and **shareToCompany**.
address	String	Sharer/Sharee company address.
companyName	String	Sharer/Sharee company name.
email	String	Sharer/Sharee email address.
firstName	String	Sharer/Sharee person first name.
lastName	String	Sharer/Sharee person last name.
phone	String	Sharer/Sharee company phone number.
street	String	Street where the sharer/sharee company is located.

Response Example

```
For sites shared with others:
{
  "data": {
    "id": "",
    "siteName": "",
    "siteCity": "",
    "siteState": "",
    "siteStreet": "",
    "location": "",
    "timeSync": true,
    "timeZone": "",
    "installerId": "",
    "installerFirstName": "",
    "installerLastName": "",
    "installerEmail": "",
    "installerPhone": "",
    "siteOwnerName ": "",
    "siteOwnerEmail": "",
    "siteOwnerPhone": ""
    "sharedInfo":
      {
       "shareState": 4,
       "shareType": 3,
       "shareToCompany":
        {
         "address": "",
         "companyName": "",
         "email": "",
         "firstName": "",
         "lastName": "",
         "phone": "",
         "street": ""
        }
      }
    },
    {
     "id": "",
   "installerFirstName": "",
   "installerId": "",
   "installerLastName": "",
     "location": "",
   "siteCity": "",
   "siteName": "",
   "siteState": "",
   "siteStreet": "",
   "timeSync": true,
   "timeZone": "182",
     "sharedInfo":
     {
      "shareState": 4,
      "shareType": 4,
      "shareFromCompany":
       {
        "address": "",
        "companyName": "",
        "email": "",
        "firstName": "",
        "lastName": "",
        "phone": "",
        "street": ""
       }
     }
   },
   "errorCode": "0"
}
```

For sites shared by others:

```
{
  "data": {
    "id": "",
    "siteName": "",
    "siteCity": "",
    "siteState": "",
    "siteStreet": "",
    "location": "",
    "timeSync": true,
    "timeZone": "",
    "installerId": "",
    "installerFirstName": "",
    "installerLastName": "",
    "installerEmail": "",
    "installerPhone": "",
    "siteOwnerName ": "",
    "siteOwnerEmail": "",
    "siteOwnerPhone": ""
    "sharedInfo":
      {
       "shareState": 4,
       "shareType": 3,
       "shareToCompany":
        {
         "address": "",
         "companyName": "",
         "email": "",
         "firstName": "",
         "lastName": "",
         "phone": "",
         "street": ""
        }
      }
    },
    "errorCode": "0"
}
```

3.43 POST /api/hpcgw/v1/person/add

Add a person.

Request Parameters

Note

Calling this API will not result in person information being added to devices. To apply person information, refer to ***POST /api/hpcgw/v1/acs/privilege/config*** .

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
employeeNo	Req.	String	Body	Employee ID. 1 to 32 numbers and letters allowed.
type	Req.	Integer	Body	Person type: 0 (employee), 1 (temporary employee), 2 (visitor).
familyName	Req.	String	Body	Family name. 1 to 32 characters allowed.
givenName	Req.	String	Body	Given name. 1 to 32 characters allowed.
email	Opt.	String	Body	Email address. 1 to 128 characters allowed.
phone	Opt.	String	Body	Phone number. 1 to 32 characters allowed.
facePicture	Opt.	String	Body	Face picture data encoded by Base 64. Only JPEG format

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
				allowed. The size should be within 200 KB.
cardNo	Opt.	String	Body	Card number. 1 to 20 numbers allowed.

Request Example

```
{
  "employeeNo": "",
  "type": 1,
  "familyName": "aa",
  "givenName": "aa",
  "email": "aaa",
  "phone": "12344535",
  "facePicture": "xxxxxxxxxxxxxxxxxxxxxxxx",
  "cardNo": "xxxxxxxxxxxxxxxxxxxxxxxx"
}
```

Response Parameters

Parameter	Data Type	Description
personId	String	Person ID.

Response Example

```
{
  "data":{
    "personId":"xxx"
    },
  "errorCode": "0"
}
```

3.44 POST /api/hpcgw/v1/person/update

Edit person information.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
personId	Req.	String	Body	Person ID.
employeeNo	Opt.	String	Body	Employee ID. 1 to 32 numbers and letters allowed.
type	Opt.	Integer	Body	Person type: 0 (employee), 1 (temporary employee), 2 (visitor).
familyName	Opt.	String	Body	Family name. 1 to 32 characters allowed.
givenName	Opt.	String	Body	Given name. 1 to 32 characters allowed.
email	Opt.	String	Body	Email address. 1 to 128 characters allowed.
phone	Opt.	String	Body	Phone number. 1 to 32 characters allowed.
facePicture	Opt.	String	Body	Face picture data encoded by Base 64. Only JPEG format allowed. The size should be within 200 KB.
cardNo	Opt.	String	Body	Card number. 1 to 20 numbers allowed.

Request Example

```
{
  "personId": "xxx",
  "employeeNo": “1111122”
}
```

Response Example

```
{
  "errorCode": "0"
}
```

Note

Calling this API will not result in person information being edited on devices. To apply edited person information, refer to ***POST /api/hpcgw/v1/acs/privilege/config*** .

3.45 POST /api/hpcgw/v1/person/delete

Delete person information.

Request Parameters

Note

Calling this API will not delete persons on devices. If you need to delete person information on devices, call the API ***POST /api/hpcgw/v1/acs/privilege/delete*** .

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
personIds	Req.	Array	Body	Person ID list.

Request Example

```
{
  "personIds": ["abc", "def"]
}
```

Response Example

```
{
  "errorCode": "0"
}
```

3.46 POST /api/hpcgw/v1/acs/privilege/config

Apply person information and permissions to an access control device.

Request Parameters

Note

It is an asynchronous API. For getting the applying status of person information and permissions, see ***POST /api/hpcgw/v1/acs/privilege/status*** .

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceAuthorities	Req.	Array	Body	Permission list. The permitted time range is all day by default.
deviceSerial	Req.	String	Body	Device serial No.
personIdList	Req.	Array	Body	Person ID list.

Request Example

```
{
  "deviceAuthorities": [
    {
    "deviceSerial":"xxxxx",
    "personIdList":["xxx","xxxx"]
    }
  ]
}
```

Response Example

```
{
  "errorCode": "0"
}
```

3.47 POST /api/hpcgw/v1/acs/privilege/status

Get the applying status of person information and permission.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
personIdList	Req.	Array	Body	Person ID list.

Request Example

```
{
  "personIdList": ["abc","def"]
}
```

Response Parameters

Parameter	Data Type	Description
personAuthorities	Array	Permission list.
personId	String	Person ID.
deviceLists	Array	Device list.
deviceSerial	String	Device serial No.
status	Integer	Applying status: 0 (applying), 1 (applying succeeded), 2 (applying failed).
subStatus	Integer	Applying sub-status: 0 (applying failed or not supported by device), 1 (applying succeeded). When **status** is 2 and **subStatus** is 0, it indicates the applying failed; when **status** is 1 and **subStatus** is 0, it indicates the applying is not supported by device. From the high figure to low figure, it represents person, card, face, and fingerprint. For example,

Parameter	Data Type	Description
		7, as in 0111b, represents applying the first 3 items succeeded while the last failed. If **status** is 1, it indicates fingerprint information is not supported by device; if **status** is 2, it indicates fingerprint information is supported but applying it failed.
error	String	Error codes, see details in ***Status or Error Code*** . For other error codes, contact the technical support for help or visit tpp.hikvision.com to get them.

Response Example

```
{
 "data":{
   "personAuthorities": [{
    "personId": "12345",
    "deviceLists": [{
     "deviceSerial": "",
     "status": 0,
     "subStatus": 7,
     "error": "xxx"
    }]
   }]
 },
 "errorCode": "0"
}
```

3.48 POST /api/hpcgw/v1/acs/privilege/delete

Delete the applied person information and permission on an access control device.

Request Parameters

Note

Deleting person information and permissions can not be completed if you only call ***POST /api/hpcgw/v1/person/delete*** . You also need to call ***POST /api/hpcgw/v1/acs/privilege/delete*** .

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceAuthorities	Req.	Array	Body	Permission list. The permitted time range is all day by default.
deviceSerial	Req.	String	Body	Device serial No.
personIdList	Req.	Array	Body	Person ID list.

Request Example

```
{
  "deviceAuthorities": [{
    "deviceSerial":"abc",
    "personIdList":["12233", "2344545"]
  }]
}
```

Response Example

```
{
  "errorCode": "0"
}
```

3.49 POST /api/hpcgw/v1/person/synchronize

Synchronize person information from device to the platform.

Request Parameters

Note

- It is an asynchronous API.
- On each device, you can only create and perform one task at a time. Each task is identified by the returned **syncTaskID**.
- Call ***POST /api/hpcgw/v1/person/synchronize/progress*** to search for the task progress.

- Call ***POST /api/hpcgw/v1/person/synchronize/details*** to search for the synchronized person details.
- If a person owns multiple cards, only the first regular card along with the first fingerprint, the face picture, and the basic person information will be synchronized for the person's credential.

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceSerial	Req.	String	Body	Device serial No.
employeeNoList	Opt.	Array	Body	Employee ID list. You can specify employees from the person list on device. Each ID should contain no more than 32 letters, digits, or letters and digits. When this field is empty or not configured, all persons will be synchronized.

Request Example

```
{
"deviceSerial":"DIPZ497",
"employeeNoList": ["00001","00002"]
}
```

Response Parameters

Parameter	Data Type	Description
syncTaskID	String	Person synchronization task ID.

Response Example

```
{
   "data":{
   "syncTaskID":"123"
   },
   "errorCode": "0"
}
```

3.50 POST /api/hpcgw/v1/person/synchronize/progress

Search for person information synchronization progress.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
syncTaskID	Req.	String	Body	Synchronization task ID, returned from ***POST /api/hpcgw/v1/person/synchronize*** . The maximum length is 64.

Response Parameters

Parameter	Data Type	Description
totalNum	Integer	Total persons to be synchronized.
taskStates	Integer	Synchronization task status: 0- failed, 1-succeeded, 2-in progress.
syncSucceedNum	Integer	Number of persons synchronized.
syncFailedNum	Integer	Number of persons failed to be synchronized.

Response Example

```
{
  "data": {
    "totalNum": 3,
    "syncSucceedNum": 1,
    "syncFailedNum": 1,
    "taskStates": 2
  },
  "errorCode": "0"
}
```

3.51 POST /api/hpcgw/v1/person/synchronize/details

Search for person synchronization details.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
syncTaskID	Req.	String	Body	Synchronization task ID, returned from ***POST /api/ hpcgw/v1/person/ synchronize*** . The maximum length is 64.
queryType	Req.	Integer	Body	Specify the search type: 0- search for failed synchronization details, 1- search for succeeded synchronization details.
page	Opt.	Integer	Body	The current page. When this field is empty, it is the first page by default.
pageSize	Opt.	Integer	Body	Number of records on each page, which is between 1 and 200. When this field is empty, it is 20 by default.

Response Parameters (When queryType is 0)

Parameter	Data Type	Description
total	Integer	Total persons in the synchronization task.
page	Integer	The current page.
pageSize	Integer	Number of records on each page, which is between 1 and 200.
totalPage	Integer	Total pages.

Parameter	Data Type	Description
rows	Array	When **queryType** is 0, only failed synchronization details will be returned; when **queryType** is 1, only succeeded synchronization details will be returned.
employeeNo	String	Employee ID, which should contain no more than 32 letters, digits, or letters and digits.
subStatus	Integer	Person synchronization sub-status: 1-succeeded, 0-failed. From the high figure to low figure, it represents basic person information, card, face, and fingerprint. For example, 7, as in 0111b, represents synchronizing the first 3 items succeeded while the last failed. See details in the corresponding error codes.
errorCode	String	Error codes, see details in ***Status or Error Code*** . For other error codes, contact the technical support for help or visit tpp.hikvision.com to get them.

Response Example (When queryType is 0)

```
{
  "data": {
    "total": 1,
    "page": 1,
    "pageSize": 1,
    "rows": [
      {
        "employeeNo": "10000",
        "errorCode": "EVZ20008",
        "subStatus": 7
      }
    ]
  },
  "totalPage": 1,
  "errorCode": "0"
}
```

Response Parameters (When queryType is 1)

Parameter	Data Type	Description
total	Integer	Total persons to be synchronized.
page	Integer	The current page.
pageSize	Integer	Number of records on each page, which is between 1 and 200.

Parameter	Data Type	Description
totalPage	Integer	Total pages.
rows	Array	When **queryType** is 0, only failed synchronization details will be returned; when **queryType** is 1, only succeeded synchronization details will be returned.
employeeNo	String	Employee ID, which is a 32-digit combination of number(s) and letter(s).
personId	Integer	Person ID, newly generated after the synchronization and different from the person ID returned in ***POST /api/hpcgw/v1/person/add*** . A person can be identified with both IDs but it is recommended to use the new one.
type	String	Person type: 0- employee, 1-temporary employee, 2-visitor.
familyName	String	Family name. The maximum length is 32.
givenName	String	Given name. The maximum length is 32.
email	String	Email address. The maximum length is 128.
phone	String	Phone No. The maximum length is 32.
facePicture	String	Face picture URL, which is valid for 10 minutes.
cardNo	String	Card No. The maximum length is 20.
fingerprint	String	Binary data of fingerprint model encoded by Base64.

Response Example (When queryType is 1)

```
{
  "data": {
    "total": 1,
    "page": 1,
    "pageSize": 1,
    "rows": [
      {
        "personId ": "8a92d0e87617e071017617e251e50000",
        "cardNo": "30000",
        "email": "email20000",
        "employeeNo": "10000",
        "facePicture": "http://faceInfo/40000/faceURL",
        "familyName": "familyName20000",
        "givenName": "givenName20000",
        "fingerprint": " ZmluZ2VycHJpbnQgZGF0YQ==",
        "phone": "phone20000",
        "type": 0
      }
    ]
  },
"totalPage": 1,
  "errorCode": "0"
}
```

3.52 POST /api/hpcgw/v1/video/by/time

Get storage file information by time.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceSerial	Req.	String	Body	Device serial No. 1 to 9 characters allowed.
channelNo	Opt.	Integer	Body	Channel No., 1 by default.
startTime	Opt.	Long	Body	Start time, which is 0 o'clock time by default, unit: ms, e.g., 1378345128000.
endTime	Opt.	Long	Body	End time, which is the current time by default, unit: ms, e.g., 1378345128000.
recType	Opt.	Integer	Body	Playback source: 0-auto selected by system (default), 1-cloud storage, 2-local recording.

Request Example

```
{
   "deviceSerial": "Q124434",
   "channelNo": 1,
   "startTime": 1689929320315,
   "endTime": 1689929356315,
   "recType": 2
}
```

Response Parameters

Parameter	Data Type	Description
recType	Integer	Playback source: 0-auto selected by system, 1-cloud storage, 2-local recording.
startTime	Long	Start time of the file.
endTime	Long	End time of the file.
localType	String	File type: "0"-ALARM, "1"-TIMING, "2"-IO.
crypt	Integer	Whether it is encrypted: 0-no, 1-yes.

Response Example

```
{
      "data":[{
     "recType": 2,
        "startTime": 1689929320315,
        "endTime": 1689929356315,
        "localType": "0",
        "crypt": 1
     }],
     "errorCode": "0"
}
```

3.53 POST /api/hpcgw/v1/hotspare/add

This API is used for configuring the type of hot spare device (spare).

Note

- For configuring the hot spare device type, you should configure the host device before the spare device, or the error code LAP026338 will be returned.
- A spare device can only be configured once. For example, if spare device No.1 has been configured and is to be configured again, the error code LAP026339 will be returned.
- Up to 3 spare devices can be configured.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
uuid	Req.	String	Body	Hot spare device UUID. The maximum length is 128 characters.
type	Req.	Integer	Body	Hot spare device type: 0-host device, 1-spare device No.1, 2-spare device No.2, 3-spare device No.3.

Request Example

```
{
  "uuid": "e7c0cee2-74a0-473f-802e-1afbb33d5303",
      "type": 0
}
```

Response Example

```
{
  "errorCode": "0"
}
```

3.54 POST /api/hpcgw/v1/hotspare/get

Search for information of hot spare device configured for the current AK.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".

Response Parameters

Parameter	Data Type	Description
uuid	String	Hot spare device UUID. The maximum length is 128 characters.
type	Integer	Hot spare device type: 0-host device, 1-spare device No.1, 2-spare device No.2, 3-spare device No.3.

Response Example

```
{
   "errorCode": "0",
   "message": "ok",
   "data": {
      "list": [{
         "uuid": "e7c0cee2-74a0-473f-802e-1afbb33d5303",
         "type": 0
      }]
   }
}
```

3.55 POST /api/hpcgw/v1/hotspare/delete

Delete hot spare device(s) under AK. Batch deleting devices or clearing all configurations under AK is supported.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deleteMode	Req.	String	Body	Deleting mode: "all" (delete all devices), "list" (delete specified devices).
list	Req.	String[]	Body	Array of UUIDs. This field is valid when **deleteMode** is "list".

Request Example

```
{
  "deleteMode":"list",  "list": ["e7c0cee2-74a0-473f-802e-1afbb33d5303"]
}
```

Response Example

```
{
  "errorCode": "0"
}
```

3.56 POST /api/hpcgw/v1/hotspare/heartbeat

Through the heartbeat interaction between the cloud and host/spare device, the spare device can tell if the host device is offline.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
uuid	Req.	String	Body	Hot spare device UUID. The maximum length is 128 characters.

Request Example

```
{
  "uuid":" e7c0cee2-74a0-473f-802e-1afbb33d5303"
}
```

Response Parameters

Parameter	Data Type	Description
uuid	String	Hot spare device UUID. The maximum length is 128 characters.
type	Integer	Hot spare device type: 0-host device, 1-spare device No.1, 2-spare device No.2, 3-spare device No.3.
timeLag	Long	The difference between the last update of heartbeat and the current time of the server, unit:ms.

Response Example

```
{
  "errorCode": "0",
  "message": "ok",
  "data": {
    "list": [{
      "uuid": "e7c0cee2-74a0-473f-802e-1afbb33d5303",
      "type": 0,
      "timeLag": 1707102237228
    }]
  }
}
```

3.57 POST /api/hpcgw/v1/hotspare/file/upload

Upload hot spare file to the cloud for backup.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
file	Req.	Binary	Body	The maximum size is 2 MB.

Response Parameters

Parameter	Data Type	Description
key	String	Storage location the file is uploaded to, which can be used for getting download URL and deleting file.

Response Example

```
{
   "errorCode": "0",
   "message": "ok",
   "data": {
        "key": ""
      }
   }
}
```

3.58 POST /api/hpcgw/v1/hotspare/file/downloadurl

Get the download URL for hot spare file.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
key	Req.	String	Body	File path.

Request Example

```
{
  "key":""
}
```

Response Parameters

Parameter	Data Type	Description
url	String	URL for downloading file.

Response Example

```
{
  "errorCode": "0",
  "message": "ok",
  "data": {
       "url": ""
     }
  }
}
```

3.59 POST api/hpcgw/v1/hotspare/file/get

Search for uploaded hot spare files.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".

Response Parameters

Parameter	Data Type	Description
key	String	Hot spare file path.
lastModifiedTime	Long	Time of last modification, with epoch timestamp, unit: ms.

Response Example

```
{
   "errorCode": "0",
   "message": "ok",
   "data": {
      "list": [{
         "key": "",
         "lastModifiedTime ": 1707102237228
      }]
   }
}
```

3.60 POST /api/hpcgw/v1/hotspare/file/delete

Delete hot spare file under AK.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
key	Req.	String	Body	File path.

Request Example

```
{
   "key":""
}
```

Response Example

```
{
   "errorCode": "0"
}
```

3.61 POST /api/hpcgw/v1/vas/opspack/active

Activate device maintenance package. If premium service exits, the premium service will be used prior to the local maintenance package.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceSerial	Req.	String	Body	Device serial No.
opspackType	Opt.	Integer	Body	Maintenance package type: 1-yearly package for all types of devices, 2-yearly package for

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
				network cameras. This parameter is required when no premium service exits.
num	Opt.	Integer	Body	Number of local items to be used: [1, 10]. This parameter is required when no premium service exits.

Request Example

```
{
   "deviceSerial": "xxxxxx",
   "opspackType": 1,
      "num": 2
}
```

Response Example

```
{
"errorCode": "0"
}
```

3.62 POST /api/hpcgw/v1/audio/file/upload

Upload an audio file.

Notes

- The audio file should be within 10 MB, and the supported formats are: MP3, WAV, and AAC.
- The main type of IP speaker is 12, and sub type is 19.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: multipart/form-data.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
fileName	Req.	String	Body	File name, which should be unique.
formatType	Req.	String	Body	File format: "mp3", "wav", "aac".
audioFile	Req.	MultipartFile	Body	Audio file. Only supports uploading a single file no larger than 10 MB.

Request Example

```
{
   "fileName": "xxxxxx",
   "formatType": "mp3",
   "audioFile": xxxxx
}
```

Response Parameters

Parameter	Data Type	Description
audioFileUrl	String	Audio file storage address.
uuid	String	Audio file unique ID.

Response Example

```
{
   "data": {
      "audioFileUrl": "xxxxx",
      "uuid":"xxxxx"
   },
   "errorCode": "0"
}
```

3.63 POST /api/hpcgw/v1/audio/file/add

Apply the audio file to the device.

Notes

- The audio file should be uploaded to get its storage URL via API ***POST /api/hpcgw/v1/audio/file/upload***.
- The audio file should be within 10 MB, and the supported formats are: MP3, WAV, and AAC.
- The main type of IP speaker is 12, and sub type is 19.

Request Parameters

Parameter	Req./Opt./Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceSerial	Req.	String	Body	Device serial number.
customAudioInfo	Req.	Object	Body	Audio content to be applied. See the table below for details.

Table 3-1 customAudioInfo Object

Parameter	Req./Opt./Dep.	Data Type	Parameter Type	Description
customAudioName	Req.	String	Body	Custom audio file name.
customAudioURL	Req.	String	Body	Custom audio file URL.
audioFileFormat	Req.	String	Body	Audio file format: "mp3", "wav", "aac".
uuid	Req.	String	Body	Audio file unique ID.

Request Example

```
{
   "deviceSerial": "xxxxxx",
   "customAudioInfo": {
      "customAudioName": "xxxxxx",
      "audioFileFormat": "xxxxxx",
      "customAudioURL": "xxxxx",
      "uuid":"xxxx"
   }
}
```

Response Example

```
{
   "errorCode": "0"
}
```

3.64 POST /api/hpcgw/v1/audio/file/list/get

Get the device's audio list. The main type of IP speaker is 12, and sub type is 19.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceSerial	Req.	String	Body	Device serial number.

Request Example

```
{
   "deviceSerial": "xxxxxx"
}
```

Response Parameters

Parameter	Data Type	Description
CustomAudioInfoList	List<Object>	
customAudioID	Integer	Custom audio file ID.
customAudioName	String	Custom audio file name.
customAudioPath	String	The directory for storing custom audio files on the server.

Parameter	Data Type	Description
audioFileFormat	String	Audio file format: "mp3", "wav", "aac".
audioFileSize	Integer	Audio file size, range: [0,2097152000], unit: byte.
audioFileDuration	Integer	Audio file duration, range: [0,3600], unit: second.
customAudioFile	Object	Custom audio file storage information. See the table below.

Table 3-2 customAudioFile Object

Parameter	Data Type	Description
filePathType	String	The access address type of custom audio file: "localPath" (device local storage), "simpleStorage" (simple storage protocol), "URL" (directly accessible address), "binary" (binary data for direct file transmission).
filePath	String	Audio file path.

Response Example

```
{
   "data": {
      "CustomAudioInfoList": [
         {
            "customAudioID": 11111,
            "customAudioName": "xxx",
            "customAudioPath": 11111,
            "audioFileFormat": 11111,
            "audioFileSize": 10,
            "audioFileDuration": 100,
            "customAudioFile": {
               "filePathType": "xxx",
               "filePath": "xxx"
            }
         }
      ]
   },
   "errorCode": "0"
}
```

3.65 POST/ api/hpcgw/v1/audio/file/del

Delete audio file(s). The main type of IP speaker is 12, and sub type is 19.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceSerial	Req.	String	Body	Device serial number.
customAudioIDList	Req.	String	List<Integer>	Audio file ID list. IDs in the list are unique.

Request Example

```
{
   "deviceSerial": "xxxxxx",
   "customAudioIDList": [1,2]
}
```

Response Parameters

Parameter	Data Type	Description
Result	List<Object>	
customID	Integer	ID of audio file to be deleted.
statusCode	Integer	Whether the operation is succeed: 1 (succeeded), other values (failed).
statusString	String	"ok" (succeeded), other values (error information).
subStatusCode	String	"ok" (succeeded), other values (error information).
errorCode	Integer	Status code: 1 (succeeded), other values (failed).
errorMsg	String	Error details.

Response Example

```
{
  "data": {
    "Result": [
      {
        "customID": 11111,
        "statusCode": 11111,
        "statusString": "xxx",
        "subStatusCode": "xxx",
        "errorCode": 111,
        "errorMsg": "xxx"
      }
    ]
  },
  "errorCode": "0"
}
```

3.66 POST /api/hpcgw/v1/audio/inter/cut

Audio cut-in. The main type (deviceCategory) of IP speaker is 12, and sub type (deviceSubCategory) is 19.

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	Authentication information, which is in the format of "Bearer <accessToken>".
deviceSerial	Req.	String	Body	Device serial number.
audioLevel	Req.	integer	Body	Priority level of audio play: [0,15]. The larger the value, the higher the priority. Compare the priority of the currently playing audio with that of cut-in audio to determine whether to play the cut-in audio immediately or wait until the current play finishes. The priority level of cut-in audio can be set higher.

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
enabled	Opt.	boolean	Body	Whether to enable cut-in: true (enable, default value), false (disable). When this field is absent, the cut-in is enabled by default.
playMode	Opt.	string	Body	Playing mode: "order" (play in order and repeat once), "loop" (loop in order). **Note** When **playMode** is loop, **playDuration** is required.
playDuration	Opt.	integer	Body	Playing duration: [0,86400], unit: second.
audioVolume	Req.	integer	Body	Broadcast volume: [0,100].
TTSLanguageType	Opt.	string	Body	TTS language type: "chinese", "english" (default value), "spanish", "russian", "japanese", "thai".
voiceType	Opt.	string	Body	Voice type: "male", "female".
pace	Opt.	integer	Body	Speech speed: [0,100].
playAudioList	Req.	List<Object>	Body	Cut-in audio content.
audioSource	Req.	string	Body	Audio source: "customAudio" (custom audio file), "speechSynthesis" (audio synthesis).
customAudioID	Opt.	integer	Body	Custom audio file ID, which is required when **audioSource** is "customAudio".
speechSynthesisContent	Opt.	string	Body	Audio synthesis content, which is required when **audioSource** is "speechSynthesis". Length: [1,4096].

Request Example

```
{
	"deviceSerial": "xxx",
	"audioLevel": 111,
	"enabled": true,
      "playMode": "xxx",
      "playDuration": 111,
      "audioVolume": 111,
      "TTSLanguageType": "xxx",
      "voiceType": "xxx",
      "pace": 111,
      "playAudioList": [
         {
            "audioSource": "xxx",
            "customAudioID": 111
         }
      ]
}
```

Response Example

```
{
   "errorCode": "0"
}
```

3.67 POST /api/hpcgw/webhook/v1/config/query

Get the message push configuration.

Request URL

https://{areaDomain}/api/hpcgw/webhook/v1/config/query

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	User access token, which is in the format of "Bearer <accessToken>".

Response Parameters

Parameter	Data Type	Description
callbackUrl	String	Callback push URL.
retryTimes	Integer	Retry attempts.
retryDelay	Long	Retry interval (millisecond).

Response Example

```
{
   "data": {
      "callbackUrl": "https://xxx.com",
      "retryTimes": 3,
      "retryDelay": 1000
   },
   "errorCode": "0"
}
```

3.68 POST /api/hpcgw/webhook/v1/config/save

Save message push configurations.

Note

- Currently, only one Webhook configuration is allowed per account.
- Callback push URLs must use HTTPS protocol.
- After the retry attempts reached the limit, messages will be discarded and persisted for 1 month. Integrators can contact technical support to re-push the valid messages.
- Refer to ***Webhook Message Push*** for the detailed process of secret key signature configurations.

Request URL

https://{areaDomain}/api/hpcgw/webhook/v1/config/save

Request Parameters

Parameter	Req./Opt./Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	User access token, which is in the format of "Bearer <accessToken>".
callbackUrl	Req.	String	Body	Callback push address (must support both GET and POST requests, and require HTTPS protocol). The maximum length is 256 characters.
retryTimes	Opt.	Integer	Body	Retry attempts. Range: [-1,5]. Default: 3. The value -1 indicates unlimited retries within 2 hours.

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
retryDelay	Opt.	Long	Body	Retry interval (millisecond).
signSecret	Opt.	String	Body	Secret key configuration for signatures (used for signing pushed information). Defaults to SecretKey (SK) if it is empty. The length is from 8 to 32 characters. Format: A combination of letters and digits.

Request Example

```
{
   "callbackUrl": "https://xxx.com",
   "retryTimes": 3,
   "retryDelay": 1000,
   "signSecret": "xxxx"
}
```

Response Example

```
{
   "errorCode": "0"
}
```

3.69 POST /api/hpcgw/webhook/v1/config/delete

Delete message push configurations.

Request URL

https://{areaDomain}/api/hpcgw/webhook/v1/config/delete

Request Parameters

Parameter	Req./Opt./ Dep.	Data Type	Parameter Type	Description
Content-Type	Req.	String	Header	Content type: application/json.
Authorization	Req.	String	Header	User access token, which is in the format of "Bearer <accessToken>".

Response Example

```
{
   "errorCode": "0"
}
```

Appendix A. Appendixes

A.1 Status or Error Code

The following are the error codes and their descriptions.

Error Code	Description
LAP300001	AK not found.
LAP300002	AK and SK mismatches.
LAP300003	The Hik-Partner Pro account bound with the AK doesn't exist.
LAP000000	System exception.
LAP000001	Parameter error.
LAP000003	No resource found.
LAP001005	The account is locked.
LAP002002	The email has been registered.
LAP002013	Incomplete admin information.
LAP002017	Deleting employees failed.
LAP004001	Sending email failed.
LAP004012	Deleting yourself is not allowed.
LAP004018	The role that linked to the site manager cannot be deleted.
LAP004030	The number of employees exceeded limit.
LAP004040	Frequent operation of inviting employees via email.
LAP006001	Adding device failed.
LAP006002	Unknown device.
LAP006006	Network exception.
LAP006008	The device serial No. already exists.
LAP006009	The device does not exist or no permission is granted.
LAP006011	The number of decoding devices reached limit.
LAP006012	Station does not exist.
LAP006013	No permission. The operator is not the site owner.

Error Code	Description
LAP006016	No permission for site operation.
LAP006018	Do not operate again.
LAP006053	Editing device...
LAP008000	Duplicate site name.
LAP008001	Site does not exist, or user has no permission.
LAP008002	You cannot edit site information unless you are a site manager.
LAP008004	Adding site failed.
LAP008006	Deleting site failed.
LAP008008	Network error.
LAP008011	Site management permission required.
LAP008015	Deleting site failed.
LAP008017	No permission to operate this resource.
LAP008024	Incomplete site manager information.
LAP008025	Only the Installer Admin or site manager can delete the site.
LAP008026	There are no sites belonging to the Installer Admin or site manager.
LAP008030	Site time zone are required.
LAP008044	Not supported operation. The site is not a site handled by sharing.
LAP008077	No permission.
LAP008081	The site is already shared.
LAP008082	The account does not exist or the account is banned.
LAP008087	The site is currently not shared.
LAP008092	The sharing credentials do not exist.
LAP008093	Sharing to your own company is not allowed.
LAP008099	There are multiple companies of the account to be shared.
LAP008103	Sharing failed. Make sure the site is not transferred.
LAP008104	The account does not have site management permissions.
LAP008127	Site of handover by sharing does not support this operation.
LAP020047	Synchronizing face picture URL failed.

Error Code	Description
LAP026338	Hot spare (host) not added.
LAP026339	Spare device No. already exists.
LAP026341	Hot spare file size exceeded limit.
LAP026342	Uploading hot spare file failed.
LAP030069	Person synchronization task in progress on the current device.
LAP033005	Getting token failed.
LAP034000	No permission for the account to access the device.
LAP034001	No permission for the account to access the site.
LAP034002	No permission for the account to access the company.
LAP035001	Requested resource not found.
LAP000000	System error.
LAP000001	Parameter error.
LAP000002	No resource found.
LAP500001	Service unavailable.
LAP500002	Open token is empty.
LAP500003	Invalid format of the open token.
LAP500004	Open token expired or incorrect (valid for 7 days).
LAP500005	Verifying the open token failed.
LAP500006	Getting information failed.
LAP500007	The number of calling times exceeds limit.
LAP031002	Uploading picture failed.
LAP031007	The file is too large.
LAP031008	Invalid file.
LAP012013	The employee does not exist.
LAP035004	Invalid format of the URL of the alarm-related picture.
LAP064001	The account information is not edited.
LAP064003	Sharing linkage already exists.
LAP064007	Duplicate accounts for sharing.

Error Code	Description
LAP068001	Other user is in search progress. (When AK and SK are occupied by searching, concurrent searching and synchronous calling are not supported.)
LAP068002	Pulling alarms failed.
VMS022554	Physical resources do not exist.
VMS050034	Linked device not found.
EVZ10001	Incorrect parameter.
EVZ10006	The IP address is restricted.
EVZ10007	Times of calling reached limit.
EVZ10013	The application has no permission to call this API.
EVZ10020	Request method is required.
EVZ10029	The API calling frequency exceeded limit.
EVZ20001	The channel does not exist.
EVZ20002	Device does not exist.
EVZ20006	Network exception.
EVZ20007	The device is offline.
EVZ20008	Device response timed out.
EVZ20010	Incorrect device verification code.
EVZ20012	Adding device failed.
EVZ20013	The device has been added by another account.
EVZ20014	Incorrect device serial No.
EVZ20015	The function is not supported by the device.
EVZ20016	Device is being formatted.
EVZ20017	The device is already added by yourself.
EVZ20018	The device is not linked to current account.
EVZ20019	The device doesn't support cloud storage service.
EVZ20020	The device is online and has been added by the current account.
EVZ20021	The device is online and hasn't been added by any account.
EVZ20022	The device is online and has been added by another account.

Error Code	Description
EVZ20023	The device is offline and hasn't been added by any account.
EVZ20024	The device is offline and has been added by another account.
EVZ20029	The device is offline and has been added by the current account.
EVZ20609	Device response timed out. Communication fault or insufficient battery of the door lock. Please try again.
EVZ49999	Data exception.
EVZ50000	Server exception.
EVZ60012	Unknown error.
EVZ60019	Encryption enabled.
EVZ60020	The command is not supported.
EVZ60040	Hik-Partner Pro is not on the same local network with the device.
EVZ60041	The device has been linked by another device or device response timed out.
EVZ60042	Incorrect device password.
EVZ60043	No more devices can be added.
EVZ60044	Accessing device network failed.
EVZ60048	Insufficient bandwidth.
EVZ60050	Adding device failed. Please upgrade the device first.
EVZ60051	The device is not supported.
EVZ60052	Incorrect channel number.
EVZ60053	Device resolution is not supported.
EVZ60054	Device account is locked.
EVZ60055	Streaming error.
EVZ60056	Deleting the device failed.

A.2 Time Zone List

Time Zone	Time Zone No.	UTC Offset
Alaska	2	UTC-09:00
Belgrade, Bratislava, Budapest, Ljubljana, Prague	27	UTC+01:00
Sarajevo, Skopje, Warsaw, Zagreb	28	UTC+01:00
Central Time (US & Canada)	30	UTC-06:00
Eastern Time(U.S. & Canada)	41	UTC-05:00
Helsinki, Kiev, Riga, Sofia, Tallinn, Vilnius	46	UTC+02:00
Dublin, Edinburgh, Lisbon, London	48	UTC+00:00
Athens, Bucharest	51	UTC+02:00
Hawaii	53	UTC-10:00
Mountain Time (US & Canada)	72	UTC-07:00
Pacific Time (US & Canada)	86	UTC-08:00
Baja California	87	UTC-08:00
Brussels, Copenhagen, Madrid, Paris	90	UTC+01:00
Indiana (Eastern)	119	UTC-05:00
Arizona	120	UTC-07:00
Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna	133	UTC+01:00
Casablanca	134	UTC+01:00
Monrovia, Reykjavik	135	UTC+00:00
Coordinated Universal Time	136	UTC+00:00
Sao Tome and Principe	137	UTC+01:00
West Central Africa	138	UTC+01:00
Amman	139	UTC+02:00

Time Zone	Time Zone No.	UTC Offset
Beirut	140	UTC+02:00
Harare, Pretoria	141	UTC+02:00
Kaliningrad	142	UTC+02:00
Damascus	143	UTC+02:00
Coordinated Universal Time+13	216	UTC+13:00
Christmas Island	217	UTC+14:00
Tripoli	144	UTC+02:00
Chisinau	118	UTC+02:00
Gaza, Hebron	145	UTC+02:00
Khartoum	146	UTC+02:00
Cairo	147	UTC+02:00
Windhoek	148	UTC+02:00
Jerusalem	149	UTC+02:00
Baghdad	150	UTC+03:00
Kuwait, Riyadh	151	UTC+03:00
Minsk	152	UTC+03:00
Moscow, St. Petersburg, Volgograd	153	UTC+03:00
Nairobi	154	UTC+03:00
Istanbul	155	UTC+03:00
Tehran	156	UTC+03:30
Abu Dhabi, Muscat	157	UTC+04:00
Astrakhan, Ulyanovsk	158	UTC+04:00
Yerevan	159	UTC+04:00
Baku	160	UTC+04:00
Tbilisi	161	UTC+04:00
Port Louis	162	UTC+04:00
Saratov	163	UTC+04:00

Time Zone	Time Zone No.	UTC Offset
Izhevsk, Samara	164	UTC+04:00
Kabul	165	UTC+04:30
Ashgabat, Tashkent	166	UTC+05:00
Ekaterinburg	167	UTC+05:00
Islamabad, Karachi	168	UTC+05:00
Chennai, Kolkata, Mumbai, New Delhi	169	UTC+05:30
Sri Jayewardenepura	170	UTC+05:30
Kathmandu	171	UTC+05:45
Astana	172	UTC+06:00
Dhaka	173	UTC+06:00
msk	174	UTC+06:00
Yangon (Rangoon)	175	UTC+06:30
Barnaul, Gorno-Altaysk	176	UTC+07:00
Hovd	177	UTC+07:00
Krasnoyarsk	178	UTC+07:00
Bangkok, Hanoi, Jakarta	179	UTC+07:00
Tomsk	180	UTC+07:00
Novosibirsk	181	UTC+07:00
Beijing, Chongqing, Hong Kong, Urumqi	182	UTC+08:00
Kuala Lumpur, Singapore	183	UTC+08:00
Taipei	184	UTC+08:00
Ulaanbaatar	185	UTC+08:00
Irkutsk	186	UTC+08:00
Perth	187	UTC+08:00
Eucla	188	UTC+08:45
Chita	189	UTC+09:00
Osaka, Sapporo, Tokyo	190	UTC+09:00

Time Zone	Time Zone No.	UTC Offset
Pyongyang	191	UTC+09:00
Seoul	192	UTC+09:00
Yakutsk	193	UTC+09:00
Adelaide	194	UTC+09:30
Darwin	195	UTC+09:30
Brisbane	196	UTC+10:00
Vladivostok	197	UTC+10:00
Guam, Port Moresby	198	UTC+10:00
Hobart	199	UTC+10:00
Canberra, Melbourne, Sydney	200	UTC+10:00
Lord Howe Island	201	UTC+10:30
Bougainville Island	202	UTC+11:00
Magadan	203	UTC+11:00
Norfolk Island	204	UTC+11:00
Chokurdakh	205	UTC+11:00
Sakhalin	206	UTC+11:00
Solomon Is., New Caledonia	207	UTC+11:00
Anadyr, Petropavlovsk-Kamchatsky	208	UTC+12:00
Auckland, Wellington	209	UTC+12:00
Coordinated Universal Time+12	211	UTC+12:00
Fiji	212	UTC+12:00
Chatham Islands	213	UTC+12:45
Nuku'alofa	214	UTC+13:00
Samoa	215	UTC+13:00
Cape Verde Islands	218	UTC-01:00
Azores	219	UTC-01:00
Coordinated Universal Time-02	220	UTC-02:00

Time Zone	Time Zone No.	UTC Offset
Araguaina	222	UTC-03:00
Brasilia	223	UTC-03:00
Buenos Aires	224	UTC-03:00
Greenland	225	UTC-03:00
Cayenne, Fortaleza	226	UTC-03:00
Montevideo	227	UTC-03:00
Punta Arenas	228	UTC-03:00
EL Salvador	229	UTC-03:00
Saint Pierre and Miquelon	230	UTC-03:00
Newfoundland	231	UTC-03:00
Atlantic Time (Canada)	232	UTC-04:00
Caracas	233	UTC-04:00
Cuiaba	234	UTC-04:00
Georgetown, La Paz, Manaus, San Juan	235	UTC-04:00
Santiago	236	UTC-04:00
Asuncion	237	UTC-04:00
Bogota, Lima, Quito, Rio Branco	238	UTC-05:00
Havana	239	UTC-05:00
Haiti	240	UTC-05:00
Chetumal	241	UTC-05:00
Turks and Caicos Islands	242	UTC-05:00
Easter Island	243	UTC-06:00
Guadalajara, Mexico City, Monterrey	244	UTC-06:00
Saskatchewan	245	UTC-06:00
Central America	246	UTC-06:00
Chihuahua, La Paz, Mazatlan	247	UTC-07:00
Coordinated Universal Time-08	248	UTC-08:00

Time Zone	Time Zone No.	UTC Offset
Coordinated Universal Time-09	249	UTC-09:00
Marquesas Islands	251	UTC-09:30
Aleutian Islands	252	UTC-10:00
Coordinated Universal Time-11	253	UTC-11:00
International Data Line West	254	UTC-12:00
Volgograd	261	UTC+04:00
Kyzylorda	262	UTC+05:00

A.3 Event Details

Feature	Type	Message Definition
CID Event Information	cidEvent	***JSON_EventNotificationAlert_cidEvent***
Motion Detection	VMD	***XML_EventNotificationAlert_VMD***
IO Alarm	IO	***XML_EventNotificationAlert_IO***
Video Tampering	shelteralarm	***XML_EventNotificationAlert_shelteralarm***
Intrusion	fielddetection	***XML_EventNotificationAlert_fielddetection***
Line Crossing	linedetection	***XML_EventNotificationAlert_linedetection***
Disk Full	diskfull	***XML_EventNotificationAlert_diskfull***
Disk Error	diskerror	***XML_EventNotificationAlert_diskerror***
Disk Recover	diskrecover	***XML_EventNotificationAlert_diskrecover***
Device Online	deviceonline	***JSON_EventNotificationAlert_deviceonline***
Device Offline	deviceoffline	***JSON_EventNotificationAlert_deviceoffline***
Device Deleted (the event is reported regardless of subscription or not)	devicedeleted	***JSON_EventNotificationAlert_devicedeleted***
Device Authorization to ARC (the event is reported regardless of subscription or not)	deviceadded	***JSON_EventNotificationAlert_deviceadded***

Feature	Type	Message Definition
Linkage	Linkage	***JSON_EventNotificationAlert_Linkage***
Video Loss	videoloss	***XML_EventNotificationAlert_videoloss***
Region Entering	regionEntrance	***XML_EventNotificationAlert_regionEntrance***
Region Exiting	regionExiting	***XML_EventNotificationAlert_regionExiting***
Video Exception	recordException	***XML_EventNotificationAlert_recordException***
ACS Event	ACSEvent	***JSON_EventNotificationAlert_ACSEvent***
Intercom Event	voiceTalkEvent	If you need the complete ISAPI protocols, contact technical support or visit tpp.hikvision.com.

A.3.1 JSON_EventNotificationAlert_cidEvent

JSON message about CID event information

Message Field Description

Field Name	Req. or Opt.	Data Type	Description
deviceSerial	Req.	String	Device serial No.
triggerTime	Req.	String	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
eventType	Req.	String	Type of event that triggers alarm, here it should be "cidEvent". The maximum length is 128 bytes.
eventDescription	Req.	String	Event description, here it is "CID event".
isVideo	Opt.	Integer	The file type: 0 (no video file, while picture may exist), 1 (AVI file), 2 (MP4 file).
relationId	Opt.	String	Correlation ID related to video review alarm
CIDEvent	Req.	Object	CID event information.
code	Req.	Integer	CID event code.
standardCode	Opt.	Integer	CID event standard code. It is valid only for CID V3.0 and later.
description	Opt.	String	CID event type.

Field Name	Req. or Opt.	Data Type	Description
system	Opt.	Integer	Partition No. When there are multiple partitions, it indicates the first partition No., for other partitions refer to **partitionNo**.
systemName	Opt.	String	Partition name.
zone	Opt.	Integer	Zone No.
zoneV30	Opt.	Integer	**zoneV30**=**zone**+1.
userNo	Opt.	Integer	User No.
userName	Opt.	String	User name.
ipcChannel	Opt.	Integer	No. of security control panel channel that is linked with the network camera.
channelSerial	Opt.	String	Channel serial No.
zoneName	Opt.	String	Zone name.
partitionNo	Opt.	String	Partition No. that is represented by 32-bit. The right bit indicates the minimum partition No. and the left bit indicates the maximum partition No., and up to 128 partitions can be represented. For example, if the value of **partitionNo** is "43" (binary number: 101011), it indicates the partition No.1, No.2, No.4, and No.6; if he value of **partitionNo** is "21,2", it indicates the partition No.2, No.33, No.35, and No.37 (starts from the highest non-zero bit).
ModNo	Opt.	Integer	The peripheral No.
deviceNo	Opt.	Integer	The device No.
temp	Opt.	Integer	The temperature will be reported when high/low temperatures are detected.
longitude	Opt.	Float	Longitude information.
latitude	Opt.	Float	Latitude information.
evttype	Opt.	String	11 (alarm), 12 (exception), 13 (operation), 31 (alarm restore), 32 (exception restore), 33 (operation over).

Field Name	Req. or Opt.	Data Type	Description
isTalk	Opt.	Integer	Whether in two-way audio mode or not. 1 stands for in two-way audio mode.
media	Opt.	Integer	When the value is 3, it means double video verification.
deviceName	Opt.	String	Device name.
linkedIntercomId	Opt.	String	Sounder ID.
linkedIntercomName	Opt.	String	Sounder name.

Message Example

```
{
  "deviceSerial":"xxx",
  "triggerTime": "2009-11-14T15:27:12",
  "eventType": "",
  "eventDescription": "CID event",
  "CIDEvent": {
    "code": 1103,
    "description":"",
    "system": 1,
    "systemName":"",
    "zone": 1,
    "userNo":1,
    "userName": "test",
    "ipcChannel": 0,
    "channelSerial": "",
    "zoneName": "",
    "partitionNo":"",
    "ModNo”:1,
    "deviceNo”:1,
    "temp”:1,
    "longitude": "",
    "latitude": ""
    "evttype": "11",
    "isTalk": 1,
    "media": 3,
    "deviceName":"aaa",
    "linkedIntercomId":"1",
    "linkedIntercomName":"aaa"
  }
}
```

A.3.2 JSON_EventNotificationAlert_devicedeleted

JSON message about device deleted alarm information

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
deviceSerial	Req.	string	Device serial No.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format with time zone (i.e., "yyyy-MM-ddThh:mm:ssZ"). The maximum length is 32 bytes.
eventType	Req.	string	Type of event that triggers alarm, here it should be "devicedeleted". The maximum length is 128 bytes.
eventDescription	Req.	string	Event description.

Message Example

```
{
  "deviceSerial":"xxx",
  "dateTime": "2009-11-14T15:27:12Z",
  "eventType": "",
  "eventDescription": ""
}
```

A.3.3 JSON_EventNotificationAlert_deviceadded

JSON message about device added alarm information

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
deviceSerial	Req.	string	Device serial No.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format with time zone (i.e., "yyyy-MM-ddThh:mm:ssZ"). The maximum length is 32 bytes.

Field Name	Req. or Opt.	Date Type	Description
eventType	Req.	string	Type of event that triggers alarm, here it should be "deviceadded". The maximum length is 128 bytes.
eventDescription	Req.	string	Event description.
deviceType	Req.	string	Device type.
companyName	Req.	string	Company name.
companyPhone	Req.	string	Company phone number.
companyEmail	Req.	string	Company email.
hcAccount	Opt.	string	Hik-Connect account that the device is handed over to. This field exists only when the device has already been handed over to a Hik-Connect account.

Message Example

```
{
  "deviceSerial": "xxx",
  "deviceType": "xxx",
  "companyName": "xxx",
  "companyPhone": "xxx",
  "companyEmail": "xxx",
  "hcAccount": "xxx",
  "dateTime": "2009-11-14T15:27:12Z",
  "eventType": "",
  "eventDescription": ""
}
```

A.3.4 JSON_EventNotificationAlert_deviceoffline

JSON message about device offline alarm information

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
deviceSerial	Req.	string	Device serial No.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format with time zone (i.e., "yyyy-MM-ddThh:mm:ssZ"). The maximum length is 32 bytes.
eventType	Req.	string	Type of event that triggers alarm, here it should be "deviceoffline". The maximum length is 128 bytes.
eventDescription	Req.	string	Event description.

Message Example

```
{
  "deviceSerial":"xxx",
  "dateTime": "2009-11-14T15:27:12Z",
  "eventType": "",
  "eventDescription": ""
}
```

A.3.5 JSON_EventNotificationAlert_deviceonline

JSON message about device online alarm information

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
deviceSerial	Req.	string	Device serial No.
dateTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format with time zone (i.e., "yyyy-MM-ddThh:mm:ssZ"). The maximum length is 32 bytes.
eventType	Req.	string	Type of event that triggers alarm, here it should be "deviceonline". The maximum length is 128 bytes.
eventDescription	Req.	string	Event description.

Message Example

```
{
  "deviceSerial":"xxx",
  "dateTime": "2009-11-14T15:27:12Z",
  "eventType": "",
  "eventDescription": ""
}
```

A.3.6 JSON_EventNotificationAlert_Linkage

JSON message about video review alarm information

Message Field Description

Field Name	Req. or Opt.	Date Type	Description
deviceSerial	Req.	string	Device serial No.
triggerTime	Req.	string	Alarm triggered time, which is in ISO 8601 time format (i.e., "yyyy-MM-ddThh:mm:ss").
eventType	Req.	string	Type of event that triggers alarm, here it should be "Linkage". The maximum length is 128 bytes.
eventDescription	Req.	string	Event description, here it is "Linkage alarm".
pictureList	Req.	array	Video review data URL
id	Req.	string	Picture ID.
url	Req.	string	URL for downloading picture or video. "isEncrypted=0" means the picture is not encrypted, while "isEncrypted=1" means the picture is encrypted.
media	Opt.	int	Under the condition of double video alarm, media=1 means there is only a right camera, media=2 means there is only a left camera, and media=3 means there are both left and right cameras. If media=3, the id with a smaller value stands for the left

Field Name	Req. or Opt.	Date Type	Description
			camera, while the id with a greater value means it is the right camera.
relationId	Req.	string	Correlation ID related to CID event

Message Example

```
{
  "deviceSerial":"xxx",
  "triggerTime": "2009-11-14T15:27:12",
  "eventType": "Linkage",
  "eventDescription": "",
  "pictureList":[{
    "id": "20220809023446-Q04814335-0-40002-2-1",
    "url":"https://isgp.ezvizlife.com/v3/alarms/pic/get?fileId=20201013030822-
Q03110476-0-40002-2-1&amp;deviceSerialNo=Q03110476&amp;cn=0&amp;isEncrypted=0&amp;isCloudStored=0&a
mp;ct=4&amp;lc=7&amp;bn=4_alialarm-sgp&amp;isDevVideo=0"
    },
    {
    "id": "20220809023446-Q04814335-0-40002-2-2",
    "url":"https://isgp.ezvizlife.com/v3/alarms/pic/get?fileId=20201013030822-
Q03110476-0-40002-2-2&amp;deviceSerialNo=Q03110476&amp;cn=0&amp;isEncrypted=0&amp;isCloudStored=0&a
mp;ct=4&amp;lc=7&amp;bn=4_alialarm-sgp&amp;isDevVideo=0"
    }],
  "media":1,
  "relationId":"5c09bee8-0d44-11eb-b416-4308bd0ace10"
}
```

A.3.7 JSON_EventNotificationAlert_ACSEvent

JSON message about access control events

```
{
  "ipv6Address": "",
/*optional, string, IPv6 address of the alarm device, the maximum length is 128 bytes*/
  "portNo": ,
/*optional, integer32, port No. of the alarm device*/
  "protocol": "",
/*optional, string, protocol type: "HTTP", "HTTPS", the maximum length is 32 bytes*/
  "macAddress": "",
/*optional, string, MAC address, the maximum length is 32 bytes*/
  "channelID": ,
/*optional, integer32, device channel No. that triggered the alarm*/
  "dateTime": "",
/*required, string, time when the alarm is triggered (UTC time), the maximum length is 32 bytes*/
  "activePostCount": ,
/*required, integer32, number of times that the same alarm has been uploaded*/
  "eventType": "",
/*required, string, triggered event type, here it should be "AccessControllerEvent", and the maximum length is 128 bytes*/
  "eventState": "",
/*required, string, event triggering status: "active" (triggered), "inactive" (not triggered), the maximum length is 32 bytes*/
  "eventDescription": "",
/*required, string, event description*/
  "deviceID": "",
/*optional, string, device ID (PUID); this node must be returned when accessing via ISUP (Intelligent Security Uplink Protocol)*/
  "AccessControllerEvent":{
    "deviceName": "",
/*optional, string, device name*/
    "majorEventType": ,
/*required, int, major alarm and event types (the type value should be converted to a decimal number for transmission), see Access Control Event Types for details*/
    "subEventType": ,
/*required, int, minor alarm and event types (the type value should be converted to a decimal number for transmission), see Access Control Event Types for details*/
    "inductiveEventType": "",
/*optional, string, inductive event type. This field is used by storage devices; for access control devices, this field is invalid*/
    "netUser": "",
/*optional, string, user name for network operations*/
    "remoteHostAddr": "",
/*optional, string, remote host address*/
    "cardNo": "",
/*optional, string, card No.*/
    "cardType": ,
/*optional, integer, card types: 1-normal card, 2-disabled card, 3-blocklist card, 4-patrol card, 5-duress card, 6-super card, 7-visitor card, 8-dismiss card*/
    "name": "",
/*optional, string, person name*/
    "whiteListNo": ,
/*optional, integer, allowlist No., which is between 1 and 8*/
    "reportChannel": ,
/*optional, integer, channel type for uploading alarm/event: 1-for uploading arming information, 2-for uploading by central group 1, 3-for uploading by central group 2*/
    "cardReaderKind": ,
/*optional, integer, authentication unit type: 1-IC card reader, 2-ID card reader, 3-QR code scanner, 4-fingerprint module*/
    "cardReaderNo": ,
/*Optional, integer, authentication unit No.*/
    "doorNo": ,
/*optional, integer, door or floor No.*/
    "verifyNo": ,
/*optional, integer, multiple authentication No.*/
    "alarmInNo": ,
/*optional, integer, alarm input No.*/
    "alarmOutNo": ,
/*optional, integer, alarm output No.*/
   "caseSensorNo": ,
/*optional, integer, event trigger No.*/
   "RS485No": ,
/*optional, integer, RS-485 channel No.*/
   "multiCardGroupNo": ,
/*optional, integer, group No.*/
   "accessChannel": ,
/*optional, integer, swing barrier No.*/
   "deviceNo": ,
/*optional, integer, device No.*/
   "distractControlNo": ,
/*optional, integer, distributed controller No.*/
   "employeeNoString": "",
/*optional, integer, employee ID. (person ID)*/
   "localControllerID": ,
/*optional, integer, distributed access controller No.: 0-access controller, 1 to 64-distributed access controller No.1 to
distributed access controller No.64*/
   "InternetAccess": ,
/*optional, integer, network interface No.: 1-upstream network interface No.1, 2-upstream network interface No.2, 3-
downstream network interface No.1*/
   "type": ,
/*optional, integer, zone type: 0-instant alarm zone, 1-24-hour alarm zone, 2-delayed zone, 3-internal zone, 4-key
zone, 5-fire alarm zone, 6-perimeter protection, 7-24-hour silent alarm zone, 8-24-hour auxiliary zone, 9-24-hour
shock alarm zone, 10-emergency door open alarm zone, 11-emergency door closed alarm zone, 255-none*/
   "MACAddr": "",
/*optional, string, physical address*/
   "swipeCardType": ,
/*optional, integer, card swiping types: 0-invalid, 1-QR code*/
   "serialNo": ,
/*optional, integer, event serial No., which is used to judge whether the event loss occurred*/
   "channelControllerID": ,
/*optional, integer, lane controller No.: 1-main lane controller, 2-sub lane controller*/
   "channelControllerLampID": ,
/*optional, integer, light board No. of lane controller, which is between 1 and 255*/
   "channelControllerIRAdaptorID":  ,
/*optional, integer, IR adapter No. of lane controller, which is between 1 and 255*/
   "channelControllerIREmitterID": ,
/*optional, integer, active infrared intrusion detector No. of lane controller, which is between 1 and 255*/
   "userType": "",
/*optional, string, person type: "normal"-normal person (household), "visitor"-visitor, "blacklist"-person in blocklist,
"administrators"-administrator*/
   "currentVerifyMode": "",
/*optional, string, authentication mode: "cardAndPw"-card+password, "card", "cardOrPw"-card or password, "fp"-
fingerprint, "fpAndPw"-fingerprint+password, "fpOrCard"-fingerprint or card, "fpAndCard"-fingerprint+card,
"fpAndCardAndPw"-fingerprint+card+password, "faceOrFpOrCardOrPw"-face or fingerprint or card or password,
"faceAndFp"-face+fingerprint, "faceAndPw"-face+password, "faceAndCard"-face+card, "face", "employeeNoAndPw"-
employee ID.+password, "fpOrPw"-fingerprint or password, "employeeNoAndFp"-employee ID.+fingerprint,
"employeeNoAndFpAndPw"-employee ID.+fingerprint+password, "faceAndFpAndCard"-face+fingerprint+card,
"faceAndPwAndFp"-face+password+fingerprint, "employeeNoAndFace"-employee ID.+face, "faceOrfaceAndCard"-
face or face+card, "fpOrface"-fingerprint or face, "cardOrfaceOrPw"-card or face or password, "cardOrFpOrPw"-card
or fingerprint or password*/
```

```
  "QRCodeInfo":"test",
/*optional, string, QR code information*/
  "thermometryUnit": "",
/*optional, string, temperature unit: "celsius"-Celsius (default), "fahrenheit"-Fahrenheit, "kelvin"-Kelvin*/
  "currTemperature": ,
/*optional, float, face temperature which is accurate to one decimal place*/
  "isAbnomalTemperature": ,
/*optional, boolean, whether the face temperature is abnormal: true-yes, false-no*/
  "RegionCoordinates":{
/*optional, face temperature's coordinates*/
    "positionX": ,
/*optional, int, normalized X-coordinate which is between 0 and 1000*/
    "positionY":
/*optional, int, normalized Y-coordinate which is between 0 and 1000*/
  },
  "picEnable": ,
/*optional, boolean, whether contains picture*/
  "attendanceStatus":"",
/*optional, string, attendance status: "undefined", "checkIn"-check in, "checkOut"-check out, "breakOut"-break out,
"breakIn"-break in, "overtimeIn"-overtime in, "overTimeOut"-overtime out*/
  "statusValue": ,
/*optional, integer, status value*/
  "label":"",
/*optional, string, custom attendance name*/
  "filename":"",
/*optional, string, file name. If multiple pictures are returned at a time, filename of each picture should be unique*/
  "mask": "",
/*optional, string, whether the person is wearing mask: "unknown", "yes"-wearing mask, "no"-not wearing mask*/
  "pictureURL": "",
/*optional, string, picture URL*/
  "helmet": "",
/*optional, string, whether the person is wearing hard hat: "unknown", "yes"-wearing hard hat, "no"-not wearing
hard hat*/
  "visibleLightPicUrl":  "test",
/*optional, string, URL of the visible light picture*/
  "thermalPicUrl":  "test",
/*optional, string, URL of the thermal picture*/
  "appType":  "attendance",
/*optional, string, application type: "attendance" (attendance application), "signIn" (check-in application, which is
only used for information release products)*/
  "HealthInfo": {
/*optional, object, health information*/
    "healthCode":  1,
/*optional, int, health code status: 0 (no request), 1 (no health code), 2 (green QR code), 3 (yellow QR code), 4 (red QR
code), 5 (no such person), 6 (other error, e.g., searching failed due to API exception), 7 (searching for the health code
timed out)*/
    "NADCode":  1,
/*optional, int, nucleic acid test result: 0 (no result), 1 (negative, which means normal), 2 (positive, which means
diagnosed), 3 (the result has expired)*/
    "travelCode":  1,
/*optional, int, trip code: 0 (no trip in the past 14 days), 1 (once left in the past 14 days), 2 (has been to the high-risk
area in the past 14 days), 3 (other)*/
```

```
      "vaccineStatus":  1
/*optional, int, whether the person is vaccinated: 0 (not vaccinated), 1 (vaccinated)*/
    },
    "PhysicalInfo": {
/*optional, object, phisical information*/
    "weight":  7000,
/*optional, integer, weight, actual weight is (kg)*100*/
    "height":  18000
/*optional, integer, height, actual weight is (cm)*100*/
    },
    "meetingID":  "test",
/*required, string, meeting number, range:[1,32]*/
    "PersonInfoExtends": [
/*optional, array, extended person information*/
    {
      "id":  1,
/*optional, integer, extended person ID, range:[1,32]*/
      "value":  "test"
/*optional, string, content of extended person information*/
    }
    ],
    "customPrompt":  "test",
/*optional, string, customized prompt, range:[1,128]*/
    "FaceRect": {
/*optional, object, rectangle for face picture*/
    "height":  1.000,
/*optional, float, height, range:[0.000,1.000]*/
    "width":  1.000,
/*optional, float, width, range:[0.000,1.000]*/
    "x":  0.000,
/*optional, float, horizontal coordinate in the upper-left corner, range:[0.000,1.000]*/
    "y":  0.000
/*optional, float, vertical coordinate in the upper-left corner, range:[0.000,1.000]*/
    }
  },
  "URLCertificationType":  "digest",
/*optional, string, authentication type of picture URL: no (no authentication type), digest (digest authentication)*/
  "deviceSerial": "ABCEDF"
/*required, string, device serial number*/
}
```

A.3.8 JSON_EventNotificationAlert_YsCallingEvent

JSON message about video intercom events.

```
{
"callingId": "20240508124817-K20924932-1-00000", //Calling message ID
"callingTime": 1715201297000, //Calling time, unit: ms
"channel": 1, //Device channel No.
"coverPicture": {
"crypt": 1, //Picture encryption type: 0-not encrypted, 1-user encryption, null-get the value from isEncrypted in the
node "url"
"length": 65536, //Picture size
"lifecycle": 90, //Retention period of cloud pictures: 7 days, 30 days, 0 refers to unknown period
"type": "JPEG" //Picture format: JEPG, etc.
},
"coverUrl": {
"id": "20240508124817-K20924932-1-00000-2-1", //Picture ID
"url": "https://isgp.ezvizlife.com/v3/alarms/pic/get?fileId=20240508124817-
K20924932-1-00000-2-1&deviceSerialNo=K20924932&cn=1&isEncrypted=1&ct=4&lc=90&bn=4_alialarm-sgp" //
Picture UEL
},
"customInfo": "", //Custom information, in JSON format, which is encoded by Base64 for uploading
"devSerial": "K20924932", // Short serial No. of device
"timestamp": "2024-05-08T20:48:17", //Message timestamp, in format of yyyy-MM-DDThh:mm:ss
"eventType":"YsCallingEvent "//Event type
}
```

A.3.9 JSON_EventNotificationAlert_manualRep

JSON message about manual capture events.

```
{
"dateTime": "2024-08-14T11:03:06", //yyyy-MM-ddTHH:mm:ss
"deviceSerial": "Q19323594",//Device serial No.
"customType": "zoneNo=0=zoneV30=1=hostAlarmType=10",
"eventDescription": "manualRep",//Event description
"eventType": "manualRep",//Event type
"customInfo":"zoneNo=0|zoneV30=1|zoneName=Zonav?aradio1|user=lyh_uat7_0403@yopmail.com|evttype=13|
UID=501", //Custom information
"pictureList": [
{
"id":"E1$7$11$0$P5LH4HP$N1$Q30344009-0$00$09685446",//Picture ID
"url": "https://ieu.ezvizlife.com/v3/alarms/pic/get?fileId=20240814090326-
Q19323594-0-12062-2-1&deviceSerialNo=Q19323594&cn=0&isEncrypted=0&isCloudStored=0&ct=101&lc=7&bn=101
_hpc-eu-prod-pircam-media&isDevVideo=0"// Picture URL
}
],
"channelID": "0",//Video channel No.
"deviceNo": "1" /*ro, opt, integer, device No., range:[1,1000], desc: After installation, the installer collates the
peripheral and sensor information corresponding to the device No. and imports the information table to the ARC.
After receiving it, the ARC can sort out the device type according to the device No. and corresponding information
}
```

A.3.10 XML_EventNotificationAlert_diskerror

XML message about disk error alarm information

```
<?xml version="1.0" encoding="utf-8"?>
<EventNotificationAlert version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
```

```
  <deviceSerial><!--required, xs:string, device serial No.--></deviceSerial>
  <dateTime>
    <!--required, xs:datetime, alarm triggered time, which is in ISO 8601 time format with time zone, i.e., yyyy-MM-
ddTHH:mm:ssZ-->
  </dateTime>
  <eventType><!--required, xs:string, event type, here it is "diskerror"--></eventType>
  <eventDescription><!--required, xs:string, event description--></eventDescription>
  <diskNo><!--optional, xs:integer, disk No.--></diskNo>
  <HDDList><!--optional-->
    <HDD>
      <id><!--required, xs:integer, HDD No., which starts from 1--></id>
      <diskNumber><!--required, xs:integer, number of HDDs--></diskNumber>
    </HDD>
  </HDDList>
</EventNotificationAlert>
```

A.3.11 XML_EventNotificationAlert_diskfull

XML message about disk full alarm information

```
<?xml version="1.0" encoding="utf-8"?>
<EventNotificationAlert version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <deviceSerial><!--required, xs:string, device serial No.--></deviceSerial>
  <dateTime>
    <!--required, xs:datetime, alarm triggered time, which is in ISO 8601 time format with time zone, i.e., yyyy-MM-
ddTHH:mm:ssZ-->
  </dateTime>
  <eventType><!--required, xs:string, event type, here it is "diskfull"--></eventType>
  <eventDescription><!--required, xs:string, event description--></eventDescription>
  <diskNo><!--optional, xs:integer, disk No.--></diskNo>
  <HDDList><!--optional-->
    <HDD>
      <id><!--required, xs:integer, HDD No., which starts from 1--></id>
      <diskNumber><!--required, xs:integer, number of HDDs--></diskNumber>
    </HDD>
  </HDDList>
</EventNotificationAlert>
```

A.3.12 XML_EventNotificationAlert_diskrecover

XML message about disk recovered alarm information

```
<?xml version="1.0" encoding="utf-8"?>
<EventNotificationAlert version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <deviceSerial><!--required, xs:string, device serial No.--></deviceSerial>
  <dateTime>
    <!--required, xs:datetime, alarm triggered time, which is in ISO 8601 time format with time zone, i.e., yyyy-MM-
ddTHH:mm:ssZ-->
  </dateTime>
  <eventType><!--required, xs:string, event type, here it is "diskrecover"--></eventType>
  <eventDescription><!--required, xs:string, event description--></eventDescription>
  <diskNo><!--optional, xs:integer, disk No.--></diskNo>
  <HDDList><!--optional-->
    <HDD>
      <id><!--required, xs:integer, HDD No., which starts from 1--></id>
      <diskNumber><!--required, xs:integer, number of HDDs--></diskNumber>
    </HDD>
  </HDDList>
</EventNotificationAlert>
```

A.3.13 XML_EventNotificationAlert_fielddetection

XML message about intrusion alarm information

```
<?xml version="1.0" encoding="utf-8"?>
<EventNotificationAlert version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <deviceSerial><!--required, xs:string, device serial No.--></deviceSerial>
  <channelID><!--dependent, xs:string, channel No.--></channelID>
  <triggerTime><!--required, xs:datetime, alarm triggered time, format: yyyy-MM-ddTHH:mm:ss--></triggerTime>
  <eventType><!--required, xs:string, event type, here it is "fielddetection"--></eventType>
  <eventDescription><!--required, xs:string, event description--></eventDescription>
  <DetectionRegionList><!--optional-->
    <DetectionRegionEntry><!--list-->
      <regionID><!--required, xs:string, detection region ID--></regionID>
      <sensitivityLevel><!--optional, xs:integer, sensitivity level, which is from 0 to 100--></sensitivityLevel>
      <RegionCoordinatesList><!--optional, list of target region coordinates-->
        <RegionCoordinates><!--optional-->
          <positionX><!--required, xs:integer, x-coordinate--></positionX>
          <positionY><!--required, xs:integer, y-coordinate--></positionY>
        </RegionCoordinates>
      </RegionCoordinatesList>
      <detectionTarget><!--optional, xs:string, target type: "human", "vehicle", "others"--></detectionTarget>
      <TargetRect><!--optional-->
    <X><!--required, xs:float, x-coordinate of target frame, value range: [0,1]--></X>
    <Y><!--required, xs:float, y-coordinate of target frame, value range: [0,1]--></Y>
    <width><!--required, xs:float, width of target frame, value range: [0,1]--></width>
    <height><!--required, xs:float, height of target frame, value range: [0,1]--></height>
      </TargetRect>
    </DetectionRegionEntry>
  </DetectionRegionList>
  <channelName><!--optional, xs:string, channel name--></channelName>
</EventNotificationAlert>
```

A.3.14 XML_EventNotificationAlert_IO

XML message about alarm input alarm information

```
<?xml version="1.0" encoding="utf-8"?>
<EventNotificationAlert version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <deviceSerial><!--required, xs:string, device serial No.--></deviceSerial>
  <channelID><!--dependent, xs:string, channel No.--></channelID>
  <triggerTime><!--required, xs:datetime, alarm triggered time, format: yyyy-MM-ddTHH:mm:ss--></triggerTime>
  <eventType><!--required, xs:string, event type, here it is "IO"--></eventType>
  <eventDescription><!--required, xs:string, event description--></eventDescription>
  <inputIOPortID><!--optional, xs:integer, local alarm input ID--></inputIOPortID>
  <dynInputIOPortID><!--optional, xs:integer, dynamic alarm input ID--></dynInputIOPortID>
  <channelName><!--optional, xs:string, channel name--></channelName>
</EventNotificationAlert>
```

A.3.15 XML_EventNotificationAlert_linedetection

XML message about line crossing alarm information

```
<?xml version="1.0" encoding="utf-8"?>
<EventNotificationAlert version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <deviceSerial><!--required, xs:string, device serial No.--></deviceSerial>
  <channelID><!--dependent, xs:string, channel No.--></channelID>
  <triggerTime><!--required, xs:datetime, alarm triggered time, format: yyyy-MM-ddTHH:mm:ss--></triggerTime>
  <eventType><!--required, xs:string, event type, here it is "linedetection"--></eventType>
  <eventDescription><!--required, xs:string, event description--></eventDescription>
  <DetectionRegionList><!--optional-->
    <DetectionRegionEntry><!--list-->
      <regionID><!--required, xs:string, detection region ID--></regionID>
      <sensitivityLevel><!--optional, xs:integer, sensitivity level, which is from 0 to 100--></sensitivityLevel>
      <RegionCoordinatesList><!--optional, list of target region coordinates-->
        <RegionCoordinates><!--optional-->
          <positionX><!--required, xs:integer, x-coordinate--></positionX>
          <positionY><!--required, xs:integer, y-coordinate--></positionY>
        </RegionCoordinates>
      </RegionCoordinatesList>
      <detectionTarget><!--optional, xs:string, target type: "human", "vehicle", "others"--></detectionTarget>
      <TargetRect><!--optional-->
    <X><!--required, xs:float, x-coordinate of target frame, value range: [0,1]--></X>
    <Y><!--required, xs:float, y-coordinate of target frame, value range: [0,1]--></Y>
    <width><!--required, xs:float, width of target frame, value range: [0,1]--></width>
    <height><!--required, xs:float, height of target frame, value range: [0,1]--></height>
      </TargetRect>
    </DetectionRegionEntry>
  </DetectionRegionList>
  <channelName><!--optional, xs:string, channel name--></channelName>
</EventNotificationAlert>
```

A.3.16 XML_EventNotificationAlert_recordException

XML message about video file exception information

```
<?xml version="1.0" encoding="utf-8"?>
<EventNotificationAlert version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <deviceSerial><!--required, xs:string, device serial No.--></deviceSerial>
  <channelID><!--dependent, xs:string, channel No.--></channelID>
  <triggerTime><!--required, xs:datetime, alarm triggered time, format: yyyy-MM-ddTHH:mm:ss--></triggerTime>
  <eventType><!--required, xs:string, event type, here it is "recordException"--></eventType>
  <eventDescription><!--required, xs:string, event description--></eventDescription>
  <channelName><!--optional, xs:string, channel name--></channelName>
</EventNotificationAlert>
```

A.3.17 XML_EventNotificationAlert_regionExiting

XML message about region exiting alarm information

```
<?xml version="1.0" encoding="utf-8"?>
<EventNotificationAlert version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <deviceSerial><!--required, xs:string, device serial No.--></deviceSerial>
  <channelID><!--dependent,xs:string channel number--></channelID>
  <dateTime><!--optional, xs:datetime, event occurred time, which is in IOS 8601 format, e.g.,
2017-04-22T15:39:01+08:00--></dateTime>
  <triggerTime><!--required, xs:datetime, alarm triggered time, format: yyyy-MM-ddTHH:mm:ss--></triggerTime>
  <activePostCount><!--optional, xs:integer, event occurred times--></activePostCount>
  <eventType><!--required, xs:string, event types, here it should be set to "regionExiting"--></eventType>
  <eventState><!--optional, xs:string, event status (for persistent event): "active", "inactive"--></eventState>
  <eventDescription><!--required, xs:string, event description--></eventDescription>
  <DetectionRegionList><!--optional-->
    <DetectionRegionEntry><!--list-->
      <regionID><!--required, xs:string, detection region ID--></regionID>
      <sensitivityLevel><!--optional, xs:integer, sensitivity level, which is between 0 and 100--></sensitivityLevel>
      <RegionCoordinatesList><!--optional, target region-->
        <RegionCoordinates><!--optional-->
          <positionX><!--required, xs:integer, X-coordinate--></positionX>
          <positionY><!--required, xs:integer, Y-coordinate--></positionY>
        </RegionCoordinates>
      </RegionCoordinatesList>
    </DetectionRegionEntry>
  </DetectionRegionList>
  <channelName><!--optional, xs:string, channel name--></channelName>
</EventNotificationAlert>
```

A.3.18 XML_EventNotificationAlert_regionEntrance

XML message about region entrance alarm information

```
<?xml version="1.0" encoding="utf-8"?>
<EventNotificationAlert version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <deviceSerial><!--required, xs:string, device serial No.--></deviceSerial>
  <channelID><!--dependent,xs:string channel number--></channelID>
  <dateTime><!--optional, xs:datetime, event occurred time, which is in IOS 8601 format, e.g.,
2017-04-22T15:39:01+08:00--></dateTime>
  <triggerTime><!--required, xs:datetime, alarm triggered time, format: yyyy-MM-ddTHH:mm:ss--></triggerTime>
  <activePostCount><!--optional, xs:integer, event occurred times--></activePostCount>
  <eventType><!--required, xs:string, event types, here it should be set to "regionEntrance"--></eventType>
  <eventState><!--optioanl, xs:string, event status (for persistent event): "active, inactive"--></eventState>
  <eventDescription><!--required, xs:string, event description--></eventDescription>
  <DetectionRegionList><!--optional-->
    <DetectionRegionEntry><!--list-->
      <regionID><!--required, xs:string, detection region ID--></regionID>
      <sensitivityLevel><!--optional, xs:integer, sensitivity level, which is between 0 and 100--></sensitivityLevel>
      <RegionCoordinatesList><!--optional, target region-->
        <RegionCoordinates><!--optional-->
          <positionX><!--required, xs:integer, x-coordinate--></positionX>
          <positionY><!--required, xs:integer, y-coordinate--></positionY>
        </RegionCoordinates>
      </RegionCoordinatesList>
    </DetectionRegionEntry>
  </DetectionRegionList>
  <channelName><!--optional, xs:string, channel name--></channelName>
</EventNotificationAlert>
```

A.3.19 XML_EventNotificationAlert_shelteralarm

XML message about video tampering alarm information

```
<?xml version="1.0" encoding="utf-8"?>
<EventNotificationAlert version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <deviceSerial><!--required, xs:string, device serial No.--></deviceSerial>
  <channelID><!--dependent, xs:string, channel No.--></channelID>
  <triggerTime><!--required, xs:datetime, alarm triggered time, format: yyyy-MM-ddTHH:mm:ss--></triggerTime>
  <eventType><!--required, xs:string, event type, here it is "shelteralarm"--></eventType>
  <eventDescription><!--required, xs:string, event description--></eventDescription>
  <channelName><!--optional, xs:string, channel name--></channelName>
</EventNotificationAlert>
```

A.3.20 XML_EventNotificationAlert_videoloss

XML message about video loss alarm information

```
<?xml version="1.0" encoding="utf-8"?>
<EventNotificationAlert version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <deviceSerial><!--required, xs:string, device serial No.--></deviceSerial>
  <channelID><!--dependent, xs:string, channel No.--></channelID>
  <triggerTime><!--required, xs:datetime, alarm triggered time, format: yyyy-MM-ddTHH:mm:ss--></triggerTime>
  <eventType><!--required, xs:string, event type, here it is "videoloss"--></eventType>
  <eventDescription><!--required, xs:string, event description--></eventDescription>
  <channelName><!--optional, xs:string, channel name--></channelName>
</EventNotificationAlert>
```

A.3.21 XML_EventNotificationAlert_VMD

XML message about motion detection alarm information

```
<?xml version="1.0" encoding="utf-8"?>
<EventNotificationAlert version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <deviceSerial><!--required, xs:string, device serial No.--></deviceSerial>
  <channelID><!--dependent, xs:string, channel No.--></channelID>
  <triggerTime><!--required, xs:datetime, alarm triggered time, format: yyyy-MM-ddTHH:mm:ss--></triggerTime>
  <eventType><!--required, xs:string, event type, here it is "VMD"--></eventType>
  <eventDescription><!--required, xs:string, event description--></eventDescription>
  <channelName><!--optional, xs:string, channel name--></channelName>
</EventNotificationAlert>
```

A.4 Request URIs

Description	URI	Method	Request and Response Message
Get device information.	/ISAPI/System/deviceInfo	GET	XML_DeviceInfo XML_ResponseStatus
Edit device information.	/ISAPI/System/deviceInfo	PUT	-
Control PTZ.	/ISAPI/PTZCtrl/channels/<ID>/continuous	PUT	XML_ResponseStatus
Get preset list.	/ISAPI/PTZCtrl/channels/<ID>/presets	GET	XML_PTZPresetList XML_ResponseStatus
Manage all configured presets.	/ISAPI/PTZCtrl/channels/<ID>/presets	POST	-
Delete all presets.	/ISAPI/PTZCtrl/channels/<ID>/presets	DELETE	-
Add a preset.	/ISAPI/PTZCtrl/channels/<ID>/presets/<ID>	PUT	XML_ResponseStatus
Delete a preset.	/ISAPI/PTZCtrl/channels/<ID>/presets/<ID>	DELETE	XML_ResponseStatus

Description	URI	Method	Request and Response Message
Get a preset.	/ISAPI/PTZCtrl/channels/<ID>/presets/<ID>	GET	-
Call a preset.	/ISAPI/PTZCtrl/channels/<ID>/presets/<ID>/goto	PUT	XML_ResponseStatus
Get partition status.	/ISAPI/SecurityCP/status/subSystems?format=json	GET	JSON_SubSysList JSON_ResponseStatus
Arm a partition.	/ISAPI/SecurityCP/control/arm/<ID>?ways=<string>&format=json	PUT	JSON_ResponseStatus
Disarm a partition.	/ISAPI/SecurityCP/control/disarm/<ID>?format=json	PUT	JSON_ResponseStatus
Clear partition alarms.	/ISAPI/SecurityCP/control/clearAlarm/<ID>?format=json	PUT	JSON_ResponseStatus
Get zone status	/ISAPI/SecurityCP/status/zones?format=json	GET	JSON_ZoneList JSON_ResponseStatus
Search partition status according to conditions.	/ISAPI/SecurityCP/status/zones?format=json	POST	-
Zone bypass.	/ISAPI/SecurityCP/control/bypass?format=json	PUT	JSON_ResponseStatus
Recover bypass of multiple zones.	/ISAPI/SecurityCP/control/bypassRecover?format=json	PUT	JSON_ResponseStatus
Get relay status by specific conditions.	/ISAPI/SecurityCP/status/outputStatus?format=json	POST	JSON_OutputSearch JSON_ResponseStatus
Control relay in batch.	/ISAPI/SecurityCP/control/outputs?format=json	POST	JSON_ResponseStatus
Get the information of all I/O output ports.	/ISAPI/System/IO/outputs	GET	XML_IOOutputPortList XML_ResponseStatus
Get status of a specific alarm output.	/ISAPI/System/IO/outputs/<ID>/status	GET	XML_IOPortStatus XML_ResponseStatus

Description	URI	Method	Request and Response Message
Manually trigger a specific alarm output.	/ISAPI/System/IO/outputs/<ID>/trigger	PUT	XML_ResponseStatus
Get device time zone.	/ISAPI/System/time	GET	XML_TimeData XML_ResponseStatus
Get or set device time parameters.	/ISAPI/System/time	PUT	-
Operations about management of all digital channels.	/ISAPI/ContentMgmt/InputProxy/channels	GET	XML_InputProxyChannelList XML_ResponseStatus
Configure operations about management of all digital channels.	/ISAPI/ContentMgmt/InputProxy/channels	PUT	-
Create digital channels	/ISAPI/ContentMgmt/InputProxy/channels	POST	-
Get status of all digital channels.	/ISAPI/ContentMgmt/InputProxy/channels/status	GET	XML_InputProxyChannelStatusList XML_ResponseStatus
Refresh the video mode manually before playback.	/ISAPI/ContentMgmt/record/control/manualRefresh/channels/<ID>	PUT	XML_ResponseStatus
Search for access control events.	/ISAPI/AccessControl/AcsEvent?format=json	POST	JSON_AcsEvent XML_ResponseStatus
Search for person information.	/ISAPI/AccessControl/UserInfo/Search?format=json	POST	JSON_UserInfoSearch XML_ResponseStatus

A.4.1 /ISAPI/AccessControl/AcsEvent?format=json

Search for access control events.

Request URI Definition

Table A-1 POST /ISAPI/AccessControl/AcsEvent?format=json

Method	POST
Description	Search for access control events.
Query	**format**: determine the format of request or response message.
Request	***JSON_AcsEventCond***
Response	Succeeded: ***JSON_AcsEvent*** Failed: ***JSON_ResponseStatus***

Remarks

- The recommended timeout of this URI is 10 seconds.
- If the response message contains picture data, the picture data will be returned by boundary method; otherwise, the response message in JSON format will be returned directly.

Example

Sample Response Message with Picture Data

```
--MIME_boundary
Content-Type: application/json
Content-Length:480

{
 "AcsEvent":{
  "searchID":"",
  "responseStatusStrg":"OK",
  "numOfMatches":1,
  "totalMatches":1,
  "InfoList":[{
   "major":1,
   "minor":1,
   "time":"2016-12-12T17:30:08+08:00",
   "netUser":"",
   "remoteHostAddr":"",
   "cardNo":"",
   "cardType":1,
   "whiteListNo":1,
   "reportChannel":1,
   "cardReaderKind":1,
   "cardReaderNo":1,
   "doorNo":1,
   "verifyNo":1,
   "alarmInNo":1,
   "alarmOutNo":1,
   "caseSensorNo":1,
   "RS485No":1,
   "multiCardGroupNo":1,
   "accessChannel":1,
   "deviceNo":1,
   "distractControlNo":1,
   "employeeNoString":"",
   "localControllerID":1,
   "InternetAccess":1,
   "type":1,
   "MACAddr":"",
   "swipeCardType":1,
   "serialNo":1,
   "channelControllerID":1,
   "channelControllerLampID":1,
   "channelControllerIRAdaptorID":1,
   "channelControllerIREmitterID":1,
   "userType":"normal",
   "currentVerifyMode":"",
   "attendanceStatus":"",
   "statusValue":1,
   "pictureURL":"",
   "picturesNumber":1,
   "filename":"picture1"
  }]
 }
}
--MIME_boundary
Content-Disposition: form-data; filename="picture1"; //Picture data
Content-Type:image/jpeg
Content-Length:12345

fgagasghshgshdasdad…
--MIME_boundary--
```

A.4.2 /ISAPI/AccessControl/UserInfo/Search?format=json

Search for person information.

Request URI Definition

Table A-2 POST /ISAPI/AccessControl/UserInfo/Search?format=json

Method	POST
Description	Search for person information.
Query	**format**: determine the format of request or response message. **terminalNo**: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after

	information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	***JSON_UserInfoSearchCond***
Response	***JSON_UserInfoSearch***

Remarks

The **Request** (user information search condition ***JSON_UserInfoSearchCond***) depends on the user information capability JSON_Cap_UserInfo (related node: <**UserInfoSearchCond**>).

A.4.3 /ISAPI/ContentMgmt/InputProxy/channels

Operations about management of all digital channels.

Request URI Definition

Table A-3 GET /ISAPI/ContentMgmt/InputProxy/channels

Method	GET
Description	Get parameters of all digital channels.
Query	None.
Request	None.
Response	***XML_InputProxyChannelList***

Table A-4 PUT /ISAPI/ContentMgmt/InputProxy/channels

Method	PUT
Description	Set parameters of all digital channels.
Query	None.
Request	***XML_InputProxyChannelList***
Response	***XML_ResponseStatus***

Table A-5 POST /ISAPI/ContentMgmt/InputProxy/channels

Method	POST
Description	Add a digital channel.
Query	None.

Request	***XML_InputProxyChannel***
Response	***XML_ResponseStatus***

A.4.4 /ISAPI/ContentMgmt/InputProxy/channels/status

Get status of all digital channels.

Request URI Definition

Table A-6 GET /ISAPI/ContentMgmt/InputProxy/channels/status

Method	GET
Description	Get status of all digital channels.
Query	None.
Request	None.
Response	***XML_InputProxyChannelStatusList***

A.4.5 /ISAPI/ContentMgmt/record/control/manualRefresh/channels/<ID>

Refresh the video mode manually before playback.

Request URI Definition

Table A-7 PUT /ISAPI/ContentMgmt/record/control/manualRefresh/channels/<ID>

Method	PUT
Description	Refresh the video mode manually before playback.
Query	None.
Request	None.
Response	***XML_ResponseStatus***

Remarks

The <**ID**> in the request URI refers to the channel No.

A.4.6 /ISAPI/PTZCtrl/channels/<ID>/continuous

Control PTZ to pan and tilt.

Request URL Definition

Table A-8 PUT /ISAPI/PTZCtrl/channels/<ID>/continuous

Method	PUT
Description	Control PTZ to pan and tilt.
Query	None.
Request	***XML_Absolute_PTZData***
Response	***XML_ResponseStatus***

Remarks

The <**ID**> in the URL refers to the channel ID.

A.4.7 /ISAPI/PTZCtrl/channels/<ID>/presets

Operations about all presets' configurations.

Request URI Definition

Table A-9 GET /ISAPI/PTZCtrl/channels/<ID>/presets

Method	GET
Description	Get all presets' parameters.
Query	None.
Request	None.
Response	Succeeded: ***XML_PTZPresetList*** Failed: ***XML_ResponseStatus***

Table A-10 POST /ISAPI/PTZCtrl/channels/<ID>/presets

Method	POST
Description	Add a preset.
Query	None.

Request	***XML_Set_PTZPreset***
Response	***XML_ResponseStatus***

Table A-11 DELETE /ISAPI/PTZCtrl/channels/<ID>/presets

Method	DELETE
Description	Delete all presets.
Query	None.
Request	None.
Response	***XML_ResponseStatus***

Remarks

The <**ID**> in the URI is the camera ID.

A.4.8 /ISAPI/PTZCtrl/channels/<ID>/presets/<ID>

Get or set the a preset's parameters, or delete a preset.

Request URI Definition

Table A-12 GET /ISAPI/PTZCtrl/channels/<ID>/presets/<ID>

Method	GET
Description	Get a preset's parameters.
Query	None.
Request	None.
Response	Succeeded: ***XML_PTZPreset*** Failed: ***XML_ResponseStatus***

Table A-13 PUT /ISAPI/PTZCtrl/channels/<ID>/presets/<ID>

Method	PUT
Description	Set a preset's parameters.
Query	None.
Request	***XML_Set_PTZPreset***
Response	***XML_ResponseStatus***

Table A-14 DELETE /ISAPI/PTZCtrl/channels/<ID>/presets/<ID>

Method	DELETE
Description	Delete a preset.
Query	None.
Request	None.
Response	***XML_ResponseStatus***

A.4.9 /ISAPI/PTZCtrl/channels/<ID>/presets/<ID>/goto

Call a preset.

Request URI Definition

Table A-15 PUT /ISAPI/PTZCtrl/channels/<ID>/presets/<ID>/goto

Method	PUT
Description	Call a preset.
Query Parameter	None.
Request	None.
Response	***XML_ResponseStatus***

Remarks

The first <**ID**> in the request URL refers to the channel ID, and the second <**ID**> refers to the preset ID.

A.4.10 /ISAPI/SecurityCP/control/arm/<ID>?ways=<string>&format=json

Arm the partition.

Request URI Definition

Table A-16 PUT /ISAPI/SecurityCP/control/arm/<ID>?ways=<string>&format=json

Method	PUT
Description	Arm the partition.
Query	**format**: determine the format of request or response message.

	ways: the arming types, including "stay"-stay arming, and "away"-away arming, e.g., ways=stay or ways=away.
Request	***JSON_Operate***
Response	***JSON_ResponseStatus***

Remarks

- The <**ID**> in the request URI refers to the partition No., which starts from 1, and 0xffffffff refers to all partitions.
- If **armProcess** is returned in the response message, it indicates that the device supports arming, and the arming process will be executed.

A.4.11 /ISAPI/SecurityCP/control/bypass?format=json

Perform bypass on multiple zones.

Request URI Definition

Table A-17 PUT /ISAPI/SecurityCP/control/bypass?format=json

Method	PUT
Description	Perform bypass on multiple zones.
Query	**format**: determine the format of request or response message.
Request	***JSON_List_ID***
Response	***JSON_ResponseStatus***

A.4.12 /ISAPI/SecurityCP/control/bypassRecover?format=json

Recover bypass of multiple zones.

Request URI Definition

Table A-18 PUT /ISAPI/SecurityCP/control/bypassRecover?format=json

Method	PUT
Description	Recover bypass of multiple zones.
Query	**format**: determine the format of request or response message.

Request	***JSON_List_ID***
Response	***JSON_ResponseStatus***

A.4.13 /ISAPI/SecurityCP/control/clearAlarm/<ID>?format=json

Clear alarms for a partition.

Request URI Definition

Table A-19 PUT /ISAPI/SecurityCP/control/clearAlarm/<ID>?format=json

Method	PUT
Description	Clear alarms for a partition.
Query	**format**: determine the format of request or response message.
Request	***JSON_Operate***
Response	***JSON_ResponseStatus***

Remarks

The <**ID**> in the request URI refers to the partition No., which starts from 1, and 0xffffffff indicates all partitions.

A.4.14 /ISAPI/SecurityCP/control/disarm/<ID>?format=json

Disarm the partition.

Request URI Definition

Table A-20 PUT /ISAPI/SecurityCP/control/disarm/<ID>?format=json

Method	PUT
Description	Disarm the partition.
Query	**format**: determine the format of request or response message.
Request	***JSON_Operate***
Response	***JSON_ResponseStatus***

Remarks

The <ID> in the request URI refers to partition No., which starts from 1, and 0xffffffff indicates all partitions.

A.4.15 /ISAPI/SecurityCP/control/outputs?format=json

Control relay in batch.

Request URI Definition

Table A-21 POST /ISAPI/SecurityCP/control/outputs?format=json

Method	POST
Description	Control relay in batch.
Query	**format**: determine the format of request or response message.
Request	***JSON_OutputsCtrl***
Response	***JSON_ResponseStatus***

A.4.16 /ISAPI/SecurityCP/status/subSystems?format=json

Get the status of all partitions.

Request URI Definition

Table A-22 GET /ISAPI/SecurityCP/status/subSystems?format=json

Method	GET
Description	Get the status of all partitions.
Query	**format**: determine the format of request or response message.
Request	None.
Response	Succeeded: ***JSON_SubSysList*** Failed: ***JSON_ResponseStatus***

A.4.17 /ISAPI/SecurityCP/status/outputStatus?format=json

Get the relay status by specific conditions.

Request URI Definition

Table A-23 POST /ISAPI/SecurityCP/status/outputStatus?format=json

Method	POST
Description	Get the relay status by specific conditions.
Query	**format**: determine the format of request or response message.
Request	***JSON_OutputCond***
Response	Succeeded: ***JSON_OutputSearch_Status*** Failed: ***JSON_ResponseStatus***

A.4.18 /ISAPI/SecurityCP/status/zones?format=json

Get the zone status.

Request URI Definition

Table A-24 GET /ISAPI/SecurityCP/status/zones?format=json

Method	GET
Description	Get the status of all zones.
Query	**format**: determine the format of request or response message.
Request	None.
Response	Succeeded: ***JSON_ZoneList*** Failed: ***JSON_ResponseStatus***

Table A-25 POST /ISAPI/SecurityCP/status/zones?format=json

Method	POST
Description	Get the zone status by specific conditions.
Query	**format**: determine the format of request or response message.
Request	***JSON_ZoneCond***
Response	Succeeded: ***JSON_ZoneSearch*** Failed: ***JSON_ResponseStatus***

A.4.19 /ISAPI/System/deviceInfo

Operations about the device information.

Request URI Definition

Table A-26 GET /ISAPI/System/deviceInfo

Method	GET
Description	Get the device information.
Query	None
Request	None.
Response	Succeeded: ***XML_DeviceInfo*** Failed: ***XML_ResponseStatus***

Table A-27 PUT /ISAPI/System/deviceInfo

Method	PUT
Description	Set the device information.
Query	None
Request	***XML_DeviceInfo***
Response	***XML_ResponseStatus***

A.4.20 /ISAPI/System/IO/outputs

Get the information of all I/O output ports.

Request URI Definition

Table A-28 GET /ISAPI/System/IO/outputs

Method	GET
Description	Get the information of all I/O output ports.
Query	None.
Request	None.
Response	***XML_IOOutputPortList***

A.4.21 /ISAPI/System/IO/outputs/<ID>/status

Get status of a specific alarm output.

Request URI Definition

Table A-29 GET /ISAPI/System/IO/outputs/<ID>/status

Method	GET
Description	Get status of a specific alarm output.
Query	None.
Request	None.
Response	Succeeded: ***XML_IOPortStatus*** Failed: ***XML_ResponseStatus***

Remarks

The <**ID**> in the request URI refers to the alarm output ID.

A.4.22 /ISAPI/System/IO/outputs/<ID>/trigger

Manually trigger a specific alarm output.

Request URI Definition

Table A-30 PUT /ISAPI/System/IO/outputs/<ID>/trigger

Method	PUT
Description	Manually trigger a specific alarm output.
Query	none.
Request	***XML_IOPortData***
Response	***XML_ResponseStatus***

Remarks

The <**ID**> in the request URI refers to the alarm output ID.

A.4.23 /ISAPI/System/time

Get or set device time parameters.

Request URI Definition

Table A-31 GET /ISAPI/System/time

Method	GET
Description	Get device time parameters.
Query	None
Request	None
Response	Succeeded: ***XML_Time*** Failed: ***XML_ResponseStatus***

Table A-32 PUT /ISAPI/System/time

Method	PUT
Description	Set device time parameters.
Query	None
Request	***XML_Time***
Response	Succeeded: ***XML_ResponseStatus_IFSTime*** Failed: ***XML_ResponseStatus***

A.5 Request and Response Messages

A.5.1 JSON_AcsEvent

AcsEvent message in JSON format

```
{
  "AcsEvent":{
    "searchID": "",
/*required, string type, search ID, which 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": "",
/*required, string, search status: "OK"-searching completed, "MORE"-searching for more results, "NO MATCH"-no matched results*/
    "numOfMatches": ,
/*required, integer, number of returned results*/
    "totalMatches": ,
/*required, integer, total number of matched results*/
    "InfoList": [{
```

```
/*optional, event details*/
    "major": ,
/*required, integer, major alarm/event types (the type value should be transformed to the decimal number), see
Access Control Event Types for details*/
    "minor": ,
/*required, integer, minor alarm/event types (the type value should be transformed to the decimal number), see
Access Control Event Types for details*/
    "time": "",
/*required, string, time (UTC time), e.g., "2016-12-12T17:30:08+08:00"*/
    "netUser": "",
/*optional, string, user name*/
    "remoteHostAddr": "",
/*optional, string, remote host address*/
    "cardNo": "",
/*optional, string, card No.*/
    "cardType": ,
/*optional, integer, card types: 1-normal card, 2-disabled card, 3-blocklist card, 4-patrol card, 5-duress card, 6-super
card, 7-visitor card, 8-dismiss card*/
    "name": "",
/*optional, string, person name*/
    "whiteListNo": ,
/*optional, integer, allowlist No., which is between 1 and 8*/
    "reportChannel": ,
/*optional, integer, channel type for uploading alarm/event: 1-for uploading arming information, 2-for uploading by
central group 1, 3-for uploading by central group 2*/
    "cardReaderKind": ,
/*optional, integer, authentication unit type: 1-IC card reader, 2-ID card reader, 3-QR code scanner, 4-fingerprint
module*/
    "cardReaderNo": ,
/*Optional, integer, authentication unit No.*/
    "doorNo": ,
/*optional, integer, door or floor No.*/
    "verifyNo": ,
/*optional, integer, multiple authentication No.*/
    "alarmInNo": ,
/*optional, integer, alarm input No.*/
    "alarmOutNo": ,
/*optional, integer, alarm output No.*/
    "caseSensorNo": ,
/*optional, integer, event trigger No.*/
    "RS485No": ,
/*optional, integer, RS-485 channel No.*/
    "multiCardGroupNo": ,
/*optional, integer, group No.*/
    "accessChannel": ,
/*optional, integer, swing barrier No.*/
    "deviceNo": ,
/*optional, integer, device No.*/
    "distractControlNo": ,
/*optional, integer, distributed controller No.*/
    "employeeNoString": "",
/*optional, integer, employee ID. (person ID)*/
```

```
    "localControllerID": ,
/*optional, integer, distributed access controller No.: 0-access controller, 1 to 64-distributed access controller No.1 to distributed access controller No.64*/
    "InternetAccess": ,
/*optional, integer, network interface No.: 1-upstream network interface No.1, 2-upstream network interface No.2, 3-downstream network interface No.1*/
    "type": ,
/*optional, integer, zone type: 0-instant alarm zone, 1-24-hour alarm zone, 2-delayed zone, 3-internal zone, 4-key zone, 5-fire alarm zone, 6-perimeter protection, 7-24-hour silent alarm zone, 8-24-hour auxiliary zone, 9-24-hour shock alarm zone, 10-emergency door open alarm zone, 11-emergency door closed alarm zone, 255-none*/
    "MACAddr": "",
/*optional, string, physical address*/
    "swipeCardType": ,
/*optional, integer, card swiping types: 0-invalid, 1-QR code*/
    "serialNo": ,
/*optional, integer, event serial No., which is used to judge whether the event loss occurred*/
    "channelControllerID": ,
/*optional, integer, lane controller No.: 1-main lane controller, 2-sub lane controller*/
    "channelControllerLampID": ,
/*optional, integer, light board No. of lane controller, which is between 1 and 255*/
    "channelControllerIRAdaptorID":  ,
/*optional, integer, IR adapter No. of lane controller, which is between 1 and 255*/
    "channelControllerIREmitterID": ,
/*optional, integer, active infrared intrusion detector No. of lane controller, which is between 1 and 255*/
    "userType": "",
/*optional, string, person type: "normal"-normal person (household), "visitor"-visitor, "blacklist"-person in blocklist, "administrators"-administrator*/
    "currentVerifyMode": "",
/*optional, string, authentication mode: "cardAndPw"-card+password, "card", "cardOrPw"-card or password, "fp"-fingerprint, "fpAndPw"-fingerprint+password, "fpOrCard"-fingerprint or card, "fpAndCard"-fingerprint+card, "fpAndCardAndPw"-fingerprint+card+password, "faceOrFpOrCardOrPw"-face or fingerprint or card or password, "faceAndFp"-face+fingerprint, "faceAndPw"-face+password, "faceAndCard"-face+card, "face", "employeeNoAndPw"-employee ID.+password, "fpOrPw"-fingerprint or password, "employeeNoAndFp"-employee ID.+fingerprint, "employeeNoAndFpAndPw"-employee ID.+fingerprint+password, "faceAndFpAndCard"-face+fingerprint+card, "faceAndPwAndFp"-face+password+fingerprint, "employeeNoAndFace"-employee ID.+face, "faceOrfaceAndCard"-face or face+card, "fpOrface"-fingerprint or face, "cardOrfaceOrPw"-card or face or password, "cardOrFpOrPw"-card or fingerprint or password*/
    "QRCodeInfo":"test",
/*optional, string, QR code information*/
    "thermometryUnit": "",
/*optional, string, temperature unit: "celsius"-Celsius (default), "fahrenheit"-Fahrenheit, "kelvin"-Kelvin*/
    "currTemperature": ,
/*optional, float, face temperature which is accurate to one decimal place*/
    "isAbnomalTemperature": ,
/*optional, boolean, whether the face temperature is abnormal: true-yes, false-no*/
    "RegionCoordinates":{
/*optional, face temperature's coordinates*/
      "positionX": ,
/*optional, int, normalized X-coordinate which is between 0 and 1000*/
      "positionY":
/*optional, int, normalized Y-coordinate which is between 0 and 1000*/
    },
     "mask": "",
/*optional, string, whether the person is wearing mask: "unknown", "yes"-wearing mask, "no"-not wearing mask*/
     "pictureURL": "",
/*optional, string, picture URL*/
     "filename":"",
/*optional, string, file name. If multiple pictures are returned at a time, filename of each picture should be unique*/
     "attendanceStatus":"",
/*optional, string, attendance status: "undefined", "checkIn"-check in, "checkOut"-check out, "breakOut"-break out,
"breakIn"-break in, "overtimeIn"-overtime in, "overTimeOut"-overtime out*/
     "label":"",
/*optional, string, custom attendance name*/
     "statusValue": ,
/*optional, integer, status value*/
     "helmet": "",
/*optional, string, whether the person is wearing hard hat: "unknown", "yes"-wearing hard hat, "no"-not wearing
hard hat*/
     "visibleLightPicUrl":  "test",
/*optional, string, URL of the visible light picture*/
     "thermalPicUrl":  "test",
/*optional, string, URL of the thermal picture*/
     "appType":  "attendance",
/*optional, string, application type: "attendance" (attendance application), "signIn" (check-in application, which is
only used for information release products)*/
     "HealthInfo": {
/*optional, object, health information*/
       "healthCode":  1,
/*optional, int, health code status: 0 (no request), 1 (no health code), 2 (green QR code), 3 (yellow QR code), 4 (red QR
code), 5 (no such person), 6 (other error, e.g., searching failed due to API exception), 7 (searching for the health code
timed out)*/
       "NADCode":  1,
/*optional, int, nucleic acid test result: 0 (no result), 1 (negative, which means normal), 2 (positive, which means
diagnosed), 3 (the result has expired)*/
       "travelCode":  1,
/*optional, int, trip code: 0 (no trip in the past 14 days), 1 (once left in the past 14 days), 2 (has been to the high-risk
area in the past 14 days), 3 (other)*/
       "vaccineStatus":  1
/*optional, int, whether the person is vaccinated: 0 (not vaccinated), 1 (vaccinated)*/
     },
     "meetingID":  "test",
/*required, string, meeting number, range:[1,32]*/
     "PersonInfoExtends": [
/*optional, array, extended person information*/
     {
       "id":  1,
/*optional, integer, extended person ID, range:[1,32]*/
       "value":  "test"
/*optional, string, content of extended person information*/
     }],
     "name":  "test",
/*optional, string, name*/
     "FaceRect": {
/*optional, object, rectangle for face picture*/
```

```
      "height":  1.000,
/*optional, float, height, range:[0.000,1.000]*/
      "width":  1.000,
/*optional, float, width, range:[0.000,1.000]*/
      "x":  0.000,
/*optional, float, horizontal coordinate in the upper-left corner, range:[0.000,1.000]*/
      "y":  0.000
/*optional, float, vertical coordinate in the upper-left corner, range:[0.000,1.000]*/
    }
   }],
  }
}
```

A.5.2 JSON_AcsEventCond

AcsEventCond message in JSON format

```
{
  "AcsEventCond": {
    "searchID": "",
/*required, string type, search ID, which 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": ,
/*required, integer, the start position of the search result in the result list. When there are multiple records and you
cannot get all search results at a time, you can search for the records after the specified position next time*/
    "maxResults": ,
/*required, integer, maximum number of search results. If maxResults exceeds the range returned by the device
capability, the device will return the maximum number of search results according to the device capability and will not
return error message*/
    "major": ,
/*required, integer, major alarm/event types (the type value should be transformed to the decimal number), see
Access Control Alarm Types for details*/
    "minor": ,
/*required, integer, minor alarm/event types (the type value should be transformed to the decimal number), see
Access Control Alarm Types for details*/
    "startTime": "",
/*optional, string, start time (UTC time), e.g., 2016-12-12T17:30:08+08:00*/
    "endTime": "",
/*optional, string, end time (UTC time), e.g.,2017-12-12T17:30:08+08:00*/
    "cardNo": "",
/*optional, string, card No.*/
    "name": "",
/*optional, string，  cardholder name*/
    "picEnable": ,
/*optional, boolean, whether to contain pictures: "false"-no, "true"-yes*/
    "beginSerialNo": ,
/*optional, integer, start serial No.*/
    "endSerialNo": ,
/*optional, integer, end serial No.*/
    "employeeNoString":"",
/*optional, string, employee ID. (person ID)*/
    "eventAttribute":"",
/*optional, string, event attribute: "attendance"-valid authentication, "other"*/
    "employeeNo":"",
/*optional, string, employee ID. (person ID)*/
    "timeReverseOrder": ,
/*optional, boolean, whether to return events in descending order of time (later events will be returned first): true-yes, false or this node is not returned-no*/
    "isAbnomalTemperature":true
/*optional, boolean, whether the skin-surface temperature is abnormal*/
    "temperatureSearchCond":  "all"
/*optional, string, temperature search conditions, all (events with temperature information), normal (events with normal temperature), abnormal (events with abnormal temperature), if it exists with isAbnormalTemperature, then the latter will be invalid.*/
  }
}
```

A.5.3 JSON_List_ID

JSON message about zone ID list

```
{
  "List":[{
    "id":
/*int, zone No., which starts from 0; it is required when performing bypass or bypass recovered on multiple zones; it is not required when performing bypass or bypass recovered on a zone*/
  }]
}
```

A.5.4 JSON_OutputCond

JSON message about conditions of getting relay status

```
{
  "OutputCond":{
    "searchID":"",
/*required, string, search ID, which 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": ,
/*required, integer32, the start position of the search result in the result list. When there are multiple records and you cannot get all search results at a time, you can search for the records after the specified position next time*/
    "maxResults": ,
/*required, integer32, maximum number of search results this time by calling this URI. If maxResults exceeds the range returned by the device capability, the device will return the maximum number of search results according to the device capability and will not return error message*/
    "outputModuleNo": ,
/*optional, int, linked output module No.*/
    "moduleType":""
/*optional, string, module type: "localWired"-local wired module, "extendWired"-extended wired module,
"localWireless"-local wireless module, "extendWireless"-extended wireless module*/
  }
}
```

A.5.5 JSON_OutputsCtrl

JSON message about relay control parameters

```
{
  "OutputsCtrl":{
    "switch":""
/*required, string, "open"-enable relay, "close"-disable relay*/
    "List":[{
/*it is required when control multiple relays, and it is not required when control only one relay*/
      "id":
/*int, relay No., which starts from 0*/
    }]
  }
}
```

A.5.6 JSON_OutputSearch_Status

JSON message about results of getting relay status

```
{
  "OutputSearch":{
    "searchID":"",
/*required, string, search ID, which 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":"",
/*required, string, search status: "OK"-searching completed, "NO MATCH"-no matched results, "MORE"-searching for
more results*/
    "numOfMatches": ,
/*required, integer32, number of results returned this time*/
    "totalMatches": ,
/*required, integer32, total number of matched results*/
    "OutputList":[{
/*optional, relay list*/
      "Output":{
        "id": ,
/*required, int, relay No.*/
        "name":"",
/*optional, string, relay name*/
        "status":"",
/*optional, string, relay status: "notRelated"-not linked, "on", "off", "offline", "heartbeatAbnormal"-heartbeat
exception*/
        "tamperEvident": ,
/*optional, boolean, zone tampering status: true (tampered), false (not tampered)*/
      "charge":"",
/*optional, string, state of charge: "normal", "lowPower"-low battery*/
      "linkage":"",
/*optional, string, event type linked to the relay: "alarm", "arming", "disarming", "manualCtrl"-manually control*/
      "signal": ,
/*optional, int, signal strength, it is between 0 and 255*/
      "temperature":  1,
/*optional, int, temperature*/
      "devIndex":  "test",
/*optional, string, device ID, the maximum length is 64 bytes*/
      "devName":  "test",
/*optional, string, device name, the maximum length is 64 bytes*/
      "durationConstOutputEnable":  true,
/*optional, boolean, whether to always keep the relay open*/
      "isAvailable":  true,
/*optional, boolean, whether the relay is enabled, if this node is not returned, it indicates that the relay is enabled by
default*/
      "accessModuleType":  "transmitter",
/*optional, enum, access module type: "transmitter", "localTransmitter", "multiTransmitter", "localRelay", "keypad"*/
      "relatedAccessModuleID":  1,
/*optional, int, linked access module ID*/
      "address":  254,
/*optional, int, wired (extended) module address, this node works with accessModuleType*/
      "subSystemList": [1, 2, 3],
/*optional, array, list of linked partitions*/
      "scenarioType": ["alarm"],
/*optional, array, scenario type*/
      "relayAttrib":  "wired",
/*optional, string, relay attribute: "wired", "wireless" (default)*/
      "deviceNo":  1
/*optional, int, device ID, range:[1,1000]*/
     }
   }]
  }
}
```

A.5.7 JSON_Operate

JSON message about operation parameters

```
{
 "Operate": {
/*optional, object, operation parameters*/
   "moduleOperateCode":  "12345"
/*optional, string, module operation code, which should be encrypted*/
  }
}
```

A.5.8 JSON_ResponseStatus

JSON message about response status

```
{
  "requestURL":"",
/*optional, string, request URL*/
  "statusCode": ,
/*optional, int, status code*/
  "statusString":"",
/*optional, string, status description*/
  "subStatusCode":"",
/*optional, string, sub status code*/
  "errorCode": ,
/*required, int, error code, which corresponds to subStatusCode, this field is required when statusCode is not 1. The
returned value is the transformed decimal number*/
  "errorMsg":"",
/*required, string, error details, this field is required when statusCode is not 1*/
  "MErrCode": "0xFFFFFFFF",
/*optional, string, error code categorized by functional modules*/
  "MErrDevSelfEx": "0xFFFFFFFF"
/*optional, string, extension of MErrCode. It is used to define the custom error code, which is categorized by
functional modules*/
}
```

A.5.9 JSON_SubSysList

JSON message about partition information list

```
{
  "SubSysList":[{
/*required, partition list*/
    "SubSys":{
/*optional, partition, it can be set to NULL if partitions are not needed*/
      "id": ,
/*required, int, partition No., which starts from 1*/
      "armType":"",
/*required, string, partition arming type: "stay"-stay arming, "away"-away arming. This node is only valid for arming
partitions in a batch*/
      "arming":"",
/*optional, string, partition arming/disarming status, "stay"-stay arming, "away"-away arming, "disarm"-disarmed,
"arming"*/
      "alarm": ,
/*optional, boolean, whether the partition alarm is triggered: true, false*/
      "preventFaultArm": ,
/*optional, boolean, whether to prevent fault arming: true, false*/
      "enabled": ,
/*optional, boolean, whether to enable the partition*/
      "name":"",
/*optional, string, partition name*/
     "moduleOperateCode":  "12345",
/*optional, string, module operation code, which should be encrypted*/
     "delayTime":  1
/*optional, int, maximum remaining delay time of the delay zones in the current partition, unit:s; this node is valid
when the value of the node arming is "stay" or "away"*/
   }
  }]
}
```

A.5.10 JSON_UserInfoSearch

UserInfoSearch message in JSON format

```
{
  "UserInfoSearch":{
    "searchID":"",
/*required, string type, search ID, which 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":"",
/*required, string, search status: "OK"-searching completed, "NO MATCH"-no matched results, "MORE"-searching for
more results*/
    "numOfMatches": ,
/*required, integer32, number of returned results this time*/
    "totalMatches": ,
/*required, integer32, total number of matched results*/
    "UserInfo":[{
/*optional, person information*/
      "employeeNo":"",
/*required, string, employee ID. (person ID)*/
      "name":"",
/*optional, string, person name*/
      "userType":"",
/*required, string, person type: "normal"-normal person (household), "visitor", "blackList"-person in blocklist*/
      "closeDelayEnabled": ,
/*optional, boolean, whether to enable door close delay: "true"-yes, "false"-no*/
      "Valid":{
/*required, parameters of the effective period*/
        "enable":"",
/*required, boolean, whether to enable the effective period: "false"-disable, "true"-enable. If this node is set to
"false", the effective period is permanent*/
        "beginTime":"",
/*required, start time of the effective period (if timeType does not exist or is "local", the beginTime is the device local
time, e.g., 2017-08-01T17:30:08; if timeType is "UTC", the beginTime is UTC time, e.g., 2017-08-01T17:30:08+08:00)*/
        "endTime":"",
/*required, end time of the effective period (if timeType does not exist or is "local", the endTime is the device local
time, e.g., 2017-08-01T17:30:08; if timeType is "UTC", the endTime is UTC time, e.g., 2017-08-01T17:30:08+08:00)*/
        "timeType":""
/*optional, string, time type: "local"- device local time, "UTC"- UTC time*/
      },
    "belongGroup":"",
/*optional, string, group*/
    "password":"",
/*optional, string, password*/
    "doorRight":"",
/*optional, string, No. of door or lock that has access permission, e.g., "1,3" indicates having permission to access
door (lock) No. 1 and No. 3*/
    "RightPlan":[{
/*optional, access permission schedule of the door or lock*/
      "doorNo": ,
/*optional, integer, door No. (lock ID)*/
      "planTemplateNo":""
/*optional, string, schedule template No.*/
    }],
    "maxOpenDoorTime": ,
/*optional, integer, the maximum authentication attempts, 0-unlimited*/
    "openDoorTime": ,
/*optional, integer, read-only, authenticated attempts*/
    "roomNumber": ,
/*optional, integer, room No.*/
    "floorNumber": ,
/*optional, integer, floor No.*/
    "doubleLockRight": ,
/*optional, boolean, whether to have the permission to open the double-locked door: "true"-yes, "false"-no*/
    "localUIRight": ,
/*optional, boolean, whether to have the permission to access the device local UI: "true"-yes, "false"-no*/
    "localUIUserType":"",
/*optional, string, user type of device local UI: "admin" (administrator), "operator", "viewer" (normal user). This node
is used to distinguish different users with different operation permissions of device local UI*/
    "userVerifyMode":"",
/*optional, string, person authentication mode: "cardAndPw"-card+password, "card"-card, "cardOrPw"-card or
password, "fp"-fingerprint, "fpAndPw"-fingerprint+password, "fpOrCard"-fingerprint or card, "fpAndCard"-fingerprint
+card, "fpAndCardAndPw"-fingerprint+card+password, "faceOrFpOrCardOrPw"-face or fingerprint or card or
password, "faceAndFp"-face+fingerprint, "faceAndPw"-face+password, "faceAndCard"-face+card, "face"-face,
"employeeNoAndPw"-employee ID.+password, "fpOrPw"-fingerprint or password, "employeeNoAndFp"-employee ID.
+fingerprint, "employeeNoAndFpAndPw"-employee ID.+fingerprint+password, "faceAndFpAndCard"-face+fingerprint
+card, "faceAndPwAndFp"-face+password+fingerprint, "employeeNoAndFace"-employee ID.+face,
"faceOrfaceAndCard"-face or face+card, "fpOrface"-fingerprint or face, "cardOrfaceOrPw"-card or face or password,
"cardOrFace"-card or face, "cardOrFaceOrFp"-card or face or fingerprint, "cardOrFpOrPw"-card or fingerprint or
password. The priority of the person authentication mode is higher than that of the card reader authentication
mode*/
    "dynamicCode": "123456",
/*optional, string, dynamic permission code, this node is write-only*/
    "callNumbers": ["","",""],
/*optional, array of string, list of called numbers, the default rule is "X-X-X-X", e.g., "1-1-1-401". This node is the
extension of the node roomNumber. When the number list is supported, you need to use this node to configure
parameters*/
    "floorNumbers": [1,2],
/*optional, array of int, floor No. list. This node is the extension of floorNumber. When the number list is supported,
you need to use this node to configure parameters*/
    "numOfFace":0,
/*optional, int, number of linked face pictures. This node is read-only and if it is not returned, it indicates that this
```

```
function is not supported*/
    "numOfFP":0,
/*optional, int, number of linked fingerprints. This node is read-only and if it is not returned, it indicates that this
function is not supported*/
    "numOfCard":0,
/*optional, int, number of linked cards. This node is read-only and if it is not returned, it indicates that this function is
not supported*/
    "gender":"",
/*optional, string, gender of the person in the face picture: "male", "female", "unknown"*/
    "PersonInfoExtends":[{
/*optional, array of object, extended fields for the additional person information. This node is used to configure the
extended person information displayed on the device's UI. For MinMoe series facial recognition terminals, currently
only one value node can be supported for displaying the employee ID. and the node id is not supported*/
      "id":1,
/*optional, int, extended ID of the additional person information, value range: [1,32]. It corresponds to the id in the
message of the request URI /ISAPI/AccessControl/personInfoExtendName?format=json and is used to link the value of
the node value and its name (the node name in the message of the request URI /ISAPI/AccessControl/
personInfoExtendName?format=json). If the node id does not exist, the ID will start from 1 by default according to the
array order*/
      "value":""
/*optional, string, extended content of the additional person information*/
    }],
    "groupName":  "test",
/*optional, string. group name, range:[1,64]*/
    "age":  0,
/*optional, integer, age, range:[0,120]*/
    "PatientInfos": {
/*optional, object, patient infomation*/
        "deviceID":  "test",
/*optional, string, device number*/
        "admissionTime":  "1970-01-01T00:00:00+08:00",
/*optional, datetime, hospitalized date*/
        "chargeNurse":  "test",
/*optional, string, nurse in charge, range:[0,32]*/
        "chargeDoctor":  "test",
/*optional, string, doctor in charge, range:[0,32]*/
        "nursingLevel":  "tertiary",
/*optional, enumerate, nursing level*/
        "doctorsAdvice":  "test",
/*optional, string, advice from doctor, range:[0,128]*/
        "allergicHistory ":  "test"
/*optional, string, allergy, range:[0,128]*/
    },
    "TromboneRule": {
/*optional, object, trombone rule*/
        "industryType":  "builidings",
/*optional, string, industry type*/
        "unitType":  "indoor",
/*optional, string, device type, indoor (idoor station), villa (villa outdoor station), confirm (double confirm), outdoor
(outdoor station), fence (outer door station), doorbell (doorbell), manage (master station), acs (access control device),
wardStation (ward extension), bedheadExtension (bedhead extension), bedsideExtension (bedside extension),
terminal (terminal), netAudio (network audio), interactive (interactive terminal), amplifier (amplifier)*/
```

```
        "SIPVersion":  "V10"
/*optional, string, private SIP version, range:[0,32]*/
      },
      "ESDType":  "handAndFoot"
/*optional, enumerate, ESD detection type: handAndFoot (detect both hand and foot), no (no detection), hand (detect hand), foot (detect foot)*/
    }]
  }
}
```

A.5.11 JSON_UserInfoSearchCond

UserInfoSearchCond message in JSON format

```
{
  "UserInfoSearchCond":{
    "searchID":"",
/*required, string type, search ID, which 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": ,
/*required, integer32 type, the start position of the search result in the result list. When there are multiple records and you cannot get all search results at a time, you can search for the records after the specified position next time*/
    "maxResults": ,
/*required, integer32 type, maximum number of search results. If maxResults exceeds the range returned by the device capability, the device will return the maximum number of search results according to the device capability and will not return error message*/
    "EmployeeNoList":[{
/*optional, person ID list (if this node does not exist or is empty, it indicates searching for all person information)*/
      "employeeNo":""
/*optional, string type, employee No. (person ID)*/
    }],
    "fuzzySearch":"",
/*optional, string, key words for fuzzy search*/
    "userType":  "normal",
/*optional, string, normal （normal user), visitor (visitor), blockList (person in blocklist), patient (patient), maintenance (maintenance people)*/
    "deviceIDList": [1, 2]
/*optional, array, device ID list*/
  }
}
```

A.5.12 JSON_ZoneCond

ZoneCond message in JSON format

```
{
  "ZoneCond":{
    "searchID":"",
/*required, string type, search ID, which 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": ,
/*required, integer32 type, the start position of the search result in the result list. When there are multiple records and you cannot get all search results at a time, you can search for the records after the specified position next time*/
    "maxResults":
/*required, integer32 type, maximum number of search results that can be obtained this time by calling the URI. If maxResults exceeds the range returned by the device capability, the device will return the maximum number of search results according to the device capability and will not return error message*/
  }
}
```

A.5.13 JSON_ZoneList

JSON message about zone status list

```
{
  "ZoneList":[{
    "Zone":{
      "id": ,
/*required, int, zone ID*/
      "name":"",
/*optional, string, zone name*/
      "status":"",
/*optional, string, zone status, "notRelated"-no zone linked, "online"-online, "offline"-offline, "trigger"-triggered, "breakDown"-fault, "heartbeatAbnormal"-heartbeat exception*/
      "reason":  "short",
/*optional, string, default reason: "short", "break"*/
      "tamperEvident": ,
/*optional, boolean, zone tampering alarm status, true-triggered, false-not triggered*/
      "shielded": ,
/*optional, boolean, zone disabling status, true-disabled, false-not disabled*/
      "bypassed": ,
/*optional, boolean, whether to bypass the zone, true-bypassed, false-bypass recovered*/
      "armed": ,
/*required, boolean, whether to arm the zone, true-armed, false-disarmed*/
      "isArming": ,
/*optional, boolean, whether the zone is armed, this node can only be set to "true"*/
      "alarm": ,
/*optional, boolean, whether the zone alarm is triggered, true-triggered, false-not triggered*/
      "charge": "",
/*optional, string, zone battery status, "normal", "lowPower"-low battery*/
      "chargeValue": ,
/*optional, int, battery power value which is between 0 and 100*/
      "signal": ,
/*optional, int, signal strength, which ranges from 0 to 255*/
      "temperature": ,
/*optional, read-only, int, temperature*/
      "detectorType":"",
/*optional, string, type of the detector linked to the zone, see details about the supported detector types in
JSON_ZoneCap*/
     "model": "",
/*optional, string, model*/
     "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*/
     "humidity":  20,
/*optional, int, read-only, humidity, the value is between 10% and 90%*/
     "healthStatus":  "normal",
/*optional, string, read-only, health status: "normal", "fault"*/
     "antiMaskingEnabled":  true,
/*optional, boolean, read-only, whether to enable anti-masking: true-enable，  false-disable*/
     "mountingType":  "wall",
/*optional, string, read-only, mounting type: "wall", "ceiling"*/
     "magnetOpenStatus":  true,
/*optional, boolean, whether the magnetic contact is open: true (open), false (closed)*/
     "version":  "test",
/*optional, string, detector version No., the maximum length is 32 bytes*/
     "pirCamConnected":  true,
/*optional, boolean, whether the outdoor triple signal detector and PIR camera are connected: true (yes), false (no)*/
     "accessModuleType":  "transmitter",
/*optional, enum, access module type: "transmitter", "localTransmitter", "multiTransmitter", "localZone", "keypad"*/
     "relatedAccessModuleID":  1,
/*optional, int, linked access module ID*/
     "address":  254,
/*optional, int, wired (extended) module address, this node works with accessModuleType*/
     "zoneAttrib":  "wired",
/*optional, enum, zone attribute: "wired", "wireless" (default)*/
     "voltage":  1,
/*optional, int, voltage of the zone*/
     "signalStrength":  1,
/*optional, int, signal strength, range:[-128,127]*/
     "mainCharge":  "normal",
/*optional, enum, main (adapter) power status: "normal", "lowPower". Main power and zone power refers to the zone's adapter power status and the zone's battery status respectively*/
     "preheatStatus":  "processing",
/*optional, enum, pre-heat status: "processing", "success"*/
     "userfulLifeStatus":  "expire",
/*optional, enum, expiry status: "expire", "normal"*/
     "mazeStatus":  "abnormal",
/*optional, enum, maze status: "abnormal", "normal"*/
     "sensorStatus":  "abnormal",
/*optional, enum, sensor status: "abnormal", "normal"*/
     "deviceNo":  1
/*optional, int, device No., range:[1,1000]*/
   }
  }]
}
```

A.5.14 JSON_ZoneSearch

JSON message about the result of zone status

```
{
  "ZoneSearch":{
    "searchID":"",
/*required, string type, search ID, which 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":"",
/*required, string type, search status: "OK"-searching completed, "NO MATCH"-no matched results, "MORE"-searching for more results*/
    "numOfMatches": ,
/*required, integer32, number of returned results this time*/
    "totalMatches": ,
/*required, integer32, total number of matched results*/
    "ZoneList":[{
      "Zone":{
        "id": ,
/*required, integer type, zone No.*/
        "name":"",
/*optional, string type, zone name*/
        "status":"",
/*optional, string type, zone status: "notRelated"-not linked, "online", "offline", "trigger", "breakDown"-fault, "heartbeatAbnormal"-heartbeat exception*/
        "tamperEvident": ,
/*optional, boolean type, zone tampering status: "true"-tampered, "false"-not tampered*/
        "shielded": ,
/*optional, boolean type, zone shielding status: "true"-shielded, "false"-not shielded*/
        "bypassed": ,
/*optional, boolean type, whether the zone is bypassed: "true"-yes, "false"-no*/
        "armed": ,
/*required, boolean type, whether the zone is armed: "true"-yes, "false"-no*/
        "isArming": ,
/*optional, boolean type, whether the zone is armed, this node can only be set to "true"*/
        "alarm": ,
/*optional, boolean type, whether the alarm is triggered in the zone: "true-yes, "false"-no*/
        "charge":"",
/*optional, string type, state of charge of the zone: "normal", "lowPower"-low battery*/
        "signal": ,
/*optional, integer type, signal strength, it is between 0 and 255*/
        "subSystemNo ": ,
/*optional, integer type, partition No.*/
        "zoneAttrib":"",
/*optional, string, zone attribute: "wired", "wireless". If this node is not returned, the default zone attribute is "wireless"*/
        "RelatedChanList":[{
/*optional, list of linked channel No.*/
          "RelatedChan":{
            "relator":"",
/*required, string type, device linked to the channel when the alarm is triggered*/
          "cameraSeq":"",
/*optional, string type, camera serial No.*/
          "relatedChan":
/*optional, integer type, linked channel No.*/
        }
       }],
       "detectorType":  "test",
/*optional, string, type of the detector linked to the zone*/
       "model":  "DS-PM1-O8-WE",
/*optional, enum, model, subType:string, "DS-PM1-O8-WE", "DS-PM1-O2-WE"*/
       "zoneType":  "Instant",
/*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*/
       "InputList": [
/*optional, array, list of input status*/
        {
         "id":  1,
/*required, int, input ID*/
         "enabled":  true,
/*required, boolean, whether it is enabled*/
         "mode":  "NO"
/*optional, enum, input type: "rolling shutter", "NC" (always closed), "NO" (always open)*/
        }
       ],
       "humidity":  10,
/*optional, int, humidity, the value is between 10% and 90%*/
       "healthStatus":  "normal",
/*optional, string, read-only, health status: "normal", "fault"*/
       "antiMaskingEnabled":  true,
/*optional, boolean, read-only, whether to enable anti-masking: true-enable，  false-disable*/
       "mountingType":  "wall",
/*optional, string, read-only, mounting type: "wall", "ceiling"*/
       "magnetOpenStatus":  true,
/*optional, boolean, whether the magnetic contact is open: true (open), false (closed)*/
       "devIndex":  "test",
/*optional, string, device ID, the maximum length is 64 bytes*/
       "devName":  "test",
/*optional, string, device name, the maximum length is 64 bytes*/
       "isAvailable":  true,
/*optional, boolean, whether the partition is available: true (default), false*/
       "isBypassedAvailable":  true,
/*optional, boolean, whether bypass is configurable: true (yes), false (no). By default, it is configurable*/
       "version":  "test",
/*optional, string, detector version No., the maximum length is 32 bytes*/
       "pirCamConnected":  true,
/*optional, boolean, whether the outdoor triple signal detector and PIR camera are connected: true (yes), false (no)*/
       "accessModuleType":  "transmitter",
/*optional, enum, access module type: "transmitter", "localTransmitter", "multiTransmitter", "localZone", "keypad"*/
       "relatedAccessModuleID":  1,
/*optional, int, linked access module ID*/
```

```
        "address":  254,
/*optional, int, wired (extended) module address, this node works with accessModuleType*/
        "deviceNo":  1
/*optional, int, device ID, range:[1,1000]*/
      }
    }]
  }
}
```

A.5.15 XML_Absolute_PTZData

XML message about PTZ control parameters

```
<?xml version="1.0" encoding="UTF-8"?>

<PTZData xmlns="http://www.isapi.org/ver20/XMLSchema" version="2.0">
  <!--req, object, PTZ value-->
  <pan>
    <!--opt, int,  panning positive direction, range: [-100,100]-->60
  </pan>
  <tilt>
    <!--opt, int, tilting positive direction, range:[-100,100]-->60
  </tilt>
  <zoom>
    <!--opt, int, zooming value, range:[-100,100]-->60
  </zoom>
  <angularVelocity>
    <!--opt, object, angular velocity-->
    <enabled>
      <!--req, bool, whether to enable it-->true
    </enabled>
    <value>
      <!--opt, int, angular velocity value, range:[1,360], unit: rad/s-->1
    </value>
  </angularVelocity>
</PTZData>
```

A.5.16 XML_DeviceInfo

XML message about device information

```
<?xml version="1.0" encoding="utf-8"?>
  <DeviceInfo version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <deviceName><!--required, xs:string--></deviceName>
  <deviceID><!--required, read-only, xs:string, uuid--></deviceID>
  <deviceDescription>
    <!--optional, xs:string, description about the device defined in RFC1213. For network camera, this node is set to
"IPCamera"; for network speed dome, this node is set to "IPDome"; for DVR or DVS, this node is set to "DVR" or
"DVS"-->
```

```
  </deviceDescription>
  <deviceLocation><!--optional, xs:string, actual location of the device--></deviceLocation>
  <deviceStatus><!--optional, read-only, xs:string, device status: "normal", "abnormal"--></deviceStatus>
  <DetailAbnormalStatus>
    <!--dependent, error status details, it is valid only when deviceStatus is "abnormal"-->
    <hardDiskFull>
      <!--optional, read-only, xs: boolean, whether the error of "HDD full" occurred: "true"-yes,"false"-no-->
    </hardDiskFull>
    <hardDiskError>
      <!--optional, read-only, xs:boolean, whether the error of "HDD error" occurred: "true"-yes,"false"-no-->
    </hardDiskError>
    <ethernetBroken>
      <!--optional, read-only, xs: boolean, whether the error of "network disconnected" occurred: "true"-yes,"false"-no-->
    </ethernetBroken>
    <ipaddrConflict>
      <!--optional, read-only, xs: boolean, whether the error of "IP address conflicted" occurred: "true"-yes,"false"-no-->
    </ipaddrConflict>
    <illegalAccess>
      <!--optional, read-only, xs: boolean, whether the error of "illegal login" occurred: "true"-yes,"false"-no-->
    </illegalAccess>
    <recordError>
      <!--optional, read-only, xs: boolean, whether the error of "recording exception" occurred: "true"-yes,"false"-no-->
    </recordError>
    <raidLogicDiskError>
      <!--optional, read-only, xs: boolean, whether the error of "RAID exception" occurred: "true"-yes,"false"-no-->
    </raidLogicDiskError>
    <spareWorkDeviceError>
      <!--optional, read-only, xs: boolean, whether the error of "working device exception" occurred: "true"-yes,"false"-no-->
    </spareWorkDeviceError>
  </DetailAbnormalStatus>
  <systemContact><!--optional, xs:string, contact information of the device--></systemContact>
  <model><!--required, read-only, xs:string--></model>
  <serialNumber><!--required, read-only, xs:string--></serialNumber>
  <macAddress><!--required, read-only, xs:string--></macAddress>
  <firmwareVersion><!--required, read-only, xs:string--></firmwareVersion>
  <firmwareReleasedDate><!--optional, read-only, xs:string--></firmwareReleasedDate>
  <bootVersion><!--optional, read-only, xs:string--></bootVersion>
  <bootReleasedDate><!--optional, read-only, xs:string--></bootReleasedDate>
  <hardwareVersion><!--optional, read-only, xs:string--></hardwareVersion>
  <encoderVersion><!--optional, read-only, xs:string--></encoderVersion>
  <encoderReleasedDate><!--optional, read-only, xs:stirng--></encoderReleasedDate>
  <decoderVersion><!--optional, read-only, xs:string--></decoderVersion>
  <decoderReleasedDate><!--optional, read-only, xs:stirng--></decoderReleasedDate>
  <softwareVersion><!--optional, read-only, xs:string, software version--></softwareVersion>
  <capacity><!--optional, read-only, xs:integer, unit: MB, device capacity--></capacity>
  <usedCapacity><!--optional, read-only, xs:integer, unit: MB, capacity usage--></usedCapacity>
  <deviceType>
    <!--required, read-only, xs:string, device type: "IPCamera", "IPDome", "DVR", "HybirdNVR", "NVR", "DVS", "IPZoom", "CVR", "Radar", "PerimeterRadar"-perimeter radar, "ACS", "PHA"-Axiom hybrid security control panel-->
  </deviceType>
  <telecontrolID><!--optional, xs:integer, keyfob control ID, the value is between 1 and 255--></telecontrolID>
  <supportBeep><!--optional, xs:boolean--></supportBeep>
  <supportVideoLoss><!--optional, xs:boolean, whether it supports video loss detection--></supportVideoLoss>
  <firmwareVersionInfo><!--optional, read-only, xs:string, firmware version information--></firmwareVersionInfo>
  <actualFloorNum>
    <!--required, xs: integer, actual number of floors, which is between 1 and 128-->
  </actualFloorNum>
  <subChannelEnabled><!--optional, xs:boolean, whether to support sub-stream live view: "true"-yes, "false"-no--></subChannelEnabled>
  <thrChannelEnabled><!--optional, xs:boolean, whether to support third stream live view: "true"-yes, "false"-no--></thrChannelEnabled>
  <radarVersion><!--optional, xs:string, radar version--></radarVersion>
  <cameraModuleVersion><!--read-only, xs:string, camera module version--></cameraModuleVersion>
  <mainversion><!--optional, xs:integer, main version No. which is between 1 and 255--></mainversion>
  <subversion><!--optional, xs:integer, sub version No. which is between 1 and 255--></subversion>
  <upgradeversion><!--optional, xs:integer, upgraded version No. which is between 1 and 255--></upgradeversion>
  <customizeversion><!--optional, xs:integer, customized version  No. which is between 1 and 255--></customizeversion>
  <companyName><!--optional, xs:string, the manufacturing company's abbreviation--></companyName>
  <copyright><!--optional, xs:string, copyright information--></copyright>
  <systemName><!--optional, xs:string , storage system name: "storageManagement"-storage management system, "distributedStorageManagement"-distrubuted storage management system--></systemName>
  <systemStatus><!--optional, xs:string,system status: "configured"-configured, "unConfigured"-not configured--></systemStatus>
  <isLeaderDevice><!--optional, xs:boolean, whether it is the corresponding device of the resource IP address--></isLeaderDevice>
  <clusterVersion><!--dependent, xs:string, system cluster version. This node is valid when the value of isLeaderDevice is true--></clusterVersion>
  <manufacturer><!--optional, xs:string, manufacturer information: "hikvision"-Hikvision devices; for neutral devices, this node should be empty--></manufacturer>
  <customizedInfo><!--optional, xs:string, order No. of the customization project. For baseline devices, this node is empty; for custom devices, the order No. of the customization project will be returned by this node--></customizedInfo>
  <localZoneNum><!--optional, xs:integer, number of local zones--></localZoneNum>
  <alarmOutNum><!--optional, xs:integer, number of alarm outputs--></alarmOutNum>
  <distanceResolution><!--optional, xs:float, resolution of distance, unit: meter--></distanceResolution>
  <angleResolution><!--optional, xs:float, resolution of angle, unit: degree--></angleResolution>
  <speedResolution><!--optional, xs:float, resolution of speed, unit: m/s--></speedResolution>
  <detectDistance><!--optional, xs:float, detection distance, unit: meter--></detectDistance>
  <languageType><!--optional, xs:string, language type: Chinese, English, Spanish, Portuguese, Italian, French, Russian, German, Polish, Turkish, Greek, Czech, Brazilian, Portuguese, Slovenian, Swedish, Norwegian, Slovak, Serbian, Dutch, Hungarian, Irish, Bulgarian, Hebrew, Thai, Indonesian, Arabic, Traditional Chinese--></languageType>
  <relayNum><!--optional, xs:integer, number of local relays--></relayNum>
  <electroLockNum><!--optional, xs:integer, number of local electronic locks--></electroLockNum>
  <RS485Num><!--optional, xs:integer, number of local RS-485--></RS485Num>
  <powerOnMode><!--optional, xs:string, device startup mode: "button"-press button to power on (default), "adapter"-connect adapter to power on--></powerOnMode>
  <DockStation>
    <!--optional, dock station configuration-->
    <Platform>
      <!--optional, platform configuration-->
      <type><!--required, xs:string, platform type: none, 9533, 8618, ISAPI--></type>
```

```
   <ip><!--optional, xs:string, IP address --></ip>
   <port><!--optional, xs:integer, communication port--></port>
   <userName><!--required, xs:string, user name, which is used for the dock station to log in to platform--></userName>
    <password><!--required, xs:string, password, which is used for the dock station to log in to platform, it should be encrypted--></password>
  </Platform>
  <centralStorageBackupEnabled><!--optional, xs:boolean, whether to enable central storage backup--></centralStorageBackupEnabled>
 </DockStation>
 <webVersion><!--optional, read-only, xs:string, web version No.--></webVersion>
 <deviceRFProgramVersion><!--optional, read-only, xs:string, version No. of the device's RF (Radio Frequency) program--></deviceRFProgramVersion>
 <securityModuleSerialNo><!--optional, read-only, xs:string, serial No. of the security module--></securityModuleSerialNo>
 <securityModuleVersion><!--optional, read-only, xs:string, version No. of the security module--></securityModuleVersion>
 <securityChipVersion><!--optional, read-only, xs:string, version No. of the security chip--></securityChipVersion>
 <securityModuleKeyVersion><!--optional, read-only, xs:string, version No. of the security module key--></securityModuleKeyVersion>
 <UIDLampRecognition><!--optional, information of the UID lamp recognition device-->
  <enabled><!--optional, xs:boolean, whether to enable--></enabled>
 </UIDLampRecognition>
 <bootTime><!--optional, xs:string, read-only, system boot time, ISO 8601 format; the maximum length is 32 bytes--></bootTime>
 <ZigBeeVersion min="0" max="16"><!--optional, xs:string, ZigBee module version--></ZigBeeVersion>
 <R3Version min="0" max="16"><!--optional, xs:string, R3 module version--></R3Version>
 <RxVersion min="0" max="16"><!--optional, xs:string, Rx module version--></RxVersion>
 <bspVersion><!--optional, xs:string, BSP software version--></bspVersion>
 <dspVersion><!--optional, xs:string, DSP software version--></dspVersion>
 <localUIVersion><!--optional, xs:string, local UI version--></localUIVersion>
 <isResetDeviceLanguage>
  <!--optional, boolean, whether it supports resetting the device language (only for Admin and Installer)-->false
 </isResetDeviceLanguage>
</DeviceInfo>
```

A.5.17 XML_InputProxyChannel

InputProxyChannel message in XML format

```
<?xml version="1.0" encoding="utf-8"?>
<InputProxyChannel version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
 <id><!--req, xs:string, starts from 1--></id>
 <name><!--opt, xs:string--></name>
 <sourceInputPortDescriptor><!--req-->
  <adminProtocol><!--req, xs:string, "HIKVISION,SONY,ISAPI,ONVIF,..."--></adminProtocol>
  <addressingFormatType><!--req, xs:string, "ipaddress,hostname"--></addressingFormatType>
  <hostName><!--dep, xs:string, domain name--></hostName>
  <ipAddress><!--dep, xs:string, IP address--></ipAddress>
  <ipv6Address><!--dep, xs:string, IPv6 address--></ipv6Address>
  <managePortNo><!--req, xs:integer--></managePortNo>
```

```
    <srcInputPort><!--req, xs:string, channel No.--></srcInputPort>
    <userName><!--req, xs:string, user name, which should be encrypted--></userName>
    <password><!--req, wo, xs:string, password, which should be encrypted--></password>
    <streamType><!--opt, xs:string, opt="auto,tcp,udp"--></streamType>
    <deviceID><!--dep, xs:string--></deviceID>
    <deviceTypeName><!--ro, opt, xs:string, device type name--></deviceTypeName>
    <serialNumber><!--ro, opt, xs:string, device serial No.--></serialNumber>
    <firmwareVersion><!--ro, opt, xs:string, firmware version--></firmwareVersion>
    <firmwareCode><!--ro, opt, xs:string, firmware code--></firmwareCode>
  </sourceInputPortDescriptor>
  <enableAnr>
    <!--opt, xs:boolean, whether enables ANR funtion-->
  </enableAnr>
  <NVRInfo>
    <ipAddressNVR>
      <!--opt, xs:string, IP address of NVR-->
    </ipAddressNVR>
    <portNVR>
      <!--opt, xs:integer, port No. of NVR-->
    </portNVR>
    <ipcChannelNo>
      <!--opt, xs:integer, channel No. of the network camera in NVR-->
    </ipcChannelNo>
  </NVRInfo>
</InputProxyChannel>
```

A.5.18 XML_InputProxyChannelList

InputProxyChannelList message in XML format

```
<?xml version="1.0" encoding="utf-8"?>
<InputProxyChannelList version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <InputProxyChannel/><!--opt, see details in InputProxyChannel-->
</InputProxyChannelList>
```

See Also

XML_InputProxyChannel

A.5.19 XML_InputProxyChannelStatus

InputProxyChannelStatus message in XML format

```
<InputProxyChannelStatus version="1.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <id><!--req, xs:string--></id>
  <sourceInputPortDescriptor/><!--req-->
  <online><!--req, xs:boolean, whether the camera is online--></online>
  <streamingProxyChannelIdList><!--req-->
    <streamingProxyChannelId>
```

```
      <!--req, xs:string, stream channel No., e.g., 101-main stream of channel 1, 102-sub-stream of channel 1-->
    </streamingProxyChannelId>
  </streamingProxyChannelIdList>
  <chanDetectResult>
    <!--opt, xs:string, network camera status: "connect"-connected, "overSysBandwidth"-insufficient bandwidth,
"domainError"-incorrect domain name, "ipcStreamFail"-getting stream failed, "connecting", "chacnNoError"-incorrect
channel No., "cipAddrConflictWithDev": IP address is conflicted with device address, "ipAddrConflicWithIpc"-IP
address conflicted, "errorUserNameOrPasswd"-incorrect user name or password, "netUnreachable"-invalid network
address, "unknownError"-unknown error, "notExist"-does not exist, "ipcStreamTypeNotSupport"-the stream
transmission mode is not supported, "ipcResolutionNotSupport"-the resolution of network camera is not supported-->
  </chanDetectResult>
</InputProxyChannelStatus>
```

A.5.20 XML_InputProxyChannelStatusList

InputProxyChannelStatusList message in XML format

```
<InputProxyChannelStatusList version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <InputProxyChannelStatus/><!--opt, see details in XML_InputProxyChannelStatus-->
</InputProxyChannelStatusList>
```

See Also

XML_InputProxyChannelStatus

A.5.21 XML_IOOutputPort

JSON message about alarm output information

```
<?xml version="1.0" encoding="utf-8"?>
<IOOutputPort version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <id><!--required, xs:integer, "2"--></id>
  <IODescriptor><!--optional, camera IO description-->
    <userName><!--required, xs:string, user name--></userName>
    <addressingFormatType><!--required, xs:string, address type: "ipaddress", "hostname"--></addressingFormatType>
    <hostName><!--dependent, xs:string, host name--></hostName>
    <ipAddress><!--dependent, xs:string, IPv4 address--></ipAddress>
    <ipv6Address><!--dependent, xs:string, IPv6 address--></ipv6Address>
    <managePortNo><!--required, xs:integer, management port No.--></managePortNo>
    <innerIOPortID><!--required, xs:integer, camera IO port No.--></innerIOPortID>
  </IODescriptor>
  <PowerOnState>
    <!--required, output port configuration parameters when the device is powered on-->
    <defaultState>
      <!--read-only, required, xs:string, default output port signal when it is not triggered, "high,low"-->
    </defaultState>
    <outputState>
      <!--read-only, required, output port signal when it is being triggered, xs:string, "high,low,pulse"-->
    </outputState>
    <pulseDuration>
      <!--dependent, xs:integer, duration of a output port signal when it is being triggered, it is valid when outputState is
"pulse", unit: milliseconds -->
    </pulseDuration>
  </PowerOnState>
  <name><!--optional, xs:string--></name>
  <IOUseType><!--optional, xs:string, "disable,electricLock,custom"--></IOUseType>
  <normalStatus><!--optional, xs:string, normal status: open-remain open, close-remain closed--></normalStatus>
  <enabled><!--optional, xs:boolean, enable DND of corresponding IO; default value: true--></enabled>
  <IOType><!--optional, read-only, xs:string, supported IO port type: "local", "digitalChannel", "analogChannel"; the
default value is "local"--></IOType>
</IOOutputPort>
```

A.5.22 XML_IOOutputPortList

XML message about alarm output list

```
<?xml version="1.0" encoding="utf-8"?>
<IOOutputPortList version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <IOOutputPort/><!--optional, see details in IOOutputPort-->
</IOOutputPort>
```

See Also

XML_IOOutputPort

A.5.23 XML_IOPortData

XML message about triggering parameters of alarm output

```
<?xml version="1.0" encoding="utf-8"?>
<IOPortData xmlns=“http://www.isapi.org/ver20/XMLSchema”>
  <outputState><!--required, xs:string, output level: "high, low"--></outputState>
</IOPortData>
```

A.5.24 XML_IOPortStatus

XML message about alarm output status

```
<?xml version="1.0" encoding="utf-8"?>
<IOPortStatus version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <ioPortID><!--required, xs: integer, I/O No.: 1, 2--></ioPortID>
  <ioPortType><!--required, xs: string, I/O type: "input", "output"--></ioPortType>
  <ioState><!--required, xs: string, I/O status: "active", "inactive"--></ioState>
</IOPortStatus>
```

A.5.25 XML_PTZPreset

XML message about preset parameters

```
<?xml version="1.0" encoding="utf-8"?>
<PTZPreset version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <enabled><!--required, xs:boolean, whether to enable preset configuration--></enabled>
  <id><!--required, xs:string, preset No.--></id>
  <presetName><!--required, xs:string, preset name--></presetName>
  <AbsoluteHigh>
    <elevation><!--optional, xs:integer, tilting parameter, the value is between -900 and 2700--></elevation>
    <azimuth><!--optional, xs:integer, panning parameter, the value is between 0 and 3600--></azimuth>
    <absoluteZoom><!--optional, xs:integer, zooming parameter, the value is between 1 and 1000--></absoluteZoom>
  </AbsoluteHigh>
</PTZPreset>
```

A.5.26 XML_PTZPresetList

XML message about preset information list

```
<?xml version="1.0" encoding="utf-8"?>
<PTZPresetList version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <PTZPreset/><!--optional, see details in XML_PTZPreset-->
</PTZPresetList>
```

See Also

XML_PTZPreset

A.5.27 XML_ResponseStatus

XML message about response status

```
<?xml version="1.0" encoding="utf-8"?>
<ResponseStatus version="2.0" xmlns="http://www.std-cgi.org/ver20/XMLSchema">
  <requestURL>
    <!--required, read-only, xs:string, request URL-->
  </requestURL>
  <statusCode>
    <!--required, read-only, xs:integer, status code: 0,1-OK, 2-Device Busy, 3-Device Error, 4-Invalid Operation, 5-Invalid XML Format, 6-Invalid XML Content, 7-Reboot Required, 9-Additional Error-->
  </statusCode>
  <statusString>
    <!--required, read-only, xs:string, status description: OK, Device Busy, Device Error, Invalid Operation, Invalid XML Format, Invalid XML Content, Reboot, Additional Error-->
  </statusString>
  <subStatusCode>
    <!--required, read-only, xs:string, describe the error reason in detail-->
  </subStatusCode>
  <MErrCode>
    <!--optional, xs:string, error code categorized by functional modules, e.g., 0x12345678-->
  </MErrCode>
  <MErrDevSelfEx>
    <!--optional, xs:string, extension field of MErrCode. It is used to define the custom error code, which is categorized
by functional modules-->
  </MErrDevSelfEx>
</ResponseStatus>
```

A.5.28 XML_ResponseStatus_IFSTime

XML message about the device time parameters

```
<ResponseStatus version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <requestURL><!--required, xs:string, request URL, read-only--></requestURL>
  <statusCode><!--required, xs:integer, status code: 0 or 1-OK, 2-Device Busy, 3-Device Error, 4-Invalid Operation, 5-
Invalid XML Format, 6-Invalid XML Content, 7-Reboot Required, read-only--></statusCode>
  <statusString><!--required, xs:string, status description: "OK,Device Busy,Device Error,Invalid Operation,Invalid XML
Format,Invalid XML Content,Reboot", read-only--></statusString>
  <subStatusCode><!--required, xs:string, detailed description of the error code, read-only--></subStatusCode>
  <FailedNodeInfoList>
    <!--optional, information list of failed nodes-->
    <FailedNodeInfo>
      <!--optional, failed node information. When the main node in the data center cluster synchronizes device time, the
main node will synchronize time of all sub nodes at the same time. If synchronizing time of all nodes failed, the failed
response message will be returned. If synchronizing time of part of nodes failed, the succeeded response message will
be returned and this node will returned detailed information of failed nodes-->
      <nodeID><!--required, xs:string, node ID--></nodeID>
      <nodeIP><!--required, xs:string, node IP--></nodeIP>
      <reason><!--optional, xs:string, reason why the node failed to synchronize time, which can be displayed on the
interface--></reason>
    </FailedNodeInfo>
  </FailedNodeInfoList>
</ResponseStatus>
```

A.5.29 XML_Set_PTZPreset

XML message about preset configuration parameters

```
<?xml version="1.0" encoding="utf-8"?>
<PTZPreset version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <enabled><!--required, xs:boolean, whether to enable preset configuration--></enabled>
  <id><!--required, xs:string, preset number--></id>
  <presetName><!--required, xs:string, preset name--></presetName>
</PTZPreset>
```

A.5.30 XML_Time

XML message about time parameters

```
<?xml version="1.0" encoding="utf-8"?>
<Time version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <timeMode><!--required, xs:string, timing mode: "manual, NTP, local, satellite, timecorrect, platform"--></timeMode>
  <localTime>
    <!--required, xs:datetime, ISO 8601 time format, device time set manually, e.g.: 2018-02-01T19:54:04. This node is required when <timemode> is "manual" or "local"-->
  </localTime>
  <timeZone>
    <!--required, xs:string, POSIX time zone based on CST for NTP synchronization, e.g., CST-8:00:00DST00:30:00,M4.1.0/02:00:00,M10.5.0/02:00:00; this node is valid when <timemode> is "manual", "local" or "NTP"-->
  </timeZone>
  <satelliteInterval><!--dependent, xs:integer, unit: minute--></satelliteInterval>
  <isSummerTime><!--optional, xs:boolean, whether the time returned by the current device is that in the DST (daylight saving time) mode: true, false--></isSummerTime>
  <platformType>
    <!--dependent, xs: string, platform type: "EZVIZ"-Hik-Connect; it is valid only when the value of timeMode is "platform"-->
  </platformType>
</Time>
```

A.6 Response Codes of Text Protocol

The response codes returned during the text protocol integration 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, and the response codes are in a one-to-one correspondence with the sub status codes.

StatusCode=1

SubStatusCode	Error Code	Description
ok	0x1	Operation completed.
riskPassword	0x10000002	Risky password.
armProcess	0x10000005	Arming process.

StatusCode=2

Sub Status Code	Error Code	Description
noMemory	0x20000001	Insufficient memory.
serviceUnavailable	0x20000002	The service is not available.
upgrading	0x20000003	Upgrading.
deviceBusy	0x20000004	The device is busy or no response.
reConnectIpc	0x20000005	The video server is reconnected.
transferUpgradePackageFailed	0x20000006	Transmitting device upgrade data failed.
startUpgradeFailed	0x20000007	Starting upgrading device failed.
getUpgradeProcessfailed.	0x20000008	Getting upgrade status failed.
certificateExist	0x2000000B	The Authentication certificate already exists.

StatusCode=3

Sub Status Code	Error Code	Description
deviceError	0x30000001	Hardware error.
badFlash	0x30000002	Flash operation error.
28181Uninitialized	0x30000003	The 28181 configuration is not initialized.
socketConnectError	0x30000005	Connecting to socket failed.
receiveError	0x30000007	Receive response message failed.
deletePictureError	0x3000000A	Deleting picture failed.
pictureSizeExceedLimit	0x3000000C	Too large picture size.
clearCacheError	0x3000000D	Clearing cache failed.
updateDatabasError	0x3000000F	Updating database failed.

Sub Status Code	Error Code	Description
searchDatabaseError	0x30000010	Searching in the database failed.
writeDatabaseError	0x30000011	Writing to database failed.
deleteDatabaseError	0x30000012	Deleting database element failed.
searchDatabaseElementError	0x30000013	Getting number of database elements failed.
cloudAutoUpgradeException	0x30000016	Downloading upgrade packet from cloud and upgrading failed.
HBPException	0x30001000	HBP exception.
UDEPException	0x30001001	UDEP exception
elasticSearchException	0x30001002	Elastic exception.
kafkaException	0x30001003	Kafka exception.
HBaseException	0x30001004	Hbase exception.
sparkException	0x30001005	Spark exception.
yarnException	0x30001006	Yarn exception.
cacheException	0x30001007	Cache exception.
trafficException	0x30001008	Monitoring point big data server exception.
faceException	0x30001009	Human face big data server exception.
SSDFileSystemIsError	0x30001013	SSD file system error (Error occurs when it is non-Ext4 file system)
insufficientSSDCapacityForFPD	0x30001014	Insufficient SSD space for person frequency detection.
wifiException	0x3000100A	Wi-Fi big data server exception
structException	0x3000100D	Video parameters structure server exception.
noLinkageResource	0x30001015	Insufficient linkage resources.

Sub Status Code	Error Code	Description
engineAbnormal	0x30002015	Engine exception.
engineInitialization	0x30002016	Initializing the engine.
algorithmLoadingFailed	0x30002017	Loading the model failed.
algorithmDownloadFailed	0x30002018	Downloading the model failed.
algorithmDecryptionFailed	0x30002019	Decrypting the model failed.
unboundChannel	0x30002020	Delete the linked channel to load the new model.
unsupportedResolution	0x30002021	Invalid resolution.
unsupportedSteamType	0x30002022	Invalid stream type.
insufficientDecRes	0x30002023	Insufficient decoding resources.
insufficientEnginePerformance	0x30002024	Insufficient engine performance (The number of channels to be analyzed exceeds the engine's capability).
improperResolution	0x30002025	Improper resolution (The maximum resolution allowed is 4096×4096).
improperPicSize	0x30002026	Improper picture size (The maximum size allowed is 5MB).
URLDownloadFailed	0x30002027	Downloading the picture via the URI failed.
unsupportedImageFormat	0x30002028	Invalid picture format (Only JPG is supported currently).
unsupportedPollingIntervalTime	0x30002029	Invalid polling interval (The interval should be more than 10s).
exceedImagesNumber	0x30002030	The number of pictures exceeds the limit (The platform can apply 1 to 100 picture URIs per time, the maximum number allowed is 100).

Sub Status Code	Error Code	Description
unsupportedMPID	0x30002031	The applied MPID does not exist in the device, so updating this MPID is not supported.
modelPackageNotMatchLabel	0x30002032	The model and the description file mismatch.
modelPackageNotMatchTask	0x30002033	The task and the model type mismatch.
insufficientSpace	0x30002034	Insufficient space (When the number of model packages does not reach the maximum number allowed but their size together exceeds the free space, the model packages cannot be added).
engineUnLoadingModelPackage	0x30002035	Applying the task failed. This engine is not linked to a model package (Canceling the linkage failed, this engine is not linked to a model package).
engineWithModelPackage	0x30002036	Linking the engine to this model package failed. The engine has been linked to another model package. Please cancel their linkage first.
modelPackageDelete	0x30002037	Linking the model package failed. The model package has been deleted.
deleteTaskFailed	0x30002038	Deleting the task failed (It is returned when the user fails to end a task).
modelPackageNumberslimited	0x30002039	Adding the model package failed. The number of model package has reached the maximum number allowed.
modelPackageDeleteFailed	0x30002040	Deleting the model package failed.

Sub Status Code	Error Code	Description
noArmingResource	0x30001016	Insufficient arming resources.
calibrationTimeout	0x30002051	Calibration timed out.
captureTimeout	0x30006000	Data collection timed out.
lowScore	0x30006001	Low quality of collected data.
uploadingFailed	0x30007004	Uploading failed.

StatusCode=4

Sub Status Code	Error Code	Description
notSupport	0x40000001	Not supported.
lowPrivilege	0x40000002	No permission.
badAuthorization	0x40000003	Authentication failed.
methodNotAllowed	0x40000004	Invalid HTTP method.
notSetHdiskRedund	0x40000005	Setting spare HDD failed.
invalidOperation	0x40000006	Invalid operation.
notActivated	0x40000007	Inactivated.
hasActivated	0x40000008	Activated.
certificateAlreadyExist	0x40000009	The certificate already exists.
operateFailed	0x4000000F	Operation failed.
USBNotExist	0x40000010	USB device is not connected.
upgradePackageMorethan2GB	0x40001000	Up to 2GB upgrade package is allowed to be uploaded.
IDNotexist	0x40001001	The ID does not exist.
interfaceOperationError	0x40001002	API operation failed.
synchronizationError	0x40001003	Synchronization failed.
synchronizing	0x40001004	Synchronizing.
importError	0x40001005	Importing failed.
importing	0x40001006	Importing.

Sub Status Code	Error Code	Description
fileAlreadyExists	0x40001007	The file already exists.
invalidID	0x40001008	Invalid ID.
backupnodeNotAlloweLog	0x40001009	Accessing to backup node is not allowed.
exportingError	0x4000100A	Exporting failed.
exporting	0x4000100B	Exporting.
exportEnded	0x4000100C	Exporting stopped.
exported	0x4000100D	Exported.
IPOccupied	0x4000100E	The IP address is already occupied.
IDAlreadyExists	0x4000100F	The ID already exists.
exportItemsExceedLimit	0x40001010	No more items can be exported.
noFiles	0x40001011	The file does not exist.
beingExportedByAnotherUser	0x40001012	Being exported by others.
needReAuthentication	0x40001013	Authentication is needed after upgrade.
unitAddNotOnline	0x40001015	The added data analysis server is offline.
unitControl	0x40001016	The data analysis server is already added.
analysis unitFull	0x40001017	No more data analysis server can be added.
unitIDError	0x40001018	The data analysis server ID does not exist.
unitExit	0x40001019	The data analysis server already exists in the list.
unitSearch	0x4000101A	Searching data analysis server in the list failed.
unitNotOnline	0x4000101B	The data analysis server is offline.
unitInfoEror	0x4000101C	Getting data analysis server information failed.
unitGetNodeInfoError	0x4000101D	Getting node information failed.
unitGetNetworkInfoError	0x4000101E	Getting the network information of data analysis server failed
unitSetNetworkInfoError	0x4000101F	Setting the network information of data analysis server failed

Sub Status Code	Error Code	Description
setSmartNodeInfoError	0x40001020	Setting node information failed.
setUnitNetworkInfoError	0x40001021	Setting data analysis server network information failed.
unitRestartCloseError	0x40001022	Rebooting or shutting down data analysis server failed.
virtualIPnotAllowed	0x40001023	Adding virtual IP address is not allowed.
unitInstalled	0x40001024	The data analysis server is already installed.
badSubnetMask	0x40001025	Invalid subnet mask.
uintVersionMismatched	0x40001026	Data analysis server version mismatches.
deviceMOdelMismatched	0x40001027	Adding failed. Device model mismatches.
unitAddNotSelf	0x40001028	Adding peripherals is not allowed.
noValidUnit	0x40001029	No valid data analysis server.
unitNameDuplicate	0x4000102A	Duplicated data analysis server name.
deleteUnitFirst	0x4000102B	Delete the added data analysis server of the node first.
getLocalInfoFailed	0x4000102C	Getting the server information failed.
getClientAddedNodeFailed	0x4000102D	Getting the added node information of data analysis server failed.
taskExit	0x4000102E	The task already exists.
taskInitError	0x4000102F	Initializing task failed.
taskSubmitError	0x40001030	Submiting task failed.
taskDelError	0x40001031	Deleting task failed.
taskPauseError	0x40001032	Pausing task failed.
taskContinueError	0x40001033	Starting task failed.
taskSeverNoCfg	0x40001035	Full-text search server is not configured.
taskPicSeverNoCfg	0x40001036	The picture server is not configured.
taskStreamError	0x40001037	Streaming information exception.
taskRecSDK	0x40001038	History recording is not supported.

Sub Status Code	Error Code	Description
taskCasaError	0x4000103A	Cascading is not supported.
taskVCARuleError	0x4000103B	Invalid VCA rule.
taskNoRun	0x4000103C	The task is not executed.
unitLinksNoStorageNode	0x4000103D	No node is linked with the data analysis server. Configure the node first.
searchFailed	0x4000103E	Searching video files failed.
searchNull	0x4000103F	No video clip.
userScheOffline	0x40001040	The task scheduler service is offline.
updateTypeUnmatched	0x40001041	The upgrade package type mismatches.
userExist	0x40001043	The user already exists.
userCannotDelAdmin	0x40001044	The administrator cannot be deleted.
userInexistence	0x40001045	The user name does not exist.
userCannotCreatAdmin	0x40001046	The administrator cannot be created.
monitorCamExceed	0x40001048	Up to 3000 cameras can be added.
monitorCunitOverLimit	0x40001049	Adding failed. Up to 5 lower-levels are supported by the control center.
monitorReginOverLimit	0x4000104A	Adding failed. Up to 5 lower-levels are supported by the area.
monitorArming	0x4000104B	The camera is already armed. Disarm the camera and try again.
monitorSyncCfgNotSet	0x4000104C	The system parameters are not configured.
monitorFdSyncing	0x4000104E	Synchronizing. Try again after completing the synchronization.
monitorParseFailed	0x4000104F	Parsing camera information failed.
monitorCreatRootFailed	0x40001050	Creating resource node failed.
deleteArmingInfo	0x40001051	The camera is already . Disarm the camera and try again.
cannotModify	0x40001052	Editing is not allowed. Select again.

Sub Status Code	Error Code	Description
cannotDel	0x40001053	Deletion is not allowed. Select again.
deviceExist	0x40001054	The device already exists.
IPErrorConnectFailed	0x40001056	Connection failed. Check the network port.
cannotAdd	0x40001057	Only the capture cameras can be added.
serverExist	0x40001058	The server already exists.
fullTextParamError	0x40001059	Incorrect full-text search parameters.
storParamError	0x4000105A	Incorrect storage server parameters.
picServerFull	0x4000105B	The storage space of picture storage server is full.
NTPUnconnect	0x4000105C	Connecting to NTP server failed. Check the parameters.
storSerConnectFailed	0x4000105D	Connecting to storage server failed. Check the network port.
storSerLoginFailed	0x4000105E	Logging in to storage server failed. Check the user name and password.
searchSerConnectFailed	0x4000105F	Connecting to full-text search server failed. Check the network port.
searchSerLoginFailed	0x40001060	Logging in to full-text search server failed. Check the user name and password.
kafkaConnectFailed	0x40001061	Connecting to Kafka failed. Check the network port.
mgmtConnectFailed	0x40001062	Connecting to system failed. Check the network port.
mgmtLoginFailed	0x40001063	Logging in to system failed. Check the user name and password.
TDAConnectFailed	0x40001064	Connecting to traffic data access server failed. Checking the server status.
86sdkConnectFailed	0x40001065	Connecting to listening port of iVMS-8600 System failed. Check the parameters.
nameExist	0x40001066	Duplicated server name.
batchProcessFailed	0x40001067	Processing in batch failed.

Sub Status Code	Error Code	Description
IDNotExist	0x40001068	The server ID does not exist.
serviceNumberReachesLimit	0x40001069	No more service can be added.
invalidServiceType.	0x4000106A	Invalid service type.
clusterGetInfo	0x4000106B	Getting cluster group information failed.
clusterDelNode	0x4000106C	Deletion node failed.
clusterAddNode	0x4000106D	Adding node failed.
clusterInstalling	0x4000106E	Creating cluster…Do not operate.
clusterUninstall	0x4000106F	Reseting cluster…Do not operate.
clusterInstall	0x40001070	Creating cluster failed.
clusterIpError	0x40001071	Invalid IP address of task scheduler server.
clusterNotSameSeg	0x40001072	The main node and sub node must be in the same network segment.
clusterVirIpError	0x40001073	Automatically getting virtual IP address failed. Enter manually.
clusterNodeUnadd	0x40001074	The specified main (sub) node is not added.
clusterNodeOffline	0x40001075	The task scheduler server is offline.
nodeNotCurrentIP	0x40001076	The analysis node of the current IP address is required when adding main and sub nodes.
addNodeNetFailed	0x40001077	Adding node failed. The network disconnected.
needTwoMgmtNode	0x40001078	Two management nodes are required when adding main and sub nodes.
ipConflict	0x40001079	The virtual IP address and data analysis server's IP address conflicted.
ipUsed	0x4000107A	The virtual IP address has been occupied.
cloudAlalyseOnline	0x4000107B	The cloud analytic server is online.
virIP&mainIPnotSameNetSegment	0x4000107C	The virtual IP address is not in the same network segment with the IP address of main/sub node.
getNodeDispatchInfoFailed	0x4000107D	Getting node scheduler information failed.

Sub Status Code	Error Code	Description
unableModifyManagementNetworkIP	0x4000107E	Editing management network interface failed. The analysis board is in the cluster.
notSpecifyVirtualIP	0x4000107F	Virtual IP address should be specified for main and sub cluster.
armingFull	0x40001080	No more device can be armed.
armingNoFind	0x40001081	The arming information does not exist.
disArming	0x40001082	Disarming failed.
getArmingError	0x40001084	Getting arming information failed.
refreshArmingError	0x40001085	Refreshing arming information failed.
ArmingPlateSame	0x40001086	The license plate number is repeatedly armed.
ArmingParseXLSError	0x40001087	Parsing arming information file failed.
ArmingTimeError	0x40001088	Invalid arming time period.
ArmingSearchTimeError	0x40001089	Invalid search time period.
armingRelationshipReachesLimit	0x4000108A	No more relation can be created.
duplicateAarmingName	0x4000108B	The relation name already exists.
noMoreArmingListAdded	0x4000108C	No more blocklist library can be armed.
noMoreCamerasAdded	0x4000108D	No more camera can be armed.
noMoreArmingListAddedWithCamera	0x4000108E	No more library can be linked to the camera.
noMoreArmingPeriodAdded	0x4000108F	No more time period can be added to the arming schedule.
armingPeriodsOverlapped	0x40001090	The time periods in the arming schedule are overlapped.
noArmingAlarmInfo	0x40001091	The alarm information does not exist.
armingAlarmUnRead	0x40001092	Getting number of unread alarms failed.
getArmingAlarmError	0x40001093	Getting alarm information failed.

Sub Status Code	Error Code	Description
searchByPictureTimedOut	0x40001094	Searching picture by picture timeout. Search again.
comparisonTimeRangeError	0x40001095	Comparison time period error.
selectMonitorNumberUpperLimit	0x40001096	No more monitoring point ID can be filtered.
noMoreComparisonTasksAdded	0x40001097	No more comparison task can be executed at the same time.
GetComparisonResultFailed	0x40001098	Getting comparison result failed.
comparisonTypeError	0x40001099	Comparison type error.
comparisonUnfinished	0x4000109A	The comparison is not completed.
facePictureModelInvalid	0x4000109B	Invalid face model.
duplicateLibraryName.	0x4000109C	The library name already exists.
noRecord	0x4000109D	No record found.
countingRecordsFailed.	0x4000109E	Calculate the number of records failed.
getHumanFaceFrameFailed	0x4000109F	Getting face thumbnail from the picture failed.
modelingFailed.	0x400010A0	Modeling face according to picture URL failed.
1V1FacePictureComparisonFailed	0x400010A1	Comparison 1 VS 1 face picture failed.
libraryArmed	0x400010A2	The blocklist library is armed.
licenseExeedLimit	0x400010A3	Dongle limited.
licenseExpired	0x400010A4	Dongle expired.
licenseDisabled	0x400010A5	Unavailable dongle.
licenseNotExist	0x400010A6	The dongle does not exist.
SessionExpired	0x400010A7	Session expired .
beyondConcurrentLimit	0x400010A8	Out of concurrent limit.
stopSync	0x400010A9	Synchronization stopped.

Sub Status Code	Error Code	Description
getProgressFaild	0x400010AA	Getting progress failed.
uploadExtraCaps	0x400010AB	No more files can be uploaded.
timeRangeError	0x400010AC	Time period error.
dataPortNotConnected	0x400010AD	The data port is not connected.
addClusterNodeFailed	0x400010AE	Adding to the cluster failed. The device is already added to other cluster.
taskNotExist	0x400010AF	The task does not exist.
taskQueryFailed	0x400010B0	Searching task failed.
modifyTimeRuleFailed	0x400010B2	The task already exists. Editing time rule is not allowed.
modifySmartRuleFailed	0x400010B3	The task already exists. Editing VAC rule is not allowed.
queryHistoryVideoFailed	0x400010B4	Searching history video failed.
addDeviceFailed	0x400010B5	Adding device failed.
addVideoFailed	0x400010B6	Adding video files failed.
deleteAllVideoFailed	0x400010B7	Deleting all video files failed.
createVideoIndexFailed	0x400010B8	Indexing video files failed.
videoCheckTypeFailed	0x400010B9	Verifying video files types failed.
configStructuredAddressFailed	0x400010BA	Configuring IP address of structured server failed.
configPictureServerAddressFailed	0x400010BB	Configuring IP address of picture storaged server failed.
storageServiceIPNotExist	0x400010BD	The storage server IP address does not exist.
syncBackupDatabaseFailed	0x400010BE	Synchronizing sub database failed. Try again.
syncBackupNTPTimeFailed	0x400010BF	Synchronizing NTP time of sub server failed.
clusterNotSelectLoopbackAddress	0x400010C0	Loopbacl address is not supported by the main or sub cluster.

Sub Status Code	Error Code	Description
addFaceRecordFailed	0x400010C1	Adding face record failed.
deleteFaceRecordFailed	0x400010C2	Deleting face record failed.
modifyFaceRecordFailed	0x400010C3	Editing face record failed.
queryFaceRecordFailed	0x400010C4	Searching face record failed.
faceDetectFailed	0x400010C5	Detecting face failed.
libraryNotExist	0x400010C6	The library does not exist.
blackListQueryExporting	0x400010C7	Exporting matched blocklists.
blackListQueryExported	0x400010C8	The matched blocklists are exported.
blackListQueryStopExporting	0x400010C9	Exporting matched blocklists is stopped.
blackListAlarmQueryExporting	0x400010CA	Exporting matched blocklist alarms.
blackListAlarmQueryExported	0x400010CB	The matched blocklists alarms are exported.
blackListAlarmQueryStopExporting	0x400010CC	Exporting matched blocklist alarms is stopped.
getBigDataCloudAnalysisFailed	0x400010CD	Getting big data cloud analytic information failed.
setBigDataCloudAnalysisFailed	0x400010CE	Configuring big data cloud analytic failed.
submitMapSearchFailed	0x400010CF	Submitting task of searching via picture comparison failed.
controlRelationshipNotExist	0x400010D0	The relation does not exist.
getHistoryAlarmInfoFailed	0x400010D1	Getting history alarm information failed.
getFlowReportFailed	0x400010D2	Getting people counting report failed.
addGuardFailed	0x400010D3	Adding arming configuration failed.

Sub Status Code	Error Code	Description
deleteGuardFailed	0x400010D4	Deleting arming configuration failed.
modifyGuardFailed	0x400010D5	Editing arming configuration failed.
queryGuardFailed	0x400010D6	Searching arming configurations failed.
uploadUserSuperCaps	0x400010D7	No more user information can be uploaded.
bigDataServerConnectFailed	0x400010D8	Connecting to big data server failed.
microVideoCloudRequestInfoBuildFailed	0x400010D9	Adding response information of micro video cloud failed.
microVideoCloudResponseInfoBuildFailed	0x400010DA	Parsing response information of micro video cloud failed.
transcodingServerRequestInfoBuildFailed	0x400010DB	Adding response information of transcoding server failed.
transcodingServerResponseInfoParseFailed	0x400010DC	Parsing response information of transcoding server failed.
transcodingServerOffline	0x400010DD	Transcoding server is offline.
microVideoCloudOffline	0x400010DE	Micro video cloud is offline.
UPSServerOffline	0x400010DF	UPS monitor server is offline.
statisticReportRequestInfoBuildFailed	0x400010E0	Adding response information of statistics report failed.
statisticReportResponseInfoParseFailed	0x400010E1	Parsing response information of statistics report failed.
DisplayConfigInfoBuildFailed	0x400010E2	Adding display configuration information failed.
DisplayConfigInfoParseFailed	0x400010E3	Parsing display configuration information failed.
DisplayConfigInfoSaveFailed	0x400010E4	Saving display configuration information failed.
notSupportDisplayConfigType	0x400010E5	The display configuration type is not supported.
passError	0x400010E7	Incorrect password.

Sub Status Code	Error Code	Description
upgradePackageLarge	0x400010EB	Too large upgrade package.
sesssionUserReachesLimit	0x400010EC	No more user can log in via session.
ISO 8601TimeFormatError	0x400010ED	Invalid ISO8601 time format.
clusterDissolutionFailed	0x400010EE	Deleting cluster failed.
getServiceNodeInfoFailed	0x400010EF	Getting service node information failed.
getUPSInfoFailed	0x400010F0	Getting UPS configuration information failed.
getDataStatisticsReportFailed	0x400010F1	Getting data statistic report failed.
getDisplayConfigInfoFailed	0x400010F2	Getting display configuration failed.
namingAnalysisBoardNotAllowed	0x400010F3	Renaming analysis board is not allowed.
onlyDrawRegionsOfConvexPolygon	0x400010F4	Only drawing convex polygon area is supported.
bigDataServerResponseInfoParseFailed	0x400010F5	Parsing response message of big data service failed.
bigDataServerReturnFailed	0x400010F6	No response is returned by big data service.
microVideoReturnFailed	0x400010F7	No response is returned by micro video cloud service.
transcodingServerReturnFailed	0x400010F8	No response is returned by transcoding service.
UPSServerReturnFailed	0x400010F9	No response is returned by UPS monitoring service.
forwardingServer ReturnFailed	0x400010FA	No response is returned by forwarding service.
storageServer ReturnFailed	0x400010FB	No response is returned by storage service.

Sub Status Code	Error Code	Description
cloudAnalysisServerReturnFailed	0x400010FC	No response is returned by cloud analytic service.
modelEmpty	0x400010FD	No model is obtained.
mainAndBackupNodeCannotModifyManagementNetworkInterfaceIP	0x400010FE	Editing the management interface IP address of main node and backup node is not allowed.
IDTooLong	0x400010FF	The ID is too long.
pictureCheckFailed	0x40001100	Detecting picture failed.
pictureModelingFailed	0x40001101	Modeling picture failed.
setCloudAnalsisDefaultProvinceFailed	0x40001102	Setting default province of cloud analytic service failed.
InspectionAreasNumberExceedLimit	0x40001103	No more detection regions can be added.
picturePixelsTooLarge	0x40001105	The picture resolution is too high.
picturePixelsTooSmall	0x40001106	The picture resolution is too low.
storageServiceIPEmpty	0x40001107	The storage server IP address is required.
bigDataServerRequestInfoBuildFail	0x40001108	Creating request message of big data service failed.
analysiTimedOut	0x40001109	Analysis time out.
high-performanceModeDisabled.	0x4000110A	Please enable high-performance mode.
configuringUPSMonitoringServerTimedOut	0x4000110B	Configurating the UPS monitoring server time out. Check IP address.
cloudAnalysisRequestInformationBuildFailed	0x4000110C	Creating request message of cloud analytic service failed.
cloudAnalysisResponseInformationParseFailed	0x4000110D	Parsing response message of cloud analytic service failed.
allCloudAnalysisInterfaceFailed	0x4000110E	Calling API for cloud analytic service failed.
cloudAnalysisModelCompareFailed	0x4000110F	Model comparison of cloud analytic service failed.

Sub Status Code	Error Code	Description
cloudAnalysisFacePictureQualityRatingFailed	0x40001110	Getting face quality grading of cloud analytic service failed.
cloudAnalysisExtractFeaturePointsFailed	0x40001111	Extracting feature of cloud analytic service failed.
cloudAnalysisExtractPropertyFailed	0x40001112	Extracting property of cloud analytic service failed.
getAddedNodeInformationFailed	0x40001113	Getting the added nodes information of data analysis server failed.
noMoreAnalysisUnitsAdded	0x40001114	No more data analysis servers can be added.
detectionAreaInvalid	0x40001115	Invalid detection region.
shieldAreaInvalid	0x40001116	Invalid shield region.
noMoreShieldAreasAdded	0x40001117	No more shield region can be drawn.
onlyAreaOfRectangleShapeAllowed	0x40001118	Only drawing rectangle is allowed in detection area.
numberReachedLlimit	0x40001119	Number reached the limit.
wait1~3MinutesGetIPAfterSetupDHCP	0x4000111A	Wait 1 to 3 minutes to get IP address after configuring DHCP.
plannedTimeMustbeHalfAnHour	0x4000111B	Schedule must be half an hour.
oneDeviceCannotBuildCluster	0x4000111C	Creating main and backup cluster requires at least two devices.
updatePackageFileNotUploaded	0x4000111E	Upgrade package is not uploaded.
highPerformanceTasksNotSupportDrawingDetectionRegions	0x4000111F	Drawing detection area is not allowed under high-performance mode.
controlCenterIDDoesNotExist	0x40001120	The control center ID does not exist.
regionIDDoesNotExist	0x40001121	The area ID does not exist.
licensePlateFormatError	0x40001122	Invalid license plate format.

Sub Status Code	Error Code	Description
managementNodeDoesNotSupportThisOperation	0x40001123	The operation is not supported.
searchByPictureResourceNotConfiged	0x40001124	The conditions for searching picture by picture are not configured.
videoFileEncapsulationFormatNotSupported	0x40001125	The video container format is not supported.
videoPackageFailure	0x40001126	Converting video container format failed.
videoCodingFormatNotSupported	0x40001127	Video coding format is not supported.
monitorOfDeviceArmingdeleteArmingInfo	0x40001129	The camera is armed. Disarm it and try again.
getVideoSourceTypeFailed	0x4000112A	Getting video source type failed.
smartRulesBuildFailed	0x4000112B	Creating VAC rule failed.
smartRulesParseFailed	0x4000112C	Parsing VAC rule failed.
timeRulesBuildFailed	0x4000112D	Creating time rule failed.
timeRulesParseFailed	0x4000112E	Parsing time rule failed.
monitoInfoInvalid	0x4000112F	Invalid camera information.
addingFailedVersionMismatches	0x40001130	Adding failed. The device version mismatches.
theInformationReturnedAfterCloudAnalysisIsEmpty	0x40001131	No response is returned by the cloud analytic service.
selectingIpAddressOfHostAndSpareNodeFailedCheckTheStatus	0x40001132	Setting IP address for main node and backup node failed. Check the node status.
theSearchIdDoesNotExist	0x40001133	The search ID does not exist.
theSynchronizationIdDoesNotExist	0x40001134	The synchronization ID does not exist.
theUserIdDoesNotExist	0x40001136	The user ID does not exist.

Sub Status Code	Error Code	Description
theIndexCodeDoesNotExist	0x40001138	The index code does not exist.
theControlCenterIdDoesNotExist	0x40001139	The control center ID does not exist.
theAreaIdDoesNotExist	0x4000113A	The area ID does not exist.
theArmingLinkageIdDoesNotExist	0x4000113C	The arming relationship ID does not exist.
theListLibraryIdDoesNotExist	0x4000113D	The list library ID does not exist.
invalidCityCode	0x4000113E	Invalid city code.
synchronizingThePasswordOfSpareServerFailed	0x4000113F	Synchronizing backup system password failed.
editingStreamingTypeIsNotSupported	0x40001140	Editing streaming type is not supported.
switchingScheduledTaskToTemporaryTaskIsNotSupported	0x40001141	Switching scheduled task to temporary task is not supported.
switchingTemporaryTaskToScheduledTaskIsNotSupported	0x40001142	Switching temporary task to scheduled task is not supported.
theTaskIsNotDispatchedOrItIsUpdating	0x40001143	The task is not dispatched or is updating.
thisTaskDoesNotExist	0x40001144	This task does not exist in the cloud analytic serice.
duplicatedSchedule	0x40001145	Schedule period cannot be overlapped.
continuousScheduleWithSameAlgorithmTypeShouldBeMerged	0x40001146	The continuous schedule periods with same algorithm type should be merged.
invalidStreamingTimeRange	0x40001147	Invalid streaming time period.
invalidListLibraryType	0x40001148	Invalid list library type.

Sub Status Code	Error Code	Description
theNumberOfMatchedResultsShouldBeLargerThan0	0x40001149	The number of search results should be larger than 0.
invalidValueRangeOfSimilarity	0x4000114A	Invalid similarity range.
invalidSortingType	0x4000114B	Invalid sorting type.
noMoreListLibraryCanBeLinkedToTheDevice	0x4000114C	No more lists can be added to one device.
InvalidRecipientAddressFormat	0x4000114D	Invalid address format of result receiver.
creatingClusterFailedTheDongleIsNotPluggedIn	0x4000114E	Insert the dongle before creating cluster.
theURLIsTooLong	0x4000114F	No schedule configured for the task.
noScheduleIsConfiguredForTheTask	0x40001150	No schedule configured for the task.
theDongleIsExpiried	0x40001151	Dongle has expired.
dongleException	0x40001152	Dongle exception.
invalidKey	0x40001153	Invalid authorization service key.
decryptionFailed	0x40001154	Decrypting authorization service failed.
encryptionFailed	0x40001155	Encrypting authorization service failed.
AuthorizeServiceResponseError	0x40001156	Authorization service response exception.
incorrectParameter	0x40001157	Authorization service parameters error.
operationFailed	0x40001158	Operating authorization service error.
noAnalysisResourceOrNoDataInTheListLibrary	0x40001159	No cloud analytic resources or no data in the list library.
calculationException	0x4000115A	Calculation exception.
allocatingList	0x4000115B	Allocating list.
thisOperationIsNotSupportedByTheCloudAnalytics	0x4000115C	This operation is not supported by the cloud analytic serice.

Sub Status Code	Error Code	Description
theCloudAnalyticsIsInterrupted	0x4000115D	The operation of cloud analytic serice is interrupted.
theServiceIsNotReady	0x4000115E	The service is not ready.
searchingForExternalApiFailed	0x4000115F	Searching external interfaces failed.
noOnlineNode	0x40001160	No node is online.
noNodeAllocated	0x40001161	No allocated node.
noMatchedList	0x40001162	No matched list.
allocatingFailedTooManyFacePictureLists	0x40001163	Allocation failed. Too many lists of big data service.
searchIsNotCompletedSearchAgain	0x40001164	Current searching is not completed. Search again.
allocatingListIsNotCompleted	0x40001165	Allocating list is not completed.
searchingForCloudAnalyticsResultsFailed	0x40001166	Searching cloud analytic serice overtime.
noDataOfTheCurrentLibraryFound	0x40001167	No data in the current library. Make sure there is data in the Hbase.
noFacePictureLibraryIsArmed	0x40001168	No face picture library is armed for big data service.
noAvailableDataSlicingVersionInformationArmFirstAndSliceTheData	0x40001169	Invalid standard version information.
duplicatedOperationDataSlicingIsExecuting	0x4000116A	Slicing failed. Duplicated operation.
slicinDataFailedNoArmedFacePictureLibrary	0x4000116B	Slicing failed. No arming information in the face big data.
GenerateBenchmarkFileFailedSlicingAgain	0x4000116C	Generating sliced file failed. Slice again.
NonprimaryNodeIsProhibitedFromSlcingData	0x4000116D	Slicing is not allowed by the backup node.
NoReadyNodeToClusterServers	0x4000116E	Creating the cluster failed. No ready node.

Sub Status Code	Error Code	Description
NodeManagementServiceIsOffline	0x4000116F	The node management server is offline.
theCamera(s)OfTheControlCenterAreAlreadyArmed.DisarmThemFirst	0x40001170	Some cameras in control center are already armed. Disarm them and try again.
theCamera(s)OfTheAreaAreAlreadyArmed.DisarmThemFirst	0x40001171	Some cameras in this area are already armed. Disarm them and try again.
configuringHigh-frequencyPeopleDetectionFailed	0x40001172	Configuring high frequency people detection failed.
searchingForHigh-frequencyPeopleDetectionLogsFailed.	0x40001173	Searching detection event logs of high-frequency people detection failed.
gettingDetailsOfSearchedHigh-frequencyPeopleDetectionLogsFailed.	0x40001174	Getting the search result details of frequently appeared person alarms failed.
theArmedCamerasAlreadyExistInTheControlCenter	0x40001175	Some cameras in control center are already armed.
disarmingFailedTheCameraIsNotArmed	0x40001177	Disarming failed. The camera is not armed.
noDataReturned	0x40001178	No response is returned by the big data service.
preallocFailure	0x40001179	Pre-allocating algorithm resource failed.
overDogLimit	0x4000117A	Configuration failed. No more resources can be pre-allocated.
analysisServicesDoNotSupport	0x4000117B	Not supported.
commandAndDispatchServiceError	0x4000117C	Scheduling service of cloud analytic serice error.
engineModuleError	0x4000117D	Engine module of cloud analytic serice error.

Sub Status Code	Error Code	Description
streamingServiceError	0x4000117E	Streaming component of cloud analytic serice error.
faceAnalysisModuleError	0x4000117F	Face analysis module of cloud analytic serice error.
vehicleAnalysisModuleError	0x40001180	Vehicle pictures analytic module of cloud analytic serice error.
videoStructuralAnalysisModuleError	0x40001181	Video structuring module of cloud analytic serice error.
postprocessingModuleError	0x40001182	Post-processing module of cloud analytic serice error.
frequentlyAppearedPersonAlarmIsAlreadyConfiguredForListLibrary	0x40001183	Frequently appeared person alarm is already armed for blocklist library.
creatingListLibraryFailed	0x40001184	Creating list library failed.
invalidIdentiryKeyOfListLibrary	0x40001185	Invalid identity key of list library.
noMoreDevicesCanBeArmed	0x40001186	No more camera can be added.
settingAlgorithmTypeForDeviceFailed	0x40001187	Allocating task resource failed.
gettingHighFrequencyPersonDetectionAlarmInformationFailed	0x40001188	Setting frequently appeared person alarm failed.
invalidSearchConfition	0x40001189	Invalid result.
theTaskIsNotCompleted	0x4000118B	The task is not completed.
resourceOverRemainLimit	0x4000118C	No more resource can be pre-allocated.
frequentlyAppearedPersonAlarmIs AlreadyConfiguredForTheCameraDisarmFirstAndTryAgain	0x4000118D	The frequently appeared person alarm of this camera is configured. Delete the arming information and try again.

Sub Status Code	Error Code	Description
switchtimedifflesslimit	0x4000123b	Time difference between power on and off should be less than 10 minutes.
associatedFaceLibNumOverLimit	0x40001279	Maximum number of linked face picture libraries reached.
noMorePeopleNumChangeRulesAdded	0x4000128A	Maximum number of people number changing rules reached.
noMoreViolentMotionRulesAdded	0x4000128D	Maximum number of violent motion rules reached.
noMoreLeavePositionRulesAdded	0x4000128E	Maximum number of leaving position rules reached.
SMRDiskNotSupportRaid	0x40001291	SMR disk does not support RAID.
OnlySupportHikAndCustomProtocol	0x400012A3	IPv6 camera can only be added via Device Network SDK or custom protocols.
vehicleEnginesNoResource	0x400012A6	Insufficient vehicle engine resources.
noMoreRunningRulesAdded	0x400012A9	Maximum number of running rules reached.
noMoreGroupRulesAdded	0x400012AA	Maximum number of people gathering rules reached.
noMoreFailDownRulesAdded	0x400012AB	Maximum number of people falling down rules reached.
noMorePlayCellphoneRulesAdded	0x400012AC	Maximum number of playing cellphone rules reached.
ruleEventTypeDuplicate	0x400012C8	Event type duplicated.
noMoreRetentionRulesAdded	0x400015AD	Maximum number of people retention rules reached.
noMoreSleepOnDutyRulesAdded	0x400015AE	Maximum number of sleeping on duty rules reached.
polygonNotAllowCrossing	0x400015C2	Polygons are not allowed to cross.

Sub Status Code	Error Code	Description
configureRuleBeforeAdvanceParam	0x400015F8	Advanced parameters fail to be configured as no rule is configured, please configure rule information first.
behaviorCanNotPackToPic	0x40001603	The behavior model cannot be packaged as a picture algorithm.
noCluster	0x40001608	No cluster created.
NotAssociatedWithOwnChannel	0x400019C1	Current channel is not linked.
AITargetBPCaptureFail	0x400019C5	Capturing reference picture for AI target comparison failed.
AITargetBPToDSPFail	0x400019C6	Sending reference picture to DSP for AI target comparison failed.
AITargetBPDuplicateName	0x400019C7	Duplicated name of reference picture for AI target comparison.
audioFileNameWrong	0x400019D0	Incorrect audio file name.
audioFileImportFail	0x400019D1	Importing audio file failed.
NonOperationalStandbyMachine	0x400019F0	Non-operational hot spare.
MaximumNumberOfDevices	0x400019F1	The maximum number of devices reached.
StandbyMmachineCannotBeDeleted	0x400019F2	The hot spare cannot be deleted.
alreadyRunning	0x40002026	The application program is running.
notRunning	0x40002027	The application program is stopped.
packNotFound	0x40002028	The software packet does not exist.
alreadyExist	0x40002029	The application program already exists.
noMemory	0x4000202A	Insufficient memory.
invalLicense	0x4000202B	Invalid License.
noClientCertificate	0x40002036	The client certificate is not installed.
noCACertificate	0x40002037	The CA certificate is not installed.

Sub Status Code	Error Code	Description
authenticationFailed	0x40002038	Authenticating certificate failed. Check the certificate.
clientCertificateExpired	0x40002039	The client certificate is expired.
clientCertificateRevocation	0x4000203A	The client certificate is revoked.
CACertificateExpired	0x4000203B	The CA certificate is expired.
CACertificateRevocation	0x4000203C	The CA certificate is revoked.
connectFail	0x4000203D	Connection failed.
loginNumExceedLimit	0x4000203F	No more user can log in.
HDMIResolutionIllegal	0x40002040	The HDMI video resolution cannot be larger than that of main and sub stream.
hdFormatFail	0x40002049	Formatting HDD failed.
formattingFailed	0x40002056	Formatting HDD failed.
encryptedFormattingFailed	0x40002057	Formatting encrypted HDD failed.
wrongPassword	0x40002058	Verifying password of SD card failed. Incorrect password.
audioIsPlayingPleaseWait	0x40002067	Audio is playing. Please wait.
twoWayAudioInProgressPleaseWait	0x40002068	Two-way audio in progress. Please wait.
calibrationPointNumFull	0x40002069	The maximum number of calibration points reached.
completeTheLevelCalibrationFirst	0x4000206A	The level calibration is not set.
completeTheRadarCameraCalibrationFirst	0x4000206B	The radar-camera calibration is not set.
pointsOnStraightLine	0x4000209C	Calibrating failed. The calibration points cannot be one the same line.
TValueLessThanOrEqualZero	0x4000209D	Calibration failed. The T value of the calibration points should be larger than 0.

Sub Status Code	Error Code	Description
HBDLibNumOverLimit	0x40002092	The number of human body picture libraries reaches the upper limit
theShieldRegionError	0x40002093	Saving failed. The shielded area should be the ground area where the shielded object is located.
theDetectionAreaError	0x40002094	Saving failed. The detection area should only cover the ground area.
invalidLaneLine	0x40002096	Saving failed. Invalid lane line.
enableITSFunctionOfThisChannelFirst	0x400020A2	Enable ITS function of this channel first.
noCloudStorageServer	0x400020C5	No cloud storage server
NotSupportWithVideoTask	0x400020F3	This function is not supported.
noDetectionArea	0x400050df	No detection area
armingFailed	0x40008000	Arming failed.
disarmingFailed	0x40008001	Disarming failed.
clearAlarmFailed	0x40008002	Clearing alarm failed.
bypassFailed	0x40008003	Bypass failed.
bypassRecoverFailed	0x40008004	Bypass recovery failed.
outputsOpenFailed	0x40008005	Opening relay failed.
outputsCloseFailed	0x40008006	Closing relay failed.
registerTimeOut	0x40008007	Registering timed out.
registerFailed	0x40008008	Registering failed.
addedByOtherHost	0x40008009	The peripheral is already added by other security control panel.
alreadyAdded	0x4000800A	The peripheral is already added.
armedStatus	0x4000800B	The partition is armed.
bypassStatus	0x4000800C	Bypassed.
zoneNotSupport	0x4000800D	This operation is not supported by the zone.
zoneFault	0x4000800E	The zone is in fault status.

Sub Status Code	Error Code	Description
pwdConflict	0x4000800F	Password conflicted.
audioTestEntryFailed	0x40008010	Enabling audio test mode failed.
audioTestRecoveryFailed	0x40008011	Disabling audio test mode failed.
addCardMode	0x40008012	Adding card mode.
searchMode	0x40008013	Search mode.
addRemoterMode	0x40008014	Adding keyfob mode.
registerMode	0x40008015	Registration mode.
exDevNotExist	0x40008016	The peripheral does not exist.
theNumberOfExDevLimited	0x40008017	No peripheral can be added.
sirenConfigFailed	0x40008018	Setting siren failed.
chanCannotRepeatedBinded	0x40008019	This channel is already linked by the zone.
inProgramMode	0x4000801B	The keypad is in programming mode.
inPaceTest	0x4000801C	In pacing mode.
arming	0x4000801D	Arming.
masterSlaveIsEnable	0x4000802c	The main-sub relationship has taken effect, the sub radar does not support this operation.
forceTrackNotEnabled	0x4000802d	Mandatory tracking is disabled.
isNotSupportZoneConfigByLocalArea	0x4000802e	This area does not support the zone type.
alarmLineCross	0x4000802f	Trigger lines are overlapped.
zoneDrawingOutOfRange	0x40008030	The drawn zone is out of detection range.
alarmLineDrawingOutOfRange	0x40008031	The drawn alarm trigger line is out of detection range.
hasTargetInWarningArea	0x40008032	The warning zone already contains targets. Whether to enable mandatory arming?
radarMoudleConnectFail	0x40008033	Radar module communication failed.

Sub Status Code	Error Code	Description
importCfgFilePasswordErr	0x40008034	Incorrect password for importing configuration files.
overAudioFileNumLimit	0x40008038	The number of audio files exceeds the limit.
audioFileNameIsLong	0x40008039	The audio file name is too long.
audioFormatIsWrong	0x4000803a	The audio file format is invalid.
audioFileIsLarge	0x4000803b	The size of the audio file exceeds the limit.
pircamCapTimeOut	0x4000803c	Capturing of pircam timed out.
pircamCapFail	0x4000803d	Capturing of pircam failed.
pircamIsCaping	0x4000803e	The pircam is capturing.
audioFileHasExisted	0x4000803f	The audio file already exists.
subscribeTypeErr	0x4000a016	This metadata type is not supported to be subscribed.
EISError	0x4000A01C	Electronic image stabilization failed. The smart event function is enabled.
jpegPicWithAppendDataError	0x4000A01D	Capturing the thermal graphic failed. Check if the temperature measurement parameters (emissivity, distance, reflective temperature) are configured correctly.
startAppFail	/	Starting running application program failed.
yuvconflict	/	The raw video stream conflicted.
overMaxAppNum	/	No more application program can be uploaded.
noFlash	/	Insufficient flash.
platMismatch	/	The platform mismatches.
emptyEventName	0x400015E0	Event name is empty.
sameEventName	0x400015E1	A same event name already exists.
emptyEventType	0x400015E2	Event type is required.
sameEventType	0x400015E3	A same event type already exists.
maxEventNameReached	0x400015E4	Maximum of events reached.

Sub Status Code	Error Code	Description
hotSpareNotAllowedExternalStorage	0x400015FC	External storage is not allowed when hot spare is enabled.
sameCustomProtocolName	0x400015FD	A same protocol name already exists.
maxPTZTriggerChannelReached	0x400015FE	Maximum of channels linked with PTZ reached.
POSCanotAddHolidayPlan	0x400015FF	No POS events during holidays.
eventTypeIsTooLong	0x40001600	Event type is too long.
eventNameIsTooLong	0x40001601	Event name is too long.
PerimeterEnginesNoResource	0x40001602	No more perimeter engines.
invalidProvinceCode	0x40001607	Invalid province code.

StatusCode=5

Sub Status Code	Error Code	Description
badXmlFormat	0x50000001	Invalid XML format.

StatusCode=6

Sub Status Code	Error Code	Description
badParameters	0x60000001	Invalid parameter.
badHostAddress	0x60000002	Invalid host IP address.
badXmlContent	0x60000003	Invalid XML content.
badIPv4Address	0x60000004	Invalid IPv4 address.
badIPv6Address	0x60000005	Invalid IPv6 address.
conflictIPv4Address	0x60000006	IPv4 address conflicted.
conflictIPv6Address	0x60000007	IPv6 address conflicted.
badDomainName	0x60000008	Invalid domain name.
connectSreverFail	0x60000009	Connecting to server failed.

Sub Status Code	Error Code	Description
conflictDomainName	0x6000000A	Domain name conflicted.
badPort	0x6000000B	Port number conflicted.
portError	0x6000000C	Port error.
exportErrorData	0x6000000D	Importing data failed.
badNetMask	0x6000000E	Invalid sub-net mask.
badVersion	0x6000000F	Version mismatches.
badDevType	0x60000010	Device type mismatches.
badLanguage	0x60000011	Language mismatches.
incorrentUserNameOrPassword	0x600000012	Incorrect user name or password.
invalidStoragePoolOfCloudServer	0x600000013	Invalid storage pool. The storage pool is not configured or incorrect ID.
noFreeSpaceOfStoragePool	0x600000014	Storage pool is full.
riskPassword	0x600000015	Risky password.
UnSupportCapture	0x600000016	Capturing in 4096*2160 or 3072*2048 resolution is not supported when H.264+ is enabled.
userPwdLenUnder8	0x60000023	At least two kinds of characters, including digits, letters, and symbols, should be contained in the password.
userPwdNameSame	0x60000025	Duplicated password.
userPwdNameMirror	0x60000026	The password cannot be the reverse order of user name.
beyondARGSRangeLimit	0x60000027	The parameter value is out of limit.
DetectionLineOutofDetectionRegion	0x60000085	The rule line is out of region.

Sub Status Code	Error Code	Description
DetectionRegionError	0x60000086	Rule region error. Make sure the rule region is convex polygon.
DetectionRegionOutOfCountingRegion	0x60000087	The rule region must be marked as red frame.
PedalAreaError	0x60000088	The pedal area must be in the rule region.
DetectionAreaABError	0x60000089	The detection region A and B must be in the a rule frame.
ABRegionCannotIntersect	0x6000008a	Region A and B cannot be overlapped.
customHBPIDError	0x6000008b	Incorrect ID of custom human body picture library
customHBPIDRepeat	0x6000008c	Duplicated ID of custom human body picture library
dataVersionsInHBDLibMismatches	0x6000008d	Database versions mismatches of human body picture library
invalidHBPID	0x6000008e	Invalid human body picture PID
invalidHBDID	0x6000008f	Invalid ID of human body picture library
humanLibraryError	0x60000090	Error of human body picture library
humanLibraryNumError	0x60000091	No more human body picture library can be added
humanImagesNumError	0x60000092	No more human body picture can be added
noHumanInThePicture	0x60000093	Modeling failed, no human body in the picture
analysisEnginesNoResourceError	0x60001000	No analysis engine.
analysisEnginesUsageExcced	0x60001001	The engine usage is overloaded.

Sub Status Code	Error Code	Description
PicAnalysisNoResourceError	0x60001002	No analysis engine provided for picture secondary recognition.
analysisEnginesLoadingError	0x60001003	Initializing analysis engine.
analysisEnginesAbnormaError	0x60001004	Analysis engine exception.
analysisEnginesFacelibImporting	0x60001005	Importing pictures to face picture library. Failed to edit analysis engine parameters.
analysisEnginesAssociatedChannel	0x60001006	The analysis engine is linked to channel.
smdEncodingNoResource	0x60001007	Insufficient motion detection encoding resources.
smdDecodingNoResource	0x60001008	Insufficient motion detection decoding resources.
diskError	0x60001009	HDD error.
diskFull	0x6000100a	HDD full.
facelibDataProcessing	0x6000100b	Handling face picture library data.
capturePackageFailed	0x6000100c	Capturing packet failed.
capturePackageProcessing	0x6000100d	Capturing packet.
noSupportWithPlaybackAbstract	0x6000100e	This function is not supported. Playback by video synopsis is enabled.
insufficientNetworkBandwidth	0x6000100f	Insufficient network bandwidth.
tapeLibNeedStopArchive	0x60001010	Stop the filing operation of tape library first.
identityKeyError	0x60001011	Incorrect interaction command.
identityKeyMissing	0x60001012	The interaction command is lost.
noSupportWithPersonDensityDetect	0x60001013	This function is not supported. The people density detection is enabled.

Sub Status Code	Error Code	Description
ipcResolutionOverflow	0x60001014	The configured resolution of network camera is invalid.
ipcBitrateOverflow	0x60001015	The configured bit rate of network camera is invalid.
tooGreatTimeDifference	0x60001016	Too large time difference between device and server.
noSupportWithPlayback	0x60001017	This function is not supported. Playback is enabled.
channelNoSupportWithSMD	0x60001018	This function is not supported. Motion detection is enabled.
channelNoSupportWithFD	0x60001019	This function is not supported. Face capture is enabled.
illegalPhoneNumber	0x6000101a	Invalid phone number.
illegalCertificateNumber	0x6000101b	Invalid certificate No.
linkedCameraOutLimit	0x6000101c	Connecting camera timed out.
achieveMaxChannelLimit	0x6000101e	No more channels are allowed.
humanMisInfoFilterEnabledChanNumError	0x6000101f	No more channels are allowed to enable preventing false alarm.
humanEnginesNoResource	0x60001020	Insufficient human body analysis engine resources.
taskNumberOverflow	0x60001021	No more tasks can be added.
collisionTimeOverflow	0x60001022	No more comparison duration can be configured.
invalidTaskID	0x60001023	Invalid task ID.
eventNotSupport	0x60001024	Event subscription is not supported.
invalidEZVIZSecretKey	0x60001034	Invalid verification code for Hik-Connect.
needDoubleVerification	0x60001042	Double verification required
noDoubleVerificationUser	0x60001043	No double verification user

Sub Status Code	Error Code	Description
timeSpanNumOverLimit	0x60001044	Max. number of time buckets reached
channelNumOverLimit	0x60001045	Max. number of channels reached
noSearchIDResource	0x60001046	Insufficient searchID resources
noSupportDeleteStrangerLib	0x60001051	Deleting stranger library is not supported
noSupportCreateStrangerLib	0x60001052	Creating stranger library is not supported
behaviorAnalysisRuleInfoError	0x60001053	Abnormal event detection rule parameters error.
safetyHelmetParamError	0x60001054	Hard hat parameters error.
OneChannelOnlyCanBindOneEngine	0x60001077	No more engines can be bound.
engineTypeMismatch	0x60001079	Engine type mismatched.
badUpgradePackage	0x6000107A	Invalid upgrade package.
AudioFileNameDuplicate	0x60001135	Duplicated audio file name.
CurrentAudioFileAIRuleInUseAlreadyDelete	0x60001136	The AI rule linkage related to current audio file has been deleted.
TransitionUseEmmc	0x60002000	Starting device failed. The EMMC is overused.
AdaptiveStreamNotEnabled	0x60002001	The stream self-adaptive function is not enabled.
AdaptiveStreamAndVariableBitrateEnabled	0x60002002	Stream self-adptive and variable bitrate function cannot be enabled at the same time.
noSafetyHelmetRegion	0x60002023	The hard hat detection area is not configured (if users save their settings without configuring the arming area, they should be prompted to configure one).

Sub Status Code	Error Code	Description
unclosedSafetyHelmet	0x60002024	The hard hat detection is enabled (If users save their settings after deleting the arming area, they should be prompted to disable hard hat detection first and then delete the arming area).
width/ heightRatioOfPictureError	0x6000202C	The width/height ratio of the uploaded picture should be in the range from 1:2 to 2:1.
PTZNotInitialized	0x6000202E	PTZ is not initialized.
PTZSelfChecking	0x6000202F	PTZ is self-checking.
PTZLocked	0x60002030	PTZ is locked.
advancedParametersError	0x60002031	Auto-switch interval in advanced parameters cannot be shorter than parking tolerance for illegal parking detection in speed dome rule settings.
resolutionError	0x60005003	Invalid resolution
deployExceedMax	0x60006018	The arming connections exceed the maximum number.
detectorTypeMismatch	0x60008000	The detector type mismatched.
nameExist	0x60008001	The name already exists.
uploadImageSizeError	0x60008016	The size of the uploaded picture is larger than 5 MB.
laneAndRegionOverlap	/	The lanes are overlapped.
unitConfigurationNotInEffect	/	Invalid unit parameter.
ruleAndShieldingMaskConflict	/	The line-rule region overlaps with the shielded area.
wholeRuleInShieldingMask	/	There are complete temperature measurement rules in the shielded area.

Sub Status Code	Error Code	Description
LogDiskNotSetReadOnlyInGroupMode	0x60001100	The log HDD in the HDD group cannot be set to read-only.
LogDiskNotSetReDundancyInGroupMode	0x60001101	The log HDD in the HDD group cannot be set to redundancy.
holidayNameContainChineseOrSpecialChar	0x60001080	No Chinese and special characters allowed in holiday name.
genderValueError	0x60001081	Invalid gender.
certificateTypeValueError	0x60001082	Invalid identification type.
personInfoExtendValueIsTooLong	0x60001083	The length of customized tags exceeds limit.
personInfoExtendValueContainsInvalidChar	0x60001084	Invalid characters are not allowed in customized tags of the face picture library.
excelHeaderError	0x60001085	Excel header error.
intelligentTrafficMutexWithHighFrames	0x60008014	Please disable all functions of traffic incident detection, violation enforcement, and traffic data collection, or adjust the video frame rate to that lower than 50 fps.
intelligentTrafficMutexWithHighFramesEx	0x60008018	Please disable all functions of traffic incident detection, violation enforcement, traffic data collection, and vehicle detection, or adjust the video frame rate to that lower than 50 fps.

StatusCode=7

SubStatusCode	Error Code	Description
rebootRequired	0x70000001	Reboot to take effect.

A.7 Error Codes Categorized by Functional Modules

The error codes returned during the text protocol integration is categorized by different functional modules. See the error codes, error descriptions, and debugging suggestions in the table below.

Public Function Module (Error Codes Range: 0x00000000, from 0x00100001 to 0x001fffff)

Error String	Error Code	Description	Debugging Suggestion
success	0x00000000	Succeeded.	
deviceNotActivated	0x00100001	The device is not activated.	Activate the device.
deviceNoPermission	0x00100002	Device operation failed. No permission.	Update user's permission.
deviceNotSupport	0x00100003	This function is not supported.	Check the device capability set and call the API corresponding to supported function.
deviceResourceNotEnough	0x00100004	Insufficient resources.	Release resources.
dataFormatError	0x00100005	Invalid message format.	
resetError	0x00100006	Restoring to factory settings failed. Reactivating device is required after the device is reboot as the Reset button may be stuck.	
parameterError	0x00100007	Incorrect parameter	
	0x00100100	Invalid channel	Check if the channel is valid.
	0x00100101	NPQ live view is not supported for stream encryption.	Replace streaming mode for stream encryption.
	0x00100102	No more channels are allowed for NPQ streaming.	Reduce NPQ streaming channels and try again.
	0x00100103	The stream type is not supported.	Check the requested stream type.

Error String	Error Code	Description	Debugging Suggestion
	0x00100104	The number of connections exceeded limit.	Reduce the number of streaming clients and try again.
	0x00100105	Not enough bandwidth.	Reduce the number of remote streaming channels.

User Function Module (Error Codes Range: from 0x00200001 to 0x002fffff)

Error String	Error Code	Description	Debugging Suggestion
passwordError	0x00200001	Incorrect user name or password.	Check if the password is correct.
userNameNotExist	0x00200002	The account does not exist.	Check if the account exists, or add the account.
userNameLocked	0x00200003	The account is locked.	Wait for the device to unlock.
userNumLimited	0x00200004	The number of users allowed to log in exceeded the upper limit.	Log out.
lowPrivilege	0x00200005	No permissions for this operation	For users operations, check the following situations: • Deleting your own account is not allowed. • Editing your own level or permission is not allowed. • Getting information about users with higher permission is not allowed. • Elevating the user's level or permission is not allowed. For other operations, check according to the following measures: If operations unrelated to user's permission configuration failed, you can check the user type and permission, if not solved, contact the developers.

Error String	Error Code	Description	Debugging Suggestion
incorrentUserNameOrPassword	0x00200006	Incorrect user name or password	Check if the configured user name and password are matched. If not, contact the administrator to configure again. If the administrator forgets the password, reset the password of the device.
riskPassword	0x00200007	Risk password	Low password strength. Change password again.
passwordMustContainMorethan8Characters	0x00200008	The password length must be greater than or equal to 8.	Check if the password length is greater than or equal to 8. If not, change password again.
passwordLenNoMoreThan16	0x00200009	The password length cannot be greater than 16.	Check if the password length is greater than16. If yes, change password again.
adminUserNotAllowedModify	0x0020000a	Editing admin information is not allowed.	Check if the edited account is admin.
confirmPasswordError	0x0020000b	Incorrect confirm password.	Check the confirm password.
passwordMustContainMorethan2Types	0x0020000c	The password must contain at least two or more of followings: numbers, lowercase, uppercase, and special characters.	Check if the configured password conforms the requirements.
passwordContainUserName	0x0020000d	The password cannot contain the user name.	Check if the password contains the user name.
userPwdNameMirror	0x0020000e	The password cannot be reversed user name.	Check if the password is reversed user name.

Time Function Module (Error Codes Range: from 0x00300001 to 0x003fffff)

Error String	Error Code	Description	Debugging Suggestion
manualAdjustmentFailed	0x00300001	Time synchronization failed.	
NTPError	0x00300002	Invalid NTP server address.	Check if the NTP server address is valid.
timeFormatError	0x00300003	Incorrect time format during time calibration. For example, the time in ISO 8601 format should be "2018-02-01T19:54:04", but the applied time is "2018-02-01 19:54:04".	Incorrect message format or incorrect time format.
beyondTimeRangeLimit	0x00300004	The calibration time is not within the time range supported by the device.	Get the device capability and check if the configured time is within the time range supported by the device.
endtimeEarlierThanBegintime	0x00300005	The start time of the validity period cannot be later than the end time.	Check if the start time and end time are valid.

Network Function Module (Error Codes Range: from 0x00400001 to 0x004fffff)

Error String	Error Code	Description	Debugging Suggestion
domainNameParseFailed	0x00400001	Parsing domain name failed.	
PPPOEConnectedFailed	0x00400002	Connecting PPPOE to the network failed.	
FTPConnectedFailed	0x00400003	The FTP server is disconnected.	
deviceIPConflicted	0x00400004	IP addresses of devices conflicted.	
libraryConnectedFailed	0x00400005	The image and video library is disconnected.	

Error String	Error Code	Description	Debugging Suggestion
fileUploadFailed	0x00400006	Uploading failed.	Check if the network connection is normal. If yes, contact after-sales.
storSerDownloadFileFailed	0x00400007	Downloading failed.	Check if the network connection is normal. If yes, contact after-sales.
storSerDownloadFileSizeZero	0x00400008	The size of file downloaded from the storage service is 0.	Check if the network connection is normal. If yes, contact after-sales.
storSerNotConfig	0x00400009	Storage service is not configured.	Check if the configuration is correct.
badHostAddress	0x0040000a	Host address error	Check if the configuration is correct.
badIPv4Address	0x0040000b	Incorrect IPv4 address.	Check if the configuration is correct.
badIPv6Address	0x0040000c	Incorrect IPv6 address.	Check if the configuration is correct.
conflictIPv4Address	0x0040000d	IPv4 address conflict.	Check the configuration status of IPV4 in the network.
conflictIPv6Address	0x0040000e	IPv6 address conflict	Check the configuration status of IPV6 in the network.
badDomainName	0x0040000f	Incorrect domain name.	Check if the configuration is correct.
connectSreverFail	0x00400010	Connecting to server failed.	Check if the network is normal and check if the configuration is correct.
conflictDomainName	0x00400011	Domain name conflict.	Check if the configuration is correct.
badPort	0x00400012	Port conflict.	Check if the configuration is correct.
portError	0x00400013	Port error	Check if the configuration is correct.

Error String	Error Code	Description	Debugging Suggestion
badNetMask	0x00400014	Subnet mask error	Check if the configuration is correct.
badVersion	0x00400015	Version mismatch	Check if the version is correct.
badDns	0x00400016	DNS error	Check if the configuration is correct.
badMTU	0x00400017	MTU error	Check if the configuration is correct.
badGateway	0x00400018	Wrong gateway	Check if the configuration is correct.
urlDownloadFail	0x00400019	Downloading via URL failed.	Check if the network is normal and check if the URL is correct.
deployExceedMax	0x0040001a	The number of armed channels exceeds the maximum number of connections.	Get the supported maximum number of arming and the number of armed channels.

Maintenance Function Module (Error Codes Range: from 0x00500001 to 0x005fffff)

Error String	Error Code	Description	Debugging Suggestion
upgradeXMLFormatError	0x00500001	Incorrect XML upgrading request.	Check if the upgrade file is correct. If the file is correct, try the local upgrade.
upgradeContentError	0x00500002	Incorrect upgrading request content.	Check if the upgrade file is correct. If the file is correct, try the local upgrade.
noUpgradePermision	0x00500003	No upgrade permission.	Switch to admin account or ask admin for advanced operation permission.
upgrading	0x00500004	Upgrading…	Wait for the upgrade to complete.
receiveUpgradePackageError	0x00500005	Receiving upgrade package failed.	Check if the network is normal.

Error String	Error Code	Description	Debugging Suggestion
upgradePackageLanguageMismatch	0x00500006	Upgrade package language mismatch.	Check the language type of upgrade package and the device.
upgradePackageMismatch	0x00500007	Upgrade file does not match with the device type.	Check the type of upgrade package and device.
OEMCodeMismatch	0x00500008	Upgrade package error. The OEM code mismatch.	Contact after-sales to get the correct upgrade package.
versionMismatch	0x00500009	Upgrade file version mismatch.	Contact after-sales to get the correct upgrade package.
upgradeHalfFailed	0x0050000c	Error occurred in the halfway of device upgrading. Flash error or cache error.	
deviceParameterImportFailed	0x0050000d	Importing device parameters failed. Device model, version, or platform mismatches.	
deviceEncryptionError	0x0050000e	Upgrade package mismatches. Device encryption error.	
SDCardFormatError	0x00500025	Formatting SD card failed.	
SDCardLoadFailed	0x00500026	Loading page failed after the SD card is inserted.	
NASFailed	0x00500027	Mounting NAS failed.	
hardDiskError	0x00500028	HDD exception (possible reasons: HDD does not exist, incompatible, encrypted, insufficient capacity, formatting exception, array exception, array incompatible, etc.)	
upgradeError	0x00500030	Upgrade error	

Error String	Error Code	Description	Debugging Suggestion
upgradePackageSizeMismath	0x00500032	Mismatch between the actual size of the downloaded upgrade package and the size in the upgrading request.	
upgradePackageSizeExceeded	0x00500033	The size of the package exceeded that of the partition.	
domainNameParseFailedForDownload	0x00500034	Parsing the domain name of the address for downloading failed.	
netWorkUnstable	0x00500035	Unstable network. Downloading timed out or the maximum number of attempts reached.	
digestValueMismatch	0x00500036	Mismatched digest value.	
signatureVerifyFailed	0x00500037	Verifying the signature failed.	
innerFormatError	0x00500038	Incorrect inner format of the upgrade package.	
memoryNotEnough	0x00500039	Insufficient memory.	
burnFailed	0x0050003a	Burning firmware failed.	
unknownError	0x0050003b	Unknown error occurred in the underlying APIs.	
userCancel	0x0050003c	User requested cancel of current operation.	
systemResume	0x0050003d	Upgrading failed. You can resume via the backup system or minimum system.	
	0x00500080	Upgrade file is not found.	Check if the upgrade package path is too long or if there is a correct upgrade

Error String	Error Code	Description	Debugging Suggestion
			package under the upgrade package path.
	0x00500081	Upgrade file does not match with the engine type.	Select the upgrade package matched with the device engine type.
	0x00500082	Parsing camera domain name failed.	Confirm if the device is correctly configured DNS service and if the camera domain is valid.
	0x00500083	Camera network is unreachable.	Confirm if the local network can access the network where the added channel located.

Live View Module (Error Codes Range: from 0x00600001 to 0x006fffff)

Error String	Error Code	Description	Debugging Suggestion
liveViewFailed	0x00600001	Live view failed. The number of streaming channels exceeded limit.	
	0x00600002	Request packaging format exception.	Check the packaging format of requested live view.
	0x00600003	NPQ will be unavailable after enabling EHome 2.x.	When EHome 2.x is enable, use other live view mode.
	0x00600005	NPQ live view is not supported for channel-zero.	User other live view mode for channel-zero.
	0x00600007	Only virtual stream supports NPQ live view.	Switch to virtual strem.
	0x0060000A	The IP channel is offline.	Check if the IP channel is online and try again.
	0x0060000B	Live view transcoding is not supported by the device.	Use other stream type for live view.
	0x0060000C	Channel-zero is not enabled.	Enable channel-zero before starting live view of channel-zero.

Error String	Error Code	Description	Debugging Suggestion
	0x0060000D	Transcoding capability exceeded limit.	Reduce camera resolution or the number of transcoding channels.
	0x00600010	The channel does not have sub-stream.	Use main stream mode for live view.
	0x00600011	NPQ live view is not supported by the device.	Switch to other live view mode.
	0x00600012	NPQ function is disabled.	Enable NPQ function or switch to other live view mode.

Playback Module (Error Codes Range: from 0x00700001 to 0x007fffff)

Error String	Error Code	Description	Debugging Suggestion
	0x00700001	Playback failed. Up to one channel's playback is supported.	
	0x00700002	The speed of playback displayed on video wall is not supported.	Reduce the playback speed.
	0x00700003	The transmission rate of playback stream is too high.	Reduce the transmission rate of playback stream.
	0x00700004	The encoding type of playback stream is not supported.	Provide the stream with encoding type supported by device.
	0x00700005	The container format of playback stream is not supported.	Provide the stream with container format supported by device.
	0x00700007	Exception occurred when decoding playback stream Possible reasons: displaying on video wall exception, image exception, display exception, decoding exception, image is stuck,	

Error String	Error Code	Description	Debugging Suggestion
		black screen, invalid stream type, live view is stuck, audio decoding exception, and blurred screen.	
	0x00700008	Playback video does not exit, or searching failed.	Search again or check if HDD is normal.
	0x00700009	Playback time parameter error.	Check if the time period of searched video is correct and try again.
	0x0070000A	Invalid video type.	Select the correct video type to search.
	0x0070000B	Invalid time type.	Select the correct time type to search.
	0x0070000C	Invalid event parameter.	Select the correct event parameter to search.
	0x0070000D	Invalid event type.	Select the correct event type to search.
	0x0070000E	The device does not support smart search.	Select the non smart search mode to search.
	0x0070000F	Invalid smart event type.	Select the correct smart event type to search.
	0x00700010	Invalid dynamic analysis sensitivity.	Select the correct sensitivity to search video.
	0x00700011	Reverse playback is not supported.	Select the correct playback mode.
	0x00700012	Invalid file status.	Select the correct file status to search.
	0x00700013	Invalid searching start position.	Use the correct searching start position to search.
	0x00700014	Invalid maximum number of searching.	Use the correct maximum number of searching to search.

Capture Module (Error Codes Range: from 0x00800001 to 0x008fffff)

Error String	Error Code	Description	Debugging Suggestion
	0x00800001	Manual capture failed.	

Two-Way Audio Module (Error Codes Range: from 0x00900001 to 0x009fffff)

Error String	Error Code	Description	Debugging Suggestion
startFailed	0x00900001	Starting two-way audio failed. Audio loss or driver error.	
codingFormatNotMatch	0x00900002	The encoding format of the intercom is inconsistent, and the negotiation fails	Check or capture the packets on the platform, then analyze if the audio encoding formats negotiated by both sides are consistent.
dialedIsBusy	0x00900003	The intercom party is already in the intercom and can no longer respond to the intercom	Check if the intercom party is already in the intercom, if not, get the protocol message and analyze the response message.
destinationLongNumberError	0x00900004	The requested destination long number is wrong	Check or capture the packets on the platform, then analyze the long number.

Video Storage Module (Error Codes Range: from 0x00a00001 to 0x00afffff)

Error String	Error Code	Description	Debugging Suggestion
videoSearchFailed	0x00a00001	Searching videos failed.	No resource stored in the device.
notFindStorageMedium	0x00a00002	No storage medium found.	
videoDownloadFailed	0x00a00003	Downloading videos failed.	

Picture Storage Module (Error Codes Range: from 0x00b00001 to 0x00bfffff)

Error String	Error Code	Description	Debugging Suggestion
	0x00b00001	Searching pictures failed.	No picture resource.

IO Function Modele (Error Codes Range: from 0x00c00001 to 0x00cfffff)

Error String	Error Code	Description	Debugging Suggestion
	0x00c00001	Invalid alarm input No.	
	0x00c00002	Invalid alarm output No.	

Event Function Module (Error Codes Range: from 0x00d00001 to 0x00dfffff)

Error String	Error Code	Description	Debugging Suggestion
	0x00d00001	Incorrect event rule.	Refer to the manual for correct configuration.

Parking Service Module (Error Codes Range: from 0x00e00001 to 0x00efffff)

Error String	Error Code	Description	Debugging Suggestion
	0x00e00001	The vehicle with parking pass already exists.	Parking pass is created by license plate, you need to check if the parking pass for this license plate already created.
	0x00e00002	The license plate number is required.	

General Function Module (Error Codes Range: from 0x00f00001 to 0x00ffffff)

Error String	Error Code	Description	Debugging Suggestion
noMemory	0x00f00001	Insufficient device memory (heap space allocation failed).	Check the free memory and send logs to the developer for analysis.
deviceBusy	0x00f00002	The device is busy or the device is not responding.	Send logs to the developers for analysis.

Error String	Error Code	Description	Debugging Suggestion
			For fingerprint collection, face collection, file application, and file uploading services, check if the last operation is completed.
notSupport	0x00f00003	The URL is not supported by the device.	Capture the packets, check if the applied URL exists in the PMP platform. If yes, send the URL to the developer for analysis.
methodNotAllowed	0x00f00004	HTTP method is not allowed.	Capture the packets, check the method corresponding to the URL in the PMP platform.
invalidOperation	0x00f00005	Invalid operation of API command.	
IDNotexist	0x00f00006	The ID does not exist (the URL should contain ID, but the actual URL does not contain the ID).	Capture the packets and check if the ID included in the URL is correct.
invalidID	0x00f00007	Invalid ID (the ID in the URL exceeds the capability set or the ID format is invalid).	Capture the packets and check if the ID included in the URL is correct. Get the capabilities of URL and check the ID range.
invalidIURL	0x00f00008	The content after the "? " in the URL is wrong.	Capture the packets and check if the URL is correct.
deviceAckTimeOut	0x00f00009	Device response timed out.	If the communication with the external module timed out, check if the external module is offline. When the above situation is eliminated, send logs to the developer for analysis.
badXmlFormat	0x00f0000a	XML format error	

Error String	Error Code	Description	Debugging Suggestion
badJsonFormat	0x00f0000b	JSON format error	
badURLFormat	0x00f0000c	URL format error	Get the URL and check if it is correct.
badXmlContent	0x00f0000d	XML message error: • The message contains only URL but no message body • The required node is not configured. • Node value exceeds the range limit (incorrect node value).	
badJsonContent	0x00f0000e	JSON message error: • The message contains only URL but no message body • The required node is not configured. • Node value exceeds the range limit (incorrect node value).	
messageParametersLack	0x00f0000f	The required node does not exists.	
invalidSearchConditions	0x00f00010	Invalid search condition, search again.	Check if searchID is correct.
operObjectNotExist	0x00f00011	The object does not exist (for the operations about door, alarm IO, the object is not added).	Check if door lock is connected.

Door Control Module (Error Codes Range: from 0x01000001 to 0x010fffff)

Error String	Error Code	Description	Debugging Suggestion
multiAuthentication Failed	0x01000001	Multi-factor authentication status operation failed.	
securityModuleOffline	0x01000002	The safety door control module is offline and fails to open the door.	Check if the safety door control is offline.

Schedule Template Module (Error Codes Range: from 0x01100001 to 0x011fffff)

Error String	Error Code	Description	Debugging Suggestion
planNumberConflict	0x01100001	Plan number conflict.	
timeOverlap	0x01100002	Time period conflict.	Check the message to find out if there is a time overlap of different time periods in one day.

Person Information Module (Error Codes Range: from 0x01200001 to 0x012fffff)

Error String	Error Code	Description	Debugging Suggestion

Certificate Module (Error Codes Range: from 0x01300001 to 0x013fffff)

Error String	Error Code	Description	Debugging Suggestion

Security Function Module (Error Codes Range: from 0x01400001 to 0x014fffff)

Error String	Error Code	Description	Debugging Suggestion
decryptFailed	0x01400001	Decryption failed, when decrypting sensitive	The import secret key should be consistent with the export.

Error String	Error Code	Description	Debugging Suggestion
		information fields or importing data files.	
certificateNotmatch	0x01400003	Certificates mismatched, SSL/TLS public and private keys need to be matched in pairs.	The public and private keys need to be generated at the same time.
notActivated	0x01400004	Device is not activated.	Activate the device by tools such as SADP before use.
hasActivated	0x01400005	Device has been activated.	
forbiddenIP	0x01400006	IP address is banned	IP address is banned when illegal login attempts exceed the upper limit.
bondMacAddressNotMatch	0x01400007	The MAC address does not match the user.	Check if the specific MAC address has linked to the user.
bondIpAddressNotMatch	0x01400008	IP address does not match the user.	Check if the specific IP address has linked to the user.
badAuthorization	0x01400009	Triggered by illegal login	Incorrect password triggered the illegal login.

Advertising Function Module (Error Codes Range: from 0x01500001 to 0x015fffff)

Error String	Error Code	Description	Debugging Suggestion
materialDownloadFailed	0x01500001	Material download failed.	• Check if the network connection is normal. • Check if the device is running normally. • Check the log print.
materialNumberIsOver	0x01500002	The number of materials in the program list reached the upper limit.	Check if the number of materials in applied program list exceeded the limit.

See Far, Go Further

UD34756B