IVI Service Layer Interface Specification – Persistent Connection Service

Prepared by

Ford Motor Company

Contributor

Team Janus

|  |  |  |  |
| --- | --- | --- | --- |
| REVISION HISTORY | | | |
| Version | Date | Name | Comment |
| 0.1 | 29-Dec-2021 | SHAN17 |  |
| 0.2 | 6-Jan-2022 | SHAN17 | Changed contents of API02 and API03 |
| 0.3 | 6-Jan-2022 | JPEI2 | Updated wording |
| 0.4 | 11-Feb-2022 | JPEI2 | Updated message API |
| 0.5 | 14-Feb-2022 | JPEI2 | Updated API01 request sample to align with GET method request;  Added new filed in message API;  Added new code 130606 and 130607 |
| 0.6 | 24-Feb-2022 | JPEI2 | Removed appId in API02, use application id in header to identify which key should be used.  Removed signature example which is not applicable for IVISL API；  Corrrected typo |
| 0.7 | 4-Mar-2022 | JPEI2 | Added nonce in API02;  Corrected request sample in API02 |
| 0.8 | 30-Mar-2022 | JLIU280 | [Add pcs notification Internal router api](#internal_router_notificaion_api) |

|  |  |  |  |
| --- | --- | --- | --- |
| ABBREVIATE TABLE | |  |  |
| IVI | In-Vehicle Infotainment | |  |
| IVT | In-Vehicle Token | |  |
| APIM | Azure API Manager | |  |

Contents

[1 Introduction 2](#_Toc100761277)

[2 Security 3](#_Toc100761278)

[2.1 Request Headers 3](#_Toc100761279)

[2.1.1 Request from IVI 3](#_Toc100761280)

[2.1.2 Request from Cloud System 3](#_Toc100761281)

[2.2 Payload Encryption 3](#_Toc100761282)

[2.2.1 Request from IVI 3](#_Toc100761283)

[2.2.2 Request from Cloud 5](#_Toc100761284)

[2.3 Request Signature 5](#_Toc100761285)

[2.3.1 Request from IVI 5](#_Toc100761286)

[2.3.2 Request from Cloud 6](#_Toc100761287)

[3 Implementation 8](#_Toc100761288)

[4 Interface Matrix 9](#_Toc100761289)

[5 API Specifications(APIM) 10](#_Toc100761290)

[5.1 API01 – Get MQTT Connection String 10](#_Toc100761291)

[Attributes 10](#_Toc100761292)

[Requests 10](#_Toc100761293)

[Request Sample 11](#_Toc100761294)

[Response 12](#_Toc100761295)

[Response Sample 12](#_Toc100761296)

[5.2 API02 – Send Message to IVI Device via Azure IoT Hub 13](#_Toc100761297)

[Attributes 13](#_Toc100761298)

[Requests 14](#_Toc100761299)

[Request Sample 16](#_Toc100761300)

[Response 16](#_Toc100761301)

[Response Sample 17](#_Toc100761302)

[6 API Specifications(Internal Router) 18](#_Toc100761303)

[6.1 API01 – Send Message to IVI Device via Azure IoT Hub 18](#_Toc100761304)

[Attributes 18](#_Toc100761305)

[Requests 18](#_Toc100761306)

[Request Data Sample 21](#_Toc100761307)

[Response 21](#_Toc100761308)

[Response Sample 21](#_Toc100761309)

[7 Staus Code 22](#_Toc100761310)

[7.1 HTTP Status Code 22](#_Toc100761311)

[7.2 Application Status Codes 23](#_Toc100761312)

[7.3 Exception Layout 25](#_Toc100761313)

[Response 25](#_Toc100761314)

[Response Sample 25](#_Toc100761315)

1. Introduction

This document describes the interfaces exposed by IVI Service Layer Persistent Connection Service.

1. Security

This section of the document explains the security mechanisms.

* 1. Request Headers
     1. Request from IVI

In addition, ***Application-Id, Platform-Id, Device-Id*** are all required in Http Header for API communication with all services provided by IVI Service Layer.

***Application-Id*** is an ID to identify an application in Ford ecosystem. The client system/app need to register the system/app following Ford standard process to get a unique Application-ID.

***Platform-Id*** is an ID provided by IVI Service Layer to identify the platform client application runs on.

***Device-Id*** is a unique value assigned to individual IVI device during the IVI device’s onboarding process.

* + 1. Request from Cloud System

***Application-Id, Authorization*** are all required in Http Header for API exposed by IVI Service Layer for Backend systems.

***Application-Id*** is an ID to identify an application in Ford ecosystem. The client system/app need to register the system/app following Ford standard process to get a unique Application-ID.

***Authorizatoin*** is Authorization token value issued by Microsoft Azure AD.

* 1. Payload Encryption
     1. Request from IVI

During IVI app deployment stage, an app based secret is embedded in app. This secret will be used along with other device info for first time device registration.

Unique **DeviceID** and **DeviceSecret** will be assigned to individual IVI device during the process. DeviceID and DeviceSecret will be used in the communication with other services provided by IVI Service Layer.

A common AES encryption pattern will be followed in various request and response scenarios.

1. AES Key: to be defined in each request
2. Cipher mode: **CBC**
3. IV: Take **first 16 bytes** of AES Key and **reverse it** to get IV
4. Padding: **PKCS5**
5. Data: content to be defined in each request. NOTE: If data size is larger than **$BLOCKSIZE bytes**, it will be cut into pieces of **$BLOCKSIZE** bytes or shorter, encrypted separately then joined together. For Phase1-3 vehicles, **$BLOCKSIZE=896**; for phase4+ vehicles, **$BLOCKSIZE=240.**
6. Encoding: default to **BASE64**, except when it’s clearly defined in request otherwise

Below is an example encrypt/decrypt util class written in Java.

### $BLOCKSIZE differ between Sync+ Phase1-3 and Phase4+. For Phase 1-3, $BLOCKSIZE=896; for phase4+, $BLOCKSIZE=240

public class AesTools {

    private static final int TEE\_ENCRYPT\_SYM\_LARGE = $BLOCKSIZE;

    private static final int TEE\_DECRYPT\_SYM\_LARGE = $BLOCKSIZE + 16;

    private volatile static AesTools newInstance = null;

    private AesTools() {

    }

    public static AesTools getInstance() {

        if (newInstance == null) {

            synchronized (AesTools.class) {

                if (newInstance == null) {

                    newInstance = new AesTools();

                }

            }

        }

        return newInstance;

    }

    /\*\*

     \*

     \* @param key AES key

     \* @param mode mode 1 is encrypt;2 is decrypt

     \* @param plain plain or encryptedData

     \* @return byte[] encryptedData or plain

     \*/

    public byte[] aesSymCopy(String key,int mode, byte[] plain) {

        if (key == null || key.length() % 16 != 0) {

            System.out.println("key error return null");

            return null;

        };

        byte[] iv = new byte[16];

        for (int i = 0; i < iv.length; ++i) {

            iv[i] = key.getBytes()[iv.length() - 1 - i];

        }

        int modeTee = (mode == 1) ? TEE\_ENCRYPT\_SYM\_LARGE : TEE\_DECRYPT\_SYM\_LARGE;

        if (plain.length <= modeTee) {

            return aesTool(key, mode, iv, plain);

        } else {

            byte[] buffer = null;

            byte[] blockBytes;

            int index = ((plain.length - 1) / modeTee) + 1;

            for (int i = 0; i < index; i++) {

                int startIndex = i \* modeTee;

                int endIndex = startIndex + modeTee;

                blockBytes = subBytes(plain, startIndex,

                        Math.min(endIndex, plain.length) - startIndex);

                if (buffer == null) {

                    buffer = aesTool(key, mode, iv, blockBytes);

                    if (buffer == null) {

                        throw new RuntimeException("encryptSymForLarge加密失败");

                    }

                } else {

                    buffer = addAllByte(buffer, aesTool(key, mode, iv, blockBytes));

                }

            }

            return buffer;

        }

    }

    private byte[] aesTool(String key, int mode, byte[] iv, byte[] bytes) {

        byte[] encryptedData = null;

        try {

            javax.crypto.Cipher cipher = javax.crypto.Cipher

                    .getInstance("AES/CBC/PKCS5Padding");

            cipher.init(mode,

                    new SecretKeySpec(key.getBytes(), "AES"),

                    new IvParameterSpec(iv));

            encryptedData = cipher.doFinal(bytes);

        } catch (Exception e) {

            // TODO: handle exception

            System.out.println("error return null");

        }

        return encryptedData;

    }

    private static byte[] addAllByte(byte[] orig, byte[] newAdd) {

        byte[] result = new byte[orig.length + newAdd.length];

        System.arraycopy(orig, 0, result, 0, orig.length);

        System.arraycopy(newAdd, 0, result, orig.length, newAdd.length);

        return result;

    }

    private static byte[] subBytes(byte[] src, int begin, int count) {

        byte[] bs = new byte[count];

        System.arraycopy(src, begin, bs, 0, count);

        return bs;

    }

}

* + 1. Request from Cloud

The encryption is based on AES256. The encryption key is appsecure and the encryption format is AES256.Encode (aesKey, content). aesKey and detailed encryption method will be communicated offline.

* 1. Request Signature
     1. Request from IVI

Request signature is required in specific APIs to prevent data tampering during transmission.

The whole picture looks like:

Note: for HTTP GET method, replate RequestBody with RequestParam

Base64(

SHA256(

AscendingOrder(RequestHeaderPart) + "." +

RequestURL + "." +

AscendingOrder(RequestBody) + "."

last16Digit(DeviceSecret)

)

)

Follow steps below to generate signature of a request.

Example Request URL:

/api/ivisl/app-router/v1/f/s-feedback/fdid00000000001/audio

Example Request body:

{

"param":"enctryptedstring",

"values":"base64encodingstring",

    "nonce":"123",

    "timestamp":"1570703617000"

}

1. Take request headers: Application-Id, Platform-Id, Device-Id, Token, Open-Id, then sort keys with **ascending** order

Application-Id=newapplication, Device-Id=999, Open-Id=777, Platform-Id=p01, Token=

1. Take values of each k-v pair and combine them into one string, empty if no value for that header

newapplication999777p01

1. Take request URL path string and append it to header value string with a dot ‘.’  
   newapplication999777p01./api/ivisl/app-router/v1/f/s-feedback/fdid00000000001/audio
2. Take raw request body(for GET method, take request param) except sign and file, then sort keys with **ascending** order

*nonce=123, param=encryptedstring, timestamp=1570703617000, values=base64encodingstring*

1. Take values of each k-v pair and combine them into one string

*123encryptedstring1570703617000base64encodingstring*

1. Append request body values string with a dot ‘.’

newapplication999777p01./api/ivisl/app-router/v1/f/s-feedback/fdid00000000001/audio. *123encryptedstring1570703617000base64encodingstring*

1. Take **last 16 characters** of **SHA256 HEX encoded DeviceSecret** (for example, 6088b8b6a2119acc4ebc2df13a97d5d49af71eed12643fcf275c48fb19133f24)

*275c48fb19133f24*

1. Combine both strings to *stringbeforehash with a dot* ‘.’

newapplication999777p01./api/ivisl/app-router/v1/f/s-feedback/fdid00000000001/audio. *123encryptedstring1570703617000base64encodingstring.275c48fb19133f24*

1. Hash *stringbeforehash* using **SHA256 with BASE64 encoding** to get signature.

*X23Q3gz7mY8QBOR7arfX0RksNpVDoW5hzVIW6pGVhRw*

* + 1. Request from Cloud

**Signture format：**

Signature = SHA256 {AppSecret2 + Alphabetical [Payload Parms + AppKey + Timestamp] +AppSecret }

AppSecret2= URL Encode{SHA256{SHA256{Current Date:(**timezone:GMT+8**)}+AppSecret3}}

AppKey: To be shared

AppSecret3: To be shared

AppSecret: To be shared

Detailed sign method will be communicated offline.

1. Implementation

|  |  |
| --- | --- |
| Description | Provides a standard set Application Services for IVI apps to consume |
| Integration Methods | Public Restful API |
| Technology | Java API |
| Implementation | The IVISL services will be a Web API implemented in Java and hosted in PCF.  Requests to the API will be sent over HTTPS.  Client applications ­­will need to pass their Authorization token on every call so the Web API can validate the caller.  Client applications will be sent to the API using the methods Restful endpoint with JSON format  Responses from the Services will be returned as JSON format containing status code and response data which defined in this document. |
| HTTP Headers | All requests need to contain the following headers.  Content-Type : application/json; char-set=utf-8  Accept : application/json; char-set=utf-8  **Please refer to section 2.1 for more header details.** |
| Query String Arguments | All query string arguments need to be URL encoded. Example  lrdt=12-21-2014%2010%3A01%3A50%20AM |

1. Interface Matrix

Below table summarize all APIs provided by IVI Service Layer

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **API name** | **API behavior** | **Comsumer** |
| API01 | Get mqtt connection string | Get mqtt connection string which can be used to connect Azure IoT Hub | IVI |
| API02 | Send message | Send message to Azure IoT Hub | Cloud System |

1. API Specifications(APIM)

This section documents the APIs hosted by IVI Service Layer

**API Domain:**

Stage: https://stgcn.api.mps.ford.com.cn

Production: https://cn.api.mps.ford.com.cn

* 1. API01 – Get MQTT Connection String

This API is used to retrieved MQTT connection string, which is used to connect Azure IoT Hub via MQTT protocol.

Attributes

|  |  |
| --- | --- |
| URL | /api/ivisl/app-router/v1/d/s-pcs/connection |
| HTTP Method | GET |
| Security Access | Authenticated Calls Only |
| Call Type | Synchronous |

Requests

Additional package data is required.

| Field | Type | Description | In | Condition | Example |
| --- | --- | --- | --- | --- | --- |
| param | String | Encrypted request json payload, refer to [section 2.2.1 Payload Encryption](#Payload_Encryption) | Param | Required |  |
| nonce | String | A random string generated for each request, 16 bytes max | Param | Required | 1570703617000abc |
| timestamp | Long | Current system time in epoch ms format | Param | Required | 1570703617000 |
| sign | String | Signature of request, refer to [section 2.3.1 Request Signature](#Request_Signature) | Param | Required |  |

param raw data fields is

| Field | Type | Description | In | Condition | Example |
| --- | --- | --- | --- | --- | --- |
| vin | String | Vehicle identification number  Limit: 17 alphanumeric characters | Param |  |  |

Request Sample

Raw Request Data Sample (before encryption):

{

"vin": "LVSHABCD000000001"

}

Request sample:

https://{domain/api/ivisl/app-router/v1/d/s-pcs/connection?param= NV9tWirKTXYVGOgxOj%2BxWPx2lY5kbTBCWI7gSKLCSS1SD%2FgVPWlp40g0qEEQXLfzcpIHXk4%2BOUD%2F8IEa5geU6qM9PcX9oP%2B6OZ13RoZ4zmrucTLTr4ifKCGaBp16SWF%2B3OpMhale6%2FviXQ5GD%2BwBpxp15tiFe8K%2BIM%2F15jubNUc%3D&nonce=1570703617000abc&timestamp=1570703617000&sign=5o%2FnjgZHAP5rmOR9wHWKT5Zr0Ccpm2hWQsYH6jdrfUc%3D

Response

|  |  |  |  |
| --- | --- | --- | --- |
| Field | Type | Description | Example |
| status | Integer | Status code | 130200 |
| statusDesc | String |  | Success |
| responseData | String | Encrypted connection info, refer to [section 2.2.1 Payload Encryption](#Payload_Encryption) |  |

Response Sample

Raw response

{

"status": 130200,

"statusDesc": "Request is processed successfully",

"responseData":"NV9tWirKTXYVGOgxOj+xWPx2lY5kbTBCWI7gSKLCSS1SD/gVPWlp40g0qEEQXLfzcpIHXk4+OUD/8IEa5geU6qM9PcX9oP+6OZ13RoZ4zmrucTLTr4ifKCGaBp16SWF+MenK022aGcoZCmdUuv3vzlsGbw58RREQV7ylwRSjDzUGv1ZHyVu4DEfpo0LIQ0/orGPV7J77OiUryUP2flMQ81UwqlX0xPgdXD9I7jyGHnQ7GK/CJZ84rFBZcIxx/u0uhiXSs9EHPpCcAwqp2Tifo46S7oJS6qeLO6aaAJNbKHA="

}

Response Data fields

|  |  |  |  |
| --- | --- | --- | --- |
| Key | Type | Description | Example |
| accessId | String | MQTT Username | cniviop-testdrive-iothub.azure-devices.cn/TEST001F3MH651106-8fdf89a52d14336818652e4b5039b531847b556b30577b93eaa29d9f249d6b26/?api-version=2018-06-30 |
| accessToken | String | MQTT password | SharedAccessSignature sr=cniviop-testdrive-iothub.azure-devices.cn%2Fdevices%2FTEST001F3MH651106-8fdf89a52d14336818652e4b5039b531847b556b30577b93eaa29d9f249d6b26&sig=vyglUlBcs%2BLnIHvmFl0mDP4%2FI22xmrsR06wvRIFMpTo%3D&se=1627103783&skn=device |
| port | String | MQTT port | 8883 |
| sendTopic | String | Send message topic from MQTT | devices/TEST001F3MH651106-8fdf89a52d14336818652e4b5039b531847b556b30577b93eaa29d9f249d6b26/messages/events/ |
| receiveTopic | String | recevice message topic from MQTT | devices/TEST001F3MH651106-8fdf89a52d14336818652e4b5039b531847b556b30577b93eaa29d9f249d6b26/messages/devicebound/# |
| deviceId | String | Device id | TEST001F3MH651106-8fdf89a52d14336818652e4b5039b531847b556b30577b93eaa29d9f249d6b26 |
| hostname | String | MQTT hostname | cniviop-testdrive-iothub.azure-devices.cn |
| protocol | String |  | MQTT |
| clientId | String | MQTT client id | TEST001F3MH651106-8fdf89a52d14336818652e4b5039b531847b556b30577b93eaa29d9f249d6b26 |
| expireAt | Long | expiration timestamp |  |

{

"accessId":"cniviop-testdrive-iothub.azure-devices.cn/TEST001F3MH651106-8fdf89a52d14336818652e4b5039b531847b556b30577b93eaa29d9f249d6b26/?api-version=2018-06-30",

"accessToken":"SharedAccessSignature sr=cniviop-testdrive-iothub.azure-devices.cn%2Fdevices%2FTEST001F3MH651106-8fdf89a52d14336818652e4b5039b531847b556b30577b93eaa29d9f249d6b26&sig=vyglUlBcs%2BLnIHvmFl0mDP4%2FI22xmrsR06wvRIFMpTo%3D&se=1627103783&skn=device",

"sendTopic":"devices/TEST001F3MH651106-8fdf89a52d14336818652e4b5039b531847b556b30577b93eaa29d9f249d6b26/messages/events/",

"receiveTopic":"devices/TEST001F3MH651106-8fdf89a52d14336818652e4b5039b531847b556b30577b93eaa29d9f249d6b26/messages/devicebound/#",

"deviceId":"TEST001F3MH651106-8fdf89a52d14336818652e4b5039b531847b556b30577b93eaa29d9f249d6b26",

"hostname":"cniviop-testdrive-iothub.azure-devices.cn",

"protocol":"MQTTS",

"clientId":"TEST001F3MH651106-8fdf89a52d14336818652e4b5039b531847b556b30577b93eaa29d9f249d6b26",

"port":"8883",

"expireAt": 1641453384000

}

* 1. API02 – Send Message to IVI Device via Azure IoT Hub

This API is used to send Cloud to Device message to Azure IoT Hub device queue.

Attributes

|  |  |
| --- | --- |
| URL | /api/ivisl/app-router/v1/d/s-pcs/notification |
| HTTP Method | PUT |
| Security Access | Authenticated Calls Only |
| Call Type | Synchronous |

Requests

Additional package data is required.

| Field | Type | Description | In | Condition | Example |
| --- | --- | --- | --- | --- | --- |
| param | String | Encrypted request json payload, refer to [section 2.2.2 Payload Encryption](#Payload_Encryption) | Body | Required |  |
| nonce | String | A random string generated for each request, 16 bytes max | Body | Required | 1570703617000abc |
| timestamp | Long | Timestamp of signature | Body |  |  |
| sign | String | Signature of request, refer to [section 2.3.2 Request Signature](#Request_Signature) | Body |  |  |

Request Data Sample：

{

"param" : "NV9tWirKTXYVGOgxOj+xWPx2lY5kbTBCWI7gSKLCSS1SD/gVPWlp40g0qEEQXLfzcpIHXk4+OUD/8IEa5geU6qM9PcX9oP+6OZ13RoZ4zmrucTLTr4ifKCGaBp16SWF+MenK022aGcoZCmdUuv3vzlsGbw58RREQV7ylwRSjDzUGv1ZHyVu4DEfpo0LIQ0/orGPV7J77OiUryUP2flMQ81UwqlX0xPgdXD9I7jyGHnQ7GK/CJZ84rFBZcIxx/u0uhiXSs9EHPpCcAwqp2Tifo46S7oJS6qeLO6aaAJNbKHA=";

"nonce": "1570703617000abc ",

"timestamp" : 1234567890123,

"sign" : "{{sign}}"

}

param raw data fields is

| Field | Type | Description | In | Condition | Example |
| --- | --- | --- | --- | --- | --- |
| messageId | String | Message id used to identify message, uuid generated by client service. | Body | Requried | f112a288-db25-49e7-a33f-60d16a624807 |
| vin | String | Vehicle identification number  Limit: 17 alphanumeric characters | Body | Required | LVSHFACA3X2938457 |
| guid | String | User guid | Body | Optional |  |
| eventType | String | Indicate which feature or apk will process the notification  Limit：50 alphanumeric characters | Body | Required | lidget |
| providerName | String | Indicate the source of the notification.  Limit：50 alphanumeric characters | Body | Required | CMS |
| messageContent | String | Cloud to Device message content(Json string). If IVI needs to know expiration timestamp, etc. please include it in this field.  Maximum length is 3KB | Body | Required |  |
| c2dExpireMinutes | Long | How many minutes will the message expire in IoT Hub.  Default is 2880 minutes. In case that notification needs expration duration more than it, backend system should have notification feedback and retry logic. | Body | Optional |  |

Request Sample

Raw Request Data Sample (before encryption):

{

"messageId":”f112a288-db25-49e7-a33f-60d16a624807",

"vin":"LVSHFACA3X2938457",

"guid":" d87304df-591a-4f9f-87c1-d735d22b98e6",

"eventType":"lidget",

"providerId":"CMS",

"messageContent":"{\"ids\": [\"ABE0981\", \"ABE0982\",\"ABE0981\"],\"status\":0, \"expirationTimestamp\":1570703617000}",

"c2dExpireMinutes": 2880

}

Response

|  |  |  |  |
| --- | --- | --- | --- |
| Field | Type | Description | Example |
| status | Integer | Status code | 130200 |
| statusDesc | String |  | Success |

Response Sample

Raw response

{

"status": 130200,

"statusDesc": "Request is processed successfully"

}

1. API Specifications(Internal Router)

This section documents the APIs hosted by IVI Service Layer Internal Router

**API Domain:**

QA: http://ivisl-app-router-qa.apps.internal

Stage: http://ivisl-app-router-stage.apps.internal

Production: http://ivisl-app-router-pd.apps.internal

**API Port**:8080

* 1. API01 – Send Message to IVI Device via Azure IoT Hub

This API is used to send Cloud to Device message to Azure IoT Hub device queue.

Attributes

|  |  |
| --- | --- |
| URL | /v1/d/is-pcs/notification |
| HTTP Method | PUT |
| Security Access | Authenticated Calls Only (Security authentication field, refer to [Request from Cloud System](#internal_router_authorization_header)) |
| Call Type | Synchronous |

Requests

Additional package data is required.

| Field | Type | Description | In | Condition | Example |
| --- | --- | --- | --- | --- | --- |
| data | Object | Request content | Body | Required | {  "messageId":"f112a288-db25-49e7-a33f-60d16a624807",  "vin":"LVSHFACA3X2938457",  "guid":" d87304df-591a-4f9f-87c1-d735d22b98e6",  "eventType":"lidget",  "providerName":"CMS",  "messageContent":"{\"ids\": [\"ABE0981\", \"ABE0982\",\"ABE0981\"],\"status\":0, \"expirationTimestamp\":1570703617000}",  "c2dExpireMinutes": 2880  } |
| nonce | String | A random string generated for each request, 16 bytes max | Body | Required | 1570703617000abc |
| timestamp | Long | Timestamp of signature | Body | Required | 1648455572000 |

Data request field:

| Field | Type | Description | In | Condition | Example |
| --- | --- | --- | --- | --- | --- |
| messageId | String | Message id used to identify message, uuid generated by client service. | data | Requried | f112a288-db25-49e7-a33f-60d16a624807 |
| vin | String | Vehicle identification number  Limit: 17 alphanumeric characters | data | Required | LVSHFACA3X2938457 |
| guid | String | User guid | data | Optional |  |
| eventType | String | Indicate which feature or apk will process the notification  Limit：50 alphanumeric characters | data | Required | lidget |
| providerName | String | Indicate the source of the notification.  Limit：50 alphanumeric characters | data | Required | CMS |
| messageContent | String | Cloud to Device message content(Json string). If IVI needs to know expiration timestamp, etc. please include it in this field.  Maximum length is 3KB | data | Required |  |
| c2dExpireMinutes | Long | How many minutes will the message expire in IoT Hub.  Default is 2880 minutes. In case that notification needs expration duration more than it, backend system should have notification feedback and retry logic. | data | Optional |  |

Request Data Sample

{

"data": {

"messageId":"f112a288-db25-49e7-a33f-60d16a624807",

"vin":"LVSHFACA3X2938457",

"guid":" d87304df-591a-4f9f-87c1-d735d22b98e6",

"eventType":"lidget",

"providerName":"CMS",

"messageContent":"{\"ids\": [\"ABE0981\", \"ABE0982\",\"ABE0981\"],\"status\":0, \"expirationTimestamp\":1570703617000}",

"c2dExpireMinutes": 2880

},

"nonce": "1570703617000abc",

"timestamp": 1648455572000

}

Response

|  |  |  |  |
| --- | --- | --- | --- |
| Field | Type | Description | Example |
| status | Integer | Status code | 130200 |
| statusDesc | String | Status desc | Request is processed successfully |

Response Sample

{

"status": 130200,

"statusDesc": "Request is processed successfully"

}

1. Staus Code
   1. HTTP Status Code

|  |  |  |
| --- | --- | --- |
| Code | Description | Retry Suggestion\* |
| 200 | Success (Response body should contain an application status code) |  |
| 201 | Created |  |
| 207 | Mutltiple status, refer to response body for more detailed info. Could be result of partial failure in backend requests. |  |
| 400 | Bad request(Response body should contain an application status code) | No, please ensure request data is valid before requesting cloud |
| 401 | Unauthorized – if the Authorization token is invalid or has expired | No |
| 403 | Forbidden | No |
| 404 | Unknown API or the API is off | No |
| 406 | Not Acceptable | No |
| 415 | Unsupported Media Type |  |
| 429 | Too Many Requests |  |
| 500 | Internal server error | Yes, suggest retry 3 times with time interval more than 10 seconds |
| 502 | Unexpected error from backend system | Yes, suggest retry 3 times with time interval more than 10 seconds |
| 503 | The server is currently unable to handle the request due to a temporary overloading or maintenance of the server. | Yes, suggest retry 3 times with time interval more than 10 seconds |
| 504 | Backend system did not respond within time limit | Yes, suggest retry 3 times with time interval more than 10 seconds |

\*Kindly note that retry suggestion is only for reference.

* Not retry means that please do not use the same parameter to call IVISL API again.
* IVI retry mechanism, including retry times and retry interval should be based on business need.
  1. Application Status Codes

Application status codes are for business returned in response body(NOT in http header).

|  |  |  |
| --- | --- | --- |
| Code | Description | Retry? |
| 130200 | Request is processed   successfully | No |
| 130207 | Request is partially successful, refer to responseData for more details | Yes, just retry error response data |
| 130400 | Invalid parameter(parameter name list which are invalid) | No, please ensure request data is valid before requesting cloud |
| 130401 | Platform Id authentication fail | No |
| 130402 | Onboarding key not found | No |
| 130403 | App Id authentication fail | No |
| 130404 | invalid deviceId | No |
| 130405 | illegal transaction id. | No, IVISL APK register device or renew key |
| 130406 | sign check fail. | No |
| 130407 | Request time is invalid. | No, please get a new timestamp |
| 130408 | Duplicate Request | No, please generate a new nonce. |
| 130409 | Decrypted content is invalid | No |
| 130429 | Too Many Requests | No |
| 130500 | Service internal error | Yes |
| 130501 | Backend service error | Yes |
| 130502 | No data found | No |
| 130503 | Csdn response description | No |
| 130504 | Invalid token when calling csdn | No |
| 130505 | VIN is invalid | No |
| 130506 | No user found | No |
| 130600 | Refresh token may be rovoked. Please request a new In-Vehicle token | No, Account APK retrieve a new IVT suite. |
| 130601 | User is inactive | No |
| 130602 | The vehicle is not bound with user | No |
| 130603 | Cannot revoke token by this userId | No |
| 130604 | Cannot revoke token on other's vehicle | No |
| 130605 | Inactive llid | No, user consent apk retrieve new llid first. |
| 130606 | Delivery Count Exceeded | No |
| 130607 | Device hasn’t been registered in IoT Hub | No |
| 130701 | Encryption key is invalid | No, functional app decides if pop up message to inform customer to contact call center |
| 130702 | Communication key is expired | No, IVISL APK renew key |
| 130703 | Device hasn't been registered. | No, IVISL APK register device |
| 130704 | Communication key not found | No, functional app decides if pop up message to inform customer to contact call center |
| 130705 | Device has been registered. | No, functional app decides if pop up message to inform customer to contact call center |
| 130801 | Device authentication fail | Yes |

* 1. Exception Layout

Exception will use fixed type with specific description, please check the below:

Response

|  |  |  |  |
| --- | --- | --- | --- |
| Field | Type | Description | Example |
| status | Integer | Status code | 130500 |
| statusDesc | String |  |  |

Response Sample

{

"status": 130500,

"statusDesc": "An exception occurs within the system"

}