

SAMSUNG



# Knox Manage Getting Device Location using APIs



Aug 2021 – v1.0  
SiDi RTAM Team

# Introduction

The objective of this guide is to show how Knox Manage (KM) APIs can be used to get device location information.

The examples described in this guide were run using Postman tool and relies on Knox Manage version 21.6.

## **Pre requisites:**

- Device enrolled in KM
- Location policy configured in KM and assigned to the device
- API Client created in KM

# 1- Set a Location Policy to Device

- Before call KM APIs to get location data from the device, it is required to set a proper location policy under KM's Menu Profile and assign it to the device.

**Location**

Highlight Work Profile on company-owned D

**Device Controls** ⓘ

GPS ⓘ - ▼

Report Device Location ⓘ Allow ▼

- Report Device Location Interval 30 minutes ▼

High Accuracy Mode ⓘ Use ▼

## 2- Create the API Client

- Create an API Client at KM's admin Portal. To do this, you must be an administrator of your Knox Manage tenant.
- This is a one-time operation. Take notes of "Client ID" and "Password" info as they will be used later to generate the authentication token via API.

The image illustrates the process of creating an API client in the Samsung Knox Manage admin portal. It is divided into three main sections:

- Navigation:** The left sidebar shows the main menu with "Advanced" circled in yellow. An arrow points from "Advanced" to the next section.
- Advanced Menu:** The "Advanced" menu is expanded, showing options like Report, Dashboard Management, AD/LDAP Sync, Certificate, EMM API, and "API Client" (circled in yellow). An arrow points from "API Client" to the next section.
- API Client Page:** The "API Client" page is shown with a table of existing clients. The "Add" button is circled in yellow. An arrow points from the "Add" button to the "Add API Client" modal form.

The "Add API Client" modal form contains the following fields:

- Client ID:** A text input field containing "teste". Below it, a message states: "The entered client ID cannot be changed."
- Password:** A password input field with a masked password "....." and a visibility toggle icon.
- Token Validity(sec):** A text input field with the error message "Only numbers are allowed."

At the bottom of the modal, there are "Cancel" and "Save" buttons. The "Save" button is circled in yellow.

# 3- Generate the Authentication Token

Once API Client was created at KM's console, call API below to obtain a bearer token:

- URL: <https://{Your Region}.manage.samsungknox.com/emm/oauth/token>
- Method GET
- Required parameters:
  - **client\_id** - the Client ID defined when API client was created appended with @[KM's tenant].
  - **client\_secret** - the Password defined when API client was created.
  - **grant\_type** - must be set to **client\_credentials**

# 3- Generate the Authentication Token

## REQUEST

GET [https://us01.manage.samsungknox.com/emm/oauth/token?grant\\_type=client\\_credentials&client\\_id=teste@mytenant.1...](https://us01.manage.samsungknox.com/emm/oauth/token?grant_type=client_credentials&client_id=teste@mytenant.1...) Send

Params Authorization Headers (6) Body Pre-request Script Tests Settings Cookies

Query Params

KEY	VALUE	DESCRIPTION	...	Bulk Edit
<input checked="" type="checkbox"/> grant_type	client_credentials			
<input checked="" type="checkbox"/> client_id	teste@mytenant.com			
<input checked="" type="checkbox"/> client_secret	Teste2018!			
Key	Value	Description		

Tenant's Region

## RESPONSE

Body Cookies (2) Headers (13) Test Results Status: 200 OK Time: 1162 ms Size: 891 B Save Response

Pretty Raw Preview Visualize JSON

```
1 {
2   "access_token": "903c4",
3   "token_type": "bearer",
4   "expires_in": 359907753,
5   "scope": "read"
6 }
```

Access token to be used to call other APIs

## 4- Get Device Detail By IMEI

- This API is to query the Enrolled Device Detailed Information by IMEI.
- With this API it will be possible to get “device Id” and “mobileId” info, which are necessary parameters to be used in the Get Device Location API.
  - URL: `https://{Your Region}.manage.samsungknox.com/emm/oapi/device/selectDeviceInfoByImei`
  - Method: POST
  - Authorization: Bearer-authentication
  - Request Body Schema: `application/x-www-form-urlencoded`
  - Body: imei

# 4- Get Device Detail By IMEI – Request

The screenshot displays a REST client interface for a POST request to `https://us01.manage.samsungknox.com/emm/oapi/device/selectDeviceInfoByImei`. The interface is divided into three main sections: Authorization, Headers, and Body.

**Authorization Section:** The 'Type' dropdown is set to 'Bearer Token'. A warning message states: "Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. [Learn more about variables](#)". A 'Token' input field is present.

**Headers Section:** The 'Headers' tab is active, showing a table of headers. The 'Authorization' header is highlighted with a yellow circle and contains the value `bearer903`. The 'Content-Type' header is set to `application/x-www-form-urlencoded`.

**Body Section:** The 'Body' tab is active, showing a table of body parameters. The 'imei' parameter is highlighted with a yellow circle.

KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/> Authorization	bearer903	
<input checked="" type="checkbox"/> Content-Type	application/x-www-form-urlencoded	

KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/> imei		

The authorization start with "bearer" followed by the access token



# 4- Get Device Detail By IMEI – Response

```
Body Cookies (2) Headers (14) Test Results Status: 200 OK
Pretty Raw Preview Visualize JSON
1 {
2   "resultValue": {
3     "deviceKind": "",
4     "enrolledType": "KME",
5     "isRooting": "N",
6     "ownerShip": "EC",
7     "groupIdList": [],
8     "wifiReceivedData": "",
9     "clientProfileId": "emmsettingspolicy-client-profile",
10    "clientProfileName": "Default",
11    "battery": "61.00",
12    "deviceId": "3211ea8a9da54d4dba60c41434b8ece2",
13    "platform": "A",
14    "deviceStatus": "A",
15    "managementType": "COWP",
16    "wifiSentData": "",
17    "orgCode": "wpc",
18    "agentProfileName": "",
19    "isDeviceLock": "Unlocked",
```

```
48   "deviceVersionName": "11",
49   "lastConnectionDate": { ...
59   },
60   "macAddress": "42:42:F1",
61   "mobileSentData": "",
62   "mobileId": "wpc_Android_1",
63   "phone": "",
64   "agentProfileUpdated": "",
65   "agentProfileId": "",
66   "mobileReceivedData": "",
67   "imei": "356697",
68   "deviceModel": "SM-A217M",
69   "updated": {
70     "date": 26,
71     "hours": 12,
72     "seconds": 35,
73     "month": 7,
74     "timezoneOffset": 0,
75     "year": 121,
```

# 5- Get Device List

- This API is to query the Device Information List enrolled.
- This is another option to get the “device Id” and “mobileId” parameters but for all enrolled devices.
  - URL: `https://{Your Region}.manage.samsungknox.com/emm/oapi/device/selectDeviceList`
  - Method: POST
  - Authorization: Bearer-authentication
  - Request Body Schema: `application/x-www-form-urlencoded`

# 5- Get Device List – Request

POST ▼ <https://us01.manage.samsungknox.com/emm/oapi/device/selectDeviceList> Send ▼

Params ● Authorization ● Headers (10) ● Body ● Pre-request Script Tests Settings Cookies

Type Bearer Token ▼

The authorization header will be automatically generated when you send the request. [Learn more about authorization](#) ↗

! Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. [Learn more about variables](#) ↗ ×

Token

Params ● Authorization ● Headers (11) ● Body ● Pre-request Script Tests Settings Cookies

Headers ◁ 9 hidden

	KEY	VALUE	DESCRIPTION	⋮	Bulk Edit	Presets <span>▼</span>
<input checked="" type="checkbox"/>	Authorization	bearer903 [REDACTED]				
<input checked="" type="checkbox"/>	Content-Type	application/x-www-form-urlencoded				

# 5- Get Device List – Response

```
Content type
application/json

Copy Expand all Collapse all

"resultCode": "0",
"resultMessage": "No Error",
- "resultValue": {
  "deviceId": "string",
  "mobileId": "string",
  "userId": "string",
  "deviceStatus": "string",
  "platform": "string",
  "phone": "string",
  "macAddress": "string",
  "deviceVersionName": "string",
  "ownership": "string",
  "deviceModel": "string",
  "deviceKind": "string",
  "deviceModelKind": "string",
  "imei": "string",
  "serialNumber": "string",
  "lastConnectionDate": "2019-08-24T14:15:22Z",
  "isDeviceLock": "string",
```

```
"updated": "2019-08-24T14:15:22Z",
"created": "2019-08-24T14:15:22Z",
"enrolledType": "string",
"managementType": "string",
"knoxId": "string",
"battery": "string",
"mobileSentData": "string",
"mobileReceivedData": "string",
"wifiSentData": "string",
"wifiReceivedData": "string",
"clientProfileId": "string",
"clientProfileName": "string",
"clientProfileUpdated": "2019-08-24T14:15:22Z",
"isRooting": "string",
- "groupList": [
  "string"
],
- "groupIdList": [
  "string"
],
"orgName": "string",
"orgCode": "string",
"agentProfileId": "string",
"agentProfileName": "string",
"agentProfileUpdated": "string"
}
```

# 6 – Collect Current Location Command

- Before get device's location data, it is necessary to send a command to trigger Device's current location.
  - URL: `https://{Your Region}.manage.samsungknox.com/emm/oapi/mdm/commonOTCServiceWrapper/sendDeviceControlForGPSInfo`
  - Method: POST
  - Authorization: Bearer-authentication
  - Request Body Schema: `application/x-www-form-urlencoded`
  - Body: `deviceId`

# 6 – Collect Current Location Command – Request

POST ▼ <https://us01.manage.samsungknox.com/emm/oapi/mdm/commonOTCServiceWrapper/sendDeviceControlForGPSInfo> Send ▼

Params Authorization ● Headers (11) **Body** ● Pre-request Script Tests Settings Cookies

none  form-data  x-www-form-urlencoded  raw  binary  GraphQL

	KEY	VALUE	DESCRIPTION	⋮	Bulk Edit
<input checked="" type="checkbox"/>	deviceId	[REDACTED]			
	Key	Value	Description		

Params ● **Authorization** ● Headers (10) ● Body ● Pre-request Script Tests Settings Cookies

Type Bearer Token ▼

The authorization header will be automatically generated when you send the request. [Learn more about authorization](#) ↗

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. [Learn more about variables](#) ↗

Token

Params ● Authorization ● **Headers (11)** ● Body ● Pre-request Script Tests Settings Cookies

Headers ◀ 9 hidden

	KEY	VALUE	DESCRIPTION	⋮	Bulk Edit	Presets <span>▼</span>
<input checked="" type="checkbox"/>	Authorization	bearer903 [REDACTED]				
<input checked="" type="checkbox"/>	Content-Type	application/x-www-form-urlencoded				

# 6 – Collect Current Location Command – Response

Content type

application/json

Copy

Expand all

Collapse all

```
{
  "resultCode": "0",
  "resultMessage": "No Error",
  - "resultValue": {
      "commandId": "fd5b6064c9071dc95bc9e4dee47a4a8e"
    }
}
```

# 7 – Get Device Location

- Once previous steps were performed, it is possible to call this API to query the GPS Information of the Device.
  - URL: `https://{Your Region}.manage.samsungknox.com/emm/oapi/device/selectDeviceLocation`
  - Method: POST
  - Authorization: Bearer-authentication
  - Request Body Schema: `application/x-www-form-urlencoded`
  - Body: `deviceId` or `mobileId`

<code>deviceId</code> <code>required</code>	<code>string</code> Device ID.
<code>mobileId</code> <code>required</code>	<code>string</code> Device Name.



# 7 – Get Device Location – Request

POST ▼ <https://us01.manage.samsungknox.com/emm/oapi/device/selectDeviceLocation> Send ▼

Params ● Authorization ● Headers (11) **Body** ● Pre-request Script Tests Settings Cookies

none  form-data  x-www-form-urlencoded  raw  binary  GraphQL

	KEY	VALUE	DESCRIPTION	...	Bulk Edit
<input checked="" type="checkbox"/>	deviceId	[REDACTED]			
<input checked="" type="checkbox"/>	mobileId	[REDACTED]			

Params ● **Authorization** ● Headers (10) Body ● Pre-request Script Tests Settings Cookies

Type Bearer Token ▼

The authorization header will be automatically generated when you send the request.  
[Learn more about authorization](#) ↗

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. [Learn more about variables](#) ↗

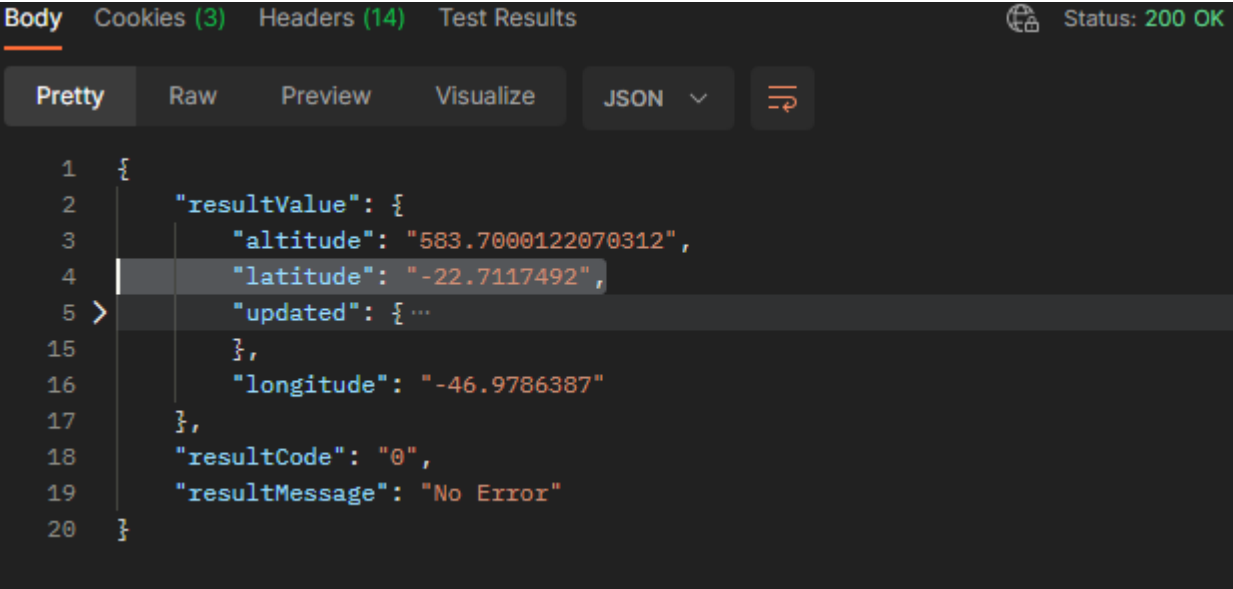
Token

Params ● Authorization ● **Headers (11)** Body ● Pre-request Script Tests Settings Cookies

Headers ◀ 9 hidden

	KEY	VALUE	DESCRIPTION	...	Bulk Edit	Presets <span>▼</span>
<input checked="" type="checkbox"/>	Authorization	bearer903 [REDACTED]				
<input checked="" type="checkbox"/>	Content-Type	application/x-www-form-urlencoded				

# 7 – Get Device Location – Response



The screenshot shows a web browser's developer console with the 'Body' tab selected. The status is '200 OK'. The JSON response is displayed in a 'Pretty' format. The response contains a 'resultValue' object with 'altitude', 'latitude', and 'longitude' fields, and a 'resultCode' of '0' with a 'resultMessage' of 'No Error'.

```
1  {
2    "resultValue": {
3      "altitude": "583.7000122070312",
4      "latitude": "-22.7117492",
5      "updated": { ...
15   },
16   "longitude": "-46.9786387"
17   },
18   "resultCode": "0",
19   "resultMessage": "No Error"
20 }
```

# 8 – Get Device Location History

- It is also possible to check history of device's location.
  - URL: `https://{Your Region}.manage.samsungknox.com/emm/oapi/device/selectDeviceLocationHistory`
  - Method: POST
  - Authorization: Bearer-authentication
  - Request Body Schema: `application/x-www-form-urlencoded`
  - Body: DeviceId, mobileId and period

deviceId required	string Device ID, the unique key of the device.
mobileId required	string Device Name.
period required	string Search Period (Day)

# 8 – Get Device Location History – Request

POST <https://us01.manage.samsungknox.com/emm/oapi/device/selectDeviceLocationHistory> Send

Params Authorization Headers (11) **Body** Pre-request Script Tests Settings Cookies

none  form-data  x-www-form-urlencoded  raw  binary  GraphQL

	KEY	VALUE	DESCRIPTION	...	Bulk Edit
<input checked="" type="checkbox"/>	deviceId	[REDACTED]			
<input checked="" type="checkbox"/>	mobileId	[REDACTED]			
<input checked="" type="checkbox"/>	period	30			

Params Authorization Headers (10) Body Pre-request Script Tests Settings Cookies

Type Bearer Token

The authorization header will be automatically generated when you send the request. [Learn more about authorization](#)

Token

! Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. [Learn more about variables](#)

Params Authorization **Headers (11)** Body Pre-request Script Tests Settings Cookies

Headers 9 hidden

	KEY	VALUE	DESCRIPTION	...	Bulk Edit	Presets
<input checked="" type="checkbox"/>	Authorization	bearer903 [REDACTED]				
<input checked="" type="checkbox"/>	Content-Type	application/x-www-form-urlencoded				

# 8 – Get Device Location History – Response

```
Content type
application/json

Copy Expand all Collapse all

{
  "total": "1",
  - "locationList": [
    - {
      "latitude": "39.990912172420714",
      "longitude": "116.32715863448607",
      "altitude": "null",
      "locationInfoUpdated": "1608197241989"
    }
  ]
}
```

# **SAMSUNG** Knox Manage

For more information on Knox Manage, please visit  
<https://www.samsungknox.com/en/solutions/it-solutions/knox-manage>