Knox Asset Intelligence

Knox Asset Intelligence is a Samsung Knox cloud service that provides you with analytics to help you improve the management, productivity, and lifecycle of your devices.

With these REST APIs, you can integrate device information from Knox Asset Intelligence into your enterprise's web service.

Audience

This guide is intended for web developers working for enterprises that use their own website to retrieve device information from the Knox Asset Intelligence service.

Where to start

If you want to	**See**
Understand the overall Knox ecosystem	The Big Picture
Get a Knox cloud services authentication token	Knox cloud services authentication
Use the Knox Asset Intelligence APIs	API reference

Get started

Legacy authentication

Before you can access the Knox Asset Intelligence API, you must set up authentication. This guide covers how to set up legacy authentication for secure access to the Knox Asset Intelligence API.

Note that support for client ID creation using Knox Cloud Authentication (legacy) has been discontinued since Knox Asset Intelligence 24.09. Existing client IDs will continue to be supported.

You must use Knox OAuth 2.0 Authentication to generate any new client IDs.

1. Sign up for Knox Asset Intelligence in your Samsung Knox account

1. Register for a Samsung Knox account. For more information, see Create a Samsung Knox account.

2. Sign in to your account once you're approved for Knox Asset Intelligence. For more information, see Access the Knox Asset Intelligence console.

2. Request access to the Knox cloud services API

To apply for Knox cloud services API access, send an email to knoxapi@samsungknox.com with your user and tenant information. You can also create a Support ticket.

3. Generate your access token

After you get Knox cloud services API access, go to the Knox Developer Portal, click **Knox Cloud API Portal** on the navigation pane, and generate an access token. When making a Knox Asset Intelligence API request, include this access token in the request header.

To let your sub-admins generate access token, go to the Knox Admin Portal, and grant the **Access Knox Cloud APIs portal** permission to the roles associated with the sub-admins.

4. Test your access token

Ensure that your access token is correctly configured by making a test call to Knox Asset Intelligence API. See Knox Asset Intelligence API for a list of operations you can call.

API restrictions

Request limit

The rate limit set for Knox Asset Intelligence APIs is 25 requests per second. That is, an API can be called up to 25 times a second by the same Knox cloud services API key, also known as the x-knox-apitoken, or by the same user in a tenant.

Tutorials

Manage devices

The Knox Asset Intelligence APIs provide functionalities for device management, allowing greater visibility into a device's status and health. This tutorial focuses on how to manage your devices.

Prerequisites

Ensure that you have the necessary permissions to set or update the Knox Asset Intelligence settings and obtain an authentication token. For more information, see Get started.

Get device information

1. To retrieve essential details about the registered devices, such as model, serial number, permissions, firmware, and operating system version, make a POST request to the /devices/getDevices endpoint.
2. In the request body, you can make use of the following optional parameters:
    - **pageNum** — Page number to retrieve.
    - **pageSize** — Number of items on a page.
    - **deviceIds** — List of the device IMEIs or serial numbers for targeted retrieval.
    - **status** — List of Knox Asset Intelligence enrollment statuses.
    - **batterySoh** — List of battery health statuses you want information about.
    - **groupName** — Name of the Knox Asset Intelligence device group you want information about.

For example, the response of the following request body provides the details of those devices which have their IMEIs listed in deviceIds, whose status is Active, whose battery health is either Good or Normal and the location permission is enabled, and which are a part of device group Group A.


```
{
 "pageNum": 2,
 "pageSize": 50,
 "deviceIds": [
```

123456789123456,123123123123123

],

"**status**": [

"Active"

],

"**batterySoh**": [

"Good", "Normal"

],

"**permissions**": [

"Location"

],

"**groupName**": "Group A"

}

You can adjust the parameter values in the request body according to the kind of information you want to fetch. For detailed response schema, see POST /devices/getDevices.

Retrieve information about device groups

1. To retrieve a list of all device groups in your tenant, make a GET request to the /devices/groups endpoint.
2. In the request, you can make use of the following optional parameters:
    - **pageNum** — Page number to retrieve.
    - **pageSize** — Number of items on a page.
    - **groupName** — Name of the Knox Asset Intelligence device group you want information about.

For example, the following sample request provides the information about the abc group. It's response includes details such as the number of groups, group name, its description, the device count in a group, manager, and last modified time.

GET

/devices/groups?

groupName=abc

You can modify the group name in the above request to reflect the specific group for which you want to retrieve information. For detailed response schema, see GET /devices/groups.

Assign group for a device

You can group devices for easy organization and management. You can also use the groups as filters on the Knox Asset Intelligence dashboard.

1. To assign groups for devices, make a POST request to the /devices/groups endpoint.
2. In the request body, you can use the **request** parameter. It's a required parameter, and is an array of objects containing the following elements:
    - **deviceId** — The device IMEIs or serial numbers for which you want to assign a group.
    - **groupName** — Name of the Knox Asset Intelligence device group to be assigned to the device.

For example, consider the following sample request which provides the status of the request, that is whether the devices with IDs AABBCC1DDEE and AAABBB1CCCC are successfully assigned to groups A and B respectively or not.

```
{
 "request": [
  {
   "deviceId": "AABBCC1DDEE",
   "groupName": "group A"
  },
  {
   "deviceId": "AAABBB1CCCC",
   "groupName": "group B"
  }
 ]
}
```

You can adjust the request body parameters based on how you want to group the devices in your tenant. For detailed response schema, see POST /devices/getDevices.

Ensure that you check the code and message in the response for any errors and handle them appropriately for your app. For detailed specification, see Knox Asset Intelligence API.

Manage diagnostic logs

The Knox Asset Intelligence APIs provide functionalities to manage the diagnostic logs of devices. This tutorial focuses on the diagnosticsLogs endpoint, it supports two use cases — generation of diagnostic logs and retrieval of these diagnostic logs.

The generation of diagnostic logs leads to an event upload by Knox Asset Intelligence. You can receive notifications for this event, if you subscribed to it in Knox Webhook Notification.

Prerequisites

Ensure that you have the necessary permissions to set or update the Knox Asset Intelligence settings and obtain an authentication token. For more information, see Get started.

Generate diagnostic logs

1. To request generation of diagnostic logs, make a POST request to the /diagnosticsLogs endpoint.
2. In the request body, you can make use of the following parameters:
    - **deviceIds** — List of the device IMEIs or serial numbers for which to generate logs, this is a required parameter.
    - **silentMode** — Specifies whether to retrieve logs with or without user consent, this is applicable only on fully managed devices. You can retrieve logs without the user consent by setting this parameter to true.
    - **category** — Category of diagnostic logs you want to generate. If set to TCPDUMPLOG, generates only TCPdump logs. Default value is ALL, which generates a comprehensive set of logs.

For example, the following request body generates the diagnostic logs for devices for which IMEIs are listed in deviceIds. This request sample doesn't seek consent from the user and generates only TCPdump logs.

```
{
 "deviceIds": [
   123456789123456,123123123123123
  ],
 "silentMode": [
   "true"
```

```
  ],
 "category": [
    "TCPDUMPLOG"
  ]
}
```

You can adjust the parameters in the request body based on your requirements. For detailed response schema, see POST /diagnosticsLogs.

You can receive notifications for these log generation events using Knox Webhook Notification, if subscribed.

Retrieve diagnostic logs

To retrieve Knox Asset Intelligence settings, make a GET request to the /diagnosticsLogs endpoint and specify query parameters in the request to get the required device diagnostic log.

The query parameter is logId which is the tracking number returned from POST /diagnosticsLogs. A maximum of 50 log IDs can be included in a single request.

For example, the following request sample returns details, such as serial number, group name, and download link for generated diagnostic logs, for the logIDs 64e851ddc136352a60a5e1a0 and 84e051ddc136352a60a5e1a3.

```
GET
/diagnosticsLogs?
logId=64e851ddc136352a60a5e1a0&
logId=84e051ddc136352a60a5e1a3
```

Ensure that you handle errors appropriately in your application by checking the code and the message in the response. For detailed specification, see Knox Asset Intelligence API reference.

Create a subscription in Knox Webhook Notification

To receive asynchronous notifications when a diagnostic log is generated:

1. Subscribe to the Knox Webhook Notification API using POST /kwn/v1/subscriptions operation.
2. In the request body, specify a subscription URL to receive callbacks and the KAI_DEVICE_DIAGNOSTICSLOGS event to subscribe to notifications for diagnostic log generation events.

For example, the following request body allows you to be notified on the specified subscription URL, when Knox Asset Intelligence completes log generation.


```
{
 "url": "https://some.domain/kwn-results",
 "events": [
  "KAI_DEVICE_DIAGNOSTICSLOGS"
 ]
}
```


The response message containing a specific download link and other log details is sent to the subscription URL. You can use the download link to view the log file generated by Knox Asset Intelligence.

For more information, see Knox Webhook Notification for Knox Asset Intelligence.

Monitor network events

The Knox Asset Intelligence APIs enable you to monitor network behavior of devices, allowing you to gather valuable data about network performance and track connectivity issues. This tutorial shows you how to retrieve the details of Wi-Fi connection and disconnection events.

Additionally, connection or disconnection of Wi-Fi leads to an event upload by Knox Asset Intelligence. You can subscribe to corresponding Knox Webhook Notification events to receive notifications for Wi-Fi related activities.

Prerequisites

Ensure that you have the necessary permissions to set or update the Knox Asset Intelligence settings, including obtaining an authentication token. For more information, see Get started.

Retrieve information about Wi-Fi connection events

1. To retrieve the Wi-Fi connection events data for a specific time period, make a GET request to the /wifi/connections endpoint.
2. In the request, you can make use of the following query parameters:
    - **pageNum** — Page number to retrieve.
    - **pageSize** — Number of items on a page.
    - **startDate** — Start time and date in milliseconds using Unix timestamp.
    - **endDate** — End time and date in milliseconds using Unix timestamp, its maximum possible duration from the start date is one day.

For example, the following request sample gives the Wi-Fi connection event information, such as channel, vendor name, serial number, and total number of Wi-Fi connection events, for the timeframe between 1675235605000 and 1675255086000 timestamps.

GET

/wifi/connections?

pageNum=0&

pageSize=100&

startDate=1675235605000&

endDate=1675255086000

You can adjust the parameters based on the network activity you want to monitor and the insights you want. For detailed response schema, see GET /network/wifiConnections.

You can receive notifications for Wi-Fi connection events using Knox Webhook Notification, if subscribed.

Retrieve information about Wi-Fi disconnection events

1. To retrieve the Wi-Fi disconnection events data for a specific time period, make a GET request to the /wifi/disconnections endpoint.
2. In the request body, you can make use of the following query parameters:
    - **pageNum** — Page number to retrieve.
    - **pageSize** — Number of items on a page.
    - **startDate** — Start time and date in milliseconds using Unix timestamp.
    - **endDate** — End time and date in milliseconds using Unix timestamp, its maximum possible duration from the start date is one day.

For example, the following request sample gives the Wi-Fi disconnection event information such as channel, vendor name, serial number, and total number of Wi-Fi disconnection events for the timeframe
between 1675235605000 and 1675255086000 timestamps.

GET

/wifi/disconnections?

pageNum=0&

pageSize=100&

startDate=1675235605000&

endDate=1675255086000

You can adjust the parameters based on your monitoring needs to gain insights into the network activity. For detailed response schema, see GET /network/wifiDisconnections.

These Wi-Fi disconnection events can be notified to you through Knox Webhook Notification, if subscribed.

Ensure that you check the code and message in the response for any errors and handle them appropriately for your app. For detailed specification, see Knox Asset Intelligence API.

Create a subscription in Knox Webhook Notification

To receive asynchronous notifications when a Wi-Fi connection or disconnection event occurs:

1. Subscribe to the Knox Webhook Notification API using the POST /kwn/v1/subscriptions operation.
2. To receive notifications for Wi-Fi connection events, in the request body, provide a subscription URL to receive callbacks and the KAI_WIFI_CONNECTIONS event.

For example,

{

"url": "https://some.domain/kwn-results",

"events": [

"KAI_WIFI_CONNECTIONS"

]

}

3. To receive notifications for Wi-Fi connection events, in the request body, provide a subscription URL to receive callbacks and the KAI_WIFI_DISCONNECTIONS event.

For example,

{

"url": "https://some.domain/kwn-results",

"events": [

"KAI_WIFI_DISCONNECTIONS"

]

}

The responses of both the above request samples contain a download link, which is then sent to the subscription URL along with other details about the logs. You can use the download link to view the log file generated by Knox Asset Intelligence.

For more information, see Knox Webhook Notification for Knox Asset Intelligence.

Monitor apps data

You can subscribe to Knox Webhook Notification events to receive notifications for the following app related data that Knox Asset Intelligence captures for your devices.

- Battery data of app usage.
- Screen time data of app usage.
- Network data of app usage.
- App no response (ANR) and force close (FC) data about ANR and FC event details of the apps.

For more information, see Knox Webhook Notification for Knox Asset Intelligence.

Monitor battery data

You can subscribe to Knox Webhook Notification events to receive notifications for the following battery related data that Knox Asset Intelligence captures for your devices.

- Battery status details which includes battery health and battery level.
- Battery charging details.
- Battery level details at the start and end of a device usage work shift.
- You can also monitor the battery level and get notified when it falls below the triggered battery level.

For more information, see Knox Webhook Notification for Knox Asset Intelligence.

Monitor miscellaneous data

The Knox Asset Intelligence APIs enable you to monitor data from the devices in your tenant, such as the status of events related to the Knox Service Plugin app. This tutorial shows you how to retrieve information related to Knox Service Plugin app for a specified time period.

Prerequisites

Ensure that you have the necessary permissions to set or update the Knox Asset Intelligence settings and obtain an authentication token. For more information, see Get started.

Get Knox Service Plugin app status

1. To retrieve information about Knox Service Plugin app status of devices, make a POST request to the /miscellaneous/getKspStatus endpoint.
2. In the request body, you can use the following optional parameters:
    - **pageNum** — Page number to retrieve.
    - **pageSize** — Number of items on a page.
    - **deviceIds** — List of the device IMEIs or serial numbers for targeted retrieval.
    - **kspStatus** — List the Knox Service Plugin app statuses that you want information for, its possible values are Success, Partial success, and Fail. If the last status is Partial success or Fail, a failure report is provided in the response.
    - **startDate** — Start time and date in milliseconds using Unix timestamp.
    - **endDate** — End time and date in milliseconds using Unix timestamp.
    - **groupName** — Name of the Knox Asset Intelligence device group you want information about. If this parameter is set to null, then all the groups are searched.

For example, the following request sample gives the Knox Service Plugin app status and details such as version, profile name, status, policy report, and policy schema for the device ID 111111112222222, in the timeframe between 1702612800000 and 17026128010000 timestamps.

```
{
  "pageNum": 0,
```

```
 "pageSize": 10,
 "deviceIds": [
  "111111112222222"
 ],
 "kspStatus": [
  "Success",
  "Partial success",
  "Fail"
 ],
 "startDate": 1702612800000,
 "endDate": 17026128010000
}
```


You can adjust the parameter values in the request body according to the kind of information you want to fetch, for example you can specify device ID, time period, kspstatus, or groupName. For detailed response schema, see POST /getKspStatus.

Ensure that you check the code and message in the response for any errors and handle them appropriately for your app. For detailed specification, see Knox Asset Intelligence API.

Manage the settings

The Knox Asset Intelligence APIs provide functionalities to manage tenant settings, offering greater visibility into device status and health. This tutorial shows you how to configure the threshold value for triggering a battery-level event using the settings endpoint. It sets up an alert for a device when its battery becomes low. Additionally, you can also use the settings endpoint to configure a device for Knox Configure enrollment.

Prerequisites

Ensure that you have the necessary permissions to set or update the Knox Asset Intelligence settings, including obtaining an authentication token. For more information, see Get started.

Set or update threshold and enrollment settings

To set or update Knox Asset Intelligence settings:

1. Make a PUT request to the /settings endpoint.
2. In the request body, use the batteryLevelThresholds property of battery object to set the threshold value for triggering a battery level event.

For example, the following request body sets the battery level threshold alert at 50 percent. This means when a device's battery level hits 50 percent, a battery level event is uploaded which notifies you through Knox Webhook Notification, if subscribed.

```
{
"battery": {
  "batteryLevelThresholds": [
  50
  ]
}
}
```

You can adjust the threshold value based on your low battery alert requirements. The possible values for the battery level threshold range from 1-99, and a maximum of three threshold values can be set.

For example, the following request body sets three battery level alerts at threshold values of 50, 30, and 10 percent. When a device's battery level hits the specified percentage value, a battery level event is uploaded.

```
{
"battery": {
  "batteryLevelThresholds": [
  50, 30, 10
  ]
}
}
```

If you are subscribed to Knox Webhook Notification for these events, you will receive notifications for them.

3. Similarly, in the request body, use the allowEnrolledToKnoxConfigure property of the enrollment object to permit enrollment of devices in Knox Configure.

For example, the following request body sets the enrollment permission to True. By default, it is set to false, and setting it to true means the devices now have permission to enroll in Knox Configure. In this example, the battery level threshold alert is also set to 50 percent.

```
{
"battery": {
  "batteryLevelThresholds": [
  50
  ]
"enrollment" : {
  "allowEnrolledToKnoxConfigure" : true}
}
}
```

For detailed response schema, see PUT /settings.

Get threshold and enrollment settings

To retrieve Knox Asset Intelligence settings, make a GET request to the /settings endpoint. It allows you to check the values set for triggering low battery level events and whether or not the devices are allowed to enroll in Knox Configure.

Ensure that you check the code and message in the response for any errors and handle them appropriately for your app. For detailed specification, see Knox Asset Intelligence API.

Create a subscription in Knox Webhook Notification

To receive asynchronous notifications when a low battery event is triggered:

1. Subscribe the Knox Webhook Notification API using POST POST /kwn/v1/subscriptions operation.
2. In the request body, provide a subscription URL to receive callbacks and the KAI_BATTERY_LEVEL_TRIGGERED event to subscribe to notifications for device battery level events.

For example, the following request body allows you to be notified on the subscription URL, when the battery level falls below the set threshold.

{

"url": "https://some.domain/kwn-results",

"events": [

"KAI_BATTERY_LEVEL_TRIGGERED"

]

}

The response message containing information about the triggered battery level event is sent to the subscription URL.

For more information, see Knox Webhook Notification for Knox Asset Intelligence.

Release notes

Improvements to Battery SOH

Previously, in POST /devices/getDevices, the batterySoh request parameter for the Battery state of health (SOH) insight supported the values: Good, Normal, Bad.

With Knox Asset Intelligence 25.01, a new value Weak is also added to indicate a drop in battery health due to frequent charging cycles. The response of POST devices/getDevices is also updated to include information about Weak Battery SOH devices.

Ability to assign devices to a group

With Knox Asset Intelligence 24.09, you can now assign a device to a group using a new operation. The POST /devices/groups operation enables you to map the device IDs to the group names, this grouping enhances the ability to manage the devices in your tenant.

Support to retrieve information about your groups

Knox Asset Intelligence 24.09 provides a new GET /devices/groups operation to retrieve a list of all groups in your tenant. This list includes information such as the number of groups, group name and description, and the device count in a group.

Support to list the devices in a group

Knox Asset Intelligence 24.09 provides a new groupName parameter in the request body of the POST devices/getDevices operation. You can specify the group name for which you want to retrieve the list of the associated devices.

The response of the POST devices/getDevices operation now also contains the group name information of the devices.

Ability to verify Knox Service Plugin details on a device

With Knox Asset Intelligence 24.09, you can now use the POST /miscellaneous/getKspStatus operation to retrieve information related to Knox Service Plugin from a specific time period. The returned information includes version, profile name, status, policy report, policy schema, and so on. You can specify the time period using the startDate and endDate parameters.

Ability to check the device storage

The POST devices/getDevices operation now provides new response parameters — internalStorage and internalUsedStorage that provide information about the internal storage status of devices.