IoT Device Management

Product Introduction

Issue	01
Date	2019-06-25

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

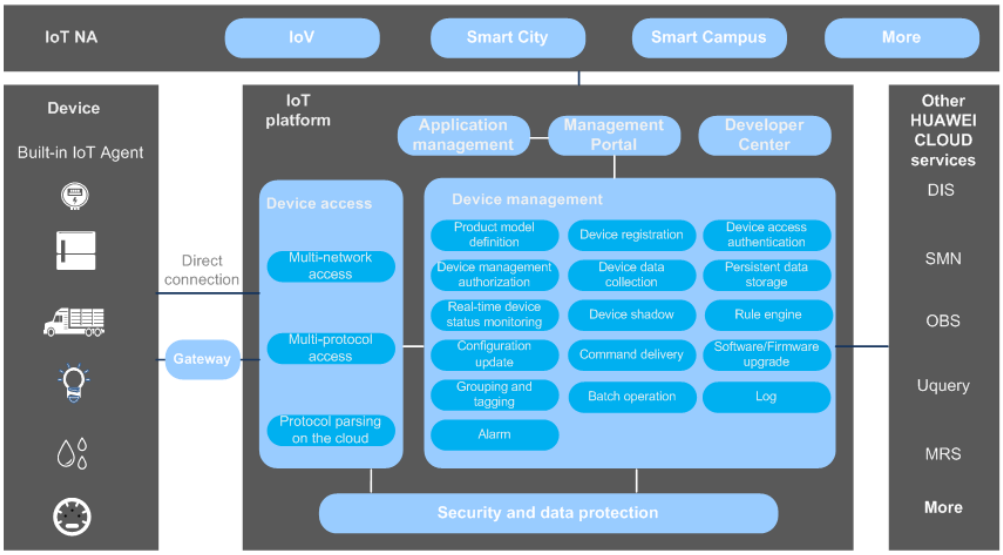
The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Platform Overview

The IoT platform connects to and manages a large number of devices. It works with other HUAWEI CLOUD services to quickly build IoT applications.



Device Access

Devices can connect to the IoT platform directly or through industrial or home gateways. They can also access the IoT platform using a variety of protocols and different Agents through multiple types of networks. Protocols are parsed on the cloud for fast device access.

- Multi-network access: Wired and wireless access, such as fixed broadband (FBB), 2G/3G/4G/5G, NB-IoT, Z-Wave, Zigbee, and eLTE-IoT are supported.
- Multi-protocol access: Access using HTTPS+MQTTS, MQTTS, and LWM2M/CoAP is supported.
- Multi-Agent access: Agents such as AgentLite and AgentTiny, and languages including C, Java, and Python are supported. Agents are pre-integrated with chipsets and modules of mainstream brands such as HiSilicon and Qualcomm to shorten the TTM.
- Protocol parsing: The IoT platform supports access protocol and device data parsing on the cloud without converting the data format on the device side.

Device Management

The IoT platform provides a broad set of device management functions. You can manage devices on the management portal or by calling APIs.

Function	Description
Product model definition	A product model includes the properties of a device, such as the color, size, collected data, identifiable commands, and reported events. The manufacturer, device type, and device model are used to uniquely identify a type of device.
Device registration	You can create a device and configures the device information on the IoT platform.
Device access authentication	The IoT platform authenticates devices while they are accessing the IoT platform. Information including device data integrity and security is authenticated, ensuring secure device access.
Device management authorization	The IoT platform allows an application to grant management rights of its bound devices to another application so that you can manage devices bound to multiple applications.
Device data collection	The IoT platform collects device data, such as device service data and alarms, and it allows applications to subscribe to device data.
Persistent data storage	The IoT platform stores data reported by devices and allows you to view historical data by hour, day, or month. Historical data can be stored for a maximum of seven days.
Real-time device status monitoring	The IoT platform monitors the device status in real time, and conveniently notifies you of status changes.
Device shadow	A device shadow is a JSON file used to store the reported and expected device status for NAs. Each device has only one shadow. The device can obtain and set its shadow to synchronize the status, either from the device shadow to the device or from the device to the device shadow.
Rule engine	The rule engine allows you to set rules for devices connected to the IoT platform as needed. After rule conditions are met, the devices trigger corresponding actions. The IoT platform supports the following rules: ● Device linkage: If a rule condition (such as temperature threshold or time) is set, the IoT platform triggers an instruction to enable the device to perform an operation (such as reporting data, enabling a device switch, or reporting an alarm) when the condition is met. ● Data forwarding: Device data received by the IoT platform can be forwarded to other services of HUAWEI CLOUD for analysis and storage.
Device configuration update	You can deliver commands to update device properties through NAs or the management portal.

Function	Description
Device command delivery	You can deliver commands to remotely control devices through NAs or the management portal.
Software/ Firmware upgrade	The software and firmware of devices can be upgraded in over the air (OTA) mode, and the software/firmware upgrade policies (on groups, upgrade time, concurrency control, and more) can be configured to provide flexible upgrades.
Device grouping and tagging	The IoT platform allows you to group and tag devices, thereby reducing device management costs.
Batch device operation	You can perform batch operations on devices, including batch device registration, batch configuration update, batch command delivery, and batch software/firmware upgrade.
Device logs	You can remotely maintain devices by checking device logs collected by the IoT platform.
Alarms	You can manage device alarms, including viewing alarm details and clearing alarms.

Security and Data Protection

The IoT platform provides multiple security measures to ensure device security and effective data protection.

- Device security: A one-device-one-secret authentication mechanism is provided to prevent unauthorized access.
- Data transmission: Secure transmission channels are provided based on TLS, DTLS, and DTLS+.
- Data protection: GDPR requirements are fully met.

Application Management

The IoT platform provides you with a wide range of APIs and SDKs, including secure NA access, device management, data collection, command delivery, batch processing, and message pushing APIs.

Management Portal

You can manage devices and applications conveniently and efficiently using the management portal. The following functions are provided:

- Dashboards: provides dashboards for you to view the usage of applications and devices.
- Logs: Logs on operations (such as login, logout, and password change) and system security are recorded for fault analysis and location.

Developer Center

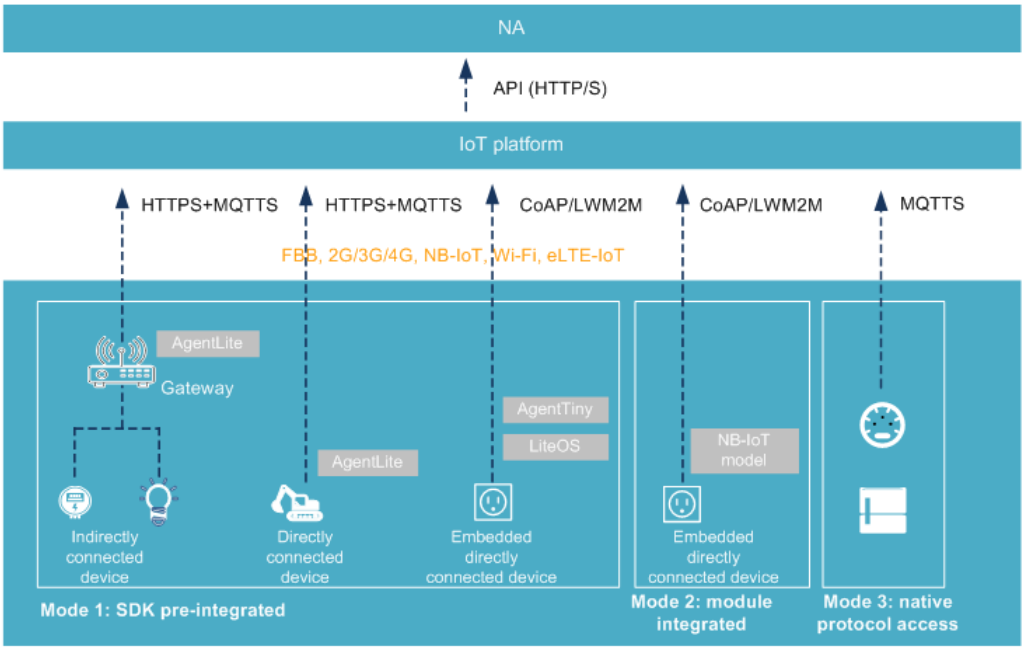
The Developer Center is a one-stop development tool provided by the IoT platform. It helps you conveniently develop products, devices (profile files), and codecs, perform automatic testing, and generate test reports.

2 Function Description

2.1 Device Access

Devices can connect to the IoT platform directly or through gateways. They can also access the IoT platform using a variety of protocols and different Agents through multiple types of networks. Protocols are parsed on the cloud for fast device access.

- Multi-Agent access: Agents such as AgentLite and AgentTiny, and languages including C, Java, and Python are supported. Agents are pre-integrated with chipsets and modules of mainstream brands such as HiSilicon and Qualcomm to shorten the TTM.
- Multi-protocol access: Access using HTTPS+MQTTS, MQTTS, and LWM2M/CoAP is supported.
- Multi-network access: Wired and wireless access, such as fixed broadband (FBB), 2G/3G/4G/5G, NB-IoT, Z-Wave, Zigbee, and eLTE-IoT are supported.



Method 1: agent pre-integrated

- Indirectly connected device: The Huawei AgentLite SDK is integrated on a gateway, and devices that do not have the IP capability are connected to the IoT platform through the gateway. This method applies to industrial IoT and smart campus scenarios.
- Directly connected device: Computing and storage devices that have IP capabilities are directly integrated with the Huawei AgentLite SDK and can connect to the IoT platform over HTTPS+MQTTS.
- Embedded, directly connected device: Lightweight embedded devices such as sensors, meters, and controllers are integrated with the Huawei AgentTiny SDK (which can be used together with LiteOS) and can connect to the IoT platform over CoAP/LWM2M. This method applies to scenarios that require low power consumption and low real-time performance, such as smart metering.

Mode 2: module integrated

Lightweight embedded devices such as sensors, meters, and controllers are integrated with Huawei certified communication modules and can connect to the IoT platform over CoAP/LWM2M. This method applies to scenarios that require low power consumption and low real-time performance, such as smart metering.

Method 3: native protocol access

Devices can connect to the IoT platform over the native MQTTS protocol. This applies to persistent connection scenarios, such as smart street lamps.

2.2 Device Management

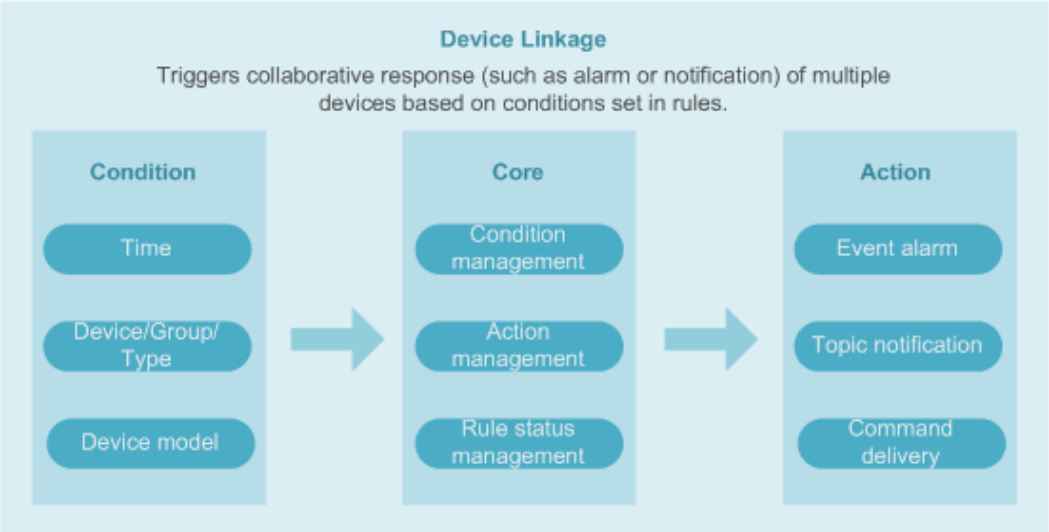
2.2.1 Rule Engine

The rule engine function allows you to set rules for devices connected to the IoT platform. If the conditions set in a rule are met, the IoT platform triggers the corresponding action. Device linkage and data forwarding rules can be created.

Device linkage rule

Device linkage is triggered by condition. Based on preset rules, the IoT platform triggers collaborative response of multiple devices to implement device linkage and intelligent control. If **Topic notification** is selected for **Action Type** in a rule, the IoT platform works with the **Simple Message Notification** service of HUAWEI CLOUD to set and deliver topic notification messages.

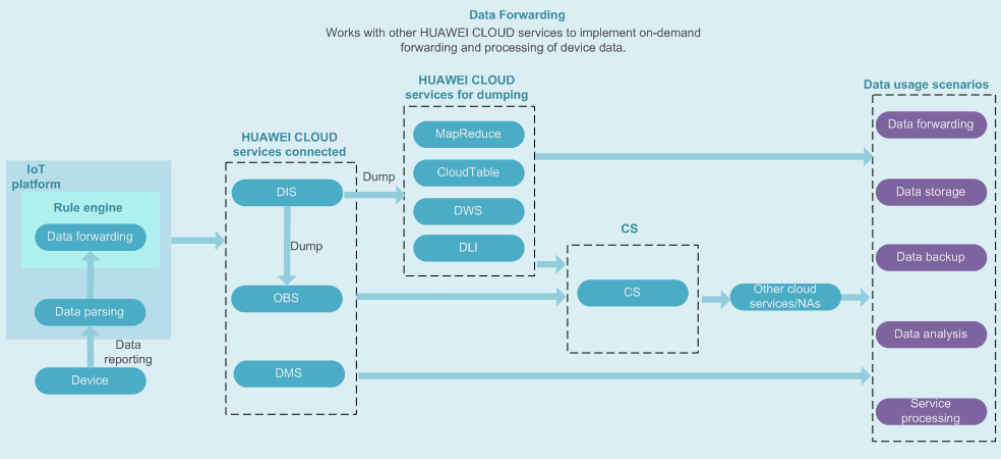
For example, when the battery level of a water meter is less than or equal to 20%, a low-battery alarm is reported. In this way, you can replace the battery in time.



Data forwarding rule

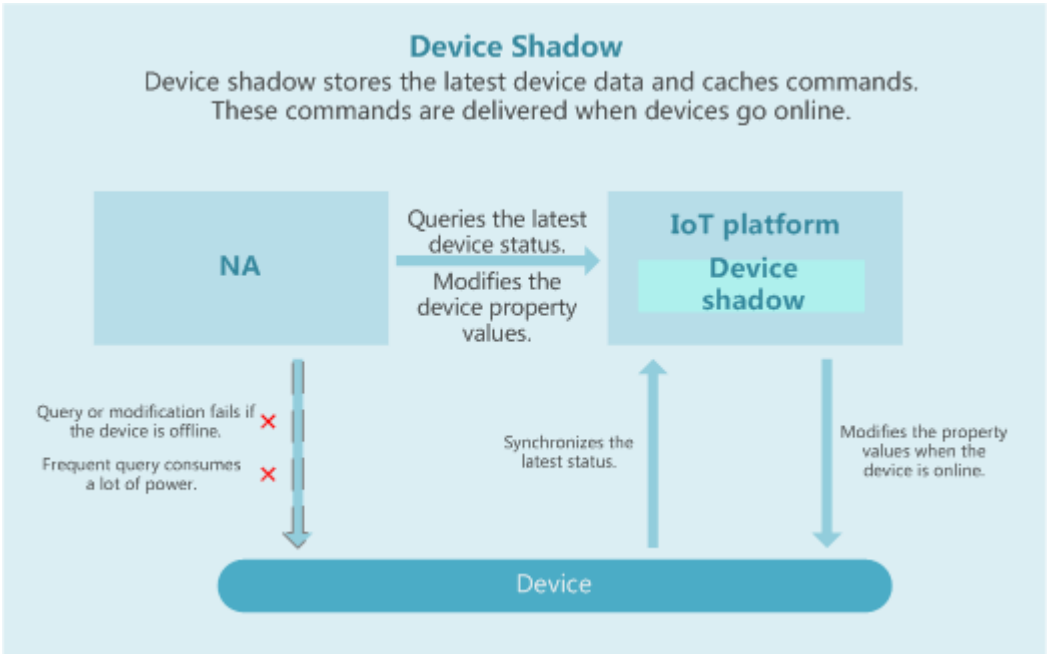
Data forwarding works with other HUAWEI CLOUD services to implement on-demand forwarding and processing of device data. You do not need to purchase servers to store, calculate, and analyze device data.

- Works with Data Ingestion Service (DIS) (coming soon) to enable efficient data collection, transmission, and distribution. You can download data by using the SDKs or APIs provided by DIS. You can also use dump tasks to forward data to Object Storage Service (OBS), MapReduce, CloudTable, Data Warehouse Service (DWS), and Data Lake Insight (DLI) for subsequent data processing, such as data storage and analysis.
- Works with **DMS** to provide message queues for device data. DMS is a message middleware service based on distributed, highly available clusters. The IoT platform functions as a producer to send messages to the DMS message queue. Your applications consume messages from the message queue. In this way, messages can be transmitted between multiple application components.
- Works with **OBS** to persistently store device data. (The IoT platform can store device data for 7 days). OBS is an object-based massive storage service that provides massive, secure, reliable, and low-cost data storage capabilities. It can archive, back up, and store data reported by devices. OBS can work with Cloud Stream (CS) (coming soon) to analyze data flows in real time. The analysis result is used for data visualization for other cloud services or third-party applications.



2.2.2 Device Shadow

The device shadow is a JSON file that stores the property values reported by a device and the property values that the IoT platform expects to deliver to the device. Only the latest reported values and expected values are stored on the device shadow. Each device has only one shadow. You can query and modify the device shadow, obtain the latest device property values, and deliver the expected values to devices through the Management Portal or by calling APIs.



The device shadow applies only to LWM2M devices in the following scenarios:

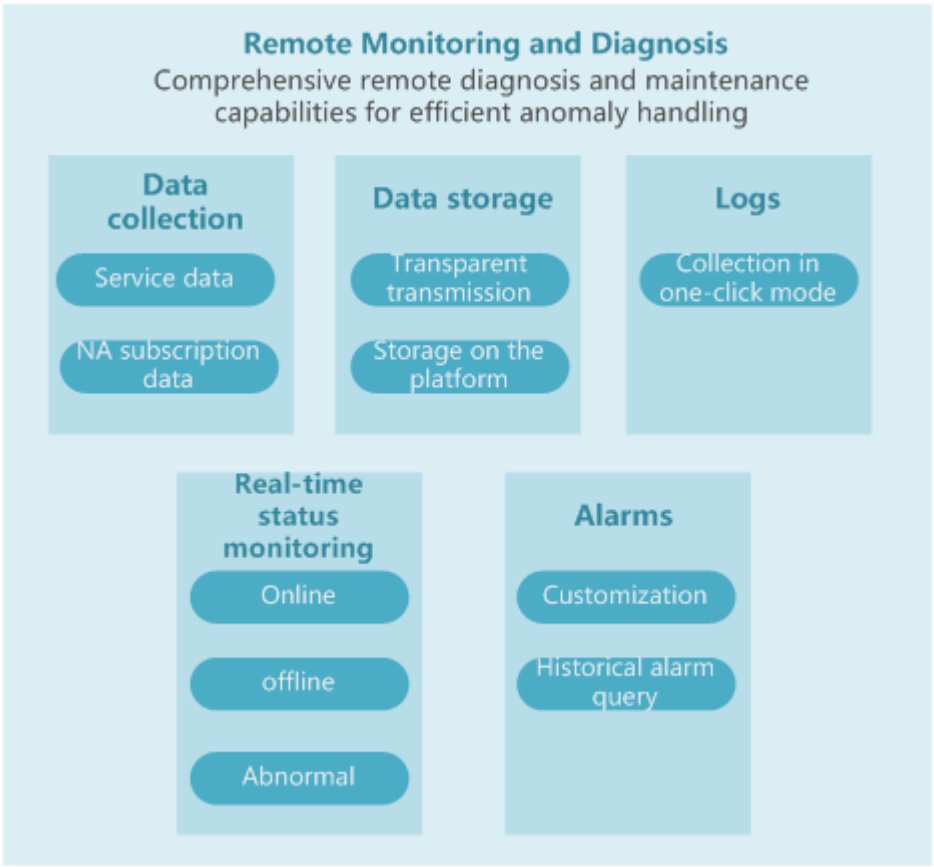
- Querying device status
  - If an NA queries the status of a device when the device is offline, the NA will not be able to obtain the device status in a timely manner. The device shadow stores the latest device status. Once the device status changes, the device synchronizes the device status to the device shadow. Using the device shadow, the NA can obtain the device status in time regardless of whether the device is online.
  - Many NAs frequently query the device status. Due to the limited processing capability of the device, frequent queries adversely affect device performance. The

device shadow enables the device to actively synchronize its status. The NAs request the device status from the device shadow. In this way, the NAs and the devices are decoupled.

- Modifying device property values: A device administrator modifies device property values through the management portal or by calling an API. If the modified configuration cannot be delivered to the device in a timely manner because the device is offline, the IoT platform stores the modified values in the device shadow. After the device comes back online, the IoT platform synchronizes the new device property values from the device shadow to the device.

2.2.3 Remote Monitoring and Diagnosis

The IoT platform provides remote diagnosis and maintenance capabilities to monitor device status in real time, and improve troubleshooting efficiency.



Device Data Collection

The IoT platform provides data collection and supports NA subscription to device events. Specifically, an NA subscribes to a device event, which carries the notification type and data such as device service data and device alarms, from the IoT platform. The IoT platform sends a message to notify the NA of the event.

You can also query the historical data that was reported by the devices, by hour, day or month.

Device Data Storage

The IoT platform processes data reported by devices in two ways:

- Transparent transmission: The IoT platform does not store or process the data reported, instead it transparently transmits the data to the NA. You can then directly process and analyze the data.
- Storage on the platform: The IoT platform stores data reported by the devices. Historical data can be stored for a maximum of seven days.

Device Logs

Device logs can be collected in one-click mode. Logs can be stored on the IoT platform for a maximum of 180 days.

Real-Time Status Monitoring

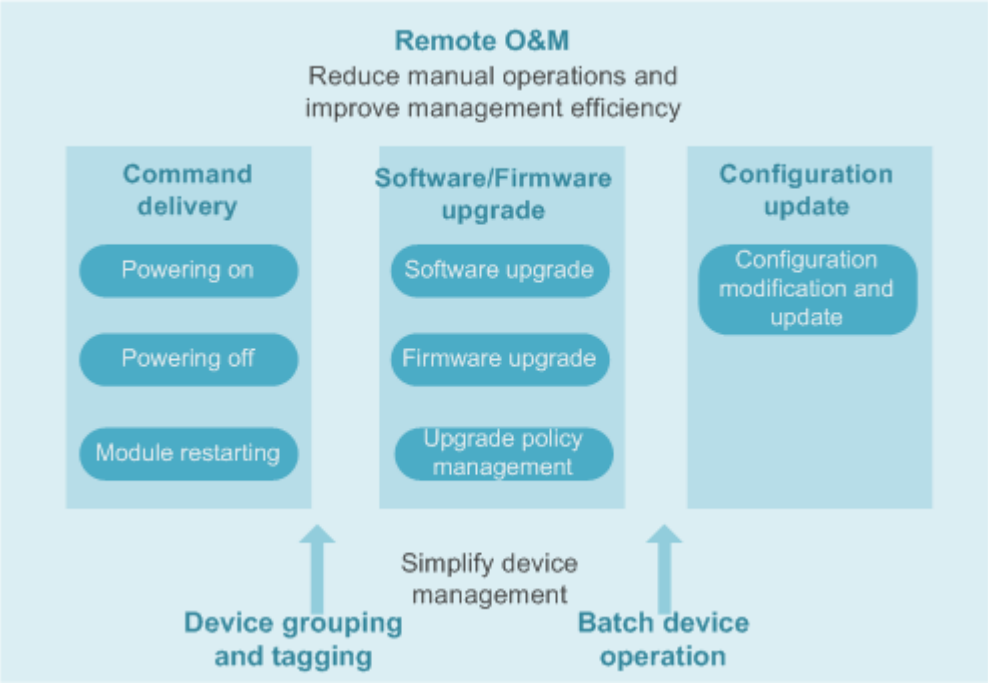
The IoT platform monitors the device status in real time, and conveniently notifies you of status changes.

Alarms

You can flexibly customize alarms and monitor device status based on the **rule engine**. You can also view historical alarms for data analysis.

2.2.4 Remote O&M

Devices can be grouped into batches to simplify their management. Remote command delivery, software/firmware upgrade, and device configuration updates improve management efficiency.



Device Command Delivery

Commands can be delivered to devices remotely through the management portal or by calling APIs, such as powering on or off a device.

You can also use the **rule engine** to automatically and intelligently control devices.

For NB-IoT devices, modules can be remotely restarted, but batch operations are not supported.

Software/Firmware Upgrade

OTA upgrade is supported for device software and firmware. You can flexibly upgrade devices using a range of upgrade policies that determine the upgrade time, upgrade group, and number of concurrent upgrade tasks.

Device Configuration Update

You can deliver commands to update device properties through the management portal or by calling APIs.

3 Product Highlights

IoT is becoming more and more popular, however, many enterprises may find their IoT transformation challenging due to issues such as fragmented access, complex device and security management, and inadequate platform capacity. To address the preceding pain points, the Huawei OceanConnect IoT Platform provides a series of solutions.

Traditional Platform		OceanConnect IoT Platform
Device access	● Different hardware development platforms, protocols, and networks complicate device access. ● Devices from multiple manufacturers and of various types are difficult to integrate with upper-layer applications.	The IoT platform supports multiple access networks, protocols, and provides SDKs in different languages for fast, convenient device access.
Device management	● Accessing a fleet of devices requires complex management. ● Devices are normally widely distributed, resulting in high labor costs.	The IoT platform provides device lifecycle management. It covers the profile definition, device registration, monitoring, configuration, upgrade, and remote fault diagnosis, which reduces manual operations and improves management efficiency.
Security and data protection	Security measures need to be developed and deployed in an end-to-end manner to ensure the security of devices, information transmission, and data.	The IoT platform provides multiple GDPR-compliant security measures to secure devices, information transmission, and data privacy.
Performance and stability	Independent architectures fail to support (concurrent) connections of a great number of devices.	The microservice carrier-class architecture supports hundreds of millions of connections and millions of concurrent connections. The service reliability achieves 99.9%.

Traditional Platform		OceanConnect IoT Platform
Scalability	Products for data storage, big data analytics, and message notification need to be purchased or developed. The labor and equipment costs are high.	The IoT platform interconnects with other HUAWEI CLOUD products based on the rule engine, such as the DIS, DMS, OBS, MRS, and SMN, which facilitates storage, computing, and intelligent analysis of a large amount of device data.

4 Limitations

The IoT platform has the following technical specifications. If the service cannot meet your service requirements, please **contact our salespersons**.

Device Access

Object	Description	Limit
Device quantity	Maximum number of devices for a single account	No limit
	Number of devices that can be connected to the IoT platform using the Developer Center during commissioning phase.	20
	Maximum number of sub devices that can be added to a gateway	1000
Connection and request	Maximum number of connections supported by a single MQTT device	1
	Maximum number of MQTT requests per second for a single connection	300
	Maximum throughput (bandwidth) of a single MQTT connection per second, including directly connected devices and gateways	3 KB/s
	Maximum length of a single message reported by an MQTT device	1 MB
	Maximum length of a single message reported by an LWM2M/CoAP device	1 MB

Device Management

Object	Description	Limit
Application	Maximum number of applications that can be created for a single account	10
	Maximum number of devices that can be registered for a single application	No limit
Product model (profile)	Maximum number of product models that can be created for a single application	20
	Maximum size of the product model package	4 MB
Batch device registration	Maximum number of devices that can be batch registered at a time	30,000
Historical device data	Maximum storage duration of historical device data (days) If a longer data storage duration is required, use the **Object Storage Service**.	7
Rule	Maximum number of rules that can be created for a single application	50
Device configuration update file	Maximum size of the configuration file for a device configuration update (only in JSON format)	200 KB
Batch command delivery	Maximum number of devices that a command can be batch delivered to	30,000
Software/Firmware upgrade	N/A	Only LWM2M devices are supported.
Number of devices for software/ firmware upgrade	Maximum number of devices for which the software/firmware can be upgraded at a time	30,000
Firmware upgrade package	Maximum size of the firmware upgrade package	200 MB
Software upgrade package	Maximum size of the software upgrade package	200 MB
Group	Maximum number of groups that can be created for a single application	10
	Maximum number of levels in a group	10
	Maximum number of groups that a device can be added to	1
Tag	Maximum number of device tags that can be created for a single application	2000

Object	Description	Limit
Device log	N/A	Only devices based on Huawei NB-IoT chipsets and LWM2M are supported.

Management Portal

Object	Description	Limit (for the IoT Advanced)
Dashboard	Maximum storage duration of report statistics	180 days
Audit log	Maximum storage duration of logs on the management portal	90 days

Northbound API

Object	Description	Limit (for the IoT Advanced)
Application	Maximum number of times that an application can call APIs per second	100
	Maximum number of messages pushed to an NA per second	Lower than 10 TPS (recommended). If the rate is higher than 10 TPS, use data forwarding rules.

5 Defined Terms

- Firmware

  Firmware refers to the drivers in a device. These are fundamental programs that run at the bottom layer of the operating system.

- Project

  A project refers to the resource space of the IoT platform. Developers need to create independent projects based on their own industries before developing IoT products and applications in the project space.

- Product

  A product is a collection of devices with the same capabilities or features. In addition to physical devices, a product also includes product information, product models (profile files), codecs, and test reports generated during IoT capability building.

- Product Model

  A product model (also called profile file) is used to describe the capabilities and features of a device. Developers construct an abstract model of a device by defining a profile file on the IoT platform so that the IoT platform can understand the services, properties, and commands supported by the device.

- Codec

  The IoT platform communicates with NAs using data in JSON format. Therefore, when a device reports data in binary format, developers need to develop codecs on Developer Center to help the IoT platform convert data into different formats.

- Device

  A device is a physical entity that belongs to a product. Each device has a unique ID. It can be a device directly connected to the IoT platform, or a gateway for sub devices to connect to the IoT platform.

- Gateway

  A gateway is a physical entity that manages sub devices and connects sub devices to the IoT platform.

- Sub Device

  A sub device is a physical entity that connects to the IoT platform through a gateway.

- Rule

  A rule is a preset condition used by the IoT platform to trigger actions. The device will report device data, which is checked against the rules. When a rule condition is met, the

IoT platform will trigger corresponding actions such as delivering a command to the device, or forwarding data to other HUAWEI CLOUD services for integration and utilization.

- Application

  The IoT platform involves applications created by users and network applications (NAs) developed by users. Applications are project entities created by users on the IoT platform. Each application is allocated an application ID and a secret for NA access authentication. An NA is an IoT application developed by users that can be connected to the IoT platform for device management.

- Message Queue Telemetry Transport (MQTT)

  MQTT is an IoT transmission protocol designed for lightweight release/subscription message transmission. It aims to provide reliable network services for IoT devices in low-bandwidth and unstable network environments.

  MQTTS refers to the combination of MQTT and SSL/TLS. The SSL and TLS protocols are used for encrypted transmission.

- Constrained Application Protocol (CoAP)

  CoAP is a software protocol designed to enable simple devices to perform interactive communication on the Internet.

  CoAPS refers to CoAP over DTLS. The DTLS protocol is used for encrypted transmission.

- Lightweight Machine to Machine (LWM2M)

  LWM2M is an IoT protocol defined by the Open Mobile Alliance (OMA). It mainly applies to NB-IoT devices with limited resources (such as limited storage and power supply).

