IoT Device Access

Service Overview

Issue 1.0

Date 2022-08-30

HUAWEI CLOUD COMPUTING 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 Cloud 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.

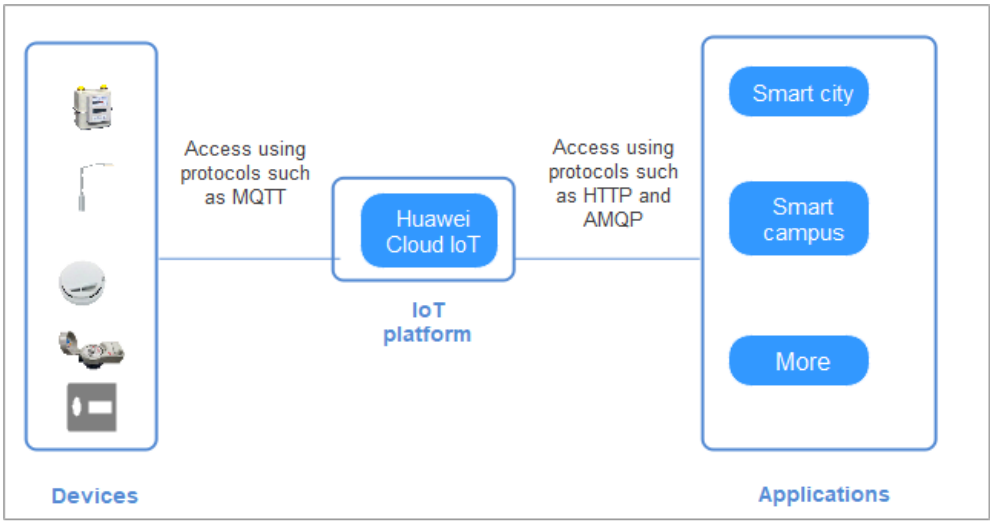
Contents

1 Overview

Huawei Cloud IoT Device Access (IoTDA) allows you to connect your physical devices to the cloud, where you can collect device data and deliver commands to devices for remote control. It can also work with other Huawei Cloud services to help you quickly develop IoT solutions.

A complete IoT solution consists of the IoT platform, devices, and applications.

- The IoT platform is located between applications and devices. It harmonizes differences between device interfaces to enable quick device access. It provides robust capabilities to help you develop diverse IoT solutions.
- Devices can access the platform via fixed broadband (FBB), 2G/3G/4G/5G, Narrowband Internet of Things (NB-IoT), and Wi-Fi networks. They can report service data to the platform using Message Queuing Telemetry Transport (MQTT), Lightweight Machine-to-Machine (LWM2M) over Constrained Application Protocol (CoAP), and Hypertext Transfer Protocol Secure (HTTPS). Devices can also receive commands from the platform.
- Applications call application programming interfaces (APIs) provided by the platform to implement service scenarios such as data collection, command delivery, and device management.



Devices can connect to the platform directly or through industrial gateways or home gateways. The platform supports multi-network access, multi-protocol

access, and serialized Agent access, preventing issues caused by complex, diversified, and fragmented device access. It also provides comprehensive device management capabilities, simplifies management of device fleets, and improves management efficiency. The following table describes the IoTDA functions.

Feature Category	Function	Description
Device access	Native protocol access	You can connect devices to the platform through MQTT, CoAP, LwM2M, and HTTP protocols.
	Generic-protocol access	Features open-source software development kits (SDKs) and technical frameworks. You can deploy cloud inter-networking gateways (CIGs) for protocol conversion or deploy the protocol drivers to edge gateways.
	Serial device SDKs	IoT Device SDK and IoT Device SDK Tiny for C and Java programming languages are supported. For details, see **Introduction to IoT Device SDKs**.
	Industry protocol access	You can connect devices to the platform through edge gateways using Modbus and OPC Unified Architecture (OPC UA) and using industry protocols based on plug-ins.
	Device access authentication	Authentication modes such as one-device-one-secret and X.509 certificates are supported.
Device management	Device lifecycle management	You can add, delete, modify, and query devices, manage device status, freeze and unfreeze devices, and manage child devices.
	Groups and tags	You can group or tag devices. For details, see **Groups and Tags**.
	Product model	You can define a product model (profile) for devices. For details, see **Product Model Definition**.
	Device shadow	You can configure and query device shadows. For details, see **Device Shadow**.
	OTA upgrade	You can upgrade the software and firmware of the device. For details, see **Firmware Upgrades** and **Software Upgrades**.
	Device file upload	Devices can upload files to OBS and request files from the cloud. For details, see **File Uploads**.
	Batch device operations	You can perform batch operations on devices, including **batch device registration**, **batch software/firmware upgrades**, and **batch command delivery** .

Feature Category	Function	Description
Message communications	Bidirectional transparent transmission	Device messages can be pushed to applications using HTTP and AMQP. Applications can deliver messages to devices asynchronously.
	Product model topic communications	Applications and devices communicate with each other based on the properties, commands, and events defined in the product model in a decoupled mode.
	Custom topic communications	You can customize topics for bidirectional message communications.
	Data parsing and conversion	You can develop codecs online to parse and convert device data.
	Command delivery	Commands can be delivered to online devices in synchronous mode. In the NB-IoT scenario, commands can be delivered in asynchronous mode. For details, see **Command Delivery**.
	Subscription and push	Applications can subscribe to data reported by devices through HTTP or AMQP.
Rules	Data forwarding	Data can be forwarded to Huawei Cloud Kafka, Object Storage Service (OBS), GaussDB, Data Ingestion Service (DIS), Distributed Message Service (DMS), ROMA Connect, and IoT Analytics (IoTA). For details, see **Rules**.
	Device linkage	You can create rules for device linkage control. For details, see **Rules**.
Monitoring and O&M	Logging	The console provides message tracing, integrates with Log Tank Service (LTS) for log analysis, and integrates with Cloud Trace Service (CTS) for log audit. For details, see **Monitoring and O&M**.
	Alarming	The platform provides notifications and management of system alarms (such as threshold alarms) and alarms triggered by device rules by integrating with Application Operations Management (AOM). For details, see **Alarms**.

Feature Category	Function	Description
	Metric monitoring	The platform provides monitoring reports of tenant-level service metrics (such as device status, commands, subscription and push, and message transfer) by integrating with AOM. For details, see **Reports**.
IoT device provisioning	Device bootstrapping	Following the bootstrap process, devices can obtain the correct target platform address when being powered on for the first time, and then establish links to the platform.
	Multiple provisioning policies	You can set multiple intelligent provisioning policies, such as fuzzy match of keywords, certificate-based provisioning, and custom provisioning policies.
	Device migration	You can reset device provisioning information as needed to migrate devices to another platform.

Security and Data Protection

IoTDA established an end-to-end trustworthy security system. It is graded level-4 of China's Multi-Level Protection Scheme 2.0 and obtains international security certifications such as ISO27001, ISO27017, ISO27018, and CSA STAR. It complies with European Union's General Data Protection Regulations (GDPR).

- Device security: It provides a one-device-one-secret authentication mechanism to prevent unauthorized access and supports device security check.
- Data transmission: Secure transmission channels are provided based on Transport Layer Security (TLS), Datagram Transport Layer Security (DTLS), and DTLS+.
- Platform security: Threat defense is performed on the entire Huawei Cloud. Huawei Cloud security service products or components and security D&R department are fully leveraged to build a comprehensive security defense system that covers security analysis, design, coding, testing, and defense.
- Data protection: It complies with European Union's General Data Protection Regulations (GDPR).

By means of quantitative traffic and remote card provisioning, Global SIM Link (GSL) enables devices deployed around the world to reliably access nearby Huawei Cloud sites and to use local payments.

2 Advantages

With service development, an increasing number of enterprises choose to combine IoT technologies for business growth. Huawei Cloud IoT services have outstanding advantages in capabilities, costs, O&M, security, and ecosystem compared with MQTT clusters managed by enterprises.

Table 2-1 Comparison

Dimension	Item	Huawei Cloud IoT	MQTT Clusters Managed by Enterprises
Capabilities	Flexible protocols	Supports mainstream IoT protocols and proprietary protocols to meet requirements of different devices and access scenarios. Provides the plug-in mechanism to parse custom protocols.	Supports only the MQTT protocol. The capability of supporting other protocols requires development. It is difficult, expensive, and inefficient to maintain multiple protocols.
	Access	Provides series of multi-language, open-source IoT device SDKs. SDKs are pre-integrated in popular modules and chips for multi-network and multi-protocol access. This simplifies device access and shortens the access time to hours.	Developers are required to be familiar with different programming languages, causing heavy development workload.

Dimension	Item	Huawei Cloud IoT	MQTT Clusters Managed by Enterprises
	Performance stability	Supports smooth and elastic expansion of service resources after purchase. Supports secure and stable connections of hundreds of millions of devices, reliable communications with 100,000 TPS concurrency, and devices going online concurrently with tens of thousands of TPS. Ensures 99.95% service availability.	R&D engineers need to perform tuning. To ensure 99.9% or higher availability, R&D engineers who are proficient in open source MQTT and senior architecture personnel are required.

Dimension	Item	Huawei Cloud IoT	MQTT Clusters Managed by Enterprises
	Features	• Cell-based technologies control the fault scope. • Message tracing facilitates fault locating and cause analysis. • Supports device shadows. • Supports over-the-air (OTA) upgrades. • Supports product models, which abstract and summarize product functions to decouple software and hardware development and improve system integration efficiency. • Supports the plug-in mechanism to parse custom protocols. • Supports data forwarding rules. Data can be forwarded to more than 10 cloud services. • Supports device linkage rules. Rules can be customized based on time, conditions, actions to configure scenario linkage and implement automatic collaboration across applications, subsystems, and devices. • The open architecture is used to leverage cutting-edge technologies and services of cloud computing. • Extensive functions and solutions have served many customers in different industries.	Open-source MQTT provides basic functions. Developers need to develop a complete solution based on open-source capabilities. However, some open-source code left unmodified during intrusive modification by developers may cause accidents on the live network during open-source middleware upgrades.
	-	-	-

Dimension	Item	Huawei Cloud IoT	MQTT Clusters Managed by Enterprises
	Technical support	Provides 24/7 professional support. The service ticket system responds within 10 minutes.	Open source MQTT does not provide technical support and has a large number of default configuration parameters. Enterprises need to adjust the parameters based on service scenarios. If developers of enterprises are not familiar with the open source code, their improper parameter adjustments pose huge potential risks to commercial systems. When problems occur, they have to solve problems by themselves.
Costs	Server cost	Servers do not need to be purchased.	Servers need to be purchased.
	Labor cost	No extra labor is required for cloud services.	Enterprises need to pay for professional development and O&M teams.
	Resource use	Resources are out-of-the-box and elastic for service growth and scale-out without interruption.	Enterprises need to develop the elastic resource scaling function by themselves.
	Architecture cost	The high-availability, high-performance, and secure architecture is built based on cloud native 2.0 and supports continuous evolution.	It is difficult for an enterprise to build the architecture that achieves high availability, high performance, and high security.
O&M	Infrastructure O&M	Provides unified O&M, quick response, scaling, upgrade, and troubleshooting based on professional teams.	Enterprises need to build their own O&M teams or use third-party O&M teams to solve scaling, upgrade, and O&M problems. Statistics show that most service faults are triggered by scaling and upgrade operations. The O&M cost is several times or even dozens of times the development cost.

Dimension	Item	Huawei Cloud IoT	MQTT Clusters Managed by Enterprises
	Service platform version	Provides unified update by public cloud service providers, fast version iteration.	It is managed by enterprises.
	O&M	• Provides full-link log analysis and message tracing. • Provides real-time monitoring and sensing of device statuses. • Supports custom service metric alarms.	It is managed by enterprises.

Dimension	Item	Huawei Cloud IoT	MQTT Clusters Managed by Enterprises
Security	System security	Establishes a trusted security system: It obtains international security certifications such as ISO27001, ISO27017, ISO27018, and CSA STAR. It complies with EU's GDPR. ● Transport network layer: Border security protection is provided based on web application firewall (WAF) and distributed denial of service (DDoS). Efficient, secure transmission protocols such as DTLS, TLS, HTTPS, CoAPS, and MQTTS are provided. ● Device side: A unique digital certificate is provisioned for each device for secure access. LiteOS-based security capabilities are provided. ● Platform side: Threat analysis is performed on entire Huawei Cloud network. Huawei Cloud security service products and public security services or components are fully reused to build a security defense system.	It is managed by enterprises. End-to-end security is a systematic project with high requirements. It is expensive and difficult to build and maintain system-level security capabilities.
	Data security	Provides a complete security protection system. Data is stored in redundant mode in the data center of the cloud service provider, ensuing data security.	Enterprises need to build data redundancy, backup, and recovery capabilities.

Dimension	Item	Huawei Cloud IoT	MQTT Clusters Managed by Enterprises
	Disaster recovery	Supports active-active service deployment, multi-data center DR, as well as high availability and DR capabilities based on multiple regions and availability zones (AZs).	Self-managed clusters usually do not have DR capabilities. Huge investment in active-active service deployment and DR devices often ends up with low return on investment (ROI).
	Vulnerability fixing	Establishes a comprehensive vulnerability management system and a dedicated security research department to detect, track, and fix vulnerabilities in a timely manner.	Most enterprises do not have a vulnerability management mechanism or fix vulnerabilities in a timely manner. As a result, they are prone to attacks and are not aware of attacks and data theft.
Ecosystem	Third-party access	Integrates upstream and downstream ecosystem resources and provides value-added services.	It is built by vendors.
	Scalability	1. The platform supports fast scale-out of tens of thousands of devices to hundreds of millions of devices without service interruption. 2. When other functions, such as AI, are required for service development, the platform can be seamlessly interconnected with other Huawei Cloud big data, EI, and middleware products to implement storage, computing, and intelligent analysis of device data at scale. In addition, cloud-based products support small-scale verification, facilitating fast, low-cost trial and error and service innovation.	The scaling period is long. Enterprises need to implement system or component interconnection. The labor and equipment costs are high.

Table 2-2 Expense comparison

Item	Huawei Cloud IoT	MQTT Clusters Managed by Enterprises
Cloud resource cost	One intermediate-frequency unit S2 allows a maximum of 10,000 registered devices, 15 million messages per day, and 1000 TPS upstream and downstream messages. Total price: CNY30,000/year	• Server resources: Two ECSs (4 vCPUs, 8 GB memory, and 40 GB high I/O disk) cost CNY4,565.80 per year. • Relational Database Service (RDS): The instance with minimal specifications (2 vCPUs, 4 GB memory, and 40 GB SSD disk) costs CNY4700 per year. • Public network access: If you use a free shared Elastic Load Balance (ELB) and purchase an Elastic IP (EIP) with the minimal specifications of 1 Mbit/s bandwidth, the price will be CNY184 per year. Total price: CNY9449.8/year
Labor cost	None	Basic middleware implements basic functions. • One engineer is required for routine O&M and R&D of the platform. • Assume that an engineer devotes 50% of efforts and the monthly salary is CNY10,000. • Total: CNY10,000 x 12 x 50% = CNY60,000/year Special functions are added based on the basic middleware. • Assume that only some functions are implemented without considering high availability, high performance, and high security of the platform. • Two full-stack development engineers are required for the platform frontend and backend development and O&M of functions such as device management, message communications, and rules. • One protocol professionals are required for device-side development, including implementing device access through native protocols, generic protocols industry protocols, and SDKs. • Assume that all engineers devote 100% of efforts and the monthly salary is CNY10,000. • Total: 3 x CNY10,000 x 12 x 100% = CNY360,000/month Bonuses and insurances are not included.

Item	Huawei Cloud IoT	MQTT Clusters Managed by Enterprises
Total	CNY30,000/year	Basic functions: CNY69,449.8/year Basic and special functions: CNY369,449.8/year

3 Specifications

Specifications of Standard Edition

IoTDA provides standard instances for device access and service processing. Each Huawei Cloud user can enable up to one standard instance in the same region. If it cannot meet your requirements, submit a service ticket. You can select the type and number of units in the standard instance to determine the total number of messages allowed per day between devices and the platform. If you increase the number of units of the same type, the total number of messages will increase and the function **limitations** will change as well.

After an instance is enabled, you are billed based on the usage duration (days) and unit type and quantity you select.

Table 3-1 Unit specifications

Unit Type	Messages/Day/ Unit	Message Size (KB)	Monthly Price/ Unit (Estimate)
Free unit SUF	10,000	4	Free
Small unit SU1	400,000	4	25 USD
Medium unit SU2	4,000,000	4	165 USD
Large unit SU3	40,000,000	4	1,050 USD

NOTE

- A standard instance can be configured with multiple units of the same type, for example, five SU1 units, but cannot be configured with different types of units, for example, two SU1 units and three SU2 units. You can change the number and type of units at any time. For example, you can upgrade two SU1 units to five SU1 units or two SU1 units to two SU2 units. You can enable only one SUF unit but 100 SU1, SU2, or SU3 units. An SUF unit can be upgraded to an SU1, SU2, or SU3 unit. After the upgrade, the original SUF unit is no longer retained.
- Number of messages: Charged messages include upstream and downstream messages between devices and the platform, messages sent by an application by calling platform APIs, and messages pushed by the platform to the server. Protocol messages, such as heartbeat messages and ACK messages at the protocol layer, are free of charge. For details, see **Table 4-2**. You are advised to limit the number of calls to ensure that the number of messages does not exceed the limit. If the limit is exceeded, IoTDA will generate an alarm and rejects messages. Upgrade the unit specifications or increase the number of units in a timely manner.
- Message size: The maximum length of a single message published using **MQTT** is 1 MB. The maximum length of a single message published using LwM2M over CoAP is 1 KB. If the message size exceeds the limit, the message will be rejected. A message that is smaller than or equal to 4 KB is counted as one message. A message that is larger than 4 KB is counted as two or more messages.
- Number of devices: A standard instance supports a maximum of two million registered devices. If you want to increase the quota, **submit a service ticket** to describe your requirements. The number of concurrent online devices supported is equal to the number of registered devices. When only an SUF unit is enabled, up to 1000 devices can be registered.
- TPS of upstream and downstream messages: It describes the maximum throughput of upstream and downstream messages per second, that is, the total number of messages sent from all devices in an instance to the platform and from the platform to devices per second. The quotas of a standard instance are determined by the type and number of units.

  Specific quota limits are as follows:

  SUF: 10 TPS/unit

  SU1: 10 TPS/unit

  SU2: 100 TPS/unit

  SU3: 1000 TPS/unit

  If the quotas cannot meet your service requirements, **submit a service ticket** to describe your requirements.
- For details about other limitations except for the specifications and quota limits listed above, see **Limitations**.

Example

Scenario: A user enables the IoTDA standard instance and plans to register 100,000 devices. The average number of online devices per day is 10,000. Each online device sends a message (smaller than 4 KB) to the platform every 5 seconds on average. No API calls or push messages are involved. The daily working duration is 8 hours.

The TPS of upstream and downstream messages is 2000 (10,000 devices ÷ 5 seconds/message/device). The total number of messages per day is 57,600,000 (8 hours x 60 x 60 seconds x 2000 TPS). In this case, you can purchase two SU3 units, which support 2000 TPS, 80 million messages per day, and up to 2 million registered devices, and cost about USD2100 (USD1050 x 2). Alternatively, you can purchase 20 SU2 units. Bills are generated and deduction is triggered every day.

4 Pricing Details

This topic describes the billing modes, billing items, configuration changes, renewal, expiration, and arrears of IoTDA.

Billing Modes and Items

Table 4-1 Standard Edition billing modes

Edition	Billing Mode	Billing Item	Unit Price
Standard	Pay per use	You are billed based on the instance specifications and required duration. For details about the Standard Edition specifications, see "Product Pricing Details".	For details about product prices, see "Product Pricing Details".

Table 4-2 IoTDA billing items

Item	Description	Billing Mode
Device messages	Messages sent by devices by calling the MQTT PUB interface	Pay per use
	Messages received by devices by calling the MQTT SUB interface	
	Messages sent by devices by calling the LWM2M Update/Notify interface	
	Response messages received by devices by calling the LWM2M Update interface	

Item	Description	Billing Mode
	Messages and properties reported by devices by calling the HTTP interface	
	Command messages sent by the platform by calling the LWM2M Read/Write/Write-Attributes/Execute interface and response messages reported by devices	
Application messages	Messages sent by applications by calling platform APIs	Pay per use
	Messages pushed by the platform to applications (including HTTP and AMQP messages)	
Messages forwarded by rules	Messages forwarded to other Huawei Cloud services using rules	Free
Protocol messages	Login messages Logout messages Heartbeat messages ACK messages at the protocol layer Subscription messages Unsubscription messages	Free

Configuration Changes of the Standard Edition

- You can increase the number of units in the instance online, for example, upgrading a Standard Edition instance from three SU2 units to five SU2 units.
- You can upgrade the unit type of an instance, for example, upgrading the instance units from SU2 to SU3.

  Note: The upgrade takes effect on all units in the instance.

Renewal

You can renew a resource package before it expires, or you can set auto-renewal rules for a resource package. For more information about renewing resource packages, see **Renewal Management**.

Expiration and Overdue Payment

Ensure that the balance in your Huawei Cloud account is sufficient to cover any upcoming charges. If a fee deduction fails due to insufficient balance, your account will be in arrears, which will affect the normal use of services. (If the balance is 0, the service can still be used.)

Huawei Cloud sets retention periods based on customer level. For details, see **What Is a Retention Period**.

- Within the retention period, new devices cannot be registered, messages cannot be reported from registered devices, and commands cannot be delivered to devices.
- If you do not pay the arrears after the retention period has expired, your IoTDA resources will be released and your devices will be deleted.

5 Limitations

The tables below describe IoTDA limits on the application, device, and platform sides. Check the specifications of the Standard Edition and Enterprise Edition in **Specifications**. If you need to extend these limits, **submit a service ticket**.

Application Limitations

Object	Description	Limit
Product	Maximum number of products that can be added using an account	1,000
	Maximum number of devices that can be added to a product	Maximum number of devices allowed in a single Standard Edition instance
Product model	Maximum size of a product model package	4 MB
Device number	Maximum number of devices that can be registered using an account	50,000
	Maximum number of online devices for an account	50,000
	Maximum number of child devices that can be added to a gateway	50,000
Device	Maximum number of devices that can be registered in a single SU1, SU2, or SU3 unit (Specifications of the same type of units can be accumulated.)	2,000,000
Device group	Maximum number of groups that can be created using an account	1,000
	Maximum depth of a group	5

Object	Description	Limit
	Maximum number of devices in a group	20,000
	Maximum number of groups that a device can be added to	10
Batch device registration	Maximum number of devices that can be registered at a time	30,000
Rules	Maximum number of data forwarding rules that can be created using an account	100
	Maximum number of device linkage rules that can be created using an account	5,000
	Maximum number of conditions that can be added to a rule	10
	Maximum number of actions that can be added to a rule	10
Batch task	Maximum number of batch tasks that can be processed by an account at a time	10
	Maximum number of subtasks that can be added to a batch task	30,000
Software/Firmware upgrade	Maximum number of software and firmware packages that can be added using an account	10,000
	Maximum size of a software package	60 MB
	Maximum size of a firmware package	60 MB
Tag	Maximum number of tags that can be bound to a resource	10
Subscription	Maximum number of subscriptions that can be added using an account	500
Application-side APIs	Maximum number of times that an account can call APIs per second (maximum number of downstream requests)	100
	Maximum number of times that an account can call a specific API per second (maximum number of downstream requests)	50 (unless otherwise specified)

Device Limitations

Object	Description	Limit
MQTT connection	Maximum number of concurrent connections to a directly connected MQTT device	1
	Maximum number of link setup requests initiated by a directly connected MQTT device per minute	5
	Maximum number of link setup requests of an account per second on the device side	500
	Maximum number of upstream requests of an account per second on the device side (assuming that the average payload of a message is 512 bytes)	20,000
	Maximum number of upstream messages per second for an MQTT connection	50
	Maximum bandwidth of an MQTT connection (upstream message)	1 MB (default)
	Maximum length of a publish message sent over an MQTT connection (Oversized messages will be rejected.)	1 MB
	Standard MQTT protocol	MQTT v5.0, MQTT v3.1.1, and MQTT v3.1
	Differences from the standard MQTT protocol	• QoS 2 is not supported. • **will** and **retain msg** are not supported.
	Security levels supported by MQTT	TCP channel and TLS (TLS v1, TLS v1.1, TLS v1.2, and TLS v1.3)
	Recommended heartbeat interval for MQTT connections	Range: 30s to 1200s; recommended: 120s

Object	Description	Limit
	MQTT message publish and subscription	A device can only publish and subscribe to messages of its own topics.
	Maximum number of subscriptions per MQTT subscription request	No limit
	Maximum length of a custom MQTT topic	64 bytes
	Maximum number of custom MQTT topics that can be added for each product	10
	Maximum number of CA certificates that can be uploaded for an account on the device side	10
LWM2M over CoAP connection	Supported LWM2M version	1.0.2
	Transport layer protocol	UDP
	Security level	DTLS v1.2
	Maximum length of a publish message (Oversized messages will be rejected.)	1 KB
	Maximum number of messages of a device per minute	300
HTTP connection	Supported HTTP version	HTTP 1.0 HTTP 1.1
	Supported HTTPS	The IoT platform supports only the HTTPS protocol. For details about how to download a certificate, see **Certificates**.
	Supported TLS version	TLS 1.2 and TLS 1.3
	Maximum body length	1 MB
	Maximum number of child devices of which properties can be reported by a gateway at a time	50

Platform Limitations

Object	Description	Limit
Device log	Device log collection	You can collect logs only for devices using Huawei NB-IoT chipsets or LWM2M on the IoTDA console.
Audit log	Maximum storage duration of logs	90 days
Dashboard	Maximum storage duration of reports	180 days
Device configuration update file	Maximum size of the configuration file for a device configuration update (only in JSON format)	200 KB

6 Terms

Term	Description
IoTDA	Short for IoT Device Access, a basic service of the Huawei Cloud IoT Platform. IoTDA provides functions such as device fleet access, bidirectional communication between devices and the cloud, batch device management, remote control and monitoring, OTA upgrade, and device linkage rules. It can flexibly transfer device data to other Huawei Cloud services. Using IoTDA, you can quickly connect devices to the platform and integrate your applications.
Product Center	A web page that displays commercial IoT products such as solutions, devices, and modules certified by Huawei's IoT ecosystem. The Product Center works with the IoT platform to make customers' products globally available, helping customers achieve profit.
Resource space	A space allocated for your applications. Resources (such as products and devices) created on the platform must belong to a resource space. You can use the resource space for domain-based management as well as resource isolation and authorization management.
AppID	Resource space ID (the **app_id** parameter for API calling) used as the unique identifier of the resource space.
ProjectID	Unique identifier of a project. A default project is provided for each Huawei Cloud region to group and isolate resources (including compute, storage, and network resources) across physical regions. IAM users can be granted permissions to access all resources in a specific project.
IAM	Short for Identity and Access Management, a Huawei Cloud service that provides identity authentication and permission management. You can use IAM to manage user accounts (such as employees, systems, and applications) and control the operation permissions of these users on your resources.

Term	Description
Subscription and push	Subscription: An application calls a platform API to learn changes to device service details (such as device registration, data reporting, and device status) and management details (such as software or firmware upgrade statuses and upgrade results) from the platform. Push: After a subscription is successful, the platform pushes the corresponding change to the specified callback URL or AMQP message queue based on the type of data subscribed.
AMQP	AMQP, an advanced message queue protocol at the application layer of the unified messaging service, is an open standard application layer protocol for message-oriented middleware.
Product	A collection of devices with the same capabilities or features. It helps developers quickly develop product models and codecs, and provides capabilities such as device integration, online commissioning, and topic customization, facilitating end-to-end IoT development and helping you improve integration development efficiency and shorten the construction period of IoT solutions.
Product ID	Identifies the product to which a device belongs. This parameter is used to associate the product model of the device.
Product model	Also called profile, a model that describes the capabilities and features of a device. You can construct an abstract model of a device type by defining a profile on the platform, allowing it to understand the services, properties, and commands supported by the device.
CoAP	A software protocol designed to enable simple devices to perform interactive communication on the Internet. CoAPS refers to CoAP over DTLS. DTLS is used for encrypted transmission.
LWM2M	Short for Lightweight Machine to Machine, an IoT protocol defined by Open Mobile Alliance (OMA). It is mainly used for NB-IoT devices with limited resources (such as limited storage and power supply).
MQTT	An IoT transmission protocol designed for lightweight publish/subscription messaging. It provides reliable network services for IoT devices in low-bandwidth and unstable network environments. MQTTS refers to the combination of MQTT and SSL/TLS. SSL and TLS are used for encrypted transmission.
Codec	Software used for format conversion. The platform communicates with applications using data in JSON format. For a device that reports data in binary format, you must develop codecs to help the platform convert data into different formats.

Term	Description
Topic	A UTF-8 character string functioning as the transmission medium of publish/subscription messaging. You can publish messages to or subscribe to messages from a topic.
Service	Part of the product model that describes the capabilities of a device. Device capabilities are divided into several services. The properties, commands, and command parameters of each service are defined in the product model.
Property	Part of the product model that describes the running status of a device, such as the current ambient temperature read by an environment monitoring device.
Command	A capability or method that can be invoked by external systems.
Event	A functional model of a device, which is an event during device running. Events can be subscribed to and pushed.
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 platform, or a gateway through which child devices are connected to the platform.
Device ID	Uniquely identifies a device. It is allocated by the platform during device registration and used for device access authentication and message transmission.
Node ID	A unique physical identifier for a device, such as its IMEI or MAC address. This parameter is used by the platform to authenticate the device during device registration.
Device CA certificate	A certificate issued by a certification authority (CA) such as VeriSign, Symantec, and GlobalSign and used to verify the identity between the server and client during HTTPS link establishment.
X.509 device certificate	A digital certificate used to authenticate communication entities. After a device with authentication mode set to X.509 certificate is created, the platform issues the X.509 certificate to the device.
Module	Also called a communications module, an independent display unit consisting of display modules, drive circuits, control circuits, chips, and mechanical parts. Devices communicate with the platform through modules. Currently, 2G/3G/4G/5G, NB-IoT, and Wi-Fi communications modules are provided.
Gateway	A physical entity that manages child devices and connects child devices to the platform.
Child device	A physical entity that connects to the platform through a gateway.
PSK	Used to encrypt the transmission channel between the platform and NB-IoT devices or devices integrated with the SDK.

Term	Description
Secret	Used for authentication when a device uses native MQTT to connect to the platform.
Firmware	A driver underlying the device hardware. It is responsible for the underlying work of a system, for example, the basic input/output system (BIOS) on a computer mainboard. Firmware upgrade, also called firmware over the air (FOTA), allows users to upgrade the firmware of LWM2M or MQTT devices in OTA mode. For example, an upgrade of an NB-IoT module is a firmware upgrade.
Software	Consists of system software and application software. The system software is for the basic device functions, such as the compilation tool and system file management. The application software provides functions such as data collection, analysis, and processing, depending on the features of the device. Software upgrade, also called software over the air (SOTA), allows users to upgrade the software of LWM2M or MQTT devices in OTA mode. For example, an MCU upgrade is a software upgrade.
PCP	A protocol that defines the communications content and format between devices and the platform for device upgrades.
IoT Edge	An open platform located close to devices or data sources. It integrates core capabilities of network, compute, storage, and applications to provide compute and intelligence services locally, making real-time services intelligent and ensuring data privacy and security.
Group	A collection of devices. You can create groups for all the devices in a project space based on different rules, such as regions and types, and you can manage and operate the devices by group.
Tag	You can define different tags, bind tags to devices, and filter devices by tag.
Device shadow	A JSON file that stores the device status, latest device properties reported, and device configurations to be delivered. Each device has only one shadow. A device can retrieve and set its shadow to synchronize the status, either from the shadow to the device or from the device to the shadow.
Rules	A preset condition used by the platform to trigger actions. The device will report device data, which is checked against the rules. When a rule condition is met, the platform will trigger corresponding actions such as delivering a command to the device or forwarding data to other Huawei Cloud services. You can create device linkage and data forwarding rules.
Token	An authentication parameter used to call platform APIs. When an application accesses the platform for the first time, it must call the authentication API to get authenticated and obtain a token.

