Alibaba Cloud IoT Platform

Product Introduction

Issue: 20190424

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

1 What is IoT Platform?

IoT Platform is a device management platform on Alibaba Cloud that enables developers of IoT applications to implement two-way communications between end devices (such as sensors, final control elements, embedded devices, and smart household electrical appliances) and the cloud by creating data channels.

IoT Platform has the following benefits:

Device Connection

IoT platform provides device SDKs to help you connect devices to Alibaba Cloud.

- Provides various solutions for connecting network equipment that uses 2G/3G/4G, NB-IOT, or LoRa technology, to help streamline the management of devices connected over heterogeneous networks.
- Provides device SDKs that support various protocols, such as the MQTT and CoAP protocols. This achieves not only real-time synchronization capabilities by enabling persistent connections, but also energy efficient requirements by enabling transient connections.
- Supports various open-source programming languages and provides guides for embedding SDKs into different chips using your preferred programming languages . This allows enterprises to connect devices with various chips to IoT Platform.

Device Communication

Devices can use the IoT platform for two-way communication with the cloud through the IoT Hub. The platform enables upload and download channels between devices and the cloud to ensure that two-way communications between the devices and the cloud are smooth and reliable.

Device Management

IoT Platform manages the entire life cycle of devices, including device registration, function definition, script parsing, online debugging, remote configuration, firmware upgrade, remote maintenance, real-time monitoring, grouping, and device removal.

- Provides Thing Specification Language to simplify application development.
- Pushes notifications when a device changes status.

- Provides data storage capabilities, making it easy to read and write massive amounts of device data in real time.
- Supports the remote upgrade of devices based on Over-The-Air (OTA) technology.
- Provides a device shadow feature that decouples devices and applications to address scenarios with unstable wireless connections.

Security

A multi-layered security strategy is provided to ensure the security of devices connected to the cloud.

- Authentication
  - Chip-level security solutions (ID^2) and the DeviceSecret mechanism are provided to prevent DeviceSecret being cracked. Security level: high.
  - The Unique Certificate per Device authentication mechanism is provided to prevent devices from being attacked. This mechanism applies to scenarios where pools of device certificates (consisting of ProductKey, DeviceName, and DeviceSecret) can be installed into device chips in mass production. Security level: high.
  - The Unique Certificate per Product authentication mechanism is provided to reduce the attack risk of devices. This mechanism applies to scenarios where pools of device certificates (consisting of ProductKey, DeviceName, and DeviceSecret) cannot be installed into device chips in mass production. Security level: medium.
- Communication Security
  - Supports various data channels that use TLS (for example, MQTT and HTTP) and DTSL (for example, CoAP) protocols to ensure the privacy and integrity of data. This applies to scenarios where hardware resources are sufficient, and devices are not sensitive to power consumption. Security level: high.
  - Supports custom data symmetric encryption channels that use TCP (for example, MQTT) and UDP (for example, CoAP) protocols. This applies to

scenarios where hardware resources are insufficient, and devices are sensitive to power consumption. Security level: medium.

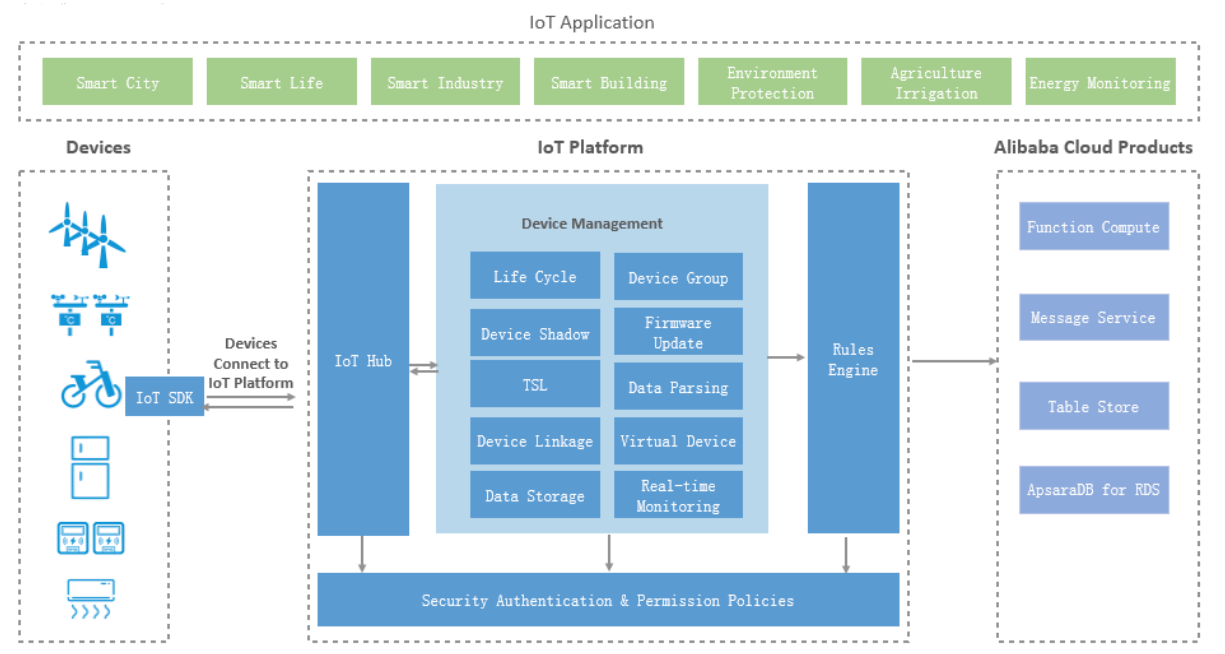
- Permission management is provided to ensure that communications between the devices and the cloud are secure.
- Device-level isolation of communication resources (such as Topic) is provided to prevent unauthorized operations on devices.

SQL parsing and data forwarding using the Rule Engine

IoT Platform can integrate with other Alibaba Cloud services by using the Rule Engine. You can set simple rules to transfer device data to Alibaba Cloud services for data storage and computing. The Rule Engine has the following features:

- Establishes M2M communications between devices using rules.
- Transfers data to Message Queue (MQ), ensuring that applications can access device data reliably.
- Transfers data to Table Store, supporting the integration of data acquisition and structured storage.
- Transfers data to Function Compute, supporting the integration of data acquisition and event-triggered processing.

2 Architecture



IoT Hub

The IoT Hub helps devices connect to the Alibaba Cloud IoT Platform service. The IoT Hub is considered as a data channel for secure communications between devices and the cloud. The IoT Hub supports both the Pub/Sub and Revert-RPC communication modes. The Pub/Sub mode is a message routing mode based on topics.

The IoT Hub has the following features:

- High scalability: supports linear dynamic scaling, and allows one billion devices to be connected simultaneously.
- End-to-end encryption: The entire communication link is encrypted with RSA and AES to ensure that the data transmission is secure.
- Real-time messages: After a data channel is successfully established between the device and the IoT Hub, it becomes a persistent connection to reduce handshake time and to ensure that messages arrive in real time.
- Data passthrough support: The IoT Hub supports binary format data passthroug h to the server. To keep data secure and controllable, the IoT Hub does not store device data.

- Various communication modes: The IoT Hub supports both the Pub/Sub and Revert-RPC communication modes in order to meet your communication needs in various scenarios.
- Support for multiple protocols: supports connecting devices to IoT Platform using the CoAP, MQTT, and HTTPS protocols.

Device management

IoT Platform offers various features to manage devices. These features manage the lifecycle, device groups, device shadows, firmware upgrade, Thing Special Language (TSL), data parsing, online debugging, remote maintenance, and real-time monitoring .

Rules engine

When a device communicates with IoT Platform using a topic, you can write an SQL expression to process the data in the topic. You can then configure rules to transfer data to other topics or Alibaba Cloud services. For example:

- You can transfer and store data to RDS, Table Store, and HiTSDB.
- You can transfer data to the DataHub and then use StreamCompute for stream computing or MaxCompute for large dataset offline computing. You can also transfer data to Function Compute for event-triggered processing.
- You can transfer data to Message Queue (MQ) for highly reliable data consumption.
- You can transfer data in one topic to another topic to establish M2M communicat ion between devices.

Security authentication and authorization policies

Security is very important to IoT. Alibaba Cloud IoT Platform offers a multi-layered security strategy to ensure that the connection between devices and the cloud is secure.

- Iot Platform issues a unique certificate for each device, and each device will use its unique certificate for authentication while connecting to the IoT Hub.
- IoT Platform provides various device authentication methods for developers to address different security needs and production line requirements.
- Authorization is provided at the device level. A device can only publish or subscribe to topics associated with that particular device. The server handles data through topics under the Alibaba Cloud account using the AccessKey.

3 Terms

The section describes the terms that are used in Alibaba Cloud IoT Platform.

Terms

Term	Description
Product	A product is a set of devices that have the same features. IoT Platform issues a unique ProductKey for each product. One product may consist of thousands of devices.
Device	A physical device that constitutes a product. IoT Platform issues a DeviceName that is unique under the same product for each device. Devices can connect directly to IoT Platform, or be mounted as sub-devices to a gateway that is connected to IoT Platform.
Gateway	A gateway can connect directly to IoT Platform and provide sub-device management features. Sub-devices can only communicate with IoT Platform through a gateway.
Sub-device	A sub-device is essentially a device. Sub-devices cannot connect directly to IoT Platform and can only get connected through a gateway.
Three key fields	The three key fields are `ProductKey`, `DeviceName`, and `DeviceSecr et`. · `ProductKey` is the unique identifier of a product in IoT Platform. This parameter is very important and used in device authentication and communication. You should keep this parameter safe. · `DeviceName` is the device name that is automatically generated or defined by the user during device registration. Each device has a unique DeviceName under the same product. This parameter is very important and used in device authentication and communication. You must keep this parameter safe. · `DeviceSecr et` is the private key issued by IoT Platform for each device. DeviceSecret is used in pair with DeviceName. This parameter is very important and used in device authentication. You must keep this parameter safe and never disclose this parameter.

Term	Description
ProductSecret	ProductSecret is the private key issued by IoT Platform for each product. ProductSecret is usually used in pair with ProductKey for unique-certificate-per-product authentication. This parameter is very important. You must keep this parameter safe and never disclose this parameter.
Topic	A topic is a UTF-8 character string that is used as a transmission medium during Pub/Sub communication. A device can publish messages to a topic or subscribe to messages from a topic.
Topic category	A topic category is a set of topics associated with different devices under the same product. ${productKey} and ${deviceName} can be combined to specify a unique device. A topic category is applicable to all devices under the same product.
Publish	The operation permission that allows a device to publish messages to a topic.
Subscribe	The operation permission that allows a device to subscribe to messages from a topic.
RRPC	RRPC is short for Revert-RPC. RPC (Remote Procedure Call) uses a form of client–server interaction, and allows you to execute a procedure in a remote place without knowing the details for the remote interaction. RRPC allows you to send a request to a specified device and receive a response from the device.
Tag	Tags consist of product tags and device tags. · Product tags describe the information that is common to all devices under the same product. · Device tags describe the unique features of devices. You can add custom tags based on your needs.
Alink	The protocol for communication between the devices and IoT Platform.
TSL model	IoT Platform uses the Thing Specification Language (TSL) to describe devices. A TSL model includes properties, services and events. TSL models use JSON format. You can organize data based on TSL and report data to the Cloud.
Property	A feature that describes the running status of a device, such as the temperature information collected by an environmental monitoring equipment. Properties support GET and SET request methods. Application systems can send requests to retrieve and set properties.

Term	Description
Service	A feature that describes the capabilities or methods provided by a device that can be used by external requesters. You can specify the input and output parameters. Compared with properties, services can use one command to implement more complex business logic, such as performing a specific task.
Event	A feature that describes the events that are generated when a device is running. Events usually contain notifications that require action or attention, and may contain multiple output parameters. For example, an event may be a notification that a task is completed, a device fault that has occurred, or a temperature alert. You can subscribe to or push events.
Data parsing script	For devices under a product created in IoT Platform Pro, if the passthrough or custom mode is used to send data to IoT Platform, you need to write data parsing scripts to convert the binary data or custom JSON data that is sent by the device to Alink JSON data.
Device shadow	A device shadow is a JSON file that is used to store the status information for a device or application. Each device has a unique device shadow in IoT Platform. Regardless of whether the device is connected to the Internet, you can use the device shadow to retrieve and set the device status through MQTT or HTTP.
Rules engine	Rules engine provides a SQL-based language that enables you to filter the data from topics and send processed data to other Alibaba Cloud services, such as Message Service and Table Store.

4 Benefits

More and more enterprises are employing Internet of Things (IoT) solutions to collect and manage data from devices and increase returns. However, transforming the IoT eco-system and building a powerful IoT platform is facing challenges. Alibaba Cloud IoT Platform offers the solutions to these issues.

The following table describes the differences between traditional IoT development and IoT development based on Alibaba Cloud IoT Platform:

	Traditional IoT development	Development based on Alibaba Cloud IoT Platform
Connect devices to IoT Platform	Requires infrastructure and support from embedded system developers and cloud developers. The development is heavy and inefficient.	Provides Software Development Kits (SDKs) for quick connections between devices and the cloud. IoT Platform supports connections to worldwide devices, devices in heterogeneous networks, devices running in multiple environments, and devices operating based on multiple protocols.
Performance	Requires manual architecture scaling. This results in difficulties in dispatching servers, load balancers, and other infrastructure at device level.	Supports persistent connections with more than 100 million devices and millions of concurrent connections, and allows horizontal architecture scaling.
Security	Requires the development and deployment of additional security measures. Securing device data can be challenging.	Provides multiple measures to secure data in the cloud: · Device authentication to guarantee the security and uniqueness of devices · Transmission encryption to prevent data tampering · Alibaba Cloud Security and authorization checks to secure the cloud

	Traditional IoT development	Development based on Alibaba Cloud IoT Platform
Stability	Requires manual detection of server faults and migrates services , and interrupts services during migration, resulting in service instability.	Ensures the service availability of up to 99.9%, and allows auto migration in a single point of failure .
Ease of use	Demands extra servers to build distributed architecture for load balancing, and requires costly development of a complete IoT system that handles connections, computing, and storage.	Supports device management on the same platform, real-time monitoring of devices, and seamless connections to Alibaba Cloud services, and enables flexible and easy implementation of complex IoT applications.

5 Limits

IoT Platform has the following limits.

Products and devices

Item	Description	Limit
Total tags	The maximum number of tags that a product, device, or device group can have.	100
Total products	The maximum number of products that an account can have.	1,000
Total devices	The maximum number of devices that a product can have. Note: If your business requires more devices, open a ticket in the Alibaba Cloud console and describe your requirements in the ticket.	500,000
Gateways and sub-devices	The maximum number of sub-devices that a gateway can have.	1,500
	The maximum number of sub-device channels that a gateway can have.	1,000
	The frequency in which sub-device configurations can be sent to the gateway.	Once every ten minutes.
Features (only for Pro Edition products)	The maximum number of features that a product can have.	200
	The maximum number of struct properties.	10
	If the data type of a feature is: · enum, the number of enumeration items cannot exceed 25. · text, the data cannot exceed 1,024 bytes. · array, the number of elements in an array cannot exceed 128.	-
	Each service can have a maximum of 20 input parameters and 20 output parameters.	20
	Each event can have a maximum of 20 output parameters.	20

Item	Description	Limit
Data parsing	The size of a data parsing script cannot exceed 48 KB.	48 KB
Remote configuration	The remote configuration file can only be in JSON format and cannot exceed 64 KB.	64 KB
Data storage	The data of Pro edition properties, events, and services is stored for 30 days.	30 days

Communication

Description	Limit
The maximum number of MQTT requests that each account can send per second.	500
The maximum number of MQTT requests that each device can send per second.	1
The maximum number of connection times that each device can try per minute.	5
The maximum number of message subscriptions that each device can have. If the maximum number is reached, new subscription request will be rejected. The device can get request results by verifying the SUBACK messages.	100
The maximum number of requests that devices of an account can send to IoT Platform per second.	10,000
The maximum number of requests that an account can send from IoT Platform to devices per second.	2,000
The maximum number of messages that can be sent to the Rules Engine per second for an account.	1,000
The maximum frequency in which a device can send messages to IoT Platform.	QoS 0: 30 messages per second. QoS 1: 10 messages per second.

Description	Limit
A device can receive messages in a frequency of 50 messages per second, but the Internet condition affects the performance. If the TCP write buffer is blocked, an error is returned. For example, if you use the Pub operation to send requests to a device, but the device cannot handle all the requests, you will receive an error due to throttling.  Note: If you use the MQTT protocol to connect your devices and IoT Platform, you cannot receive error messages resulting from throttling. However, you can view logs to detect which devices are being throttled.	50 messages per second
Bandwidth.	1,024 KB
The maximum number of unconfirmed message publishing requests that a single device can have. When the limitation is reached, no new publishing request from the device will be accepted, unless the server returns PUBACK messages.	100
The maximum storage time for messages that are sent with the sending method of QoS 1. If no PUBACK message from the device is received after the maximum storage time is used up, the request will be discarded.	7 days
The maximum size of a single message that is sent using MQTT. Messages exceed the size limit will be rejected.	256 KB
The maximum size of a single message that is sent using CoAP. Messages exceed the size limit will be rejected.	1 KB
The heartbeat interval of an MQTT connection can be 30 to 1200 seconds. If the heartbeat time is not within this range, the server will refuse to connect. We recommend that you set a value larger than 300 seconds. A heartbeat interval begins at the time when IoT Platform sends a CONNACK message to respond to a CONNECT message. When a message of PUBLISH, SUBSCRIBE, PING or PUBACK is received, the timer is reset. If no message is received after an amount of time has passed that is equal to 1.5 times the specified heartbeat interval, the connection will be closed.	30 to 1,200 seconds

Topics

Description	Limit
A product can have a maximum of 50 topic categories.	50
A device can only publish messages to and subscribe to its own topics.	-
Topics use UTF-8 encoded characters and cannot exceed 128 bytes.	128 bytes
The maximum number of slashes (/) can be included in a single topic.	7
The maximum number of messages to which servers of an account can subscribe per second.	1,000
The maximum number of topics that can be included in a subscription request.	8
After you subscribe to or unsubscribe from a topic, the change will take effect in 10 seconds. Subscriptions remain in effect until you unsubscribe from the topic. We recommend that you subscribe to topics in advance to avoid missing information. Example: A device sends a SUB request to topic A. After 10 seconds, the subscription takes effect and the device starts to receive messages in real time. The device will keep receiving messages from topic A.	10 seconds
Broadcast topic. A maximum of 1,000 devices can subscribe to the same broadcast topic. The server SDK can only send one broadcast per second.	1,000

Device shadow

Description	Limit
The maximum depth level of a device shadow JSON file.	5
The maximum size of a device shadow JSON file.	16 KB
The maximum number of attributes in a device shadow JSON file.	128
The maximum number of requests that a device can send per second.	20

Rules Engine

Description	Limit
Each account can have up to 1,000 rules.	1,000
Each rule can include a maximum of 10 data forwarding actions.	10
Data forwarding performance depends on the instance of the target cloud product. If the target instance has enough performance resources, Rule Engine can provide a data forwarding capability of 1,000 QPS for a single account. RAM users share the quota of the main account. A maximum of 1,000 messages can be forwarded to other cloud product instances by the Rule Engine per second. RAM users share the quota of the main account. A maximum of 1,000 messages can be forwarded to other cloud product instances by the Rule Engine per second.	1,000 QPS
Make sure that the instance of the target cloud product is in use. If the target instance crashes or has overdue payments, invalid parameters (such as invalid values and changed authorizations) or incorrect configurations, data forwarding will fail.	-
Data forwarded by Rules Engine may be received more than once. In a distributed environment, message balancing in real time may cause a message to be sent more than once.	-

APIs

API	One tenant (QPS)	One IP address (QPS)
Pub	1,600	100
RRpc	1000	100
PubBroadcast	1	100
Other APIs	50	100

- If you are calling an API and you receive an error (such as 29-31 in *Common errors*), try again later.