ALIBABA CLOUD

Alibaba Cloud

物联网平台

Product Introduction

Document Version: 20201030

Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice 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.
Warning	A warning notice 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 restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of 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 features:

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/5G, or NB-IOT 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.

Message Communication

Devices can use the IoT platform for two-way communication with your servers. The platform enables upstream and downstream channels to ensure that two-way communications between devices and servers are smooth and reliable.

Device Management

IoT Platform manages the entire life cycle of devices, including device registration, Thing Specification Language (TSL) definition, data parsing, online debugging, remote configuration, OTA 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 IoT Platform.

- Authentication
  - Chip-level security solutions 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 Rules Engine. You can set rules to transfer device data to Alibaba Cloud services for data storage and computing. The Rules Engine has the following features:

- Establishes M2M communications between devices.
- Transfers data to Message Service, ensuring that applications can access device data reliably.
- Transfers data to Tablestore, 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

Devices connect to IoT Platform, and communicate with IoT Platform. IoT Platform can forward device data to other Alibaba Cloud services for storage and processing. This is the basis to build IoT applications.

IoT SDK

IoT Platform provides multiple device SDKs to help you develop your devices and connect them to IoT Platform. After a device is integrated with a device SDK, you can securely connect the device to IoT Platform and use features such as device management, data analytics, and data forwarding.

Only devices that support the TCP/IP protocol can integrate with the provided SDKs.

For more information, see Device SDK Developer Guide.

IoT Hub

IoT Hub helps devices connect to Alibaba Cloud IoT Platform. IoT Hub acts as a data channel for secure communications between devices and IoT Platform. IoT Hub supports both the Pub/Sub and RRPC communication modes. The Pub/Sub mode is a topic-based message routing mode.

IoT Hub has the following features:

- High scalability: Supports linear dynamic scaling, and allows up to one billion devices to connect to IoT Platform simultaneously.
- End-to-end encryption: The entire communication link is encrypted with RSA or AES to ensure secure data transmission.
- Real-time messages: After a data channel is established between a device and IoT Hub, the channel becomes a persistent connection that can minimize the handshake time and ensure real-time arrival of messages.
- Support for data passthrough: IoT Hub supports binary data passthrough to the IoT Platform server. To keep data manageable and secure, IoT Hub does not store device data.
- Support for multiple communication modes: IoT Hub supports both the Pub/Sub and RRPC communication modes to meet your communication needs in various scenarios.
- Support for multiple protocols: Allows you to use the CoAP, MQTT, or HTTPS protocol to connect devices to IoT Platform.

Device management

Data forwarding

When a device communicates with IoT Platform by using a topic, you can write an SQL expression to process the data in the topic. You can then configure rules to forward data to other topics or other Alibaba Cloud services for processing and storage. Examples:

- Forward data to ApsaraDB for RDS and Table Store for storage.
- Forward data to Function Compute for event computing.
- Forward data to Message Service for consumption of highly available data.
- Forward data to another topic to implement M2M communication.

Security authentication and authorization policies

Security is very important to IoT. Alibaba Cloud IoT Platform provides multiple security policies to ensure secure communications between devices and IoT Platform.

- IoT Platform issues a unique certificate to each device. Each device uses its unique certificate for authentication when they try to connect to IoT Platform.
- IoT Platform provides multiple device authentication methods for developers to address different security needs and production requirements.
- IoT Platform grants permissions on a device basis. A device can publish messages and subscribe only to its own topic. IoT Platform identifies user permissions according to AccessKey information and allows users to operate only on authorized topics.

3.Terms

The article describes the terms that are used in 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.
device	A physical device that belongs to a product. IoT Platform issues a DeviceName that is unique under the same product for each device. Devices can directly connect to IoT Platform, or be attached as sub-devices to a gateway that is connected to IoT Platform.
group	IoT Platform allows you to create device groups. Each device group can contain devices of different products. You can use device groups to manage devices across products.
gateway	A gateway can directly connect to IoT Platform and allows you to manage sub-devices. Sub-devices can communicate with IoT Platform only by using a gateway.
sub-device	Sub-devices cannot directly connect to IoT Platform and must be attached to a gateway.
device certificate	A device certificate consists of ProductKey, DeviceName, and DeviceSecret. • ProductKey is the unique identifier of a product in IoT Platform. This parameter is required in device authentication and communication. You must safely keep this parameter. • DeviceName is the device name that is generated by IoT Platform during device registration. You can also upload custom device names. Each device has a unique DeviceName under the same product. This parameter is required in device authentication and communication. You must safely keep this parameter. • DeviceSecret is the private key that is issued by IoT Platform for each device. DeviceSecret is used in pair with DeviceName. This parameter is required in device authentication and communication. You must safely keep this parameter.
ProductSecret	ProductSecret is the private key that is issued by IoT Platform for each product. ProductSecret is used in pair with ProductKey for unique-certificate-per-product authentication. This parameter is required in device authentication and communication. You must safely keep this parameter.
Topic	A topic is a UTF-8 character string that is used as a transmission medium during publish/subscribe 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 that are associated with different devices under the same product. *${productKey}* and *${deviceName}* are used to specify a unique device. A topic category is applicable to all devices under the same product.

Term	Description
Publish	The allowed operation of a topic. If the Allowed Operation parameter of a topic is set to Publish, you can publish messages to the topic.
Subscribe	The allowed operation of a topic. If the Allowed Operation parameter of a topic is set to Subscribe, you can subscribe to messages from the topic.
RRPC	RRPC is short for revert-RPC. A remote procedure call (RPC) uses the client/server mode, and allows you to request a remote service without understanding the underlying protocol. An RRPC allows you to send a request from the server to a device and receive a response from the device.
tag	You can add tags to products, devices, and groups. • Product tags are used to describe the information that is common to all devices under the same product. • Device tags are used to describe the unique features of devices. You can add custom tags based on your needs. • Group tags are used to describe the information that is common to all devices in a group.
Alink protocol	The protocol for communication between the devices and IoT Platform.
TSL model	IoT Platform uses the Thing Specification Language (TSL) to describe device features. A TSL model defines the device properties, services, and events. TSL models use the JSON format. You can organize data based on a TSL model and submit the data to IoT Platform.
property	A TSL feature that describes the running status of a device, such as the temperature information that is collected by an environmental monitoring device. Properties support the GET and SET request methods. Applications can send requests to retrieve and set properties.
desired property value	IoT Platform allows you to set desired property values for a device. If the device is online, the property values on the device is updated in real time. If the device is offline, the desired property values are cached in IoT Platform. After the device goes online, it obtains the desired property values and updates the property values on the device.
service	A TSL feature that describes the capabilities or methods of a device. These capabilities or methods can be used by external requesters. You can specify the input and output parameters of a service. Compared with properties, services can use one command to implement more complex business logic, such as performing a specific task.
event	A TSL feature that describes the runtime events of a device. Typically, an event contains a notification that requires action or attention. An event 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.

Term	Description
data parsing script	For devices that use pass-through or custom-format data, you must write data parsing scripts in IoT Platform to parse the data. You must convert the binary data or custom JSON data that is submitted by the devices to the Alink JSON data that is supported by IoT Platform. You must also convert the Alink JSON data that is sent by IoT Platform to the custom-format data that is supported by the devices.
device shadow	A device shadow is a JSON file that is used to store the status information of a device or application. Each device has a unique device shadow in IoT Platform. Device shadows allow you to obtain and set the status of devices by using the MQTT or HTTP protocol regardless of whether the devices are connected to the Internet.
rules engine	You can create and configure rules in IoT Platform to achieve the following features: server-side subscription, data forwarding, and scene orchestration.
server-side subscription	Your business server can subscribe to messages of a product in IoT Platform. The following types of messages are included: upstream device messages, notifications of device status changes, notifications when a gateway discovers new sub-devices, notifications of device lifecycle changes, and notifications of device topology changes. Server-side subscription supports the following two methods: • AMQP: uses the Advanced Message Queuing Protocol (AMQP) to implement a server-side subscription. Your server connects to IoT Platform by using the AMQP protocol and receives messages from IoT Platform. • MNS: forwards messages to a specified Message Service (MNS) queue. Then, your server receives messages from the MNS queue.
data forwarding	You can use the data forwarding feature to forward data from a topic to another topic or another Alibaba Cloud service for storage or processing.
scene orchestration	You can use the scene orchestration feature to develop automated business logic in a visualized manner. You can define interaction rules between devices and deploy the rules in IoT Platform or edge instances.
unique-certificate-per-device authentication	A device certificate is burned to each device. The device certificate includes a ProductKey, DeviceName, and DeviceSecret. When you connect a device to IoT Platform, IoT Platform authenticates the device based on the certificate.
unique-certificate-per-product authentication	A product certificate is burned to all devices under the same product. A product certificate includes a ProductKey and ProductSecret. When a device sends an activation request, IoT Platform authenticates the device based on the certificate. If the authentication succeeds, IoT Platform issues a DeviceSecret to the device. Then, the device uses the DeviceSecret to connect with IoT Platform.
public instance	You can manage resources such as products, devices, and rules in IoT Platform instances. IoT Platform provides public instances by default. Public instances are deployed on Alibaba Cloud classic networks. Each public instance is shared by multiple Alibaba Cloud accounts. These accounts are logically isolated.

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
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.

	Traditional IoT development	Development based on Alibaba Cloud IoT Platform
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

This article describes the limits of IoT Platform.

Products and devices

Limited item	Description	Limit
Tags	The maximum number of tags that you can attach to a product, device, or device group.	100
Products	The maximum number of products that an Alibaba Cloud account can create.	1,000
Devices	The maximum number of devices that you can add to a product. Note • To obtain the number of devices in a product in a timely manner, we recommend that you set an alert threshold for the number of devices. This avoids unexpected errors when you add new devices to the product. For more information, see Create a threshold-triggered alarm rule. • If the number of devices exceeds the limit, you must create another product.	1,000,000
	The maximum number of devices that you can add to products by using an Alibaba Cloud account. Note If you need to extend the limit based on your business requirements, submit a tichet.	10,000,000
Gateways and sub-devices	The maximum number of sub-devices that you can attach to a gateway.	1,500
Thing Specification	The maximum number of features that you can add to a product.	300
	The maximum number of properties, events, or services that you can add to a product.	256
	The maximum number of parameters that can be specified for a property of the STRUCT data type.	50
	The maximum number of enumeration items that can be specified for a feature of the ENUM data type.	100
	The maximum number of characters that can be specified for a feature of the text data type.	10,240 characters

Specification Language (TSL) features	Description	Limit
	The maximum number of elements that can be specified for a feature of the array data type.	128
	The maximum number of request or response parameters that can be specified for a service.	20
	The maximum number of output parameters that can be specified for an event.	50
	The number of the last versions that can be saved for a single TSL model.	10
	The maximum size of a file when you import a TSL model.	256 KB
Device groups	The maximum number of groups that you can create by using an Alibaba Cloud account. These groups include parent groups and subgroups.	1,000
	The maximum number of devices that you can add to a group.	20,000
	The maximum number of groups to which a device can be added.	10
Data parsing	The maximum size of a script file that can be uploaded for data parsing.	128 KB
Remote configuration	The maximum size of a remote configuration file. The remote configuration file supports only the JSON format.	64 KB
Data retention period	The maximum number of days that property, event, and service data can be retained. Data is no longer retained after the specified period ends.	30
File management	The maximum size of files that an Alibaba Cloud account can store on IoT Platform servers.	1 GB
	The maximum number of files that a device can store.	1,000
OTA update	The maximum number of update packages that an Alibaba Cloud account can contain.	500
	The maximum size of a update package.	1,000 MB
	The maximum number of devices that can be updated at a time.	100,000

Connections and communications

Limited item	Description	Limit

Limited item	Description	Limit
Device access	The maximum number of connections that can be established with IoT Platform at a time if you use the same device certificate information. The device certificate information includes the Productkey and DeviceName parameters.	1
Connections	The maximum number of MQTT connection requests that an Alibaba Cloud account can make per second.	500
	The maximum number of connection requests that a device can make per minute.	5
Device subscription	The maximum number of topics to which a device can subscribe. After the limit is exceeded, subscription requests will be rejected. The device can check whether a subscription request succeeds by verifying the received SUBACK message.	100
Requests	The maximum number of requests that the devices of an Alibaba Cloud account can send to IoT Platform per second.	10,000
	The maximum number of requests that IoT Platform can send to the devices of an Alibaba Cloud account per second.	2,000
Service subscription	The maximum number of messages that an Alibaba Cloud Message Queue for AMQP consumer group can receive per second.	1,000
Message communication	The maximum number of messages that a device can report per second. **Note** If a device uses the Pub API to report messages over the MQTT protocol but the messages are blocked due to throttling, no throttling error is returned. However, you can view device logs to find the devices whose messages are blocked due to throttling.	• QoS 0: 30 messages per second • QoS 1: 10 messages per second
	The maximum number of messages that a device can receive per second. The limit changes based on the network environment. If the maximum TCP write buffer size is exceeded, an error message is returned. If IoT Platform uses the Pub API operation to send requests to a device and the device cannot process the requests in a timely manner, a throttling error message is returned.	50 messages per second

Limited item	Description	Limit
Bandwidth	The maximum throughput (bandwidth) per connection.	1,024 KB
Cache requests	The maximum number of unacknowledged message publishing requests from a device. After the limit is reached, IoT Platform rejects new message publishing requests from the device unless a PUBACK message is received.	100
Message retention period	The maximum number of days that a QoS 1 message can be retained. If no PUBACK message is received before the maximum retention period ends, the message publishing request is rejected.	7
MQTT message size	The maximum size of a message that can be sent by using the MQTT protocol. Messages that exceed this limit are discarded.	256 KB
CoAP message size	The maximum size of a message that can be sent by using the CoAP protocol. Messages that exceed this limit are discarded.	1 KB
MQTT keep-alive mechanism	The heartbeat timeout of an MQTT connection. If the heartbeat timeout exceeds the range, IoT Platform rejects the connection request. We recommend that you set a value greater than 300 seconds. A timer starts when IoT Platform sends a CONNACK message as a respond to a CONNECT message. When IoT Platform receives a PUBLISH, SUBSCRIBE, PING, or PUBACK message, the timer is reset. If no message is received within 1.5 times the specified heartbeat interval, the server terminates the connection.	30 to 1,200 seconds
RRPC timeout period	The timeout period for devices to respond to RRPC requests.	8 seconds

Topics

Limited item	Description	Limit
Custom topic categories	The maximum topic categories that can be defined for a product.	50
Permissions	A device can publish messages and subscribe only to its own topics.	-
Topic length	The maximum length of a topic that is encoded in UTF-8.	128 bytes

Limited item	Description	Limit
Topic levels	The maximum number of category levels that a topic can include. The number of category levels is indicated by the number of slashes (/) in the topic.	7
Subscriptions	The maximum number of topics that can be included in a subscription request.	8
Time to take effect	The period that a subscribe or unsubscribe operation requires to take effect. A subscription remains effective until you unsubscribe from the topic. We recommend that you subscribe to topics in advance to avoid missing information. For example, a device sends a subscription request to Topic A. After 10 seconds, the subscription takes effect and the device starts to receive messages from Topic A in real time. The device keeps receiving messages from Topic A unless you unsubscribe from the topic.	10 seconds
Topic broadcasting	The maximum size of a message to be broadcasted. To generate a message body, you must convert a raw message into binary data and encode the data by using Base64.	64 KB
	The number of messages that can be broadcasted per minute by using the server SDK.	1

Device shadows

Limited item	Description	Limit
JSON levels	The maximum number of levels that can be specified in a device shadow JSON file.	5
File size	The maximum size of a device shadow JSON file.	16 KB
Properties	The maximum number of properties that can be specified in a device shadow JSON file.	128
Requests per second	The maximum number of requests that a device can send per second.	20

Data forwarding

Limited item	Description	Limit
Rules	The maximum number of rules that an Alibaba Cloud account can create.	1,000

Limited item	Description	Limit
Data forwarding destinations	The maximum number of data forwarding operations in a rule.	10
Messages processed by the rules engine	The maximum number of data forwarding queries that can be processed per second for an Alibaba Cloud account. RAM users share the quota of the Alibaba Cloud account. After a message is processed, it can be written to multiple Alibaba Cloud services. For more information, see the next row: messages written to Alibaba Cloud services. If a message is blocked due to throttling, the system attempts to rewrite the message later. If multiple retry attempts fail, the message is discarded.	1,000 QPS
Messages written to Alibaba Cloud services	The maximum number of data forwarding queries that can be processed per second for an Alibaba Cloud account. The maximum number can be reached only if the instance of an Alibaba Cloud service provides a high level of performance. Resource Access Management (RAM) users share the quota of the Alibaba Cloud account. If the limit is exceeded or if the number of concurrent write requests to an Alibaba Cloud service exceeds 40, data forwarding fails due to throttling. If data forwarding fails due to changes in an Alibaba Cloud service, such as RocketMQ, RDS, or TSDB, the system does not forward data to the service, and displays abnormal information. IoT Platform retries data forwarding for three times at an interval of 1, 3, and 10 seconds. If all retry attempts fail, the data is discarded and an error message is sent to the destination Alibaba Cloud service.	2,000 QPS
Requirements of data forwarding destinations	Make sure that the destination service instance runs as expected. Data forwarding fails in multiple scenarios. These scenarios include instance failure, overdue payments, improper configurations, and invalid parameter settings, such as invalid values and lack of permissions.	-
Message deduplication	Data forwarding does not guarantee that a message is received only once. In a distributed environment, rebalance may be temporarily inconsistent and a message may be sent multiple times. If multiple messages have the same ID, deduplication is required when an application receives the messages.	-

Service subscription

The following table describes the limits on AMQP service subscription.

Limit	Description
Authentication timeout	An authentication request is sent immediately after a connection is established. If the authentication is not successful within 15 seconds, the server closes the connection.
Data timeout	When the server establishes a connection with IoT Platform, the heartbeat time (the idle-timeout parameter in the AMQP) is required. The value ranges from 30 to 300, in seconds. After the connection is established, the server must send ping packets within the heartbeat time to maintain the connection. If no ping packet is sent within the heartbeat time, IoT Platform closes the connection.
Policy for message pushing retries	Messages accumulated due to consumer offline or slow message consumption are re-sent again. The interval between push retries is one minute.
The number of saved messages	Up to 100 million messages can be accumulated for a consumer group.
Message retention period	One day.
Limits on the real-time message push rate	The maximum QPS value for a consumer group is 1000.
Limits on the offline message push rate	The maximum QPS value for a consumer group is 200.
The number of consumer groups with which a product can be associated	A product can be associated with up to 10 consumer groups.
The number of products with which a consumer group can be associated	A consumer group can be associated with up to 1,000 products.
Maximum number of consumer groups	An account can have up to 1,000 consumer groups.
Maximum number of consumers	A consumer group can have up to 64 consumers.
Connection limits	The maximum number of consumer requests in a consumer group is 100 per minute.

For more information about the limits of MNS service subscription, see the limits of MNS queues in the MNS limits topic.

Cloud API operations

The maximum number of queries per second (QPS) for the IoT Platform API. For more information, see API reference.

If you receive a throttling error when you call an API operation, retry the call. For more information about throttling errors, see common errors. Errors 29 to 31 are throttling errors.