ALIBABA CLOUD

Alibaba Cloud

物联网平台

Product Introduction

Document Version: 20220617

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

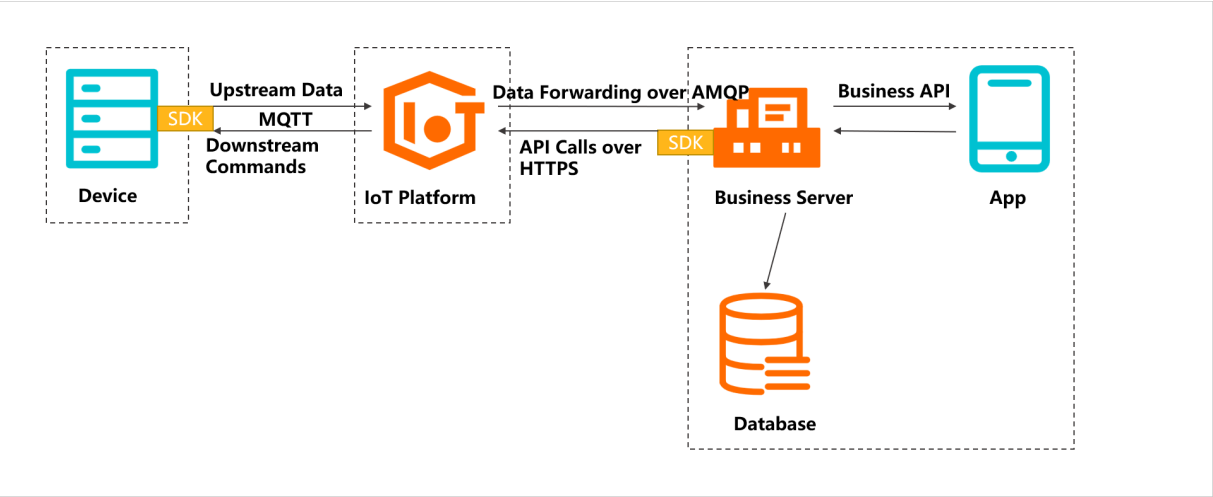
Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	**Danger:** Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major 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 platform that integrates capabilities such as device management, secure data communication, and message subscription. You can connect a large number of devices to IoT Platform and collect device data to IoT Platform. You can also call API operations of IoT Platform on your business server to send remote commands to devices.

The following figure shows the communication process among IoT Platform, devices, business servers, and clients.



To achieve communication, you must develop devices, IoT Platform servers, databases, and mobile apps. You can use IoT Platform SDK to develop IoT Platform servers. When you develop devices and IoT Platform servers, you must define and process device messages.

The following table describes the upstream and downstream messaging between devices and IoT Platform.

Communication type	Description
Upstream messaging	A device establishes a persistent connection with IoT Platform by using the MQTT protocol. Then, the device submits data to IoT Platform by publishing payloads to a topic.
	IoT Platform forwards data to your business server by using an AMQP consumer group.
	IoT Platform processes submitted device data and then forwards the data to ApsaraDB RDS, Tablestore, TSDB, Message Queue for Apache RocketMQ or Function Compute by using the data forwarding feature.
Downstream messaging	You can send a command by using your mobile app. Then, your business server calls the HTTPS-based Pub API operation to send the command to an IoT Platform topic.
	IoT Platform sends data to devices by publishing payloads to specified topics. The MQTT protocol is used for communication.

For more information about device communication, see What is a topic?

2.Functions and features

IoT Platform provides capabilities such as device connection, device management, and rules engine to empower developers in various IoT scenarios and industries.

Device connection

IoT Platform allows you to connect a large number of devices to the cloud. Devices communicate with IoT Platform in a stable and reliable manner.

Feature	Description
Link SDK	Supports various open source programming languages and provides guides for code porting across platforms. This allows enterprises to connect devices from various platforms to IoT Platform. IoT Platform provides device SDKs to connect different devices to IoT Platform.
Device authentication	• Provides the unique-certificate-per-device authentication mechanism to reduce security risks. This mechanism is applicable if a device certificate including ProductKey, DeviceName, and DeviceSecret can be burned to the chip of each device. Security level: high. • Provides the unique-certificate-per-product authentication mechanism. A device is burned with a product certificate including ProductKey and ProductSecret. Then, the device dynamically obtains a device certificate including ProductKey, DeviceName, and DeviceSecret during authentication. This mechanism is applicable if a device certificate cannot be burned to each device during mass production. Security level: medium.
Communication topics	Provides product and device topics to facilitate the communication between devices and IoT Platform. This simplifies the authorization process.
Connection over MQTT, CoAP, or HTTPS	Provides device SDKs that support various protocols. You can establish persistent connections to meet real-time requirements. You can also establish short-lived connections to reduce resource consumption.
IoT as Bridge SDK	Provides the IoT as Bridge SDK to deploy a bridging service and establish connections between devices and IoT Platform.

Message communication

You can use the following features to synchronize, convert, filter, and store messages that are transferred among devices, business servers, and IoT Platform.

Feature	Description
Server-side subscription	Allows you to subscribe to messages of one or more types from all devices of a specific product. Your server can use an AMQP client or Message Service (MNS) client to obtain the subscribed messages.

Feature	Description
Data forwarding	Forwards the specified fields of topic messages to a destination based on a data forwarding rule for storage and computing. For more information about the scenarios and benefits of data forwarding, see Compare data forwarding solutions. For more information about data forwarding destinations, see the following articles: • Use an SQL statement to forward data • Use a parser script to forward data
Scene orchestration	Allows you to configure a rule to forward the data of a device to other devices.
RRPC communication	Provides the RRPC and Pub/Sub communication modes to meet your business requirements in different scenarios. Pub/Sub is a message routing mode based on topics.
Broadcast messages	

Device management

Feature	Description
TSL models	Provides Thing Specification Language (TSL) models to simplify application development.
Data parsing	Supports passing through binary data to your server. To ensure data security, IoT Platform does not store device data.
Tags	Classifies devices and manages devices cross products.
Device groups	
Device shadow	Provides the device shadow feature to decouple devices and applications in unstable wireless network conditions.
File management	Stores, downloads, and deletes device files.
NTP service	Synchronizes the server time to embedded devices with limited resources.
Gateways and sub-devices	Manages topological relationships between sub-devices and gateways. You can also manage and monitor sub-devices.

Monitoring and O&M

Feature	Description
Real-time monitoring	Monitors metrics that are related to devices, messages, TSL models, and rules engine in real time and generates alerts by using CloudMonitor.
Online debugging	Sends commands to devices by using the IoT Platform console to debug device features.

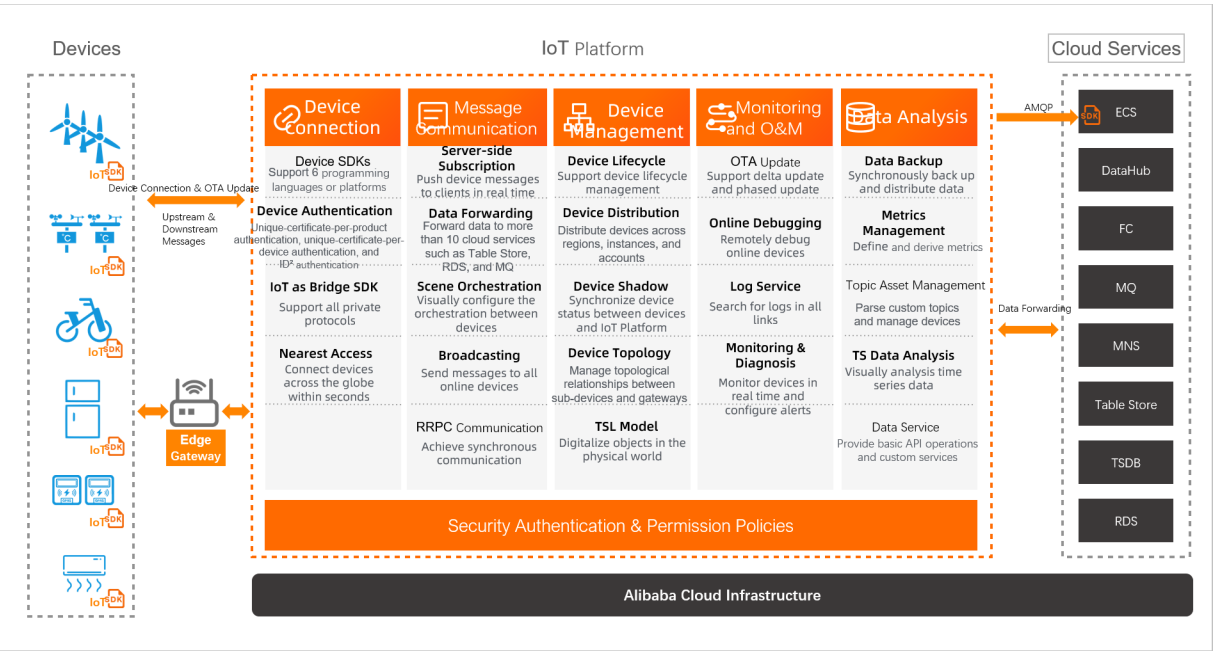
Feature	Description
Device simulation	Simulates a real device to establish a connection with IoT Platform, uses the simulated data to test the communication between IoT Platform and the device, and identifies errors.
Log service	Provides IoT Platform logs and local device logs to identify errors and analyze the causes.
OTA update	Provides the remote update feature.
Remote configuration	Allows you to remotely update the system and network parameters

Cloud-side development guide

IoT Platform SDK and API operations: IoT Platform provides SDKs for Java, Python, PHP,.NET, and Go. You can call the API operations of IoT Platform to manage products, manage devices, manage topics, forward data to other cloud services, and send data to devices.

3.Service architecture

Devices connect and then communicate with IoT Platform. IoT Platform can forward device data to other Alibaba Cloud services for storage and processing. You can deploy IoT applications based on the IoT Platform architecture. This article describes the IoT Platform architecture.



- Devices: You can connect devices to IoT Platform by using different protocols and SDKs. Then, you can manage the devices.
- IoT Platform: After devices are connected to IoT Platform, you can submit device data to IoT Platform. IoT Platform allows you to collect, forward, store, analyze, and monitor device data in real time. IoT Platform provides authentication methods and permission policies to ensure data security.
- Alibaba Cloud services: IoT Platform can integrate with other cloud services. You can transfer data between devices and business servers. You can also forward device data to from IoT Platform to other cloud services for storage.

4.Benefits

Enterprises are deploying Internet of Things (IoT) solutions to collect and manage data from devices and increase returns. However, enterprises are facing various challenges in building a powerful IoT system. Alibaba Cloud IoT Platform offers solutions to these challenges and has advantages over user-created MQTT clusters and MQTT servers.

Differences between IoT Platform and user-created MQTT clusters

The following table describes the differences of capabilities between Alibaba Cloud IoT Platform and user-created MQTT clusters.

Item	IoT Platform	User-created MQTT cluster
Cost-effectiveness	Supports multiple billing methods, including pay-as-you-go and subscription. Supports automatic scaling to meet business growth.	Supports the subscription billing method, which requires a one-time investment in IaaS resources. Requires manual scaling to meet business growth.
Device connection	Provides device SDKs to establish connections between devices and IoT Platform. IoT Platform supports connections to devices around the world. These devices include devices in heterogeneous networks, devices that run in various environments, and devices that run based on different protocols. Supports stable connections to hundreds of millions of devices, and automatic scaling. IoT Platform processes device messages within 50 ms.	Requires the efforts of embedded system developers and cloud developers in infrastructure deployment. The development features high workloads and low efficiency. The architecture may have difficulties in maintaining stable connections to millions of devices. If a large number of devices go online or offline at the same time, the platform may break down.
Concurrency	Processes millions of concurrent messages and supports horizontal scaling. The core message processing system uses a stateless architecture without failure dependency. If a message fails to be sent, IoT Platform automatically retries.	The architecture may have difficulties in processing millions of concurrent messages. A large number of concurrent upstream and downstream messages have negative impacts on the system. The load balancing feature is not supported. The business is affected during peak hours.

Item	IoT Platform	User-created MQTT cluster
Security	Supports three levels of Multi-Level Protection Scheme (MLPS) 2.0 to protect device data. • The access layer uses high Anti-DDoS Pro to prevent DDoS attacks. • Device authentication is supported to guarantee the security and uniqueness of devices. • Device data transmission supports TLS encryption to prevent data tampering. • Important keys and data are encrypted to prevent thefts. • Alibaba Cloud Security and permission control ensure data security in IoT Platform. • IoT Platform is protected by the Alibaba Cloud security team.	Requires the development and deployment of security measures. Securing device data is a challenge. If an enterprise does not have security professionals or sufficient security awareness, the enterprise cannot eliminate security risks in a timely manner.
Availability	Adopts multi-data center deployment to eliminate failure dependency. Guarantees the 99.9% service availability. If the guaranteed service availability is not reached, claims will be settled based on the relevant standard. IoT Platform can detect a fault within 1 minute, locate a fault within 5 minutes, and troubleshoot a fault within 20 minutes.	Requires manual troubleshooting. If an MQTT cluster does not respond during data migration, you must locate and resolve the error. Service may be interrupted during the data migration. Therefore, service availability is not guaranteed. Provides no quantitative service availability. Errors must be handled by the technical team and the O&M team. The timeliness of error handling cannot be guaranteed. Enterprises must bear the losses that are caused by the errors.

Item	IoT Platform	User-created MQTT cluster
Ease of use	Supports plug-and-play deployment, and provides a console, device SDKs, and IoT Platform SDKs to simplify development and deployment. Provides a one-stop device management platform that monitors devices in real time. IoT Platform is also integrated with multiple Alibaba Cloud services. IoT Platform allows you to build complex IoT applications with ease. Supports Thing Specification Language (TSL) models. TSL models eliminate the need to define data syntax, and simplify data analysis and visualization. Provides a comprehensive monitoring and alert platform. After you configure the alert settings, you can receive alerts in real time if a system or business exception occurs. Provides APIs and supports data transfer among devices, IoT Platform, and business servers.	Requires server deployment to build a load-balanced distributed architecture, and requires considerable investment into an IoT system that handles connection, computing, and storage requests. Provides no consoles. Enterprises must set up both the frontend and backend. The device connection management, lifecycle management, and remote O&M are complex.
Global access	IoT Platform is globallyavailable in six regions. The regions are distributed in Asia, Europe, and North America. Your devices can be connected to the nearest access points. Provides the domain acceleration feature to reduce the latency in global communications. Complies with GDPR provisions to ensure data security.	Requires high costs to deploy devices in other regions. High latency is required to access these devices. Security compliance must also be considered.
Synchronous server call	Supports synchronous RRPC responses.	Unsupported.
Data parsing based on custom protocols	Supports data parsing based on custom protocols. The related scripts are hosted on the cloud.	Unsupported. The data must be parsed by business servers.
Data forwarding	Supports data forwarding among various cloud services by using the rules engine.	Unsupported. Coding is required to
Device shadow	Supported.	
OTA updates	Supports multiple firmware update modes.	

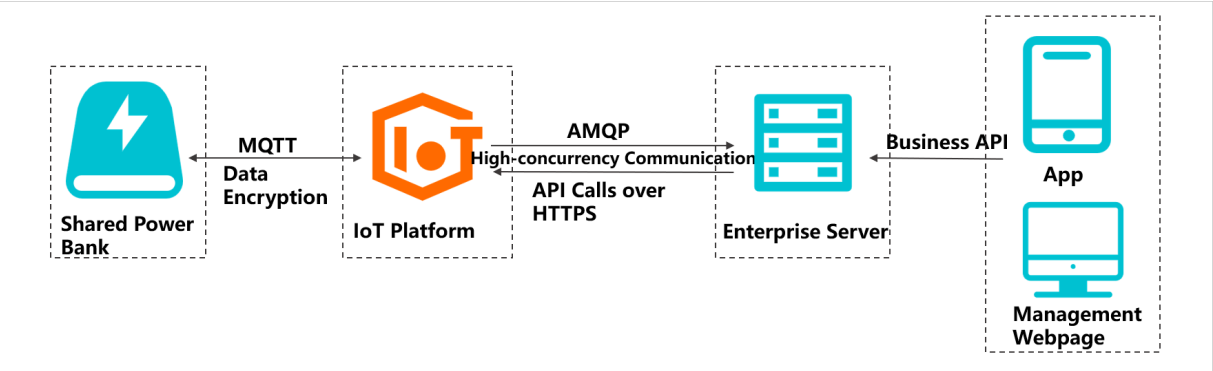
Item	IoT Platform	implement the data forwarding feature. User-created MQTT cluster
Logging	Supports the log query feature and large-scale log storage.	
Real-time Monitoring	Visualizes real-time metric data on charts, and supports threshold-based alerts and event alerts.	

5.Common scenarios

IoT Platform can establish stable connections with a large number of devices. IoT Platform also provides API operations for cloud servers to send remote commands to devices with low latency. The following sections describe typical scenarios of IoT Platform.

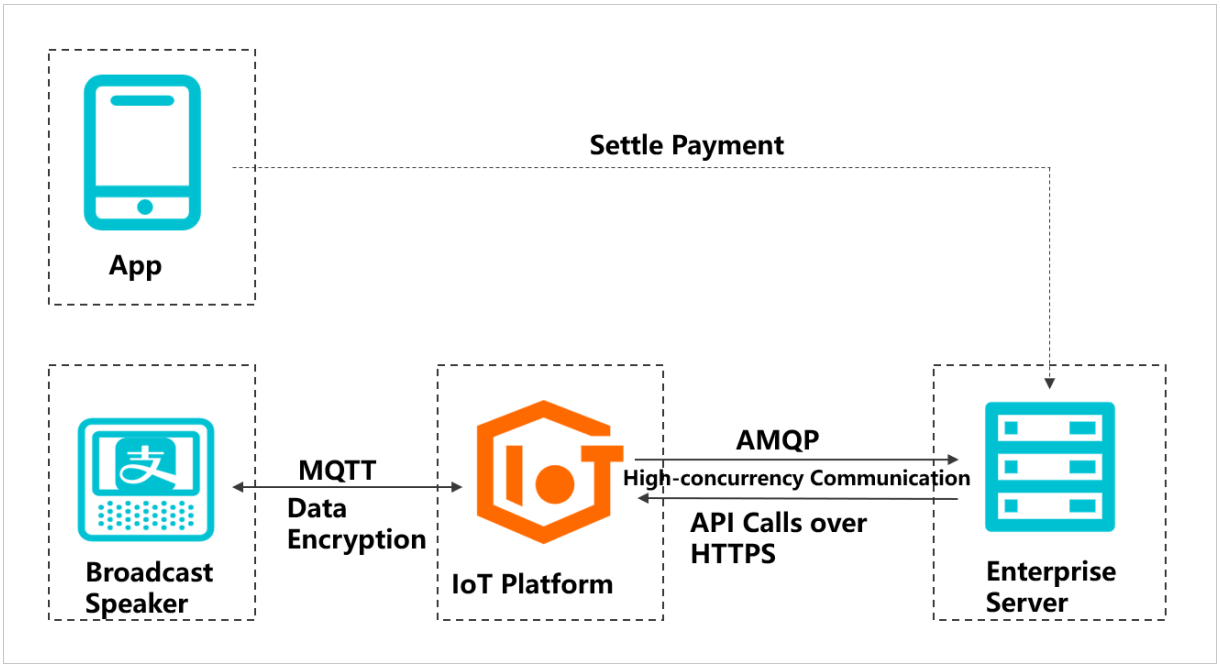
Shared power bank

After a shared power bank is connected to IoT Platform, the power information and borrowing status of the power bank is submitted to IoT Platform. If a user scans the code to use the power bank, IoT Platform sends a command to eject the power bank from the base. An enterprise operator can obtain the status of the power bank in real time.



Smart speakers

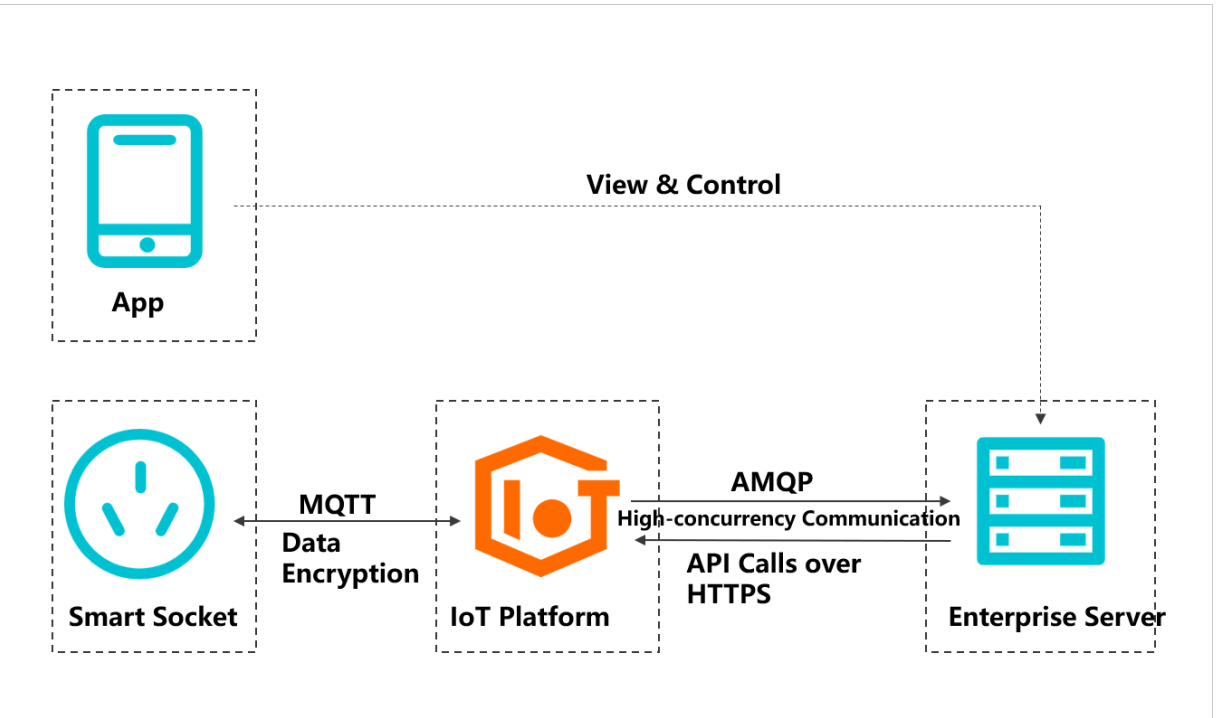
After a broadcast speaker is connected to IoT Platform and a consumer scans the code of the speaker to complete the payment, the payment amount is broadcast to the consumer and merchant in real time.



Smart appliances

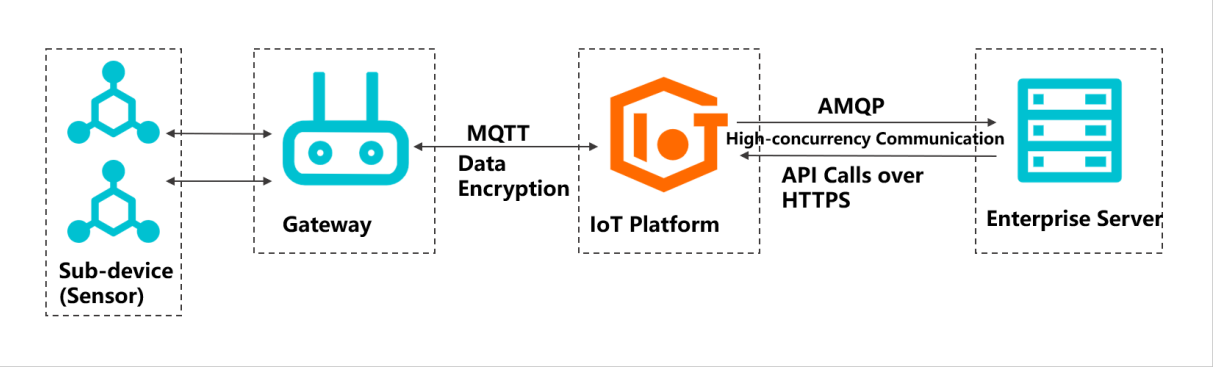
IoT Platform is widely used in smart home appliances. Take a smart socket as an example. Users can remotely check the usage of the socket and control its switch to prevent overheating of high-power appliances.

You can use the unique-certificate-per-device authentication method to prevent mass attacks when you connect a large number of devices to IoT Platform.



Agricultural equipment

Various sensor devices and communication networks are used to monitor and collect data in agricultural greenhouses in real time. You can connect sensor devices to a gateway by using the RS485 bus, and then connect the devices to IoT Platform by using the gateway. You can view and manage data in IoT Platform.

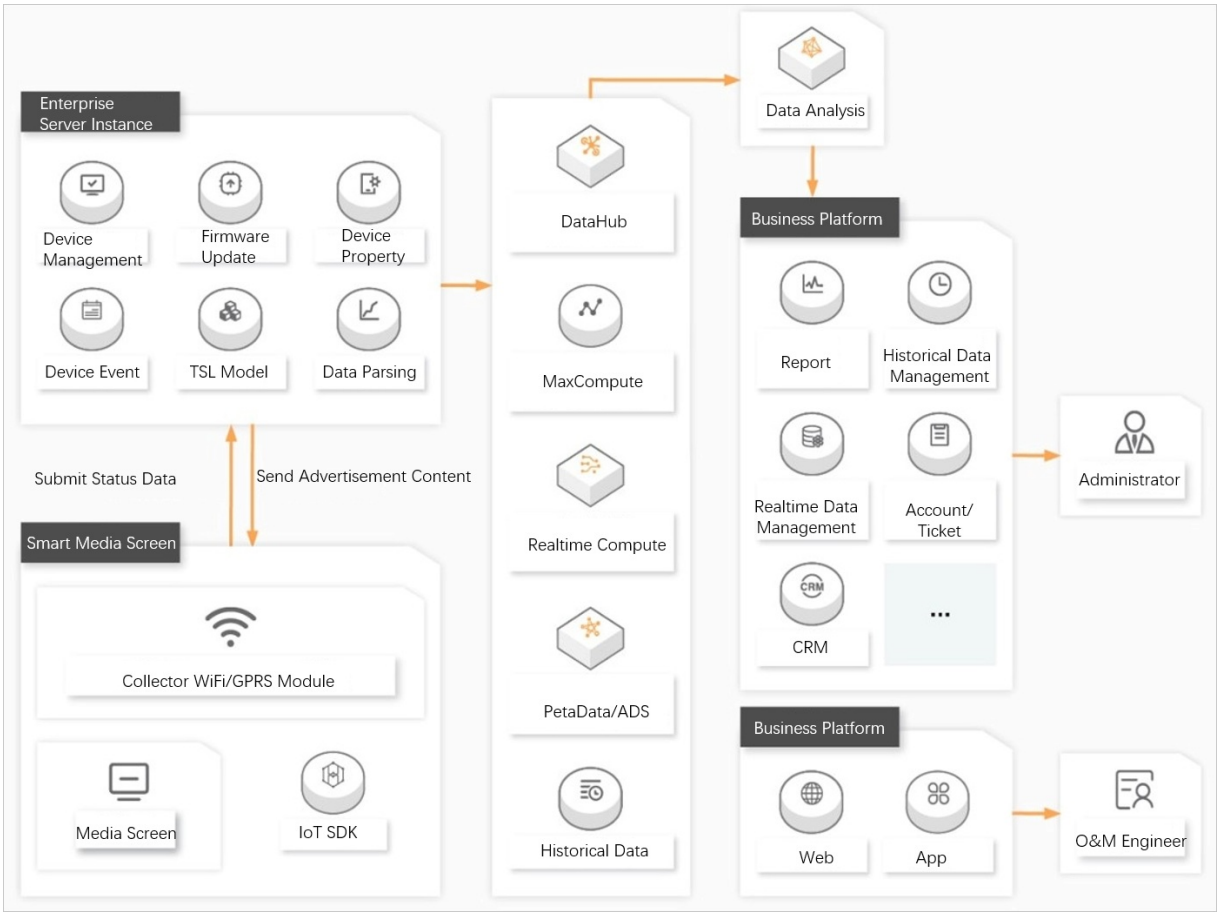


Smart media screen

After a media screen is connected to IoT Platform, you can monitor the device status and refresh the screen content in real time. This allows you to achieve the smart and fine-grained operations of the media screen. This also helps you reduce costs and improve efficiency.

- You can manage all media screens in IoT Platform and achieve smart operations of new media content.

- You can use ECS instances to remotely deliver media content. This significantly reduces the manual maintenance costs of traditional media screens.
- You can flexibly scale ECS instances based on your business requirements.



6.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 device 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	A sub-device is essentially a device. Sub-devices cannot directly connect to IoT Platform and must be attached to a gateway.
device certificate	A device certificate consists of a ProductKey, a DeviceName, and a DeviceSecret. • A ProductKey is the unique identifier of a product in IoT Platform. ProductKeys are required in device authentication and communication. You must safely keep them. • A DeviceName is generated by IoT Platform for each device during device registration. You can also upload custom DeviceNames. Each device has a unique DeviceName under the same product. DeviceNames are required in device authentication and communication. You must safely keep them. • A DeviceSecret is the private key that is issued by IoT Platform for each device. A DeviceSecret is used in pair with a DeviceName. DeviceSecrets are required in device authentication and communication. You must safely keep them.
ProductSecret	A ProductSecret is the private key issued by IoT Platform for each product. A ProductSecret is usually used in pair with a ProductKey for unique-certificate-per-product authentication. ProductSecrets are required in device authentication and communication. You must safely keep them.
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.
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.

Term	Description
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 Alink protocol is used for communication between devices and IoT Platform.
TSL	IoT Platform uses 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 report the data to IoT Platform.
property	A property is a TSL feature that describes the 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. Application systems can initiate requests to obtain 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 are 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 service is 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	An event is a TSL feature that describes the runtime events of a device. An event contains a notification that requires actions or attentions. An event may contain multiple output parameters. For example, an event may be a notification indicating that a task is complete, a device fault that has occurred, or a temperature alert. You can subscribe to or push events.
data parsing script	If devices use pass-through or custom-formatted data, you must write data scripts in IoT Platform to parse the data. You must convert the binary data or custom JSON data that is reported 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-formatted data that is supported by the devices.

Term	Description
device shadow	A device shadow is a JSON file that is used to store the status information of a device or an 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 indicating that 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: Use 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: Forward 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 consists of a ProductKey, a DeviceName, and a 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 consists of a ProductKey and a 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 to IoT Platform.
instance	You can manage resources such as products, devices, and rules in IoT Platform instances. The following two types of instances are supported: • Public instance (default): After the IoT Platform service is activated, a public instance is provided by default. Public instances are deployed on Alibaba Cloud classic networks. • Enterprise Edition instance: The instance you purchase is an Enterprise Edition instance. Enterprise Edition instances are deployed on Alibaba Cloud Virtual Private Cloud (VPC). You can use an Alibaba Cloud account to purchase multiple Enterprise Edition instances and exclusively enjoy the resources of these instances.

7.Limits

This topic describes the limits on the following features and services of IoT Platform.

Device connection

- Product quantity

Region	Description	Limit
China (Shanghai), Singapore (Singapore), Germany (Frankfurt), US (Silicon Valley), and US (Virginia)	The maximum number of products that you can create by using an Alibaba Cloud account.	1,000
Japan (Tokyo)	The maximum number of products that you can create for an instance.	1,000

- Device quantity

> **Note** If the limit no longer meets your business requirements, submit a ticket to increase the limit.

  - The maximum number of devices that can be added to a product.

Region	Limit
China (Shanghai)	3,000,000
Singapore (Singapore), Germany (Frankfurt), US (Silicon Valley), US (Virginia), and Japan (Tokyo)	1,000,000

> **Note**
>
> - To ensure that new devices can be added to a product, we recommend that you configure a threshold alert for the number of devices that you have added to the product. This allows you to obtain the number of existing devices in the product in real time. For more information, see Create a threshold-triggered alert rule.
> - If the number of devices exceeds the limit, you must create another product.

- The maximum number of devices that can be added to an instance.

Region	Instance	Limit
China (Shanghai), Singapore (Singapore), Germany (Frankfurt), US (Silicon Valley), and US (Virginia)	This limit applies only to public instances because Enterprise Edition instances are unavailable in the regions.	You can refer to the limit on the number of devices that you can add by using an Alibaba Cloud account.
Japan (Tokyo)	Enterprise Edition instances and public instances	1,000,000

> **Note**
>
> - For more information about how to purchase an Enterprise Edition instance, see Purchase Enterprise Edition instances.
> - If the value that you selected for the device quantity specification of an Enterprise Edition instance that you purchased is less than this limit, you can upgrade the configuration of the instance. For more information, see Upgrade the configuration of an Enterprise Edition instance.
> - If the number of devices that you want to create for a public instance of the new version exceeds 500, we recommend that you upgrade the public instance to an Enterprise Edition instance. For more information, see Upgrade to an Enterprise Edition instance..

- The maximum number of devices that you can add by using an Alibaba Cloud account.

Region	Limit
Japan (Tokyo)	None. You can refer to the limit on the number of devices that you can add to an instance.
China (Shanghai), Singapore (Singapore), Germany (Frankfurt), US (Silicon Valley), and US (Virginia)	10,000,000

- Gateway sub-device

  You can attach up to 1,500 sub-devices to a gateway.

  For more information about throttling limits, see the *Message communication* item in the Connections and communications section.

Device management

Item	Description	Limit
Thing Specification Language (TSL) features	The maximum number of TSL modules that can be created for a product, including the default modules and custom modules.	20
	The maximum number of features that can be added to a TSL module.	300
	The maximum number of parameters that can be specified for a property of the STRUCT data type.	50
	The maximum number of items that can be specified for a feature of the ENUM data type.	100
	The maximum length that can be specified for a feature of the TEXT data type.	10,240 characters
	The maximum number of elements that can be specified for a feature of the ARRAY data type.	512
	The maximum number of input parameters and output parameters that can be added to all services and events.	300
	The maximum number of input parameters that can be added to a service.	100
	The maximum number of output parameters that can be added to a service.	100
	The maximum number of output parameters that can be added to an event.	100
	The maximum number of TSL module files that can be imported at the same time.	20
	The maximum number of latest versions that can be saved for a TSL model.	10
	The maximum size of an imported TSL module in the JSON format.	512 KB
	The maximum number of valid characters that can be contained in an imported TSL module in the JSON format. Valid characters do not include line feeds and alignment characters.	256 KB
	The maximum size of a ZIP file that can be obtained by compressing multiple JSON-formatted files when you import a TSL model.	2.5 MB

Item	Description	Limit
	The maximum number of recursive nesting levels that are supported if you nest the *ARRAY* and *STRUCT* data types for the ThingModelJson parameter when you call TSL-related operations. For example, you can nest data of the *STRUCT* type only in data of the *ARRAY* type. The data of the *STRUCT* type cannot contain data of the *ARRAY* or *STRUCT* type.	2
Tags	The maximum number of tags that can be attached to a product, device, or device group.	100
Device groups	The maximum number of groups and sub-groups that each Alibaba Cloud account can create.	1,000
	The maximum number of devices that can be added to a group.	100,000
	The maximum number of groups to which a device can be added.	10
Data parsing	The maximum size of a data parsing script.	128 KB
Remote configuration	The maximum size of a remote configuration file. Remote configuration files support only the JSON format.	64 KB
Data retention period	The maximum number of days for which property data, event data, and service data can be retained. Data is deleted after the retention period ends.	30
File management	The maximum size of files that can be stored in an instance.	1 GB
	The maximum size of a single file that can be uploaded by a device over MQTT.	16 MB
	The maximum number of files that can be stored on a device.	1,000
OTA update	The maximum number of update packages that can be uploaded in an instance under each Alibaba Cloud account.	500
	The maximum size of an update package.	2,000 MB
	The maximum number of devices that can be specified for a batch update.	100,000
Device jobs	The maximum number of device jobs that each Alibaba Cloud account can add in a single region.	10,000

Connections and communications

Item	Description	Limit
Device connection	The maximum number of connections that can be established with IoT Platform by using 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 each Alibaba Cloud account can initiate per second.	500
	The maximum number of connection requests that a device can send per minute without being throttled.	5
Device subscription	The maximum number of topics to which a device can subscribe. After the limit is reached, new subscription requests are rejected. The device can check whether a subscription request succeeds by verifying the 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
Message communication	The maximum number of messages that a device can send to IoT Platform per second. **Note** If you use the MQTT protocol to publish messages, no throttling information is returned. 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
Bandwidth	The maximum throughput (bandwidth) per connection.	8 Mbps

Item	Description	Limit
Cached 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 until a PUBACK message is received.	100
Message retention period	The maximum number of days for which 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 over MQTT. Messages whose size exceeds this limit are discarded.	256 KB
CoAP message size	The maximum size of a message that can be sent over CoAP. Messages whose size exceeds this limit are discarded.	1 KB
MQTT keep-alive mechanism	The heartbeat interval for an MQTT connection ranges from 30 to 1,200 seconds. If a heartbeat interval is out of the specified value range, the server rejects the connection request. We recommend that you specify a value that is greater than 300 seconds. Default value: 1200. Unit: seconds. For more information about how to specify a keep-alive period for a device, see Connection over MQTT examples. A timer starts when IoT Platform sends a CONNACK message as a response to a CONNECT message. When IoT Platform receives a PUBLISH, SUBSCRIBE, PING, or PUBACK message, the timer is reset. If no message is received during a period of time that is 1.5 times the specified heartbeat interval, the server terminates the connection.	30 to 1,200 seconds
RRPC timeout period	The timeout period during which devices must respond to RRPC requests.	8 seconds
MQTT 5.0 protocol	The maximum number of custom properties that can be added.	20
	The maximum length of a custom property key or custom property value.	128 characters
	The maximum length of the ResponseTopic parameter or CorrelationData parameter that can be configured in the request/response communication mode.	128 characters

Topics

Item	Description	Limit
Custom topic categories	The maximum number of topic categories that you can define for a product.	50
Permissions	A device can publish messages and subscribe only to the topics that are associated with the device.	None
Topic length	The maximum length of a topic that is encoded in UTF-8.	128 bytes
Topic levels	The maximum number of category levels that can be included in a topic. The number of category levels is equal to 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 operation or unsubscribe operation requires to take effect. A subscription remains valid until you unsubscribe from the topic. We recommend that you subscribe to topics in advance to prevent information missing. 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 continues to receive messages from Topic A until you unsubscribe from the topic.	10 seconds
Message broadcasting	The maximum size of a message that can 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

Item	Description	Limit
JSON levels	The maximum number of levels that can be included in the JSON file of a device shadow.	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
QPS	The maximum number of requests that a device can send per second.	20

Data forwarding (previous version)

Item	Description	Limit
Rules	The maximum number of rules that each Alibaba Cloud account can create.	1,000
Data forwarding destinations	The maximum number of data forwarding actions that you can specify 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. The RAM users of an Alibaba Cloud account 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 item: Messages written to Alibaba Cloud services. If a message is blocked due to throttling, IoT Platform retries to process the message. If multiple retries fail, the message is discarded.	1,000 TPS
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. The RAM users of an Alibaba Cloud account 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 a destination service such as Message Queue for Apache RocketMQ, ApsaraDB RDS, or ApsaraDB for Lindorm is unavailable due to the resource changes of the service, IoT Platform stops forwarding messages and displays the abnormal rule. If an error occurs due to another cause when you send a message, IoT Platform retries three times at the intervals of 1, 3, and 10 seconds. If all retries fail, the message is discarded and an error message is sent to the destination cloud service.	2,000 TPS
Requirements of data forwarding destinations	Make sure that the instance of a destination cloud service 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.	None

Item	Description	Limit
Message deduplication	When you forward a message, the message may be repeatedly sent until the client returns an ACK message or the message expires. If multiple messages use the same message ID, you can deduplicate the messages based on the ID.	None

Data forwarding (new version)

The limits on the messages related to Data forwarding (previous version) are the same as the limits on the messages related to data forwarding (new version).

Item	Description	Limit
Parser	The maximum number of parsers that an instance can contain.	1,000
Data Sources	The maximum number of data sources that can be associated with a parser.	1
	The maximum number of topics that a data source can contain.	1,000
Data destination	The maximum number of data destinations that can be associated with a parser.	10
	The maximum number of operations that a data destination can contain.	1
	The maximum number of error data destinations that can be associated with a parser.	1
Parser script	The maximum size of a parser script.	120 KB
	The maximum number of times that a data forwarding function can be executed in a loop in a parser script. For more information about data forwarding functions, see Forward data to destinations.	100

Server-side subscription

The following table describes the limits on AMQP server-side subscription.

Item	Description
Authentication timeout	An authentication request is sent after a connection is established. If the authentication fails within 15 seconds, the server ends the connection.

Item	Description
Data timeout	When a server establishes a connection with IoT Platform, the heartbeat timeout period (the idle-timeout parameter in AMQP) must be specified. The timeout period ranges from 30 to 300 seconds. If no frame is transmitted within the heartbeat timeout period, IoT Platform ends the connection. After the connection is established, the server must send ping packets within the heartbeat timeout period to maintain the connection. Otherwise, IoT Platform ends the connection. **Note** If the connection is established by using an Alibaba Cloud SDK, the server does not need to send ping packets to maintain the connection. During the keep-alive time that is provided by the SDK, make sure that the main process does not exit.
Policy for message pushing retries	Messages may not be consumed in real time due to some issues. In this case, these messages are accumulated. These issues include that consumers disconnect from IoT Platform and the speed at which these messages are consumed is slow. • After these consumers re-connect to IoT Platform and start to consume messages at a stable speed, IoT Platform pushes accumulated messages to these consumers. • If consumers fail to consume these pushed messages, the queue where accumulated messages reside may be blocked. After an interval of about 1 minute, IoT Platform retries to push accumulated messages to consumers.
Maximum number of saved messages	Each consumer group can retain a maximum of 100 million messages.
Message retention period	One day.
Maximum push rate for real-time messages	Each connection can be used to process a maximum of 1,000 transactions per second (TPS). A maximum of 64 connections can be established.
Maximum push rate for accumulated messages	A consumer group can process a maximum of 200 TPS. **Note** To prevent a large number of accumulated messages, make sure that consumers are connected to IoT Platform. You must also make sure that these consumers send ACK responses to messages that are pushed by IoT Platform.
Maximum number of consumer groups with which a product can be associated	10.

Item	Description
Maximum number of products with which a consumer group can be associated	1,000.
Maximum number of consumer groups	Each Alibaba Cloud account can create a maximum of 1,000 consumer groups.
Maximum number of consumers	Each consumer group can have a maximum of 64 consumers.
Maximum connection requests	Each consumer can initiate a maximum of 100 connection requests within 1 minute. **Note** Consumers indicate AMQP clients that are used to receive IoT Platform messages. These consumers are not devices.

For more information about the limits on Message Service (MNS) server-side subscription, see the limits on MNS queues in MNS limits.

Cloud API operations

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

If a throttling error message is returned when you call an operation, retry to call the operation.For more information about throttling errors, see Type 29 to 31 in common errors.

8.Regions

This topic describes the regions that are supported by IoT Platform.

Region

A region is a geographic location where Alibaba Cloud data centers are deployed. After a resource is created, you cannot change the region of the resource. The following table describes the mappings between the supported regions, cities where the regions reside, and region IDs.

- In the Chinese mainland

Region	City	Region ID
China (Shanghai)	Shanghai	cn-shanghai

- Outside the Chinese mainland

Country	Region	Region ID
Singapore	Singapore (Singapore)	ap-southeast-1
Japan	Japan (Tokyo)	ap-northeast-1
US	US (Silicon Valley)	us-west-1
US	US (Virginia)	us-east-1
Germany	Germany (Frankfurt)	eu-central-1

Description

When you select a region, take note of the following items:

- Geographical locations

  Select a region based on the geographical location where you and your users reside.

  - Regions in the Chinese mainland

    In the Chinese mainland, we recommend that you select a region that is the closest to the geographical location of your users to speed up access. However, in terms of network infrastructures, Border Gateway Protocol (BGP) network quality, quality of service (QoS), and usage of and configurations on Elastic Compute Service (ECS) instances, Alibaba Cloud regions in the Chinese mainland are almost the same. BGP networks ensure fast access to all regions in the Chinese mainland.

  - Outside the Chinese mainland

    The bandwidth provided in the regions outside the Chinese mainland takes effect for the users in the regions. If you reside in the Chinese mainland, we recommend that you do not select the regions outside the Chinese mainland because high latency may occur if you select the regions.

- Connection between Alibaba Cloud services

  If you use multiple Alibaba Cloud services together, take note of the following items:

- ECS instances, ApsaraDB RDS instances, and Object Service Storage (OSS) buckets that are created in different regions cannot communicate with each other over internal networks.
- Server Load Balancer (SLB) cannot balance requests from ECS instances deployed in different regions. ECS instances that you purchased in different regions cannot be deployed on the same SLB instance.

- ICP license and ICP filing

  When you select a region, take note of the special requirements of specific areas. If you want to apply for an ICP filing or ICP license for an enterprise in Beijing, select **China (Beijing)** as the region.

  > **Note** The approval requirements for ICP licenses vary from province to province. For information about the latest requirements, visit the ICP license application website of the local communications administration.

References

For more information about the IoT Platform that are supported by each region, see View the endpoint of an instance.