

# 阿里云 物联网平台

## 产品简介

文档版本 : 20181008

# 法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或惩罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。未经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

# 通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 禁止： 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 警告： 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 说明： 您也可以通过按 <b>Ctrl + A</b> 选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 确定。
courier 字体	命令。	执行 <code>cd /d C:/windows</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid Instance_ID</code>
<code>[]</code> 或者 <code>[a b]</code>	表示可选项，至多选择一个。	<code>ipconfig [-all/-t]</code>
<code>{}</code> 或者 <code>{a b}</code>	表示必选项，至多选择一个。	<code>swich {stand / slave}</code>

# 目录

---

法律声明.....	1
通用约定.....	1
1 什么是物联网平台.....	1
2 产品架构.....	3
3 产品规格.....	6
4 名词解释.....	10
5 产品优势.....	12
6 使用限制.....	13

# 1 什么是物联网平台

---

物联网平台是阿里云面向物联网领域开发人员推出的设备管理平台，旨在帮助开发者搭建数据通道，方便终端（如传感器、执行器、嵌入式设备、智能家电等）和云端进行双向通信。

物联网平台的主要功能如下：

## 设备接入

物联网平台提供设备端SDK让设备轻松接入阿里云。

- 提供2/3/4G、NB-IoT、LoRa等不同网络设备接入方案，解决企业异构网络设备接入管理痛点。
- 提供MQTT、CoAP等多种协议的设备SDK，既满足长连接的实时性需求，也满足短连接的低功耗需求。
- 开源多种平台设备端代码，提供跨平台移植指导，赋能企业基于多种平台做设备接入。

## 设备通信

设备可以使用物联网平台，通过IoT Hub与云端进行双向通信。物联网平台提供了设备与云端的上下行通道，为设备上报与指令下发提供稳定可靠的支撑。

## 设备管理

提供完整的设备生命周期管理功能，支持设备注册、功能定义、脚本解析、在线调试、远程配置、固件升级、远程维护、实时监控、分组管理、设备删除。

- 提供设备物模型，简化应用开发。
- 提供设备上下线变更通知服务，方便实时获取设备状态。
- 提供数据存储能力，方便用户海量设备数据的存储及实时访问。
- 支持OTA升级，赋能设备远程升级。
- 提供设备影子缓存机制，将设备与应用解耦，解决不稳定无线网络下的通信不可靠痛点。

## 安全能力

阿里云物联网平台提供多重防护有效保障设备云端安全。

- 身份认证
- 提供芯片级安全存储方案（ID<sup>2</sup>）及设备秘钥安全管理机制，防止设备密钥被破解。安全级别很高。

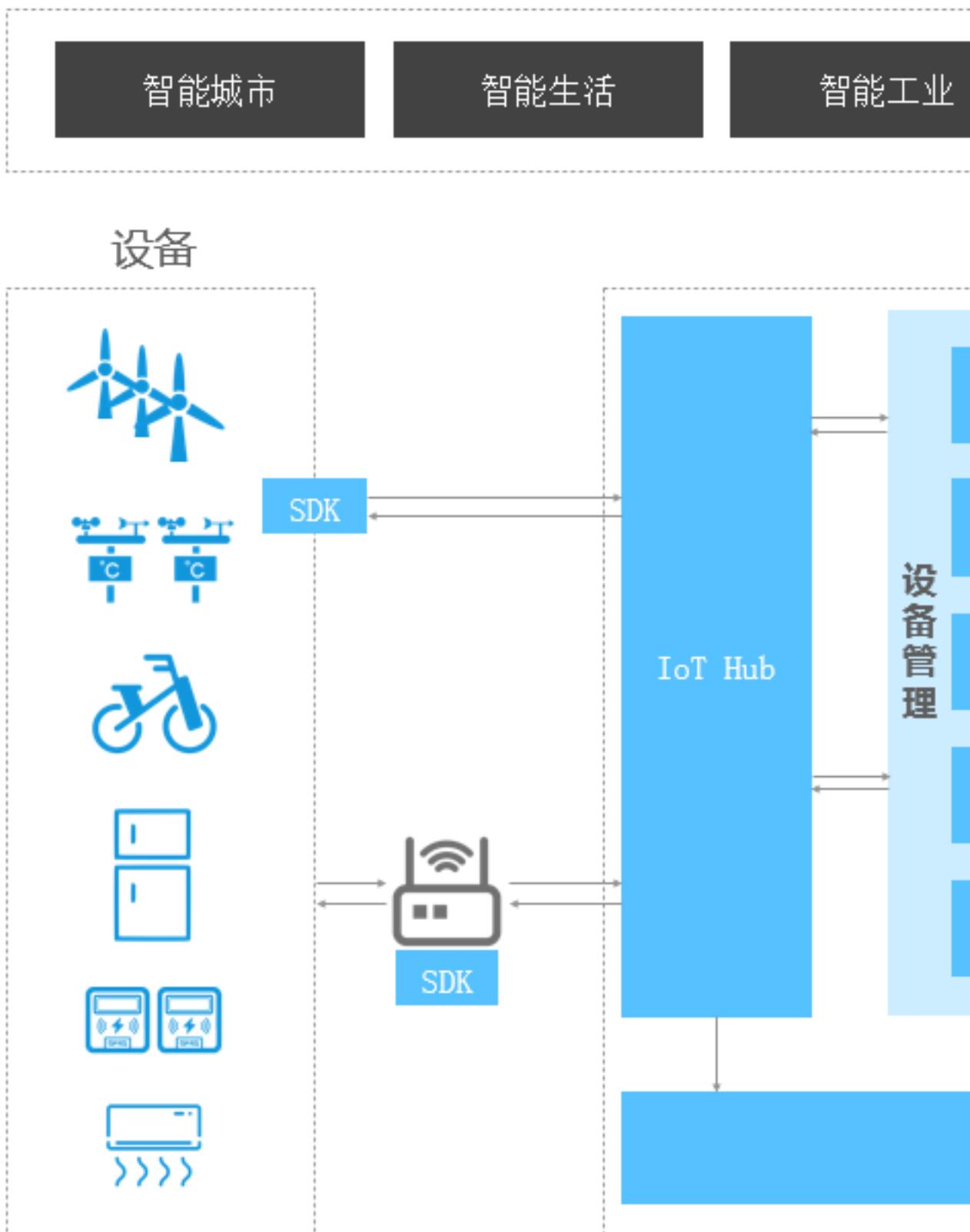
- 提供一机一密的设备认证机制，降低设备被攻破的安全风险，适合有能力批量预分配ID密钥烧入到每个芯片的设备。安全级别高。
- 提供一型一密的设备预烧，认证时动态获取三元组，适合批量生产时无法将三元组烧入每个设备的情况。安全级别普通。
- 通信安全
  - 支持TLS ( MQTT\HTTP ) 、 DTLS(CoAP)数据传输通道，保证数据的机密性和完整性，适用于硬件资源充足、对功耗不是很敏感的设备。安全级别高。
  - 支持TCP(MQTT)、 UDP(CoAP)上自定义数据对称加密通道，适用于资源受限、功耗敏感的设备。安全级别普通。
  - 支持设备权限管理机制，保障设备与云端安全通信。
  - 支持设备级别的通信资源 ( TOPIC等 ) 隔离，防止设备越权等问题。

## 规则引擎解析转发数据

规则引擎将物联网平台与阿里云的产品无缝打通，您可以配置简单规则，将设备数据转发至云产品中，进而获得存储、计算等其他服务。例如，基于规则引擎您可以：

- 配置规则实现设备与设备之间的通信，快速实现M2M场景。
- 将数据转发到消息队列 ( MQ ) 中，保障应用 消费 设备上行数据 的稳定可靠性。
- 将数据转发到表格存储 ( Table Store )，提供设备数据采集 + 结构化存储的联合方案。
- 将数据转发到函数计算中，提供设备数据采集 + 事件计算的联合方案。

## 2 产品架构



## IoT Hub

IoT Hub帮助设备连接阿里云IoT服务，是设备与云端安全通信的数据通道。IoT Hub支持PUB/SUB与RRPC两种通信方式，其中PUB/SUB是基于Topic进行的消息路由。

IoT Hub具有下列特性：

- 高性能扩展：支持线性动态扩展，可以支撑十亿设备同时连接。
- 全链路加密：整个通信链路以RSA，AES加密，保证数据传输的安全。
- 消息实时到达：当设备与IoT Hub成功建立数据通道后，两者间将保持长连接，以减少握手时间，保证消息实时到达。
- 支持数据透传：IoT Hub支持将数据以二进制透传的方式传到自己的服务器上，不保存设备数据，从而保证数据的安全可控性。
- 支持多种通信模式：IoT Hub支持RRPC和PUB/SUB两种通信模式，以满足您在不同场景下的需求。
- 支持多种设备接入协议：支持设备使用CoAP、MQTT、HTTPS协议接入物联网平台。

## 设备管理

物联网平台为您提供功能丰富的设备管理服务。包括：生命周期、设备组、设备影子、固件升级、物模型、数据解析、在线调试、远程维护、数据存储、实时监控等。不同版本的物联网平台设备管理功能有所不同，具体请参考[产品规格](#)。

## 规则引擎

当设备基于Topic进行通信时，您可以编写SQL对Topic中的数据进行处理，然后配置转发规则将数据转发到其他Topic或阿里云服务上。例如：

- 可以转发到RDS、Table Store、HiTSDB中进行存储。
- 可以转发到DataHub中进而使用Streamcompute进行流计算，使用MaxCompute进行大规模离线计算；或转发到函数计算进行事件计算。
- 转发到消息队列MQ实现高可靠消费数据。
- 可以将Topic中的数据处理转发到另一个Topic中实现M2M通信。

## 安全认证&权限策略

安全是IoT的重要话题。阿里云物联网平台提供多重防护保障设备云端安全。

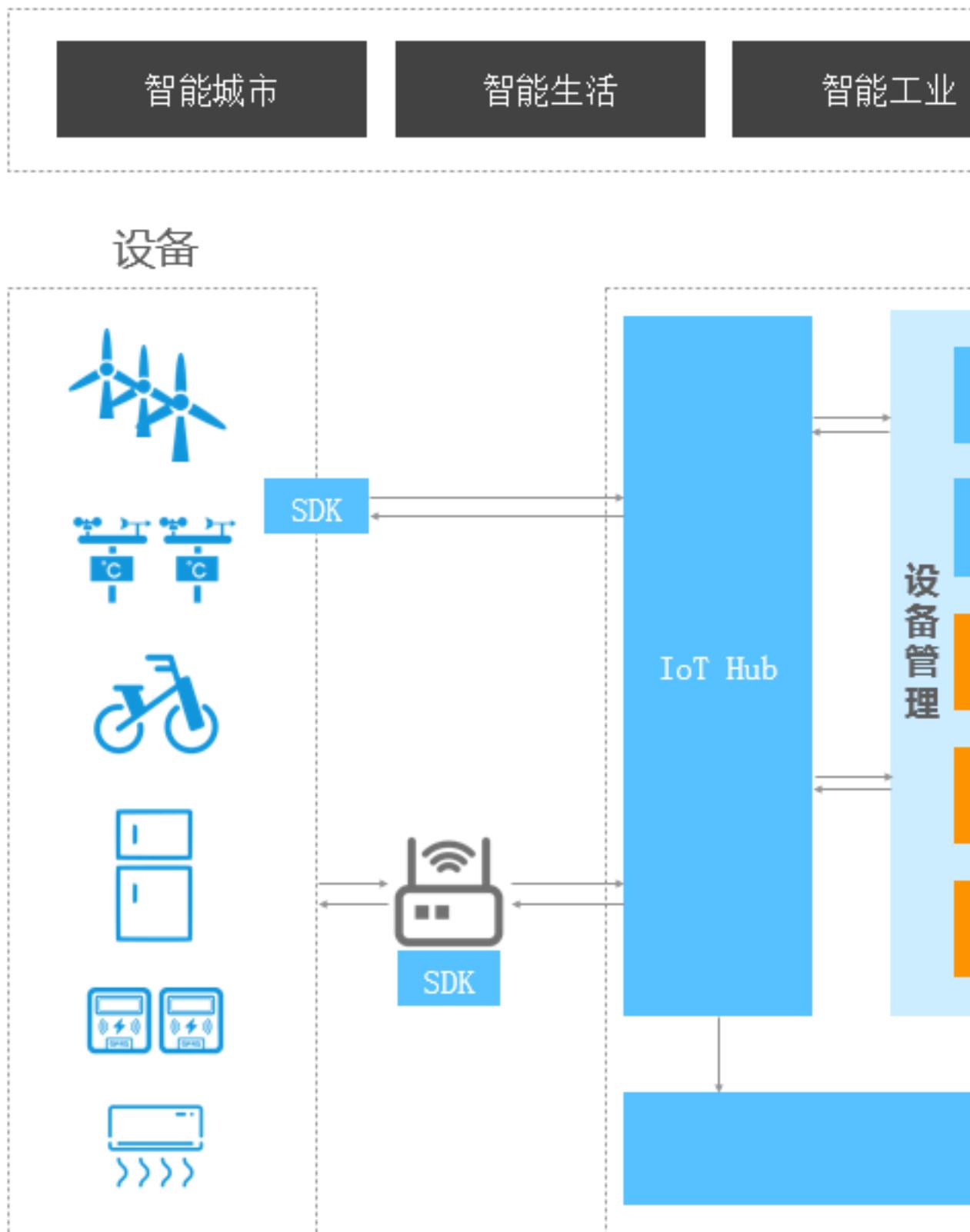
- 物联网平台为每个设备颁发唯一证书，设备使用证书进行身份验证连接IoT Hub。

- 针对不同安全等级和产线烧录的要求，物联网平台为开发者提供了多种设备认证方式。
- 授权粒度精确到设备级别，任何设备只能对自己所属的Topic发布订阅消息，服务端凭借阿里云AK对账号下所属的Topic进行操作。

## 3 产品规格

---

物联网平台有两种版本：基础版和高级版。下图中黄色模块是高级版特有的功能。



基础版

- 版本说明：提供安全可靠的亿级设备连接能力，提供基础的设备管理和固件升级能力，支持规则引擎进行数据引流。不支持设备数据的解析和存储。其他阿里云产品如存储、消息服务等需另外购买。
- 适用场景：开发者具有较强的软硬件实力，且希望能够灵活组合阿里云各产品搭建业务系统的场景。

高级版：

- 版本说明：在基础版所有功能的基础上，增加Alink协议支持、提供更加完整的设备全生命周期管理能力、支持设备模型定义、数据解析、在线调试和远程维护、提供数据存储，可实时获取设备运行状态或历史数据。
- 适用场景：需要较小的机器智能化周期，需要同时解决设备的数据格式和存储问题，需要开发者聚焦于垂直业务系统搭建等快速实现智能转型的场景。

基础版、高级版具体功能对比如下表：

功能	基础版	高级版
设备认证	√	√
设备连接	√	√
设备数据上行	√	√
设备远程控制	√	√
远程禁用设备	√	√
设备拓扑关系维护	√	√
设备影子	√	-
设备模型定义	-	√
云端脚本解析	-	√
设备数据存储	-	√
设备实时状态查询	√	√
设备历史数据查询	-	√
设备服务调用	-	√
设备事件上报	-	√
在线调试设备	-	√
设备位置轨迹	-	√

功能	基础版	高级版
远程配置设备	-	√
设备固件升级	√	√
日志分析	√	√
规则引擎	√	√

## 4 名词解释

本章主要介绍物联网平台中相关的产品名词。

### 产品名词解释

名词	描述
产品	设备的集合，通常指一组具有相同功能的设备。物联网平台为每个产品颁发全局唯一的ProductKey。每个产品下可以有成千上万的设备。
设备	归属于某个产品下的具体设备。物联网平台为设备颁发产品内唯一的证书 DeviceName。设备可以直接连接物联网平台，也可以作为子设备通过网关连接物联网平台。
网关	能够直接连接物联网平台的设备，且具有子设备管理功能，能够代理子设备连接云端。
子设备	本质上也是设备。子设备不能直接连接物联网平台，只能通过网关连接。
三元组	三元组指ProductKey、DeviceName、DeviceSecret。 <ul style="list-style-type: none"><li><b>ProductKey</b>：是物联网平台为产品颁发的全局唯一标识。该参数很重要，在设备认证以及通信中都会用到，因此需要您保管好。</li><li><b>DeviceName</b>：在注册设备时，自定义的或自动生成的设备名称，具备产品维度内的唯一性。该参数很重要，在设备认证以及通信中都会用到，因此需要您保管好。</li><li><b>DeviceSecret</b>：物联网平台为设备颁发的设备密钥，和DeviceName成对出现。该参数很重要，在设备认证时会用到，因此需要您保管好并且不能泄露。</li></ul>
ProductSecret	由物联网平台颁发的产品密钥，通常与ProductKey成对出现，可用于一型一密的认证方案。该参数很重要，需要您保管好，不能泄露。
Topic	Topic是UTF-8字符串，是发布/订阅（Pub/Sub）模型中消息的传输中介。可以向Topic发布或者订阅消息。
Topic类	同一产品下不同设备的Topic集合，用\${productkey}和\${deviceName}通配一个唯一的设备，一个Topic类对一个ProductKey下所有设备通用。
发布	操作Topic的权限类型，对应的英文名称为Pub，具有往Topic中发布消息的权限。
订阅	操作Topic的权限类型，对应的英文名称为Sub，具有从Topic中订阅消息的权限。

名词	描述
RRPC	全称：Revert-RPC。RPC ( Remote Procedure Call ) 采用客户机/服务器模式，用户不需要了解底层技术协议，即可远程请求服务。RRPC则可以实现由服务端请求设备端并能够使设备端响应的功能。
标签	标签分为产品标签和设备标签。 <ul style="list-style-type: none"><li>产品标签：描述同一个产品下，所有设备所具有的共性信息。</li><li>设备标签：通常根据设备的特性为设备添加的特有的标记，您可灵活自定义标签内容。</li></ul>
Alink	阿里云定义的设备与云端之间的通信协议。
物模型	是对设备在云端的功能描述，包括设备的属性、服务和事件。物联网平台通过定义一种物的描述语言来描述物模型，称之为 TSL ( 即 Thing Specification Language )，采用JSON格式，您可以根据TSL组装上报设备的数据。
属性	设备的功能模型之一，一般用于描述设备运行时的状态，如环境监测设备所读取的当前环境温度等。属性支持 GET 和 SET 请求方式。应用系统可发起对属性的读取和设置请求。
服务	设备的功能模型之一，设备可被外部调用的能力或方法，可设置输入参数和输出参数。相比于属性，服务可通过一条指令实现更复杂的业务逻辑，如执行某项特定的任务。
事件	设备的功能模型之一，设备运行时的事件，事件一般包含需要被外部感知和处理的通知信息，可包含多个输出参数。如，某项任务完成的信息，或者设备发生故障或告警时的温度等，事件可以被订阅和推送。
数据解析脚本	针对高级版产品中采用透传格式/自定义格式的设备，需要在云端编写数据解析脚本，将设备上报的二进制数据或自定义的JSON数据，转换为平台上的Alink JSON数据格式。
设备影子	是一个 JSON 文档，用于存储设备或者应用的当前状态信息。每个设备都会在云端有唯一的设备影子对应，无论该设备是否连接到 Internet，您都可以使用设备影子通过 MQTT 协议或 HTTP 协议获取和设置设备的状态。
规则引擎	提供类SQL语言的规则引擎，帮助您对Topic中的数据进行过滤，并能够将处理后的数据发送到阿里云其他服务，例如MNS、Table Store、DataHub等等。

## 5 产品优势

企业基于物联网通过运营设备数据实现效益提升已是行业趋势、业内共识。然而，物联网转型或物联网平台建设过程中往往存在各类阻碍。针对此类严重制约企业物联网发展的问题，阿里云物联网平台提供了一系列解决方案。

以下是传统开发与基于阿里云物联网平台开发的对比结果：

	传统开发	基于阿里云物联网平台的开发
设备接入	需要搭建基础设施、寻找并联合嵌入式开发人员与云端开发人员。 开发工作量大、效率低。	提供设备端SDK，快速连接设备上云，效率高。 同时支持全球设备接入、异构网络设备接入、多环境下设备接入、多协议设备接入。
性能	自行实现扩展性架构，极难做到从设备粒度调度服务器、负载均衡等基础设施。	具有亿级设备的长连接能力、百万级并发的能力，架构支撑水平性扩展。
安全	需要额外开发、部署各种安全措施，保障设备数据安全是个极大挑战。	提供多重防护保障设备云端安全： <ul style="list-style-type: none"><li>设备认证保障设备安全与唯一性</li><li>传输加密保障数据不被篡改</li><li>云盾护航、权限校验保障云端安全</li></ul>
稳定	需自行发现宕机并完成迁移，迁移时服务会中断。稳定性无法保障。	服务可用性高达99.9%。单点故障，自动迁移。
简单易用	需要购买服务器搭建负载均衡分布式架构，需要花费大量人力物力开发“接入 + 计算 + 存储”一整套物联网系统。	一站式设备管理、实时监控设备场景、无缝连接阿里云产品，物联网复杂应用的搭建灵活简便。

## 6 使用限制

物联网平台使用限制如下：

限制类别	描述
产品数量	单账号最多可以创建1000个产品。
设备数量	单个产品最多可以添加50万台设备。
网关与子设备	<ul style="list-style-type: none"><li>单个网关下最多添加1500个子设备。</li><li>单个网关下最多添加1000个子设备通道。</li></ul>
标签数量	单个产品、设备、分组最多分别可以添加100个标签。
数据解析脚本	数据解析上传的脚本文件大小不能超过48KB。
远程配置	远程配置文件，仅支持JSON格式，大小不能超过64KB。
功能定义（仅针对高级版产品）	单个产品可添加的功能上限为100个。
	struct类的属性，可添加的参数不超过10个。
	当功能的数据类型： <ul style="list-style-type: none"><li>为enum时，枚举项最多不超过25个。</li><li>为text时，数据长度不超过1024字节。</li><li>为array时，数组内的元素不超过128个</li></ul>
	服务中可添加的入参和出参分别不超过10个。
	事件中可添加的出参不超过10个。
Topic类	一个产品最多可以定义50个Topic类。
广播Topic	同一个Topic最多可以被1000个设备订阅，服务端SDK每秒只可发一条广播。
Topic的长度	不能超过128字节。
协议包大小	CoAP协议包不能超过1K。
	MQTT协议包不能超过256K。
通信	设备只能对自己的Topic进行消息发布与订阅。
设备订阅	订阅和取消订阅都是操作10秒后生效，一次订阅永久生效。建议您提前订阅Topic以免漏失信息。 示例：设备向Topic A发送SUB请求，10秒后，订阅生效，设备开始收到实时消息，除非取消订阅，设备将一直接收Topic A的消息。
规则引擎	单个账号最多可以设置1000条规则。

限制类别	描述
	<p>一条规则中转发数据的操作不能超过10个。</p> <p>数据转发性能依赖所转发的云产品实例，在云产品实例性能足够的情况下，规则引擎为单账号提供1000QPS数据转发能力。如果请求量超出该限制或云产品写入耗时超过1s，数据转发会被限流。</p> <p>数据转发依赖其他云产品，使用时需确保目标云产品实例正常。目标云产品的实例宕机、欠费、参数错误（如授权变更、值非法）、配置错误等异常状况将会导致消息流转失败。</p>
流量限制	<p>单个设备的数据：</p> <ul style="list-style-type: none"><li>上报上限QoS0为30条/秒，QoS1为10条/秒。</li><li>下行接收限制为50条/秒。</li><li>下行单设备最大带宽512K，同时受限于网络环境。如果网络tcp write buffer拥堵，将直接返回错误。比如，您通过Pub接口发指令给设备，如果设备接收不过来，将收到限流错误。</li></ul> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <b>说明：</b><p>MQTT的Pub上报消息限流，协议上是没有任何答应的。您可以通过日志服务发现设备被限流的警告。</p></div> <p>云端API接口限制：</p> <ul style="list-style-type: none"><li>单个IP：默认单个IP入口调用API的限制是100QPS。</li><li>单个帐号：每个接口业务上有限流，比如 RRPC为500QPS，Pub 1500QPS，其它接口如无特别说明默认50QPS。</li></ul> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <b>说明：</b><ul style="list-style-type: none"><li>若以上限制不满足您的业务需求，请提工单说明业务情况和所需额度。</li><li>若您调用接口收到限流报错，像<a href="#">公共错误</a>中29-31类型报错，可以重新尝试调用。</li></ul></div>