

Alibaba Cloud

Key Management Service Product Introduction

Document Version: 20220627

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 <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.What is Key Management Service?	05
2.Benefits	08
3.Common scenarios	10
4.Terms	14
5.Limits	16

1. What is Key Management Service?

Key Management Service (KMS) is an end-to-end service platform for key management and data encryption. KMS provides simple, reliable, secure, and standard-compliant capabilities to encrypt and protect data. KMS greatly reduces your costs of procurement, O&M, and research and development (R&D) on cryptographic infrastructure and data encryption products. This way, you can focus more on your business.

Functions and features

KMS consists of four components: Key Service, Secrets Manager, Certificates Manager, and Dedicated KMS.

Component	Description	References
Key Service	Key Service fully manages and protects your keys. Key Service supports data encryption and digital signature in simple mode based on cloud-native API operations.	Overview
Secrets Manager	Secrets Manager provides the secret encryption, secret hosting, regular rotation, secure distribution, and centralized management features. Secrets Manager reduces the security risks caused by static secrets that are configured in traditional IT facilities.	Overview
Certificates Manager	Certificates Manager provides highly available and secure capabilities to manage keys and certificates. Certificates Manager also allows you to obtain certificates to generate and verify signatures.	Overview
Dedicated KMS	Dedicated KMS is a key management service that you can fully manage. For example, you can specify the virtual private cloud (VPC) in which Dedicated KMS is deployed and configure the cryptographic resource pool used by Dedicated KMS. You can also define role-based access control (RBAC) policies to allow access from applications.	Overview

Benefits

The following table lists the benefits of each feature.

Feature	Benefit	Description	References
	Leading security compliance capabilities	KMS supports industry-leading cryptographic infrastructure and meets your security level and security compliance requirements.	Compliance

Feature	Benefit	Description	References
Key Service	Fully managed implementation	You do not need to procure cryptographic hardware or software. You do not need to invest in O&M or R&D of cryptographic facilities. You can directly use the features provided by Key Service and extend the features.	Use managed HSMs
	Cloud-native capabilities	KMS can be integrated with a variety of Alibaba Cloud services based on cloud-native API operations. KMS allows you to configure server-side encryption (SSE) with only a few clicks.	Alibaba Cloud services that can be integrated with KMS
	Simplified application access	KMS provides multiple methods such as KMS SDKs and Encryption SDKs to help you use the KMS encryption API. This way, you can encrypt and decrypt data, as well as generate and verify digital signatures in a convenient manner.	<ul style="list-style-type: none"> Code samples of KMS SDK for Java Quick start of Encryption SDK for Java
	Centralized and large-scale management	KMS can be automatically activated and supports services such as Resource Orchestration Service (ROS) and Terraform. KMS allows you to implement automatic data encryption for multi-account logons by using the default encryption policy. KMS automatically enables SSE for resources such as Elastic Compute Service (ECS) instances that use cloud disks, Object Storage Service (OSS) buckets, ApsaraDB RDS instances, and MaxCompute projects.	Activate KMS by using the API
Secrets Manager	Cloud-native capabilities	KMS generates dynamic ApsaraDB RDS secrets based on cloud-native API operations, which helps you handle the major security threats to databases.	Overview
	Simplified application access	KMS provides multiple methods such as KMS SDKs, Secrets Manager Client, and the Kubernetes plug-in to help you use dynamic secrets.	Connect an application to Secrets Manager
	Centralized and large-scale management	KMS can be automatically activated and supports services such as ROS and Terraform. KMS allows you to implement the automatic orchestration of Alibaba Cloud resources such as databases and OSS buckets, and the automatic management of secrets. The secrets are fully managed in Secrets Manager. This achieves centralized secret management.	Activate KMS by using the API

Feature	Benefit	Description	References
Certificates Manager	Secure key storage	Certificates Manager uses managed hardware security modules (HSMs) to ensure that keys and certificates are securely generated and stored.	Overview
	Lifecycle management	Certificates Manager allows you to manage keys and certificates. You can generate certificate signing requests (CSRs), import certificates and certificate chains, verify the signatures of certificate chains, and check certificate validity.	<ul style="list-style-type: none">• Quick start• Import private keys and certificates
	Easy API-based integration	Certificates Manager provides multiple API operations to help you integrate a certificate service with your development environment, accelerate product deployment, and roll out certificate-related features.	Certificate operations
Dedicated KMS	Access over private networks	Dedicated KMS allows you to deploy a tenant-specific instance in the VPC of the tenant. This way, Dedicated KMS is accessible over a private network.	Overview
	Resource isolation and cryptographic isolation	Dedicated KMS uses a tenant-specific cryptographic resource pool to implement resource isolation and cryptographic isolation. This improves security. The pool is also called an HSM cluster.	Overview
	Key management	Dedicated KMS allows you to use HSMs in an easier manner. Dedicated KMS provides upper-layer key management and cryptographic operation services for HSMs in a stable and easy manner.	Overview
	Integration with multiple Alibaba Cloud services	Dedicated KMS allows you to integrate your HSMs with Alibaba Cloud services in a seamless manner. This helps improve encryption security and controllability for Alibaba Cloud services.	Alibaba Cloud services that can be integrated with KMS

Related information

- [Benefits](#)
- [Common scenarios](#)
- [Terms](#)
- [Limits](#)
- [Billing of KMS](#)
- [Overview](#)

2. Benefits

Compared with key management infrastructure (KMI), Key Management Service (KMS) features multi-service integration, ease of use, high reliability, and cost-effectiveness.

Multi-service integration

- Authentication and access control

KMS authenticates the validity of requests by using AccessKey pairs. KMS is integrated with Resource Access Management (RAM). This allows you to configure a variety of custom policies to meet requirements in different authorization scenarios. Requests that are initiated by valid users and pass attribute-based access control (ABAC) of RAM can be accepted by KMS. For more information, see [Use RAM to control access to KMS resources](#).

- Key usage auditing

KMS is integrated with ActionTrail. This allows you to view the recent KMS usage and store the KMS usage information in other services such as OSS to meet audit requirements in the long term. For more information, see [Use ActionTrail to query KMS event logs](#).

- Data encryption for integrated cloud services

KMS is integrated with multiple Alibaba Cloud services such as ECS, ApsaraDB for RDS, and OSS. You can easily use customer master keys (CMKs) in KMS to encrypt and control the data stored in these services and maintain control over the cloud computing and storage environments. You only need to pay for the service and do not need to implement complex encryption capabilities. In addition, KMS also protects native data of these services. For more information, see [Integration with KMS and Alibaba Cloud services that can be integrated with KMS](#).

Ease of use

- Easy encryption

KMS simplifies abstract cryptographic concepts and provides cryptographic API operations that allow you to easily encrypt and decrypt data. For applications that require a key hierarchy, KMS provides convenient envelope encryption to quickly implement the key hierarchy: It generates data keys (DKs) and uses CMKs as key encryption keys (KEKs) to protect DKs. For more information, see [What is envelope encryption?](#)

- Centralized key hosting

KMS provides centralized key hosting and control.


- You can create a new CMK at any time and use RAM to easily manage who can access the CMK.
- You can use ActionTrail to audit key usage.
- You can import keys to KMS from KMI or from hardware security modules (HSMs) of Data Encryption Service. For keys that are imported from external sources or created in KMS, their confidential information or sensitive data is used by other Alibaba Cloud services for data encryption and protection.

- BYOK

KMS supports Bring Your Own Key (BYOK). You can import your own keys to KMS to encrypt data on the cloud. This facilitates key management. You can import the following types of keys to KMS:

- Keys in your on-premises KMI

- Keys in user-managed HSMs of Alibaba Cloud Data Encryption Service

 **Note** Keys imported to managed HSMs in KMS cannot be exported by using any method because secure key exchange algorithms are used in KMS. Operators or third parties are not allowed to check the plaintext of keys. For more information, see [Import key material](#) and [Key control](#).

- Custom key rotation policies

KMS supports automatic rotation of symmetric encryption keys based on security policies. You only need to configure a custom rotation cycle for a CMK. KMS automatically generates new CMK versions. A CMK can have multiple key versions. Each version can be used to decrypt corresponding ciphertext data. The latest key version (called the primary version) is an active encryption key and is used to encrypt current data. For more information, see [Automatic key rotation](#).

High reliability, availability, and scalability

As a fully managed distributed service, KMS builds multi-zone redundant cryptographic computing capabilities in each region. This ensures that Alibaba Cloud services and your custom applications can send requests to KMS with low latency. You can create many keys in KMS across multiple regions based on your business requirements without the need to scale the underlying infrastructure.

Security and compliance

KMS has passed strict security design and verification to ensure stringent protection of your keys on the cloud.

- KMS only provides TLS-based access channels and uses secure transmission encryption algorithm suites. It complies with security standards such as PCI DSS.
- KMS provides cryptographic facilities verified and certified by regulatory agencies. It offers HSMs that are tested and certified by State Cryptography Administration (SCA) or have passed FIPS 140-2 Level 3 validation. For more information, see [Compliance](#).
- KMS uses HSMs to host keys for higher levels of security. For more information, see [Overview](#).

Low costs

With KMS, you only pay for the resources that you use.

- You do not need to pay for the initial cost of HSMs, as well as the cost of operating, maintaining, repairing, and replacing HSMs.
- KMS reduces the costs of building highly available and reliable cryptographic device clusters and reduces the R&D and maintenance costs for user-created key management facilities.
- KMS is integrated with other cloud services to eliminate the R&D overhead of a data encryption system. You only need to manage keys to achieve controllable data encryption on the cloud.

3.Common scenarios

Key Management Service (KMS) is applicable to a wide range of scenarios. This topic describes the typical scenarios in which you can use KMS.

Typical scenarios

Role	Demand	Typical scenario	Solution
Application developer	Make sure the security of sensitive data in applications.	An application developer needs to use sensitive business data and operating data in an application. The application developer wants to encrypt the sensitive data and use KMS to protect the encryption keys.	Encrypt and protect sensitive data
IT operations and maintenance (O&M) engineer	Provide a secure environment for IT facilities deployed in the cloud.	The IT infrastructure in the cloud is shared with other tenants. As a result, an IT O&M engineer cannot establish physical security boundaries in the cloud like in traditional data centers. However, the IT O&M engineer still needs to build a trusted, visible, and controllable security mechanism for the cloud computing and storage hosting environment.	Control the cloud computing and storage environment
Chief security officer (CSO)	Make sure the security and compliance of information systems.	A CSO needs to meet key management requirements in some compliance standards and use cryptographic technologies to meet more requirements for application and information system security.	Help information systems meet compliance requirements
Independent service vendor (ISV)	Use third-party encryption to provide security capabilities for a service.	An ISV is asked by customers to encrypt and protect user data in a service. <ul style="list-style-type: none">The ISV wants to focus on developing business features rather than implementing key management and distribution features.Customers hope that the ISV provide controllable and reliable capabilities to encrypt and protect data.	Provide a third-party encryption solution for ISVs

Encrypt and protect sensitive data

You can use data encryption to protect sensitive data generated or stored in the cloud. Alibaba Cloud provides multiple ways to encrypt and protect sensitive data.

Encryption method	Description	Related topic
-------------------	-------------	---------------

Encryption method	Description	Related topic
Envelope encryption	<p>The envelope encryption feature stores your customer master keys (CMKs) in KMS. You only need to deploy enveloped data keys (EDKs). You can use KMS to decrypt the EDKs and use the returned plaintext data keys (DKs) to encrypt or decrypt your local business data.</p> <p>You can also use Encryption SDK in which the envelope encryption feature is encapsulated to encrypt data.</p>	<ul style="list-style-type: none">• What is envelope encryption?• Use envelope encryption to encrypt and decrypt local data• Quick start of Encryption SDK for Java
Direct encryption	You can call the Encrypt API operation of KMS to directly encrypt sensitive data by using CMKs.	Use a KMS CMK to encrypt and decrypt data online
Server-side encryption (SSE)	If you use Alibaba Cloud services to store data, you can use the SSE feature of these services to encrypt and protect data in an effective way. For example, you can use the SSE feature of Object Storage Service (OSS) to protect buckets that store sensitive data or use transparent data encryption (TDE) to protect tables that store sensitive data.	Alibaba Cloud services that can be integrated with KMS
Secrets Manager-based encryption	You can host sensitive data, such as passwords, tokens, SSH keys, and AccessKeys, in Secrets Manager and manage them by using a secure method. You can also dynamically rotate secrets to prevent data leaks.	<ul style="list-style-type: none">• Rotate generic secrets• Overview

Control the cloud computing and storage environment

You can integrate KMS with other Alibaba Cloud services to use the SSE feature. This way, you can control the cloud computing and storage environment, and isolate and protect your computing and storage resources in a distributed multi-tenant system. You can control the distributed computing and storage environment by managing the lifecycle, usage status, and access control policies for CMKs in KMS. You can also integrate KMS with ActionTrail to check and audit key usage in KMS. KMS is typically used in the scenarios that are described in the following table to control the cloud computing and storage environment.

Scenario	Description	Related topic
Elastic Compute Service (ECS)	After you authorize ECS to use KMS keys, ECS can encrypt and protect system disks, data disks, snapshots, and images. For example, to start an ECS instance, you must decrypt both the system disk and data disk. You must encrypt snapshots that are created from encrypted disks. These limits enhance the security of ECS instances and storage resources by using KMS.	Encryption overview

Scenario	Description	Related topic
Persistent storage	The persistent storage services provided by Alibaba Cloud, such as ApsaraDB RDS, OSS, and Apsara File Storage NAS, ensure data storage reliability by using the distributed and redundancy method. When KMS is integrated with these services to encrypt data before the data is stored, data redundancy in distributed systems becomes controllable and visible. For any read requests, data must first be decrypted by KMS.	N/A
Other computing and storage scenarios	Multiple Alibaba Cloud services support integration with KMS.	Alibaba Cloud services that can be integrated with KMS

Help information systems meet compliance requirements

Enterprises or organizations may encounter the following situations when they evaluate the compliance requirements for cryptographic technologies:

- Compliance regulations require that information systems be protected by cryptographic technologies and that the cryptographic technologies meet relevant technical standards and security specifications.
- Although the use of cryptographic technologies is not mandatory in compliance specifications, it conduces to the compliance process. For example, the use of cryptographic technologies helps you obtain higher scores in scoring rules.

KMS provides the capabilities that are described in the following table to help enterprises meet compliance requirements.

Feature	Description	Related topic
Cryptographic compliance	KMS supports managed hardware security modules (HSMs). The managed HSMs are third-party hardware devices that are certified by regulatory agencies. They run in an approved security mode. The managed HSMs have passed the certification by State Cryptography Administration (SCA) and FIPS 140-2 Level 3 validation.	<ul style="list-style-type: none">• Overview• Use managed HSMs
Key rotation	KMS supports automatic rotation of encryption keys. Enterprises can customize rotation policies to meet data security specifications and best practices.	<ul style="list-style-type: none">• Overview• Automatic key rotation
Secret rotation	You can use Secrets Manager to meet the rotation requirement for secrets such as passwords and AccessKeys. In addition, you can enjoy effective and reliable emergency response to data leaks.	Rotate generic secrets
Data confidentiality	KMS allows you to encrypt and protect personal privacy data. This help you prevent privacy leaks when your system are attacked and meet the requirements of laws and regulations related to data protection.	N/A

Feature	Description	Related topic
Data integrity	KMS is integrated with Log Service and ActionTrail. You can use KMS to encrypt logs of Alibaba Cloud services to prevent the logs from being tampered with. In addition, KMS ensures the confidentiality and integrity of log data.	N/A
Authentication and access control	KMS is integrated with Resource Access Management (RAM) to implement centralized authentication and authorization.	Use RAM to control access to KMS resources
Key usage auditing	KMS stores all API call records in ActionTrail, which allows you to perform compliance auditing on key usage.	Use ActionTrail to query KMS event logs

Provide a third-party encryption solution for ISVs

As an ISV, you can integrate KMS as a third-party data security solution to protect the data of customers in your services. After you allow customers to manage keys in KMS and authorize ISV services to use these keys, KMS acts as a third-party security protection system between the ISV services and customers. Customers and ISV services can work together to protect system security.

Role	Description	Related topic
Customer administrator	An administrator generates keys in KMS and manages their lifecycle. The administrator can use RAM to manage the permissions on keys. The administrator can allow ISV services to use specified keys in KMS by using methods such as resource authorization across Alibaba Cloud accounts.	Use a RAM role to grant permissions across Alibaba Cloud accounts
ISV service	An ISV service uses the specified keys to encrypt and protect data by integrating KMS API.	List of operations by function
Customer auditor	An auditor uses ActionTrail to audit the usage records of keys in KMS.	Use ActionTrail to query KMS event logs

4. Terms

This topic introduces the terms that are used in Key Management Service (KMS).

Term	Description
Key Service	<p>Key Service fully manages and protects your keys. Key Service supports data encryption and digital signature in simple mode based on cloud-native API operations.</p> <p>For more information about Key Service, see Overview.</p>
customer master key (CMK)	<p>A CMK is used to encrypt data keys and generate enveloped data keys (EDKs). A CMK can also be used to encrypt a small volume of data. You can call the CreateKey operation to create a CMK.</p>
key material	<p>Key material is required when you perform cryptographic operations. To make sure that you can perform cryptographic operations based on the key material, we recommend that you keep the key material confidential. Key material can be encrypted by using private keys of asymmetric cryptographic algorithms or by using symmetric cryptographic algorithms.</p> <p>CMKs are basic resources of KMS. A CMK is composed of a key ID, basic metadata, and key material. By default, key material is generated by KMS when you create a CMK. In this case, the value of the Origin parameter is Aliyun_KMS. You can also set the Origin parameter to EXTERNAL when you create a CMK. In this case, KMS does not generate key material, and you must import external key material for the CMK.</p> <p>For more information about key material, see Import key material.</p>
envelope encryption	<p>To encrypt business data, you can call the GenerateDataKey or GenerateDataKeyWithoutPlaintext operation to generate a symmetric key and use a specified CMK to encrypt the symmetric key. An EDK is generated. The EDK is secure even if it is stored and transferred over unsecured communication channels. If you want to use the symmetric key, you need only to call the Decrypt operation to decrypt the EDK.</p> <p>For more information about envelope encryption, see What is envelope encryption?.</p>
data key	<p>A data key is a plaintext key that is used to encrypt data.</p> <p>You can call the GenerateDataKey operation to generate a data key, use a specified CMK to encrypt the data key, and then obtain the plaintext and ciphertext of the data key.</p>
enveloped data key or encrypted data key	<p>An EDK is a ciphertext data key that is generated by using envelope encryption.</p> <p>If the plaintext of a data key is not needed, you can call the GenerateDataKeyWithoutPlaintext operation to obtain only the ciphertext of the data key.</p>

Term	Description
hardware security module (HSM)	<p>An HSM is a hardware device that performs cryptographic operations and securely generates and stores keys. KMS provides the Managed HSM feature. This feature meets both the testing and validation requirements of regulatory agencies. This feature provides you with high security for your keys that are managed in KMS.</p> <p>For more information about HSMs, see Overview.</p>
encryption context	<p>An encryption context refers to the encapsulation of authenticated encryption with associated data (AEAD) in KMS. For more information about AEAD, see An Interface and Algorithms for Authenticated Encryption. KMS uses the imported encryption context as the additional authenticated data (AAD) to support cryptographic operations in which symmetric encryption algorithms are used. The encryption context helps improve the integrity and authenticity of data that needs to be encrypted.</p> <p>For more information about encryption contexts, see EncryptionContext.</p>
Secrets Manager	<p>Secrets Manager allows you to manage your secrets throughout their lifecycle and allows applications to use secrets in a secure and efficient manner. This prevents sensitive data leaks that are caused by hardcoded secrets.</p> <p>For more information about Secrets Manager, see Overview.</p>
application access point	<p>An application access point (AAP) is a method that is originally used by KMS to authenticate the identity of the user that accesses KMS resources.</p> <p>For more information, see Manage AAPs.</p>
Certificates Manager	<p>Certificates Manager provides highly available and secure capabilities to manage keys and certificates. Certificates Manager also allows you to obtain certificates to generate and verify signatures.</p> <p>For more information about Certificates Manager, see Overview.</p>
Dedicated KMS	<p>Dedicated KMS is a key management service that you can fully manage. For example, you can specify the virtual private cloud (VPC) in which Dedicated KMS is deployed and configure the cryptographic resource pool used by Dedicated KMS. You can also define role-based access control (RBAC) policies to allow access from applications.</p> <p>For more information about Dedicated KMS, see Overview.</p>

5.Limits

This topic describes the limits of Key Management Service (KMS).

KMS is a region-specific service. The limits of KMS vary based on regions. For more information about the regions supported by KMS, see the "Endpoints" section of the [Request method](#) topic.

Resource quotas

KMS defines resource quotas to provide fast and elastic capabilities. Some resource quotas apply to the resources that you create, but do not apply to the resources that are created by Alibaba Cloud. If the resources that you use do not belong to your Alibaba Cloud account, the resources are not counted in your resource quotas.

If the quota of a resource is exhausted, the system reports the error `Rejected.LimitExceeded` for new requests to create this type of resource.

The following table describes the KMS resource quotas for each Alibaba Cloud account in a region.

Resource type	Default quota	Description
Customer master key (CMK)	200	The maximum number of CMKs that you can create in a region
Alias	300	The maximum number of aliases that you can create in a region
CMK version	10000	The maximum number of versions for all CMKs that you can create in a region

Request quotas

KMS defines quotas for the number of API operations that you can call per second. When a request quota is exceeded, KMS blocks valid requests and returns an error similar to the following code. This type of error can be fixed by retries. You can configure the request backoff and retry policies for your application. For more information, see [Use the exponential backoff method to retry requests](#).

```
{
  "HttpStatus": 429
  "Code": "Rejected.Throttling"
  "Message": "QPS Limit Exceeded"
  "RequestId": "e85db688-a2d3-44ca-9790-4259etas154f"
}
```

The following table describes the KMS request quotas for each Alibaba Cloud account in a region.

Default request quotas for CMKs per second

CMK specification	Create operation	Cryptographic operation	Read-only operation	Write operation
<ul style="list-style-type: none">Aliyun_AES_256Aliyun_SM4	10	750	20	10

CMK specification	Create operation	Cryptographic operation	Read-only operation	Write operation
<ul style="list-style-type: none">RSA_2048RSA_3072	10	200	20	10
<ul style="list-style-type: none">EC_P256EC_P256KEC_SM2	10	200	20	10

The default request quotas for CMKs are grouped by operation. All operations in a group share the request quota for the group. The following groups are defined:

- Create operation group: includes only the CreateKey operation. For more information, see [CreateKey](#).
- Cryptographic operation group: includes the cryptographic operations for a specific CMK. For more information, see [Key service operations](#).
- Read-only operation group: includes the operations that are related to CMKs, aliases, and CMK tags but do not change the metadata, properties, or status of resources.
- Write operation group: includes the operations that are related to CMKs, aliases, and CMK tags and change the metadata, properties, or status of resources.